

BVMS

Table des matières

1	Utilisation de l'aide	14
1.1	Recherche d'informations	14
1.2	Impression de l'aide	15
2	Signification des messages de sécurité	16
3	Introduction	17
3.1	Éditions BVMS	18
3.2	Vue d'ensemble de l'activation de la licence BVMS	19
4	Vue d'ensemble du système	21
4.1	Configuration matérielle requise	22
4.2	Configuration logicielle requise	22
4.3	Licences nécessaires	22
5	Concepts	23
5.1	Concepts de conception BVMS	23
5.1.1	Système Management Server unique	23
5.1.2	Enterprise System	24
5.1.3	Server Lookup	25
5.1.4	Unmanaged site	26
5.2	Enregistrement	28
5.2.1	Automated Network Replenishment (ANR)	28
5.2.2	Enregistrement double/de basculement	29
5.2.3	Modes d'enregistrement VRM	31
5.2.4	Lecture de sources d'enregistrements VRM	33
5.2.5	Vue d'ensemble des événements liés au stockage	38
5.3	Gestion des alarmes	39
5.4	Mappage des événements ONVIF	41
5.5	Déconnexion en cas d'inactivité	42
5.6	Operator Client non dépendant de la version	43
5.6.1	Utilisation du mode Compatibilité	43
5.7	Affichage des modes d'une caméra panoramique	43
5.7.1	Caméra panoramique à 360 ° - fixée au sol ou au plafond	44
5.7.2	Caméra panoramique à 180 ° - fixée au sol ou au plafond	46
5.7.3	Caméra panoramique à 360 ° - fixée au mur	47
5.7.4	Caméra panoramique à 180 ° - fixée au mur	48
5.7.5	Vue recadrée sur une caméra panoramique	49
5.8	Tunnelisation SSH	50
5.9	Trajets multiples	50
5.10	Open ID Connect (OIDC) et fournisseur d'identité (IDP)	51
6	Matériel pris en charge	52
6.1	Installation du matériel	53
6.2	Installation d'un clavier KBD universel XF	53
6.3	Connexion d'un clavier IntuiKey Bosch à BVMS	53
6.3.1	Scénarios de connexion d'un clavier numérique IntuiKey de Bosch	54
6.3.2	Connexion d'un clavier numérique IntuiKey de Bosch à un décodeur	56
6.3.3	Mise à jour du firmware clavier numérique IntuiKey de Bosch	56
6.4	Connexion de la matrice Bosch Allegiant à BVMS	57
6.4.1	Présentation de la connexion Bosch Allegiant	57
6.4.2	Configuration du canal de contrôle	59
6.4.3	Concept de Bosch Allegiant Satellite System	61

6.5	Commandes Allegiant CCL prises en charge dans BVMS	62
7	Utiliser les derniers logiciels	64
8	Mise en route	65
8.1	Installation des modules logiciels	65
8.2	Utilisation de l'assistant de configuration	65
8.3	Démarrage de Configuration Client	72
8.4	Configuration de la langue de Configuration Client	73
8.5	Configuration de la langue de Operator Client	73
8.6	Recherche de périphériques	74
8.7	Accès au système	74
8.8	Utilisation de la recherche de serveur	74
8.9	Activation des licences des logiciels	75
8.9.1	Boîte de dialogue Gestionnaire de licences (menu Outils)	76
8.9.2	Ajouter la boîte de dialogue de licence	77
8.9.3	Boîte de dialogue Inspecteur de licence (menu Outils)	77
8.10	Maintenance de BVMS	77
8.11	Remplacement d'un périphérique	78
8.11.1	Remplacement d'un serveur/serveur d'entreprise	79
8.11.2	Remplacement d'un VRM	80
8.11.3	Remplacement d'un encodeur ou d'un décodeur	81
8.11.4	Remplacement d'un Operator Client	84
8.11.5	Tests finaux	84
8.11.6	Récupération de Divar IP 3000/7000	84
8.12	Configuration de la synchronisation temporelle	84
8.13	Configuration du support de stockage d'un encodeur	84
9	Création d'un système d'entreprise	86
9.1	Configuration de la liste des serveurs pour le système d'entreprise	86
9.2	Création d'un Enterprise User Group	87
9.3	Création d'un Enterprise Account	88
9.4	Authentification basée sur les jetons	88
10	Configuration de Scripts de Commande	90
10.1	Gestion des Scripts de Commande	90
10.2	Configuration d'un Script de Commande à exécution automatique	91
10.3	Importation d'un Script de Commande	91
10.4	Exportation d'un Script de Commande	92
10.5	Configuration d'un script de commande de démarrage (page des paramètres)	92
11	Gestion des données de configuration	93
11.1	Activation de la configuration en cours d'utilisation	93
11.2	Activation d'une configuration	94
11.3	Exportation de données de configuration	95
11.4	Importation de données de configuration	95
11.5	Exportation de données de configuration vers OPC	96
11.6	Vérification de l'état de vos encodeurs/décodeurs	96
11.7	Configuration de la surveillance SNMP	96
11.8	Création d'un rapport	97
12	Exemples de configuration	98
12.1	Ajout d'une interface ATM/POS Bridge Bosch	98
12.2	Ajout d'une alarme d'entrée Bosch Allegiant	99
12.3	Ajout et configuration de 2 caméras IP Dinion avec enregistrement VRM	99

13	Fenêtres générales de Configuration Client	101
13.1	Fenêtre de configuration	101
13.2	Commandes des menus	102
13.3	Boîte de dialogue Gestionnaire d'activation (menu Système)	105
13.4	Boîte de dialogue Activer la configuration (menu Système)	105
13.5	Boîte de dialogue Recherche de dispositif initiale (menu Matériel)	106
13.6	Boîte de dialogue Protéger les dispositifs avec un mot de passe global par défaut (menu Matériel)	106
13.7	Boîte de dialogue Protéger les stockages iSCSI avec un mot de passe CHAP (menu Matériel)	107
13.8	Boîte de dialogue de changement des mots de passe (Menu Matériel)	107
13.9	Boîte de dialogue de mise à jour du firmware du dispositif (menu Matériel)	108
13.10	Boîte de dialogue de modification des paramètres IP et réseau de dispositif (menu Matériel)	109
13.11	Boîte de dialogue Moniteur de dispositifs (menu Matériel)	111
13.12	Boîte de dialogue Éditeur de Script de Commande (menu Outils)	112
13.13	Boîte de dialogue Gestionnaire de ressources (menu Outils)	112
13.14	Boîte de dialogue Générateur de séquence (menu Outils)	112
13.15	Boîte de dialogue Gestionnaire de licences (menu Outils)	112
13.15.1	Ajouter la boîte de dialogue de licence	113
13.16	Boîte de dialogue Inspecteur de licence (menu Outils)	113
13.17	Boîte de dialogue Surveillance de la station de travail (menu Outils)	114
13.18	Boîtes de dialogue des rapports (menu Rapports)	114
13.18.1	Boîte de dialogue Planifications d'Enregistrement	114
13.18.2	Boîte de dialogue Paramètres d'enregistrement planifié	114
13.18.3	Boîte de dialogue Planifications de Tâches	114
13.18.4	Boîte de dialogue des paramètres de caméra et d'enregistrement	115
13.18.5	Boîte de dialogue Paramètres de qualité du flux	115
13.18.6	Boîte de dialogue des paramètres d'événement	115
13.18.7	Boîte de dialogue des paramètres d'événements combinés	115
13.18.8	Boîte de dialogue Paramètres d'alarme	115
13.18.9	Boîte de dialogue des utilisateurs configurés	115
13.18.10	Boîte de dialogue Groupes d'utilisateurs et Comptes	115
13.18.11	Boîte de dialogue Autorisations de périphérique	115
13.18.12	Boîte de dialogue Autorisations d'exploitation	116
13.18.13	Boîte de dialogue Autorisations de configuration	116
13.18.14	Boîte de dialogue Autorisations d'un groupe d'utilisateurs	116
13.18.15	Boîte de dialogue Paramètres de sécurité	116
13.18.16	Boîte de dialogue Autorisations d'application	116
13.18.17	Boîte de dialogue Dispositifs exclus	116
13.19	Boîte de dialogue Paramètres de l'alarme (menu Paramètres)	116
13.20	Boîte de dialogue Paramètres SNMP (menu Paramètres)	116
13.21	Boîte de dialogue Paramètres du serveur LDAP (menu Paramètres)	117
13.21.1	Association d'un groupe LDAP	119
13.22	Boîte de dialogue Définir un groupe d'utilisateurs LDAP (menu Paramètres)	120
13.23	Boîte de dialogue Access token settings (Paramètres de jeton d'accès) (menu Paramètres)	120
13.24	Boîte de dialogue Trusted certificate settings (Paramètres du certificat approuvé) (menu Paramètres)	121
13.25	Boîte de dialogue Options (menu Paramètres)	122
14	Page Périphériques	126
14.1	Mise à jour de l'état et des fonctions et des périphériques	126

14.2	Modification du mot de passe des périphériques IP	127
14.3	Ajout d'un dispositif	127
14.4	Page Liste de serveurs / Carnet d'adresses	130
14.4.1	Boîte de dialogue Ajouter Serveur	131
14.4.2	Configuration de Server Lookup	132
14.4.3	Configuration de la liste des serveurs	132
14.4.4	Exportation de la liste des serveurs	132
14.4.5	Importation d'une liste de serveurs	133
14.5	Page DVR (enregistreur vidéo numérique)	133
14.5.1	Périphériques DVR	133
14.5.2	Ajout d'un dispositif DVR via un balayage	134
14.5.3	Boîte de dialogue Ajouter un DVR	135
14.5.4	Onglet Paramètres	135
14.5.5	Onglet Caméras (Caméras)	135
14.5.6	Onglet Entrées	136
14.5.7	Onglet Relais	136
14.5.8	Configuration de l'intégration d'un DVR	136
14.6	Page Commutateurs Matriciels	136
14.6.1	Ajout d'un dispositif Allegiant Bosch	137
14.6.2	Configuration d'un périphérique Bosch Allegiant	137
14.6.3	Page Sorties	137
14.6.4	Page Entrées	138
14.6.5	Page Connexion	139
14.6.6	Page Caméras	139
14.7	Page Poste de commande	139
14.7.1	Ajout manuel d'un poste de commande	140
14.7.2	Configuration d'un clavier numérique IntuiKey de Bosch (page des paramètres) (poste de commande)	140
14.7.3	Configuration d'un script de commande de démarrage (page des paramètres)	141
14.7.4	Page Paramètres	141
14.7.5	Modification de l'adresse réseau d'un poste de commande	143
14.8	Page Décodeurs	143
14.8.1	Ajout manuel d'un encodeur	143
14.8.2	Boîte de dialogue Modifier encodeur / décodeur	145
14.8.3	Modification du mot de passe d'un encodeur / décodeur (modifier mot de passe / entrer mot de passe)	146
14.8.4	Profil de décodeur	147
14.8.5	Affichage sur moniteur	148
14.8.6	Configuration d'un clavier numérique IntuiKey de Bosch (décodeur)	148
14.8.7	Configuration d'un décodeur pour une utilisation avec un clavier numérique IntuiKey de Bosch	148
14.8.8	Supprimer le logo du décodeur	149
14.9	Page Groupes de moniteurs	149
14.9.1	Ajout manuel d'un groupe de moniteurs	149
14.9.2	Configuration d'un groupe de moniteurs	150
14.10	Page Périphériques de communication	150
14.10.1	Ajout d'un serveur de messagerie/SMTP	151
14.10.2	Page Serveur SMTP	151
14.10.3	Configuration d'un périphérique de communication	152
14.10.4	Boîte de dialogue Envoyer e-mail test	152

14.11	Page ATM/POS Bridge	152
14.11.1	Ajout manuel d'une interface ATM/POS Bridge Bosch	153
14.11.2	Page Interface ATM/POS Bridge	153
14.11.3	Configuration d'un périphérique	154
14.11.4	Page Paramètres DTP	154
14.11.5	Page Paramètres ATM	155
14.11.6	Page Entrées	155
14.12	Lecteurs de cartes Foyer	155
14.12.1	Boîte de dialogue Ajouter un lecteur de cartes Foyer	156
14.12.2	Page Paramètres du lecteur de cartes Foyer	156
14.13	Page Entrées virtuelles	157
14.13.1	Ajout manuel d'entrées virtuelles	157
14.14	Page RMon et Snmp	157
14.14.1	Ajout manuel de SNMP	158
14.14.2	Configuration d'un récepteur de trap SNMP (page récepteur de trap SNMP)	158
14.14.3	Boîte de dialogue Journal trap SNMP	159
14.15	Page Attribution de clavier	159
14.16	Page Modules E/S	161
14.16.1	Ajout manuel d'un module E/S	161
14.16.2	Configuration d'un module E/S	161
14.16.3	Page ADAM	162
14.16.4	Page Entrées	162
14.16.5	Page Relais	162
14.17	Page Émulation CCL Allegiant	162
14.17.1	Ajout manuel d'une émulation CCL Allegiant	163
14.17.2	Commandes Allegiant CCL	163
14.17.3	Configuration d'une émulation CCL Allegiant	164
14.18	Page du service vidéo mobile	164
14.18.1	Service vidéo mobile	164
14.18.2	Ajout manuel d'entrées Mobile Video Service	165
14.19	Page Centrales d'intrusion	165
14.19.1	Ajout manuel d'une centrale d'intrusion	166
14.19.2	Page Paramètres	166
14.20	Page des systèmes de contrôle d'accès	166
14.20.1	Ajout d'un système de contrôle d'accès	167
14.20.2	Modification d'un système de contrôle d'accès	167
14.20.3	Page Paramètres	168
14.21	Page Vidéo Analytics	168
14.21.1	Page Paramètres Vidéo Analytics	168
14.21.2	Ajout d'un dispositif Vidéo Analytics	168
14.21.3	Page Person Identification device	169
14.21.4	Ajout d'un dispositif d'identification de personne (PID)	169
14.21.5	Page PID	170
14.21.6	Restauration de l'accès à un PID après une panne du serveur Management Server	170
14.21.7	Ajout de caméras à un dispositif d'identification de la personne (PID)	171
14.21.8	Configuration des paramètres de caméra pour les alarmes d'identification de la personne	172
14.21.9	Configuration des groupes de personnes	172
14.21.10	Ajout d'un périphérique LPR	173
14.22	Page Périphériques VRM	174

14.22.1	Ajout de dispositifs VRM via un balayage	174
14.22.2	Ajout manuel d'un VRM primaire ou secondaire	176
14.22.3	Modification d'un dispositif VRM	177
14.22.4	Page Paramètres du VRM	178
14.22.5	Page SNMP	178
14.22.6	Page Comptes	178
14.22.7	Page Avancé	178
14.22.8	Chiffrement d'un enregistrement pour VRM	179
14.22.9	Modification du mot de passe d'un périphérique VRM	180
14.22.10	Ajout d'une zone de stockage VRM	180
14.22.11	Ajout manuel d'un VRM de basculement	181
14.22.12	Ajout manuel d'un VRM redondant	182
14.22.13	Ajout d'encodeurs via un balayage	183
14.22.14	Ajout de dispositifs VSG via un balayage	183
14.22.15	Synchronisation de la configuration BVMS	184
14.22.16	Importer la configuration à partir de VRM	184
14.23	Page Zone	185
14.23.1	Configuration du mode d'enregistrement automatique sur une zone de stockage	186
14.23.2	Ajout manuel d'un encodeur	187
14.23.3	Ajout manuel d'un dispositif iSCSI	188
14.23.4	Ajout manuel d'un composant Video Streaming Gateway	189
14.23.5	Ajout manuel d'un dispositif iSCSI DSA E-Series	190
14.23.6	Ajout d'encodeurs via un balayage	193
14.23.7	Ajout de dispositifs VSG via un balayage	193
14.23.8	Configuration de l'enregistrement double dans l'Arborescence des périphériques	194
14.24	Page Encodeur/Décodeur Bosch	194
14.25	Page de périphérique iSCSI	194
14.25.1	Zone de stockage iSCSI	195
14.25.2	Ajout manuel d'un dispositif iSCSI	196
14.25.3	Ajout manuel d'un dispositif iSCSI DSA E-Series	197
14.25.4	Configuration d'un périphérique iSCSI	199
14.25.5	Page Configuration de base	200
14.25.6	Boîte de dialogue Équilibrage de charge	202
14.25.7	Déplacement d'un système iSCSI vers une autre zone de stockage (Modifier la zone de stockage)	202
14.25.8	Page LUN	202
14.25.9	Ajout d'un LUN	203
14.25.10	Formatage d'un LUN	204
14.25.11	Boîte de dialogue iqn-Mapper	205
14.26	Page du dispositif Video Streaming Gateway	205
14.26.1	Ajout manuel d'un composant Video Streaming Gateway	206
14.26.2	Modification d'une passerelle Video Streaming Gateway	207
14.26.3	Ajout d'une caméra à un VSG	208
14.26.4	Boîte de dialogue Ajouter un encodeur Bosch	208
14.26.5	Boîte de dialogue Ajouter un encodeur ONVIF	209
14.26.6	Boîte de dialogue Ajouter une caméra JPEG	211
14.26.7	Boîte de dialogue Ajouter un encodeur RTSP	212
14.26.8	Déplacement d'un VSG vers une autre zone de stockage (Modifier la zone de stockage)	213
14.26.9	Configuration du multicast (onglet Multicast)	213
14.26.10	Configuration de la journalisation (onglet Avancé)	214

14.26.11	Démarrage de ONVIF Camera Event Driver Tool à partir de Configuration Client	215
14.27	Page Temps Réel Uniquement	215
14.27.1	Ajout de dispositifs temps réel uniquement via un balayage	215
14.27.2	Ajout manuel d'un encodeur	216
14.27.3	Indication du mot de passe de destination d'un décodeur (Authentifier...)	217
14.28	Page Stockage local	218
14.29	Page Unmanaged Site	218
14.29.1	Ajout manuel d'un élément unmanaged site	219
14.29.2	Importation de sites non gérés	219
14.29.3	Page Unmanaged Site	220
14.29.4	Ajout d'un dispositif réseau non géré	220
14.29.5	Configuration du fuseau horaire	221
15	Page Encodeur / Décodeur / Caméra Bosch	222
15.1	Ajout manuel d'un encodeur	224
15.2	Ajout d'un encodeur à une zone de stockage VRM	225
15.3	Ajout d'un encodeur temps réel uniquement	225
15.4	Ajout d'un encodeur pour stockage local	225
15.5	Ajout d'une caméra avec un seul espace réservé	226
15.6	Importation de caméras à partir d'un fichier CSV	226
15.7	Modification d'un encodeur	228
15.7.1	Chiffrement de vidéo en temps réel (Modifier l'encodeur)	228
15.7.2	Mise à jour des fonctions du dispositif (Modifier l'encodeur)	229
15.7.3	Boîte de dialogue Modifier encodeur / décodeur	229
15.8	Gestion de la vérification d'authenticité	231
15.8.1	Vérification d'authenticité	231
15.8.2	Configuration de l'authentification	232
15.8.3	Chargement d'un certificat	233
15.8.4	Téléchargement d'un certificat	233
15.8.5	Installation d'un certificat sur un poste de travail	234
15.9	Indication du mot de passe de destination d'un décodeur (Authentifier...)	234
15.10	Modification du mot de passe d'un encodeur / décodeur (modifier mot de passe / entrer mot de passe)	234
15.11	Déplacement d'un encodeur vers une autre zone de stockage (Modifier la zone de stockage)	235
15.12	Récupération des enregistrements à partir d'un encodeur remplacé (Associer avec les enregistrements du prédécesseur)	236
15.13	Configuration des encodeurs / décodeurs	237
15.13.1	Configuration du support de stockage d'un encodeur	237
15.13.2	Configuration de plusieurs encodeurs et décodeurs	238
15.13.3	Configuration du mode d'enregistrement de basculement sur un encodeur	240
15.13.4	Page Gestion des enregistrements	240
15.13.5	Page Recording preferences (Préférences d'enregistrement)	241
15.13.6	Configuration des décodeurs pour l'affichage à l'écran (OSD)	241
15.14	Configuration du multicast	242
16	Page ONVIF	243
16.1	Ajout d'un dispositif ONVIF en temps réel par balayage	243
16.2	Page Encodeur ONVIF	243
16.3	Page Événements d'encodeur ONVIF	244
16.3.1	Ajout et suppression d'un profil ONVIF	246
16.3.2	Exportation d'un fichier de tableau de mappage ONVIF	247

16.3.3	Importation d'un fichier de tableau de mappage ONVIF	247
16.3.4	Configuration d'un tableau de mappage ONVIF	248
16.4	Page Configuration ONVIF	250
16.4.1	Accès à l'appareil	250
16.4.2	Date / Heure	251
16.4.3	Gestion des utilisateurs	252
16.4.4	Page Profil d'encodeur vidéo	253
16.4.5	Profil d'encodeur audio	255
16.4.6	Imagerie - Généralités	256
16.4.7	Compensation de contre-jour	256
16.4.8	Exposition	257
16.4.9	Mise au point	258
16.4.10	Plage dynamique étendue (WDR)	259
16.4.11	Balance des blancs	259
16.4.12	Accès réseau	260
16.4.13	Portées	262
16.4.14	Relais	263
16.5	Page Source d'événement ONVIF	264
16.6	Affectation d'un profil ONVIF	265
17	Page Cartes et structure	266
18	Configuration de cartes et de l'arborescence logique	268
18.1	Configuration de l'Arborescence Logique	268
18.2	Ajout d'un périphérique à l'Arborescence Logique	269
18.3	Suppression d'un élément de l'arborescence	270
18.4	Gestion des fichiers ressources	270
18.4.1	Boîte de dialogue Gestionnaire de ressources	271
18.4.2	Boîte de dialogue Sélectionner une ressource	272
18.5	Ajout d'un document	272
18.5.1	Boîte de dialogue Ajouter URL	273
18.6	Lien vers la boîte de dialogue Application externe	273
18.7	Ajout d'un Script de Commande	274
18.8	Ajout d'une séquence de caméras	274
18.8.1	Boîte de dialogue Générateur de séquence	274
18.9	Gestion des séquences de caméra préconfigurées	275
18.9.1	Boîte de dialogue Ajouter une séquence	277
18.9.2	Boîte de dialogue Ajouter un pas de séquence	277
18.10	Ajout d'un dossier	277
18.11	Ajout d'une carte	277
18.12	Ajout d'un lien vers une autre carte	278
18.12.1	Boîte de dialogue Sélectionner une carte pour le lien	278
18.13	Affectation d'une carte à un dossier	278
18.14	Gérer des dispositifs sur une carte de site	279
18.15	Configurer la carte globale et les zones de visualisation de carte	280
18.15.1	Configurer la carte globale	280
18.15.2	Configuration des caméras sur la carte globale	281
18.15.3	Ajouter des cartes sur la carte globale	283
18.16	Ajouter une zone de visualisation de carte	284
18.17	Activer le Map-based tracking assistant	285
18.18	Ajout d'un relais de dysfonctionnement	285

18.18.1	Boîte de dialogue Relais de dysfonctionnement	286
18.19	Configuration de l'exclusion de dispositifs	286
19	Page Planifications	288
19.1	Page Planifications d'Enregistrement	288
19.2	Page Planifications de Tâches	289
20	Configuration des planifications	291
20.1	Configuration d'une Planification d'Enregistrement	291
20.2	Ajout d'une Planification des Tâches	292
20.3	Configuration d'une Planification des Tâches standard	292
20.4	Configuration d'une Planification des Tâches récurrente	292
20.5	Suppression d'une Planification des Tâches	293
20.6	Ajout de jours fériés et de jours d'exception	293
20.7	Suppression de jours fériés et de jours d'exception	294
20.8	Modification du nom d'une planification	294
21	Page Caméras et enregistrement	296
21.1	Page Caméras	297
21.2	Pages des paramètres d'enregistrement	301
22	Configuration des caméras et des paramètres d'enregistrement	302
22.1	Copier et coller une sélection dans les tableaux	302
22.2	Exportation du Tableau des caméras	303
22.3	Configuration des paramètres de qualité du flux	304
22.3.1	Boîte de dialogue Paramètres de qualité du flux	304
22.4	Configuration des propriétés d'une caméra	307
22.5	Configuration des paramètres d'enregistrement (uniquement VRM et stockage local)	308
22.6	Boîte de dialogue Paramètres d'enregistrement planifié (uniquement VRM et stockage local)	308
22.7	Configuration des paramètres de port PTZ	311
22.8	Configuration de positions prédéfinies et de commandes auxiliaires	311
22.9	boîte de dialogue des positions prédéfinies et des commandes auxiliaires	313
22.10	Configuration de la fonction ROI	313
22.11	Configuration de la fonction ANR	314
22.12	Configuration de l'enregistrement double dans le Tableau des caméras	314
22.13	Gestion de Video Streaming Gateway	315
22.13.1	Affectation d'un profil ONVIF	315
23	Page Événements	316
23.1	Onglet Paramètres de réponse	317
23.2	Onglet Paramètres pour l'affichage de carte avancé	317
23.3	Onglet Paramètres pour la configuration des événements	318
23.4	Boîte de dialogue Éditeur de Script de Commande	319
23.5	Créer un Événement Combiné / Boîte de dialogue Modifier l'Événement Combiné	319
23.6	Boîte de dialogue Sélectionner un langage de script	320
23.7	Boîte de dialogue Modifier les priorités du type d'événement	320
23.8	Boîte de dialogue Sélectionner les périphériques	321
23.9	Boîte de dialogue Enregistrement de données texte	321
24	Page Alarmes	322
24.1	Boîte de dialogue Paramètres d'alarme	323
24.2	Boîte de dialogue Sélectionner le contenu du volet des Images	324
24.3	Boîte de dialogue Sélectionner le contenu du volet des Images (MG)	325
24.4	Boîte de dialogue Options d'alarmes	325
24.5	Boîte de dialogue Sélectionner une ressource	329

25	Configuration des événements et des alarmes	331
25.1	Copier et coller une sélection dans les tableaux	332
25.2	Suppression d'une ligne de tableau	332
25.3	Gestion des fichiers ressources	332
25.4	Configuration d'un événement	332
25.5	Duplication d'un événement	333
25.6	Consignation des événements utilisateur	333
25.7	Configuration des boutons d'événement utilisateur	333
25.8	Création d'un Événement Combiné	334
25.9	Modification d'un Événement Combiné	335
25.10	Configuration d'une alarme	336
25.11	Configuration de paramètres pour toutes les alarmes	336
25.12	Configuration des durées pré-alarme et post-alarme d'une alarme	337
25.13	Déclenchement de l'enregistrement d'alarme avec des données texte	337
25.14	Ajout de données texte à l'enregistrement continu	338
25.15	Protection de l'enregistrement d'alarme	338
25.16	Configuration de zones réactives clignotantes	339
25.17	Événements et alarmes pour les systèmes de contrôle d'accès	340
25.18	Événements et alarmes pour l'identification d'une personne	340
26	Page Groupes d'utilisateurs	341
26.1	Page Propriétés du groupe d'utilisateurs	343
26.2	Page Propriétés de l'utilisateur	344
26.3	Page Propriétés de combinaison de connexion	345
26.4	Page Autorisations de caméra	346
26.5	Page Priorité des commandes	347
26.6	Boîte de dialogue Copier les autorisations du groupe d'utilisateurs	348
26.7	Page Autorisations de décodeur	348
26.8	Page Événements et alarmes	349
26.9	Page d'identifiants	349
26.10	Page Arborescence Logique	350
26.11	Page des fonctionnalités d'Operator	350
26.12	Page Priorités	354
26.13	Page Interface utilisateur	354
26.14	Page Accès au serveur	355
26.15	Page Autorisations de configuration	356
26.16	Page Autorisations du groupe d'utilisateurs	357
26.17	Page Stratégies de compte	358
26.17.1	Operator Client hors ligne	360
26.18	Autorisations de connexion par page de type d'application	362
26.19	Page des paramètres de gestion des menaces	363
27	Configuration des utilisateurs, des autorisations et de l'accès d'entreprise	365
27.1	Créer un groupe ou un compte	366
27.1.1	Création d'un groupe d'utilisateurs standard	366
27.1.2	Création d'un Enterprise User Group	367
27.1.3	Création d'un Enterprise Account	367
27.2	Création d'un utilisateur	368
27.3	Création d'un groupe de double autorisation	369
27.4	Ajout d'une combinaison de connexion au groupe de double autorisation	370
27.5	Configuration du groupe admin.	370

27.6	Sélectionner un groupe LDAP associé	371
27.7	Planification des autorisations de connexion utilisateur	372
27.8	Configuration des autorisations d'exploitation	372
27.9	Configuration des autorisations d'utilisation des dispositifs	372
27.10	Configuration de priorités diverses	373
27.11	Copie des autorisations d'un groupe d'utilisateurs	374
28	Page Audit Trail	375
28.1	Détails de la journalisation pour Audit Trail	375
28.2	Boîte de dialogue de filtre Audit Trail	376
29	Configuration de la détection incendie basée sur la vidéo	378
29.1	Configuration d'une caméra de détection incendie	378
29.2	Ajout d'un encodeur à une zone de stockage VRM	379
29.3	Ajout d'encodeurs via un balayage	379
29.4	Ajout de dispositifs temps réel uniquement via un balayage	380
29.5	Ajout d'encodeurs à stockage local via un balayage	380
29.6	Configuration d'un événement d'incendie	381
29.7	Configuration d'une alarme incendie	381
30	Configuration de MIC IP 7000 connecté à VIDEOJET connect 7000	382
31	Dépannage	383
31.1	Configuration de la langue dans Windows	385
31.2	Rétablissement de la connexion à un clavier numérique IntuiKey de Bosch	385
31.3	Réduction du nombre de caméras Allegiant	385
31.4	Ports utilisés	385
31.5	Activation de la journalisation des événements ONVIF	392
	Glossaire	394
	Index	404

1 Utilisation de l'aide



Remarque!

Ce document décrit certaines fonctions non disponibles pour BVMS Viewer.

Pour plus de détails sur les différentes versions BVMS, consultez le site


www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Pour des conseils pratiques sur BVMS, accédez à l'aide en ligne en suivant l'une des méthodes ci-dessous.

Pour utiliser les onglets **Table des matières**, **Index** ou **Recherche** :

- ▶ Dans le menu **Aide**, cliquez sur **Afficher l'aide**. Utilisez les boutons et les liens pour naviguer dans l'aide.

Pour obtenir de l'aide sur une fenêtre ou une boîte de dialogue :

- ▶ Dans la barre d'outils, cliquez sur  .
- OU
- ▶ Appuyez sur F1 pour obtenir de l'aide dans n'importe quelle fenêtre ou boîte de dialogue du programme.

1.1 Recherche d'informations

Vous disposez de plusieurs méthodes pour rechercher des informations dans l'aide.

Pour rechercher des informations dans l'aide en ligne :

1. Dans le menu **Aide**, cliquez sur **Aide**.
2. Si le volet gauche n'est pas visible, cliquez sur le bouton **Afficher**.
3. Dans la fenêtre Aide, procédez comme suit :

Cliquez sur :	Pour :
Contenu	Afficher le sommaire de l'aide en ligne. Cliquez sur les icônes de livre pour afficher une liste de pages renvoyant à des rubriques. Cliquez ensuite sur une page pour afficher la rubrique correspondante dans le volet droit.
Index	Rechercher des mots ou expressions particuliers ou les sélectionner dans la liste des mots clés de l'index. Double-cliquez sur le mot clé souhaité pour afficher la rubrique correspondante dans le volet droit.
Rechercher	Rechercher des mots ou des expressions figurant dans les rubriques. Saisissez le mot ou l'expression dans le champ de texte, appuyez sur ENTRÉE, puis sélectionnez la rubrique qui vous intéresse dans la liste proposée.

Les options de l'interface utilisateur apparaissent en **gras**.

- ▶ Les flèches indiquent que vous pouvez cliquer sur le texte souligné ou sur un élément dans l'application.

Rubriques connexes

- ▶ Cliquez pour afficher une rubrique apportant des informations sur la fenêtre de l'application en cours d'utilisation. Cette rubrique comporte des informations sur les commandes présentes dans la fenêtre de l'application.

Concepts, page 23 Elle fournit des informations générales sur les sujets sélectionnés.

**Remarque!**

Ce symbole indique un risque potentiel de dommages matériels ou de perte de données.

1.2**Impression de l'aide**

Lorsque vous utilisez l'aide en ligne, vous pouvez imprimer des rubriques et des informations directement depuis la fenêtre de votre navigateur.

Pour imprimer une rubrique d'aide :

1. Cliquez avec le bouton droit de la souris dans le volet droit, puis sélectionnez **Imprimer**.
La boîte de dialogue **Imprimer** s'affiche.
2. Cliquez sur **Imprimer**.
⇒ La rubrique est imprimée sur l'imprimante spécifiée.

2 Signification des messages de sécurité

Dans ce manuel, les notations et symboles suivants attirent l'attention du lecteur sur des situations particulières :

**Danger!**

Risque élevé : ce symbole indique un danger immédiat de type « risque d'électrocution » à l'intérieur du produit qui, s'il n'est pas évité, peut entraîner des blessures corporelles graves, voire mortelles.

**Attention!**

Risque moyen : indique une situation potentiellement dangereuse qui, si elle n'est pas évitée, peut entraîner des blessures mineures ou modérées. Ce symbole permet à l'utilisateur d'identifier les instructions importantes concernant l'appareil.

**Attention!**

Risque faible : indique une situation potentiellement dangereuse qui, si elle n'est pas évitée, peut entraîner des dommages matériels ou endommager le périphérique.

**Remarque!**

Ce symbole signale des informations ou une politique de la société concernant directement ou indirectement la sécurité du personnel ou la protection du matériel.

3 Introduction

Cliquez sur le lien ci-après pour accéder aux licences logicielles open source utilisées par BVMS et l'Application mobile :

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



Couverts par une ou plusieurs déclarations de brevets figurant à l'adresse patentlist.hevcadvance.com.

Ce manuel vous guide à travers les procédures standard à suivre pour configurer BVMS. Pour des explications plus précises, consultez le manuel de configuration ou l'aide en ligne.

BVMS

BVMS intègre la vidéo, le son et les données numériques sur n'importe quel réseau IP.

Ce système se compose des modules logiciels suivants :

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

Pour que le système fonctionne, vous devez effectuer les tâches suivantes :

- Installation des services (Management Server et VRM)
- Installation de Operator Client et de Configuration Client
- Connexion au réseau
- Connexion des dispositifs au réseau
- Configuration de base :
 - Ajout des dispositifs (en effectuant une recherche de dispositif, par exemple)
 - Création d'une structure logique
 - Configuration des planifications, des caméras, des événements et des alarmes
 - Configuration des groupes d'utilisateurs

BVMS Export Player

BVMS Export Player affiche les enregistrements exportés.

BVMS Viewer


BVMS Viewer est une application de sécurité vidéo IP pour le visionnage et la lecture en temps réel de caméras et enregistreurs Bosch reliés au réseau. Le pack logiciel comporte un Operator Client pour le visionnage en temps réel et la lecture de vidéos et un Configuration Client. BVMS Viewer prend en charge la gamme de produits vidéo IP Bosch actuelle ainsi que les dispositifs vidéo Bosch existants.


Cliquez sur le lien pour accéder aux licences logicielles Open Source utilisées par BVMS Viewer :

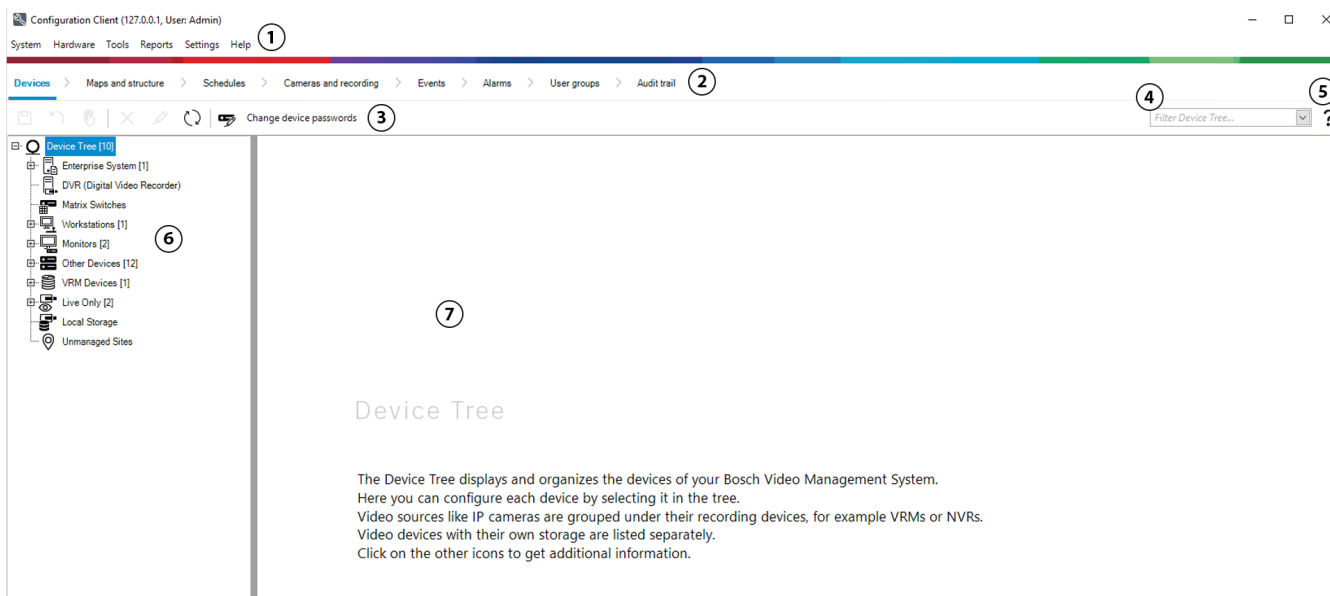
<http://www.boschsecurity.com/oss>.

BVMS Configuration Client

L'idée de BVMS Configuration Client est de commencer par la configuration des dispositifs, puis de poursuivre avec la configuration de l'arborescence logique. Une fois ces deux étapes effectuées, les planifications, enregistrements, événements et alarmes des dispositifs peuvent être configurés sur leurs pages respectives. La dernière étape consiste à configurer les groupes d'utilisateurs sur la page des groupes d'utilisateurs. Après la configuration de toutes les pages de gauche à droite, tout est configuré et l'opérateur peut démarrer à l'aide d'Operator Client.

Après la configuration de chaque page, enregistrez la configuration en cliquant sur  dans le menu Outils.

Pour que les modifications apparaissent dans BVMS Operator Client, cliquez sur .



1	Barre des menus	Permet de sélectionner une commande dans un menu.
2	Barre des pages	Permet de configurer toutes les étapes nécessaires de gauche à droite.
3	Barre d'outils	Affiche les boutons disponibles en fonction de l'onglet actif. Survolez l'icône pour afficher l'infobulle correspondante.
4	Barre de recherche	Permet de rechercher un dispositif spécifique ainsi que ses parents dans l'arborescence des dispositifs.
5	Icône d'aide	Affiche l'aide en ligne de BVMS Configuration Client.
6	Fenêtre de sélection	Liste hiérarchique de tous les dispositifs disponibles dans le système.
7	Fenêtre de configuration	Permet de configurer le dispositif sélectionné.

BVMS Operator Client

3.1

Éditions BVMS

Les différentes éditions BVMS vous offrent une évolutivité complète pour vous permettre d'étendre votre système de vidéosurveillance en fonction de vos besoins.

Les éditions BVMS disponibles sont les suivantes :

- BVMS Professional
- BVMS Enterprise
- BVMS Plus

- BVMS Lite
- BVMS Viewer

BVMS Viewer et BVMS Professional sont des produits uniquement logiciels. Vous ne pouvez pas les utiliser sur des dispositifs Bosch DIVAR IP.

Vous pouvez utiliser BVMS Lite et BVMS Plus sur des dispositifs Bosch DIVAR IP en tant que produits uniquement logiciels sur tout autre matériel.

Pour plus d'informations sur les différentes éditions BVMS, consultez le site

www.boschsecurity.com et le Guide de sélection rapide de BVMS :

[Guide de sélection rapide de BVMS.](#)

3.2

Vue d'ensemble de l'activation de la licence BVMS

Ce chapitre présente la procédure d'activation de la licence BVMS.

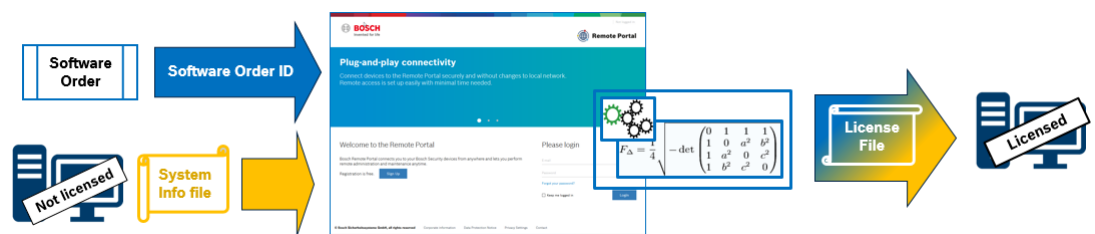
Commande de licence

- Pour la commande, utilisez le bureau des commandes de Bosch.
- La confirmation de commande inclut le nouvel ID de commande logicielle qui est nécessaire pour le processus d'activation logiciel ultérieur.
- À compter de BVMS 11.0, la licence de base et les licences d'extension de BVMS ne dépendent plus de la version logicielle.

Activation de licence

- Bosch Remote Portal (<https://www.remote.boschsecurity.com>) remplace Bosch **Gestionnaire de licences**.
- Un nouvel enregistrement de l'utilisateur est nécessaire dans Bosch Remote Portal.
- Il est obligatoire d'indiquer, pour l'activation de la licence, le fichier d'information système et l'ID de commande de logiciel.
- Remote Portal produit le fichier de licence et tous les détails d'activation. Ajoutez ce fichier au système BVMS installé.
- Le processus d'activation définit la date de début de la période d'assurance logicielle. La date de fin est affichée dans le gestionnaire **Gestionnaire de licences** de BVMS Configuration Client.

Processus d'activation de licence logicielle



Pour activer vos licences logicielles, effectuez les opérations suivantes :

1. Commander les produits logiciels
 - Pour commander vos produits logiciels, suivez le processus de commande Bosch standard.
 - Les commandes de logiciels peuvent comprendre un ou plusieurs produits d'une ou de plusieurs éditions de produits.
2. Recevoir l'ID de commande logicielle

- Suite à la commande est générée une confirmation de commande logicielle qui contient l'ID de commande de logiciel.
 - L'ID de commande de logiciel permet de connecter le logiciel installé (sur le système d'exploitation et le matériel) aux produits logiciels commandés.
3. Activer la licence
- Il est obligatoire d'indiquer, pour l'activation de la licence, le fichier d'information système qui représente le système d'exploitation unique et le matériel où le logiciel est installé.
 - L'activation connecte l'ID de commande logicielle au logiciel installé et produit le fichier de licence.
 - L'activation définit les attributs du système, comme la date de début et de fin de l'assurance logicielle.
4. Activer le logiciel
- Afin d'activer le logiciel, ajoutez le fichier de licence au logiciel installé.
 - Les fichiers de licence permettent d'activer les fonctions de BVMS en fonction des éléments activés.

Remarque!**Le fichier de licence comprend les détails d'activation suivants :**

- édition du produit BVMS
- version autorisée de BVMS
- Date d'expiration de l'assurance logicielle
- Nombre de licences d'extension/de fonctionnalité

Se reporter à

- *Activation des licences des logiciels, page 75*

4 Vue d'ensemble du système



Remarque!

Ce document décrit certaines fonctions non disponibles pour BVMS Viewer.

Pour plus de détails sur les différentes versions BVMS, consultez le site

www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Si vous avez l'intention d'installer et de configurer BVMS, inscrivez-vous à une formation sur le système BVMS.

Reportez-vous aux notes de mise à jour de la version actuelle de BVMS pour connaître les versions de firmware et de matériel prises en charge et pour obtenir d'autres informations pertinentes.

Reportez-vous aux fiches techniques des postes de commande et serveurs Bosch pour obtenir des informations sur les ordinateurs sur lesquels BVMS peut être installé.

Vous pouvez éventuellement installer les modules logiciels BVMS sur un seul PC.

Composants importants

Composant	Description
Management Server (sélectionnable dans la configuration)	Gestion des flux, gestion des alarmes, gestion des priorités, gestion du journal des connexions, gestion des utilisateurs, gestion de l'état des dispositifs. Licence Enterprise System supplémentaire : gestion des Enterprise User Groups et des Enterprise Accounts.
Config Wizard	Configuration facile et rapide d'un système d'enregistrement.
Configuration Client (sélectionnable dans la configuration)	Configuration et administration du système pour Operator Client.
Operator Client (sélectionnable dans la configuration)	Surveillance en temps réel, récupération et lecture des enregistrements, gestion des alarmes et contrôle de l'accès simultané à plusieurs ordinateurs Management Server.
Video Recording Manager (sélectionnable dans la configuration)	Répartition des capacités de stockage des dispositifs iSCSI sur les encodeurs, tout en maintenant l'équilibre des charges entre les différents dispositifs iSCSI. Transfert des données vidéo et audio des dispositifs iSCSI à Operator Clients.
Mobile Video Service (sélectionnable dans la configuration)	Fournit un service de transcodage qui transcode les flux vidéo en temps réel et archivés provenant d'une caméra configurée dans BVMS vers la bande passante réseau disponible. Cette option permet aux clients vidéo Web ou iPhone de recevoir des flux transcodés, par exemple pour des connexions réseau non fiables avec bande passante limitée.

Composant	Description
Client Web	Vous pouvez accéder à des vidéos en temps réel et archivées via un navigateur Web.
Application mobile	Vous pouvez utiliser l'application iPhone ou iPad pour accéder à des vidéos en temps réel et archivées.
Bosch Video Streaming Gateway (sélectionnable dans la configuration)	Assure l'intégration des caméras tierces, par ex., dans les réseaux à faible bande passante.
Cameo SDK (sélectionnable dans la configuration)	Le Cameo SDK sert à intégrer des volets des images BVMS en temps réel et archivés dans votre logiciel externe tiers. Les volets des images suivent les autorisations utilisateur fondées sur BVMS. Le Cameo SDK fournit un sous-ensemble de fonctionnalités BVMS Operator Client qui vous permet de créer des applications similaires à Operator Client.
Client Enterprise SDK	Le Client Enterprise SDK sert à contrôler et surveiller le comportement du Operator Client d'un Enterprise System par des applications externes. Le kit de développement logiciel permet de parcourir les dispositifs accessibles par le Operator Client en cours d'utilisation et connecté, et de contrôler certaines fonctionnalités UI.
Client SDK / Server SDK	Le Server SDK permet de contrôler et surveiller le Management Server par des scripts et des applications externes. Vous pouvez utiliser les interfaces avec un compte administrateur valide. Le Client SDK permet de contrôler et surveiller le Operator Client par des applications externes et des scripts (partie de la configuration du serveur).

4.1 Configuration matérielle requise

Reportez-vous à la fiche technique de BVMS. Des fiches techniques sont également disponibles pour les plates-formes PC.

4.2 Configuration logicielle requise

Vous ne pouvez pas installer BVMS où un autre composant BVMS Viewer est installé. Reportez-vous à la fiche technique de BVMS.

4.3 Licences nécessaires

Reportez-vous à la fiche de données de BVMS pour obtenir les licences disponibles.

5 Concepts



Remarque!

BVMS Viewer offre uniquement des fonctionnalités de base. Les fonctionnalités avancées sont incluses dans BVMS Professional. Pour de plus amples informations sur les différentes éditions BVMS, consultez le site www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Ce chapitre fournit des informations générales sur les sujets sélectionnés.

5.1 Concepts de conception BVMS

Systeme Management Server unique, page 23

Un seul système BVMS Management Server gère, surveille et contrôle jusqu'à 2 000 caméras/encodeurs.

Enterprise System, page 24

Un Enterprise Management Server fournit un accès simultané à plusieurs Management Servers. Le Enterprise System permet d'accéder pleinement à des événements et des alarmes provenant de plusieurs sous-systèmes.

Server Lookup, page 25

La fonction Server Lookup fournit une liste de BVMS Management Servers disponibles au BVMS Operator Client. L'opérateur peut sélectionner un serveur dans la liste des serveurs disponibles. Connecté au Management Server, le client dispose d'un accès total au Management Server.

Unmanaged site, page 26

Les dispositifs peuvent être regroupés en unmanaged sites. Les dispositifs sous unmanaged sites ne sont pas surveillés par le Management Server. Le Management Server fournit une liste de unmanaged sites à l'Operator Client. L'opérateur peut se connecter à la demande au site et accéder aux données vidéo en temps réel et aux données vidéos enregistrées. Les événements et la gestion d'alarme ne sont pas disponibles dans le concept d'unmanaged site.

5.1.1 Systeme Management Server unique

- Un BVMS Management Server unique peut gérer jusqu'à 2 000 canaux.
- Un BVMS Management Server assure la gestion, la surveillance et le contrôle de l'ensemble du système.
- Le BVMS Operator Client est connecté au Management Server et reçoit des événements et alarmes à partir du BVMS Management Server et affiche les données en temps réel et en lecture.
- Dans la plupart des cas, tous les dispositifs sont sur un réseau local avec une bande passante élevée et une faible latence.

Responsabilités :

- Configuration des données
- Journal des événements (journal des connexions)
- Profils utilisateur
- Priorités utilisateur
- Gestion des licences
- Gestion des événements et des alarmes



	Temps réel, lecture, événements, alarmes
	Management Server
	Operator Client / Configuration Client
	Caméras
	VRM
	iSCSI
	Autres dispositifs

5.1.2

Enterprise System

- L'objectif d'un BVMS Enterprise System est de permettre à un utilisateur d'un Operator Client d'accéder simultanément à plusieurs Management Servers (sous-systèmes).
- Les clients connectés à un serveur d'entreprise (Enterprise Server) disposent d'un accès total à l'ensemble des caméras et des enregistrements des sous-systèmes.
- Les clients connectés à un serveur d'entreprise sont sensibilisés en temps réel aux événements et aux alarmes de tous les sous-systèmes.
- Domaines d'application types :
 - Métro
 - Aéroports



	Temps réel, lecture, événements, alarmes
	BVMS Enterprise Management Server
	BVMS Operator Client / Configuration Client
	Sous-système BVMS

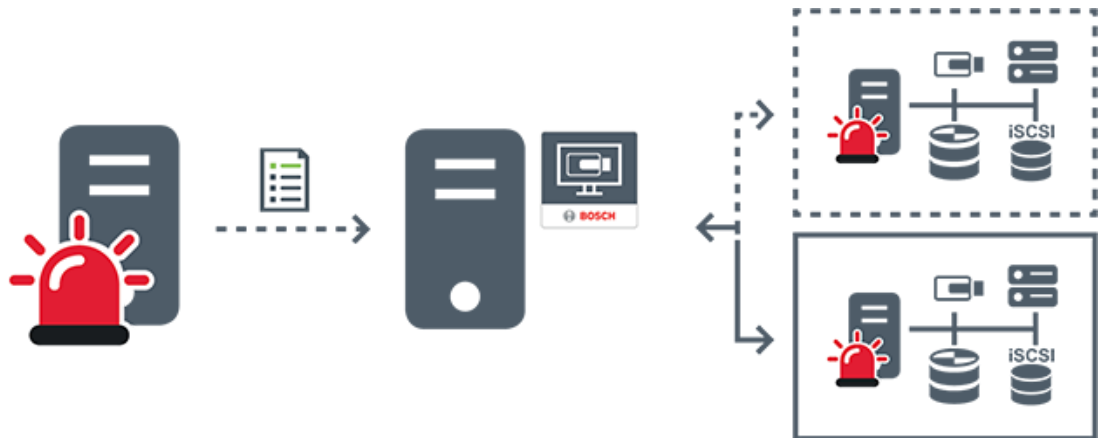
Se reporter à

- *Création d'un système d'entreprise, page 86*
- *Configuration de la liste des serveurs pour le système d'entreprise, page 86*
- *Configuration des utilisateurs, des autorisations et de l'accès d'entreprise, page 365*
- *Accès au système, page 74*

5.1.3

Server Lookup

- La fonction BVMS Server Lookup permet aux opérateurs de se connecter à un BVMS Management Server qui ne figure pas dans une liste de serveurs fournie.
- Un seul utilisateur de Configuration Client ou Operator Client peut se connecter depuis plusieurs points d'accès au système de manière séquentielle.
- Les points d'accès au système peuvent être Management Server ou Enterprise Management Server.
- Server Lookup utilise le Management Server dédié pour héberger la liste des serveurs.
- Server Lookup et Management Server ou Enterprise Management Server peuvent être exécutés sur un ordinateur.
- Server Lookup vous aide à localiser des points d'accès au système par leur nom ou description.
- Une fois connecté au Management Server, le Operator Client reçoit des événements et alarmes provenant de BVMS Management Server et affiche les données en temps réel et en lecture.



	À la demande en temps réel, lecture, événements, alarmes - connexion
	À la demande en temps réel, lecture, événements, alarmes - pas de connexion
	Management Server
	Liste de serveurs
	Operator Client
	BVMS connecté à partir de la liste des serveurs
	BVMS non connecté à partir de la liste des serveurs

Se reporter à

- Configuration de Server Lookup, page 132
- Page Liste de serveurs / Carnet d'adresses, page 130
- Utilisation de la recherche de serveur, page 74
- Exportation de la liste des serveurs, page 132
- Importation d'une liste de serveurs, page 133

5.1.4

Unmanaged site

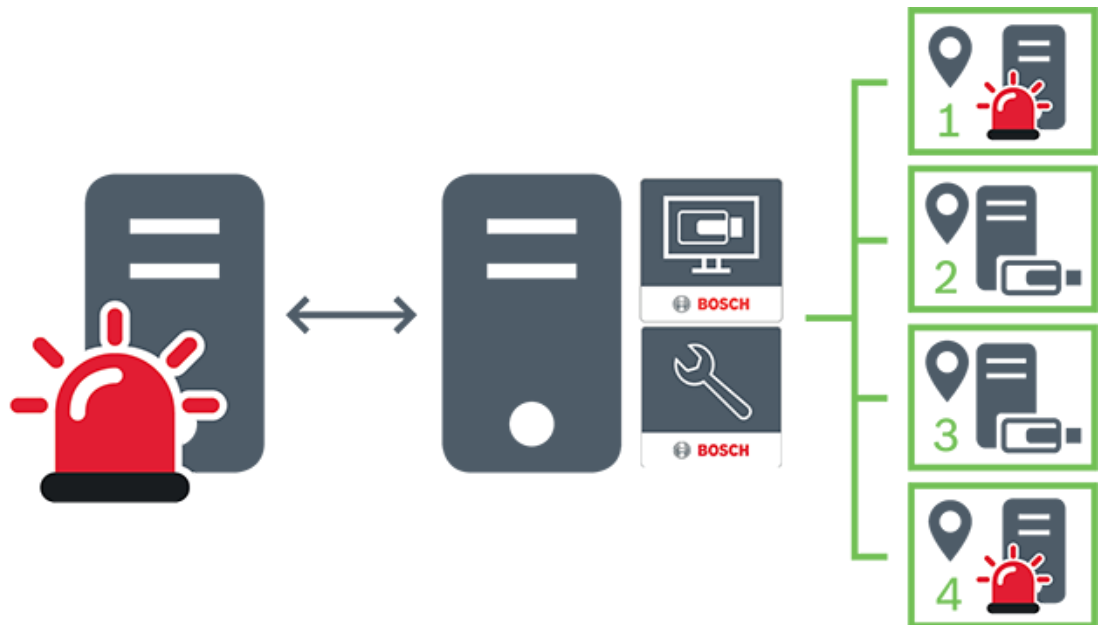
- Une option de conception de système de BVMS avec un grand nombre de petits sous-systèmes.
- Permet de configurer jusqu'à 9 999 emplacements dans un BVMS Management Server

- Les opérateurs peuvent accéder simultanément aux données vidéo en temps réel et enregistrées d'un maximum de 20 sites.
- Pour faciliter la navigation, les sites peuvent être regroupés en dossiers ou être placés sur des cartes. Un nom d'utilisateur et un mot de passe prédéfinis permettent aux opérateurs de se connecter rapidement à un site.

Le concept d'unmanaged site prend en charge système BVMS basé sur IP ainsi que les solutions DVR analogiques :

- Enregistreurs analogiques Bosch DIVAR AN 3000 / 5000
- Enregistreurs DIVAR hybrid
- Enregistreurs DIVAR network
- Enregistrement basé sur l'IP des unités DIP 3000/7000
- Système BVMS Management Server unique

L'ajout d'un site pour la surveillance centrale ne requiert qu'une licence par site et est indépendant du nombre de canaux du site.



	Temps réel, lecture, événements, alarmes
	Trafic vidéo en temps réel et en lecture
	Management Server
	Operator Client / Configuration Client
	site

	DVR
---	-----

Se reporter à

- *Ajout manuel d'un élément unmanaged site, page 219*

5.2 Enregistrement

Ce chapitre présente les différentes fonctions d'enregistrement et de relecture sur le système.

5.2.1 Automated Network Replenishment (ANR)

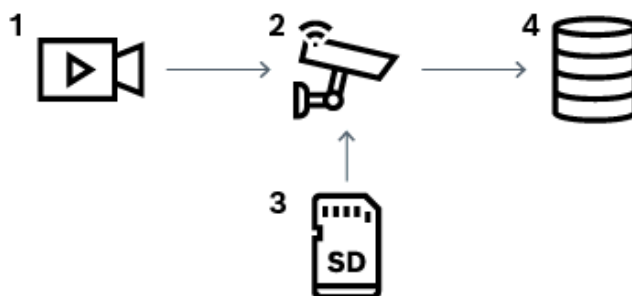
**Remarque!**

BVMS Viewer offre uniquement des fonctionnalités de base. Les fonctionnalités avancées sont incluses dans BVMS Professional. Pour de plus amples informations sur les différentes éditions BVMS, consultez le site www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Utilisation prévue

En cas de panne réseau ou de stockage centralisé, la fonction ANR assure que l'encodeur transmet l'enregistrement mis en mémoire tampon localement de la période manquante au stockage centralisé une fois la panne résolue.

Le graphique suivant présente la transmission de données vidéo après la résolution d'une panne réseau ou de stockage.



1	Vidéo
2	Encodeur, réseau IP
3	Carte SD (mémoire tampon en boucle)
4	Cible iSCSI (stockage central)

Exemple : Contourner une panne réseau

Si le réseau subit une panne inattendue, la fonction ANR effectue le stockage central avec l'enregistrement mis en mémoire tampon localement lorsque le réseau est de nouveau disponible.

Exemple : Stocker des données vidéo lorsque le réseau n'est pas disponible

Un métro n'a pas de connexion réseau au stockage central lorsqu'il se trouve entre deux stations. L'enregistrement mis en mémoire tampon ne peut être transmis au stockage central que pendant les arrêts réguliers.

Assurez-vous que la durée requise pour le transfert de l'enregistrement mis en mémoire tampon ne dépasse pas la durée d'un arrêt.

Exemple : ANR pour un enregistrement d'alarme

L'enregistrement de pré-alarme est stocké localement. Cet enregistrement de pré-alarme ne peut être transmis au stockage central qu'en cas d'alarme. Si aucune alarme ne se déclenche, l'enregistrement de pré-alarme obsolète n'est pas transmis au stockage central et, par conséquent, ne charge pas le réseau.

Limitations**Remarque!**

Vous ne pouvez pas utiliser la fonction de lecture à partir du support de stockage local lorsque les mots de passe pour « user » et « live » sont définis sur l'encodeur. Au besoin, supprimez les mots de passe.

La fonction ANR n'est opérationnelle qu'avec un enregistrement VRM.

La fonction ANR ne fonctionne pas avec un encodeur pour lequel une connexion sécurisée pour l'affichage en temps réel est configurée.

Pour utiliser la fonction ANR, vous devez avoir configuré le support de stockage d'un encodeur.

L'encodeur pour lequel vous configurez la fonction ANR doit avoir la version de firmware 5.90 ou ultérieure. Tous les types d'encodeurs ne prennent pas en charge la fonction ANR.

Il est impossible d'utiliser la fonction ANR avec l'enregistrement double.

Votre système de stockage iSCSI doit être correctement configuré.

La liste suivante contient les causes possibles de votre impossibilité de configurer la fonction ANR :

- L'encodeur n'est pas accessible (adresse IP incorrecte, panne réseau, etc.).
- Le support de stockage de l'encodeur n'est pas disponible ou est en lecture seule.
- La version du firmware est incorrecte.
- Le type d'encodeur ne prend pas en charge la fonction ANR.
- L'enregistrement double est actif.

Se reporter à

- *Configuration d'un périphérique iSCSI, page 199*
- *Configuration du support de stockage d'un encodeur, page 84*
- *Configuration de la fonction ANR, page 314*

5.2.2**Enregistrement double/de basculement****Utilisation prévue**

Un VRM principal gère l'enregistrement normal de caméras de votre système. Vous utilisez un VRM secondaire pour obtenir un enregistrement double de vos caméras.

L'enregistrement double permet d'enregistrer les données vidéo provenant d'une même caméra à différents emplacements.

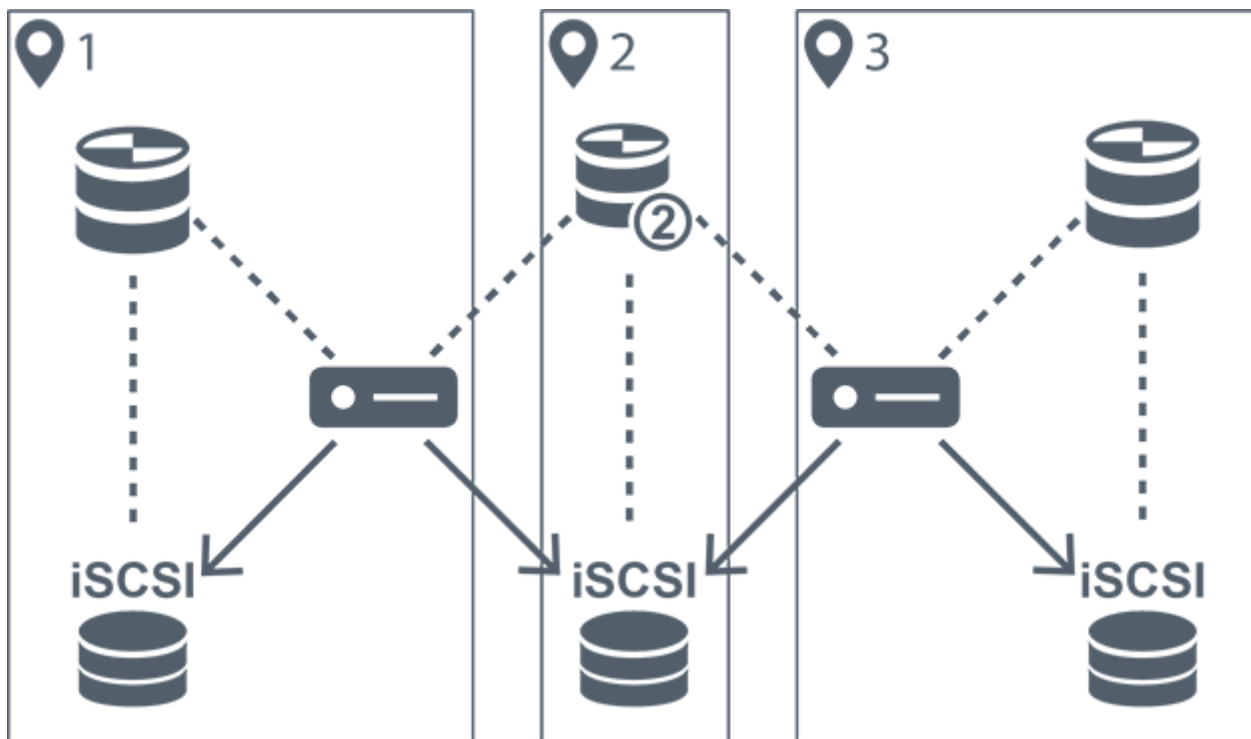
L'enregistrement double est généralement effectué avec différents paramètres de flux et modes d'enregistrement. Dans le cas particulier de l'enregistrement double, vous pouvez configurer un enregistrement redondant : un même signal vidéo est enregistré deux fois à différents emplacements.

L'enregistrement double est obtenu en utilisant 2 serveurs VRM gérant plusieurs périphériques iSCSI qui peuvent se trouver à divers emplacements.

Un VRM secondaire peut gérer l'enregistrement secondaire pour plusieurs VRM principaux. L'utilisateur peut choisir entre les enregistrements gérés par le VRM principal et ceux gérés par le VRM secondaire. Pour une seule caméra, l'utilisateur peut passer aux enregistrements du VRM secondaire/principal. L'utilisateur peut également afficher simultanément les enregistrements de cette même caméra gérés par le VRM principal et le VRM secondaire. Pour l'enregistrement double, vous devez installer un VRM secondaire au cours de la configuration.

Un serveur VRM de basculement permet de poursuivre l'enregistrement d'un serveur VRM principal ou VRM secondaire défaillant.

Le graphique suivant présente un exemple de scénario d'enregistrement double :



1	Site 1		Encodeur
2	Site central		Périphérique de stockage iSCSI
3	Site 2	Connexion de contrôle
	VRM principal		Flux vidéo
	VRM secondaire		

Restrictions

Il est impossible d'utiliser l'enregistrement double avec la fonction ANR. Cameo SDK prend uniquement en charge la lecture de l'enregistrement principal.

Se reporter à

- Configuration de l'enregistrement double dans le Tableau des caméras, page 314
- Ajout manuel d'un VRM redondant, page 182
- Ajout manuel d'un VRM de basculement, page 181
- Page Caméras, page 297

5.2.3

Modes d'enregistrement VRM

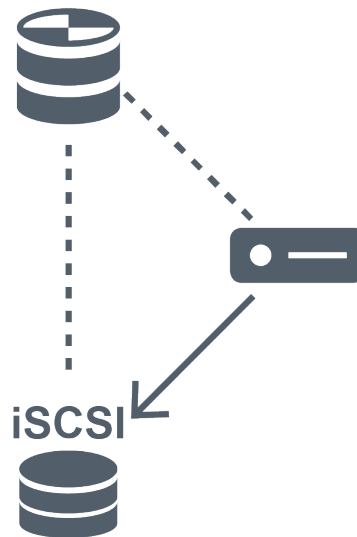
Ce chapitre présente les graphiques destinés à illustrer les modes d'enregistrement VRM possibles.




Liste des modes d'enregistrement VRM possibles :

- Enregistrement VRM principal
- Enregistrement VRM redondant
- Enregistrement VRM secondaire
- Enregistrement de serveur VRM de basculement

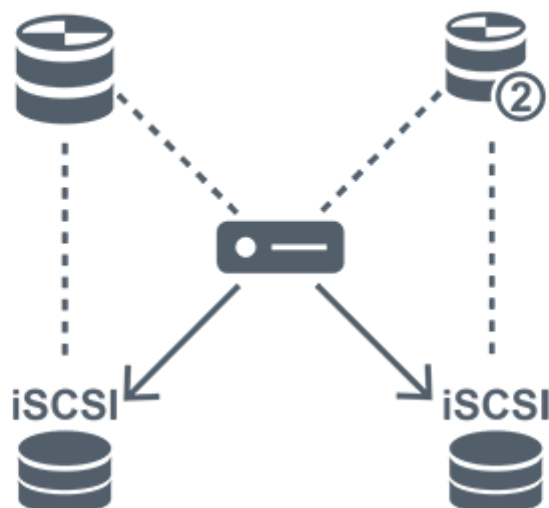
Pour l'enregistrement ANR, reportez-vous au chapitre *Automated Network Replenishment (ANR)*, page 28.

Enregistrement VRM principal



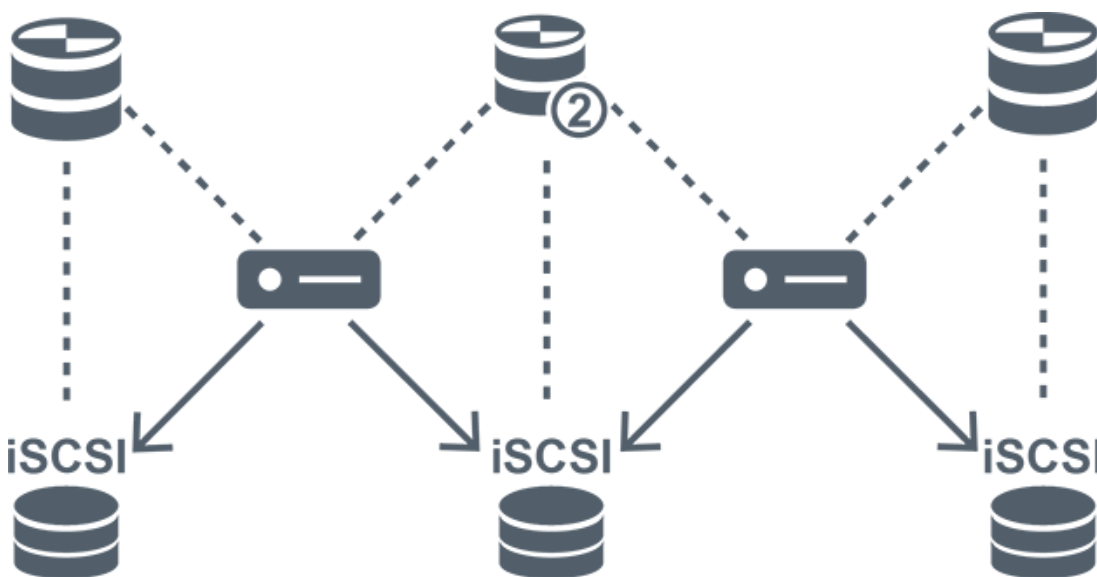
	VRM principal	-----	Connexion de contrôle
	Périphérique de stockage iSCSI	→	Flux vidéo
	Encodeur		

Enregistrement VRM redondant



	VRM principal		VRM secondaire
	Dispositif de stockage iSCSI		Connexion de contrôle
	Encodeur		Flux vidéo

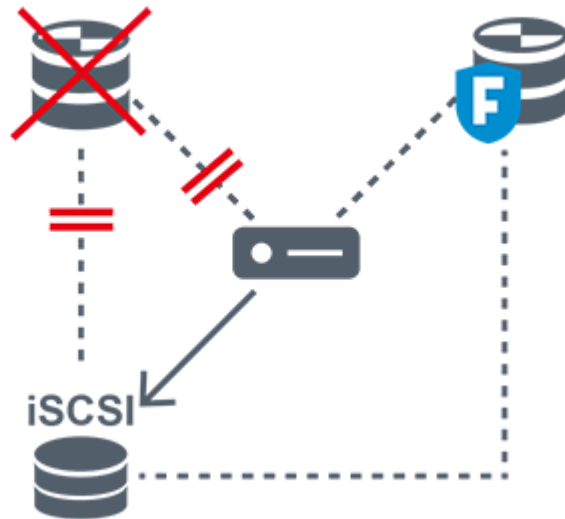
Enregistrement VRM secondaire







	VRM principal		VRM secondaire
	Périphérique de stockage iSCSI		Connexion de contrôle



Enregistrement de serveur VRM de basculement



	VRM principal		Serveur VRM de basculement principal
	Périphérique de stockage iSCSI		Encodeur
.....	Connexion de contrôle	→	Flux vidéo

5.2.4


Lecture de sources d'enregistrements VRM

Les graphiques suivants présentent les volets des Images avec la lecture à partir de toutes les sources d'enregistrements VRM possibles. Chaque graphique indique le périphérique de stockage, l'instance de VRM (le cas échéant) et une section du volet des Images comme exemple de la lecture. Le cas échéant, la source des enregistrements est indiquée par une icône appropriée, sur la barre du volet des Images.



- *Lecture d'un enregistrement unique, page 33*
- *Lecture d'enregistrement VRM double, page 34*
- *Lecture de l'enregistrement VRM principal avec serveur VRM de basculement facultatif, page 35*
- *Lecture de l'enregistrement VRM secondaire avec serveur VRM de basculement facultatif, page 36*
- *Automatic Network Replenishment, page 37*

Lecture d'un enregistrement unique

Le volet des Images s'affiche lorsqu'un VRM principal seulement est configuré. Vous ne pouvez pas sélectionner une autre source d'enregistrement.

 : Si la lecture est configurée pour ce poste de commande, elle est assurée directement par le périphérique de stockage iSCSI.






	Périphérique de stockage iSCSI
	VRM principal

Lecture d'enregistrement VRM double

Un VRM principal et un VRM secondaire sont configurés. Cliquez sur l'icône de la source des enregistrements pour afficher la lecture principale ou secondaire.

Si la lecture est configurée pour ce poste de commande, elle est assurée directement par le périphérique de stockage iSCSI.



	Périphérique de stockage iSCSI
	VRM principal
	VRM secondaire

Lecture de l'enregistrement VRM principal avec serveur VRM de basculement facultatif

Pendant que le serveur VRM principal fonctionne, il assure la lecture. Le serveur VRM de basculement fonctionne dans l'état inactif.

Si la lecture est configurée pour ce poste de commande, elle est assurée directement par le dispositif de stockage iSCSI.

Si un enregistrement VRM secondaire ou ANR est configuré, vous pouvez changer la source des enregistrements.







Lorsque le VRM principal n'est pas connecté, le VRM de basculement configuré assure la lecture. Fermez le volet des Images et affichez de nouveau la caméra dans un volet des Images :



Lorsque le VRM principal et le VRM de basculement principal facultatif ne sont connectés ni l'un ni l'autre, l'encodeur assure la lecture. Fermez le volet des Images et affichez de nouveau la caméra dans un volet des Images :



	Dispositif de stockage iSCSI
	VRM principal
	Serveur VRM de basculement principal
	Encodeur

La lecture de l'encodeur ne peut accéder qu'à une période d'enregistrement limitée.

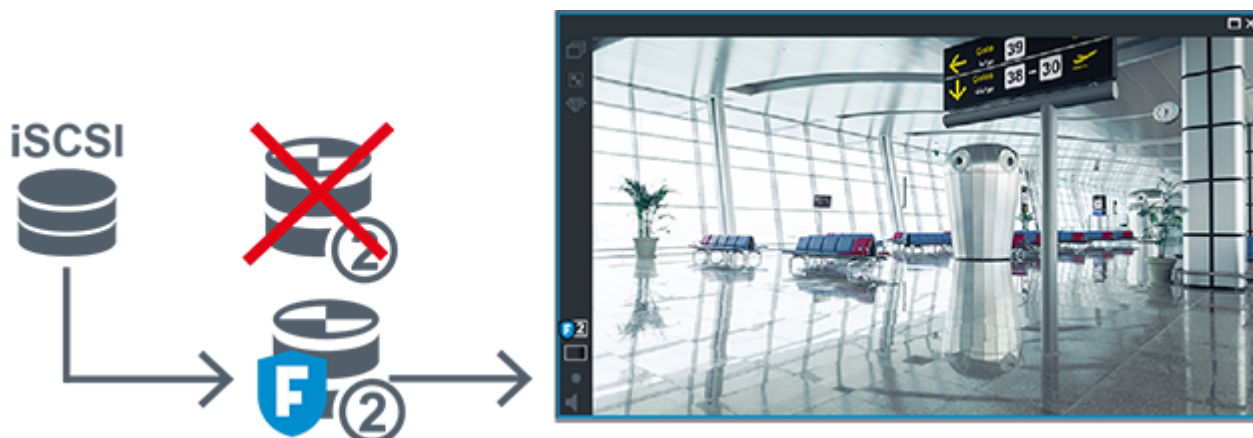
Lecture de l'enregistrement VRM secondaire avec serveur VRM de basculement facultatif

Pendant que le VRM secondaire fonctionne, il assure la lecture. Le serveur VRM de basculement fonctionne dans l'état inactif.

Si la lecture est configurée pour ce poste de commande, elle est assurée directement par le dispositif de stockage iSCSI.







Lorsque le VRM secondaire n'est pas connecté, le VRM de basculement configuré assure la lecture. Fermez le volet des Images et affichez de nouveau la caméra dans un volet des Images :



Lorsque le VRM secondaire et le VRM de basculement secondaire facultatif ne sont ni l'un ni l'autre connectés, l'encodeur assure la lecture. Fermez le volet des Images et faites glisser de nouveau la caméra vers un volet des Images :



	Dispositif de stockage iSCSI
	VRM principal
	Serveur VRM de basculement secondaire
	Encodeur

La lecture de l'encodeur ne peut accéder qu'à une période d'enregistrement limitée.




Automatic Network Replenishment

ANR est configuré. Cliquez sur l'icône de la source des enregistrements pour afficher la lecture principale (lecture de basculement principale, lecture de l'encodeur principale) ou la lecture de l'ANR.

Si la lecture est configurée pour ce poste de commande, elle est assurée directement par le dispositif de stockage iSCSI.





	Dispositif de stockage iSCSI
	VRM principal
	Carte SD

5.2.5

Vue d'ensemble des événements liés au stockage

Ce chapitre décrit les différents événements liés au stockage.

État du stockage tampon

En cas de panne réseau ou de stockage centralisé, la fonction ANR assure que l'encodeur transmet l'enregistrement mis en mémoire tampon localement de la période manquante au stockage centralisé une fois la panne résolue.

Les états possibles du stockage tampon sont les suivants :

- **État du stockage inconnu**
- **État du stockage OK**
- **Niveau de remplissage critique du stockage tampon**
- **État du stockage en échec**

Dépassement du stockage tampon

Cet événement indique que le tampon de stockage est déjà plein et que l'enregistrement n'est plus transmis au stockage central.

État du stockage / État du stockage secondaire

État du stockage indique l'état de la connexion entre une caméra et le stockage central.

L'événement **État du stockage en échec** est déclenché si la caméra perd la connexion au stockage central. Si la déconnexion ne dure qu'un court moment, cet événement n'indique pas nécessairement que les données vidéo sont perdues.

Les états de stockage sont les suivants :

- **État du stockage inconnu**
- **État du stockage OK**
- **État du stockage en échec**

État du moniteur d'enregistrement / État du moniteur d'enregistrement secondaire

Cet événement indique une surveillance de l'enregistrement. Tant que la caméra peut mettre en mémoire tampon l'enregistrement dans la RAM, aucune alarme n'est déclenchée.

L'événement **Perte de l'enregistrement d'état du moniteur d'enregistrement** n'est

déclenché que si, dans les deux dernières minutes, les données vidéo ne peuvent plus être mise en mémoire tampon dans la RAM et sont perdues. L'événement indique également la période pendant laquelle les données vidéo ont été perdues.

Les états du moniteur d'enregistrement sont les suivants :

- **État du moniteur d'enregistrement inconnu**
- **État du moniteur d'enregistrement ok**
- **Perte de l'enregistrement d'état du moniteur d'enregistrement**

Se reporter à

- *Automated Network Replenishment (ANR), page 28*
- *Configuration des événements et des alarmes, page 331*

5.3

Gestion des alarmes

Il est possible de configurer les alarmes individuellement de façon à ce qu'elles soient traitées par un ou plusieurs groupes d'utilisateurs. Lorsqu'une alarme se déclenche, elle apparaît dans la liste des alarmes de tous les utilisateurs des groupes configurés pour recevoir cette alarme. Lorsque l'un de ces utilisateurs commence à traiter l'alarme, cette dernière disparaît de la liste des alarmes de tous les autres utilisateurs.

Les alarmes s'affichent sur le moniteur d'alarme d'un poste de commande. Ce comportement est décrit dans les paragraphes suivants.

Déroulement d'une alarme

1. Une alarme se produit dans le système.
2. Les notifications d'alarme apparaissent dans les listes des alarmes de tous les utilisateurs configurés pour cette alarme. Les images vidéo d'alarme s'affichent immédiatement sur les moniteurs configurés. S'il s'agit d'une alarme avec affichage contextuel automatique, la vidéo liée à cette alarme s'affiche également automatiquement sur les moniteurs d'alarme du poste de commande Operator Client. Si l'alarme est configurée pour s'effacer automatiquement, elle disparaît de la liste des alarmes une fois que la durée d'effacement automatique (configurée dans Configuration Client) s'est écoulée.
Sur les moniteurs, les éventuelles vues en quadravision des VIP XD sont temporairement remplacées par des affichages plein écran.
3. L'un des utilisateurs accepte l'alarme. La vidéo en état d'alarme s'affiche alors sur le poste de commande de cet utilisateur (si elle ne s'est pas déjà affichée via la fonction d'affichage contextuel automatique). L'alarme est supprimée de toutes les autres listes des alarmes et vues affichant les vidéos en état d'alarme.
4. L'utilisateur ayant accepté l'alarme appelle un flux de travail pouvant impliquer, par exemple, de lire un plan d'action et d'entrer des commentaires. Cette étape est facultative. Les conditions pour les flux de travail peuvent en fait être configurées par l'administrateur.
5. Pour terminer, l'utilisateur efface l'alarme. Cette opération supprime l'alarme de sa liste des alarmes et de l'affichage des alarmes.
Sur un groupe de moniteurs, les moniteurs réaffichent les images des caméras qui étaient affichées avant le déclenchement de l'alarme.

Fenêtre d'image d'alarme

1. Lorsqu'il faut afficher une vidéo en état d'alarme, la fenêtre d'image d'alarme vient remplacer la fenêtre d'image en temps réel ou Lecture sur le moniteur chargé d'afficher les alarmes.

2. Chaque alarme est associée à une ligne de volets des Images pouvant comporter 5 volets maximum. Ces volets peuvent afficher des vidéos en Mode Temps Réel, des vidéos en Mode Lecture et des cartes.
Sur un groupe de moniteurs, chaque alarme peut appeler les caméras d'une ligne de moniteurs. Le nombre de caméras de la ligne est limité au nombre de colonnes du groupe de moniteurs. Les moniteurs de la ligne qui ne sont pas utilisés pour la vidéo d'alarme peuvent être configurés pour poursuivre l'affichage en cours ou pour afficher un écran vierge.
3. Les alarmes prioritaires s'affichent au-dessus des alarmes de niveau de priorité inférieur, à la fois sur les lignes de moniteurs et sur les lignes d'alarmes du poste de commande Operator Client.
4. Si une alarme supplémentaire doit être affichée mais qu'il n'y a plus suffisamment de place dans la fenêtre d'image d'alarme, les alarmes les moins importantes « s'empilent » dans la ligne du bas. Vous pouvez faire défiler les alarmes empilées à l'aide des commandes situées à gauche de la ligne d'alarmes.
Vous pouvez faire défiler les alarmes empilées sur les groupes de moniteurs à l'aide des boutons de commande de la fenêtre **Moniteurs** de l'écran du poste de commande Operator Client. Les moniteurs en alarme sont signalés par des icônes rouges aux voyants clignotants.
Le titre, l'heure et la date de l'alarme peuvent s'afficher, au choix, sur tous les moniteurs, ou uniquement sur le premier moniteur de la ligne d'alarmes.
5. Pour les alarmes de priorité égale, l'administrateur peut configurer l'ordre d'affichage :
 - Mode Dernier entré, premier sorti : les nouvelles alarmes s'insèrent *au-dessus* des alarmes existantes de même priorité.
 - Mode Premier entré, premier sorti : les nouvelles alarmes s'insèrent *en dessous* des alarmes existantes de même priorité.
6. La ligne de l'image d'une alarme peut s'afficher dans la fenêtre d'image d'alarme de deux manières différentes :
 - Au moment de la génération de l'alarme (affichage contextuel automatique) : C'est le cas quand la priorité d'alarme est supérieure à la priorité d'affichage.
 - Au moment de l'acceptation de l'alarme : C'est le cas quand la priorité d'alarme est inférieure à la priorité d'affichage.

Alarmes avec affichage contextuel automatique

Il est possible de configurer les alarmes pour qu'elles s'affichent automatiquement (affichage contextuel) dans la fenêtre Image d'alarme, en fonction de leur niveau de priorité. Un niveau de priorité est également associé aux vues en Mode Temps Réel et Lecture de chaque groupe d'utilisateurs. Lors de la réception d'une alarme ayant une priorité supérieure à celle de la vue de l'utilisateur, une ligne correspondante s'affiche automatiquement dans la fenêtre Image d'alarme. Si la fenêtre Image d'alarme n'est pas ouverte, elle vient automatiquement remplacer la fenêtre Image en temps réel ou Lecture sur le moniteur d'alarme.

Bien que les alarmes à affichage contextuel automatique s'affichent dans la fenêtre Image d'alarme, elles ne sont pas automatiquement acceptées. Il est possible de les afficher simultanément sur les vues de plusieurs utilisateurs. Lorsqu'un utilisateur accepte une alarme à affichage contextuel automatique, l'alarme est supprimée de la Liste des Alarmes et des vues d'alarme de tous les autres utilisateurs.

Gestion d'alarme en cas d'arrêt

À l'arrêt du serveur, toutes les alarmes actives sont conservées. Les alarmes sont rétablies et réapparaissent dans la fenêtre **Liste des Alarmes**, lorsque le système redémarre.

Les alarmes à l'état **Acceptée** ou **Flux de travail** sont automatiquement redéfinies sur l'état **Active** lorsque le système redémarre. Les commentaires saisis pour les alarmes à l'état **Flux de travail** sont conservés.

**Remarque!**

Les données d'alarme sont automatiquement enregistrées toutes les minutes, la perte de données maximum se limite donc aux données accumulées pendant une minute.

Se reporter à

- *Configuration des durées pré-alarme et post-alarme d'une alarme, page 337*

5.4

Mappage des événements ONVIF

**Remarque!**

Sachez que cette fonctionnalité sera bientôt obsolète.

Utilisez ONVIF Camera Event Driver Tool pour un mappage des événements ONVIF plus facile.

Voir *Démarrage de ONVIF Camera Event Driver Tool à partir de Configuration Client, page 215.*

Utilisation prévue

L'utilisation prévue est le mappage des événements ONVIF aux événements BVMS. Les événements ONVIF peuvent alors déclencher des alarmes et des enregistrements BVMS. Vous pouvez définir des mappages d'événements par défaut uniquement valides pour un dispositif ONVIF spécifique, pour tous les dispositifs ONVIF de même fabricant et de même modèle, ou pour tous les dispositifs ONVIF d'un même fabricant. Les mappages d'événements par défaut sont automatiquement affectés à tous les encodeurs ONVIF ajoutés à l'aide de l'Assistant de balayage BVMS ou ajoutés manuellement.

Lorsque vous ajoutez un encodeur ONVIF à la configuration BVMS sans connexion à cet encodeur ONVIF, aucun mappage d'événement n'est affecté. Vous pouvez mettre à jour un encodeur ONVIF de ce type avec des mappages d'événements provenant d'un encodeur ONVIF du même fabricant et/ou de même modèle que ceux déjà ajoutés.

Vous définissez des mappages d'événements spécifiques pour chacune des sources suivantes :

- Encodeur ONVIF
- Caméras de cet encodeur ONVIF
- Relais de cet encodeur ONVIF
- Entrées de cet encodeur ONVIF

Exemple

Un événement de détection de mouvement se produit dans une caméra ONVIF. Cet événement déclenche un événement **Mouvement détecté** dans BVMS.

Pour ce faire, vous configurez cette caméra ONVIF comme suit :

- Rubrique ONVIF (*MotionDetection*)
- Élément de données ONVIF (*motion*)
- Type de données ONVIF (*boolean*)
- Valeur de données ONVIF (*true*)

Remarque : il n'est pas suffisant de configurer uniquement l'événement **Mouvement détecté**. Vous devez également configurer l'événement **Mouvement arrêté**. Vous devez toujours configurer les événements par deux.

Importation ou exportation d'un tableau de mappage

Vous pouvez exporter un tableau de mappage à partir de l'ordinateur sur lequel vous l'avez créé et importer ce tableau de mappage sur un ordinateur sur lequel le tableau de mappage requis n'est pas disponible.

Dépannage

Vous pouvez créer des fichiers journaux à des fins de dépannage.

Se reporter à

- *Configuration d'un tableau de mappage ONVIF, page 248*
- *Activation de la journalisation des événements ONVIF, page 392*
- *Page Événements d'encodeur ONVIF, page 244*

5.5

Déconnexion en cas d'inactivité

Utilisation prévue

L'utilisation prévue de la déconnexion en cas d'inactivité est de protéger un Operator Client ou un Configuration Client en l'absence de l'opérateur ou de l'administrateur.

Vous pouvez configurer le système par groupe d'utilisateurs de telle sorte que l'Operator Client soit automatiquement déconnecté après une période donnée sans activité. Pour le Configuration Client, il n'existe aucun groupe d'utilisateurs. Le paramètre de déconnexion en cas d'inactivité est uniquement valide pour l'utilisateur **admin**.

Toutes les opérations effectuées avec le clavier, la souris et le clavier de vidéosurveillance affectent la période définie pour la déconnexion en cas d'inactivité. Les activités automatiques d'Operator Client n'affectent pas cette durée. Les activités automatiques du Configuration Client comme le chargement d'un firmware ou la configuration d'iSCSI empêchent la déconnexion en cas d'inactivité.

Vous pouvez également configurer la déconnexion en cas d'inactivité pour un client Web BVMS.

Juste avant une déconnexion en cas d'inactivité, une boîte de dialogue rappelle à l'utilisateur d'empêcher de manière active la déconnexion en cas d'inactivité.

Le Journal des Connexions enregistre une entrée lorsqu'une déconnexion en cas d'inactivité se produit.

Exemple

Si un poste de commande se trouve dans une zone publique, la déconnexion en cas d'inactivité minimise le risque qu'une personne non autorisée accède à un poste de commande Operator Client laissé sans surveillance.

Un membre du groupe d'administrateurs doit être automatiquement déconnecté après une période d'inactivité, mais un agent de surveillance (du groupe des opérateurs) visionne simplement les vidéos sans utiliser le système et ne souhaite pas une déconnexion en cas d'inactivité.

Restrictions

L'activité du Client SDK ne prend pas en charge la déconnexion en cas d'inactivité. Cela signifie que l'activité du Client SDK n'affecte pas la période spécifiée.

Se reporter à

- *Boîte de dialogue Options (menu Paramètres), page 122*
- *Page des fonctionnalités d'Operator, page 350*

5.6 Operator Client non dépendant de la version

Pour le mode compatibilité, l'Operator Client et le Management Server doivent tous deux avoir une version ultérieure à 5.5.

Un utilisateur d'Operator Client peut se connecter à un Management Server sur lequel une version logicielle antérieure est exécutée.

Si le serveur dispose d'une configuration plus récente que celle du poste de commande Operator Client, cette configuration est copiée automatiquement sur le poste de commande Operator Client. L'utilisateur peut choisir de télécharger la nouvelle configuration.

L'Operator Client offre un ensemble réduit de fonctionnalités et est connecté à ce Management Server.

Les fonctionnalités suivantes relatives au Management Server sont disponibles après connexion à un Management Server exécutant une version précédente :

- Préférences utilisateur
- Démarrage manuel de l'enregistrement
- Affichage de l'état des dispositifs
- Permutation de l'état des relais
- Recherche dans le journal des connexions
La recherche d'événements n'est pas possible.
- Recherche de serveur
- Exportation à distance

5.6.1 Utilisation du mode Compatibilité



: cet état de l'Operator Client s'affiche en mode compatibilité.

Dans la version ultérieure à la version 5.5, l'Operator Client fonctionne en mode compatibilité si la version du Management Server est inférieure à la version de l'Operator Client.

Dans la version ultérieure à 10.0, l'Operator Client fonctionne en mode compatibilité dans les cas suivants :

- Tous les services de communication ne peuvent pas être connectés par l'Operator Client.
- Exemple : le Management Server est en cours d'exécution, mais WebServiceHost est arrêté.
- Des modifications ont été apportées à l'interface de communication entre l'Operator Client et le Management Server

Seules les modifications de l'interface sémantique ou l'arrêt partiel des services peuvent entraîner l'absence de certaines fonctionnalités dans l'Operator Client.

5.7 Affichage des modes d'une caméra panoramique

Ce chapitre illustre les modes d'affichage d'une caméra panoramique qui sont disponibles dans BVMS.

Les modes d'affichage suivants sont disponibles :

- Vue circulaire
- Vue panoramique
- Vue recadrée

Les modes d'affichage panoramique et recadré sont créés par le processus de déformation dans BVMS. La déformation d'angle n'est pas utilisée.

L'administrateur doit configurer la position de montage d'une caméra panoramique dans Configuration Client.

Vous pouvez redimensionner le volet des images d'une caméra si nécessaire. Le volet des images n'est pas limité au rapport hauteur/largeur de 4:3 ou 16:9.

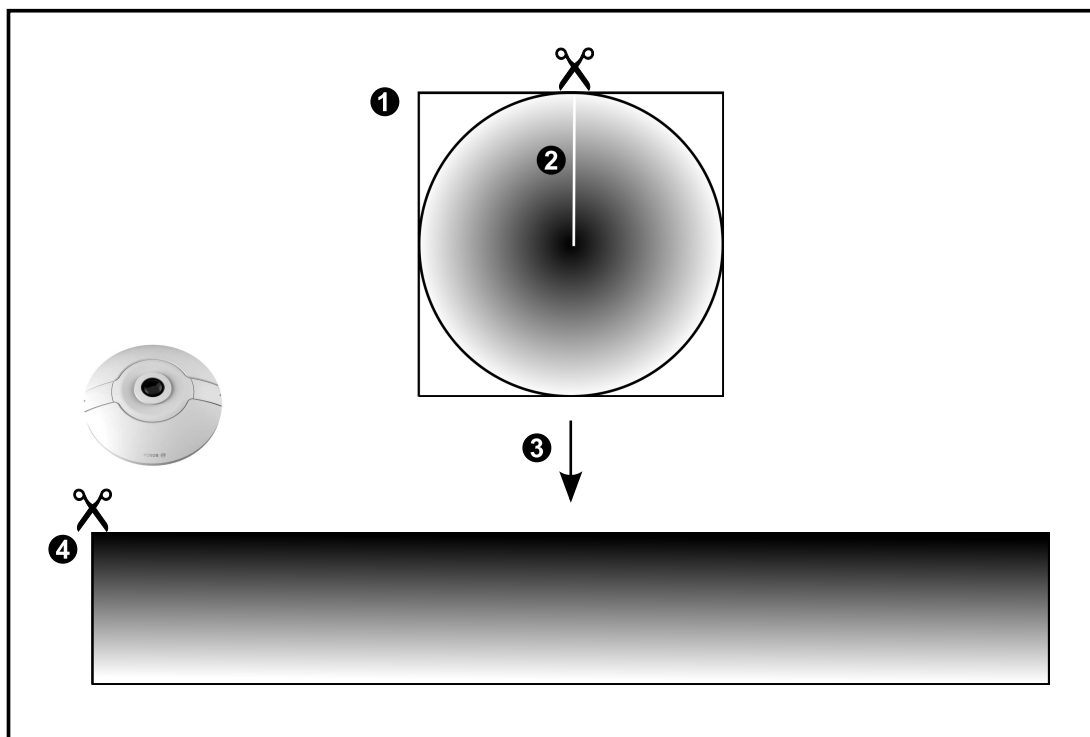
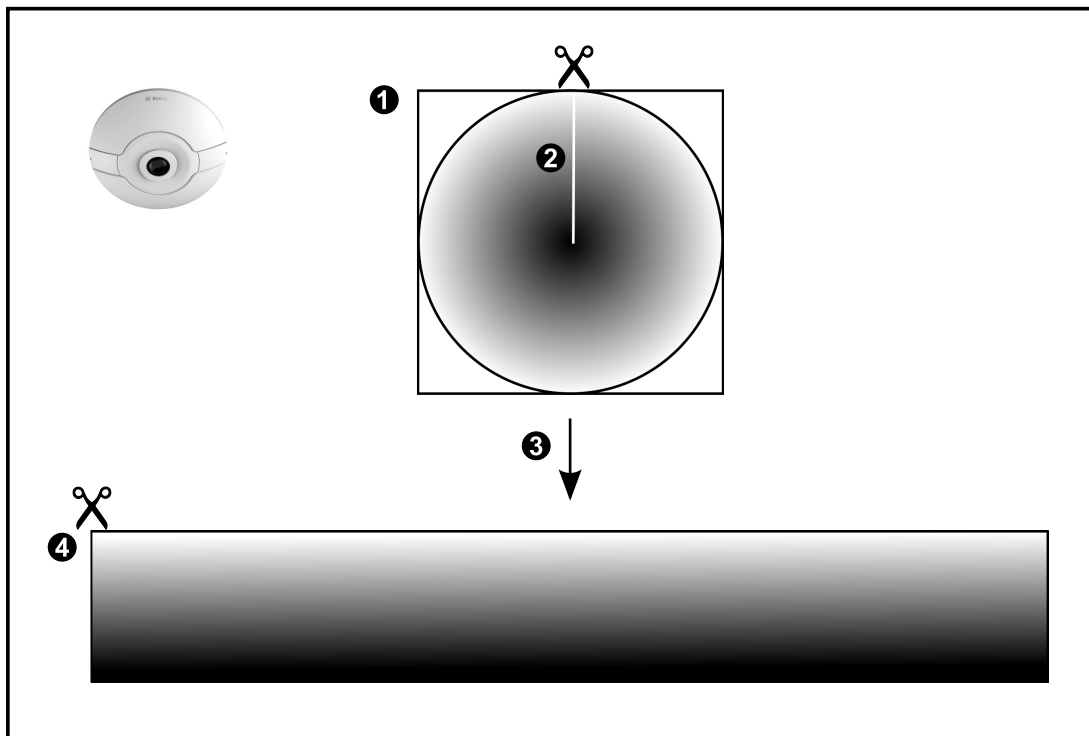
Se reporter à

- *Configuration de positions prédéfinies et de commandes auxiliaires, page 311*

5.7.1

Caméra panoramique à 360 ° - fixée au sol ou au plafond

La figure suivante illustre la déformation d'une caméra à 360 ° qui est fixée au sol ou au plafond.

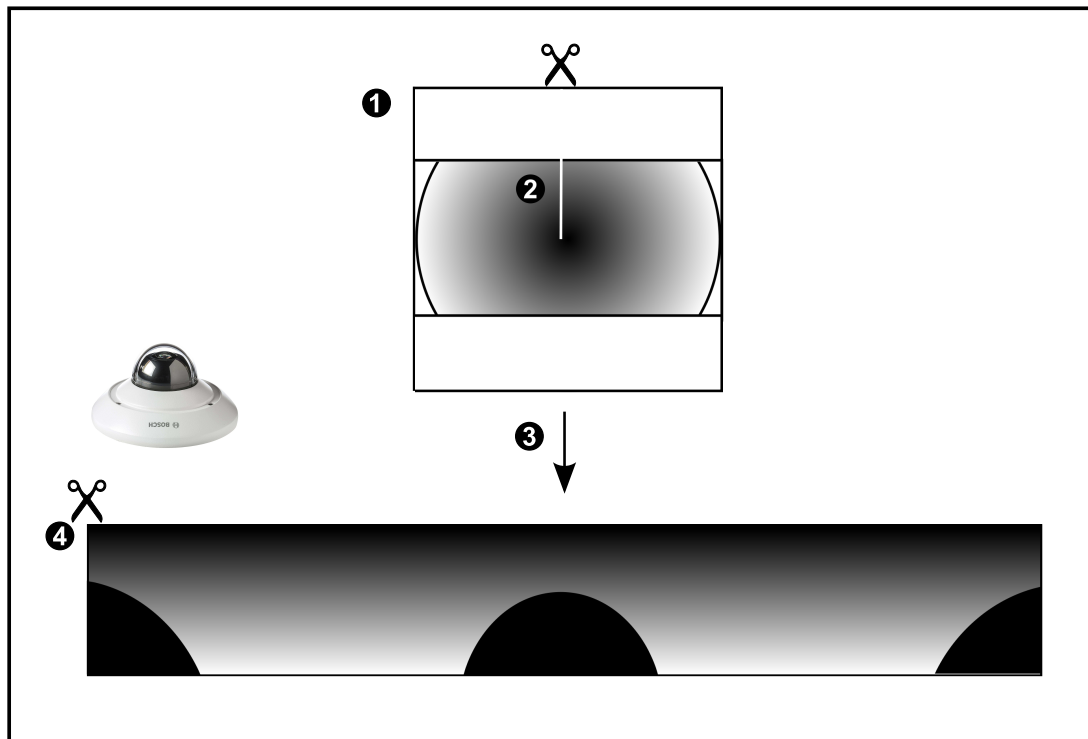
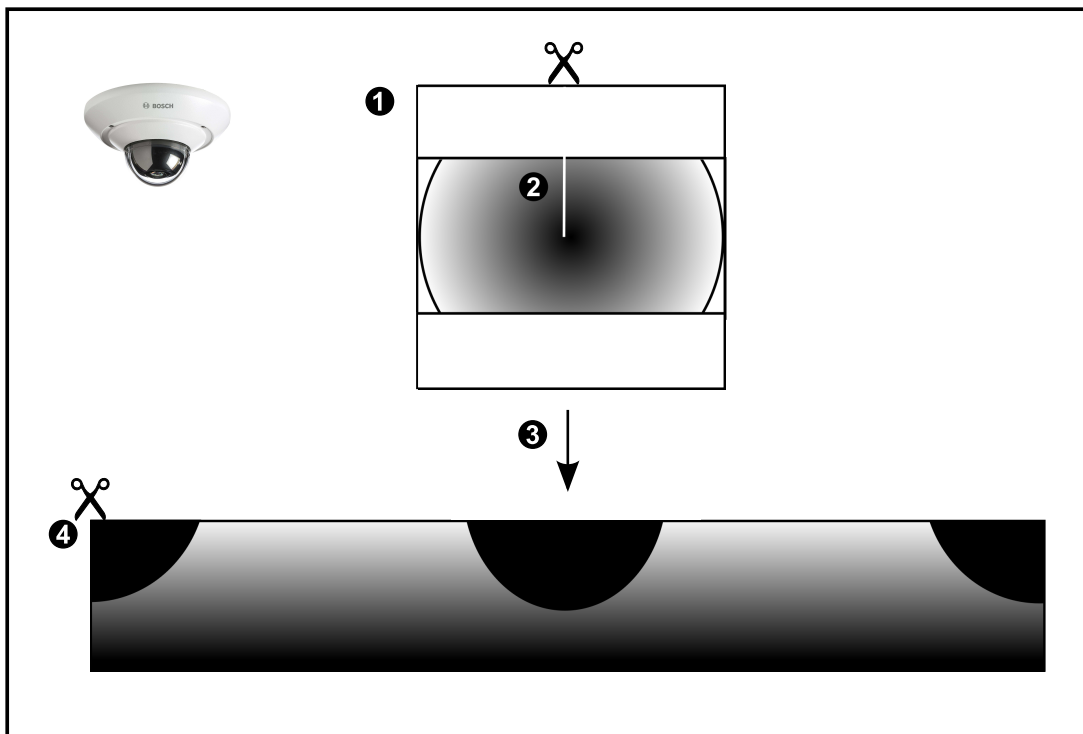


1	Image continue	3	Déformation
2	Ligne de découpe (l'opérateur peut changer sa position lorsqu'il n'est pas en zoom avant)	4	Vue panoramique

5.7.2

Caméra panoramique à 180 ° - fixée au sol ou au plafond

La figure suivante illustre la déformation d'une caméra à 180 ° qui est fixée au sol ou au plafond.

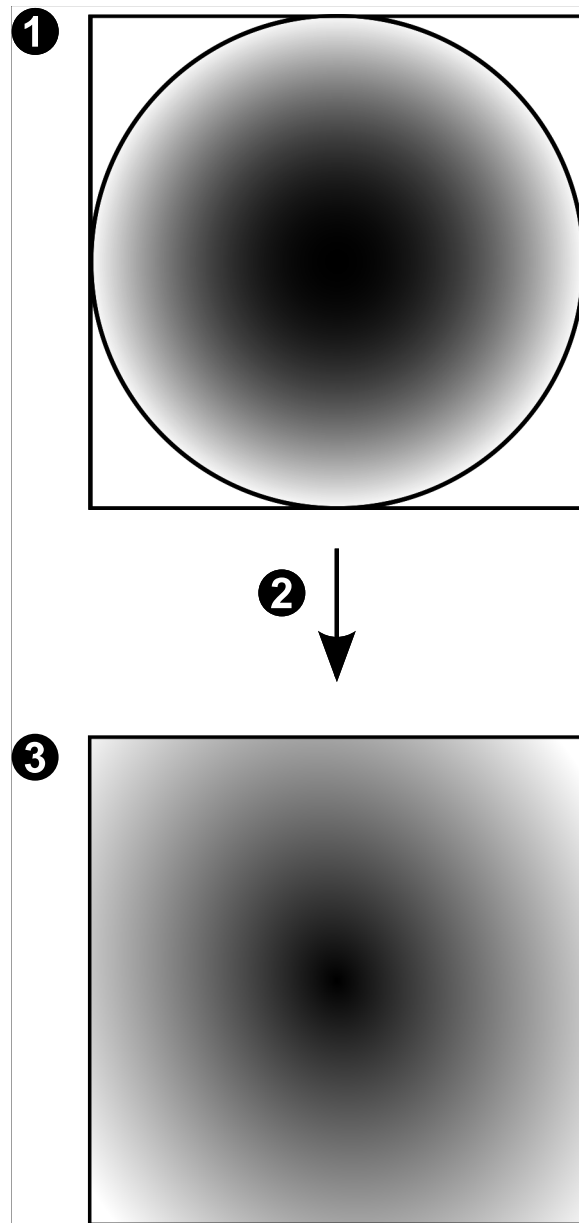


1	Image continue	3	Déformation
2	Ligne de découpe (l'opérateur peut changer sa position lorsqu'il n'est pas en zoom avant)	4	Vue panoramique

5.7.3

Caméra panoramique à 360 ° - fixée au mur

La figure suivante illustre la déformation d'une caméra à 360 ° qui est fixée au mur.

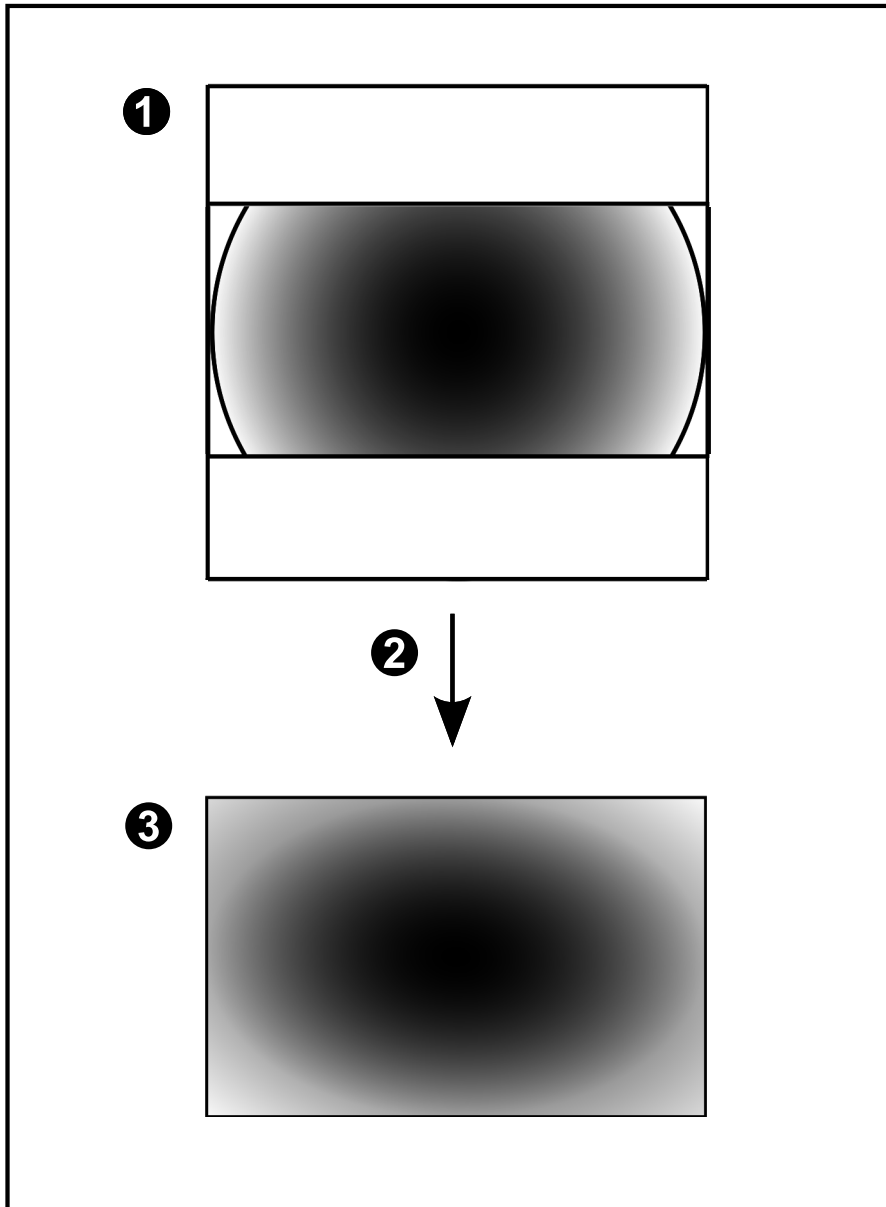


1	Image continue	3	Vue panoramique
2	Déformation		

5.7.4

Caméra panoramique à 180 ° - fixée au mur

La figure suivante illustre la déformation d'une caméra à 180 ° qui est fixée au mur.



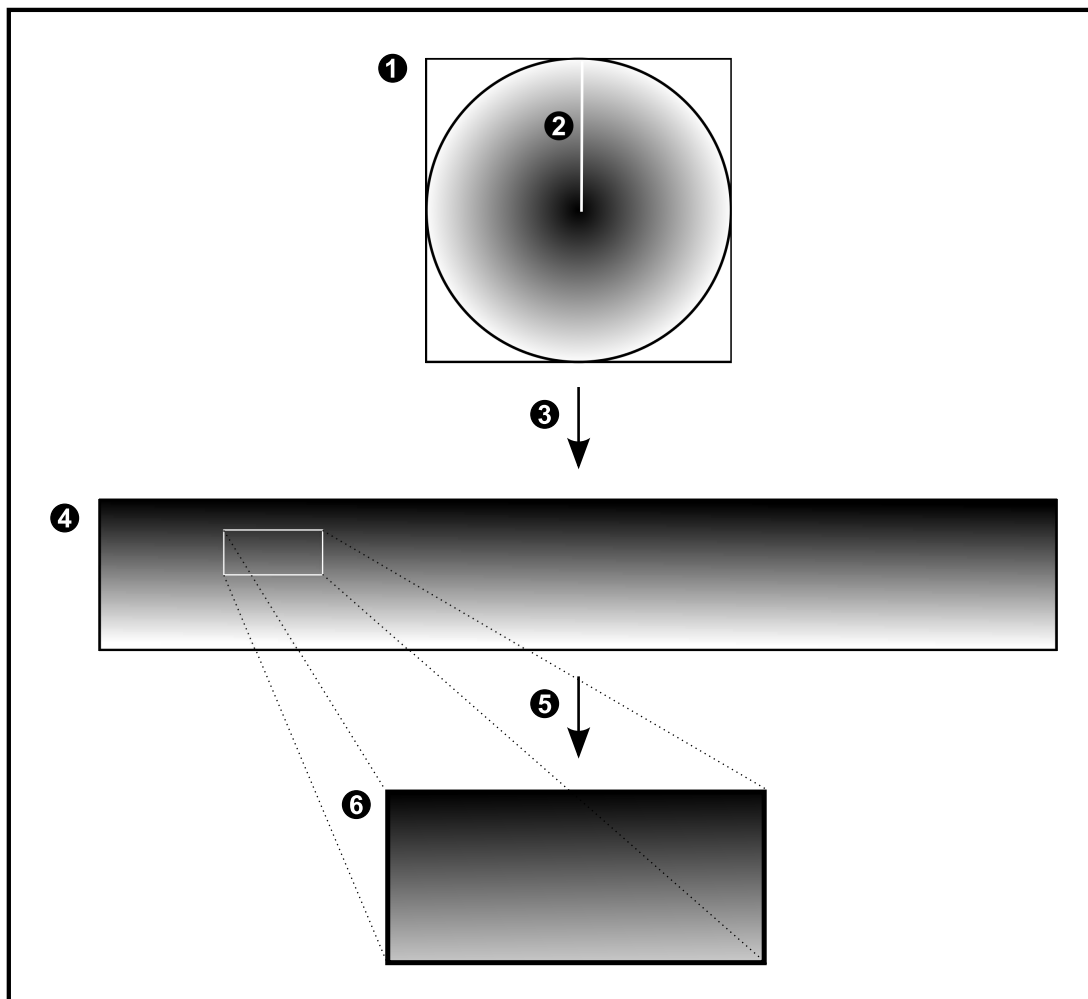
1	Image continue	3	Vue panoramique
2	Déformation		

5.7.5

Vue recadrée sur une caméra panoramique

L'exemple suivant illustre le recadrage d'une caméra à 360 ° qui est fixée au sol ou au plafond.

La section rectiligne utilisée pour le recadrage est fixe. Vous pouvez modifier cette section dans le volet de l'image recadrée à l'aide des commandes PTZ disponibles.



1	Image continue	4	Vue panoramique
2	Ligne de découpe (l'opérateur peut changer sa position lorsqu'il n'est pas en zoom avant)	5	Recadrage
3	Déformation	6	Volet d'image recadrée

5.8 Tunnelisation SSH

BVMS offre une connectivité à distance via la tunnelisation SSH (Secure Shell). La tunnelisation SSH construit un tunnel chiffré établi par une protocole SSH/une connexion socket. Ce tunnel chiffré peut fournir transport au trafic chiffré et non chiffré. La mise en œuvre de Bosch SSH utilise également le protocole Omni-Path, qui est un protocole de communication à faible latence hautement performant développé par Intel.

Aspects techniques et restrictions

- La tunnelisation SSH utilise le port 5322. Ce port ne peut pas être modifié.
- Le service SSH doit être installé sur le même serveur que le Management Server BVMS.
- (Enterprise) les comptes utilisateur doivent avoir un mot de passe configuré.
- (Enterprise) les comptes utilisateur sans mot de passe ne peuvent pas se connecter au moyen d'une connexion SSH.
- Les caméras à stockage locale ne prennent pas en charge la connexion SSH.
- Configuration Client ne peut pas se connecter à distance via SSH. Une connexion Configuration Client doit s'effectuer par un mappage de port.
- Operator Client vérifie la connexion avec le service SSH toutes les 15 secondes. Si la connexion est interrompue, Operator Client reteste la connexion chaque minute.

Mappage de port

- ▶ Configurez un acheminement de port afin que le Management Server BVMS utilise le port 5322 pour les connexions à la fois internes et externes.
Il s'agit de l'unique entrée de mappage de port que vous devez effectuer pour tout le système. Le mappage de port BVMS n'est pas nécessaire.

Communication chiffrée

Une fois la connexion établie via un tunnel SSH, toutes les communications entre le Management Server BVMS et un client distant sont chiffrées.

5.9 Trajets multiples

BVMS fournit des trajets multiples pour les systèmes à contrôleur double. Les trajets multiples constituent une technique de tolérance aux pannes qui définit plusieurs chemins d'accès physiques entre la caméra et ses périphériques de stockage iSCSI via des connexions réseau redondantes. Lorsque vous utilisez les trajets multiples, l'enregistrement et la lecture de données vidéo sont possibles, même en cas de défaillance du contrôleur iSCSI.

Exigences préalables et restrictions

- L'unité iSCSI NetApp E2800 à double contrôleur est installée.
- Firmware 6.43 permet aux dispositifs qui enregistrent sur E2800 d'utiliser des chemins alternatifs.
- Les trajets multiples de VRM 3.71 pour surveiller et consigner les dispositifs sont activés.
- Deux ports physiques iSCSI sont configurés par contrôleur : 2 x 2 RJ45 ou 2 x 2 ports optiques.
- La vitesse de la liaison doit être de 10 Gbit/s pour obtenir des performances optimales.
- Le mode Dual Simplex utilisé dans l'E2700 n'est plus pris en charge.

Pour plus d'informations sur l'installation de DSA E2800 Full Duplex, voir le manuel d'installation de DSA E-Series E2800.

5.10 **Open ID Connect (OIDC) et fournisseur d'identité (IDP)**

BVMS prend en charge l'authentification via un service de fournisseur d'autorisation externe. Avec Open ID Connect (OIDC), l'authentification est gérée via un fournisseur d'identité (IdP) préconfiguré, tandis que BVMS se concentre sur la tâche d'autorisation.

Cela est utile pour les grands groupes d'entreprises qui ne souhaitent pas gérer les utilisateurs de manière individuelle. Grâce au mappage des groupes d'utilisateurs aux groupes IdP, l'accès est accordé aux utilisateurs selon leurs besoins.

Pour plus d'informations, voir : *Boîte de dialogue Options (menu Paramètres), page 122* et *Page Groupes d'utilisateurs, page 341*.

6 Matériel pris en charge



Remarque!

Ne connectez jamais un périphérique à plusieurs BVMS ! Vous risqueriez d'enregistrer des temps morts et de provoquer d'autres effets indésirables.

Vous pouvez connecter le matériel suivant à BVMS :

- Clients vidéo mobiles comme un iPhone ou un iPad via DynDNS
- Diverses caméras IP. encodeurs et ONVIF caméras (en temps réel uniquement ou via Video Streaming Gateway)
Connexion via le réseau
- Encodeurs temps réel uniquement avec stockage local
Connexion via le réseau
- Stockeurs iSCSI
Connexion via le réseau
- Caméras analogiques
Connectées aux encodeurs,
- Décodeurs
Connexion via le réseau
- Moniteurs
Connectés à un décodeur, à une matrice Bosch Allegiant, à un poste de commande BVMS client
- Matrice Allegiant Bosch (version du firmware : 8.75 ou supérieure, version MCS : 2.80 ou supérieure)
Connexion à un port de communication du Management Server ou à un ordinateur distant et à un encodeur IP sur le réseau.
- Clavier KBD-Universal XF
Connecté à un port USB d'un poste de commande BVMS.
- Bosch IntuiKey
Connecté au port de communication d'un poste de commande BVMS (version de firmware : 1.82 ou ultérieure) ou à un décodeur matériel (VIP XD).
Si vous connectez le clavier à un poste de commande, l'utilisateur peut commander l'intégralité du système. Si vous connectez le clavier à un décodeur VIP XD, l'utilisateur ne peut commander que les moniteurs.
- Serveur de messagerie SMTP
Connexion via le réseau
- POS
Connexion via le réseau
- ATM
Connexion via le réseau
- Dispositif de surveillance réseau
Connexion via le réseau
- Modules E/S
Connexion via le réseau
Seuls les périphériques ADAM sont pris en charge.

Tous les dispositifs connectés via le réseau sont reliés à un commutateur réseau. Les ordinateurs de BVMS sont également connectés à ce dispositif.

6.1 Installation du matériel

BVMS prend en charge les composants matériel suivants :

- KBD-Universal XF
 - Bosch IntuiKey
 - Matrice Bosch Allegiant avec caméras et moniteur : connexion au port COM de l'un des ordinateurs du réseau et aux encodeurs IP reliés au réseau
 - Encodeurs avec caméras analogiques
 - Encodeurs pour stockage local
 - Caméras IP et AutoDomes IP
 - Moniteurs connectés à un décodeur (il est possible d'utiliser des groupes de moniteurs pour le traitement des alarmes)
 - Systèmes DVR avec caméras
 - Dispositifs ATM / POS
 - Modules E/S
- Seuls les dispositifs ADAM sont pris en charge.

6.2 Installation d'un clavier KBD universel XF



Remarque!

Consultez le manuel d'Instructions fourni avec votre clavier KBD-Universal XF disponible dans le catalogue produit en ligne.

Pour en savoir plus

Pour plus d'informations et de détails sur les logiciels, le téléchargement et la documentation, visitez le site www.boschsecurity.com et affichez la page produit respective.

Vous pouvez connecter le matériel suivant à BVMS :

- Clients vidéo mobiles comme un iPhone ou un iPad via DynDNS
- Diverses caméras IP, encodeurs et ONVIF caméras (en temps réel uniquement ou via Video Streaming Gateway)
Connexion via le réseau
- Encodeurs temps réel uniquement avec stockage local
Connexion via le réseau
- Stockeurs iSCSI
Connexion via le réseau
- Caméras analogiques
Connectées aux encodeurs,
- Décodeurs
Connexion via le réseau
- Moniteurs
Connectés à un décodeur, à une matrice Bosch Allegiant, à un poste de commande BVMS client
- Matrice Allegiant Bosch (version du firmware : 8.75 ou supérieure, version MCS : 2.80 ou supérieure)
Connexion à un port de communication du Management Server ou à un ordinateur distant et à un encodeur IP sur le réseau.

6.3 Connexion d'un clavier IntuiKey Bosch à BVMS

Ce chapitre fournit des informations générales sur la configuration d'un clavier Bosch IntuiKey.

6.3.1

Scénarios de connexion d'un clavier numérique IntuiKey de Bosch

Vous pouvez connecter un clavier Bosch IntuiKey au port COM d'un poste de commande BVMS (scénario 1) ou à un décodeur matériel (par exemple, VIP XD, scénario 2).

En connectant le clavier à un poste de commande BVMS, vous pouvez contrôler l'ensemble du système. En connectant le clavier à un décodeur, vous ne pouvez contrôler que les moniteurs analogiques du système.

Si vous connectez le clavier à un Enterprise Operator Client, vous pouvez contrôler les caméras d'un Management Server spécifique en appuyant tout d'abord sur la touche serveur pour saisir le numéro du serveur, puis en saisissant le numéro de la caméra.

Remarque!

Pour raccorder le clavier Bosch IntuiKey à un poste de commande BVMS, utilisez le câble Bosch indiqué.

Pour raccorder le clavier Bosch IntuiKey à un décodeur VIP XD, vous avez besoin d'un câble reliant un port de communication série du clavier à l'interface série du décodeur. Reportez-vous à Connexion d'un clavier de vidéosurveillance à un décodeur pour les connexions.

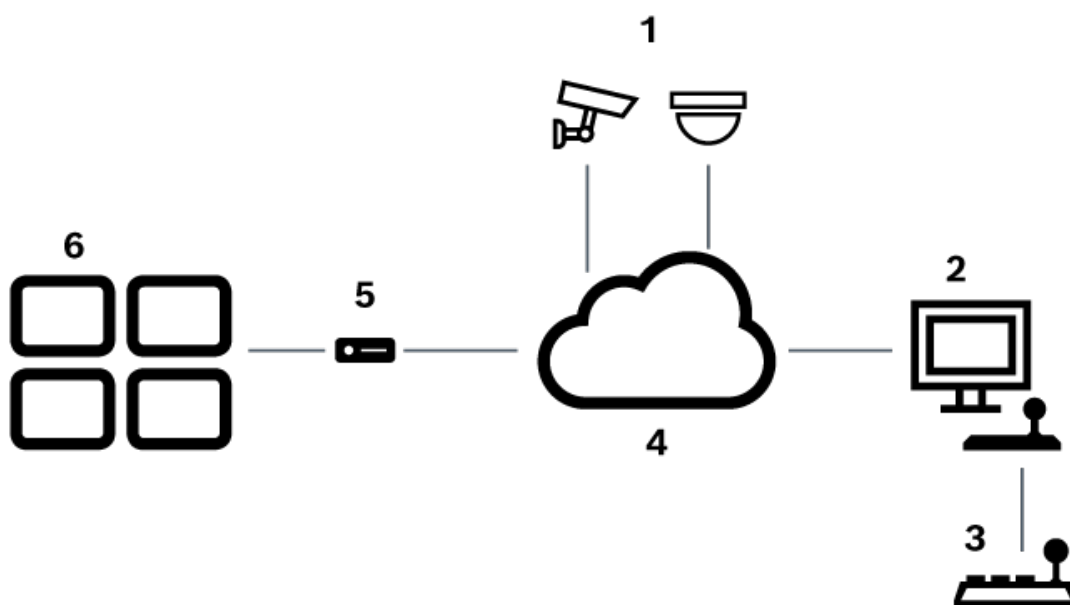
**Clavier Bosch IntuiKey connecté à un poste de commande BVMS**

Figure 6.1: Scénario 1 : clavier IntuiKey de Bosch connecté à un poste de commande Bosch Video Management System

1	Diverses caméras connectées au réseau via des encodeurs
2	Poste de commande BVMS
3	Clavier Bosch IntuiKey
4	Réseau BVMS
5	Décodeur
6	Moniteurs

Clavier Bosch IntuiKey connecté à un décodeur

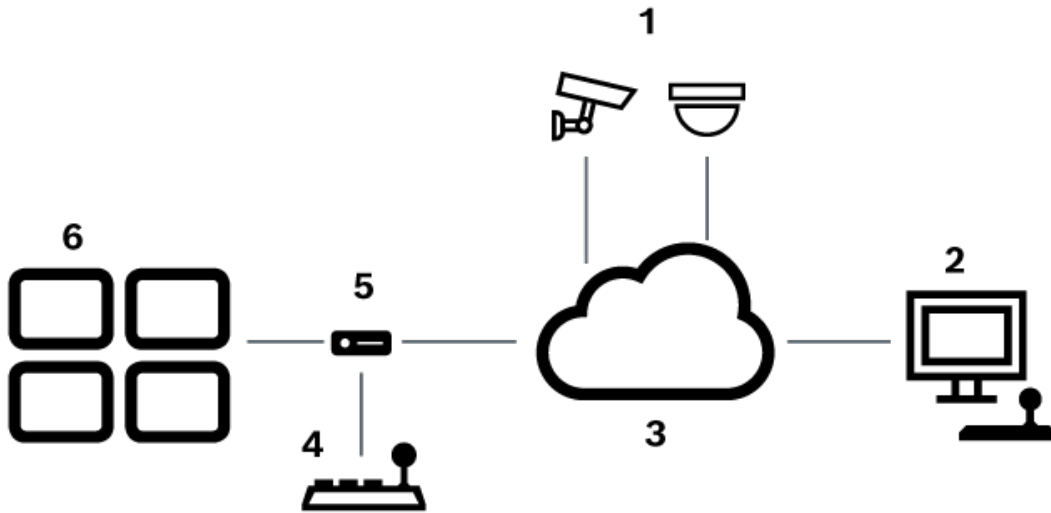


Figure 6.2: Scénario 2 : clavier IntuiKey de Bosch connecté à un décodeur

1	Diverses caméras connectées au réseau via des encodeurs
2	Poste de commande BVMS
3	Réseau BVMS
4	Clavier Bosch IntuiKey
5	Décodeur
6	Moniteurs

Pour obtenir des informations détaillées sur les fenêtres disponibles, reportez-vous aux sections suivantes :

- Page Attribution de clavier, page 159

Pour obtenir davantage d'informations sur les instructions détaillées disponibles, reportez-vous aux sections suivantes :

- Configuration d'un clavier numérique IntuiKey de Bosch (page des paramètres) (poste de commande), page 140
- Configuration d'un clavier numérique IntuiKey de Bosch (décodeur), page 148
- Configuration d'un décodeur pour une utilisation avec un clavier numérique IntuiKey de Bosch, page 148

Se reporter à

- Page Attribution de clavier, page 159

6.3.2 Connexion d'un clavier numérique IntuiKey de Bosch à un décodeur

Configuration du décodeur

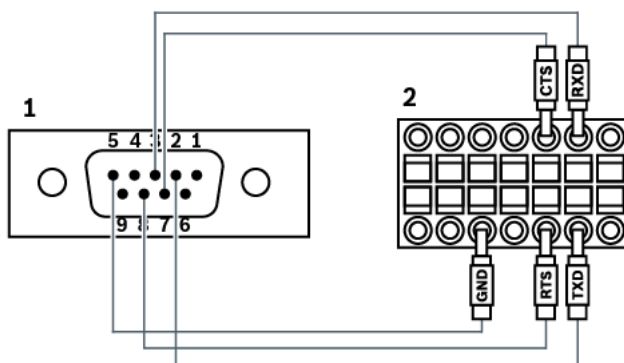
Voir *Configuration d'un décodeur pour une utilisation avec un clavier numérique IntuiKey de Bosch*, page 148 pour plus d'informations.

Connexion entre un port COM et le décodeur VIP XD

Le tableau suivant donne la liste des connexions entre un adaptateur RS232 et une interface série d'un décodeur VIP XD :

Adaptateur RS232	Interface série d'un décodeur VIP XD
1	
2	Tx
3	Rx
4	
5	MASSE
6	
7	CTS
8	RTS
9	

L'illustration suivante représente le brochage d'un adaptateur RS232 standard (1) et celui de l'adaptateur série du décodeur (2) :



6.3.3 Mise à jour du firmware clavier numérique IntuiKey de Bosch

1. Installez le programme de téléchargement IntuiKey sur n'importe quel PC.
2. Lancez l'utilitaire IntuiKey de mise à niveau du firmware.
3. Raccordez le clavier au PC par un câble série approprié (consultez l'assistance Bosch si vous ne disposez pas d'un câble de ce type).
4. Sur le clavier, appuyez sur la touche programmable Keyboard Control, puis sur Firmware Upgrade.
5. Saisissez le mot de passe : 0 et 1 simultanément.
Le clavier est en mode chargeur de démarrage.
6. Sur le PC, cliquez sur Browse pour sélectionner le fichier du firmware : par exemple kbd.s20
7. Définissez le port COM.

8. Cliquez sur le bouton Download pour télécharger le firmware. Programming apparaît sur l'afficheur du clavier. N'appuyez pas encore sur le bouton Clr. Si vous le faites, le clavier sera inutilisable après le redémarrage (lire la remarque ci-dessous).
9. Cliquez sur le bouton Browse pour sélectionner la langue : par exemple, 8900_EN_.82.s20 . Programming s'affiche sur le clavier.
10. Fermez l'utilitaire IntuiKey de mise à niveau du firmware.
11. Sur le clavier, appuyez sur Clr pour sortir. Le clavier redémarre. Attendez quelques secondes que le menu du choix de langue du clavier apparaisse.
12. Sélectionnez la langue de votre choix avec une touche programmable. L'écran d'accueil par défaut s'affiche.

**Remarque!**

Pour lancer directement le mode chargeur de démarrage, vous pouvez débrancher l'alimentation du clavier, appuyer simultanément sur 0 et 1, rebrancher l'alimentation, puis relâcher 0 et 1.

6.4

Connexion de la matrice Bosch Allegiant à BVMS

L'interface BVMS Allegiant de la matrice Allegiant fournit un accès transparent aux caméras matricielles analogiques dans l'interface Operator Client. Les caméras Allegiant sont quasi identiques aux caméras IP. La seule différence est la petite grille symbolisée sur la caméra, indiquant qu'il s'agit d'une caméra Allegiant. Vous pouvez afficher ces caméras à l'aide des mêmes tâches que pour les caméras IP. Elles sont incluses à la fois dans l'Arborescence Logique et dans les plans de site ; les utilisateurs peuvent les ajouter à leur Arborescence des Favoris. Les caméras mobiles connectées à la matrice Allegiant peuvent être directement commandées via la fenêtre vidéo ; vous pouvez également afficher aisément des caméras Allegiant sur des moniteurs connectés à des décodeurs IP.

BVMS fournit une interface avec la matrice via l'application MCS (Master Control Software) d'Allegiant. Dans ce cas, le logiciel MCS s'exécute de manière transparente en arrière-plan. Ce logiciel offre une interface efficace, orientée événements, avec la matrice Allegiant. Il permet également à la matrice Allegiant de fournir une réponse aux événements rapide et en temps réel à BVMS. Par exemple, si un câble coaxial défectueux entraîne une perte de vidéo dans la matrice Allegiant, une notification est immédiatement envoyée à BVMS. Par ailleurs, vous pouvez programmer BVMS pour qu'il réagisse aux alarmes Allegiant.

6.4.1

Présentation de la connexion Bosch Allegiant

Pour réaliser une connexion entre BVMS et une matrice de commutation Allegiant, vous devez configurer un canal de contrôle entre le BVMS et la matrice Allegiant.

Deux scénarios sont possibles :

- Connexion locale
Le Management Server commande la matrice Allegiant.
- Connexion à distance
Un PC Bosch Allegiant dédié relié au réseau commande la matrice Allegiant.

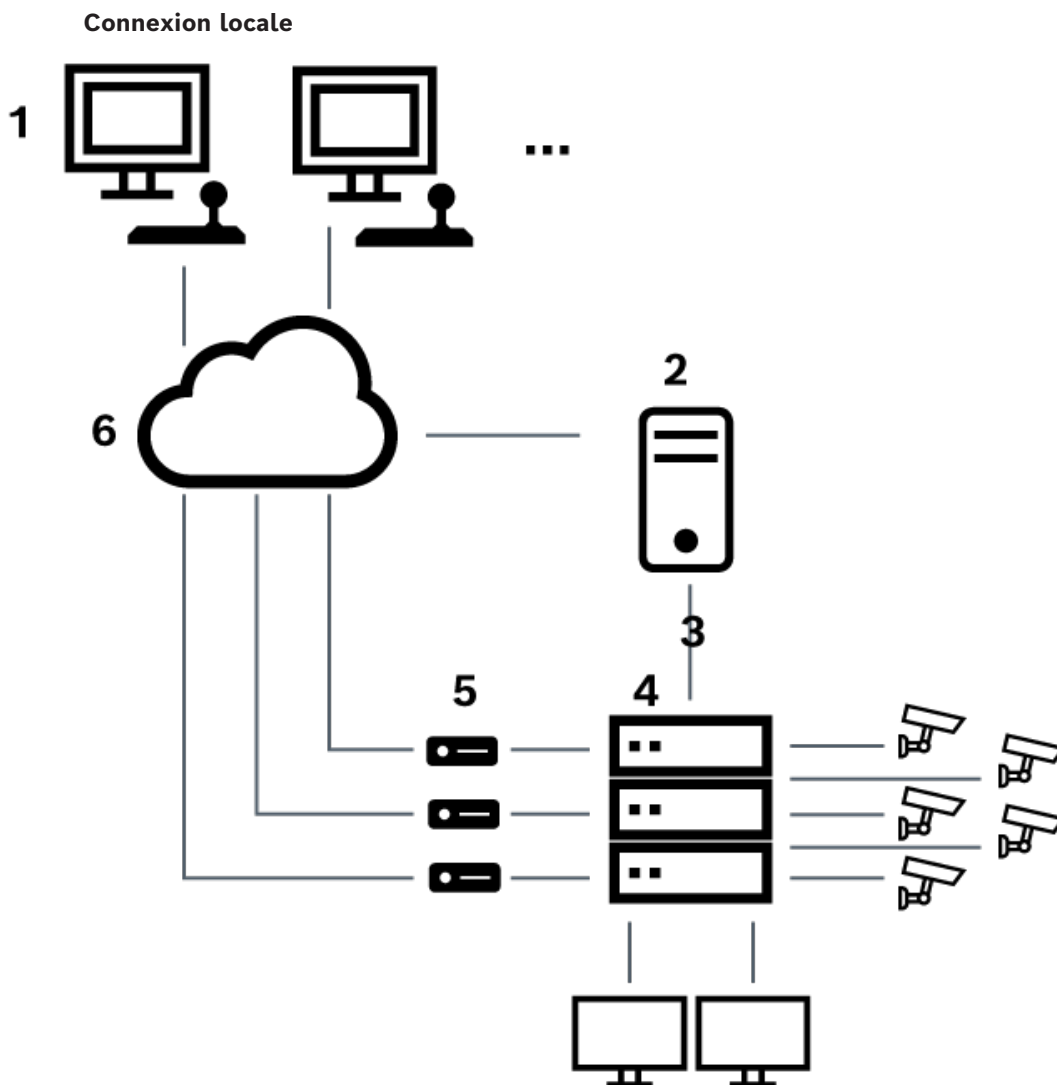


Figure 6.3: Connexion locale de Bosch Video Management System à la matrice Allegiant Bosch

1	Postes de commande client BVMS
2	Management Server doté du logiciel MCS
3	Connexion RS-232
4	matrice Allegiant
5	Encodeurs
6	Réseau

Connexion à distance

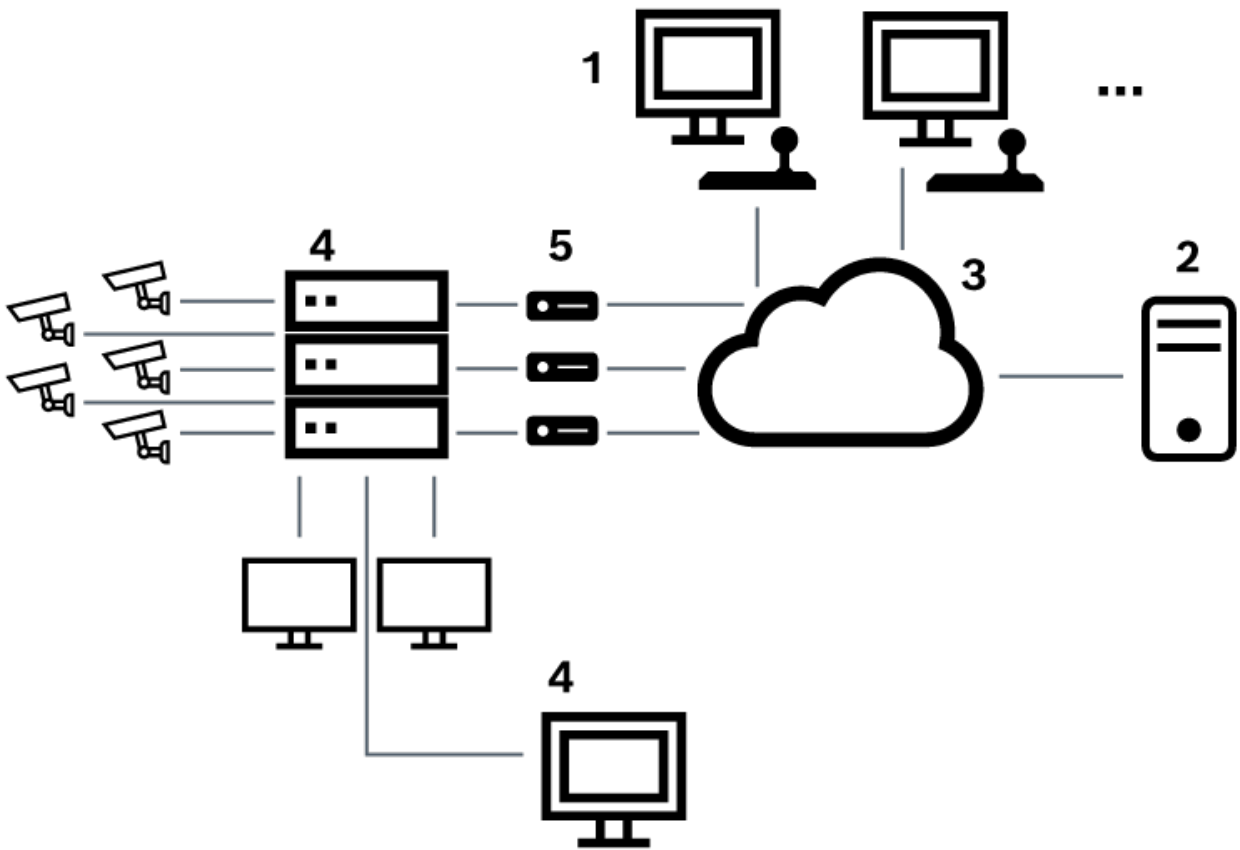


Figure 6.4: Connexion à distance de Bosch Video Management System à la matrice Allegiant Bosch

1	Postes de commande client BVMS
2	Management Server doté du logiciel MCS
3	Réseau
4	Ordinateur Allegiant doté du logiciel MCS
5	Connexion RS-232
6	Encodeurs
7	matrice Allegiant

6.4.2 Configuration du canal de contrôle

Pour configurer le canal de contrôle, effectuez les tâches suivantes :

- Câblage
- Installation du logiciel
- Création d'un fichier de configuration Allegiant
- Ajout de la matrice Allegiant à BVMS
- Configuration des noms d'utilisateur

Câblage

Pour configurer le canal de contrôle entre BVMS et la matrice Allegiant, connectez un PC au port console de la matrice Allegiant via un port série RS-232 (pour cette connexion, utilisez le câble Bosch indiqué). Il peut s'agir du Management Server de BVMS ou de tout autre ordinateur présent sur le réseau.

Installation du logiciel MCS Allegiant

1. Arrêtez le service du Management Server, le cas échéant (**Démarrer** > **Panneau de configuration** > **Services** > Cliquez avec le bouton droit de la souris sur BVMS Management Server > **Arrêter**).
2. Installez le logiciel MCS d'Allegiant sur le Management Server et sur le PC Allegiant (le cas échéant).
3. Sur un PC Allegiant distant, configurez-le pour qu'il lance le programme Network Host Allegiant (ld_alghw.exe) au démarrage. Ce programme permet de démarrer les services Allegiant requis pour autoriser d'autres ordinateurs du réseau à accéder à la matrice Allegiant. Il s'exécute de manière transparente. Il n'est pas nécessaire de disposer d'une clé électronique sur cet ordinateur.
Pour que le service soit automatiquement lancé au démarrage de l'ordinateur, copiez un lien vers ld_alghw.exe dans le dossier Démarrage de votre ordinateur.

Création d'un fichier de configuration Bosch Allegiant

1. Le logiciel MCS Allegiant permet de créer un fichier de configuration Allegiant désignant l'ordinateur connecté à la matrice Allegiant. Cette tâche requiert la clé électronique du logiciel MCS.
2. Dans le menu Transfer, cliquez sur Communication Setup. Dans la liste Current Host, saisissez le nom DNS de l'ordinateur connecté à la matrice Allegiant, puis saisissez les paramètres (numéro de port COM, débit, etc.) du port série connecté à la matrice Allegiant. Le logiciel MCS installé sur le Management Server ou sur l'ordinateur peut de cette manière communiquer en ligne avec le système Allegiant. Si cette tâche échoue, assurez-vous que le logiciel MCS ou le programme Network Host est en cours d'exécution sur l'ordinateur connecté à la matrice Allegiant et que la sécurité réseau est configurée de manière à autoriser l'accès distant à cet ordinateur.
3. Dans le menu Transfer, cliquez sur Upload. Sélectionnez tous les tableaux et cliquez sur Upload. Pour enregistrer le fichier de configuration, sélectionnez un répertoire.
4. Quittez le logiciel MCS.

Ajout de la matrice Bosch Allegiant à BVMS

1. Démarrez le service du BVMS de Management Server, démarrez Configuration Client, puis ajoutez le périphérique Allegiant via l'ajout ce fichier de configuration (voir les instructions détaillées de Ajout d'un périphérique).
2. Assurez-vous que le fichier de configuration MCS utilisé dans BVMS correspond à la configuration actuelle de la matrice Allegiant.
BVMS exécute les composants requis du logiciel MCS de manière transparente, en arrière-plan.

Configuration du nom d'utilisateur pour la connexion aux services Allegiant

Si la matrice Allegiant est connectée à un ordinateur et non pas au Management Server, assurez-vous que les services Allegiant sur cet ordinateur et sur le Management Server relèvent du même compte utilisateur de connexion. Cet utilisateur doit être membre d'un groupe d'administrateurs.

Documentation complémentaire

Pour obtenir des informations détaillées sur les fenêtres disponibles, reportez-vous aux sections suivantes :

- Page Commutateurs Matriciels, page 136

Pour obtenir davantage d'informations sur les instructions détaillées disponibles, reportez-vous aux sections suivantes :

- Configuration d'un périphérique Bosch Allegiant, page 137

Se reporter à

- Page Commutateurs Matriciels, page 136

6.4.3

Concept de Bosch Allegiant Satellite System

La matrice Allegiant permet l'interliaison de plusieurs systèmes Allegiant à l'aide du concept de « satellite ». Dans ce cas, plusieurs systèmes Allegiant peuvent apparaître sur le BVMS en tant que système unique de grande taille, fournissant l'accès à l'ensemble des caméras de tous ces systèmes.

Dans un système satellite Allegiant, les sorties moniteur d'un système Allegiant esclave sont reliées aux entrées vidéo du système Allegiant maître. Cette connexion est appelée « ligne de jonction ». En outre, un canal de contrôle est établi entre le maître et l'esclave.

Lorsqu'une caméra du système Allegiant esclave est appelée par le système Allegiant maître, une commande est envoyée, ordonnant le basculement de ladite caméra vers une ligne de jonction. Parallèlement, le système Allegiant maître fait basculer l'entrée de jonction vers la sortie moniteur requise. De cette manière, la connexion vidéo entre la caméra esclave appelée et le moniteur maître requis peut être établie.

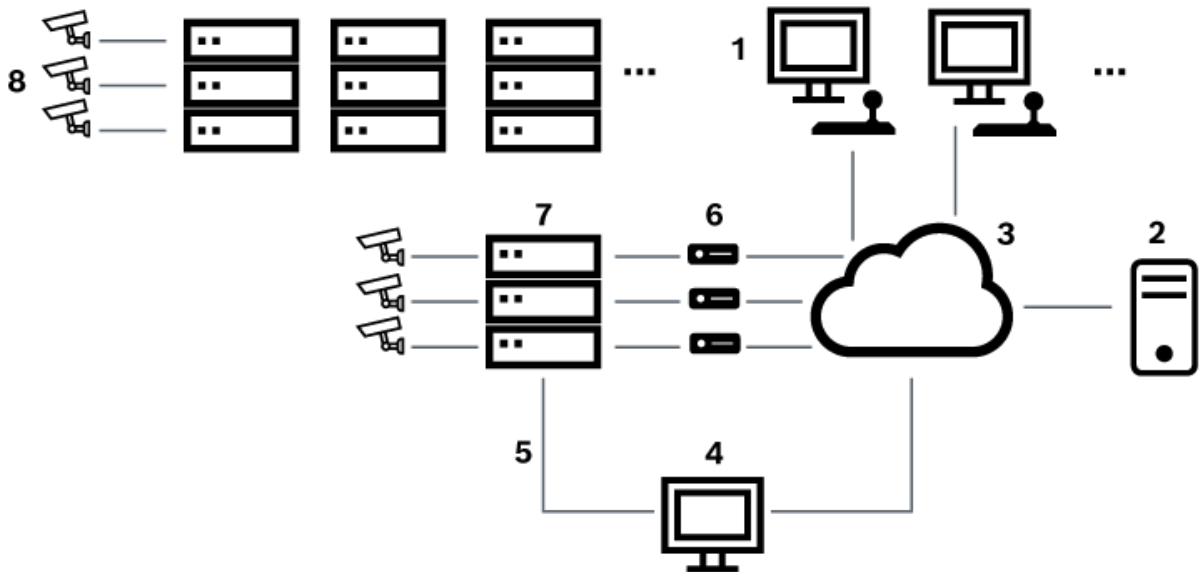


Figure 6.5: Système Bosch Allegiant étendu à l'aide de systèmes de commutation satellites

1	Postes de commande client BVMS
2	Management Server doté du logiciel MCS
3	Réseau
4	Ordinateur Allegiant doté du logiciel MCS
5	Connexion RS-232

6	Encodeurs
7	matrice Allegiant
8	Matrice satellite Allegiant

Vous pouvez appliquer le concept de satellite de manière à ce qu'une matrice Allegiant puisse être à la fois esclave et maître. Chaque système Allegiant peut alors afficher les caméras des autres systèmes. Il suffit de connecter les lignes de jonction et de contrôle dans les deux sens et de configurer correctement les tableaux Allegiant.

Ce concept peut être encore davantage étendu, de manière quasi illimitée, à des systèmes Allegiant multiples. Un système Allegiant peut comporter de nombreux esclaves tout en étant lui-même esclave de nombreux systèmes maîtres. Vous pouvez programmer les tables Allegiant de sorte à autoriser ou interdire l'accès des utilisateurs aux affichages des caméras, en fonction de la politique de votre site.

6.5 Commandes Allegiant CCL prises en charge dans BVMS

Pour utiliser les commandes CCL, vous avez besoin du Guide d'utilisation de CCL. Ce guide est disponible dans le catalogue de produits en ligne dans la section documentation de chaque matrice LTC Allegiant.

Commande prise en charge	Description	Remarques
Commutation/séquence		
LCM	Commutation de la caméra logique au moniteur	Les commandes LCM, LCM+ et LCM- sont équivalentes.
LCMP	Commutation de la caméra logique au moniteur avec appel de préposition	
MON+CAM	Commutation de la caméra physique au moniteur	
MON-RUN	Exécution de séquence par numéro de moniteur	
MON-HOLD	Maintien de séquence par numéro de moniteur	
SEQ-REQ	Demande de séquence	
SEQ-ULD	Décharge de séquence	
Module de réception/pilotage		
R/D	Commandes de contrôle de base	

Commande prise en charge	Description	Remarques
Commutation/séquence		
REMOTE-ACTION	Commandes de contrôle simultanées d'orientation/inclinaison/zoom	
REMOTE-TGL	Commandes de contrôle d'orientation/inclinaison/zoom	
PREPOS-SET	Définir la préposition	
PREPOS	Appel de préposition	
AUX-ON AUX-OFF	Commandes de contrôle auxiliaire – Auxiliaire activé – Auxiliaire désactivé	
VARSPEED_PTZ	Commandes de contrôle de vitesse variable	
Alarme		Utilisé pour contrôler les entrées virtuelles. Par exemple « +alarme 1 » permet de fermer l'entrée virtuelle 1, « -alarme 1 » d'ouvrir l'entrée virtuelle 1
+ALARM	Activation d'une alarme	Permet d'ouvrir une entrée virtuelle dans BVMS.
-ALARM	Désactivation d'une alarme	Permet de fermer une entrée virtuelle dans BVMS.
Système		
TC8x00>HEX	Définir le Mode hexadécimal	
TC8x00>DECIMAL	Définir le Mode décimal	

7 Utiliser les derniers logiciels

Avant d'utiliser le dispositif pour la première fois, assurez-vous d'avoir installé la dernière version applicable du logiciel. Afin de garantir la cohérence de la fonctionnalité, de la compatibilité, des performances et de la sécurité du dispositif, mettez régulièrement à jour son logiciel tout au long de sa durée de vie. Suivez les instructions contenues dans la documentation produit concernant les mises à jour logicielles.

Nous créons de nouvelles mises à jour uniquement pour les versions logicielles en état de disponibilité générale ou limitée. Pour plus d'informations, voir :

[Bosch Building Technologies Software - Assistance technique et service.](#)

Pour plus d'informations, cliquez sur les liens suivants :

- Informations générales : <https://www.boschsecurity.com/xc/en/support/product-security/>
- Conseils de sécurité, avec une liste des vulnérabilités et des solutions possibles : <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch n'assume aucune responsabilité pour tout dommage causé par le fait que les produits livrés ont été mis en service avec du firmware obsolète.

8 Mise en route

Ce chapitre explique comment mettre en route BVMS.

8.1 Installation des modules logiciels

**Remarque!**

Installez les modules logiciels sur les ordinateurs appropriés.

Pour procéder à l'installation :

Fermez Configuration Client avant de démarrer la configuration de BVMS.

1. Exécutez Setup.exe ou lancez le programme d'installation de BVMS via la fenêtre d'accueil.
2. Dans la boîte de dialogue suivante, sélectionnez les modules à installer sur l'ordinateur.
3. Suivez les instructions qui s'affichent à l'écran.

8.2 Utilisation de l'assistant de configuration

L'utilisation prévue de l'Config Wizard est la configuration rapide et aisée d'un système de plus petite envergure. L'Config Wizard vous permet d'obtenir un système configuré avec VRM, le système iSCSI, Mobile Video Service, des caméras, des profils d'enregistrement et des groupes d'utilisateurs.

Vous devez ajouter des systèmes iSCSI manuellement à une installation standard du logiciel.

Les groupes d'utilisateurs et leurs autorisations sont configurés automatiquement. Vous pouvez ajouter ou supprimer des utilisateurs et définir des mots de passe.

L'Config Wizard peut accéder à Management Server uniquement sur l'ordinateur local.

Vous pouvez enregistrer une configuration activée à des fins de sauvegarde et importer cette configuration par la suite. Vous pouvez modifier cette configuration importée après son importation.

Config Wizard ajoute les VRM locaux automatiquement à une installation standard du logiciel, à DIVAR IP 3000 et DIVAR IP 7000.

Sur un DIVAR IP 3000 et un DIVAR IP 7000, le périphérique iSCSI local est également ajouté automatiquement, si cela n'a pas déjà été fait.

Sur un DIVAR IP 3000 et un DIVAR IP 7000, un Mobile Video Service local est ajouté automatiquement, s'il n'est pas déjà disponible.

**Remarque!**

Si vous voulez utiliser des décodeurs dans votre système, assurez-vous que tous les encodeurs utilisent le même mot de passe pour le niveau d'autorisation user.

Pour démarrer Config Wizard :

- ▶ Cliquez sur **Démarrer > Tous les programmes > BVMS > Config Wizard**
La page Welcome s'affiche.

Page Welcome

Welcome

Config Wizard helps you set up your BVMS quickly.

The following prerequisites must be fulfilled:

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

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

Restrictions of Config Wizard

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

About Config Wizard

BVMS - Config Wizard 11.1
Build 11.1.0.74

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

[Open Source Licenses](#)

Next

► Cliquez sur **Next** pour continuer.

Page Basic

Latest saved configuration

Devices and services included in the latest saved configuration

Network address	Device type	Recording Profile	Recorder
172.30.11.39	AUTODOME IP starlight		Live Only
172.31.23.168	DINION IP ultra 8000 MF		Live Only
172.31.20.20	E-Series Storages		
172.30.11.237	MIC IP starlight 7000i		Live Only
Internal	Monitor group		
172.31.21.21	VIP X1600	Continuous, Alarm Recording	VRM(172.30.11.128)
172.31.21.20	VIP X1600 XFM4	(non-uniform)	VRM(172.30.11.128)
Internal	Virtual Input		
172.30.11.128	VRM		
172.31.20.22	VRM Storage		

The active configuration is identical with the latest saved configuration.

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

Please select the network adapter for your local video network:

Ethernet (Type: Ethernet; IPv4-Address: 172.30.11.128)

Next

Import configuration

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

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

[Import configuration ...](#)

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

Cette page affiche la dernière configuration enregistrée. Vous pouvez importer un fichier BVMS en tant que modification dans la configuration existante. Cette modification est enregistrée, mais n'est pas activée lorsque vous cliquez sur **Next**.

Vous pouvez sélectionner la carte réseau de l'ordinateur connecté aux périphériques vidéo (caméras IP, encodeurs, décodeurs, systèmes de stockage iSCSI) de votre système. L'adresse IP de cette carte réseau est utilisée comme adresse IP du VRM, du VSG et du système de stockage iSCSI local. Cliquez sur **Port Mapping** pour spécifier l'adresse IP publique ou le nom DNS si l'accès au système doit se faire via Internet.

Page Scan

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 7000i	172.31.22.144	00-07-5f-7a-c2-b6	FLEXIDOME IP dynamic 7000i
FlexiDome panorama 5000i	172.31.22.62	00-07-5f-88-74-dd	FLEXIDOME IP panoramic 5000i
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 6000i	172.31.23.147	00-07-5f-8d-21-a5	FLEXIDOME IP starlight 6000i
FLEXIDOME IP panoramik 7000i	172.31.23.124	00-07-5f-84-89-e6	FLEXIDOME IP panoramic 7000i
FLEXIDOME IP panoramik 7000i	172.31.23.123	00-07-5f-84-8a-e1	FLEXIDOME IP panoramic 7000i
FLEXIDOME IP panoramik 7000i	172.31.23.122	00-07-5f-8b-f8-c1	FLEXIDOME IP panoramic 7000i
DINION IP ultra 8000 MP	172.31.23.114	00-07-5f-8d-33-bd	DINION IP ultra 8000 MP
FLEXIDOME IP indoor 5000i	172.31.23.113	00-07-5f-7c-64-32	FLEXIDOME IP indoor 5000i
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

Remarque :

La recherche de dispositifs peut prendre du temps. Vous pouvez annuler une telle recherche. Tous les dispositifs qui ont déjà été analysés sont affichés dans le tableau. Cette page affiche tous les dispositifs vidéo qui ne sont pas inclus dans la dernière configuration enregistrée.

Désactivez les cases à cocher pour les dispositifs qui ne doivent pas être ajoutés à la configuration, puis cliquez sur **Next**.

Si les dispositifs ne sont pas situés dans la même plage IP que celle du système DIVAR IP, vous pouvez changer l'adresse IP des dispositifs en spécifiant l'adresse de début de la plage IP du dispositif.

Page Authentication

Enter passwords for devices

Device name	IP address	User name	Password	Status
172.31.23.150	172.31.23.150	service	<input type="password"/>	
Decoder (172.31.21.204)	172.31.21.204	service	<input type="password"/>	
NDC-284-P (172.31.23.15)	172.31.23.15	service	<input type="password"/>	
VIP10 (172.31.23.24)	172.31.23.24	service	<input type="password"/>	
VIPX-1600XFMD (172.31.22.4)	172.31.22.4	service	<input type="password"/>	
VIPX-1600XFMD (172.31.22.5)	172.31.22.5	service	<input type="password"/>	

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

Cette page vous permet de vous authentifier sur les dispositifs protégés par un mot de passe. Pour faciliter l'authentification avec le même mot de passe pour plusieurs dispositifs, vous pouvez utiliser le Presse-papiers (CTRL+C, CTRL+V) :

1. Cliquez sur **Show passwords**.
2. Sélectionnez une ligne ayant un dispositif authentifié avec succès (affichage d'un verrou vert), appuyez sur CTRL+C, sélectionnez plusieurs lignes affichant un verrou rouge, puis appuyez sur CTRL+V.

La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.

Vous pouvez fournir un mot de passe par défaut global pour tous les dispositifs qui, actuellement, ne sont pas protégés par un mot de passe.

Si un dispositif nécessite un mot de passe initial,  s'affiche.

Pour définir un mot de passe initial :

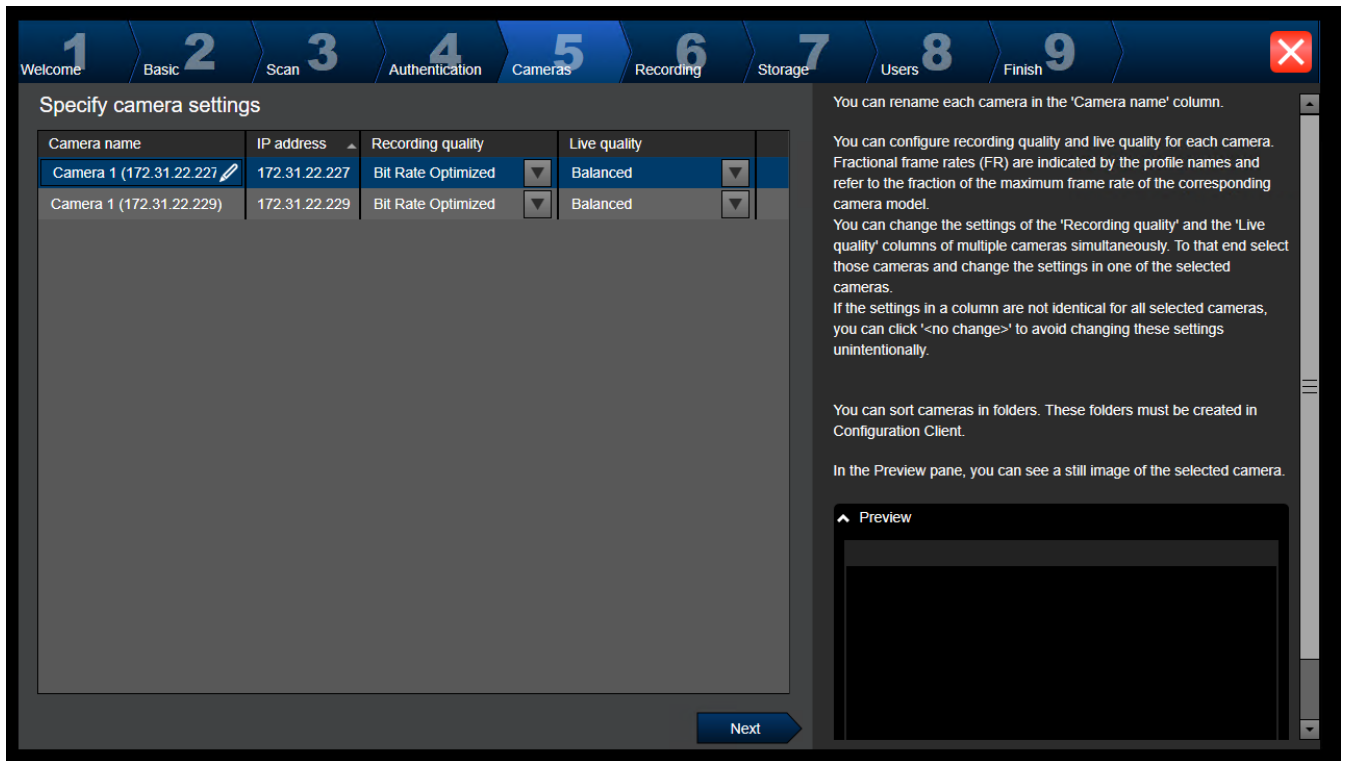
1. Dans le champ **Password**, saisissez le mot de passe.
2. Cliquez sur **Set Initial Passwords**.

Le mot de passe initial est défini.

Remarque : Tant que vous n'avez pas défini le mot de passe initial de tous les périphériques nécessitant un mot de passe initial, vous ne pouvez pas continuer.

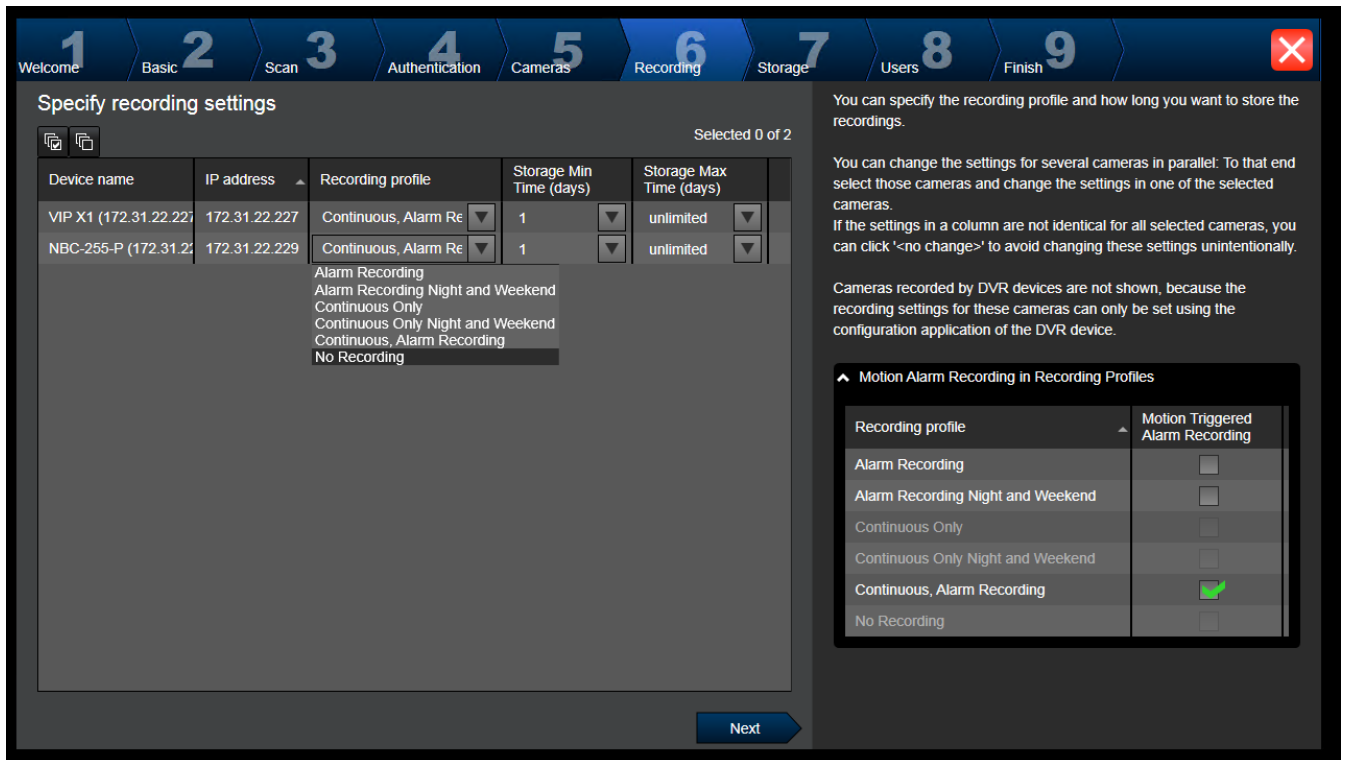
3. Cliquez sur **Next** pour continuer.

Page Cameras



Cette page permet de gérer les caméras de votre système.

Page Recording

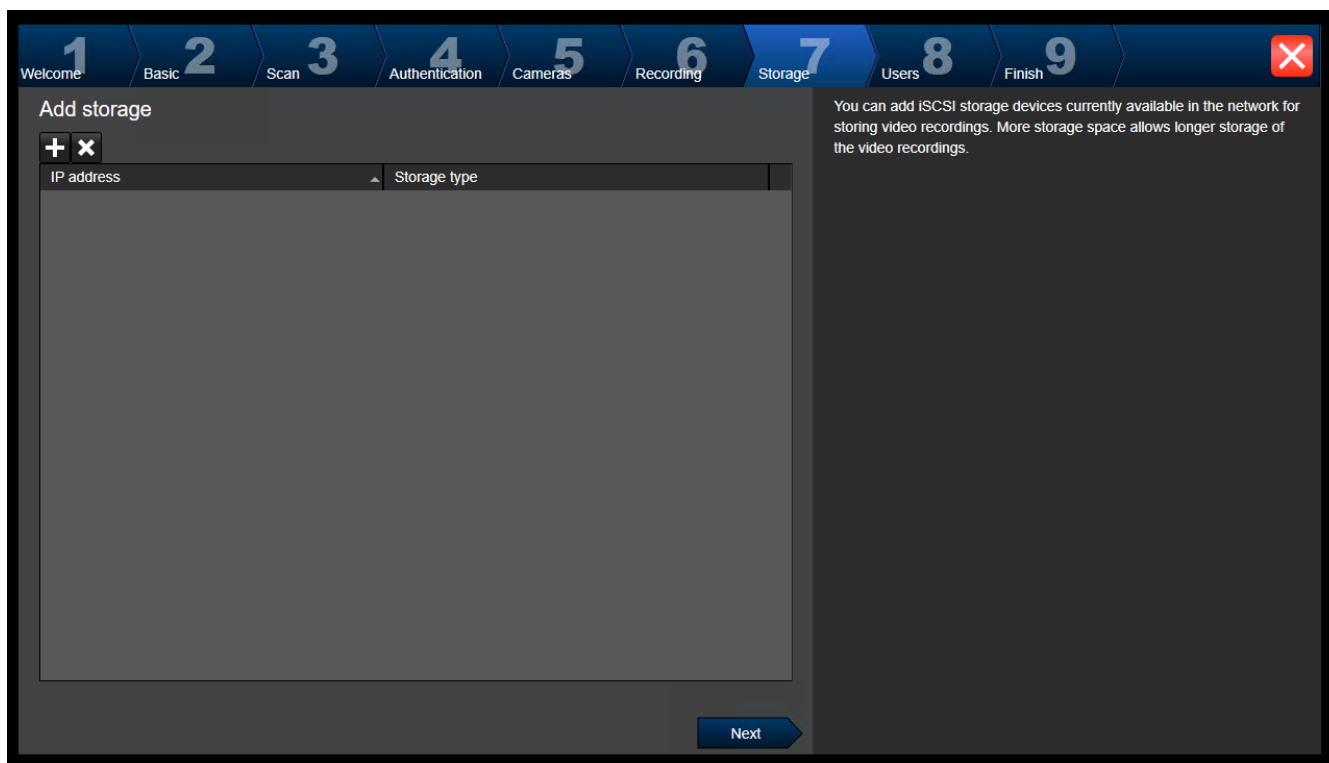


Seules les caméras venant d'être ajoutées sont affichées sur cette page. Dès lors que vous activez cette configuration, vous ne pouvez plus modifier l'affectation des profils de ces caméras.

Vous pouvez activer l'enregistrement de mouvements pour les profils d'enregistrement avec à la fois l'enregistrement et l'enregistrement d'alarme activés. Si nécessaire, configurez l'enregistrement et l'enregistrement d'alarme dans la boîte de dialogue Configuration Client (**Paramètres d'enregistrement planifié**).

VCA est activé automatiquement pour chaque caméra nouvellement ajoutée.

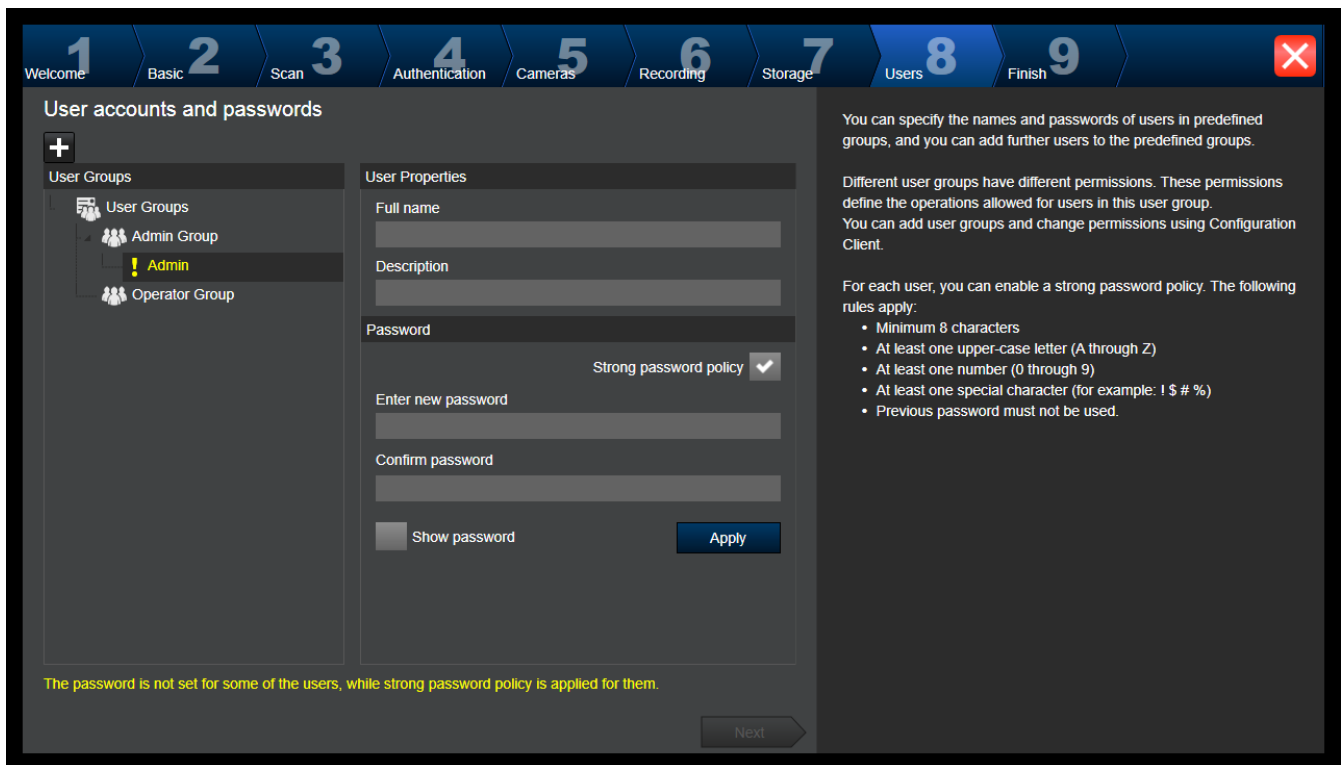
Page Storage



The screenshot shows a configuration wizard with 9 steps: 1 Welcome, 2 Basic, 3 Scan, 4 Authentication, 5 Cameras, 6 Recording, 7 Storage, 8 Users, and 9 Finish. The 'Storage' step is active. The main content area is titled 'Add storage' and features a table with two columns: 'IP address' and 'Storage type'. There are '+' and 'x' icons at the top left of the table area. A 'Next' button is positioned at the bottom right. On the right side, there is a text box that reads: 'You can add iSCSI storage devices currently available in the network for storing video recordings. More storage space allows longer storage of the video recordings.'

Cette page permet d'ajouter des dispositifs de stockage iSCSI supplémentaires.

Page Users



Dans cette page, vous pouvez ajouter de nouveaux utilisateurs aux groupes d'utilisateurs existants.

- ▶ Pour chaque nouvel utilisateur, saisissez le nom d'utilisateur et la description et définissez un mot de passe.

Strong password policy

La case à cocher **Strong password policy** est présélectionnée pour tous les nouveaux groupes d'utilisateurs créés.

Il est fortement recommandé de conserver ce paramètre pour améliorer la protection de votre ordinateur contre tout accès non autorisé.

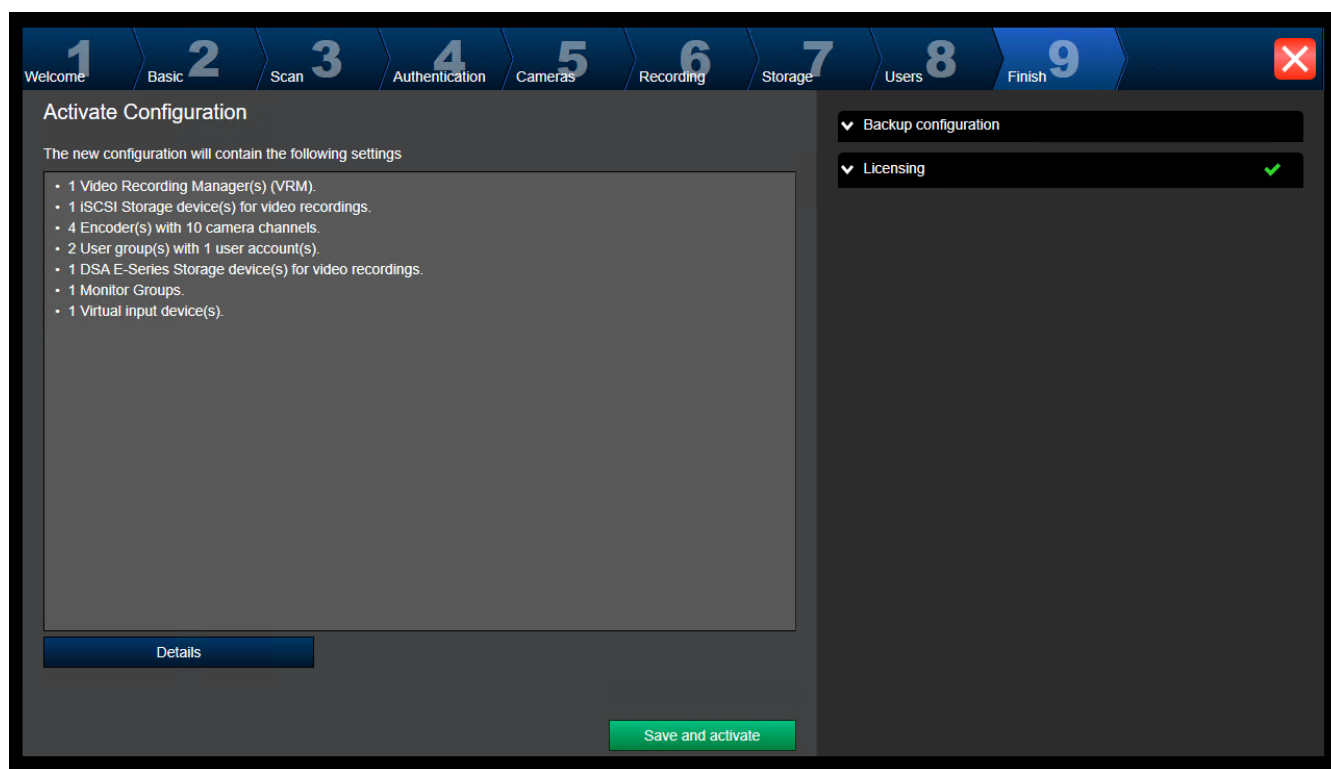
Les règles suivantes sont applicables :

- Longueur minimale du mot de passe défini dans la page **Stratégies de compte** pour le groupe d'utilisateurs approprié.
- Ne pas utiliser l'un des mots de passe précédents.
- Utiliser au moins une lettre majuscule (A à Z).
- Utiliser au moins un chiffre (0 à 9).
- Utiliser au moins un caractère spécial (Exemple : ! \$ # %).
- ▶ Cliquez sur **Apply** pour appliquer les paramètres, puis cliquez sur **Next** pour continuer.

Remarque : tant qu'il existe des utilisateurs pour lesquels aucun mot de passe n'a été défini, bien que le paramètre **Strong password policy** soit activé, vous ne pouvez pas continuer. Pour poursuivre, définissez les mots de passe manquants.

Utilisez le Configuration Client pour ajouter des groupes d'utilisateurs et modifier leurs autorisations.

Page Finish



Avant de pouvoir activer votre configuration, vous devez effectuer les tâches suivantes :

- Fournir un mot de passe par défaut global pour tous les dispositifs qui, actuellement, ne sont pas protégés par un mot de passe.
- Activer votre licence si nécessaire.

Mot de passe par défaut global

Si dans Configuration Client l'option **Enforce password protection on activation (Paramètres -> Options)** est désactivée, vous n'êtes pas obligé de fournir un mot de passe global par défaut pour l'activer.

Gestion des licences

Développez **Licensing** et cliquez sur **License Wizard** pour activer votre licence.

Lorsque vous cliquez sur **Save and activate**, la configuration est activée.

Une fois l'activation réussie, la page **Finish** s'affiche de nouveau. Vous pouvez à présent enregistrer une sauvegarde de la configuration si vous le souhaitez : cliquez sur **Save backup copy**.

Lorsque vous cliquez sur **Save and activate**, la configuration est activée.

Une fois l'activation réussie, la page **Terminer** s'affiche de nouveau. Vous pouvez à présent enregistrer une sauvegarde de la configuration si vous le souhaitez : cliquez sur **Save backup copy**.

8.3

Démarrage de Configuration Client



Remarque!

Seuls les utilisateurs admin peuvent se connecter à Configuration Client.

L'utilisateur admin pré-configuré par défaut est Admin. Seul cet utilisateur peut se connecter à Configuration Client lorsque vous démarrez Configuration Client pour la première fois.

Une fois que vous avez démarré Configuration Client, vous pouvez renommer l'utilisateur Admin et modifier le mot de passe.

Remarque :

Vous ne pouvez pas démarrer Configuration Client si un autre utilisateur a déjà lancé Configuration Client sur un autre ordinateur du système.

Pour démarrer Configuration Client :

1. Dans le menu **Démarrer**, sélectionnez **Programme** > BVMS > Configuration Client. La boîte de dialogue d'ouverture de session s'affiche.
2. Dans le champ **Nom d'utilisateur** :, saisissez votre nom d'utilisateur. Lorsque vous lancez l'application pour la première fois, entrez Admin comme nom d'utilisateur ; aucun mot de passe n'est requis.
3. Dans le champ **Mot de passe** :, saisissez votre mot de passe.
4. Cliquez sur **OK**.
L'application démarre.

Lorsque l'utilisateur Admin démarre Configuration Client pour la première fois, la boîte de dialogue **Violation de la politique de mot de passe** s'affiche et l'invite à définir un mot de passe pour le compte utilisateur Admin. Nous vous recommandons fortement de conserver ce paramètre et de définir un mot de passe sécurisé pour le compte utilisateur Admin, dans le respect des règles de la politique de mot de passe.

Se reporter à

- *Stratégie de mot de passe fort* , page 365
- *Configuration du groupe admin.*, page 370

8.4 Configuration de la langue de Configuration Client

La langue de Configuration Client se configure indépendamment de votre installation Windows.

Pour configurer la langue :



1. Dans le menu **Paramètres**, cliquez sur **Options**.
La boîte de dialogue **Options** s'affiche.
2. Dans la liste **Langue**, sélectionnez la langue de votre choix.
Si vous sélectionnez l'entrée **Langue système**, la langue de votre installation Windows est utilisée.
3. Cliquez sur **OK**.
Le changement de langue deviendra effectif au prochain redémarrage de l'application.

8.5 Configuration de la langue de Operator Client

La langue de Operator Client se configure indépendamment de votre installation Windows et de votre client de configuration. Cette étape s'exécute dans Configuration Client.

Pour configurer la langue :

1. Cliquez sur **Groupes d'utilisateurs** >  . Cliquez sur l'onglet **Propriétés du groupe d'utilisateurs**. Cliquez sur l'onglet **Autorisations d'utilisation**.
2. Sélectionnez la langue souhaitée dans la liste **Langue**.

3. Cliquez sur  pour enregistrer les paramètres.
4. Cliquez sur  pour activer la configuration.
Redémarrez Operator Client.

8.6 Recherche de périphériques

Fenêtre principale > **Périphériques**

Vous pouvez rechercher les périphériques suivants pour les ajouter à l'aide de la boîte de dialogue **BVMS Scan Wizard** :

- Dispositifs VRM
- Encodeurs
- Encodeurs temps réel uniquement
- Encodeurs ONVIF en temps réel uniquement
- Encodeurs pour stockage local
- Décodeurs
- Dispositifs Video Streaming Gateway (VSG)
- Dispositifs DVR

Si vous souhaitez ajouter des dispositifs via un balayage, consultez la rubrique des dispositifs respectifs dans le chapitre *Page Périphériques*, page 126.

Se reporter à

- *Ajout de dispositifs VRM via un balayage*, page 174
- *Ajout d'un dispositif ONVIF en temps réel par balayage*, page 243
- *Ajout de dispositifs temps réel uniquement via un balayage*, page 215
- *Ajout d'un dispositif*, page 127

8.7 Accès au système

Pour accéder à un système, procédez comme suit :

1. Effectuez l'une des actions suivantes pour sélectionner l'adresse réseau du système souhaité :
 - Cliquez sur une entrée présélectionnée de la liste.
 - Saisissez manuellement une adresse réseau.
 - Sélectionnez une adresse réseau via la recherche de serveur.
2. Connectez-vous au système souhaité :
 - Système à serveur unique
 - Enterprise System

8.8 Utilisation de la recherche de serveur

- La fonction BVMS Server Lookup permet aux opérateurs de se connecter à un BVMS Management Server qui ne figure pas dans une liste de serveurs fournie.
- Un seul utilisateur de Configuration Client ou Operator Client peut se connecter depuis plusieurs points d'accès au système de manière séquentielle.
- Les points d'accès au système peuvent être Management Server ou Enterprise Management Server.
- Server Lookup utilise le Management Server dédié pour héberger la liste des serveurs.
- Server Lookup et Management Server ou Enterprise Management Server peuvent être exécutés sur un ordinateur.

- Server Lookup vous aide à localiser des points d'accès au système par leur nom ou description.
- Une fois connecté au Management Server, le Operator Client reçoit des événements et alarmes provenant de BVMS Management Server et affiche les données en temps réel et en lecture.

Pour y accéder :

1. Démarrer Operator Client ou Configuration Client.
La boîte de dialogue de connexion s'affiche.
2. Dans la liste **Raccordement**, sélectionnez **<Carnet d'adresses...>** pour Configuration Client ou **<Carnet d'adresses...>** pour Operator Client.
Si une adresse IP privée et publique a été configurée pour un serveur, elle s'affiche.
Si vous sélectionnez **<Carnet d'adresses...>** ou **<Carnet d'adresses...>** pour la première fois, la boîte de dialogue **Server lookup** s'ouvre.
3. Dans le champ **Adresse Management Server (Enterprise)**, saisissez une adresse réseau valide pour le serveur souhaité.
4. Entrez un nom d'utilisateur et un mot de passe valides.
5. Le cas échéant, cliquez sur **Mémoriser les paramètres**.
6. Cliquez sur **OK**.
La boîte de dialogue **Server lookup** s'affiche.
7. Sélectionnez le serveur souhaité.
8. Cliquez sur **OK**.
9. Si le serveur sélectionné comporte des adresses réseau privée et publique, une boîte de message s'affiche et vous demande si vous utilisez un ordinateur situé dans le réseau privé du serveur sélectionné.
Le nom du serveur est ajouté à la liste **Raccordement** dans la boîte de dialogue de connexion.
10. Sélectionnez ce serveur dans la liste **Raccordement**, puis cliquez sur **OK**.
Si vous avez coché la case **Mémoriser les paramètres**, vous pouvez sélectionner ce serveur directement lorsque vous voulez y accéder.

8.9 Activation des licences des logiciels

Lorsque vous installez BVMS pour la première fois, vous devez activer les licences des logiciels que vous avez commandés, y compris celles du logiciel standard et des modules d'extension et/ou des fonctions en option.

Pour activer le système :

1. Démarrez Configuration Client BVMS.
2. Dans le menu **Outils**, cliquez sur **Gestionnaire de licences...**
La boîte de dialogue **Gestionnaire de licences** s'affiche.
3. Cliquez sur **Ajouter** pour ajouter vos licences.
La boîte de dialogue **Ajouter une licence** s'affiche.
4. Suivez les instructions dans la boîte de dialogue.
5. Une fois l'activation effectuée, fermez la boîte de dialogue **Ajouter une licence**.
6. Fermez la boîte de dialogue **Gestionnaire de licences**.

Pour plus d'informations, consultez le livre blanc relatif aux licences BVMS correspondant.

Se reporter à

- *Boîte de dialogue Inspecteur de licence (menu Outils), page 77*

- Boîte de dialogue Gestionnaire de licences (menu Outils), page 76
- Ajouter la boîte de dialogue de licence, page 77
- Vue d'ensemble de l'activation de la licence BVMS, page 19

8.9.1

Boîte de dialogue Gestionnaire de licences (menu Outils)

Fenêtre principale > menu **Outils** > commande **Gestionnaire de licences...**

Permet de mettre sous licence le logiciel BVMS commandé et d'effectuer des mises à niveau en ajoutant de nouvelles fonctions.

État des licences

Affiche l'état d'activation de licence.

Empreinte digitale système

Au cas où une assistance s'avérerait nécessaire, nous vous recommandons de fournir le **Empreinte digitale système**.

Site d'installation

Lors de l'activation de votre licence de base dans Bosch Remote Portal, vous fournissez des informations sur le site d'installation de votre système. Ces informations s'affichent ici.

Remarque : Vous pouvez également fournir ces informations dans d'autres licences, mais seules les informations fournies dans la licence de base s'affichent ici.

Licences

1. Cliquez sur **Ajouter** pour ajouter vos licences.
La boîte de dialogue **Ajouter une licence** s'affiche.
2. Suivez les instructions dans la boîte de dialogue.

Licence effective

Affiche la licence de base que vous avez activée.

Caractéristiques

- ▶ Cliquez sur **Inspecteur de licences...**
La boîte de dialogue **Inspecteur de licences** s'affiche.

Affiche le nombre de fonctionnalités sous licence qui sont actuellement installées.

Vous pouvez vérifier si le nombre de licences BVMS installées excède le nombre de licences achetées.

Version BVMS installée

Affiche la version BVMS actuellement installée, par exemple 11.0.

Versions BVMS sous licence

Affiche toutes les versions BVMS qui sont incluses et prises en charge dans le fichier de licence fourni actuellement.

Par exemple : BVMS 11.0 et toutes versions BVMS 11.x mineures à venir.

Date d'activation

Affiche la date d'activation de votre version BVMS installée.

Date d'expiration

Affiche la date d'expiration de votre version BVMS installée. Une date d'expiration ne s'applique que lorsque vous installez une licence d'urgence ou une licence de démonstration de vente.

Software Maintenance Agreement

Date d'expiration

Si vous en avez acheté et activé un Software Maintenance Agreement, la date d'expiration s'affiche ici.

Se reporter à

- *Activation des licences des logiciels, page 75*
- *Ajouter la boîte de dialogue de licence, page 77*
- *Boîte de dialogue Inspecteur de licence (menu Outils), page 77*

8.9.1.1**Ajouter la boîte de dialogue de licence**

Fenêtre principale > menu **Outils** > commande **Gestionnaire de licences...** > **Licences** >

Ajouter

Vous permet d'ajouter vos licences achetées ou licences de démonstration du site Web Bosch Remote Portal remote.boschsecurity.com à votre système BVMS.

Pour ajouter vos licences, suivez les instructions de la boîte de dialogue.

Pour plus d'informations, consultez le livre blanc relatif aux licences BVMS correspondant.

8.9.2**Ajouter la boîte de dialogue de licence**

Fenêtre principale > menu **Outils** > commande **Gestionnaire de licences...** > **Licences** >

Ajouter

Vous permet d'ajouter vos licences achetées ou licences de démonstration du site Web Bosch Remote Portal remote.boschsecurity.com à votre système BVMS.

Pour ajouter vos licences, suivez les instructions de la boîte de dialogue.

Pour plus d'informations, consultez le livre blanc relatif aux licences BVMS correspondant.

8.9.3**Boîte de dialogue Inspecteur de licence (menu Outils)**

Fenêtre principale > menu **Outils**, cliquez sur la commande **Inspecteur de licences...** > boîte de dialogue **Inspecteur de licences**

Affiche le nombre de fonctionnalités sous licence qui sont actuellement installées.

Vous pouvez vérifier si le nombre de licences BVMS installées excède le nombre de licences achetées.

Remarque : Si la configuration actuelle du système dépasse les limites des licences actuellement installées, vous ne pouvez pas activer la configuration.

8.10**Maintenance de BVMS**

Ce chapitre explique comment effectuer la maintenance d'un système BVMS qui vient d'être installé ou mis à niveau.

Pour assurer la maintenance du système, effectuez les tâches suivantes :

- Exportez la configuration de BVMS et les paramètres utilisateur. L'historique des versions (toutes les versions de la configuration précédemment activées) n'est pas exporté. Il est recommandé d'activer votre configuration avant l'exportation.
 - Pour connaître la procédure correspondante, reportez-vous à la section *Pour exporter des données de configuration* :, page 78.

Ou

- Effectuez une sauvegarde du fichier `elements.bvms`. Cette opération est nécessaire si vous voulez restaurer un serveur d'entreprise incluant l'historique des versions. Les paramètres utilisateur ne sont pas inclus.
 - Pour connaître la procédure correspondante, reportez-vous à la section *Pour effectuer une sauvegarde* :, page 78.
- Enregistrez le fichier de configuration VRM (`config.xml`).
 - Pour connaître la procédure correspondante, reportez-vous à la section *Pour enregistrer la configuration VRM* :, page 78.

Cette configuration exportée ne conserve pas l'historique du système. Aucun retour en arrière n'est possible.

L'ensemble de la configuration du système, y compris l'historique complet des modifications apportées au système, est stocké dans un seul fichier :

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

Pour exporter des données de configuration :

1. Dans le menu **Système**, cliquez sur **Exporter la configuration....**

La boîte de dialogue **Exporter le fichier de configuration** s'affiche.

Remarque : Si votre copie de la configuration en cours d'utilisation n'est pas activée



(est actif), vous pouvez exporter cette copie en cours d'utilisation et non la configuration activée.

2. Cliquez sur **Enregistrer**.

3. Entrez un nom de fichier.

La configuration actuelle est exportée. Un fichier .zip avec une base de données et des données d'utilisateur est créé.

Pour effectuer une sauvegarde :

1. Arrêtez le service **serveur central** BVMS sur (Enterprise) Management Server.
2. Copiez le fichier elements.bvms dans le répertoire souhaité pour le sauvegarder.
3. Démarrez le service **serveur central** BVMS sur (Enterprise) Management Server.

La configuration VRM est stockée dans un seul fichier chiffré config.xml.

Le fichier peut être copié et stocké pour la sauvegarde pendant que le service VRM est opérationnel.

Le fichier est chiffré et contient toutes les données VRM nécessaires telles que les suivantes :

- Les données d'utilisateur
- Tous les dispositifs du système et leurs paramètres VRM pertinents

Certaines parties de la configuration VRM sont également stockées dans la configuration de BVMS. Lorsque vous modifiez une valeur dans ces données, elle est écrite dans config.xml après l'activation de la configuration de BVMS.

Les paramètres suivants ne sont pas stockés dans la configuration de BVMS :

- **Paramètres du VRM > Paramètres principaux**
- **Réseau > SNMP**
- **Administration > Avancé**
- **Préférences d'enregistrement**
- **Équilibrage des charges**

Lorsque vous modifiez une valeur sur l'une de ces pages, elle est immédiatement écrite sur le serveur VRM et n'est pas enregistrée dans la configuration de BVMS.

Pour enregistrer la configuration VRM :

- ▶ Copiez Config.xml dans un endroit sûr.

Ce fichier se trouve dans le répertoire suivant d'un VRM principal :

C:\ProgramData\Bosch\VRM\primary

Ce fichier se trouve dans le répertoire suivant d'un VRM secondaire :

C:\ProgramData\Bosch\VRM\secondary

8.11

Remplacement d'un périphérique

Ce chapitre explique comment réparer le système lorsque, par exemple, des dispositifs subissent une défaillance et doivent être remplacés.

Prérequis

Les opérations de maintenance ont été effectuées.

Se reporter à

- *Maintenance de BVMS, page 77*

8.11.1**Remplacement d'un serveur/serveur d'entreprise**

Il n'y a aucune différence entre le remplacement d'un Management Server et celui d'un Management Server d'Enterprise.

Vous pouvez soit restaurer la configuration de l'ancien Management Server ou Management Server d'Enterprise, soit importer la configuration exportée.

Lorsque vous restaurez la configuration, l'ID serveur (Server ID) reste inchangé.

Lorsque vous importez la configuration, l'ID serveur (Server ID) du nouveau système est utilisé. Vous avez besoin d'un nouvel ID serveur (Server ID) si vous voulez créer un Enterprise System à l'aide d'une configuration exportée que vous importez dans chaque Management Server en tant que modèle. Chaque Management Server de ce Enterprise System doit avoir un ID serveur (Server ID) unique.

Vous pouvez importer une configuration exportée et les paramètres utilisateur de cette configuration. Les paramètres utilisateur contiennent les utilisateurs qui ont été ajoutés à cette configuration et leurs paramètres dans l'Operator Client, comme la taille des fenêtres et les favoris.

Remarque : l'importation d'une configuration ne restaure pas l'historique des versions de l'ancienne configuration. Lorsque vous importez une configuration, aucun paramètre utilisateur n'est importé. Vous devez restaurer manuellement les paramètres utilisateurs exportés.

Pour importer la configuration :

1. Dans le menu **Système**, cliquez sur **Import configuration ...**
La boîte de dialogue **Importer le fichier de configuration** s'affiche.
2. Sélectionnez le fichier à importer et cliquez sur **Ouvrir**.
La boîte de dialogue **Importer la configuration** s'affiche.
3. Entrez le mot de passe approprié et cliquez sur **OK**.
Le Configuration Client redémarre. Vous devez vous reconnecter.
La configuration importée n'est pas activée, mais modifiable dans Configuration Client.

Pour restaurer la configuration exportée :

Vous ne pouvez accéder à ce fichier (le copier, le supprimer) que lorsque le service **Serveur central** BVMS est arrêté.

1. Arrêtez le service **serveur central** BVMS sur (Enterprise) Management Server.
2. Si nécessaire, renommez le fichier de sauvegarde en Elements.bvms.
3. Remplacez le fichier Elements.bvms existant.
4. Démarrez le service **serveur central** BVMS sur (Enterprise) Management Server.

Remarque : pour réinitialiser le système avec une configuration vide, arrêtez le service, puis supprimez le fichier Elements.bvms.

Autres fichiers de configuration :

- Elements.bvms.bak (à partir de la V.2.2) : fichier de sauvegarde automatique de la dernière activation, historique des versions inclus. Les modifications ultérieures de la configuration qui ne sont pas activées ne sont pas incluses.
- Elements_Backup*****.bvms : configuration à partir d'une version plus ancienne. Ce fichier est créé après une mise à jour logicielle.

Pour restaurer les paramètres utilisateur exportés :

1. Extrayez le fichier ZIP qui a été créé lors de l'exportation de la maintenance.
Le fichier `export.bvms` et le répertoire `UserData` sont extraits.

- Sur le Management Server (d'Enterprise) de votre choix : copiez le répertoire UserData vers C:\ProgramData\Bosch\VMS\.

8.11.2

Remplacement d'un VRM

Exigences préalables

- Le système d'exploitation doit être installé avec des paramètres réseau corrects et la version appropriée du VRM.

Pour remplacer le dispositif VRM à partir du système BVMS :

- Démarrez le Configuration Client BVMS.
- Dans l'Arborescence des dispositifs, sélectionnez le dispositif VRM.
- Effectuez les configurations sur les pages suivantes, puis enregistrez et activez la configuration :

- Fenêtre principale > **Périphériques** > Développez  > Développez  > 
- Fenêtre principale > **Périphériques** > Développez  > Développez  > **Paramètres du VRM** > **Paramètres principaux**
- Fenêtre principale > **Périphériques** > Développez  > Développez  > **Réseau** > **SNMP**
- Fenêtre principale > **Périphériques** > Développez  > Développez  > **Administration** > **Avancé**
- Fenêtre principale > **Périphériques** > Développez  > Développez  >  >  >  > **Paramètres avancés** > **Préférences d'enregistrement**
- Fenêtre principale > **Périphériques** > Développez  > Développez  >  >  >  > **Équilibrage des charges**

Pour remplacer le dispositif VRM sans le système BVMS :

Utilisez la sauvegarde d'origine config.xml du dispositif VRM, laquelle contient tous les paramètres de configuration (aucun autre paramètre n'est nécessaire).

- Arrêtez le service **Video Recording Manager**.
- Copiez config.xml sur le nouveau serveur.
- Démarrez le service **Video Recording Manager**.

Pour remplacer un périphérique iSCSI (basculement planifié) :

- Ajoutez le nouveau dispositif iSCSI.
- À l'aide de Configuration Manager, sur le dispositif iSCSI à remplacer, configurez tous les LUN comme étant en lecture seule.

Remarque : vous pouvez supprimer l'ancien périphérique iSCSI lorsque vous n'avez plus besoin des anciens enregistrements.

**Remarque!**

Si vous configurez le nouveau dispositif iSCSI, nous vous recommandons d'utiliser le même mot de passe CHAP que pour l'ancien dispositif.

Si vous utilisez un nouveau mot de passe CHAP, assurez-vous de le définir comme un mot de passe CHAP à l'échelle du système et de l'affecter à tous les dispositifs iSCSI.

Dans le cas contraire, vous ne serez pas en mesure de vous authentifier sur le dispositif iSCSI et d'afficher la lecture directe à partir du dispositif iSCSI.

8.11.3**Remplacement d'un encodeur ou d'un décodeur****Remarque!**

Ne supprimez pas un périphérique de l'Arborescence des périphériques si vous voulez conserver ses enregistrements. Pour remplacer ce périphérique, échangez le matériel.

Remplacement d'un encodeur/décodeur du même type

Un préalable est un dispositif doté des paramètres par défaut (adresse IP = 192.168.0.1).

1. Déconnectez l'ancien dispositif du réseau.
2. Ne supprimez pas le dispositif de l'Arborescence des dispositifs dans BVMS Configuration Client. Lors de la suppression du dispositif d'un système VRM, l'enregistrement est perdu.
3. Connectez le nouveau périphérique du même type au réseau.

**Remarque!**

Les étapes suivantes nécessitent l'adresse IP par défaut mentionnée ci-dessus. Avec les adresses IP affectées par DHCP, vous pouvez effectuer la recherche de périphériques initiale.

4. Configuration Client : Dans le menu **Matériel**, cliquez sur **Recherche de périphérique initiale...**
La boîte de dialogue **Recherche de périphérique initiale** s'affiche.
5. Cliquez sur une cellule pour modifier l'adresse souhaitée. Pour modifier plusieurs périphériques, sélectionnez les lignes de votre choix. Vous pouvez sélectionner plusieurs dispositifs en appuyant sur la touche CTRL ou MAJ. Cliquez avec le bouton droit de la souris sur les lignes sélectionnées, puis cliquez sur **Définir les adresses IP...** ou sur **Définir le masque de sous-réseau...** pour modifier les valeurs correspondantes. Vous devez entrer l'adresse IP et le masque de sous-réseau corrects.
Le masque de sous-réseau et l'adresse IP doivent être identique à ceux du dispositif remplacé.
6. Cliquez sur **OK**.
7. Après quelques secondes, vous pouvez accéder aux paramètres du périphérique dans l'Arborescence des périphériques.
8. Modifiez tous les paramètres appropriés du dispositif qui ne sont pas contrôlés par BVMS (reportez-vous aux informations ci-dessous).
9. Enregistrez et activez.

Notes :

- La recherche initiale de dispositifs ne détecte que ceux ayant l'adresse IP par défaut (192.168.0.1) ou dont l'adresse IP est un doublon.
- N'utilisez pas la recherche VRM pour détecter les dispositifs par défaut, car vous ne pourrez plus modifier l'adresse IP.




Remplacement d'un encodeur avec l'adresse IP affectée par DHCP :


Un préalable est un encodeur avec les paramètres par défaut (IP affectée par DHCP).



1. Connectez l'encodeur directement au port Ethernet de votre ordinateur.
2. Notez la configuration de la carte réseau pour TCP/IPv4 afin de la restaurer ultérieurement.
3. Sur la carte réseau de votre ordinateur, configurez l'adresse IP fixe et le masque de sous-réseau suivants pour votre carte réseau :
192.168.0.2
255.255.255.0
4. Démarrez Internet Explorer.
5. Dans la barre d'**adresse**, saisissez 192.168.0.1.
La page Web du périphérique s'affiche.
6. Cliquez sur **Paramètres**, puis sur **Réseau**.
7. Sur la page **Réseau**, dans la liste **DHCP**, sélectionnez **Désactivé**.
8. Dans les champs **Adresse IP**, **Masque de sous-réseau** et **Adresse passerelle**, saisissez les valeurs appropriées valides pour votre réseau.
9. Cliquez sur **Définir et réinitialiser**.
10. Restaurez la configuration de la carte réseau.

Remplacement d'un encodeur/décodeur par un autre type de dispositif

- Déconnectez l'ancien dispositif du réseau.
- Ne supprimez pas le dispositif de l'arborescence des dispositifs dans BVMS Configuration Client.
- Connectez le nouveau dispositif du nouveau type au réseau.

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier l'encodeur** > Boîte de dialogue **Modifier l'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier l'encodeur** > Boîte de dialogue **Modifier l'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier l'encodeur** > Boîte de dialogue **Modifier l'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier le décodeur** > Boîte de dialogue **Modifier le décodeur**

Après une mise à niveau du périphérique, vous pouvez mettre à jour les fonctions du périphérique. Un message vous informe si les fonctions récupérées du périphérique correspondent à celles enregistrées dans BVMS.

Pour mettre à jour :

1. Cliquez sur **OK**.

Une boîte de message s'affiche avec le texte suivant :

Si vous appliquez les fonctions du périphérique, il se peut que les paramètres d'enregistrement soient modifiés. Vérifiez ces paramètres pour ce périphérique.

2. Cliquez sur **OK**.

Les fonctions du périphérique sont mises à jour.

Remplacement d'une caméra VSG

Lorsque vous remplacez une caméra VSG, assurez-vous que la caméra remplacée a le même type, la même adresse IP et le même profil ONVIF que l'ancienne caméra.

Par ailleurs, vous devez effectuer les configurations suivantes sur la nouvelle caméra AXIS via l'interface Web de la caméra VSG avant de remplacer l'ancienne caméra AXIS :

- Définir un mot de passe pour la racine de l'utilisateur
- Configurer la synchronisation temporelle
- Désactiver l'adresse locale du lien
- Créer un utilisateur ONVIF
- Désactiver la protection contre les attaques par relecture

Paramètres contrôlés par BVMS

Les encodeurs et décodeurs configurés dans un système BVMS sont contrôlés par le serveur BVMS. Par conséquent, ils ne peuvent pas être partagés avec d'autres applications.

Vous pouvez utiliser le Gestionnaire de périphériques BVMS pour vérifier quel périphérique comporte une configuration incompatible différente de la configuration de BVMS.

BVMS Configuration Client propose des pages de configuration pour tous les dispositifs BVIP.

L'échelle des paramètres dépend du modèle BVIP particulier (par exemple, VIPX 1600 XFM4).

BVMS garde le contrôle de tous les paramètres BVIP requis pour une intégration en toute transparence dans le système BVMS.

Paramètres contrôlés par BVMS :

- Nom de la caméra
- Paramètres du serveur de synchronisation
- Gestion des enregistrements (profils, durées de conservation, planifications)
- Définition de paramètres de qualité
- Mots de passe

Stockés dans la configuration BVMS mais non modifiés sur les dispositifs :

- Adresse IP (vous pouvez modifier les adresses IP avec la fonctionnalité Configuration de périphériques IP de BVMS)
- Noms de relais/d'entrées (affichage de la différence entre les noms sur le dispositif et les noms configurés dans BVMS)

Événements système pour une configuration de périphérique incompatible

- Les événements SystemInfo (Informations sur le système) sont générés une fois que la configuration d'un périphérique a été corrigée pendant un contrôle périodique.
- Les événements SystemWarning (Avertissement système) sont générés une fois qu'une configuration incompatible a été détectée pour la première fois sur un périphérique. Les contrôles suivants ne déclenchent pas cet événement tant que la configuration n'a pas été corrigée par une activation ou une correction périodique.

- Les événements SytemError (Erreur système) sont générés une fois qu'une erreur relative à la configuration a été détectée pendant une activation ou des contrôles périodiques. Les contrôles suivants ne déclenchent pas cet événement tant que la configuration n'a pas été corrigée par une activation ou une correction périodique.

8.11.4 Remplacement d'un Operator Client

Pour remplacer un poste de commande Operator Client :

1. Remplacez l'ordinateur.
2. Commencez l'installation de BVMS sur le nouvel ordinateur.
3. Dans la liste des composants à installer, sélectionnez Operator Client.
Le cas échéant, sélectionnez d'autres composants qui étaient installés sur l'ordinateur remplacé.
4. Installez les logiciels.

8.11.5 Tests finaux

Pour vérifier le remplacement d'un serveur/serveur d'entreprise et le remplacement de l'Operator Client :

1. Activez la configuration.
2. Démarrez Operator Client.
3. Vérifiez l'Arborescence logique dans l'Operator Client.
Elle doit être identique à l'Arborescence logique dans Configuration Client.

Pour vérifier le remplacement d'un VRM :

- ▶ Démarrez le VRM Monitor et vérifiez les enregistrements actifs.

8.11.6 Récupération de Divar IP 3000/7000

Reportez-vous aux manuels d'installation de DIVAR IP 3000 ou de DIVAR IP 7000. Pour savoir comment procéder, reportez-vous au chapitre relatif à la récupération de l'unité.

8.12 Configuration de la synchronisation temporelle



Remarque!

, assurez-vous que l'heure de tous les ordinateurs de BVMS est synchronisée avec Management Server. À défaut, vous risquez de perdre les enregistrements. Configurez le logiciel du serveur de synchronisation sur le Management Server. Sur les autres ordinateurs, configurez l'adresse IP du Management Server comme serveur de synchronisation à l'aide des procédures Windows standard.

8.13 Configuration du support de stockage d'un encodeur

Fenêtre principale > **Périphériques** > Développez  > Développez  >  >  > **Paramètres avancés** > **Gestion des enregistrements**

Remarque : vérifiez que les caméras souhaitées de cet encodeur sont ajoutées à Arborescence logique.

Vous devez configurer le support de stockage d'un encodeur pour utiliser la fonction ANR.



Remarque : Si vous voulez configurer le support de stockage d'un encodeur qui a déjà été ajouté à votre système et qui est enregistré via VRM, assurez-vous que l'enregistrement secondaire est arrêté.

General Camera **Recording** Alarm VCA Interfaces Network Service


Recording Management Recording Preferences SD Card Status



Primary Recording

Preferred storage target type: Managed

Recording is managed by: 172.30.11.75 Encryption  

Secondary Recording

Preferred storage target type: SD card 

Local target: 172.31.22.52  98% of 14.75 GB in use 

Retention time [days]: Auto

La fonction ANR ne peut fonctionner que sur les encodeurs dotés de la version 5.90 (ou ultérieure) du firmware. Tous les types d'encodeurs ne prennent pas en charge ANR même si la version de firmware correcte est installée.

Pour configurer le support de stockage d'un encodeur :

1. Sous **Enregistrement secondaire**, dans la liste **Types cible de stockage préférés**, sélectionnez les supports de stockage. En fonction du type de dispositif, différents supports sont disponibles.
2. Si nécessaire, cliquez sur le bouton ... pour formater le support de stockage. Une fois le processus de formatage terminé, le support de stockage est prêt pour être utilisé avec la fonction ANR.
3. Configurez la ANR de cet encodeur dans la page **Caméras et enregistrement**.

Se reporter à

- Page *Gestion des enregistrements*, page 240
- Page *Configuration de la fonction ANR*, page 314

9 Création d'un système d'entreprise

Effectuez les tâches ci-après pour créer un système d'entreprise sur un Enterprise Management Server et sur plusieurs ordinateurs Management Server.

1. Configuration de la liste des serveurs pour le système d'entreprise, page 86
2. Création d'un Enterprise User Group, page 87
3. Création d'un Enterprise Account, page 88

Vous avez besoin de licences valides pour l'utilisation d'un Enterprise System.

Se reporter à

- Enterprise System, page 24

9.1 Configuration de la liste des serveurs pour le système d'entreprise

Fenêtre principale > **Périphériques** > **Enterprise System** > **Liste de serveurs / Carnet d'adresses**




Vous pouvez configurer plusieurs ordinateurs serveurs dans la liste des serveurs d'un Management Server approprié.

Pour un accès simultané, vous devez configurer un ou plusieurs Enterprise User Groups. Cela transforme Management Server en Enterprise Management Server.

Un utilisateur de Operator Client peut se connecter avec le nom d'utilisateur d'un Enterprise User Group pour obtenir un accès simultané aux ordinateurs Management Server configurés dans la liste des serveurs.

Les autorisations d'exploitation sont configurées sur Enterprise Management Server dans **Groupes d'utilisateurs**, onglet Enterprise User Group.

Les autorisations des périphériques sont configurées sur chaque Management Server dans **Groupes d'utilisateurs**, onglet Enterprise Access.

- Cliquez sur  pour enregistrer les paramètres.
- Cliquez sur  pour annuler le dernier paramètre.
- Cliquez sur  pour activer la configuration.

Pour ajouter des serveurs :

1. Cliquez sur **Ajouter un serveur**.
La boîte de dialogue **Ajouter un serveur** s'affiche.
2. Saisissez un nom d'affichage pour le serveur et saisissez l'adresse réseau privée (nom DNS ou adresse IP).
Remarque : Si vous utilisez une connexion SSH, saisissez l'adresse au format suivant : ssh://IP ou nomserveur:5322
3. Cliquez sur **OK**.
4. Répétez les étapes suivantes jusqu'à ce que vous ayez ajouté tous les ordinateurs Management Server souhaités.

Pour ajouter des colonnes :

- ▶ Cliquez avec le bouton droit de la souris sur l'en-tête du tableau et cliquez sur **Ajouter une colonne**.

Vous pouvez ajouter jusqu'à 10 colonnes.

Pour supprimer une colonne, cliquez avec le bouton droit de la souris sur la colonne souhaitée, puis sur **Supprimer la colonne**.

- ⇒ La liste des serveurs que vous exportez contiendra également les colonnes ajoutées. Les ordinateurs Management Server pour votre Enterprise System sont configurés.

Se reporter à

- *Enterprise System, page 24*
- *Page Liste de serveurs / Carnet d'adresses, page 130*
- *Page Groupes d'utilisateurs, page 341*
- *Utilisation de la recherche de serveur, page 74*

9.2

Création d'un Enterprise User Group

Fenêtre principale > **Groupes d'utilisateurs**


Vous effectuez la tâche suivante : créer un Enterprise User Group pour un Enterprise System sur le Enterprise Management Server.

Vous créez un Enterprise User Group avec les utilisateurs pour configurer leurs autorisations d'exploitation. Ces autorisations d'exploitation sont disponibles sur un Operator Client qui est connecté à l'Enterprise Management Server. L'interface utilisateur du moniteur d'alarme est un exemple d'autorisation d'exploitation.

Pour créer un Enterprise User Group :

1. Cliquez sur l'onglet **Enterprise User Groups**.

Remarque : L'onglet **Enterprise User Groups** est disponible uniquement si la licence appropriée est disponible, et si un ou plusieurs ordinateurs Management Server sont configurés dans **Périphériques > Enterprise System > Liste de serveurs / Carnet d'adresses**.

2. Cliquez sur .
3. Tapez le nom et une description.
4. Cliquez sur **OK**.
Le Enterprise User Group est ajouté à l'arborescence correspondante.
5. Cliquez avec le bouton droit de la souris sur le groupe Enterprise, puis cliquez sur **Renommer**.
6. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.
7. Dans la page **Autorisations d'utilisation**, configurez les autorisations d'exploitation et l'accès aux serveurs des ordinateurs Management Server configurés, comme cela est requis.

Se reporter à

- *Page Propriétés du groupe d'utilisateurs, page 343*
- *Page des fonctionnalités d'Operator, page 350*
- *Page Priorités, page 354*
- *Page Interface utilisateur, page 354*
- *Page Accès au serveur, page 355*

9.3 Création d'un Enterprise Account

Fenêtre principale > **Groupes d'utilisateurs**




Remarque!

Au moins un dispositif doit être configuré dans l'arborescence des dispositifs pour que vous puissiez ajouter un Enterprise Account.

Vous effectuez la tâche suivante : créer un Enterprise Account sur un Management Server. Répétez cette tâche sur chaque Management Server membre de votre Enterprise System. Vous pouvez créer un Enterprise Account pour configurer les autorisations du dispositif pour un Operator Client à l'aide de Enterprise System.

Pour créer un Enterprise Account:

1. Cliquez sur l'onglet **Accès Enterprise**.
2. Cliquez sur .
La boîte de dialogue **Nouveau compte Enterprise Account** s'affiche.
3. Tapez le nom et une description.
4. La case **L'utilisateur doit changer le mot de passe lors de la prochaine connexion** est présélectionnée pour tous les nouveaux comptes utilisateur créés.
Saisissez la clé en suivant les règles de clé et confirmez cette clé.
5. Cliquez sur **OK**.
Un nouvel Enterprise Account est ajouté à l'arborescence correspondante.
6. Cliquez avec le bouton droit de la souris sur le nouvel Enterprise Account, puis cliquez sur **Renommer**.
7. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.
8. Dans la page **Autorisations du périphérique**, configurez les identifiants et les autorisations de dispositif comme il convient.

Se reporter à

- *Stratégie de mot de passe fort*, page 365
- *Page d'identifiants*, page 349
- *Page Arborescence Logique*, page 350
- *Page Événements et alarmes*, page 349
- *Page Priorité des commandes*, page 347
- *Page Autorisations de caméra*, page 346
- *Page Autorisations de décodeur*, page 348

9.4 Authentification basée sur les jetons

L'Enterprise Account permet aux clients de gestion Enterprise d'accéder à un Management Server qui est configuré dans la liste d'accès au serveur du Enterprise Management Server. L'Enterprise Account est sécurisé par une clé. Lorsque vous devez modifier cette clé, celle-ci doit également être modifiée sur le Management Server ainsi que sur le EnterpriseManagement Server. Par ailleurs, vous devez activer la configuration modifiée. Si un grand nombre de Management Server sont connectés à un Enterprise Management Server, cela peut s'avérer chronophage.

Au lieu de sécuriser l'Enterprise Account avec un nom d'utilisateur et une clé, vous pouvez configurer l'authentification basée sur des jetons.

1. Le Enterprise Management Server crée le jeton.

2. Le jeton est signé à l'aide d'un certificat appelé Token Issuer.
3. Le Management Server autorise l'accès lorsque le jeton est valide.
Le Management Server n'autorise l'accès que si le Management Server est configuré pour faire confiance au certificat Token Issuer.

Exigences préalables

Pour signer et valider le jeton, vous avez besoin d'un certificat ou d'une chaîne de certificats.

Remarque : les certificats ne sont ni générés ni installés par BVMS. Vous devez les fournir et les installer de façon indépendante. BVMS peut utiliser les certificats installés dans le Windows Certificate Store.

Il existe différentes prérequis concernant les machines Enterprise Management Server et Management Server. Les exemples ci-après expliquent quels environnements requièrent quels certificats.

Certificat

- Le Enterprise Management Server requiert le certificat et sa clé privée.
- Le Management Server requiert le certificat.

Chaîne de certificats

Une chaîne de certificats commence par un certificat Root que vous utilisez pour signer un autre certificat. Vous pourrez ensuite utiliser à nouveau ce certificat pour signer un autre certificat. Vous pouvez définir vous-même la longueur des chaînes de certificats.

- L'Enterprise Management Server requiert l'intégralité de la chaîne de certificats. Pour le dernier certificat de la chaîne (Token Issuer), une clé privée est requise.
- Le Management Server ne nécessite que certaines parties de la chaîne de certificats, selon les paramètres du jeton d'accès configurés.

Pour configurer l'authentification basée sur des jetons, procédez comme suit :

1. Configuration du Enterprise Management Server
 - Définir l'authentification par jeton d'accès pour les Enterprise Accounts
 - Configurer les paramètres de jeton d'accès
2. Configuration du Management Server
 - Spécifier les certificats approuvés
 - Refuser l'accès au Enterprise Account par clé




Pour obtenir des informations détaillées sur un sujet spécifique, consultez le livre blanc sur l'authentification basée sur les jetons.

Se reporter à

- *Boîte de dialogue Access token settings (Paramètres de jeton d'accès) (menu Paramètres), page 120*
- *Page Accès au serveur, page 355*

10 Configuration de Scripts de Commande

Ce chapitre explique comment configurer des Scripts de commande. Les Scripts de commande apparaissent à différents endroits de BVMS.

1. Cliquez sur  pour enregistrer les paramètres.
2. Cliquez sur  pour annuler le dernier paramètre.
3. Cliquez sur  pour activer la configuration.



Remarque!

Les scripts de serveur sont activés lors du redémarrage du service de Management Server même s'ils ne sont pas activés à partir du Configuration Client.

10.1 Gestion des Scripts de Commande

Fenêtre principale


Vous pouvez créer un script de Commande en utilisant les langages de script suivants :

- C#
- VB.Net

Vous ne pouvez pas modifier le langage de script d'un script de commande existant.

Vous pouvez créer un script client ou serveur.

Il est en outre possible d'ajouter des scriptlets à n'importe quel script.

Pour une aide sur la saisie du code, cliquez sur  dans la boîte de dialogue **Éditeur de Script de Commande**. L'aide du script de l'interface API de Bosch s'affiche.

Pour ajouter un scriptlet serveur :

1. Dans le menu **Outils**, cliquez sur la commande **Éditeur de Script de Commande...**
La boîte de dialogue **Sélectionner un langage de script** s'ouvre si aucun script de commande n'a été créé.
2. Dans la liste **Langage de script** :, sélectionnez l'entrée requise.
La boîte de dialogue **Éditeur de Script de Commande** s'ouvre.
3. Dans le volet gauche de la boîte de dialogue **Éditeur de Script de Commande**, cliquez avec le bouton droit de la souris sur **ServerScript**, puis cliquez sur **Nouveau scriptlet**.
Un nouveau scriptlet est ajouté.
4. Entrez votre code.


Pour ajouter un scriptlet client

1. Dans le menu **Outils**, cliquez sur la commande **Éditeur de Script de Commande...**
La boîte de dialogue **Sélectionner un langage de script** s'ouvre si aucun script de commande n'a été créé.
2. Dans la liste **Langage de script** :, sélectionnez l'entrée requise.
La boîte de dialogue **Éditeur de Script de Commande** s'ouvre.
3. Dans le volet gauche de la boîte de dialogue **Éditeur de Script de Commande**, cliquez avec le bouton droit de la souris sur **ClientScript**, puis cliquez sur **Nouveau scriptlet**.
Un nouveau scriptlet est ajouté.
4. Entrez votre code.


Pour supprimer un scriptlet :

1. Ouvrez la boîte de dialogue **Éditeur de Script de Commande**.
2. Cliquez sur l'onglet **Script de serveur** ou **Script de client** selon le cas.

3. Dans l'Arborescence des Événements, cliquez avec le bouton droit de la souris sur

l'événement approprié, puis cliquez sur .
Le scriptlet est supprimé.

Pour quitter la boîte de dialogue Éditeur de Script de Commande :

- ▶ Cliquez sur .

Se reporter à

- *Boîte de dialogue Éditeur de Script de Commande, page 319*

10.2

Configuration d'un Script de Commande à exécution automatique

Fenêtre principale > **Alarmes** >  ou  > colonne **Options d'alarmes** > ...

Vous pouvez configurer un Script de Commande client qui sera exécuté dans les cas suivants :

- Au démarrage du poste de commande.
- Lorsque l'utilisateur accepte une alarme.

Pour configurer un Script de Commande qui sera exécuté dès le démarrage du poste de commande :

Voir Configuration d'un Script de Commande de démarrage.

Pour configurer un Script de Commande qui sera exécuté dès l'acceptation d'une alarme par un utilisateur :

1. Cliquez sur l'onglet **Flux de travail**.
2. Dans la liste **Lorsque l'alarme est acceptée, exécutez le script de client suivant :**, sélectionnez le Script client souhaité.
Ce script sera exécuté dès l'acceptation de l'alarme sélectionnée par un utilisateur.

Se reporter à

- *Boîte de dialogue Options d'alarmes, page 325*
- *Configuration d'un script de commande de démarrage (page des paramètres), page 92*


10.3

Importation d'un Script de Commande

Fenêtre principale

Vous pouvez importer des scripts de commande qui ont été développés sur un autre ordinateur. Le fichier doit être écrit dans le même langage de script que celui utilisé sur votre système.

Pour importer un Script de Commande :

1. Dans le menu **Outils**, cliquez sur la commande **Éditeur de Script de Commande...**
La boîte de dialogue **Éditeur de Script de Commande** s'affiche.
2. Cliquez sur .
3. Sélectionnez le fichier de script requis, puis cliquez sur **OK**.

Se reporter à


- *Boîte de dialogue Éditeur de Script de Commande, page 319*

10.4 Exportation d'un Script de Commande

Fenêtre principale

Vous pouvez exporter des scripts de commande qui ont été développés sur un autre ordinateur.

Pour exporter un Script de Commande :

1. Dans le menu **Outils**, cliquez sur la commande **Éditeur de Script de Commande...**
La boîte de dialogue **Éditeur de Script de Commande** s'affiche.
2. Cliquez sur .
La boîte de dialogue d'enregistrement d'un fichier s'affiche.
3. Entrez le nom du fichier de script requis, puis cliquez sur **OK**.

Se reporter à

- *Boîte de dialogue Éditeur de Script de Commande, page 319*

10.5 Configuration d'un script de commande de démarrage (page des paramètres)

Fenêtre principale > **Périphériques** > Développer  >  > page **Paramètres**

Vous pouvez configurer un Script de Commande qui sera exécuté au démarrage du Operator Client sur le poste de commande sélectionné.

Vous devez créer un Script de Commande correspondant.

Pour créer un Script de Commande, voir *Gestion des Scripts de Commande, page 90*.

Pour créer un script de démarrage :

- ▶ Dans la liste **Script de démarrage :**, sélectionnez le Script de Commande requis.

Se reporter à

- *Page Poste de commande, page 139*




11 Gestion des données de configuration

Fenêtre principale

Vous devez activer la configuration actuelle pour que le Management Server and Operator Client puisse s'en servir. Le système vous rappelle de l'activer lorsque vous quittez le Configuration Client.

Toute configuration activée est enregistrée avec sa date et sa description, le cas échéant. Vous pouvez à tout moment restaurer une configuration récemment activée. Toutes les configurations enregistrées entre-temps sont perdues.

Vous pouvez exporter la configuration en cours d'utilisation dans un fichier de configuration pour importer ce fichier ultérieurement. Cela permettra de restaurer la configuration exportée. Toutes les configurations enregistrées entre-temps sont perdues.

- Cliquez sur  pour enregistrer les paramètres.
- Cliquez sur  pour annuler le dernier paramètre.
- Cliquez sur  pour activer la configuration.

11.1 Activation de la configuration en cours d'utilisation

Fenêtre principale

Vous activez la configuration en cours d'utilisation. Operator Client utilise la configuration activée au prochain démarrage si l'utilisateur l'a acceptée. Si l'activation est effective, toutes les instances d'Operator Client ouvertes sur le réseau se ferment et redémarrent. L'utilisateur de chaque instance Operator Client n'a généralement pas besoin de se reconnecter.

Vous pouvez configurer une heure d'activation ultérieure. Si vous configurez une heure d'activation ultérieure, la configuration de travail ne sera pas activée immédiatement, mais à l'heure définie. Si vous configurez une autre heure d'activation par la suite (ultérieure ou non), cette nouvelle heure prévaut. L'heure d'activation configurée auparavant est supprimée.

Lorsque vous quittez le Configuration Client, le système vous rappelle d'activer la copie de la configuration en cours d'utilisation.

Vous ne pouvez pas activer une configuration qui contient un périphérique sans protection par mot de passe.



Remarque!


Si l'activation est effective, chaque instance d'Operator Client redémarre lorsque la configuration est activée. Évitez les activations inutiles. Effectuez les activations de préférence la nuit ou pendant les périodes de faible activité.



Remarque!

Si le système comprend des périphériques qui ne sont pas protégés par mot de passe, vous devez sécuriser ces périphériques avant de pouvoir activer une configuration. Vous pouvez désactiver cette mise en application du mot de passe.

Pour activer la configuration en cours d'utilisation :

1. Cliquez sur  .
La boîte de dialogue **Activer la configuration** s'affiche.
Si votre configuration contient des périphériques qui ne sont pas protégés par un mot de passe, vous ne pouvez pas l'activer. Dans ce cas, la boîte de dialogue **Protéger les périphériques avec un mot de passe par défaut...** s'affiche.
Suivez les instructions de cette boîte de dialogue et cliquez sur **Appliquer**.
La boîte de dialogue **Activer la configuration** s'affiche de nouveau.
2. Si nécessaire, saisissez une heure d'activation ultérieure. Par défaut, l'heure d'activation est l'heure actuelle. Si vous ne définissez pas une heure d'activation ultérieure, l'activation intervient immédiatement.
Si nécessaire, cochez **Forcer l'activation pour tous les Operator Clients**.
3. Saisissez une description, puis cliquez sur **OK**.
La configuration actuelle est activée.
Chaque poste de commande Operator Client redémarre instantanément s'il est connecté au réseau et que l'activation est effective. Si un poste de commande n'est pas connecté, il redémarre dès qu'il est connecté de nouveau.
Si vous avez configuré une heure d'activation ultérieure, la configuration sera activée ultérieurement.

Remarque : L'activation retardée n'est pas exécutée tant que l'utilisateur est connecté à Configuration Client.

Se reporter à

- Boîte de dialogue Protéger les dispositifs avec un mot de passe global par défaut (menu Matériel), page 106
- Boîte de dialogue Activer la configuration (menu Système), page 105

11.2 Activation d'une configuration

Fenêtre principale

Vous pouvez activer une version antérieure de la configuration préalablement enregistrée.

Pour activer une configuration :

1. Dans le menu **Système**, cliquez sur **Gestionnaire d'activation...**
La boîte de dialogue **Gestionnaire d'activation** s'affiche.
2. Dans la liste, sélectionnez la configuration à activer.
3. Cliquez sur **Activer**.
Une boîte de message s'affiche.
4. Cliquez sur **OK**.
La boîte de dialogue **Activer la configuration** s'affiche.
5. Si nécessaire, cochez **Forcer l'activation pour tous les Operator Clients**. Chaque poste de commande Operator Client est automatiquement redémarré pour activer la nouvelle configuration. L'utilisateur ne peut pas refuser la nouvelle configuration.
Si la case **Forcer l'activation pour tous les Operator Clients** n'est pas cochée, une boîte de dialogue s'affiche pendant quelques secondes sur chaque poste de commande Operator Client. L'utilisateur peut accepter ou refuser la nouvelle configuration. La boîte de dialogue se ferme au bout de quelques secondes si l'utilisateur n'intervient pas. Dans ce cas, la nouvelle configuration n'est pas acceptée.

Se reporter à

- Boîte de dialogue Activer la configuration (menu Système), page 105
- Boîte de dialogue Gestionnaire d'activation (menu Système), page 105

11.3**Exportation de données de configuration**

Fenêtre principale

Vous pouvez exporter les données de configuration de BVMS dans un fichier .zip. Ce fichier .zip contient le fichier de données (Export.bvms) et les données d'utilisateur (fichier .dat).

Vous pouvez utiliser ces fichiers pour restaurer la configuration d'un système qui a déjà été exportée auparavant sur le même Management Server (Enterprise) ou pour l'importer sur un autre Management Server (Enterprise). Le fichier de données d'utilisateur ne peut pas être importé, mais vous pouvez vous en servir pour restaurer manuellement la configuration utilisateur.

Pour exporter des données de configuration :

1. Dans le menu **Système**, cliquez sur **Exporter la configuration...**

La boîte de dialogue **Exporter le fichier de configuration** s'affiche.

Remarque : Si votre copie de la configuration en cours d'utilisation n'est pas activée



(est actif), vous pouvez exporter cette copie en cours d'utilisation et non la configuration activée.

2. Cliquez sur **Enregistrer**.
3. Entrez un nom de fichier.

La configuration actuelle est exportée. Un fichier .zip avec une base de données et des données d'utilisateur est créé.

Se reporter à

- Importation de données de configuration, page 95

11.4**Importation de données de configuration**

Fenêtre principale

Les cas d'utilisation suivants sont couverts :

- Importer une configuration qui a déjà été exportée (une sauvegarde a été effectuée) auparavant sur le même serveur
- Importer un modèle de configuration qui a été préparé et exporté sur un autre serveur
- Importer la configuration d'une version antérieure de BVMS.

Vous pouvez importer une configuration uniquement si les derniers changements de la copie en cours d'utilisation sont enregistrés et activés.

Pour importer les données de configuration, vous avez besoin du mot de passe approprié.

Vous ne pouvez pas importer des données d'utilisateur.

Pour importer la configuration :

1. Dans le menu **Système**, cliquez sur **Import configuration ...**

La boîte de dialogue **Importer le fichier de configuration** s'affiche.

2. Sélectionnez le fichier à importer et cliquez sur **Ouvrir**.

La boîte de dialogue **Importer la configuration** s'affiche.

3. Entrez le mot de passe approprié et cliquez sur **OK**.

Le Configuration Client redémarre. Vous devez vous reconnecter.

La configuration importée n'est pas activée, mais modifiable dans Configuration Client.

**Remarque!**

Si vous souhaitez éditer la configuration qui a été activée pour votre Management Server, effectuez un retour arrière dans la boîte de dialogue **Activer la configuration**.

Se reporter à

– *Exportation de données de configuration, page 95*

11.5**Exportation de données de configuration vers OPC**

Fenêtre principale

Vous pouvez exporter les données de configuration des dispositifs de BVMS dans un fichier XML pour l'importer dans une application de serveur OPC. Ce fichier doit être stocké dans le répertoire bin de votre installation de BVMS.

Pour configurer une connexion BVMS - BIS, le manuel d'installation BVMS - BIS Connectivity et la Note de service technique BVMS OPC Server sont disponibles.

**Remarque!**

Installez le serveur BIS et BVMS Management Server sur deux ordinateurs différents. L'exécution des deux systèmes sur un même ordinateur réduit leurs performances et risque de provoquer de graves défaillances logicielles.

Pour exporter des données de configuration :

1. Dans le menu **Système**, cliquez sur **Exporter les informations sur le périphérique pour OPC**.
La boîte de dialogue **Exporter le fichier d'informations sur le périphérique** s'affiche.
2. Saisissez un nom de fichier, puis cliquez sur **Enregistrer**.
Le fichier est enregistré.
Vous pouvez importer ce fichier dans l'application serveur OPC.

11.6**Vérification de l'état de vos encodeurs/décodeurs**

Fenêtre principale > menu **Matériel** > commande **Moniteur de périphériques...** > boîte de dialogue **Moniteur de périphériques**

Vous pouvez vérifier l'état de tous les encodeurs/décodeurs activés dans l'arborescence des périphériques.

Se reporter à

– *Boîte de dialogue Moniteur de dispositifs (menu Matériel), page 111*

11.7**Configuration de la surveillance SNMP**

Fenêtre principale

Pour procéder à une configuration :

1. Dans le menu **Paramètres**, cliquez sur **Paramètres SNMP...**
La boîte de dialogue **Paramètres SNMP** s'affiche.
2. Définissez les paramètres requis, puis cliquez sur **OK**.

Pour désactiver GetRequest SNMP :

- ▶ Dans le champ **Port GET SNMP**, supprimez le contenu du champ.
BVMS n'écoute plus les GetRequest SNMP.

Se reporter à

– *Boîte de dialogue Paramètres SNMP (menu Paramètres), page 116*

11.8 Création d'un rapport

Fenêtre principale

Vous pouvez créer des rapports dans lesquels les informations sur la configuration actuelle sont collectées.

Pour créer un rapport :

1. Dans le menu **Rapports**, cliquez sur la commande souhaitée.
. La boîte de dialogue correspondante s'affiche.
2. Cliquez sur **Exporter en CSV**.
3. Entrez le chemin et le nom de fichier du nouveau rapport.
4. Ouvrez le fichier CSV dans Microsoft Excel ou une autre application de tableur afin d'en vérifier le contenu.

Se reporter à

- *Boîte de dialogue Planifications d'Enregistrement, page 114*
- *Boîte de dialogue Planifications de Tâches, page 114*
- *Boîte de dialogue des paramètres de caméra et d'enregistrement, page 115*
- *Boîte de dialogue Paramètres de qualité du flux, page 115*
- *Boîte de dialogue des paramètres d'événement, page 115*
- *Boîte de dialogue des paramètres d'événements combinés, page 115*
- *Boîte de dialogue Paramètres d'alarme, page 115*
- *Boîte de dialogue des utilisateurs configurés, page 115*
- *Boîte de dialogue Groupes d'utilisateurs et Comptes, page 115*
- *Boîte de dialogue Autorisations d'exploitation, page 116*

12 Exemples de configuration

Ce chapitre présente des exemples montrant comment configurer les périphériques sélectionnés dans BVMS.






12.1 Ajout d'une interface ATM/POS Bridge Bosch




Cet exemple décrit la manière de configurer une ATM/POS Bridge Bosch.

Configuration de la ATM/POS Bridge

1. Vérifiez que le périphérique est sous tension.
2. Pour configurer l'adresse IP et le masque de sous-réseau du périphérique, raccordez-le à un port COM de votre ordinateur à l'aide d'un câble RS-232 (utilisez le câble Bosch spécifié). Pour plus de détails, consultez le Manuel de d'installation de la ATM/POS Bridge.
3. Sur cet ordinateur, lancez une session HyperTerminal (en règle générale : **Démarrer > Tous les programmes > Accessoires > Communications > HyperTerminal**).
4. Saisissez un nom pour la session et cliquez sur **OK**.
5. Sélectionnez le numéro du port COM et cliquez sur **OK**.
6. Définissez les paramètres de port COM suivants :
 - 9 600 bit/s
 - 8 bits de données
 - sans contrôle de parité ;
 - 1 bit d'arrêt
 - contrôle du flux matériel
 Cliquez sur **OK**.
7. Appuyez sur F1 pour afficher le menu des options système du périphérique.
8. Saisissez 1 pour définir l'adresse IP et le masque de sous-réseau comme il convient.
9. Conservez les paramètres par défaut des ports :
 - port1 : **4201**
 - port2 : **4200**



Ajouter la ATM/POS Bridge à BVMS

1. Connectez le périphérique à votre réseau BVMS.
2. Démarrez Configuration Client.
3. Cliquez sur **Périphériques**, développez l'arborescence logique, développez , cliquez avec le bouton droit de la souris sur , cliquez sur **Ajouter interface ATM/POS-Bridge Bosch**.
La boîte de dialogue **Ajouter interface ATM/POS-Bridge Bosch** s'affiche.
4. Tapez le nom voulu et les paramètres que vous avez configurés antérieurement.
5. Cliquez sur l'onglet **Entrées** et sélectionnez les entrées voulues.
6. Cliquez sur  pour enregistrer les paramètres.
7. Cliquez sur **Événements**.

8. Développez , développez **Entrée passerelle POS**, cliquez sur **Entrée de données**.
9. Dans la liste **Déclencher l'alarme**, sélectionnez **Toujours** afin que cet événement déclenche toujours une alarme. Si vous souhaitez que l'événement ne déclenche une alarme que pendant un certain laps de temps, sélectionnez une planification.

10. Cliquez sur  pour enregistrer les paramètres.
11. Cliquez sur **Alarmes**.
12. Configurez les paramètres voulus pour cet événement.
13. Cliquez sur  pour enregistrer les paramètres, puis sur  pour activer la configuration.
14. Procédez à un essai pour vous assurer que l'alarme fonctionne correctement.

12.2 Ajout d'une alarme d'entrée Bosch Allegiant

Après qu'un périphérique Bosch Allegiant est ajouté à BVMS, vous pouvez ajouter des entrées d'alarme.

1. Cliquez sur l'entrée du périphérique Allegiant dans l'Arborescence des Périphériques.
2. Cliquez sur l'onglet **Entrées** et cliquez sur **Ajouter entrée**.
3. Ajoutez les alarmes d'entrée voulues.
4. Cliquez sur **Événements**.
5. Dans l'Arborescence des Événements, développez **Périphériques Allegiant**, développez **Entrée Allegiant** et cliquez sur **Entrée fermée** ou **Entrée ouverte** (selon votre application).
6. Dans la liste **Déclencher l'alarme**, sélectionnez **Toujours** afin que cet événement déclenche toujours une alarme. Si vous souhaitez que l'événement ne déclenche une alarme que pendant un certain laps de temps, sélectionnez une planification.
7. Cliquez sur  pour enregistrer les paramètres, puis sur  pour activer la configuration.
8. Procédez à un essai pour vous assurer que l'alarme fonctionne correctement.

12.3 Ajout et configuration de 2 caméras IP Dinion avec enregistrement VRM

Cette section explique les marches à suivre pour ajouter 2 caméras IP Dinion pour l'enregistrement VRM, configurer des paramètres d'enregistrement différents et configurer la Recherche judiciaire pour ces caméras.

Prérequis :


Le VRM et les périphériques iSCSI sont correctement configurés.

Autrement dit :

- Le VRM a été ajouté à l'Arborescence des Périphériques.
- Un périphérique iSCSI comportant une cible et des LUNs configurés a été attribué à ce VRM.

Pour ajouter des caméras IP à un VRM existant :

Fenêtre principale > **Périphériques** > Développez 

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Ajouter encodeur**. La boîte de dialogue **Ajouter un encodeur** s'affiche.
2. Saisissez l'adresse IP de la caméra IP et sélectionnez le type d'encodeur (Dinion IP). Cliquez sur **OK**. Répétez cette étape pour l'autre caméra IP.

Pour ajouter les caméras IP à l'Arborescence Logique :

Fenêtre principale > **Cartes et structure**


- ▶ Faites glisser les caméras vers l'Arborescence Logique.

Pour modifier les propriétés d'une caméra :

Fenêtre principale > onglet **Caméras et enregistrement** >  >  tab

1. Dans la colonne **Vidéo en temps réel**, configurez la qualité d'affichage des images en temps réel. Pour ces périphériques, vous pouvez uniquement définir la qualité temps réel par caméra, et non par planification.
2. Effectuez les réglages appropriés dans les autres colonnes.

Pour configurer les paramètres d'enregistrement pour les caméras :

1. Cliquez sur .
2. Sélectionnez la gamme de périphériques correspondante.
3. Sélectionnez le paramètre d'enregistrement disponible correspondant.
4. Sélectionnez la planification d'enregistrement correspondante, par exemple **Jour**.
5. Sous **Enregistrement continu ou de pré-alarme**, sélectionnez le mode d'enregistrement, le flux et la qualité souhaités.
Si vous sélectionnez le mode d'enregistrement **Pré-alarme**, le paramètre **Durée** est disponible pour sélectionner la durée d'enregistrement d'alarme avant l'alarme, en secondes.
6. Sous **Enregistrement d'alarme**, dans la colonne **Durée**, cliquez sur une cellule et saisissez la durée d'enregistrement souhaitée après le déclenchement de l'alarme, en secondes.
7. Répétez les étapes précédentes pour configurer les paramètres d'enregistrement de l'autre gamme de caméras.

13 Fenêtres générales de Configuration Client



Remarque!

BVMS Viewer offre uniquement des fonctionnalités de base. Les fonctionnalités avancées sont incluses dans BVMS Professional. Pour de plus amples informations sur les différentes éditions BVMS, consultez le site www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).




Ce chapitre décrit certaines fenêtres standard de BVMSConfiguration Client.





13.1 Fenêtre de configuration

Fenêtre principale

Permet de configurer le système. Les boutons de la barre d'outils représentent les diverses pages à configurer pour que le système fonctionne. Leur séquence représente les actions recommandées pour effectuer la configuration.

- ▶ Cliquez sur un élément de l'arborescence pour afficher les pages de propriété disponibles.

Périphériques	Cliquez sur ce bouton pour afficher la page Périphériques répertoriant tous les dispositifs connectés au système.
Cartes et structure	Cliquez sur ce bouton pour afficher la page Cartes et structure comprenant l'Arborescence Logique, l'Arborescence des dispositifs et les cartes.
Planifications	Cliquez sur ce bouton pour afficher la page Planifications d'Enregistrement et Planifications de Tâches .
Caméras et enregistrement	Cliquez sur ce bouton pour afficher la page Caméras et enregistrement comportant le Tableau des caméras et les paramètres d'enregistrement de toutes les caméras.
Événements	Cliquez sur ce bouton pour afficher la page Événements .
Alarmes	Cliquez sur ce bouton pour afficher la page Alarmes .
Groupes d'utilisateurs	Cliquez sur ce bouton pour afficher la page Groupes d'utilisateurs répertoriant tous les utilisateurs.
	Cliquez sur ce bouton pour enregistrer les paramètres modifiés dans la fenêtre en cours d'utilisation.
	Cliquez sur ce bouton pour rétablir les paramètres enregistrés de la fenêtre en cours d'utilisation. Remarque : seuls les réglages effectués dans BVMS sont restaurés, et non ceux qui ont été effectués directement sur le périphérique. Cette situation risque de rendre les périphériques inaccessibles.
	Cliquez sur ce bouton pour afficher la boîte de dialogue Activer la configuration .

	Cliquez sur ce bouton pour supprimer l'élément sélectionné (non disponible sur toutes les pages).
	Cliquez sur ce bouton pour renommer l'élément sélectionné (non disponible sur toutes les pages).
	Cliquez sur ce bouton pour afficher de l'aide sur la fenêtre actuelle.
	Cliquez pour mettre à jour les informations d'état pour tous les périphériques et fonctions de périphérique si nécessaire (non disponible sur chaque page). Vous pouvez mettre à jour l'état d'un seul dispositif : cliquez avec le bouton droit de la souris sur le dispositif, puis cliquez sur Actualiser l'état . Remarque : Lorsque vous avez un vaste système comptant plusieurs milliers de périphériques configurés, le processus de mise à jour des états de périphériques et des fonctions des périphériques peut prendre un certain temps.

13.2

Commandes des menus

commandes du menu Système

Enregistrer les modifications	Enregistre toutes les modifications effectuées sur cette page.
Annuler toutes les modifications de la page	Rétablit les paramètres de cette page depuis le dernier enregistrement.
Gestionnaire d'activation...	Affiche la boîte de dialogue Gestionnaire d'activation .
Exporter la configuration...	Affiche la boîte de dialogue Exporter le fichier de configuration .
Importer la configuration...	Affiche la boîte de dialogue Importer le fichier de configuration .
Exporter les informations sur le périphérique pour OPC	Affiche une boîte de dialogue permettant de créer un fichier de configuration que vous pouvez importer dans un système de gestion tiers.
Quitter	Ferme le programme.

Commandes du menu Matériel

Recherche de périphérique initiale...	Affiche la boîte de dialogue Recherche de périphérique initiale .
Protéger les périphériques avec un mot de passe par défaut...	Affiche la boîte de dialogue Protéger les périphériques avec un mot de passe par défaut global .
Protéger les stockages iSCSI avec un mot de passe CHAP...	Affiche la boîte de dialogue Protéger les stockages iSCSI avec un mot de passe CHAP .

Changer les mots de passe du périphérique...	Affiche la boîte de dialogue Changer les mots de passe du périphérique.
Mettre à jour le firmware du périphérique...	Affiche la boîte de dialogue Mettre à jour le firmware du périphérique.
Changer l'IP du périphérique et les paramètres réseau...	Affiche la boîte de dialogue Changer les paramètres IP du périphérique et réseau.
Moniteur de périphériques...	Affiche la boîte de dialogue Moniteur de périphériques.

Commandes du menu Outils

Éditeur de Script de Commande...	Affiche la boîte de dialogue Éditeur de Script de Commande.
Gestionnaire de ressources...	Affiche la boîte de dialogue Gestionnaire de ressources.
Générateur de séquence...	Affiche la boîte de dialogue Générateur de séquence.
Gestionnaire de licences...	Affiche la boîte de dialogue Gestionnaire de licences.
Inspecteur de licences...	Affiche la boîte de dialogue Inspecteur de licences.

Commandes du menu Rapports

Planifications d'enregistrement...	Affiche la boîte de dialogue de rapport Planifications d'enregistrement.
Paramètres d'enregistrement planifié...	Affiche la boîte de dialogue de rapport Paramètres d'enregistrement planifié.
Planifications de tâches...	Affiche la boîte de dialogue de rapport Planifications de tâches.
Paramètres d'enregistrements et de caméras...	Affiche la boîte de dialogue de rapport Caméras et paramètres d'enregistrement.
Paramètres de qualité de flux...	Affiche la boîte de dialogue de rapport Paramètres de qualité du flux.
Paramètres d'événement...	Affiche la boîte de dialogue de rapport Paramètres de l'événement.
Paramètres d'événement composé...	Affiche la boîte de dialogue de rapport Paramètres d'événement combiné.
Paramètres d'alarme...	Affiche la boîte de dialogue de rapport Paramètres de l'alarme.
Utilisateurs configurés...	Affiche la boîte de dialogue de rapport Utilisateurs configurés.
Groupes d'utilisateurs et comptes...	Affiche la boîte de dialogue de rapport Groupes d'utilisateurs et comptes.

Autorisations de périphérique...	Affiche la boîte de dialogue de rapport Autorisations de périphérique .
Autorisations de fonctionnement...	Affiche la boîte de dialogue de rapport Autorisations d'exploitation .
Autorisations de configuration...	Affiche la boîte de dialogue de rapport Autorisations de configuration .
Autorisations du groupe d'utilisateurs...	Affiche la boîte de dialogue de rapport Autorisations du groupe d'utilisateurs .
Paramètres de sécurité...	Affiche la boîte de dialogue de rapport Paramètres de sécurité .
Périphériques ignorés...	Affiche la boîte de dialogue de rapport Périphériques ignorés .

Commandes des menus Paramètres

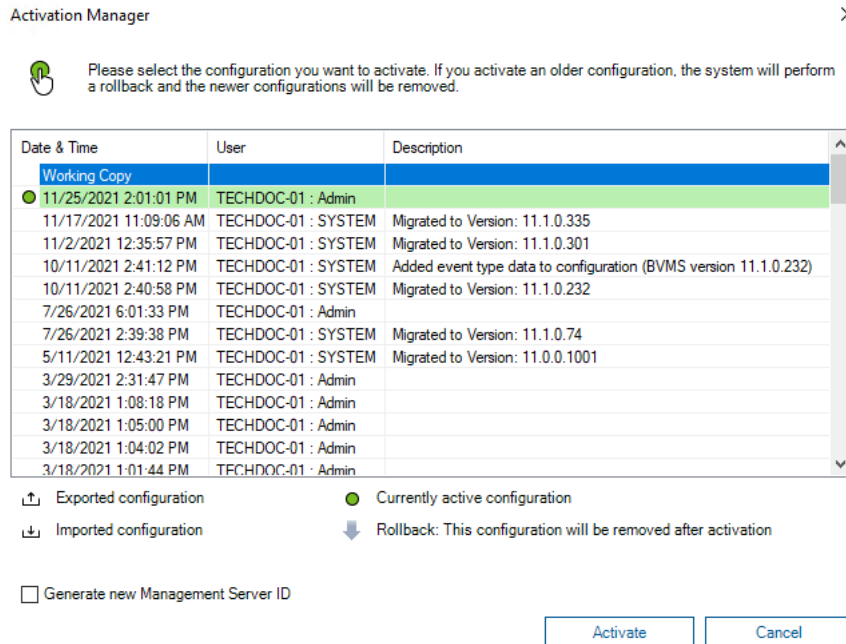
Paramètres d'alarme...	Affiche la boîte de dialogue Paramètres de l'alarme .
Paramètres SNMP...	Affiche la boîte de dialogue Paramètres SNMP .
Paramètres du serveur LDAP...	Affiche la boîte de dialogue Paramètres du serveur LDAP .
Définir l'ordre du groupe d'utilisateurs LDAP...	Affiche la boîte de dialogue Définir l'ordre du groupe d'utilisateurs LDAP...
Paramètres des certificats autorisés...	Affiche la boîte de dialogue Paramètres du jeton d'accès .
Définir les qualités d'enregistrement...	Affiche la boîte de dialogue Paramètres du certificat autorisé . Remarque : le menu Paramètres des certificats autorisés... n'est disponible que si vous lancez Configuration Client avec des autorisation d'admin et si l'utilisateur qui se connecte dispose de l'autorisation Configurer les groupes d'utilisateurs/comptes Enterprise Accounts .
Options	Affiche la boîte de dialogue Paramètres de qualité du flux .
Options	Affiche la boîte de dialogue Options .

Commandes du menu Aide

Afficher l'aide	Affiche l'aide en ligne de BVMS.
À propos de...	Affiche une boîte de dialogue contenant des informations sur le système installé, par exemple le numéro de version.

13.3 Boîte de dialogue Gestionnaire d'activation (menu Système)

Fenêtre principale > menu **Système** > commande **Gestionnaire d'activation...**
 Permet d'activer la configuration actuelle ou de rétablir la configuration précédente.



Activer
 Cliquez sur ce bouton pour afficher la boîte de dialogue **Activer la configuration**.

Se reporter à

- Activation de la configuration en cours d'utilisation, page 93
- Activation d'une configuration, page 94

13.4 Boîte de dialogue Activer la configuration (menu Système)



Fenêtre principale >
 Permet d'entrer la description de la copie en cours d'utilisation de la configuration à activer.

Définir l'heure d'activation retardée

Cliquez pour sélectionner une heure d'activation retardée.

Remarque : L'activation retardée n'est pas exécutée tant que l'utilisateur est connecté à Configuration Client.

Forcer l'activation pour tous les Operator Clients

Si cette option est activée, chaque poste de commande Operator Client est automatiquement redémarré pour activer la nouvelle configuration. L'utilisateur ne peut pas refuser la nouvelle configuration.

Si l'option n'est pas activée, une boîte de dialogue apparaît pendant quelques secondes sur chaque poste de commande Operator Client. L'utilisateur peut accepter ou refuser la nouvelle configuration. La boîte de dialogue se ferme au bout de quelques secondes si l'utilisateur n'intervient pas. Dans ce cas, la nouvelle configuration n'est pas acceptée.

Se reporter à

– *Activation de la configuration en cours d'utilisation, page 93*

13.5**Boîte de dialogue Recherche de dispositif initiale (menu Matériel)**

Fenêtre principale > menu **Matériel**, cliquez sur la commande **Recherche de périphérique initiale...**

Affiche les périphériques dont l'adresse IP est un doublon ou qui ont une adresse IP par défaut (192.168.0.1).

Vous permet de changer ces adresses IP et masques de sous-réseau.

Vous devez entrer le masque de sous-réseau approprié avant de pouvoir modifier une adresse IP.

13.6**Boîte de dialogue Protéger les dispositifs avec un mot de passe global par défaut (menu Matériel)**

Fenêtre principale > menu **Matériel** > commande **Protéger les périphériques avec un mot de passe par défaut...**

ou



Fenêtre principale >

Cette boîte de dialogue apparaît si une activation est en attente et si votre configuration contient des périphériques qui ne sont pas protégés par un mot de passe. Elle permet de saisir un mot de passe par défaut global qui est appliqué à tous les périphériques affectés.

Actualiser les états et les fonctions

Cliquez pour effectuer un nouveau balayage du réseau pour rechercher tous les périphériques non protégés par un mot de passe.

Global default password

Saisissez un mot de passe qui est utilisé pour tous les périphériques qui ne sont pas protégés actuellement.

Afficher les mots de passe

Cliquez sur ce bouton pour que tous les mots de passe de cette boîte de dialogue soient visibles.

Enforce password protection on activation

Cliquez sur cette case pour la cocher. Si cette option est activée, vous devez appliquer un mot de passe par défaut global pour les périphériques qui ne sont pas protégés par un mot de passe.

Appliquer

Cliquez sur ce bouton pour appliquer le mot de passe par défaut global.

La boîte de dialogue **Modification des mots de passe** s'affiche. Les changements de mots de passe sont répertoriés.

Cliquez sur **OK** pour fermer la boîte de dialogue.

Si vous avez commencé à activer votre configuration, la boîte de dialogue **Gestionnaire d'activation** s'affiche.

Se reporter à

– *Activation de la configuration en cours d'utilisation, page 93*

13.7

Boîte de dialogue Protéger les stockages iSCSI avec un mot de passe CHAP (menu Matériel)

Utilisez cette boîte de dialogue pour définir des mots de passe CHAP sur les dispositifs iSCSI et VRM . Le système transfère automatiquement ces mots de passe vers les comptes **Utilisateur** et **Destination** des encodeurs, décodeurs et dispositifs VSG.

Sur les dispositifs nouvellement ajoutés, les mots de passe sont définis automatiquement lorsque vous activez la configuration.

Remarque : La définition d'un mot de passe CHAP vide supprime le mot de passe CHAP sur les dispositifs iSCSI et VRM .



Remarque!

- Sur l'ensemble des DSA E-Series, le mot de passe CHAP est configuré automatiquement.
- Les périphériques VRM transfèrent le mot de passe CHAP aux encodeurs. Mais il vous faut définir le mot de passe CHAP sur le périphérique iSCSI correspondant pour assurer l'enregistrement.
- Sur tous les périphériques DIVAR IP, vous devez définir manuellement le mot de passe CHAP. Consultez le manuel DIVAR IP correspondant pour obtenir des instructions plus détaillées. Dans le cas contraire, l'enregistrement s'interrompt ou la lecture ne fonctionne pas.

Mot de passe CHAP global

Saisissez le mot de passe CHAP iSCSI requis pour vous authentifier sur le périphérique de stockage iSCSI et pour activer une lecture directe à partir du dispositif iSCSI.

Confirmer le mot de passe CHAP global

Confirmez le mot de passe CHAP iSCSI.

Afficher le mot de passe

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Appliquer

Cliquez sur ce bouton pour appliquer le mot de passe CHAP.

Remarque : Vérifiez le résultat de l'opération. Il se peut que vous deviez définir manuellement le mot de passe CHAP sur certains dispositifs iSCSI.

13.8

Boîte de dialogue de changement des mots de passe (Menu Matériel)

Fenêtre principale > **Périphériques** >  **Changer les mots de passe du périphérique** > **Changer les mots de passe du périphérique**

ou

Fenêtre principale > menu **Matériel** > commande **Changer les mots de passe du périphérique...** > boîte de dialogue **Changer les mots de passe du périphérique**



Cliquez pour actualiser les informations d'état pour tous les dispositifs. Vous pouvez actualiser l'état d'un seul dispositif : cliquez avec le bouton droit de la souris sur le dispositif, puis cliquez sur **Actualiser l'état**.

Remarque : lorsque vous avez un vaste système comptant plusieurs milliers de dispositifs configurés, le processus d'actualisation des états peut prendre un certain temps.



Cliquez pour sélectionner tous les dispositifs disponibles en une seule fois.

Afficher les mots de passe

Sélectionnez la case si vous souhaitez que les mots de passe configurés soient affichés sous une forme lisible.

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.

Remarque : Il est possible de rechercher également les mots de passe, uniquement si la case **Afficher les mots de passe** est sélectionnée,

Ce tableau vous permet de définir les propriétés suivantes des dispositifs IP disponibles :

- Mot de passe Service
- Mot de passe User
- Mot de passe Live
- Mot de passe Destination

Pour modifier le mot de passe des dispositifs IP :

1. Sélectionnez le dispositif requis.
2. Cliquez avec le bouton droit de la souris sur les dispositifs sélectionnés, puis cliquez sur **Modifier le mot de passe...**
La boîte de dialogue **Changer les mots de passe du périphérique** s'affiche.
3. Sélectionnez le type de mot de passe requis.
4. Saisissez le nouveau mot de passe.
5. Cliquez sur **OK**.
Le nouveau mot de passe est mis à jour sur le dispositif sélectionné.

Pour modifier les paramètres de plusieurs dispositifs :

Voir *Configuration de plusieurs encodeurs et décodeurs*, page 238.

13.9

Boîte de dialogue de mise à jour du firmware du dispositif (menu Matériel)

Fenêtre principale > menu **Matériel** > commande **Mettre à jour le firmware du périphérique...** > boîte de dialogue **Mettre à jour le firmware du périphérique**



Cliquez pour actualiser les informations d'état pour tous les dispositifs. Vous pouvez actualiser l'état d'un seul dispositif : cliquez avec le bouton droit de la souris sur le dispositif, puis cliquez sur **Actualiser l'état**.

Remarque : lorsque vous avez un vaste système comptant plusieurs milliers de dispositifs configurés, le processus d'actualisation des états peut prendre un certain temps.



Cliquez pour sélectionner tous les dispositifs disponibles en une seule fois.



Cliquez pour mettre à jour la version du firmware.

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.

Pour mettre à jour la version du firmware :

1. Sélectionnez le dispositif requis.
2. Cliquez sur **Mettre à jour le firmware**.
Une fenêtre d'informations Configuration Client s'affiche.
3. Cliquez sur **OK**.
L'Explorateur de fichiers s'ouvre.
4. Sélectionnez le fichier contenant la mise à jour.
5. Cliquez sur **Ouvrir**.
La fenêtre **État du chargement du firmware** s'ouvre.
6. Cliquez sur **Démarrer** pour lancer le téléchargement.
7. Cliquez sur **Fermer**.
Le firmware est mis à jour.

Pour modifier les paramètres de plusieurs dispositifs :

Voir *Configuration de plusieurs encodeurs et décodeurs*, page 238.

13.10

Boîte de dialogue de modification des paramètres IP et réseau de dispositif (menu Matériel)

Fenêtre principale > menu **Matériel** > commande **Changer l'IP du périphérique et les paramètres réseau...** > boîte de dialogue **Changer les paramètres IP du périphérique et réseau**



Cliquez pour actualiser les informations d'état pour tous les dispositifs. Vous pouvez actualiser l'état d'un seul dispositif : cliquez avec le bouton droit de la souris sur le dispositif, puis cliquez sur **Actualiser l'état**.

Remarque : lorsque vous avez un vaste système comptant plusieurs milliers de dispositifs configurés, le processus d'actualisation des états peut prendre un certain temps.



Cliquez pour sélectionner tous les dispositifs disponibles en une seule fois.

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.

Ce tableau vous permet de définir les propriétés suivantes des dispositifs IP disponibles :

- Nom affiché
- Adresse IP
- Masque de sous-réseau
- Adresse IP de la passerelle



Remarque!

Au lieu d'utiliser les commandes, vous pouvez saisir les paramètres appropriés dans le champ requis.

Pour définir le nom d'affichage des dispositifs IP :

1. Sélectionnez le dispositif requis.
2. Cliquez avec le bouton droit de la souris sur les dispositifs sélectionnés, puis cliquez sur **Définir les noms affichés...** La boîte de dialogue **Définir les noms affichés** s'affiche.
3. Saisissez la première chaîne dans le champ **Commencer par** .
4. Cliquez sur **Calculer**. Le champ **Terminer par** : affiche la dernière chaîne de la plage réservée aux dispositifs sélectionnés.
5. Cliquez sur **OK**.
6. Dans la boîte de dialogue **Changer les paramètres IP du périphérique et réseau**, cliquez sur **Appliquer**.
Le nom calculé est mis à jour sur le dispositif sélectionné.

Boîte de dialogue Définir les noms affichés

Commencer par :

Saisissez le premier nom.

Terminer par :

Affiche le dernier nom des périphériques sélectionnés dès que vous cliquez sur **Calculer**.

Calculer

Cliquez sur ce bouton pour calculer la plage des noms affichés pour les dispositifs sélectionnés.

Pour définir l'adresse IP des dispositifs IP :

1. Sélectionnez le dispositif requis.
2. Cliquez avec le bouton droit de la souris sur le dispositif sélectionné, puis cliquez sur **Définir les adresses IP...** La boîte de dialogue **Définir les adresses IP** s'affiche.
3. Saisissez la première adresse IP dans le champ **Commencer par :**
4. Cliquez sur **Calculer**. Le champ **Terminer par :** affiche la dernière adresse IP de la plage réservée au dispositif sélectionné.
5. Cliquez sur **OK**.
6. Dans la boîte de dialogue **Changer les paramètres IP du périphérique et réseau**, cliquez sur **Appliquer**.
La nouvelle adresse IP est mise à jour sur le dispositif sélectionné.

Boîte de dialogue Définir les adresses IP**Commencer par :**

Saisissez la première adresse IP.

Terminer par :

Affiche la dernière adresse IP pour les dispositifs sélectionnés dès que vous cliquez sur **Calculer**.

Calculer

Cliquez sur ce bouton pour calculer la plage d'adresses IP pour les dispositifs sélectionnés.

Pour définir le masque de sous-réseau/l'ID passerelle des dispositifs IP :

1. Cliquez dans le champ requis.
2. Saisissez la valeur appropriée.
3. Cliquez sur **Appliquer**.
La nouvelle valeur est mise à jour sur le dispositif sélectionné.

Appliquer

Cliquez sur ce bouton pour configurer les périphériques avec les valeurs entrées sans fermer la boîte de dialogue.

Pour modifier les paramètres de plusieurs dispositifs :

Voir *Configuration de plusieurs encodeurs et décodeurs*, page 238.

13.11

Boîte de dialogue Moniteur de dispositifs (menu Matériel)

Fenêtre principale > menu **Matériel** > commande **Moniteur de périphériques...** > boîte de dialogue **Moniteur de périphériques**

Permet de vérifier l'état des encodeurs/décodeurs de votre arborescence des périphériques qui sont actifs dans votre BVMS.

Afficher nom

Nom du périphérique qui a été configuré dans BVMS.

Adresse réseau

Adresse IP du périphérique.

État

Les états suivants peuvent être affichés :

- **Configuré** : La configuration de ce périphérique est activée.
- **Différence de configuration** : La configuration de ce périphérique n'est pas activée.
- **Inconnu** : Impossible de déterminer l'état.
- **Non connecté** : Non connecté.

Dernière vérification

Date et heure d'ouverture de la boîte de dialogue et d'exécution de la vérification. Tant que la boîte de dialogue est affichée, les périphériques ne sont pas revérifiés.

Se reporter à

- *Vérification de l'état de vos encodeurs/décodeurs, page 96*

13.12 Boîte de dialogue Éditeur de Script de Commande (menu Outils)

Pour plus d'informations, voir *Boîte de dialogue Éditeur de Script de Commande, page 319*.

Se reporter à

- *Boîte de dialogue Éditeur de Script de Commande, page 319*

13.13 Boîte de dialogue Gestionnaire de ressources (menu Outils)

Pour plus d'informations, voir *Boîte de dialogue Gestionnaire de ressources, page 271*.

Se reporter à

- *Boîte de dialogue Gestionnaire de ressources, page 271*

13.14 Boîte de dialogue Générateur de séquence (menu Outils)

Pour plus d'informations, voir *Boîte de dialogue Générateur de séquence, page 274*.

Se reporter à

- *Boîte de dialogue Générateur de séquence, page 274*

13.15 Boîte de dialogue Gestionnaire de licences (menu Outils)

Fenêtre principale > menu **Outils** > commande **Gestionnaire de licences...**

Permet de mettre sous licence le logiciel BVMS commandé et d'effectuer des mises à niveau en ajoutant de nouvelles fonctions.

État des licences

Affiche l'état d'activation de licence.

Empreinte digitale système

Au cas où une assistance s'avérerait nécessaire, nous vous recommandons de fournir le **Empreinte digitale système**.

Site d'installation

Lors de l'activation de votre licence de base dans Bosch Remote Portal, vous fournissez des informations sur le site d'installation de votre système. Ces informations s'affichent ici.

Remarque : Vous pouvez également fournir ces informations dans d'autres licences, mais seules les informations fournies dans la licence de base s'affichent ici.

Licences

1. Cliquez sur **Ajouter** pour ajouter vos licences.
La boîte de dialogue **Ajouter une licence** s'affiche.
2. Suivez les instructions dans la boîte de dialogue.

Licence effective

Affiche la licence de base que vous avez activée.

Caractéristiques

- ▶ Cliquez sur **Inspecteur de licences...**

La boîte de dialogue **Inspecteur de licences** s'affiche.

Affiche le nombre de fonctionnalités sous licence qui sont actuellement installées.

Vous pouvez vérifier si le nombre de licences BVMS installées excède le nombre de licences achetées.

Version BVMS installée

Affiche la version BVMS actuellement installée, par exemple 11.0.

Versions BVMS sous licence

Affiche toutes les versions BVMS qui sont incluses et prises en charge dans le fichier de licence fourni actuellement.

Par exemple : BVMS 11.0 et toutes versions BVMS 11.x mineures à venir.

Date d'activation

Affiche la date d'activation de votre version BVMS installée.

Date d'expiration

Affiche la date d'expiration de votre version BVMS installée. Une date d'expiration ne s'applique que lorsque vous installez une licence d'urgence ou une licence de démonstration de vente.

Software Maintenance Agreement

Date d'expiration

Si vous en avez acheté et activé un Software Maintenance Agreement, la date d'expiration s'affiche ici.

Se reporter à

- *Activation des licences des logiciels, page 75*
- *Ajouter la boîte de dialogue de licence, page 113*
- *Boîte de dialogue Inspecteur de licence (menu Outils), page 113*

13.15.1

Ajouter la boîte de dialogue de licence

Fenêtre principale > menu **Outils** > commande **Gestionnaire de licences...** > **Licences** >

Ajouter

Vous permet d'ajouter vos licences achetées ou licences de démonstration du site Web Bosch Remote Portal remote.boschsecurity.com à votre système BVMS.

Pour ajouter vos licences, suivez les instructions de la boîte de dialogue.

Pour plus d'informations, consultez le livre blanc relatif aux licences BVMS correspondant.

13.16

Boîte de dialogue Inspecteur de licence (menu Outils)

Fenêtre principale > menu **Outils**, cliquez sur la commande **Inspecteur de licences...** > boîte de dialogue **Inspecteur de licences**

Affiche le nombre de fonctionnalités sous licence qui sont actuellement installées.

Vous pouvez vérifier si le nombre de licences BVMS installées excède le nombre de licences achetées.

Remarque : Si la configuration actuelle du système dépasse les limites des licences actuellement installées, vous ne pouvez pas activer la configuration.

13.17 Boîte de dialogue Surveillance de la station de travail (menu Outils)

Fenêtre principale > menu **Outils** > commande **Surveillance des postes de travail...** > boîte de dialogue **Surveillance des postes de travail**

Affiche la liste de toutes les stations de travail actuellement connectées au Management Server BVMS.

Remarque : La liste affiche tous les clients Operator Clients et Cameo SDK connectés.

Pour déconnecter une station de travail :

1. Sélectionnez l'entrée correspondante dans la liste.
2. Cliquez sur **Déconnecter**.

Remarque : Cette fonction n'est active que si l'utilisateur dispose des droits correspondants.

3. Cliquez sur **Oui**.
Si la session de l'Operator Client correspondante s'est bien éteinte, l'entrée de liste est supprimée.

Remarque : Vous ne pouvez déconnecter que les stations de travail de l'Operator Client.

13.18 Boîtes de dialogue des rapports (menu Rapports)

Ce chapitre présente toutes les boîtes de dialogue qui sont disponibles pour les rapports de configuration.

Se reporter à

- *Création d'un rapport, page 97*

13.18.1 Boîte de dialogue Planifications d'Enregistrement

Fenêtre principale > menu **Rapports** > commande **Planifications d'enregistrement...**

Répertorie les planifications d'enregistrement configurées.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

13.18.2 Boîte de dialogue Paramètres d'enregistrement planifié

Fenêtre principale > menu **Rapports** > commande **Paramètres d'enregistrement planifié...**

Répertorie les paramètres d'enregistrement planifié configurés.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

13.18.3 Boîte de dialogue Planifications de Tâches

Fenêtre principale > menu **Rapports** > commande **Planifications de tâches...**

Répertorie les planifications de tâches configurées.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

- 13.18.4 Boîte de dialogue des paramètres de caméra et d'enregistrement**
Fenêtre principale > menu **Rapports** > commande **Paramètres d'enregistrements et de caméras...**
Répertorie les paramètres d'enregistrement qui sont configurés dans le tableau des caméras et le tableau des enregistrements.
- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.
- 13.18.5 Boîte de dialogue Paramètres de qualité du flux**
Fenêtre principale > menu **Rapports** > commande **Paramètres de qualité de flux...**
Répertorie les paramètres de qualité du flux configurés de toutes les caméras.
- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.
- 13.18.6 Boîte de dialogue des paramètres d'événement**
Fenêtre principale > menu **Rapports** > commande **Paramètres d'événement composé...**
Répertorie les événements pour lesquels une planification pour le déclenchement d'une alarme est configurée.
- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.
- 13.18.7 Boîte de dialogue des paramètres d'événements combinés**
Fenêtre principale > menu **Rapports** > commande **Paramètres d'événement composé...**
Répertorie tous les événements combinés.
- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.
- 13.18.8 Boîte de dialogue Paramètres d'alarme**
Fenêtre principale > menu **Rapports** > commande **Paramètres d'alarme...**
Répertorie tous les paramètres des alarmes configurées, y compris les paramètres de la boîte de dialogue **Options d'alarmes**.
- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.
- 13.18.9 Boîte de dialogue des utilisateurs configurés**
Fenêtre principale > menu **Rapports** > commande **Utilisateurs configurés...**
Répertorie les utilisateurs qui sont autorisés à se connecter à Operator Client.
- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.
- 13.18.10 Boîte de dialogue Groupes d'utilisateurs et Comptes**
Fenêtre principale > menu **Rapports** > commande **Groupes d'utilisateurs et comptes...**
Répertorie les groupes d'utilisateurs Enterprise Accounts, Enterprise User Groups configurés et les groupes de double autorisation.
- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.
- 13.18.11 Boîte de dialogue Autorisations de périphérique**
Fenêtre principale > menu **Rapports** > commande **Autorisations de périphérique...**
Répertorie les autorisations relatives à l'utilisation des dispositifs configurés pour chaque groupe d'utilisateurs.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

13.18.12 **Boîte de dialogue Autorisations d'exploitation**

Fenêtre principale > menu **Rapports** > commande **Autorisations de fonctionnement...**

Répertorie les autorisations relatives à l'utilisation d'Operator Client pour chaque groupe d'utilisateurs.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

13.18.13 **Boîte de dialogue Autorisations de configuration**

Fenêtre principale > menu **Rapports** > commande **Autorisations de configuration...**

Répertorie les autorisations relatives à l'utilisation d'Configuration Client pour chaque groupe d'utilisateurs.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

13.18.14 **Boîte de dialogue Autorisations d'un groupe d'utilisateurs**

Fenêtre principale > menu **Rapports** > commande **Autorisations du groupe d'utilisateurs...**

Répertorie les autorisations relatives à la configuration de groupes d'utilisateurs pour chaque groupe d'utilisateurs.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

13.18.15 **Boîte de dialogue Paramètres de sécurité**

Fenêtre principale > menu **Rapports** > commande **Paramètres de sécurité...**

Affiche la liste des paramètres de sécurité configurés pour chaque groupe d'utilisateurs et Enterprise User Groups.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

13.18.16 **Boîte de dialogue Autorisations d'application**

Fenêtre principale > menu **Rapports** > commande **Autorisations de l'application...**

Liste tous les groupes d'utilisateurs et les autorisations d'application.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

13.18.17 **Boîte de dialogue Dispositifs exclus**

Fenêtre principale > menu **Rapports** > commande **Périphériques ignorés...**

Répertorie tous les dispositifs configurés et les dispositifs qui sont exclus.

- ▶ Cliquez sur **Exporter en CSV** pour enregistrer toutes les informations de cette boîte de dialogue dans un fichier CSV.

13.19 **Boîte de dialogue Paramètres de l'alarme (menu Paramètres)**

Voir *Boîte de dialogue Paramètres d'alarme*, page 323 pour plus d'informations.

13.20 **Boîte de dialogue Paramètres SNMP (menu Paramètres)**

Fenêtre principale > menu **Paramètres** > commande **Paramètres SNMP...**

Permet de configurer la surveillance SNMP sur votre ordinateur Management Server. Vous spécifiez pour quel événement une interruption SNMP est envoyée, certaines informations supplémentaires sur votre système, ainsi que les adresses IP des ordinateurs prévus pour recevoir des interruptions SNMP de BVMS.

Le serveur envoie des interruptions SNMP quand des événements se produisent. Vous pouvez recevoir ces interruptions avec le récepteur SNMP disponible dans le Configuration Client à l'aide de l'outil **Journal trap SNMP**. Vous pouvez également utiliser un autre logiciel pouvant recevoir des interruptions SNMP.

L'agent SNMP de BVMS prend en charge les GetRequest SNMP. Lorsqu'un logiciel de gestion SNMP (par exemple iReasoning MIB Browser) envoie un GetRequest SNMP au Management Server BVMS, le Management Server envoie un message de réponse correspondant.

Le fichier MIB se trouve à l'emplacement suivant :

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

Seuls SNMPv1 et SNMPv2 sont pris en charge.

Remarque : SNMPv1 et SNMPv2 ne sont pas totalement compatibles. Par conséquent, il est recommandé de ne pas utiliser SNMPv1 et SNMPv2 ensemble.

Port GET SNMP

Saisissez le numéro du port pour le GetRequest SNMP. Il s'agit du numéro du port où l'agent SNMP du Management Server BVMS écoute les GetRequest SNMP.

Remarque : BVMS n'utilise pas le numéro de port standard 161 pour les GetRequest SNMP, car ce port peut être utilisé par l'agent SNMP de l'ordinateur sur lequel le Management Server BVMS est installé.

La valeur par défaut est 12544.

Contact système

Saisissez les données de contacts de votre système BVMS. Vous pouvez récupérer ces informations à l'aide d'un GetRequest SNMP en utilisant l'OID .1.3.6.1.2.1.1.4.

Description du système

Saisissez une description de votre BVMS. Vous pouvez récupérer ces informations à l'aide d'un GetRequest SNMP en utilisant l'OID .1.3.6.1.2.1.1.5.

Emplacement du système

Saisissez l'emplacement de votre BVMS. Cette chaîne doit spécifier l'emplacement physique de l'ordinateur serveur, par exemple le bâtiment, le numéro de salle, le numéro de rack, etc. Vous pouvez récupérer ces informations à l'aide d'un GetRequest SNMP en utilisant l'OID .1.3.6.1.2.1.1.6.

Récepteurs trap

Saisissez l'adresse IP de l'ordinateur auquel BVMS est censé envoyer les interruptions SNMP.

Filtre trap

Cliquez sur ce bouton pour sélectionner les événements dans l'arborescence des événements et filtrer les traps SNMP envoyés.

Se reporter à

– *Configuration de la surveillance SNMP, page 96*

13.21

Boîte de dialogue Paramètres du serveur LDAP (menu Paramètres)

Fenêtre principale > menu **Paramètres** > commande **Paramètres du serveur LDAP...**

Vous pouvez saisir les paramètres du serveur LDAP configurés hors de BVMS. Vous aurez besoin du concours de l'administrateur qui a configuré le serveur LDAP pour les entrées suivantes.

Tous les champs sont obligatoires, sauf les champs situés dans la zone de groupe **Tester l'utilisateur / le groupe d'utilisateurs**.

Paramètres du serveur LDAP

Serveur LDAP

Saisissez le nom ou l'adresse IP du serveur LDAP.

Port

Saisissez le numéro de port du serveur LDAP (HTTP par défaut : 389, HTTPS : 636)

Connexion sécurisée

Cochez cette case pour activer la transmission de données sécurisée.

Mécanisme d'authentification

La négociation sélectionne automatiquement le protocole d'authentification approprié. Elle transmet simplement les identifiants de connexion non chiffrés en texte clair.

Authentification proxy

Anonyme

Permet de se connecter en tant qu'invité. Sélectionnez cette option si le serveur LDAP la prend en charge et si vous ne pouvez pas configurer d'utilisateur proxy spécifique.

Utilisez les identifiants suivants

Nom d'utilisateur

Saisissez le nom unique de l'utilisateur proxy. Cet utilisateur est nécessaire pour permettre aux membres de ce groupe d'utilisateurs BVMS d'accéder au serveur LDAP.

Mot de passe

Saisissez le mot de passe de l'utilisateur proxy.

Test

Cliquez sur ce bouton pour tester l'accès de l'utilisateur proxy au serveur LDAP.

Base LDAP d'utilisateur

Saisissez le nom unique (DN = nom distinct) du chemin LDAP dans lequel vous pouvez rechercher un utilisateur.

Exemple de DN de la base LDAP : CN=Users,DC=Security,DC=MyCompany,DC=com

Filtre d'utilisateur

Sélectionnez un filtre pour la recherche d'un nom d'utilisateur unique. Des exemples sont prédéfinis. Remplacez-le %username% par le nom d'utilisateur réel.

Base LDAP de groupe

Saisissez le nom unique du chemin LDAP dans lequel vous pouvez rechercher des groupes. Exemple de DN de la base LDAP : CN=Users,DC=Security,DC=MyCompany,DC=com

Filtre de recherche d'un membre de groupe

Sélectionnez un filtre pour la recherche d'un membre de groupe.

Des exemples sont prédéfinis. Remplacez %usernameDN% par le nom d'utilisateur et son DN réels.

Filtre de recherche de groupe

Ne laissez pas ce champ vide. Sans entrée, vous ne pouvez pas affecter un groupe LDAP à un groupe d'utilisateurs BVMS.

Sélectionnez un filtre pour la recherche d'un groupe d'utilisateurs.

Des exemples sont prédéfinis.

Tester l'utilisateur / le groupe d'utilisateurs

Les entrées de cette zone de groupe ne sont pas enregistrées lorsque vous cliquez sur **OK**. Elles servent uniquement au test.

Nom d'utilisateur

Saisissez le nom d'un utilisateur test. Ne renseignez pas le DN.

Mot de passe

Saisissez le mot de passe de l'utilisateur test.

Tester l'utilisateur

Cliquez sur ce bouton pour vérifier si l'association du nom d'utilisateur et du mot de passe est exacte.

Groupe (DN)

Saisissez le nom de groupe unique auquel est associé l'utilisateur.

Tester le groupe

Cliquez sur ce bouton pour tester l'association de l'utilisateur au groupe.

Se reporter à

- *Sélectionner un groupe LDAP associé, page 371*

13.21.1

Association d'un groupe LDAP

Vous associez un groupe LDAP à un groupe d'utilisateurs BVMS pour donner aux utilisateurs de ce groupe LDAP l'accès à Operator Client. Les utilisateurs du groupe LDAP héritent des droits d'accès du groupe d'utilisateurs où vous configurez le groupe LDAP.

L'aide de l'administrateur informatique responsable du serveur LDAP vous sera probablement nécessaire.

Vous pouvez configurer les groupes LDAP dans les groupes d'utilisateurs standard ou les Enterprise User Groups.



Remarque!

Si un groupe LDAP est associé à un groupe d'utilisateurs BVMS, les utilisateurs de ce groupe peuvent démarrer Operator Client à l'aide d'une connexion unique.



Remarque!

Un utilisateur LDAP peut être associé à plusieurs groupes d'utilisateurs LDAP, eux-mêmes associés à un groupe d'utilisateurs BVMS particulier.

L'utilisateur LDAP obtient les autorisations du groupe d'utilisateurs BVMS est commandé au-dessus des autres groupes d'utilisateurs LDAP associés à cet utilisateur LDAP.

Pour associer un groupe LDAP :

1. Cliquez sur **Paramètres du serveur LDAP...**

La boîte de dialogue **Paramètres du serveur LDAP** s'affiche.

2. Saisissez les paramètres de votre serveur LDAP, puis cliquez sur **OK**.

Pour de plus amples informations sur les différents champs, cliquez ci-dessous sur le lien de la fenêtre concernée.

Se reporter à

- *Boîte de dialogue Paramètres du serveur LDAP (menu Paramètres), page 117*
- *Page Propriétés du groupe d'utilisateurs, page 343*

13.22 Boîte de dialogue Définir un groupe d'utilisateurs LDAP (menu Paramètres)

Affiche la liste **Changer l'ordre du groupe d'utilisateurs LDAP**. La liste répertorie les groupes d'utilisateurs LDAP avec les groupes d'utilisateurs BVMS associés et les Enterprise User Groups. Il est possible de modifier l'ordre des groupes par glisser-déposer ou à l'aide des touches fléchées haut et bas.

Remarque!



Un utilisateur LDAP peut être associé à plusieurs groupes d'utilisateurs LDAP, eux-mêmes associés à un groupe d'utilisateurs BVMS particulier.

L'utilisateur LDAP obtient les autorisations du groupe d'utilisateurs BVMS est commandé au-dessus des autres groupes d'utilisateurs LDAP associés à cet utilisateur LDAP.

13.23 Boîte de dialogue Access token settings (Paramètres de jeton d'accès) (menu Paramètres)

Fenêtre principale > menu **Paramètres** > commande **Paramètres du jeton d'accès...**

Si vous avez configuré la connexion au Management Server à l'aide d'un jeton d'accès, vous devez d'abord définir les paramètres du jeton.

Un jeton est créé par le Enterprise Management Server et doit être signé par un certificat à partir d'un magasin de certificats sur l'ordinateur local. Pour savoir quel certificat utiliser, vous devez identifier le certificat.

Remarque : BVMS ne prend pas en charge les certificats qui utilisent un algorithme de hachage sécurisé SHA-1 et dont la clé est d'une longueur inférieure à 2 048 bits.

Propriétés du certificat de signature

Saisissez une chaîne de propriétés pour identifier le certificat correspondant.

Remarque : si plusieurs certificats correspondent aux critères, le certificat valide le plus récent est utilisé.

Respectez les règles suivantes pour saisir une chaîne de propriétés valide dans le champ

Propriétés du certificat de signature :

- La chaîne se compose d'une ou de plusieurs conditions.
- Les conditions sont séparées par des points-virgules (;).
- Les conditions sont des paires de noms de propriétés de certificats et de valeurs attendues, séparées par un signe égale (=).
- Les noms des propriétés de certificats peuvent être constitués d'une ou de plusieurs parties séparées par une virgule (,).
- Les noms des propriétés et les valeurs attendues ne sont pas sensibles à la casse.

Exemples :

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

- La partie Nom commun (CN) du nom de l'objet du certificat doit être égale au BVMS Token Issuer.
- En outre, la partie Nom commun du nom de l'objet du parent du certificat doit être égale à BVMS Intermediate. Le parent est le certificat qui a été utilisé pour signer le certificat en cours.

```
Parent.Thumbprint=A95FF7C6EC374127174D3AFA8EA67C94E8E66C3F
```


- L'empreinte du certificat parent du certificat doit être telle que spécifiée.

Liste des noms de propriétés de certificats pris en charge :

Nom	Type de retour
Empreinte	Chaîne
SerialNumber	Chaîne
SubjectName	Nom distinctif de l'objet
IssuerName	Nom distinctif de l'émetteur
Parent	Certificat utilisé pour signer le certificat en cours (autorité de certification émettrice)

Liste des noms de propriétés pris en charge pour le nom distinctif :

Nom	Type de retour
CN	Chaîne : nom commun
OU	Chaîne : nom de l'unité organisationnelle
O	Chaîne : nom de l'organisation
L	Chaîne : nom de la localité
S	Chaîne : nom de l'État ou de la province
C	Chaîne : nom du pays

Exemples d'utilisation des noms distinctifs :

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

Chaîne de certificat

Cochez la case pour inclure la chaîne de certificats.

Remarque : si exactement le même certificat est installé sur le Management Server, vous n'avez pas nécessairement besoin d'inclure la chaîne de certificats.

Nombre de certificats inclus

Indiquez le nombre exact de certificats inclus dans le jeton d'accès.

Remarque : vous ne devez pas inclure le certificat Root.

Durée de vie du jeton d'accès

Saisissez une durée en heures afin de définir pendant combien de temps les jetons restent valides après leur création par le Enterprise Management Server.

Se reporter à

- *Authentification basée sur les jetons, page 88*

13.24

Boîte de dialogue Trusted certificate settings (Paramètres du certificat approuvé) (menu Paramètres)

Fenêtre principale > menu **Paramètres** > commande **Paramètres des certificats autorisés...**

Cette boîte de dialogue vous permet de présenter l'empreinte du certificat qui est utilisé par le Management Server afin d'authentifier le jeton d'accès.

Remarque : Le menu **Paramètres des certificats autorisés...** n'est disponible que si vous démarrez le Configuration Client avec des autorisations d'admin et si l'utilisateur qui se connecte dispose de l'autorisation **Configurer les groupes d'utilisateurs/comptes Enterprise Accounts**.

Empreinte digitale du certificat autorisé

Affiche une empreinte déjà configurée ou une empreinte vide si aucune configuration n'est trouvée dans le registre. Saisissez ou modifiez l'empreinte du certificat root.

L'empreinte fournie est écrite dans le chemin d'accès

HKEY_LOCAL_MACHINE\SOFTWARE\Bosch Sicherheitssysteme GmbH\Bosch Video Management System\TrustedCertificates de la clé « BvmsTrustedCertificate ».

Remarque : l'empreinte n'est pas incluse lors de l'exportation de la configuration.

Remarque : BVMS ne prend pas en charge les certificats qui utilisent un algorithme de hachage sécurisé SHA-1 et dont la clé est d'une longueur inférieure à 2 048 bits.

13.25

Boîte de dialogue Options (menu Paramètres)

Remarque : Certaines fonctionnalités nécessitent l'achat de la licence respective.

Fenêtre principale > menu **Paramètres** > commande **Options**

Configuration Client

Langue

Vous permet de configurer la langue de votre Configuration Client. Si vous sélectionnez

Langue système, la langue de votre installation Windows est utilisée.

Ce paramètre est activé après le redémarrage de Configuration Client.

Déconnexion automatique

Vous permet de configurer la déconnexion automatique de Configuration Client.

Configuration Client se déconnecte à l'issue de la période configurée.

Les modifications apportées aux pages de configuration des dispositifs suivants dans la page **Périphériques** ne sont pas enregistrées automatiquement et sont perdues lorsqu'une déconnexion en cas d'inactivité se produit :

- Encodeurs
- Décodeurs
- Dispositifs VRM
- Dispositifs iSCSI
- Dispositifs VSG

Toutes les autres modifications de configuration en attente sont enregistrées automatiquement.

Remarque : Les modifications que vous n'avez pas confirmées en cliquant sur **OK** dans les boîtes de dialogue ne sont pas enregistrées.

Scan options

Vous permet de configurer s'il est possible de rechercher les dispositifs dans le sous-réseau correspondant ou dans tous les sous-réseaux.

Operator Client

Connexions multiples

Autoriser les connexions simultanées avec le même utilisateur

Vous pouvez configurer qu'un utilisateur du client Web BVMS SDK, BVMS, de l'application mobile BVMS, ou de Operator Client peut exécuter plusieurs connexions synchrones avec le même nom d'utilisateur.

Paramètres du serveur

Chaîne de connexion à la base de données

Vous permet de configurer la chaîne de connexion de la base de données du journal des connexions.



Remarque!

Ne modifiez cette chaîne que lorsque vous souhaitez configurer un serveur SQL distant pour le Journal des Connexions et uniquement si vous maîtrisez la technologie des serveurs SQL.

Période de rétention

Vous permet de définir une durée de conservation maximale des entrées dans le journal des connexions. Une fois cette durée de conservation définie, les entrées sont automatiquement supprimées.

Ce paramètre est activé après l'activation de la configuration.

Vous devez disposer d'une autorisation pour modifier les paramètres suivants :

Paramètres Audit Trail

Audit Trail

Activer ou désactiver la fonction Audit Trail.

Remarque : La page Audit Trail est disponible uniquement dans Configuration Client lorsque la fonction est activée.

Durée de rétention maximale

Vous permet de définir une durée de conservation maximale des entrées dans la Audit Trail. Une fois cette durée de conservation définie, les entrées sont automatiquement supprimées.

Langue

Sélectionnez la langue de la Audit Trail.

Exception : Toutes les entrées de la Audit Trail de la catégorie de filtre **Dispositifs (Configuration de la caméra)** s'afficheront dans la langue configurée de Configuration Client.

Remarque : Assurez-vous d'installer la base de données Audit Trail en la sélectionnant dans la configuration BVMS (fonction de configuration en option).

Les paramètres de la Audit Trail sont activés uniquement après l'activation de la configuration.

Périphériques

Groupe de moniteurs

Permet de définir une configuration de telle sorte que les utilisateurs puissent contrôler tous les groupes de moniteurs avec chaque ordinateur client BVMS. Il n'est alors pas obligatoire de configurer les ordinateurs comme postes de commande dans l'arborescence des dispositifs.

Sélection de flux du décodeur

Permet de configurer l'utilisation d'un flux compatible, et pas nécessairement du flux en temps réel, par tous les décodeurs du système.

Ce paramètre est activé après l'activation de la configuration.

Serveur horaire pour encodeur

Vous permet de configurer les paramètres du serveur de temps pour les encodeurs. Par défaut, l'adresse IP du serveur central est utilisée.

Fonctionnalités système

Cartes

Type d'arrière-plan

Vous permet de sélectionner le type de carte d'arrière-plan pour la carte globale. Les types de cartes suivants sont disponibles si vous avez accès à Internet (mode en ligne) :

- **Plan des rues HERE**
- **Plan des rues sombre HERE**
- **Carte satellite HERE**

Si vous n'avez pas accès à Internet (mode hors ligne), sélectionnez **Aucun**.

Clé API spécifique au client

Entrez votre clé API pour l'utilisation des cartes en ligne Here).

Afficher la clé d'API

Sélectionnez la case à cocher pour afficher la clé API.



Remarque!

Si vous passez le type de carte d'arrière-plan du mode en ligne (cartes Here) au mode hors ligne (**Aucun**) ou l'inverse, vous perdez toutes les zones réactives de la caméra positionnés et les zones de visualisation de carte.

Vous ne pouvez définir qu'un seul arrière-plan pour la carte globale. Cet arrière-plan s'applique à toutes les zones de visualisation de la carte.

Map-based tracking assistant

Activer la fonction système

Vous permet de configurer qu'un utilisateur d'Operator Client peut utiliser le Map-based tracking assistant.

Affichage avancé des états

Désactiver la coloration des points chauds dans les cartes

Vous permet de configurer la désactivation des zones réactives clignotantes dans les cartes.

Affichage d'état avancé activé (coloration des points chauds sur les cartes en fonction de l'état)

Vous pouvez configurer pour tous les états d'événement que les zones actives des dispositifs appartenant à cet événement s'affichent avec une couleur d'arrière-plan et clignotent lorsque l'événement configuré se produit.

Activer l'affichage avancé des alarmes (coloration des points chauds sur les cartes en fonction de l'alarme)

Vous permet de configurer pour toutes les alarmes que les zones actives des dispositifs appartenant à cette alarme s'affichent avec une couleur d'arrière-plan et clignotent lorsque l'alarme configurée se produit.

La configuration de l'affichage d'état avancé est possible une fois que vous avez enregistré la configuration. Les zones réactives s'affichent sur une carte dans Operator Client après que vous avez activé la configuration.

Exporter avec Privacy overlay**Activer la fonction système**

Vous permet de configurer qu'un utilisateur d'Operator Client peut exporter une vidéo avec Privacy overlay.

Fournisseur d'identité**Fournisseur d'identité**

Sélectionnez votre fournisseur d'identité (IDP). Une fois la sélection effectuée, d'autres options s'affichent.

ID locataire (pour Microsoft IDP)

Fournissez les informations demandées en fonction de votre fournisseur d'identité externe.

URL de l'émetteur (pour IDP Amazon Federation)

Fournissez les informations demandées en fonction de votre fournisseur d'identité externe.

ID application

Fournissez les informations demandées en fonction de votre fournisseur d'identité externe.

Secret d'application

Remplissez ce champ si vous souhaitez utiliser une chaîne confidentielle pour identifier votre connexion au service de fournisseur d'identité externe.

Ce champ est facultatif.

Adresse externe

Si nécessaire, indiquez dans ce champ une adresse réseau externe pour une connexion acheminée vers BVMS Management Server, par exemple une connexion SSH utilisant une IP externe.

Ce champ est facultatif.

Cliquez sur **Enregistrer les modifications**.

14 Page Périphériques

Fenêtre principale > **Périphériques**



Remarque!

BVMS Viewer ne prend pas en charge les décodeurs.

Affiche l'Arborescence des Périphériques et les pages de configuration.

Le nombre d'éléments au-dessous d'une entrée est affiché entre crochets.

Permet de configurer les périphériques disponibles, tels que les services de vidéo mobile, les encodeurs ONVIF, les périphériques Bosch Video Streaming Gateway, les encodeurs, des décodeurs, les VRM, les encodeurs de stockage locaux, les matrices analogiques ou les périphériques tels que la ATM/POS Bridge.

Remarque :

Les dispositifs sont présentés sous forme d'arborescence et regroupés par structure de réseau physique et par catégories de dispositifs.

Les sources vidéo telles que les encodeurs se trouvent sous les VRM.

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.

- ▶ Cliquez sur un élément de l'arborescence pour afficher la page correspondante.

14.1 Mise à jour de l'état et des fonctions et des périphériques

Fenêtre principale > **Périphériques**

Par exemple, après une mise à jour du firmware, il peut être nécessaire de synchroniser les fonctions de tous les décodeurs, encodeurs et passerelles de diffusion de flux vidéo (VSG) configurés. Avec cette fonctionnalité, les fonctions de chaque périphérique sont comparées aux fonctions déjà stockées au sein de BVMS. Vous pouvez mettre à jour les fonctions de tous les périphériques dans l'arborescence de périphériques en une seule opération.

Il est également possible de copier dans le presse-papiers une liste des périphériques dont les fonctions ont été modifiées. Vous pouvez ensuite coller la liste, par exemple, dans un éditeur de texte pour examiner les modifications en détail.

La liste des périphériques du presse-papiers est présentée dans un format CSV et elle contient les informations suivantes :

- Dispositif
- Type de dispositif
- Adresse IP


Remarque : Lorsque vous avez un vaste système comptant plusieurs milliers de périphériques configurés, le processus d'actualisation des états de périphériques et mise à jour des fonctions des périphériques peut prendre un certain temps.



Remarque!

Les fonctions ne sont extraites que pour les périphériques accessibles. Pour voir, si un périphérique n'est pas accessible, vous devez vérifier l'état de ce périphérique.

Pour mettre à jour les états et les fonctions des périphériques :

1. Cliquez sur .
La boîte de dialogue **Mettre à jour les fonctions du périphérique** s'affiche. Les informations d'état de tous les périphériques sont mises à jour et les fonctions des périphériques sont extraites.
Ce n'est possible que si les fonctions des périphériques ne sont pas à jour, si les périphériques appropriés sont affichés dans une liste et si le bouton **Mise à jour** est activé.
2. Le cas échéant, cliquez sur **Copier la liste de périphériques dans le Presse-papiers**.
3. Cliquez sur **Mise à jour**.
4. Cliquez sur **OK**.
⇒ Les fonctions des périphériques sont maintenant à jour.



Remarque!

Les informations d'état de tous les périphériques seront toujours mises à jour, même si vous annulez la boîte de dialogue **Mise à jour des fonctions du périphérique**.

14.2

Modification du mot de passe des périphériques IP

Fenêtre principale > **Périphériques** >  **Changer les mots de passe du périphérique** > **Changer les mots de passe du périphérique**

ou

Fenêtre principale > menu **Matériel** > commande **Changer les mots de passe du périphérique...** > boîte de dialogue **Changer les mots de passe du périphérique**

Pour modifier le mot de passe des dispositifs IP :

1. Sélectionnez le dispositif requis.
2. Cliquez avec le bouton droit de la souris sur les dispositifs sélectionnés, puis cliquez sur **Modifier le mot de passe...**

La boîte de dialogue **Changer les mots de passe du périphérique** s'affiche.

3. Sélectionnez le type de mot de passe requis.
4. Saisissez le nouveau mot de passe.
5. Cliquez sur **OK**.

Le nouveau mot de passe est mis à jour sur le dispositif sélectionné.

Pour plus d'informations, voir *Boîte de dialogue de changement des mots de passe (Menu Matériel)*, page 107.

Pour modifier les paramètres de plusieurs dispositifs :

Voir *Configuration de plusieurs encodeurs et décodeurs*, page 238.

Se reporter à

- *Boîte de dialogue de changement des mots de passe (Menu Matériel)*, page 107

14.3

Ajout d'un dispositif

Fenêtre principale > **Périphériques**

Vous pouvez ajouter manuellement les dispositifs suivants à l'arborescence des dispositifs, ce qui signifie que vous devez connaître l'adresse réseau du dispositif à ajouter :

- Dispositifs vidéo IP de Bosch
- Matrice analogique
Pour ajouter un dispositif Bosch Allegiant, vous avez besoin d'un fichier de configuration Allegiant valide.
- Poste de commande BVMS
Les postes de commande doivent être équipés du logiciel Operator Client.
- Dispositif de communication
- ATM/POS Bridge Bosch, dispositif DTP
- Entrée virtuelle
- Dispositif de surveillance réseau
- Bosch IntuiKey
- KBD-Universal XF
- Groupe de moniteurs
- Module d'E/S
- Émulation CCL Allegiant
- Centrale d'intrusion de Bosch
- Dispositif d'analyse basée sur le serveur
- Systèmes de contrôle d'accès de Bosch

Vous pouvez rechercher les périphériques suivants pour les ajouter à l'aide de la boîte de dialogue **BVMS Scan Wizard** :

- Dispositifs VRM
- Encodeurs
- Encodeurs temps réel uniquement
- Encodeurs ONVIF en temps réel uniquement
- Encodeurs pour stockage local
- Décodeurs
- Dispositifs Video Streaming Gateway (VSG)
- Dispositifs DVR



**Remarque!**

Après l'ajout d'un périphérique, cliquez sur  pour enregistrer les paramètres.


**Remarque!**

Ajoutez l'enregistreur DVR en utilisant le compte administrateur du périphérique. Si vous utilisez un compte utilisateur DVR avec des droits restreints, certaines fonctions peuvent ne pas être utilisables dans BVMS, par exemple l'utilisation de la commande d'une caméra PTZ.


Boîte de dialogue BVMS Scan Wizard

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Rechercher des encodeurs** > Boîte de dialogue **BVMS Scan Wizard**

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Rechercher les passerelles de diffusion de flux** > Boîte de dialogue **BVMS Scan Wizard**

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Rechercher des encodeurs en temps réel uniquement** > Boîte de dialogue **BVMS Scan Wizard**

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Rechercher les encodeurs à stockage local** > Boîte de dialogue **BVMS Scan Wizard**

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Rechercher des décodeurs** > Boîte de dialogue **BVMS Scan Wizard**

Cette boîte de dialogue permet de rechercher les périphériques disponibles sur votre réseau, de les configurer et de les ajouter à votre système au cours du même processus.

Utiliser

Cliquez sur ce bouton pour sélectionner un périphérique à ajouter au système.

Type (non disponible pour les périphériques VSG).

Affiche le type du périphérique.

Nom affiché

Affiche le nom de périphérique qui a été saisi dans l'arborescence des périphériques.

Adresse réseau

Affiche l'adresse IP du périphérique.

Nom d'utilisateur

Affiche le nom d'utilisateur qui est configuré sur le périphérique.

Mot de passe

Saisissez le mot de passe nécessaire à l'authentification auprès de ce périphérique.

État


Affiche l'état de l'authentification.



: Réussite



: Échec

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Rechercher les périphériques VRM** > Boîte de dialogue BVMS Scan Wizard

**Remarque!**

Pour configurer un VRM secondaire, vous devez d'abord installer les logiciels appropriés sur l'ordinateur souhaité. Exécutez Setup.exe, puis sélectionnez **VRM secondaire**.

Rôle

Dans la liste, sélectionnez l'entrée appropriée.

Le tableau suivant répertorie les rôles que chaque type de VRM peut avoir :

Rôle/Type	VRM principal	VRM secondaire
Principal (Normal)	X	
Secondaire (Normal)		X
Basculement principal	X	
Basculement secondaire		X
Redondant		X

À un VRM principal, vous pouvez ajouter un dispositif VRM avec les rôles suivants :

- VRM de basculement
- VRM redondant

À un VRM secondaire, vous pouvez ajouter des dispositifs VRM avec le rôle suivant :

- VRM de basculement

VRM maître

Dans la liste, sélectionnez l'entrée appropriée.

Nom d'utilisateur

Affiche le nom d'utilisateur qui est configuré sur le périphérique VRM.

Vous pouvez saisir un autre nom d'utilisateur, si nécessaire.

Se reporter à

- *Ajout de dispositifs VRM via un balayage, page 174*
- *Ajout d'un encodeur à une zone de stockage VRM, page 225*
- *Ajout d'un encodeur temps réel uniquement, page 225*
- *Ajout d'un encodeur pour stockage local, page 225*
- *Recherche de périphériques, page 74*

14.4**Page Liste de serveurs / Carnet d'adresses**

Fenêtre principale > **Périphériques** > **Enterprise System** > **Liste de serveurs / Carnet d'adresses**

Vous pouvez ajouter plusieurs ordinateurs Management Server pour un accès simultané dans un système d'entreprise BVMS. Vous pouvez également ajouter plusieurs ordinateurs Management Server pour un accès séquentiel dans la recherche de serveur.

Vous pouvez ajouter des colonnes supplémentaires dans la liste des serveurs. Cela vous permet d'ajouter des informations supplémentaires que l'utilisateur peut rechercher en utilisant Server Lookup. Les colonnes ajoutées sont également affichées sur la page **Accès au serveur** (Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >

Onglet  > **Accès au serveur**).

Ajouter un serveur

Cliquez sur ce bouton pour afficher la boîte de dialogue **Ajouter un serveur**.

Supprimer le serveur

Cliquez sur ce bouton pour effacer les entrées Management Server.

Management Server

Affiche les noms de tous les ordinateurs Management Server supplémentaires. Vous pouvez modifier chaque entrée.

Remarque : si vous utilisez une connexion SSH, saisissez l'adresse au format suivant :
ssh://IP ou nomserveur:5322

Adresse réseau privée

Affiche les adresses réseau privé de tous les ordinateurs Management Server supplémentaires. Vous pouvez modifier chaque entrée.

Numéro du serveur

Affiche les numéros logiques de tous les ordinateurs Management Server supplémentaires. Vous pouvez modifier chaque entrée.

Description du serveur

Saisissez une description pour ce Management Server. Vous avez besoin de cette description pour le trouver dans la liste de tous les serveurs disponibles lorsque vous voulez accéder exclusivement à Management Server, par exemple pour clarifier une alarme en provenance d'un autre système de gestion.

Cliquez pour accéder à des instructions détaillées :

- *Configuration de la liste des serveurs pour le système d'entreprise, page 86*
- *Configuration de Server Lookup, page 132*
- *Exportation de la liste des serveurs, page 132*
- *Importation d'une liste de serveurs, page 133*

Se reporter à

- *Tunnelisation SSH, page 50*

14.4.1**Boîte de dialogue Ajouter Serveur**

Fenêtre principale > **Périphériques** > **Enterprise System** > **Liste de serveurs / Carnet d'adresses**

Nom du serveur

Saisissez le nom d'affichage du Management Server.

Remarque : si vous utilisez une connexion SSH, saisissez l'adresse au format suivant :
ssh://IP ou nomserveur:5322

Adresse réseau privée

Saisissez l'adresse IP privée ou le nom DNS du Management Server.

Adresse réseau publique

Saisissez l'adresse réseau publique.

Description du serveur

Saisissez une description pour le Management Server.

14.4.2 Configuration de Server Lookup

Pour la recherche de serveur, l'utilisateur de Operator Client ou Configuration Client doit se connecter avec le nom d'utilisateur d'un groupe d'utilisateurs normal, pas en tant qu'utilisateur d'un Enterprise User Group.

Se reporter à

- *Server Lookup, page 25*
- *Page Liste de serveurs / Carnet d'adresses, page 130*
- *Utilisation de la recherche de serveur, page 74*

14.4.3 Configuration de la liste des serveurs

Fenêtre principale > **Périphériques** > **Enterprise System** > **Liste de serveurs / Carnet d'adresses**

Pour ajouter des serveurs :

1. Cliquez sur **Ajouter un serveur**.
La boîte de dialogue **Ajouter un serveur** s'affiche.
2. Saisissez un nom d'affichage pour le serveur et saisissez l'adresse réseau privée (nom DNS ou adresse IP).
Remarque : Si vous utilisez une connexion SSH, saisissez l'adresse au format suivant : ssh://IP ou nomserveur:5322
3. Cliquez sur **OK**.
4. Répétez les étapes suivantes jusqu'à ce que vous ayez ajouté tous les ordinateurs Management Server souhaités.

Pour ajouter des colonnes :

- ▶ Cliquez avec le bouton droit de la souris sur l'en-tête du tableau et cliquez sur **Ajouter une colonne**.
Vous pouvez ajouter jusqu'à 10 colonnes.
Pour supprimer une colonne, cliquez avec le bouton droit de la souris sur la colonne souhaitée, puis sur **Supprimer la colonne**.
- ⇒ La liste des serveurs que vous exportez contiendra également les colonnes ajoutées.

Se reporter à

- *Configuration de la liste des serveurs pour le système d'entreprise, page 86*

14.4.4 Exportation de la liste des serveurs

Fenêtre principale > **Périphériques** > **Enterprise System** > **Liste de serveurs / Carnet d'adresses**

Vous pouvez exporter la liste des serveurs ainsi que tous les paramètres de configuration pour les modifier et les importer par la suite.

Lorsque vous modifiez le fichier CSV exporté dans un éditeur externe, notez les restrictions décrites dans le chapitre Liste des serveurs.

Pour exporter :

1. Cliquez avec le bouton droit de la souris sur l'en-tête du tableau et cliquez sur **Exporter une liste de serveurs...**
 2. Saisissez un nom pour le fichier d'exportation et cliquez sur **Enregistrer**.
- ⇒ Toutes les colonnes de la liste des serveurs sont exportées dans un fichier csv.

Rubriques connexes

- *Server Lookup, page 25*
- Liste des serveurs

- *Page Liste de serveurs / Carnet d'adresses, page 130*

14.4.5 Importation d'une liste de serveurs

Fenêtre principale > **Périphériques** > **Enterprise System** > **Liste de serveurs / Carnet d'adresses**

Lorsque vous modifiez le fichier CSV exporté dans un éditeur externe, notez les restrictions décrites dans le chapitre Liste des serveurs.

Pour importer :

1. Cliquez avec le bouton droit de la souris sur l'en-tête du tableau et cliquez sur **Importer une liste de serveurs...**
2. Cliquez sur le fichier que vous souhaitez importer, puis cliquez sur **Ouvrir**.

Rubriques connexes

- *Server Lookup, page 25*
- Liste des serveurs
- *Page Liste de serveurs / Carnet d'adresses, page 130*

14.5 Page DVR (enregistreur vidéo numérique)

Fenêtre principale > **Périphériques** >  > 

Affiche les pages de propriété d'un DVR sélectionné.

Permet d'intégrer un DVR au système.

- ▶ Cliquez sur un onglet pour afficher la page de propriété correspondante.



Remarque!

Vous ne devez pas configurer le DVR lui-même, mais uniquement l'intégration du périphérique DVR dans BVMS.



Remarque!

Ajoutez l'enregistreur DVR en utilisant le compte administrateur du périphérique. Si vous utilisez un compte utilisateur DVR avec des droits restreints, certaines fonctions peuvent ne pas être utilisables dans BVMS, par exemple l'utilisation de la commande d'une caméra PTZ.

Se reporter à

- *Périphériques DVR, page 133*
- *Configuration de l'intégration d'un DVR, page 136*

14.5.1 Périphériques DVR

Ce chapitre fournit des informations générales sur les périphériques DVR que vous pouvez intégrer à BVMS.

Certains modèles de DVR (par exemple DHR-700) prennent en charge les enregistrements depuis des encodeurs/caméras IP. D'autres modèles de DVR prennent uniquement en charge les caméras analogiques.

Un encodeur/caméra IP ne doit pas être intégré à la configuration de deux systèmes vidéo (enregistreurs numériques ou systèmes de gestion vidéo).

Si les encodeurs/caméras IP sont connectés à un enregistreur numérique qui est déjà intégré à BVMS, ces encodeurs/caméras IP ne sont pas détectés par le balayage de périphérique réseau BVMS. Ceci est valable pour le balayage réseau lancé depuis Configuration Client ou Config Wizard.

Si un enregistreur numérique avec encodeurs/caméras IP connectés est intégré à BVMS et si ces encodeurs/caméras IP sont déjà ajoutés à BVMS, un message d'avertissement s'affiche. Retirez ces encodeurs/caméras IP de l'enregistreur numérique ou de BVMS. Config Wizard n'ajoute pas de périphérique DVR avec caméras IP en conflit avec la configuration.

Les périphériques DVR prennent en charge un nombre limité de connexions simultanées. Ce numéro définit le nombre maximum d'utilisateurs Operator Client pouvant afficher simultanément des vidéos depuis ce DVR sans volets des images noirs.

**Remarque!**

Ajoutez l'enregistreur DVR en utilisant le compte administrateur du périphérique. Si vous utilisez un compte utilisateur DVR avec des droits restreints, certaines fonctions peuvent ne pas être utilisables dans BVMS, par exemple l'utilisation de la commande d'une caméra PTZ.

**Remarque!**

DIVAR AN 3000/5000 : lorsque vous supprimez des données vidéo de l'enregistreur DVR, notez que vous supprimez toujours au moins l'heure complète des données vidéo. Par exemple, si vous sélectionnez une période allant de 6:50 à 7:05, vous supprimerez en réalité les données vidéo de 6:00 à 8:00.

Enregistreurs HD hybrides et réseau série 700 de Bosch : la suppression démarre toujours avec le début des enregistrements de toutes les caméras affichées dans Operator Client, et prend fin au moment précis que vous avez défini.


Se reporter à

- Page DVR (enregistreur vidéo numérique), page 133
- Configuration de l'intégration d'un DVR, page 136

14.5.2

Ajout d'un dispositif DVR via un balayage

Pour ajouter des dispositifs DVR via un balayage :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Rechercher les DVR**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Cochez les boîtes de dialogue des dispositifs que vous souhaitez ajouter.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit sur ce champ et sélectionnez **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions qui ont abouti sont indiquées par le symbole





les connexions qui ont échoué sont indiquées par le symbole



5. Cliquez sur **Terminer**.

L'élément est ajouté dans l'arborescence des dispositifs.

14.5.3 Boîte de dialogue Ajouter un DVR

Fenêtre principale > **Périphériques** > Développer  >  > **Ajouter un DVR**
Permet d'ajouter manuellement un périphérique DVR.

Adresse réseau/Port

Saisissez l'adresse IP de votre enregistreur numérique (DVR). Si nécessaire, modifiez le numéro de port.

Nom d'utilisateur :

Saisissez le nom d'utilisateur pour la connexion à l'enregistreur numérique.

Mot de passe :

Saisissez le mot de passe pour la connexion à l'enregistreur numérique.

Sécurité

La case **Connexion sécurisée** est cochée par défaut.

Si aucune connexion sécurisée n'est possible, un message s'affiche. Cliquez sur ce bouton pour effacer la sélection.



Remarque!

Si la case **HTTPS** est cochée, les connexions de commande et de contrôle sont sécurisées. Le flux de données vidéo n'est pas sécurisé.



Se reporter à

- Ajout d'un dispositif, page 127



14.5.4 Onglet Paramètres

Fenêtre principale > **Périphériques** >  >  > Onglet **Paramètres**
Affiche les paramètres réseau du DVR connecté au système. Vous permet de modifier les paramètres de base en fonction des besoins.

14.5.5 Onglet Caméras (Caméras)

Fenêtre principale > **Périphériques** >  >  > Onglet **Caméras**
Affiche tous les canaux vidéo du DVR en tant que caméras. Permet de supprimer des caméras.
Une entrée vidéo qui est désactivée dans un périphérique DVR est affichée comme caméra active dans BVMS parce qu'il se peut qu'il existe déjà des enregistrements précédents pour cette entrée.

14.5.6 Onglet Entrées

Fenêtre principale > **Périphériques** >  >  > Onglet **Entrées**
Affiche toutes les entrées du DVR.
Permet de supprimer des éléments.

14.5.7 Onglet Relais

Fenêtre principale > **Périphériques** >  >  > Onglet **Relais**
Affiche tous les relais du DVR. Permet de supprimer des éléments.

14.5.8 Configuration de l'intégration d'un DVR

Fenêtre principale > **Périphériques** > Développer  > 

Remarque!



Ajoutez l'enregistreur DVR en utilisant le compte administrateur du périphérique. Si vous utilisez un compte utilisateur DVR avec des droits restreints, certaines fonctions peuvent ne pas être utilisables dans BVMS, par exemple l'utilisation de la commande d'une caméra PTZ.

Remarque!



Vous ne devez pas configurer le DVR lui-même, mais uniquement l'intégration du périphérique DVR dans BVMS.

Pour supprimer un élément :

1. Cliquez sur l'onglet **Paramètres**, sur l'onglet **Caméras**, sur l'onglet **Entrées** ou sur l'onglet **Relais**.
2. Cliquez avec le bouton droit de la souris sur un élément, puis cliquez sur **Supprimer**. L'élément est supprimé.

Remarque!



Pour rétablir un élément retiré, cliquez avec le bouton droit de la souris sur le périphérique DVR et cliquez sur **Rechercher de nouveau sur le DVR**.



Pour renommer un périphérique DVR :

1. Cliquez avec le bouton droit de la souris sur un périphérique DVR, puis cliquez sur **Renommer**.
2. Saisissez le nouveau nom de l'élément.

Se reporter à

- *Ajout d'un dispositif, page 127*
- *Page DVR (enregistreur vidéo numérique), page 133*

14.6 Page Commutateurs Matriciels

Fenêtre principale > **Périphériques** >  > 
Affiche les pages de propriété du périphérique Bosch Allegiant.

Vous ne devez pas configurer le périphérique Bosch Allegiant proprement dit, mais uniquement les propriétés du système relatives au BVMS. Pour connecter un périphérique Allegiant au système BVMS, reportez-vous au chapitre **Concepts** de cette aide en ligne. Ce chapitre fournit des informations générales sur les sujets sélectionnés.

Vous pouvez également configurer la priorité des commandes pour les lignes de jonction Allegiant.

- ▶ Cliquez sur un onglet pour afficher la page de propriété correspondante.


Se reporter à

- *Configuration d'un périphérique Bosch Allegiant, page 137*
- *Connexion de la matrice Bosch Allegiant à BVMS, page 57*

14.6.1

Ajout d'un dispositif Allegiant Bosch

Pour ajouter un périphérique Allegiant Bosch :

1. Cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Ajouter Allegiant**. La boîte de dialogue **Ouvrir** s'affiche.
2. Sélectionnez le fichier de configuration Allegiant approprié, puis cliquez sur **OK**. Le dispositif Allegiant Bosch est ajouté au système.

Remarque : vous ne pouvez ajouter qu'une seule matrice Allegiant Bosch.

14.6.2

Configuration d'un périphérique Bosch Allegiant

Fenêtre principale > **Périphériques** > Développer  > 

Vous ne devez pas configurer le périphérique Bosch Allegiant proprement dit, mais uniquement les propriétés relatives à BVMS.

Pour affecter une sortie à un encodeur :

1. Cliquez sur l'onglet **Sorties**.
2. Dans la colonne **Utilisation**, cliquez sur **Jonction numérique** pour les cellules voulues.
3. Dans la colonne **Encodeur**, sélectionnez l'encodeur approprié.

Ajout d'une entrée à un périphérique Bosch Allegiant :

1. Cliquez sur l'onglet **Entrées**.
2. Cliquez sur **Ajouter entrées**. Une nouvelle ligne est ajoutée au tableau.
3. Entrez les paramètres requis dans les cellules.

Suppression d'une entrée :

1. Cliquez sur l'onglet **Entrées**.
2. Cliquez sur la ligne concernée dans le tableau.
3. Cliquez sur **Supprimer entrée**. La ligne est supprimée du tableau.

Se reporter à

- *Connexion d'un clavier IntuiKey Bosch à BVMS, page 53*
- *Page Connexion, page 139*
- *Page Caméras, page 139*
- *Page Sorties, page 137*
- *Page Entrées, page 138*

14.6.3

Page Sorties

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Sorties**

Permet de stipuler dans la configuration ce à quoi la sortie d'un périphérique Bosch Allegiant doit servir et d'affecter un encodeur à une sortie.

Pour stocker les données vidéo de la sortie d'un périphérique Bosch Allegiant dans BVMS, vous devez affecter un encodeur à la sortie. Cet encodeur doit être connecté à la sortie.

N°

Affiche le numéro de la sortie.

N° logique du système Allegiant

Affiche le numéro logique de la sortie dans Allegiant.

N° logique BVMS

Permet de changer le numéro logique de la sortie dans BVMS. Si vous saisissez un numéro déjà utilisé, un message s'affiche.

Nom

Affiche le nom de la sortie.

Utilisation

Vous permet de modifier l'utilisation de la sortie.

Si vous sélectionnez **Jonction numérique**, vous pouvez affecter un encodeur à cette sortie dans le champ **Encodeur**. La sortie Allegiant devient alors compatible avec le réseau.

Si vous sélectionnez **Moniteur Allegiant**, l'utilisateur peut affecter le signal de la caméra à un moniteur matériel dans Operator Client. La commande de balayage horizontal/vertical et de zoom est utilisable si la caméra est configurée en tant que caméra mobile. Dans Operator Client, l'utilisateur ne peut pas faire glisser cette caméra sur le volet des Images.

Si vous sélectionnez **Inutilisé**, l'utilisateur ne peut pas affecter de moniteur à une caméra Allegiant.

Encodeur



Permet d'affecter une sortie à un encodeur. Vous ne pouvez sélectionner un encodeur qu'après avoir coché **Jonction numérique**. L'encodeur est verrouillé pour l'Arborescence logique. Si vous affectez un encodeur déjà présent dans l'arborescence logique, il est supprimé. Dans Operator Client, l'utilisateur peut faire glisser une caméra vers le volet des Images.

Se reporter à

- *Configuration d'un périphérique Bosch Allegiant, page 137*

14.6.4

Page Entrées

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Entrées**
Permet d'ajouter des entrées à un périphérique Bosch Allegiant.

Ajouter entrée

Cliquez sur ce bouton pour ajouter une ligne au tableau et définir une nouvelle entrée.

Supprimer entrée

Cliquez sur ce bouton pour supprimer une ligne du tableau.

N° d'entrée

Entrez le numéro de l'entrée. Si vous saisissez un numéro déjà utilisé, un message s'affiche.

Nom de l'entrée

Saisissez le nom de l'entrée.

Se reporter à

- *Configuration d'un périphérique Bosch Allegiant, page 137*

14.6.5 Page Connexion

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Connexion**

Affiche le nom du fichier de configuration Bosch Allegiant.

BVMS peut lire un fichier de configuration dans un format de stockage structuré contenant tous les noms et toutes les informations de configuration de toutes les caméras connectées au périphérique Bosch Allegiant.

Mettre à jour la configuration

Cliquez sur ce bouton pour sélectionner un fichier de configuration Bosch Allegiant mis à jour.

Se reporter à

- *Configuration d'un périphérique Bosch Allegiant, page 137*

14.6.6 Page Caméras

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Caméras**

Affiche un tableau des caméras connectées au périphérique Bosch Allegiant.

N°

Affiche le numéro séquentiel de la caméra.

N° logique du système Allegiant

Affiche le numéro logique de la caméra.

Nom de la caméra

Affiche le nom de la caméra.

Se reporter à

- *Configuration d'un périphérique Bosch Allegiant, page 137*

14.7 Page Poste de commande



Fenêtre principale > **Périphériques** > Développez  > 

Les postes de commande doivent être équipés du logiciel Operator Client.

Permet de configurer les paramètres suivants pour un poste de commande :

- Ajoutez un clavier de vidéosurveillance connecté à un poste de commande Bosch Video Management System.
- Affectez un Script de Commande qui sera exécuté lors du démarrage du poste de commande.
- Sélectionnez le flux par défaut pour l'affichage en temps réel. Vous pouvez sélectionner des flux pour les caméras à double flux et pour des caméras à plusieurs flux.

Remarque : Vous ne pouvez pas configurer un clavier de vidéosurveillance pour un poste de commande par défaut. Cela n'est possible que pour certains postes de commande configurés.

Pour ajouter un clavier Bosch IntuiKey connecté à un décodeur, développez , puis cliquez sur .


Se reporter à

- *Ajout manuel d'un poste de commande, page 140*
- *Configuration d'un script de commande de démarrage (page des paramètres), page 141*

14.7.1

Ajout manuel d'un poste de commande

Pour ajouter un poste de commande BVMS :

1. Cliquez avec le bouton droit de la souris sur .
2. Cliquez sur **Ajouter un poste de commande**.
La boîte de dialogue **Ajouter un poste de commande** s'affiche.
3. Entrez la valeur appropriée.
4. Cliquez sur **OK**.

Le poste de commande  est ajouté à votre système

Pour ajouter un poste de commande BVMS par défaut :

- ▶ Cliquez avec le bouton droit de la souris sur .
- Cliquez sur **Ajouter une station de travail par défaut**.

Le poste de commande  est ajouté à votre système



Remarque!

Vous ne pouvez ajouter qu'un seul poste de commande par défaut.

Si un poste de commande par défaut est configuré, les paramètres s'appliquent à chaque poste de commande connecté à ce serveur et ils ne sont pas configurés séparément. Si un poste de travail est configuré, les paramètres de ce poste de travail spécifique s'appliquent et non les paramètres du poste de commande par défaut.

14.7.2

Configuration d'un clavier numérique IntuiKey de Bosch (page des paramètres) (poste de commande)

Fenêtre principale > **Périphériques** > Développez  > 

Pour configurer un clavier numérique IntuiKey de Bosch connecté à un poste de commande :

1. Cliquez sur l'onglet **Paramètres**.
2. Dans le champ **Paramètres du clavier**, sélectionnez les paramètres appropriés.
Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Se reporter à

- *Page Poste de commande, page 139*

14.7.3 Configuration d'un script de commande de démarrage (page des paramètres)

Fenêtre principale > **Périphériques** > Développer  >  > page **Paramètres**

Vous pouvez configurer un Script de Commande qui sera exécuté au démarrage du Operator Client sur le poste de commande sélectionné.

Vous devez créer un Script de Commande correspondant.

Pour créer un Script de Commande, voir *Gestion des Scripts de Commande, page 90*.

Pour créer un script de démarrage :

- ▶ Dans la liste **Script de démarrage** , sélectionnez le Script de Commande requis.

Se reporter à

- *Page Poste de commande, page 139*

14.7.4 Page Paramètres

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Paramètres**

Permet de configurer un script qui est exécuté dès que l'Operator Client est démarré sur le poste de commande.

Permet de configurer TCP ou UDP comme protocole de transmission de toutes les caméras affichées en Mode Temps Réel sur votre poste de commande.

Permet de stipuler dans la configuration quel flux d'un dispositif IP servira à l'affichage temps réel.

Permet d'activer la recherche judiciaire pour ce poste de commande.

Vous pouvez également configurer le clavier connecté à ce poste de commande.

Adresse réseau :

Saisissez le nom DNS ou l'adresse IP de votre poste de commande.

Script de démarrage :

Sélectionnez le script que vous souhaitez exécuter au démarrage du Operator Client du poste de commande. Vous pouvez créer ou importer ce script sur la page **Événements**.

Protocole de caméra par défaut :

Sélectionnez le protocole de transmission par défaut de toutes les caméras affectées à l'arborescence logique du poste de travail.

Remplacer les paramètres de la page "Caméras et enregistrement"

Cochez cette case pour activer la sélection du flux voulu pour l'affichage en temps réel.

Remarque : Pour les dispositifs DVR qui offrent plusieurs flux (par exemple, DIVAR AN 3000/5000), le paramètre de flux en temps réel depuis ce DVR est également modifié ici.

Les paramètres de flux en temps réel ne sont pas disponibles dans la page **Caméras et enregistrement**.

Flux en temps réel

Sélectionnez le flux souhaité pour la visualisation en temps réel. Vous pouvez sélectionner des flux pour les caméras à double flux et pour des caméras à plusieurs flux.

Lorsque vous sélectionnez **Optimisation de la taille du volet des images**, la résolution de chaque caméra affichée est automatiquement ajustée à la taille du Volet des images en fonction de la résolution du moniteur utilisé. Cela est utile pour l'affichage de plusieurs caméras avec une résolution élevée, par exemple les caméras 4K ultra HD. Seules les caméras avec des flux dont la résolution peut être configurée indépendamment, permettent de régler la résolution sur le volet des images. L'utilisateur d'Operator Client peut modifier la sélection du flux pour chaque caméra individuellement.

Caméras à double flux

Sélectionnez le flux par défaut pour l'affichage en temps réel des caméras à double flux.

Caméras à multi-diffusion

Sélectionnez le flux par défaut pour l'affichage en temps réel des caméras à plusieurs flux.

Utiliser le flux transcodé à la place, si disponible

Sélectionnez la case à cocher permettant d'autoriser l'utilisation d'un flux transcodé le cas échéant. Ce flux transcodé est utilisé à la place du flux sélectionné pour la visualisation en temps réel.

Pour qu'un flux transcodé soit disponible dans BVMS, soit MVS doit être installé ou votre ordinateur VRM est doté d'un transcodeur matériel intégré.

Lorsqu'une caméra s'affiche en mode temps réel, le flux par défaut défini pour le poste de commande est utilisée. Si la caméra ne dispose d'aucun flux 2 ou si le service de transcodage (logiciel et matériel) n'est pas disponible, le flux 1 sera utilisé même si un autre paramètre est configuré dans les paramètres du poste de commande.

Utiliser la lecture directe du périphérique de stockage

Cochez cette case pour envoyer le flux vidéo directement du périphérique de stockage à ce poste de commande. À présent le flux n'est pas envoyé via VRM. Le poste de commande a toujours besoin d'une connexion au VRM pour garantir une lecture correcte.

Remarque : Vous ne pouvez utiliser la lecture directe à partir du périphérique de stockage iSCSI que si vous avez défini le mot de passe CHAP global iSCSI.

Récupérer la vidéo en temps réel de Video Streaming Gateway au lieu de la caméra

Affiche la liste des périphériques Video Streaming Gateway. Sélectionnez les entrées souhaitées pour permettre la transmission de données vidéo via des segments de faible bande passante entre la source vidéo et ce poste de commande.

Remarque : si vous sélectionnez un dispositif Video Streaming Gateway pour récupérer la vidéo en temps réel, le paramètre **Vidéo en temps réel - Profil** indiqué sur la page **Caméras et enregistrement** est obsolète. Au lieu de cela, le paramètre **Enregistrement - Profil** est également utilisé pour la vidéo en temps réel.

Type de clavier :

Sélectionnez le type du clavier connecté à votre poste de commande.

Port :

Sélectionnez le port COM utilisé pour connecter le clavier.

Débit en bauds :

Sélectionnez la vitesse maximale (en bits par seconde - bps) à laquelle les données doivent être transmises via ce port. Il s'agit généralement de la vitesse maximale prise en charge par l'ordinateur ou le périphérique avec lequel vous communiquez.

Bits de données :

Affiche le nombre de bits de données à utiliser pour chaque caractère transmis et reçu.

Bits d'arrêt :

Affiche l'intervalle de temps entre chaque caractère transmis (lorsque le temps est mesuré en bits).

Parité :

Affiche le type de contrôle d'erreur que vous souhaitez utiliser pour le port sélectionné.

Type de port :

Affiche le type de connexion utilisée pour relier le clavier numérique IntuiKey de Bosch au poste de commande.


Se reporter à

- *Configuration d'un script de commande de démarrage (page des paramètres), page 141*



14.7.5**Modification de l'adresse réseau d'un poste de commande**

Fenêtre principale > **Périphériques** > Développez 

Pour changer l'adresse IP :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Modifier l'adresse réseau**.
La boîte de dialogue **Modifier l'adresse réseau** s'affiche.
2. Modifiez l'adresse dans le champ en fonction de vos exigences.

14.8**Page Décodeurs**

Fenêtre principale > **Périphériques** > Développez  >  >
Permet d'ajouter et de configurer des décodeurs.

**Remarque!**

BVMS Viewer ne prend pas en charge les décodeurs.

**Remarque!**


Si vous voulez utiliser des décodeurs dans votre système, assurez-vous que tous les encodeurs utilisent le même mot de passe pour le niveau d'autorisation user.

Se reporter à


- *Recherche de périphériques, page 74*
- *Page Encodeur / Décodeur / Caméra Bosch, page 222*

14.8.1**Ajout manuel d'un encodeur**


Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec

le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**

ou

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**

ou

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**

ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la






souris sur  > Cliquez sur **Ajouter décodeur** > Boîte de dialogue **Ajouter encodeur**


Vous permet d'ajouter un encodeur manuellement. Cette fonction s'avère très utile lorsque vous souhaitez ajouter un périphérique vidéo IP de Bosch (uniquement pour VRM).

Remarque :

Si vous ajoutez un encodeur vidéo IP de Bosch avec l'option **<Détection automatique>**, ce dispositif doit être disponible sur le réseau.

Pour ajouter un dispositif vidéo IP Bosch :

1. Développez , puis , cliquez avec le bouton droit de la souris sur .
Ou
cliquez avec le bouton droit de la souris sur .
Ou
cliquez avec le bouton droit de la souris sur .
2. Cliquez sur **Ajouter encodeur**.
La boîte de dialogue **Ajouter un encodeur** s'affiche.
3. Saisissez l'adresse IP correspondante.
4. Dans la liste, sélectionnez **<Détection automatique>**, saisissez le mot de passe du dispositif et cliquez sur **Authentifier**.
Ou
Dans la liste, sélectionnez un type d'encodeur concret ou **<Caméra avec un seul espace réservé>**.
5. Cliquez sur **OK**.
Le dispositif est ajouté au système.

L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

Boîte de dialogue Ajouter encodeur**Adresse réseau**

Saisissez une adresse IP valide.

Type d'encodeur

Pour les dispositifs dont le type est connu, sélectionnez l'entrée correspondante. Le périphérique ne doit pas obligatoirement être disponible sur le réseau.

Si vous souhaitez ajouter un dispositif vidéo IP de Bosch, sélectionnez **<Détection automatique>**. Le dispositif doit être disponible sur le réseau.

Si vous souhaitez ajouter une caméra pour une configuration hors ligne, sélectionnez **<Caméra avec un seul espace réservé>**.

Nom d'utilisateur

Affiche le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le dispositif.

Afficher le mot de passe



Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Authentifier

Permet de vous authentifier sur le dispositif avec les identifiants saisis précédemment.

14.8.2

Boîte de dialogue Modifier encodeur / décodeur

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier L'encodeur** > Boîte de dialogue **Modifier L'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier L'encodeur** > Boîte de dialogue **Modifier L'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier L'encodeur** > Boîte de dialogue **Modifier L'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier le décodeur** > Boîte de dialogue **Modifier le décodeur**

Permet de vérifier et de mettre à jour les fonctionnalités d'un dispositif. À l'ouverture de cette boîte de dialogue, le périphérique est connecté. Le mot de passe est vérifié et les fonctions de ce périphérique sont comparées à celles enregistrées dans BVMS.

Nom

Affiche le nom du dispositif. Lorsque vous ajoutez un dispositif vidéo IP de Bosch, son nom est généré. Modifiez les valeurs si nécessaire.

Adresse réseau

Saisissez l'adresse réseau du dispositif. Si nécessaire, modifiez le numéro de port.

Nom d'utilisateur

Affiche le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le dispositif.

Afficher le mot de passe

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Authentifier

Permet de vous authentifier sur le dispositif avec les identifiants saisis précédemment.

Sécurité

La case **Connexion sécurisée** est cochée par défaut.

Si aucune connexion sécurisée n'est possible, un message s'affiche. Cliquez sur ce bouton pour effacer la sélection.

Les décodeurs suivants prennent en charge une connexion sécurisée :

- VJD 7000
- VJD 8000
- VIP XD HD

**Remarque!**

La connexion entre un décodeur et un encodeur est uniquement sécurisée, si les deux sont configurés avec une connexion sécurisée.

Flux vidéo

UDP : permet la diffusion multidiffusion chiffrée pour les décodeurs pris en charge.

TCP : permet la diffusion monodiffusion chiffrée pour les décodeurs pris en charge.

Remarque : si aucune adresse multidiffusion n'est configurée pour un encodeur, le décodeur récupère le flux par monodiffusion.

**Remarque!**

BVMS ne prend pas en charge les caméras Bosch connectées à un VSG.

BVMS ne prend en charge que le chiffrement UDP pour les plates-formes plus anciennes que CPP13.

Fonctions du périphérique

Permet de trier les fonctions affichées par catégorie ou par ordre alphabétique.





Un message vous informe si les fonctions détectées correspondent aux fonctions actuelles du périphérique.

Cliquez sur **OK** pour appliquer les modifications des fonctions après une mise à niveau du périphérique.

Se reporter à

- *Chiffrement de vidéo en temps réel (Modifier l'encodeur), page 228*
- *Mise à jour des fonctions du dispositif (Modifier l'encodeur), page 229*

14.8.3**Modification du mot de passe d'un encodeur / décodeur (modifier mot de passe / entrer mot de passe)**

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > 

ou

Fenêtre principale > **Périphériques** >  > 

ou


Fenêtre principale > **Périphériques** >  > 

ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > 

Définissez ou modifiez le mot de passe pour chaque niveau. Saisissez le mot de passe (19 caractères maximum ; aucun caractère spécial) correspondant au niveau sélectionné.

Pour modifier le mot de passe :

1. Cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Modifier le mot de passe...**

- La boîte de dialogue **Entrer le mot de passe** s'affiche.
2. Dans la liste **Entrez le nom de l'utilisateur**, sélectionnez l'utilisateur pour lequel vous souhaitez modifier le mot de passe.
 3. Dans le champ **Entrez le mot de passe de l'utilisateur**, saisissez le nouveau mot de passe.
 4. Cliquez sur **OK**.
- ⇒ Le mot de passe est immédiatement modifié sur le dispositif.

Un mot de passe empêche tout accès non autorisé à l'unité. Vous pouvez utiliser différents niveaux d'autorisation pour restreindre l'accès.

Une protection par mot de passe n'est valide que si tous les niveaux d'autorisation supérieurs sont également protégés par un mot de passe. Par conséquent, vous devez toujours commencer par le niveau d'autorisation le plus élevé lorsque vous attribuez des mots de passe.

Vous pouvez définir et modifier un mot de passe pour chaque niveau d'autorisation si vous êtes connecté au compte utilisateur « service ».

L'appareil reconnaît trois niveaux d'autorisation : service, user et live.

- service représente le niveau d'autorisation le plus élevé. Après avoir saisi le mot de passe approprié, vous pouvez accéder à toutes les fonctions et modifier tous les paramètres de configuration.
- user représente le niveau d'autorisation intermédiaire. À ce niveau, vous pouvez faire fonctionner le périphérique, lire les enregistrements et commander une caméra, mais pas modifier la configuration.
- live représente le niveau d'autorisation le plus bas. À ce niveau, vous pouvez uniquement visualiser l'image vidéo en temps réel et passer d'une image en temps réel à une autre.

Pour un décodeur, le niveau d'autorisation suivant remplace le niveau d'autorisation live :

- destination password (disponible uniquement pour les décodeurs)
Utilisé pour accéder à un encodeur.

Se reporter à

- *Indication du mot de passe de destination d'un décodeur (Authentifier...), page 217*


14.8.4

Profil de décodeur

Permet de définir les différentes options d'affichage des images vidéo sur un moniteur VGA.

Nom du moniteur

Saisissez le nom du moniteur. Le nom de moniteur facilite l'identification de l'emplacement distant du moniteur. Utilisez un nom permettant d'identifier facilement l'emplacement.

Cliquez sur  pour actualiser le nom dans l'Arborescence des Périphériques.

Standard

Sélectionnez le signal vidéo de sortie du moniteur utilisé. Huit paramètres VGA préconfigurés sont disponibles en plus des options PAL et NTSC des moniteurs vidéo analogiques.



Remarque!

La sélection d'un paramètre VGA dont les valeurs dépassent les caractéristiques techniques du moniteur peut gravement endommager ce dernier. Consultez la documentation technique du moniteur utilisé.

Mise en page fenêtre

Sélectionnez la disposition par défaut de l'affichage du moniteur.

Taille d'écran VGA

Indiquez le rapport hauteur/largeur de l'écran (par exemple 4 x 3) ou sa taille physique en millimètres. Le périphérique se fonde sur ces données pour afficher une image mise à l'échelle exacte et non distordue.

14.8.5**Affichage sur moniteur**

Le périphérique reconnaît les interruptions de transmission et affiche un avertissement sur le moniteur.

Affich. si perturb. transmissions

Sélectionnez **Activé** pour afficher un avertissement en cas d'interruption de transmission.

Sensibilité aux perturbations

Déplacez le curseur pour ajuster le niveau de l'interruption déclenchant l'avertissement.

Texte de notification de la perturbation

Tapez le texte de l'avertissement affiché par le moniteur en cas de perte de connexion. Le champ peut comporter au maximum 31 caractères.

14.8.6**Configuration d'un clavier numérique IntuiKey de Bosch (décodeur)**

Fenêtre principale > **Périphériques** > Développez  > 

**Remarque!**

Vous ne pouvez pas connecter un clavier KBD-Universal XF à un décodeur.

Pour configurer un clavier numérique IntuiKey de Bosch connecté à un décodeur :

1. Dans la colonne **Connexion**, cliquez sur une cellule, puis sélectionnez le décodeur approprié.

Vous pouvez également sélectionner un poste de commande, si le clavier Bosch IntuiKey y est connecté.

Un poste de commande doit être configuré sur la page .

2. Dans le champ **Paramètres de connexion**, sélectionnez les paramètres appropriés. Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Se reporter à

- *Page Attribution de clavier, page 159*
- *Scénarios de connexion d'un clavier numérique IntuiKey de Bosch, page 54*
- *Connexion d'un clavier numérique IntuiKey de Bosch à un décodeur, page 56*

14.8.7**Configuration d'un décodeur pour une utilisation avec un clavier numérique IntuiKey de Bosch**

Fenêtre principale > **Périphériques** > Développez  > Développez 

Appliquez la procédure suivante pour configurer un décodeur VIP XD connecté à un clavier Bosch IntuiKey.

Pour configurer un décodeur :

1. Cliquez sur le décodeur utilisé pour connecter un clavier Bosch IntuiKey.
2. Cliquez sur l'onglet **Périphériques**.
3. Vérifiez que les paramètres suivants sont appliqués :
 - Fonction port série : **Transparent**
 - Débits en bauds : **19 200**
 - Bits d'arrêt : **1**
 - Vérification de la parité : **Aucune**
 - Mode d'interface : **RS232**
 - Mode half-duplex : **Désactivé**




Se reporter à

- *Scénarios de connexion d'un clavier numérique IntuiKey de Bosch, page 54*
- *Connexion d'un clavier numérique IntuiKey de Bosch à un décodeur, page 56*
- *Mise à jour du firmware clavier numérique IntuiKey de Bosch, page 56*

14.8.8 Supprimer le logo du décodeur

Cliquez pour supprimer le logo configuré dans la page Web du décodeur.

14.9 Page Groupes de moniteurs

Fenêtre principale > **Périphériques** > Développez  >  >
 Permet d'ajouter et de configurer des groupes de moniteurs. Vous affectez un groupe de moniteurs à un poste de commande BVMS dans .

**Remarque!**

Vous ne pouvez pas contrôler un groupe de moniteurs dans Operator Client lorsque la connexion au Management Server est perdue.

Se reporter à

- *Ajout manuel d'un groupe de moniteurs, page 149*
- *Configuration d'un groupe de moniteurs, page 150*
- *Configuration de positions prédéfinies et de commandes auxiliaires, page 311*
- *Configuration d'une alarme, page 336*
- *Boîte de dialogue Options d'alarmes, page 325*
- *Boîte de dialogue Sélectionner le contenu du volet des Images (MG), page 325*

14.9.1 Ajout manuel d'un groupe de moniteurs

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter un groupe de moniteurs**

1. Cliquez sur **Ajouter un groupe de moniteurs**.
 La boîte de dialogue **Ajouter un groupe de moniteurs** s'affiche. Saisissez le nom du nouveau groupe de moniteurs.

2. Cliquez sur OK.
Le groupe de moniteurs est ajouté au système.
3. Cliquez sur **Cartes et structure**.
4. Faites glisser le groupe de moniteurs vers l'arborescence logique.

14.9.2

Configuration d'un groupe de moniteurs

Fenêtre principale > **Périphériques** > Développer 



Remarque!

Vous ne pouvez pas contrôler un groupe de moniteurs dans Operator Client lorsque la connexion au Management Server est perdue.

Vous pouvez configurer les moniteurs dans un groupe de moniteurs de manière logique dans des lignes et des colonnes. Cette organisation ne doit pas obligatoirement correspondre à la disposition physique des moniteurs.

Pour configurer un groupe de moniteurs :

1. Faites glisser les moniteurs appropriées de l'onglet **Moniteurs non affectés** vers le champ des groupes de moniteurs.
2. Dans l'onglet **Disposition**, sélectionnez la disposition appropriée.
3. Faites glisser n'importe quelle caméra disponible de l'onglet **Caméras** vers un volet des moniteurs, à gauche.
Le numéro logique de la caméra s'affiche en noir dans le volet du moniteur et la couleur de ce volet change.
4. Modifiez les numéros logiques des volets des images, le cas échéant. Si vous saisissez un numéro déjà utilisé, une boîte de message s'affiche.
5. Dans l'onglet **Options**, vous pouvez indiquer si le nom de la caméra et son numéro de caméra seront visibles dans le volet du moniteur. Vous pouvez également choisir la position de ces informations.

Remarque : Pour VIDEOJET decoder 7513, VIDEOJET decoder 7523 et VIDEOJET decoder 8000, ces options sont valides uniquement une fois que vous avez configuré les paramètres décodeurs respectifs

Voir

- *Configuration des décodeurs pour l'affichage à l'écran (OSD), page 241*

Image moniteur

Le numéro noir en gras, le cas échéant, correspond au numéro logique de la caméra initiale. Le numéro noir non gras correspond au numéro logique du moniteur.
Pour annuler l'affectation d'une caméra, cliquez droit sur le volet du moniteur, puis cliquez sur **Volet vide** ou faites glisser la caméra à l'extérieur du volet des images.

Se reporter à

- *Ajout manuel d'un groupe de moniteurs, page 149*

14.10

Page Périphériques de communication

Fenêtre principale > **Périphériques** > Développez 

Permet d'ajouter ou de configurer un dispositif de communication.



Vous pouvez configurer le dispositif de communication suivant :

- E-mail

Se reporter à

- *Configuration d'un périphérique de communication, page 152*

14.10.1**Ajout d'un serveur de messagerie/SMTP****Pour ajouter un dispositif de communication :**

1. Développez , cliquez avec le bouton droit de la souris sur , puis cliquez sur **Ajouter périphérique e-mail/SMTP**.
La boîte de dialogue **Ajouter périphérique e-mail/SMTP** s'affiche.
2. Entrez les paramètres appropriés.
3. Cliquez sur **OK**.
Le dispositif de communication est ajouté au système.

Boîte de dialogue Ajouter périphérique e-mail/SMTP**Nom :**

Saisissez le nom affiché du serveur de messagerie.

14.10.2**Page Serveur SMTP**

Fenêtre principale > **Périphériques** > Développez  > Développez  > ,
Permet de configurer les paramètres de messagerie du système. Sur la page **Événements**, vous pouvez affecter un événement à un e-mail. Lorsque l'événement se produit, le système envoie un e-mail. Vous ne pouvez pas recevoir d'e-mails dans BVMS.

Nom du serveur SMTP

Saisissez le nom du serveur de messagerie. Pour connaître ce paramètre, contactez votre fournisseur. Il s'agit généralement de l'adresse IP ou du nom DNS de votre serveur de messagerie.

Adresse de l'expéditeur

Saisissez l'adresse e-mail qui est utilisée comme adresse de l'expéditeur lorsque le système envoie un e-mail, par exemple dans le cas d'une alarme par e-mail.

SSL/TLS

Cochez cette case pour permettre l'utilisation d'une connexion SSL/TLS sécurisée. Dans ce cas, le port réseau bascule automatiquement sur 587.

Port

Entrez le numéro de port réseau pour les messages sortants. Pour connaître ce paramètre, contactez votre fournisseur.

Le port 25 est sélectionné automatiquement lorsque vous désactivez le paramètre **SSL/TLS**. Vous pouvez sélectionner un autre port si nécessaire.

Délai d'attente de connexion [s]

Entrez la durée d'inactivité (en secondes) après laquelle la connexion est coupée.

Authentification

Cochez la case de la méthode d'authentification requise. Pour connaître ce paramètre, contactez votre fournisseur.

Nom d'utilisateur

Saisissez le nom d'utilisateur nécessaire à l'authentification sur le serveur de messagerie. Pour connaître ce paramètre, contactez votre fournisseur.

Mot de passe :

Saisissez le mot de passe nécessaire à l'authentification sur le serveur de messagerie. Pour connaître ce paramètre, contactez votre fournisseur.

Envoyer e-mail test

Cliquez sur ce bouton pour afficher la boîte de dialogue **Envoyer e-mail test**.


Se reporter à

- *Configuration d'un périphérique de communication, page 152*

14.10.3**Configuration d'un périphérique de communication**

Fenêtre principale > **Périphériques** > Développez  > Développez 

Pour configurer un dispositif de communication :

1. Cliquez sur .

2. Définissez les paramètres appropriés.

Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Se reporter à

- *Ajout d'un serveur de messagerie/SMTP, page 151*
- *Page Serveur SMTP, page 151*

14.10.4**Boîte de dialogue Envoyer e-mail test**

Fenêtre principale > **Périphériques** > Développez  > Développez  >  >

Bouton Envoyer e-mail test

Permet d'envoyer un e-mail test.

De :

Entrez l'adresse e-mail de l'expéditeur.

Pour

Entrez l'adresse e-mail du destinataire.

Objet

Entrez l'objet du message.

Message

Entrez le message.

Envoyer e-mail test

Cliquez sur ce bouton pour envoyer le message.

Se reporter à

- *Configuration d'un périphérique de communication, page 152*

14.11**Page ATM/POS Bridge**

Fenêtre principale > **Périphériques** > Développez  > 

Permet d'ajouter et de configurer des dispositifs périphériques, tels qu'une ATM/POS Bridge Bosch.

Pour ajouter plusieurs interfaces sur un seul serveur, vous devez utiliser des ports différents.

Se reporter à

- Ajout d'une interface ATM/POS Bridge Bosch, page 98
- Configuration d'un périphérique, page 154

14.11.1**Ajout manuel d'une interface ATM/POS Bridge Bosch**

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la

souris sur  > **Ajouter interface ATM/POS-Bridge Bosch** .
Permet d'ajouter un périphérique ATM Bosch.

Pour ajouter un périphérique :

1. Développez , cliquez sur  avec le bouton droit de la souris, puis cliquez sur **Ajouter interface ATM/POS-Bridge Bosch**.
La boîte de dialogue **Ajouter interface ATM/POS-Bridge Bosch** s'affiche.
2. Entrez les paramètres appropriés.
3. Cliquez sur **OK**.
Le dispositif périphérique est ajouté au système.

Boîte de dialogue Ajouter interface ATM/POS-Bridge Bosch**Nom :**

Saisissez le nom du périphérique.

Adresse IP :

Saisissez l'adresse IP du périphérique.

Port 1 :

Saisissez le numéro de port approprié utilisé en tant que port d'écoute de la ATM/POS Bridge.

Port 2 :

Saisissez le numéro de port approprié utilisé en tant que port d'écoute de BVMS Management Server.





**Remarque!**

Si vous ajoutez plusieurs ATM/POS Bridges à votre système, assurez-vous que les numéros du port 2 de chaque dispositif varient. Si le même numéro est utilisé plusieurs fois pour le port 2, cela peut provoquer une perte de données au niveau de la ATM/POS.

Se reporter à

- Ajout d'une interface ATM/POS Bridge Bosch, page 98

14.11.2**Page Interface ATM/POS Bridge**

Fenêtre principale >  **Périphériques** > Développez  > Développez  >  > onglet **Interface ATM/POS Bosch**

Permet de configurer une ATM/POS Bridge Bosch.

Adresse IP :

Saisissez l'adresse IP du dispositif.

Port 1 :

Saisissez le numéro de port approprié utilisé en tant que port d'écoute de la ATM/POS Bridge.

Port 2 :

Saisissez le numéro de port approprié utilisé en tant que port d'écoute de BVMS Management Server.

**Remarque!**

Si vous ajoutez plusieurs ATM/POS Bridges à votre système, assurez-vous que les numéros du port 2 de chaque dispositif varient. Si le même numéro est utilisé plusieurs fois pour le port 2, cela peut provoquer une perte de données au niveau de la ATM/POS.

Se reporter à

- *Configuration d'un périphérique, page 154*
- *Ajout d'une interface ATM/POS Bridge Bosch, page 98*

14.11.3**Configuration d'un périphérique**

Fenêtre principale >  **Périphériques** > Développez  > Développez  >

**Interface ATM/POS Bosch**

ou

Fenêtre principale >  **Périphériques** > Développez  > Développez  >

**Périphérique DTP >****Pour configurer un périphérique :**

- ▶ Modifiez les paramètres appropriés.

Pour de plus amples informations sur les différents champs, cliquez ci-dessous sur le lien de la fenêtre concernée.

Se reporter à

- *Page Paramètres ATM, page 155*
- *Page Interface ATM/POS Bridge, page 153*
- *Page Paramètres DTP, page 154*

14.11.4**Page Paramètres DTP**

Fenêtre principale >  **Périphériques** > Développez  > Développez  > 

Permet de configurer un dispositif DTP avec au maximum 4 périphériques ATM connectés à ce périphérique DTP.

Port série

Dans la liste, sélectionnez le port approprié.

Se reporter à

- *Page Paramètres ATM, page 155*

– *Configuration d'un périphérique, page 154*

14.11.5 Page Paramètres ATM

Fenêtre principale >  **Périphériques** > Développez  > Développez  > 

Permet de configurer un périphérique ATM connecté à un périphérique DTP.

Numéro d'entrée du périphérique DTP

Sélectionnez le numéro d'entrée souhaité. Si ce numéro est déjà utilisé par un autre périphérique ATM, vous pouvez remplacer les numéros d'entrée.

Délai d'expiration de la connexion [heures]

Saisissez le nombre d'heures souhaité. Si le périphérique ATM n'a pas envoyé de données de transaction au cours de cette période, BVMS suppose que la connexion est interrompue. Un événement correspondant est déclenché. L'événement **Non authentifiée** est disponible pour un périphérique ATM, mais il n'est pas pertinent.

Saisir **0** signifie qu'aucune vérification de la connexion n'est effectué.

Entrées de données

Cliquez sur cette option pour activer les entrées souhaitées, puis saisissez le nom de votre choix pour ces entrées.

Se reporter à

– *Configuration d'un périphérique, page 154*

14.11.6 Page Entrées

Fenêtre principale >  **Périphériques** > Développez  > Développez  >  > Onglet **Entrées**



Permet de configurer les entrées d'une ATM/POS Bridge Bosch.

Se reporter à

– *Configuration d'un périphérique, page 154*

– *Ajout d'une interface ATM/POS Bridge Bosch, page 98*

14.12 Lecteurs de cartes Foyer

Fenêtre principale > **Périphériques** > Développez  >  > onglet **Paramètres globaux des lecteurs de carte foyer**

Vous pouvez configurer les paramètres valides pour tous les lecteurs de cartes Foyer du système.

Port série

Sélectionnez le port série auquel le lecteur de cartes Foyer est connecté.

Verrouillé

Permet d'ajouter des codes d'acheminement bancaire pour le verrouillage. Ceci signifie que les cartes ayant les caractéristiques de verrouillage indiquées ici ne disposent pas d'une autorisation d'accès. L'accès est refusé par le lecteur de cartes Foyer. Le mode par défaut de libération du verrou de la porte électrique du lecteur de cartes Foyer doit être défini sur :

Automatique

La liste peut contenir des entrées avec des caractères génériques.

? : Représente un caractère quelconque ou aucun caractère à cette position.



* : Représente une suite (un ou plusieurs caractères) d'un caractère quelconque (exception :

* seul signifie que tous les codes de tri bancaires sont verrouillés).

Ignorer le code pays sur les cartes EC

Cliquez sur cette option pour faire en sorte que BVMS n'analyse pas les données de carte qui sont utilisées pour identifier le pays d'émission de la carte. L'accès est autorisé pour les cartes ayant un code pays différent.

14.12.1**Boîte de dialogue Ajouter un lecteur de cartes Foyer**

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Commande **Ajouter un lecteur de cartes foyer**
Vous pouvez ajouter un lecteur de cartes Foyer.


Nom

Saisissez un nom pour le périphérique.

Identifiant de périphérique

Sélectionnez un numéro unique pour le périphérique. Si aucun numéro n'est disponible, cela signifie que le nombre maximal de lecteurs de cartes Foyer a déjà été ajouté au système.

14.12.2**Page Paramètres du lecteur de cartes Foyer**

Fenêtre principale > **Périphériques** > Développez  >  >  > Onglet **Paramètres pour le lecteur de carte foyer**

Vous pouvez configurer un lecteur de cartes Foyer.

Identifiant de périphérique

Affiche le numéro unique du périphérique.

Activer la protection contre le clonage

Cliquez sur cette option pour faire en sorte que BVMS déclenche un événement lorsqu'un dispositif de clonage connecté détecte un clonage. Cette opération n'est pas prise en charge par tous les lecteurs de cartes Foyer.

Mode par défaut d'ouverture du verrou de porte électrique

Ouvrir : La porte est ouverte et tout le monde peut accéder au dispositif sans carte.

Fermé : La porte est fermée, quelle que soit la carte insérée.

Automatique : La porte s'ouvre uniquement lorsqu'une carte disposant d'une autorisation d'accès est insérée dans le lecteur.

Activer le contrôle selon la planification

Cliquez sur cette option pour pouvoir affecter une planification au mode de libération du verrou de la porte sélectionné.

Lorsqu'une planification devient active, BVMS fait passer le lecteur de cartes Foyer dans le mode de libération correspondant.

Si les planifications sélectionnées se chevauchent, le mode effectif d'ouverture de la porte est déterminé par l'ordre de priorité des modes suivant : 1. **Ouvrir** 2. **Fermé** 3. **Automatique**

14.13 Page Entrées virtuelles

Fenêtre principale > **Périphériques** > Développez  > 

Affiche les entrées virtuelles configurées dans le système.

Permet d'ajouter de nouvelles entrées virtuelles et d'effacer des entrées existantes.

Ajouter entrées

Cliquez sur ce bouton pour afficher une boîte de dialogue permettant d'ajouter de nouvelles entrées virtuelles.

Supprimer entrées

Cliquez sur ce bouton pour supprimer une entrée virtuelle sélectionnée.

Numéro

Affiche le numéro de l'entrée virtuelle.



Nom

Cliquez sur une cellule pour modifier le nom de l'entrée virtuelle.

14.13.1 Ajout manuel d'entrées virtuelles

Fenêtre principale > **Périphériques** > Développez  > Bouton **Ajouter entrées**
Permet d'ajouter des entrées virtuelles.

Pour ajouter une entrée virtuelle :

1. Développez , cliquez sur .
La page correspondante s'affiche.
2. Cliquez sur **Ajouter entrées**.
Une nouvelle ligne est ajoutée au tableau.
3. Définissez les paramètres appropriés.
4. Cliquez sur **Ajouter**.
L'entrée virtuelle est ajoutée au système.

Boîte de dialogue Ajouter entrées

Début :

Sélectionnez le premier numéro des nouvelles entrées virtuelles.

Fin :

Sélectionnez le dernier numéro des nouvelles entrées virtuelles.

Nom :

Saisissez le nom de chaque nouvelle entrée virtuelle. Un numéro leur est ajouté.

Ajouter

Cliquez sur ce bouton pour ajouter de nouvelles entrées virtuelles.

14.14 Page RMon et Snmp

Fenêtre principale > **Périphériques** > Développez  > 

Permet d'ajouter ou de configurer la mesure des SNMP afin de maintenir la qualité du réseau.

Se reporter à

- *Configuration d'un récepteur de trap SNMP (page récepteur de trap SNMP), page 158*

14.14.1



Ajout manuel de SNMP

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la

souris sur  > Commande **Ajouter récepteur de trap SNMP / RMon**

Permet d'ajouter un système de surveillance réseau à BVMS.

Pour ajouter un dispositif de surveillance réseau :

1. Développez , cliquez sur  avec le bouton droit de la souris, puis cliquez sur **Ajouter récepteur de trap SNMP / RMon**.
La boîte de dialogue **Ajouter récepteur de trap SNMP / RMon** s'affiche.
2. Saisissez un nom pour le dispositif SNMP.
Le dispositif de surveillance du réseau est ajouté au système.

Boîte de dialogue Ajouter récepteur de trap SNMP / RMon

Nom :

Saisissez le nom à donner au périphérique de surveillance réseau.

Se reporter à


- *Configuration d'un récepteur de trap SNMP (page récepteur de trap SNMP), page 158*

14.14.2

Configuration d'un récepteur de trap SNMP (page récepteur de trap SNMP)



Fenêtre principale > **Périphériques** > Développez 

Pour configurer le SNMP trap receiver :

1. Cliquez sur  pour afficher la page **Récepteur de trap SNMP**.
2. Sélectionnez les paramètres appropriés.

Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Page Récepteur de trap SNMP.

Fenêtre principale > **Périphériques** > Développer  > Développer 
Permet de sélectionner des dispositifs à surveiller et de sélectionner des OID de traps SNMP qui déclenchent un événement pour les dispositifs sélectionnés lorsqu'ils sont reçus.



Remarque!

Vous devez introduire l'adresse IP du Bosch Video Management System Management Server comme récepteur de trap dans les dispositifs que vous souhaitez surveiller.

Périphériques émetteurs de trap SNMP

Permet de définir la plage d'adresses IP des dispositifs réseau surveillés. Pour surveiller un dispositif particulier, saisissez l'adresse IP correspondante dans la cellule **Début**.

Soyez attentifs lorsque vous changez ces adresses. Si vous saisissez une adresse erronée, la surveillance réseau de ce dispositif s'arrête.

Règles de filtre de trap SNMP



Permet de saisir les OID et les valeurs correspondantes. Vous pouvez utiliser des caractères génériques tels que * et ? pour étendre la portée du filtre. Si vous saisissez des OID et des valeurs sur plus d'une ligne, un événement ne sera déclenché que si toutes ces règles de filtre sont respectées simultanément. Vous pouvez saisir une expression régulière entre {} dans les deux colonnes. Si des caractères figurent en dehors des crochets, l'expression régulière n'est pas évaluée.

Afficher journal trap

Cliquez sur ce bouton pour afficher la boîte de dialogue **Journal trap SNMP** autorisant le traçage des OID de trap SNMP.

14.14.3

Boîte de dialogue Journal trap SNMP

Fenêtre principale > **Périphériques** > Développez  > Développez  > Sélectionnez un récepteur de trap SNMP génériques > Cliquez sur **Afficher journal trap**

Permet de tracer les OID d' interruptions SNMP. Vous pouvez recevoir des interruptions de tous les périphériques de votre réseau ou uniquement des périphériques sélectionnés. Vous pouvez filtrer les traps à recevoir et vous pouvez ajouter les OID et les valeurs des traps sélectionnés au tableau **Règles de filtre de trap SNMP**.

Démarrer/Pause

Cliquez sur ces boutons pour lancer ou arrêter le traçage.

Uniquement traps de l'émetteur

Saisissez l'adresse IP ou le nom DNS d'un périphérique. Seuls les traps de ce périphérique sont tracés.

Uniquement traps contenant

Introduisez une chaîne qu'un trap peut contenir. Vous pouvez utiliser * et ? en tant que caractères génériques. Les chaînes entre {} sont considérées comme des expressions rationnelles. Seuls les traps contenant une telle chaîne sont tracés.

Traps reçus

Affiche les traps reçus par traçage.



Cliquez ici pour supprimer toutes les entrées du champ **Traps reçus**.

Détails des traps

Affiche les données des traps. Vous pouvez copier l'OID et la valeur dans le tableau **Règles de filtre de trap SNMP**.

Se reporter à

– *Configuration d'un récepteur de trap SNMP (page récepteur de trap SNMP), page 158*

14.15



Page Attribution de clavier

Fenêtre principale > **Périphériques** > Développez  > 

Permet d'ajouter un clavier KBD-Universal XF (connecté à un poste de commande BVMS) ou un clavier Bosch IntuiKey (connecté à un poste de commande BVMS ou à un décodeur).

Pour ajouter un clavier de vidéosurveillance :

Remarque : pour ajouter un clavier, vous devez ajouter un poste de commande.

1. Développez , cliquez sur .
La page correspondante s'affiche.
2. Cliquez sur **Ajouter un clavier**.
Une nouvelle ligne est ajoutée au tableau.
3. Dans le champ approprié de la colonne **Type de clavier**, sélectionnez le type de clavier souhaité :
Clavier IntuiKey
KBD-Universal XF Keyboard
4. Dans le champ approprié de la colonne **Connexion**, sélectionnez le poste de commande connecté au clavier.
5. Définissez les paramètres appropriés.
Le clavier est ajouté au système.

Ajouter un clavier

Cliquez sur ce bouton pour ajouter une ligne au tableau, pour la configuration d'un clavier.

Supprimer un clavier

Cliquez sur ce bouton pour supprimer la ligne sélectionnée.

Type de clavier



Affiche le type de clavier connecté à votre poste de commande ou à votre décodeur.

Cliquez sur une cellule pour sélectionner le type de clavier requis.

- **IntuiKey**
Sélectionnez ce type si vous avez branché un clavier IntuiKey de Bosch.
- **KBD-Universal XF Keyboard**
Sélectionnez ce type si vous avez relié un clavier KBD-Universal XF.

Connexion

Dans une cellule, sélectionnez le périphérique connecté à votre clavier. Si vous sélectionnez

un poste de commande, le clavier est également ajouté à la page  > .

Port

Dans une cellule, sélectionnez le port COM souhaité.

Débit en bauds

Dans une cellule, sélectionnez la vitesse maximale (en bits par seconde - bps) à laquelle les données doivent être transmises via ce port. Il s'agit généralement de la vitesse maximale prise en charge par l'ordinateur ou le périphérique avec lequel vous communiquez.

Bits de données

Affiche le nombre de bits de données à utiliser pour chaque caractère transmis et reçu.

Bits d'arrêt

Affiche l'intervalle de temps entre chaque caractère transmis (lorsque le temps est mesuré en bits).

Parité

Affiche le type de contrôle d'erreur que vous souhaitez utiliser pour le port sélectionné.



Type de port

Affiche le type de connexion utilisée pour relier le clavier numérique IntuiKey de Bosch au poste de commande.

Se reporter à

- Configuration d'un décodeur pour une utilisation avec un clavier numérique IntuiKey de Bosch, page 148
- Configuration d'un clavier numérique IntuiKey de Bosch (page des paramètres) (poste de commande), page 140
- Configuration d'un clavier numérique IntuiKey de Bosch (décodeur), page 148

14.16**Page Modules E/S**



Fenêtre principale > **Périphériques** > Développez  > 
 Permet d'ajouter ou de configurer un module E/S.
 Actuellement, seuls les dispositifs ADAM sont pris en charge.

Se reporter à

- Configuration d'un module E/S, page 161

14.16.1**Ajout manuel d'un module E/S**

Pour ajouter un module E/S :

1. Développez  , cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Ajouter un nouveau périphérique ADAM**.
 La boîte de dialogue **Ajouter un nouvel ADAM** s'affiche.
2. Saisissez l'adresse IP du dispositif.
3. Sélectionnez le type de dispositif.
 La page correspondante s'affiche.
4. Le cas échéant, cliquez sur l'onglet **ADAM** pour modifier les noms d'affichage des entrées.
5. Le cas échéant, cliquez sur l'onglet **Nom** pour modifier les noms d'affichage des relais.

**Remarque!**

Vous pouvez également lancer une recherche sur les dispositifs ADAM (**Rechercher les périphériques ADAM**). Les adresses IP des dispositifs sont détectées. Le cas échéant, le type de dispositif est présélectionné. Vous devez confirmer cette présélection.

14.16.2**Configuration d'un module E/S**

Fenêtre principale > **Périphériques** > Développez  > Développez  > 
Pour configurer un module E/S :

**Remarque!**

Évitez de modifier le type de dispositif.
 Lorsque vous réduisez le nombre d'entrées ou de relais, toutes les données de configuration des entrées ou des relais supprimés sont supprimées.

1. Cliquez sur l'onglet **ADAM**.
2. Dans la liste **Type ADAM :**, sélectionnez le type de périphérique approprié.
3. Cliquez sur l'onglet **Entrées**.

4. Dans la colonne **Nom**, modifiez le nom affiché d'une entrée, le cas échéant.
5. Cliquez sur l'onglet **Relais**.
6. Dans la colonne **Relais**, modifiez le nom d'un relais, le cas échéant.

Pour changer une adresse IP :

1. Dans l'arborescence des dispositifs, cliquez avec le bouton droit sur un dispositif ADAM.
 2. Sélectionnez **Modifier l'adresse réseau**.
 3. Saisissez la nouvelle adresse IP, puis cliquez sur **OK**.
 4. Activez la configuration.
- ⇒ La nouvelle adresse IP est utilisée pour accéder au dispositif.

Se reporter à

– Page Modules E/S, page 161

14.16.3

Page ADAM

Fenêtre principale > **Périphériques** > Développez  >  >  > Onglet **ADAM**

Affiche des informations sur le périphérique ADAM sélectionné.

Permet de modifier le nom affiché d'un périphérique ADAM.

Type ADAM :

Sélectionnez le type de périphérique approprié.

Total entrées :

Affiche le nombre total d'entrées disponibles avec ce type de périphérique.

Total des relais/sorties :

Affiche le nombre total de relais disponibles avec ce type de périphérique.

14.16.4

Page Entrées

Fenêtre principale > **Périphériques** > Développez  >  >  > Onglet **Entrées**

Permet de modifier les noms affichés des entrées du périphérique ADAM sélectionné.

Numéro

Affiche le numéro logique de l'entrée.

Nom

Cliquez sur une cellule pour modifier le nom affiché d'une entrée.

14.16.5

Page Relais

Fenêtre principale > **Périphériques** > Développez  >  >  > Onglet **Relais**

Permet de modifier les noms affichés des relais du périphérique ADAM sélectionné.

Numéro

Cliquez sur une cellule pour modifier le numéro logique d'un relais.

Nom

Saisissez le nom affiché du relais.

14.17

Page Émulation CCL Allegiant

Fenêtre principale > **Périphériques** > Développez  > 

Permet d'activer l'émulation CCL Allegiant.

La section *Commandes Allegiant CCL prises en charge dans BVMS*, page 62 répertorie les commandes CCL prises en charge dans Bosch Video Management System.

Remarque :

Ne configurez pas l'émulation CCL Allegiant et un périphérique Allegiant sur le même port COM. Si le même port COM est configuré pour les deux périphériques, le périphérique Allegiant prévaut. L'échec de l'accès au périphérique d'émulation CCL Allegiant entraîne l'affichage du message correspondant.

Pour résoudre ce problème, le serveur doit disposer de deux ports COM différents, ou bien vous devez connecter le périphérique Allegiant à un autre ordinateur.

Activer l'émulation CCL Allegiant

Cochez cette option pour activer l'émulation.

Débit en bauds

Sélectionnez le débit de transmission en bits/s.

Bits d'arrêt

Sélectionnez le nombre de bits d'arrêt par caractère.

Vérification de la parité

Sélectionnez le type de Vérification de la parité.

Prise de contact

Sélectionnez la méthode souhaitée pour le contrôle du flux.

Modèle

Sélectionnez le modèle Allegiant que vous voulez émuler.



Se reporter à

– *Configuration d'une émulation CCL Allegiant*, page 164

14.17.1

Ajout manuel d'une émulation CCL Allegiant

Pour ajouter une émulation CCL Allegiant :

1. Développez  , cliquez sur  .
L'onglet **Émulation CCL Allegiant** s'affiche.
2. Cliquez sur l'option **Activer l'émulation CCL Allegiant** pour la sélectionner.
3. Sélectionnez les paramètres appropriés.
Le service d'émulation Allegiant CCL est lancé sur le Management Server.

14.17.2

Commandes Allegiant CCL

Vous pouvez utiliser des commandes CCL pour commuter des encodeurs ou caméras IP en décodeurs IP, tous deux configurés dans BVMS. Vous ne pouvez pas utiliser des commandes CCL pour contrôler directement des caméras analogiques ou la matrice Allegiant elle-même.

L'émulation CCL Allegiant lance un service BVMS interne qui traduit les commandes CCL de la matrice dans BVMS. Vous configurez un port COM du Management Server pour qu'il écoute ces commandes CCL. L'émulation CCL facilite l'échange de dispositifs Allegiant existants avec Bosch Video Management System ou permet d'utiliser Bosch Video Management System avec des applications compatibles avec les commandes CCL Allegiant. L'ancien matériel Allegiant configuré dans BVMS ne peut pas être contrôlé à l'aide de ces commandes.

14.17.3 Configuration d'une émulation CCL Allegiant

Fenêtre principale > **Périphériques** > Développez  >

Vous avez besoin du guide de l'utilisateur de CCL pour utiliser les commandes CCL. Ce guide est disponible dans le catalogue de produits en ligne dans la section documentation de chaque matrice LTC Allegiant.

Les *Commandes Allegiant CCL prises en charge dans BVMS*, page 62 répertorient les commandes CCL prises en charge par Bosch Video Management System.

Pour configurer une émulation CCL Allegiant :

1. Cliquez sur **Activer l'émulation CCL Allegiant**.
 2. Configurez les paramètres de communication en fonction des besoins.
- Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Se reporter à

- *Page Émulation CCL Allegiant*, page 162

14.18 Page du service vidéo mobile

Fenêtre principale > **Périphériques** > 

Permet d'ajouter une ou plusieurs entrée(s) de service de transcodage à votre BVMS. Ce service de transcodage adapte le flux vidéo à partir d'une caméra configurée dans BVMS à la bande passante disponible pour le réseau. Cette option permet aux clients vidéo mobiles (iPhone, iPad ou client Web, par exemple) de recevoir des données vidéo en modes Temps réel ou Lecture, via des connexions réseau non fiables, avec bande passante limitée.

Se reporter à

- *Ajout manuel d'entrées Mobile Video Service*, page 165

14.18.1 Service vidéo mobile

Mobile Video Service transcode des flux vidéo depuis la source vers la bande passante disponible des clients connectés. Les interfaces de Mobile Video Service sont conçues pour prendre en charge des clients sur plusieurs plates-formes, comme par exemple des périphériques mobiles (iOS ; iPad, iPhone) et un client Windows Internet Explorer HTML. Mobile Video Service est basé sur le service d'informations Microsoft Internet.

Un service mobile peut servir plusieurs clients de manière synchronisée.

Pour les limites, reportez-vous aux fiches techniques et à la note technique Mobile Video Service disponibles dans le catalogue de produits en ligne pour BVMS.

Service d'informations Internet

Configurez les paramètres du service d'informations Internet sur l'ordinateur où vous comptez installer SVM pour BVMS.

Instructions d'installation

Vous ne pouvez pas ajouter un Mobile Video Service (MVS) dans la Configuration Client lorsque l'heure n'est pas synchronisée entre l'ordinateur de la Configuration Client et l'ordinateur du Mobile Video Service. Assurez-vous que l'heure est synchronisée entre les ordinateurs concernés.

Installez et configurez le service d'informations Internet (SII) avant d'installer Mobile Video Service. Si le SII n'est pas installé, la configuration BVMS pour l'installation de Mobile Video Service est abandonnée.

Vous pouvez sélectionner le composant Mobile Video Service pour l'installation pendant la configuration de BVMS.

Vous ne pouvez pas installer VRM et Mobile Video Service sur le même ordinateur.

Nous vous déconseillons d'installer Mobile Video Service et Management Server sur le même ordinateur.

L'Application mobile vous permet d'effectuer les tâches suivantes :


- Affichage de données vidéo
 - En temps réel
 - Lecture
- Surveillance du réseau et du serveur

Se reporter à

- *Ajout manuel d'entrées Mobile Video Service, page 165*

14.18.2

Ajout manuel d'entrées Mobile Video Service

Fenêtre principale > **Périphériques** > Cliquer avec le bouton droit de la souris sur  > Cliquer sur **Ajouter un service vidéo mobile**

Vous pouvez ajouter une ou plusieurs entrées Mobile Video Service à BVMS.

Pour effectuer un ajout :

1. Saisissez l'URI de votre Mobile Video Service.
 2. Cliquez sur **OK**.
- ⇒ Désormais, Mobile Video Service et Management Server se connaissent et le Mobile Video Service peut recevoir des données de configuration depuis Management Server.

Boîte de dialogue Ajouter un service vidéo mobile

URI

Saisissez l'URI de votre Mobile Video Service. Suivez les règles de syntaxe de l'exemple :

<https://www.MyDomain.org/mvs>

Le début de l'entrée doit toujours commencer par `https://`, même si vous n'avez pas configuré un accès chiffré à votre serveur Web.

14.19

Page Centrales d'intrusion

Fenêtre principale > **Périphériques** > Développez  > 

Permet d'ajouter et de configurer des centrales d'intrusion Bosch. Le dispositif doit être connecté et disponible.

Une fois les centrales d'intrusion ajoutées, les zones et points, les portes et les relais sont affichés hiérarchiquement dans l'arborescence des dispositifs.

Vous pouvez supprimer ou renommer la centrale, chaque zone, chaque point, chaque porte et chaque relais.

Si la configuration de la centrale d'intrusion a été modifiée, vous devez effectuer une nouvelle recherche du dispositif pour afficher les modifications dans BVMS.



Remarque!

Tous les événements d'alarme pouvant se produire à un moment donné sont automatiquement configurés en tant qu'alarme BVMS.

Exemple : alarme incendie



Remarque!



Si une porte n'est pas affectée à un point dans la configuration d'une centrale d'intrusion ajoutée à un système BVMS, les alarmes provenant de cette porte ne déclenchent pas d'événements BVMS et, par conséquent, pas d'alarme BVMS.

14.19.1

Ajout manuel d'une centrale d'intrusion

Fenêtre principale > **Périphériques** > Développez  > Cliquer avec le bouton droit de la souris sur  > Commande **Ajouter une centrale**
Permet d'ajouter une centrale d'intrusion Bosch.

Pour ajouter une centrale d'intrusion :

1. Développez , cliquez sur  avec le bouton droit de la souris, puis cliquez sur **Ajouter une centrale**.
La boîte de dialogue **Ajouter la centrale d'intrusion** s'affiche.
2. Entrez les valeurs appropriées.
3. Cliquez sur **OK**.
La centrale d'intrusion est ajoutée au système.

Boîte de dialogue Ajouter la centrale d'intrusion

Adresse réseau

Saisissez l'adresse IP du dispositif.

Port réseau

Sélectionnez le numéro de port configuré sur le dispositif.

Code d'automatisation

Saisissez le code d'accès nécessaire à l'authentification sur le dispositif.



14.19.2

Page Paramètres

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > onglet **Paramètres**
Permet de modifier les paramètres de connexion de la centrale d'intrusion.

14.20

Page des systèmes de contrôle d'accès

Fenêtre principale > **Périphériques** > Développez  >  >
Permet d'ajouter et de configurer des systèmes de contrôle d'accès Bosch. Le dispositif doit être connecté et disponible. Une fois que vous avez ajouté un système de contrôle d'accès, le contrôleur, les entrées, les lecteurs et les portes s'affichent hiérarchiquement dans l'arborescence des dispositifs.
Vous pouvez supprimer ou renommer le contrôleur, les entrées, les lecteurs et les portes sur la page **Cartes et structure**.
Si la configuration ou la hiérarchie des contrôleurs, lecteurs ou portes du système de contrôle d'accès a été modifiée, vous devez effectuer une nouvelle recherche du dispositif pour afficher les modifications dans BVMS.

Certificat HTTPS pour Client

Afin de sécuriser la connexion entre le système de contrôle d'accès et BVMS, vous devez exporter un certificat client depuis le système de contrôle d'accès, puis l'importer dans BVMS. Ce processus est décrit dans la section **Certificat HTTPS pour Client** de la documentation du système de contrôle d'accès.



Remarque!


Si le certificat n'est pas ajouté, les systèmes ne pourront pas échanger d'informations entre eux.

14.20.1

Ajout d'un système de contrôle d'accès

Fenêtre principale > **Périphériques** > Développez  > 

Pour ajouter un système de contrôle d'accès :

1. Cliquez avec le bouton droit de la souris sur .
2. Cliquez sur **Ajouter un système de contrôle d'accès**.

La boîte de dialogue **Ajouter un système de contrôle d'accès** s'affiche.

Remarque : Lors de l'ajout d'un système de contrôle d'accès, des portes, des lecteurs, des entrées et des relais configurés sont répertoriés dans l'arborescence de la page **Cartes et structure**.

Boîte de dialogue Ajouter un système de contrôle d'accès

Nom d'hôte / port HTTPS

Entrez le nom d'hôte du dispositif. Si nécessaire, modifiez le numéro de port.

Nom d'utilisateur

Affiche le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le dispositif.

Pour tester la connexion :


1. Cliquez sur Se connecter.
BVMS Configuration Client tente de se connecter au système de contrôle d'accès et de récupérer les informations pertinentes.
2. Cliquez sur OK.
Le système de contrôle d'accès est ajouté au système, selon les informations affichées.

14.20.2

Modification d'un système de contrôle d'accès

Fenêtre principale > **Périphériques** > Développez  >  > 

Pour modifier un système de contrôle d'accès :

1. Cliquez avec le bouton droit de la souris sur .
2. Cliquez sur **Modifier le système de contrôle d'accès**.
La boîte de dialogue **Modifier le système de contrôle d'accès** s'affiche.

14.20.3 Page Paramètres

Fenêtre principale > **Périphériques** > Développez  >  >  > Onglet **Paramètres**

Permet de modifier les paramètres de connexion du système de contrôle d'accès.

14.21 Page Video Analytics

Fenêtre principale > > **Périphériques** > Développez  > 

Vous permet d'ajouter des dispositifs Video Analytics, Person Identification (PID) et LPR.

14.21.1 Page Paramètres Video Analytics

Fenêtre principale > > **Périphériques** > Développez  > Développez  >  **Video Analytics** > page **Paramètres Video Analytics**

Vous pouvez ajouter un dispositif Video Analytics basée sur le serveur.

Les identifiants et le chemin d'installation de l'application de la visionneuse d'analyses utilisée pour le dispositif Video Analytics doivent être disponibles.

Adresse réseau

Saisissez l'adresse IP du dispositif Video Analytics. Aucun nom DNS n'est autorisé.

Nom d'utilisateur

Saisissez le nom d'utilisateur comme configuré sur le dispositif Video Analytics.

Mot de passe

Saisissez le mot de passe comme configuré sur le dispositif d'analyse basée sur le serveur.

Chemin visionneuse Analytics

Saisissez le chemin d'accès relatif d'installation de l'application de la visionneuse d'analyses. Le chemin d'accès est relatif à C:\Program Files (x86)\ sur l'ordinateur sur lequel l'application de la visionneuse est utilisée.


Exemple : l'application de la visionneuse d'analyses (*AnalyticsViewer.exe*) est installée dans le répertoire suivant :

```
C:\Program Files (x86)\VideoAnalytics\
```

Configurez le chemin suivant dans le champ **Chemin visionneuse Analytics** :



```
VideoAnalytics\AnalyticsViewer.exe
```

14.21.2 Ajout d'un dispositif Video Analytics

Fenêtre principale > > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Commande **Ajouter un dispositif de Video Analytics** > Boîte de dialogue **Ajouter un dispositif de Video Analytics**

Lorsque vous ajoutez un dispositif d'analyse basée sur le serveur, vous saisissez les identifiants du nouveau dispositif.

Pour ajouter un dispositif d'analyse basée sur le serveur :

1. Développez , cliquez avec le bouton droit de la souris sur  puis cliquez sur **Ajouter un dispositif de Video Analytics**.
La boîte de dialogue **Ajouter un dispositif de Video Analytics** s'affiche.
2. Entrez les valeurs appropriées.

3. Cliquez sur **OK**.
Le dispositif est ajouté au système.

Boîte de dialogue Ajouter un dispositif de Video Analytics

Adresse réseau

Saisissez l'adresse IP du dispositif Video Analytics. Aucun nom DNS n'est autorisé.

Nom d'utilisateur

Saisissez le nom d'utilisateur comme configuré sur le dispositif Video Analytics.

Mot de passe

Saisissez le mot de passe comme configuré sur le dispositif d'analyse basée sur le serveur.

14.21.3

Page Person Identification device

Fenêtre principale > > **Périphériques** > Développez  > Développez  >  Page Person Identification device

Vous permet d'ajouter un dispositif Person Identification. Le dispositif doit être connecté et disponible. Vous pouvez ajouter des caméras à votre dispositif Person Identification et configurer des événements et des alarmes Person Identification.

Groupes de personnes

Dans l'onglet **Groupes de personnes**, vous pouvez ajouter et configurer des groupes de personnes.

Caméras

Dans l'onglet **Caméras**, vous pouvez ajouter des caméras à votre dispositif d'Person Identification. Les caméras ajoutées apparaissent dans une liste.

Remarque : Commencez par ajouter les caméras appropriées à l'arborescence logique.

14.21.4

Ajout d'un dispositif d'identification de personne (PID)



Remarque!

En cas de panne d'un serveur central Management Server, vous devez restaurer la configuration BVMS et le certificat Bosch VMS CA. Dans le cas contraire, vous ne pouvez pas utiliser un PID existant sans réinitialisation, ce qui entraîne la suppression de toutes les personnes enregistrées.

Nous vous recommandons de créer une sauvegarde de la configuration BVMS et du certificat Bosch VMS CA.

Lors de l'ajout d'un dispositif Person Identification, assurez-vous que le certificat affiché dans la boîte de dialogue **Ajouter le périphérique d'identification de personne** correspond au PID que vous souhaitez ajouter.


À compter de la version 10.1 de BVMS, vous pouvez ajouter plusieurs dispositifs PID.

Le premier dispositif PID que vous ajoutez est le dispositif principal connecté au système BVMS. Ce premier dispositif PID établit la connexion avec les autres dispositifs PID et la base de données de la personne y est stockée.

Remarque : Avant de supprimer le premier dispositif PID, vous devez supprimer tous les autres dispositifs PID configurés.

Pour ajouter un dispositif Person Identification :

1. Développez  .

2. Cliquez avec le bouton droit de la souris sur .
3. Cliquez sur **Ajouter le périphérique d'identification de personne**.
La boîte de dialogue **Ajouter le périphérique d'identification de personne** s'affiche.
4. Entrez les valeurs appropriées.
5. Cliquez sur **Afficher le certificat...** pour vérifier si le certificat correspond au PID.
6. Pour confirmer, cliquez sur **OK**.
7. Cliquez sur **OK**.
Le dispositif est ajouté au système.

Boîte de dialogue Ajouter le périphérique d'identification de personne

Adresse réseau

Saisissez l'adresse IP du dispositif.

Numéro de port

Saisissez le numéro de port du dispositif.

Se reporter à

- *Restauration de l'accès à un PID après une panne du serveur Management Server, page 170*
- *Pour exporter des données de configuration :, page 95*

14.21.5

Page PID

Fenêtre principale > **Périphériques** > Développez  > Développez  > 
 Dispositif Person Identification >  Page PID

Connexion

L'onglet **Connexion** affiche l'adresse réseau et le numéro de port de votre dispositif Person Identification. Les paramètres de connexion d'un dispositif Person Identification sont en lecture seule.

14.21.6

Restauration de l'accès à un PID après une panne du serveur Management Server

Remarque!

En cas de panne d'un serveur central Management Server, vous devez restaurer la configuration BVMS et le certificat Bosch VMS CA. Dans le cas contraire, vous ne pouvez pas utiliser un PID existant sans réinitialisation, ce qui entraîne la suppression de toutes les personnes enregistrées.

Nous vous recommandons de créer une sauvegarde de la configuration BVMS et du certificat Bosch VMS CA.

Pour plus d'informations sur la sauvegarde de la configuration BVMS, voir *Pour exporter des données de configuration :, page 78*. Les certificats sont gérés en dehors de BVMS dans l'application Windows de **gestion des certificats de l'ordinateur**.



**Remarque!**

Les certificats contiennent des informations confidentielles. Pour les protéger, procédez comme suit :

- Définissez un mot de passe fort.
- Stockez le certificat dans une zone à accès restreint, par exemple, un serveur non public.
- Veillez à ce que seul le personnel autorisé puisse accéder au certificat.

Pour créer une sauvegarde du certificat Bosch VMS CA :

1. Ouvrez l'application Windows de **gestion des certificats d'ordinateurs**.
2. Dans le dossier des **autorités de certification racine de confiance**, sélectionnez le certificat Bosch VMS CA.
3. Exportez le certificat à l'aide de la clé privée en sélectionnant **Oui, exporter la clé privée**.
4. Utilisez le format d'échange d'informations personnelles.
5. Définissez un mot de passe fort.
6. Enregistrez le certificat en tant que fichier PFX.

Pour restaurer l'accès au PID à partir d'un serveur Management Server BVMS nouvellement installé :

1. Ouvrez l'application Windows de **gestion des certificats d'ordinateurs**.
2. Importez le fichier PFX contenant le certificat Bosch VMS CA dans le dossier des **autorités de certification racine de confiance** du nouveau Management Server. Incluez toutes les propriétés étendues.
3. Importez la sauvegarde de configuration BVMS.




Se reporter à

- *Exportation de données de configuration, page 95*

14.21.7**Ajout de caméras à un dispositif d'identification de la personne (PID)**

Vous pouvez ajouter des caméras à votre dispositif Person Identification, s'il est déjà ajouté à l'arborescence logique.

Pour ajouter des caméras à un dispositif Person Identification :

1. Développez .
2. Développez .
3. Cliquez sur .
4. Cliquez sur l'onglet **Caméras**.
5. Faites glisser les caméras appropriées de la fenêtre **Arborescence Logique** vers la fenêtre **Caméras**.

Ou

double-cliquez sur les caméras appropriées dans la fenêtre **Arborescence Logique**.

Les caméras sont ajoutées à votre dispositif Person Identification et elles apparaissent dans la liste **Caméras**.

14.21.8 Configuration des paramètres de caméra pour les alarmes d'identification de la personne

Pour chaque caméra disponible, vous pouvez configurer des paramètres de caméra pour les alarmes Person Identification afin de réduire les fausses alarmes.

Paramètre de la caméra



Nom	Informations valeur	Description
Probabilité de seuil (%)	Par défaut : 55 % Min : 0 % Max : 100 %	Probabilité minimale d'identification positive d'un visage pour la génération d'un événement Person Identification.
Taille du visage (%)	Par défaut : 7,5 % Min : 5 % Max : 100 %	Taille minimale d'un visage pour la détection par rapport à la taille de l'ensemble de l'image vidéo.
Nombre d'images min.	Par défaut : 4 Min. : 1	Nombre minimum d'images vidéo consécutives dans lesquels un visage doit apparaître pour être détecté.
Images à analyser (%)	Par défaut : 100 % Min : 10 % Max : 100 %	Pourcentage d'images analysées pour identifier les personnes. La valeur 50 % signifie que chaque deuxième image est analysée.

14.21.9 Configuration des groupes de personnes

Fenêtre principale > > **Périphériques** > Développez



Pour configurer des groupes de personnes :

- Sélectionnez l'onglet **Groupes de personnes**.
- Cliquez sur  pour ajouter un nouveau groupe de personnes.
- Entrez les valeurs appropriées.
- Cliquez sur  pour supprimer un groupe de personnes.



Remarque!

Vous ne pouvez ni supprimer ni modifier les valeurs du groupe par défaut.

Tableau des groupes de personnes

Groupe de personnes	Saisissez le nom du groupe de personnes.
---------------------	--

Couleur de l'alarme	Double-cliquez pour sélectionner la couleur d'alarme.
Titre de l'alarme	Saisissez le titre de l'alarme qui sera affiché dans Operator Client.

Pour modifier les valeurs du tableau de groupes de personnes :

1. Double-cliquez sur le champ de tableau approprié.
2. Modifiez la valeur.

Priorité d'alarme

Vous pouvez définir la priorité d'alarme pour les alarmes Person Identification sur la page **Alarmes**.



Remarque!

Vous pouvez définir différentes priorités d'alarme pour chaque caméra du groupe de personnes approprié.
 Vous pouvez également modifier la priorité d'alarme du groupe de personnes par défaut.

Se reporter à

– Page Alarmes, page 322

14.21.10

Ajout d'un périphérique LPR

Fenêtre principale > > **Périphériques** > Développez  >  > 

Les dispositifs LPR identifient et détectent les numéros de plaque de licence. Vous pouvez configurer des événements et des alarmes LPR en conséquence.


Si le dispositif LPR doit détecter des numéros de plaque de licence spécifiques, vous devez d'abord configurer une liste de numéros de plaque de licence directement sur le dispositif LPR. Pour plus d'informations, reportez-vous à la documentation utilisateur du dispositif.



Remarque!

Le dispositif doit être connecté et disponible.
 BVMS se connecte uniquement si l'authentification est activée sur le dispositif LPR et si le nom d'utilisateur et le mot de passe sont spécifiés. Le nom d'utilisateur et le mot de passe ne peuvent pas être vides.

Pour ajouter un périphérique LPR :

1. Cliquez avec le bouton droit de la souris sur  .
2. Cliquez sur **Ajouter un périphérique LPR**.
 La boîte de dialogue **Ajouter un périphérique LPR** s'affiche.
3. Entrez les valeurs appropriées.
4. Cliquez sur **Authentifier**.
5. Cliquez sur **OK**.
 Le dispositif est ajouté au système.



Remarque!

Vous devez spécifier l'adresse IP de BVMSManagement Server dans la configuration du dispositif LPR. Dans le cas contraire, le système BVMS ne récupère pas les événements de ce dispositif LPR.

Boîte de dialogue Ajouter un périphérique LPR**Adresse réseau**

Saisissez l'adresse IP du dispositif.

Numéro de port

Saisissez le numéro de port du dispositif.

Nom d'utilisateur

Saisissez le nom d'utilisateur valide pour l'authentification sur le dispositif.

Mot de passe



Saisissez un mot de passe valide pour vous authentifier sur le dispositif.

Authentifier

Permet de vous authentifier sur le dispositif avec les identifiants saisis précédemment.

14.22

Page Périphériques VRM

Fenêtre principale > **Périphériques** > Développer  > 

Permet d'ajouter et de configurer des périphériques VRM. Un périphérique VRM a au moins besoin d'un encodeur, d'un périphérique iSCSI, d'un LUN affecté au périphérique iSCSI et d'une zone de stockage. Consultez les notes de mise à jour et la fiche technique pour connaître les versions actuelles du micrologiciel.

**Remarque!**

Après avoir ajouté un périphérique iSCSI et ses encodeurs respectifs à BVMS, vous devez ajouter l'IQN de chaque encodeur à ce périphérique iSCSI (valable pour certains types de périphérique iSCSI).

Pour plus d'informations, voir *Configuration d'un périphérique iSCSI, page 199*.

**Remarque!**

Assurez-vous que l'heure de l'ordinateur VRM est synchronisée avec Management Server. À défaut, vous risquez de perdre les enregistrements.

Configurez le logiciel du serveur de synchronisation sur Management Server. Sur l'ordinateur VRM, configurez l'adresse IP du Management Server comme serveur de synchronisation par les procédures Windows standard.

Se reporter à

- *Configuration du multicast, page 242*
- *Synchronisation de la configuration BVMS, page 184*
- *Page Paramètres du VRM, page 178*
- *Page Zone, page 185*
- *Page de périphérique iSCSI, page 194*
- *Modification du mot de passe d'un périphérique VRM, page 180*

14.22.1

Ajout de dispositifs VRM via un balayage

Fenêtre principale > **Périphériques** >

Vous avez besoin, dans votre réseau, d'un service VRM qui s'exécute sur un ordinateur et d'un périphérique iSCSI.




Remarque!

Si vous ajoutez un périphérique iSCSI sans cibles ni LUN configurés, lancez une configuration par défaut et ajoutez l'IQN de chaque encodeur à ce périphérique iSCSI. Si vous ajoutez un périphérique iSCSI avec des cibles et des LUNs préconfigurés, ajoutez l'IQN de chaque encodeur à ce périphérique iSCSI.

Pour plus d'informations, voir *Configuration d'un périphérique iSCSI*, page 199.

Pour ajouter des dispositifs VRM via un balayage :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Rechercher les périphériques VRM**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Cochez les boîtes de dialogue des dispositifs que vous souhaitez ajouter.
3. Dans la liste **Rôle**, sélectionnez le rôle souhaité.
Il varie en fonction du type actuel du dispositif VRM.
Si vous sélectionnez **Mis en miroir** ou **Basculement**, l'étape de configuration suivante est également nécessaire.
4. Dans la liste **Rôle**, sélectionnez le rôle souhaité.
Il varie en fonction du type actuel du dispositif VRM.
5. Cliquez sur **Suivant >>**
6. Dans la liste **VRM maître**, sélectionnez le VRM maître pour le VRM redondant ou de basculement sélectionné.
7. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
8. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit sur ce champ et sélectionnez **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions qui ont abouti sont indiquées par le symbole




les connexions qui ont échoué sont indiquées par le symbole



9. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.

Remarque : Tous les dispositifs VRM sont ajoutés avec une connexion sécurisée par défaut.

Pour modifier une connexion sécurisée/non sécurisée :

1. Cliquez avec le bouton droit de la souris sur .
2. Cliquez sur **Modifier périphérique VRM**.
La boîte de dialogue **Modifier périphérique VRM** s'affiche.
3. Sélectionnez la case **Connexion sécurisée**.
Le port utilisé change automatiquement sur le port HTTPS.
Ou bien
désélectionnez la case **Connexion sécurisée**.
Le port utilisé change automatiquement sur le port rcpp.

Se reporter à

- Ajout d'un dispositif, page 127
- Page Périphériques VRM, page 174
- Configuration d'un périphérique iSCSI, page 199
- Enregistrement double/de basculement, page 29

14.22.2**Ajout manuel d'un VRM primaire ou secondaire**

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur >

Cliquez sur **Ajouter VRM** > Boîte de dialogue **Ajouter VRM**

Permet d'ajouter un périphérique VRM. Vous pouvez sélectionner le type du périphérique et saisir les identifiants.

Vous ne pouvez en fait affecter un VRM de basculement à un VRM maître que lorsque les deux sont en ligne et authentifiés avec succès. Les mots de passe sont alors synchronisés.

Vous pouvez ajouter un dispositif VRM principal manuellement si vous connaissez son adresse IP et son mot de passe.

Pour ajouter un dispositif VRM principal :

1. Définissez les paramètres requis pour votre dispositif VRM.
2. Dans la liste **Type**, sélectionnez l'entrée **Principal**.
3. Cliquez sur **OK**.

Le dispositif VRM est ajouté.

Vous pouvez ajouter un dispositif VRM secondaire manuellement si vous connaissez son adresse IP et son mot de passe.

**Remarque!**

Pour configurer un VRM secondaire, vous devez d'abord installer les logiciels appropriés sur l'ordinateur souhaité. Exécutez Setup.exe, puis sélectionnez **VRM secondaire**.

Pour ajouter un dispositif VRM secondaire :

1. Définissez les paramètres requis pour votre dispositif VRM.
2. Dans la liste **Type**, sélectionnez l'entrée **Secondaire**.
3. Cliquez sur **OK**.

Le dispositif VRM est ajouté.

Vous pouvez à présent configurer le VRM secondaire comme n'importe quel VRM principal.

Boîte de dialogue Ajouter VRM**Nom**

Saisissez un nom d'affichage pour le dispositif.

Adresse réseau/Port

Saisissez l'adresse IP de votre périphérique.

Si la case **Connexion sécurisée** est sélectionnée, le port bascule automatiquement sur le port HTTPS.

Vous pouvez modifier le numéro de port, si aucun port par défaut n'est utilisé.

Type

Sélectionnez le type de périphérique souhaité.

Nom d'utilisateur

Saisissez un nom d'utilisateur pour l'authentification.

Mot de passe

Saisissez le mot de passe pour l'authentification.

Afficher le mot de passe

Cliquez sur cette option pour que le mot de passe soit visible.

Sécurité

La case **Connexion sécurisée** est sélectionnée par défaut si le protocole HTTPS est pris en charge.

**Remarque!**

Si vous effectuez une migration vers BVMS version 10,0 ou supérieure, la case **Connexion sécurisée** n'est pas sélectionnée par défaut et la connexion n'est pas sécurisée (rcpp).

Pour modifier une connexion sécurisée ou non sécurisée, utilisez la commande **Modifier périphérique VRM**, puis sélectionnez ou désélectionnez la case **Connexion sécurisée**.

Test

Cliquez sur ce bouton pour vérifier si le périphérique est connecté et si l'authentification a réussi.

Propriétés

Si nécessaire, changez les numéros de port du port HTTP et du port HTTPS. Ce processus n'est possible que lorsque vous ajoutez ou modifiez un VRM qui n'est pas connecté. Si le VRM est connecté, les valeurs sont récupérées et vous ne pouvez pas les modifier. La ligne du tableau **VRM maître** indique le périphérique sélectionné, le cas échéant.

Se reporter à


- *Modification d'un dispositif VRM, page 177*
- *Ajout manuel d'un VRM redondant, page 182*
- *Ajout manuel d'un VRM de basculement, page 181*

14.22.3**Modification d'un dispositif VRM**

Fenêtre principale > **Périphériques**

Vous permet de modifier un dispositif.

Pour modifier une connexion sécurisée/non sécurisée :

1. Cliquez avec le bouton droit de la souris sur  .
2. Cliquez sur **Modifier périphérique VRM**.
La boîte de dialogue **Modifier périphérique VRM** s'affiche.
3. Sélectionnez la case **Connexion sécurisée**.
Le port utilisé change automatiquement sur le port HTTPS.
Ou bien
désélectionnez la case **Connexion sécurisée**.
Le port utilisé change automatiquement sur le port rcpp.

**Remarque!**

Après une mise à niveau vers une version plus récente, nous vous recommandons de changer pour une connexion sécurisée.

Pour de plus amples informations sur le paramètre de la boîte de dialogue **Modifier périphérique VRM**, reportez-vous au chapitre Ajout manuel d'un VRM primaire ou secondaire.

Se reporter à

– *Ajout manuel d'un VRM primaire ou secondaire, page 176*

14.22.4 Page Paramètres du VRM

Fenêtre principale > **Périphériques** > Développez  >  > **Paramètres principaux** > **Paramètres du VRM**

Nom de l'initiateur du serveur

Affiche le nom de l'initiateur iSCSI de VRM Server.

14.22.5 Page SNMP

Fenêtre principale > **Périphériques** > Développez  > Développez  > **Réseau** > **SNMP**

1. Adresse SNMP hôte 2. Adresse SNMP hôte

VRM prend en charge le SNMP (Simple Network Management Protocol) pour la gestion et la surveillance des composants du réseau, et envoie des messages SNMP (traps) aux adresses IP. L'appareil prend en charge SNMP MIB II dans le code unifié. Si vous souhaitez envoyer des traps SNMP, saisissez ici les adresses IP d'une ou de deux cibles.

Certains événements sont envoyés uniquement sous forme de traps SNMP. Reportez-vous au fichier MIB pour obtenir des descriptions.

14.22.6 Page Comptes

Pour configurer la publication d'images ainsi que pour exporter une vidéo au format MP4, vous devez créer un compte dans lequel vous pouvez les enregistrer et les consulter. Il est possible de créer jusqu'à quatre (4) comptes.

Type

Sélectionnez le type de compte : **FTP** ou **Dropbox**.

Adresse IP

Saisissez l'adresse IP du serveur sur lequel vous souhaitez enregistrer les images.

Nom d'utilisateur

Saisissez le nom d'utilisateur pour le serveur.

Mot de passe

Indiquez le mot de passe qui permet d'accéder au serveur. Pour vérifier le mot de passe, cliquez sur le bouton **Vérifier** à droite.

Vérifier

Cliquez sur ce bouton pour vérifier le mot de passe.

Chemin

Saisissez le chemin d'accès exact de l'emplacement où vous souhaitez placer les images et la vidéo sur le serveur.

14.22.7 Page Avancé

Fenêtre principale > **Périphériques** > Développez  > Développez  > **Administration** > **Avancé**

Journalisation RCP+ / Débogage journalisation / Relecture journalisation / Journalisation VDP / Journalisation des performances

Activez les différents fichiers journaux pour le VRM Server et Configuration Manager.

Les fichiers journaux de VRM Server sont conservés sur l'ordinateur sur lequel VRM Server a été lancé. Ils peuvent être consultés ou téléchargés avec VRM Monitor.

Les fichiers journaux de Configuration Manager sont conservés localement dans le répertoire suivant :

%USERPROFILE%\My Documents\Bosch\Video Recording Manager\Log

Durée de conservation (en jours)

Spécifiez la durée de conservation des fichiers journaux, en jours.

Fichier de vidage de mémoire complet

N'activez cette case qu'en cas de besoin, par exemple, si l'équipe technique du Service clientèle vous demande un historique complet de la mémoire principale.

Prise en charge Telnet

Activez cette case si l'accès avec le protocole Telnet doit être pris en charge. N'activez cette case qu'en cas de besoin.



Remarque!

Une journalisation étendue nécessite un processeur extrêmement puissant, ainsi qu'un disque dur doté d'une capacité importante.

N'utilisez pas la journalisation étendue en fonctionnement continu.

14.22.8

Chiffrement d'un enregistrement pour VRM

L'enregistrement chiffré pour les encodeurs VRM n'est pas activé par défaut.

Vous devez activer l'enregistrement chiffré pour le VRM principal et le secondaire séparément.



Remarque!

Vous devez créer une clé de redondance (certificat de sauvegarde) avant d'activer l'enregistrement chiffré pour la première fois. Il suffit de créer une clé de redondance pour chaque module VRM.

En cas de perte de la clé de chiffrement normale, vous pouvez déchiffrer les enregistrements à l'aide de la clé de redondance.

Nous recommandons de conserver une copie de la clé de redondance dans un endroit sûr (par exemple, dans un coffre-fort).

Pour créer une clé de redondance :


1. Sélectionnez le dispositif VRM approprié.
2. Sélectionnez l'onglet **Administration**.
3. Sélectionnez l'onglet **Chiffrement de l'enregistrement**.
4. Cliquez sur **Clé de redondance**.
5. Sélectionnez un emplacement de magasin de certification.
6. Saisissez un mot de passe conforme aux exigences de complexité des mots de passe et confirmez.
7. Cliquez sur **Créer**.

La clé de redondance (certificat de sauvegarde) est créée.

Pour activer/désactiver l'enregistrement chiffré :

1. Sélectionnez le dispositif VRM approprié.
2. Sélectionnez l'onglet **Administration**.

3. Sélectionnez l'onglet **Chiffrement de l'enregistrement** .
4. Sélectionnez/désélectionnez la case à cocher **Activer l'enregistrement chiffré**.

5. Cliquez sur  .

Remarque : Le chiffrement est uniquement activé après la prochaine modification de bloc. Cette opération peut prendre un certain temps. Assurez-vous que les encodeurs peuvent chiffrer.

Pour vérifier que les encodeurs VRM peuvent chiffrer :

1. Sélectionnez le dispositif VRM approprié.
2. Sélectionnez l'onglet **Administration**.
3. Sélectionnez l'onglet **Chiffrement de l'enregistrement** .

Remarque : Vous pouvez également vous reporter à l'onglet **Monitoring** de VRM Monitor.




Remarque!

Tous les encodeurs VRM prenant en charge le chiffrement chiffrent automatiquement les enregistrements une fois le chiffrement activé dans VRM. Le chiffrement peut être désactivé pour un seul encodeur. Les encodeurs VSG chiffrent toujours, si le chiffrement est activé dans VRM.

Pour activer/désactiver l'enregistrement chiffré pour un seul encodeur VRM :

1. Sélectionnez l'encodeur VRM approprié.
2. Sélectionnez l'onglet **Enregistrement**.
3. Sélectionnez l'onglet **Gestion des enregistrements**.
4. Sélectionnez/désélectionnez la case **Chiffrement**.

5. Cliquez sur  .

14.22.9

Modification du mot de passe d'un périphérique VRM

Fenêtre principale > **Périphériques** > Développez  > 

Pour changer le mot de passe :

1. Cliquez avec le bouton droit de la souris sur  et cliquez sur **Modifier mot de passe VRM**.

La boîte de dialogue **Modifier le mot de passe** s'affiche.

2. Dans le champ **Anc. mot de passe**, saisissez le mot de passe approprié.
3. Dans le champ **Nv. mot passe**, saisissez le nouveau mot de passe. Cliquez ensuite dans le deuxième champ **Nv. mot passe** et répétez cette entrée.

Cliquez sur **OK**.



- ▶ Confirmez la boîte de dialogue suivante.
- ⇒ Le mot de passe est immédiatement modifié sur le dispositif.

14.22.10

Ajout d'une zone de stockage VRM

Fenêtre principale > **Périphériques** > Développez 

Pour ajouter une zone de stockage VRM :

- ▶ Cliquez sur le bouton droit de la souris sur  ou , puis sur **Ajouter un groupe**. Une nouvelle zone de stockage est ajoutée au système.

Se reporter à

- *Zone de stockage iSCSI, page 195*

14.22.11**Ajout manuel d'un VRM de basculement**

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter un VRM de basculement** > Boîte de dialogue **Ajouter un VRM de basculement**

**Remarque!**

Pour configurer un VRM secondaire, vous devez d'abord installer les logiciels appropriés sur l'ordinateur souhaité. Exécutez Setup.exe, puis sélectionnez **VRM secondaire**.

Le rôle de VRM de basculement peut être assuré par un VRM principal ou par un VRM secondaire. Vous ajoutez un VRM de basculement principal à un VRM principal, ou vous ajoutez un VRM de basculement secondaire à un VRM secondaire.

Vous pouvez ajouter un périphérique VRM de basculement manuellement si vous connaissez son adresse IP et son mot de passe. Le VRM sélectionné initialement est le VRM maître pour ce VRM de basculement.

Vous pouvez ajouter un dispositif VRM de basculement. Vous pouvez soit l'ajouter manuellement, soit sélectionner un dispositif dans la liste des dispositifs VRM détectés. Vous ne pouvez en fait affecter un VRM de basculement à un VRM maître que lorsque les deux sont en ligne et authentifiés avec succès. Les mots de passe sont alors synchronisés.

Pour ajouter un dispositif VRM de basculement :

1. Définissez les paramètres requis pour votre dispositif VRM.
 2. Assurez-vous que le VRM maître approprié est sélectionné. Si ce n'est pas le cas, annulez cette procédure.
 3. Cliquez sur **OK**.
- ⇒ Le dispositif VRM de basculement est ajouté au VRM maître sélectionné.

Boîte de dialogue Ajouter un VRM de basculement**Adresse réseau**

Saisissez l'adresse IP de votre dispositif ou sélectionnez une adresse réseau dans la liste **Serveurs VRM analysés**.

Serveurs VRM analysés

Affiche la liste des ordinateurs VRM détectés. Pour effectuer une nouvelle recherche, fermez la boîte de dialogue et affichez-la de nouveau.

**Remarque!**

Le dispositif de basculement VRM hérite des paramètres configurés dans le VRM maître. Si des paramètres du VRM maître sont modifiés, les paramètres du dispositif de basculement VRM sont modifiés en conséquence.

Se reporter à

– *Enregistrement double/de basculement, page 29*

14.22.12**Ajout manuel d'un VRM redondant**

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter un VRM en miroir** > Boîte de dialogue **Ajouter VRM**

**Remarque!**

Pour configurer un VRM secondaire, vous devez d'abord installer les logiciels appropriés sur l'ordinateur souhaité. Exécutez Setup.exe, puis sélectionnez **VRM secondaire**.

Seul un VRM secondaire peut assurer le rôle de VRM redondant. Vous ajoutez un VRM redondant à un VRM principal.

Vous pouvez ajouter un dispositif VRM redondant manuellement si vous connaissez son adresse IP et son mot de passe. Le VRM sélectionné initialement est le VRM maître pour ce VRM redondant.

Pour ajouter un dispositif VRM redondant :

1. Définissez les paramètres requis pour votre dispositif VRM.
2. Assurez-vous que le VRM maître approprié est sélectionné. Si ce n'est pas le cas, annulez cette procédure.
3. Cliquez sur **OK**.

Le dispositif VRM redondant est ajouté au VRM principal sélectionné.

Boîte de dialogue Ajouter VRM**Nom**

Saisissez un nom d'affichage pour le dispositif.

Adresse réseau/Port

Saisissez l'adresse IP de votre périphérique.

Si la case **Connexion sécurisée** est sélectionnée, le port bascule automatiquement sur le port HTTPS.

Vous pouvez modifier le numéro de port, si aucun port par défaut n'est utilisé.

Type

Sélectionnez le type de périphérique souhaité.

Nom d'utilisateur

Saisissez un nom d'utilisateur pour l'authentification.

Afficher le mot de passe

Cliquez sur cette option pour que le mot de passe soit visible.

Mot de passe

Saisissez le mot de passe pour l'authentification.

Sécurité

La case **Connexion sécurisée** est sélectionnée par défaut si le protocole HTTPS est pris en charge.

**Remarque!**

Si vous effectuez une migration vers BVMS version 10,0 ou supérieure, la case **Connexion sécurisée** n'est pas sélectionnée par défaut et la connexion n'est pas sécurisée (rcpp).

Pour modifier une connexion sécurisée ou non sécurisée, utilisez la commande **Modifier périphérique VRM**, puis sélectionnez ou désélectionnez la case **Connexion sécurisée**.

Test

Cliquez sur ce bouton pour vérifier si le périphérique est connecté et si l'authentification a réussi.

Propriétés

Si nécessaire, changez les numéros de port du port HTTP et du port HTTPS. Ce processus n'est possible que lorsque vous ajoutez ou modifiez un VRM qui n'est pas connecté. Si le VRM est connecté, les valeurs sont récupérées et vous ne pouvez pas les modifier.

La ligne du tableau **VRM maître** indique le périphérique sélectionné, le cas échéant.


Se reporter à

- *Ajout manuel d'un VRM primaire ou secondaire, page 176*
- *Enregistrement double/de basculement, page 29*

14.22.13

Ajout d'encodeurs via un balayage


Pour ajouter un encodeur via un balayage :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Rechercher des encodeurs**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Sélectionnez les encodeurs appropriés, sélectionnez la zone de stockage VRM souhaitée, puis cliquez sur **Affecter** pour les affecter à la zone de stockage VRM.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit de la souris sur ce champ, puis cliquez sur **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions réussies sont indiquées par .

Les connexions qui ont échoué sont indiquées par .


5. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.



L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

14.22.14



Ajout de dispositifs VSG via un balayage

Pour ajouter des dispositifs VSG via un balayage :


1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Rechercher les passerelles de diffusion de flux**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.

2. Sélectionnez les dispositifs VSG appropriés, sélectionnez la zone de stockage VRM souhaitée, puis cliquez sur **Affecter** pour les affecter à la zone de stockage VRM.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit sur ce champ et sélectionnez **Copier la cellule dans la colonne**.
Dans la colonne **État**, les connexions qui ont abouti sont indiquées par le symbole .
les connexions qui ont échoué sont indiquées par le symbole .
5. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.

14.22.15 Synchronisation de la configuration BVMS

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur la  > Commande **Synchronisation de la configuration BVMS** de BVMS 6.0, VRM 3.50 est pris en charge. Lorsque vous n'effectuez pas une mise à niveau de VRM vers la version 3.50 pendant la mise à niveau vers BVMS 6.0, l'enregistrement se poursuit, mais vous ne pouvez pas modifier la configuration de l'ancien VRM. Si vous avez mis à niveau votre logiciel VRM vers la version 3.50, vous devez synchroniser manuellement la configuration de BVMS.


14.22.16 Importer la configuration à partir de VRM

Fenêtre principale > **Périphériques** > Développez  > 
Si vous devez échanger un dispositif VRM principal, vous pouvez importer la configuration de l'ancien dispositif VRM principal.

Remarque : Ceci est possible uniquement pour les dispositifs VRM principaux.

Prérequis : une sauvegarde du fichier de configuration (**config.xml**) de l'ancien dispositif VRM a été effectuée. Pour savoir comment effectuer une sauvegarde, voir *Maintenance de BVMS*, page 77.

Pour importer une configuration à partir de VRM :

1. Copiez le fichier de configuration de sauvegarde (config.xml) de VRM dans C:
\ProgramData\Bosch\VRM\primary.
2. Cliquez avec le bouton droit de la souris sur  .
3. Sélectionnez **Importer la configuration à partir de VRM**.
La configuration de l'ancien VRM est importée.






Remarque!

Seule la configuration de l'encodeur, de VSG et d'iSCSI est importée. Vous devez recommencer toutes les autres configurations, par exemple en ajoutant les dispositifs requis à l'**Arborescence Logique**, en configurant des alarmes ou des paramètres d'enregistrement.

14.23

Page Zone

Fenêtre principale > **Périphériques** > Développez  > Développez  > 

Vous permet de configurer les paramètres d'enregistrement valides pour tous les périphériques rassemblés dans cette zone de stockage.

Identification du groupe

Affiche le numéro de pool.

Mode Préférences d'enregistrement

– Basculement

Les enregistrements ne sont effectués que sur une cible principale. S'il n'est pas possible d'enregistrer sur cette cible, l'enregistrement est effectué sur la cible indiquée sous la cible secondaire.

Une situation de panne se produit si la cible principale ne fournit pas de blocs de stockage, par exemple, en raison d'un système en panne, d'une erreur réseau ou d'une capacité épuisée.

Il est inutile de renseigner la liste des cibles secondaires. Dans ce cas, aucun basculement n'est possible mais le nombre de sessions iSCSI requises est réduit et aucun espace disque sur la cible secondaire n'est alloué. Cela permet de réduire les frais généraux du système et d'étendre la durée de conservation du système.

Remarque : Pour chaque caméra et encodeur, vous devez alors configurer la cible primaire et secondaire.

– automatique

L'équilibrage des charges est configuré automatiquement. Le mode **Automatique** essaie automatiquement d'optimiser la durée de conservation des cibles iSCSI disponibles.

Pour affecter les blocs de la deuxième cible iSCSI, sélectionnez **Activé** dans la liste

Utilisation d'une cible secondaire.

Intervalle des vérifications d'intégrité (jours)

Entrez la période requise. Au terme de cette période, le programme Video Recording Manager analyse si la distribution de stockage en mode **Automatique** est toujours optimale. Et si ce n'est pas le cas, le Video Recording Manager, le programme apporte des modifications.

Utilisation de cible secondaire

Permet de sélectionner si les blocs sont distribués à partir d'une deuxième cible.

Sélectionnez **Activé** ou **Désactivé** pour activer ou désactiver l'utilisation d'une cible secondaire.

- **Activé :** Sélectionnez **Activé** pour utiliser une cible secondaire qui réduit l'intervalle sans enregistrement en cas de défaillance de la cible principale. Si la cible principale est disponible, les blocs sur la cible secondaire ne sont pas utilisés mais le stockage est attribué. Cette redondance réduit la durée de conservation du système.

- **Désactivé** : Sélectionnez **Désactivé** si vous ne souhaitez pas utiliser de cible secondaire. En cas de défaillance de la cible principale, le programme Video Recording Manager nécessite davantage de temps pour se réorganiser. Cela signifie que l'intervalle sans enregistrement est plus long.

Réservation du bloc pour les temps d'arrêt

Saisissez le nombre de jours pendant lesquels les encodeurs affectés sont enregistrés même si le VRM Server est en panne.

Par exemple, si vous entrez 4, les encodeurs sont enregistrés pendant une durée correspondant à environ 4 jours d'interruption du VRM Server.

Si votre système comporte des encodeurs à faible débit, vous pouvez réduire considérablement l'espace disque pré-alloué. Cela garantit une distribution appropriée de la capacité de stockage et permet d'étendre la durée de conservation.

Autoriser les LUN de plus de 2 To

Cliquez pour activer l'utilisation de LUN d'une taille supérieure à 2 To.

Les LUN d'une taille supérieure à 2 To (« LUN de grande taille ») ne sont pas prises en charge par les périphériques suivants :

- Périphériques VRM antérieurs à la version 3.60
- Périphériques VSG avec une version de firmware antérieure à la version 6.30
- Encodeurs avec une version de firmware antérieure à la version 6.30

BVMS vous empêche d'effectuer les procédures suivantes :

- Ajouter ou déplacer des périphériques avec une version de firmware antérieure à la version 6.30 vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer des périphériques qui ne sont pas actuellement connectés au réseau, vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer un périphérique iSCSI qui contient des LUN de grande taille, vers un pool qui n'autorise pas les LUN de grande taille.
- Autoriser les LUN de grande taille sur un pool contenant des périphériques avec un firmware dont la version est antérieure à la version 6.30.
- Désactiver les LUN de grande taille sur un pool avec un périphérique iSCSI contenant des LUN de grande taille.

Veillez déplacer les périphériques dont le firmware est d'une version antérieure à la version 6.30 vers un pool qui n'autorise pas les LUN de grande taille.

Se reporter à

- *Ajout d'un LUN, page 203*
- *Ajout d'une zone de stockage VRM, page 180*

14.23.1

Configuration du mode d'enregistrement automatique sur une zone de stockage

Fenêtre principale > **Périphériques** > Développez  > Développez  > 

Remarque :

si vous avez déjà configuré un mode d'enregistrement de basculement, cette configuration est écrasée.

Pour procéder à une configuration :




- ▶ Dans la liste **Enregistrement du mode préférences**, sélectionnez **Automatique**. Une fois la configuration activée, le mode d'enregistrement **Automatique** est actif. Sur la page **Préférences d'enregistrement** d'un encodeur, la liste des cibles principales et secondaires est désactivée.


Rubriques connexes


– *Configuration du mode d'enregistrement de basculement sur un encodeur, page 240*

14.23.2

Ajout manuel d'un encodeur

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**
ou

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**
ou




Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter décodeur** > Boîte de dialogue **Ajouter encodeur**
Vous permet d'ajouter un encodeur manuellement. Cette fonction s'avère très utile lorsque vous souhaitez ajouter un périphérique vidéo IP de Bosch (uniquement pour VRM).


Remarque :

Si vous ajoutez un encodeur vidéo IP de Bosch avec l'option **<Détection automatique>**, ce dispositif doit être disponible sur le réseau.


Pour ajouter un dispositif vidéo IP Bosch :

1. Développez  , puis  , cliquez avec le bouton droit de la souris sur  .
Ou

cliquez avec le bouton droit de la souris sur  .
Ou

cliquez avec le bouton droit de la souris sur  .

2. Cliquez sur **Ajouter encodeur**.
La boîte de dialogue **Ajouter un encodeur** s'affiche.
3. Saisissez l'adresse IP correspondante.
4. Dans la liste, sélectionnez **<Détection automatique>**, saisissez le mot de passe du dispositif et cliquez sur **Authentifier**.
Ou
Dans la liste, sélectionnez un type d'encodeur concret ou **<Caméra avec un seul espace réservé>**.
5. Cliquez sur **OK**.
Le dispositif est ajouté au système.

L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

Boîte de dialogue Ajouter encodeur

Adresse réseau

Saisissez une adresse IP valide.

Type d'encodeur

Pour les dispositifs dont le type est connu, sélectionnez l'entrée correspondante. Le périphérique ne doit pas obligatoirement être disponible sur le réseau.

Si vous souhaitez ajouter un dispositif vidéo IP de Bosch, sélectionnez **<Détection automatique>**. Le dispositif doit être disponible sur le réseau.

Si vous souhaitez ajouter une caméra pour une configuration hors ligne, sélectionnez **<Caméra avec un seul espace réservé>**.

Nom d'utilisateur

Affiche le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le dispositif.

Afficher le mot de passe

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Authentifier

Permet de vous authentifier sur le dispositif avec les identifiants saisis précédemment.

14.23.3

Ajout manuel d'un dispositif iSCSI

Fenêtre principale > **Périphériques** >  > Développez  > Cliquez avec le bouton

droit de la souris sur  > **Ajouter un périphérique iSCSI** > Boîte de dialogue **Ajouter un périphérique iSCSI**

Permet d'ajouter un dispositif iSCSI à un VRM.

Pour ajouter un dispositif iSCSI :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Ajouter un périphérique iSCSI**.
La boîte de dialogue **Ajouter un périphérique iSCSI** s'affiche.
2. Saisissez le nom d'affichage souhaité, l'adresse réseau d'un dispositif iSCSI et le type de dispositif, puis cliquez sur **OK**.
Le dispositif iSCSI est ajouté au pool VRM sélectionné.
Si nécessaire, ajoutez des cibles et des LUN.

Boîte de dialogue Ajouter un périphérique iSCSI

Nom

Saisissez un nom d'affichage pour le dispositif.

Adresse réseau

Saisissez une adresse réseau valide pour le dispositif.

Type de périphérique iSCSI

Sélectionnez le type de dispositif approprié.

Nom d'utilisateur

Saisissez un nom d'utilisateur pour l'authentification.

Mot de passe

Saisissez le mot de passe pour l'authentification.

Activer la surveillance

Si un dispositif DIVAR IP est sélectionné comme type de dispositif iSCSI et qu'une surveillance SNMP (Simple Network Management Protocol) est prise en charge pour ce type de dispositif DIVAR IP, la case à cocher **Activer la surveillance** est activée.

Cochez la case pour activer la surveillance de l'état d'état du dispositif DIVAR IP. BVMS reçoit et analyse désormais automatiquement les traps SNMP du dispositif DIVAR IP et active les événements et les alarmes de surveillance de l'état (par exemple, unité centrale, stockage, ventilateur,...). Par défaut, seules les alarmes critiques sont déclenchées.

Remarque : Assurez-vous de d'abord configurer SNMP sur le dispositif DIVAR IP.

Remarque : Ce paramètre est disponible uniquement pour les dispositifs pris en charge. Pour plus d'informations sur la configuration de SNMP sur un dispositif DIVAR IP, consultez la documentation DIVAR IP respective.

Rubriques connexes

- *Ajout de dispositifs VRM via un balayage, page 174*


Se reporter à

- *Page RMon et Snmp, page 157*
- *Configuration de la surveillance SNMP, page 96*


14.23.4**Ajout manuel d'un composant Video Streaming Gateway**

Fenêtre principale > **Périphériques** > Développez  > 
 Vous pouvez ajouter des dispositifs VSG à une zone de stockage VRM.

Pour ajouter un dispositif VSG manuellement :

1. Cliquez avec le bouton droit de la souris sur  et cliquez sur **Ajouter une passerelle de diffusion de flux**.
 La boîte de dialogue **Ajouter une passerelle de diffusion de flux** s'affiche.
2. Définissez les paramètres requis pour votre dispositif VSG.
3. Cliquez sur **Ajouter**.
 ⇒ Le périphérique VSG est ajouté au système. Les caméras affectées à ce périphérique VSG sont enregistrées.

Boîte de dialogue Ajouter une passerelle de diffusion de flux

Cliquez avec le bouton droit de la souris sur la boîte de dialogue  > **Ajouter une passerelle de diffusion de flux** > **Ajouter une passerelle de diffusion de flux**

Nom

Saisissez le nom d'affichage souhaité pour le périphérique.

Nom d'utilisateur

Saisissez le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Généralement : service

Adresse réseau/Port

Saisissez l'adresse IP de votre dispositif.

Si la case **Connexion sécurisée** est sélectionnée, le port bascule automatiquement sur le port HTTPS.

Vous pouvez modifier le numéro de port, si aucun port par défaut n'est utilisé ou si les instances VSG sont configurées dans un ordre différent.

Ports par défaut

Instance 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

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le périphérique.

Show password

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Sécurité

La case **Connexion sécurisée** est sélectionnée par défaut si le protocole HTTPS est pris en charge.

À compter de VSG version 7.0, VSG prend en charge une connexion sécurisée.



Remarque!

Si vous effectuez une migration vers BVMS version 10,0 ou supérieure, la case **Connexion sécurisée** n'est pas sélectionnée par défaut et la connexion n'est pas sécurisée (rcpp).

Pour modifier une connexion sécurisée ou non sécurisée, utilisez la commande **Modifier la passerelle de diffusion de flux**, puis sélectionnez ou désélectionnez la case **Connexion sécurisée**.

Test

Permet de vous authentifier sur le périphérique avec les identifiants saisis précédemment.

Se reporter à

– *Modification d'une passerelle Video Streaming Gateway, page 207*

14.23.5

Ajout manuel d'un dispositif iSCSI DSA E-Series

Fenêtre principale > **Périphériques** > Développez  > Développer  > 

Vous pouvez ajouter un dispositif iSCSI E-Series qui est déjà initialisé ou vous ajoutez un dispositif iSCSI E-Series non initialisé.

Vous pouvez ajouter des LUN d'une taille supérieure à 2 To si le pool est activé pour les LUN de grande taille.

Les LUN d'une taille supérieure à 2 To (« LUN de grande taille ») ne sont pas prises en charge par les périphériques suivants :


- Périphériques VRM antérieurs à la version 3.60
- Périphériques VSG avec une version de firmware antérieure à la version 6.30
- Encodeurs avec une version de firmware antérieure à la version 6.30

BVMS vous empêche d'effectuer les procédures suivantes :




- Ajouter ou déplacer des périphériques avec une version de firmware antérieure à la version 6.30 vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer des périphériques qui ne sont pas actuellement connectés au réseau, vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer un périphérique iSCSI qui contient des LUN de grande taille, vers un pool qui n'autorise pas les LUN de grande taille.
- Autoriser les LUN de grande taille sur un pool contenant des périphériques avec un firmware dont la version est antérieure à la version 6.30.
- Désactiver les LUN de grande taille sur un pool avec un périphérique iSCSI contenant des LUN de grande taille.

Veillez déplacer les périphériques dont le firmware est d'une version antérieure à la version 6.30 vers un pool qui n'autorise pas les LUN de grande taille.

Pour ajouter un dispositif iSCSI initialisé :




1. Cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Ajouter périphérique DSA E-Series**.
La boîte de dialogue **Ajouter périphérique DSA E-Series** s'affiche.
2. Saisissez l'adresse IP de gestion et le mot de passe.
3. Cliquez sur **Connecter**
Si la connexion est établie, les champs dans les groupes **Contrôleur** et/ou **2ème contrôleur** sont remplis.
4. Cliquez sur **OK**.
Le dispositif est ajouté au système.
Les cibles disponibles sont automatiquement analysées et les LUN sont affichés.
Vous pouvez utiliser le dispositif iSCSI.
Si le pool est activé pour les LUN de grande taille, et si le dispositif iSCSI comporte des LUN de grande taille configurés, la colonne **LUN volumineux** affiche une coche pour les LUN concernés.

Pour ajouter un dispositif iSCSI non initialisé :

1. Cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Ajouter périphérique DSA E-Series**.
La boîte de dialogue **Ajouter périphérique DSA E-Series** s'affiche.
2. Saisissez l'adresse IP de gestion et le mot de passe.
3. Cliquez sur **Connecter**
Si la connexion est établie, les champs dans les groupes **Contrôleur** et/ou **2ème contrôleur** sont remplis.
4. Cliquez sur **OK**.
Le dispositif est ajouté au système.
5. Cliquez sur  , puis sur  .
6. Cliquez sur l'onglet **Configuration de base**.
7. Saisissez la capacité de LUN souhaitée.

- Si vous saisissez une valeur supérieure à 2 To, vous devez activer votre pool pour des LUN d'une taille supérieure à 2 To.
8. Cliquez sur **Initialiser**.
Les LUN sont créés.
 9. Cliquez sur **Fermer**.
 10. Cliquez avec le bouton droit de la souris sur le dispositif iSCSI, puis cliquez sur **Rechercher cible**.
Les LUN sont affichés avec un état inconnu.
 11. Enregistrez et activez la configuration.
 12. Formatez tous les LUN.
 13. Si vous avez ajouté un dispositif iSCSI avec double contrôleur, supprimez les LUN souhaités du premier contrôleur, cliquez avec le bouton droit de la souris sur le deuxième contrôleur, puis cliquez sur **Rechercher cible** pour ajouter ces LUN.

Boîte de dialogue Ajouter périphérique DSA E-Series

Fenêtre principale > **Périphériques** >  > Développez  > Cliquez avec le bouton droit de la souris sur  > **Ajouter périphérique DSA E-Series** > Boîte de dialogue **Ajouter périphérique DSA E-Series**

Permet d'ajouter un dispositif iSCSI DSA E-Series. Ce type de dispositif comporte une adresse IP de gestion différente de l'adresse IP du stockage iSCSI. Via cette adresse IP de gestion, le dispositif est automatiquement détecté et configuré.

Nom

Saisissez un nom d'affichage pour le dispositif.

Adresse de gestion

Saisissez l'adresse IP pour la configuration automatique du dispositif.

Mot de passe :

Entrez le mot de passe de ce dispositif.

Type DSA E-Series

Affiche le type du dispositif.

Adresse réseau iSCSI Ch

Affiche l'adresse IP du port iSCSI du dispositif. Si cette fonction est disponible, vous pouvez sélectionner une autre adresse IP.

Adresse de gestion

Affiche l'adresse IP pour une configuration automatique du deuxième contrôleur, si disponible. Si cette fonction est disponible, vous pouvez sélectionner une autre adresse IP.

Adresse réseau iSCSI Ch

Affiche l'adresse IP du port iSCSI du deuxième contrôleur, si disponible. Si cette fonction est disponible, vous pouvez sélectionner une autre adresse IP.

Connecter

Cliquez pour détecter les paramètres du dispositif.

Si la connexion est établie, les champs des groupes **Contrôleur** et **2ème contrôleur** sont remplis.


Se reporter à

- *Page Configuration de base, page 200*

– *Formatage d'un LUN, page 204*

14.23.6 Ajout d'encodeurs via un balayage


Pour ajouter un encodeur via un balayage :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Rechercher des encodeurs**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Sélectionnez les encodeurs appropriés, sélectionnez la zone de stockage VRM souhaitée, puis cliquez sur **Affecter** pour les affecter à la zone de stockage VRM.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit de la souris sur ce champ, puis cliquez sur **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions réussies sont indiquées par .


Les connexions qui ont échoué sont indiquées par .

5. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.

L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

14.23.7 Ajout de dispositifs VSG via un balayage

Pour ajouter des dispositifs VSG via un balayage :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Rechercher les passerelles de diffusion de flux**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Sélectionnez les dispositifs VSG appropriés, sélectionnez la zone de stockage VRM souhaitée, puis cliquez sur **Affecter** pour les affecter à la zone de stockage VRM.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit sur ce champ et sélectionnez **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions qui ont abouti sont indiquées par le symbole



les connexions qui ont échoué sont indiquées par le symbole



5. Cliquez sur **Terminer**.

L'élément est ajouté dans l'arborescence des dispositifs.

14.23.8

Configuration de l'enregistrement double dans l'Arborescence des périphériques

Fenêtre principale > **Périphériques** > Développez




Vous devez désactiver la fonction ANR pour configurer l'enregistrement double.

Si vous configurez l'enregistrement double pour une caméra d'un encodeur multivoie, le système s'assure que la même cible d'enregistrement est configurée pour toutes les caméras de cet encodeur.

Vous pouvez configurer l'enregistrement double en affectant des encodeurs qui sont enregistrés par un VRM principal sur un VRM secondaire. Cela s'avère utile lorsque, par exemple, vous voulez affecter uniquement une partie des encodeurs qui sont enregistrés par un VRM principal.

Un VRM secondaire doit avoir été ajouté.

Pour procéder à une configuration :

1. Cliquez avec le bouton droit de la souris sur  et cliquez sur **Ajouter un encodeur pour le VRM principal**.

La boîte de dialogue **Ajouter des encodeurs** s'affiche.

2. Cliquez pour sélectionner les encodeurs souhaités.

Lorsque vous sélectionnez un pool ou un VRM, tous les éléments enfants sont automatiquement sélectionnés.

3. Cliquez sur **OK**.

Les encodeurs sélectionnés sont ajoutés au VRM secondaire.

Se reporter à

- *Configuration de l'enregistrement double dans le Tableau des caméras, page 314*
- *Configuration de la fonction ANR, page 314*
- *Enregistrement double/de basculement, page 29*

14.24

Page Encodeur/Décodeur Bosch

Pour configurer un encodeur / décodeur Bosch, reportez-vous à la *Page Encodeur / Décodeur / Caméra Bosch, page 222*.

14.25

Page de périphérique iSCSI

Fenêtre principale > **Périphériques** > Développez



> Développez



> Développez



> Développez



Vous pouvez ajouter soit un périphérique iSCSI série E, soit tout autre périphérique iSCSI pris en charge.

Se reporter à

- Ajout manuel d'un dispositif iSCSI, page 196
- Ajout manuel d'un dispositif iSCSI DSA E-Series, page 197
- Configuration d'un périphérique iSCSI, page 199
- Ajout d'un LUN, page 203
- Formatage d'un LUN, page 204

14.25.1**Zone de stockage iSCSI**

Une zone de stockage peut être utilisée pour obtenir un mappage logique de la topologie du réseau au système Video Recording Manager. Par exemple : deux bâtiments, contenant un stockage et des dispositifs, pour vous permettre d'éviter d'acheminer le trafic réseau d'un immeuble à l'autre.

Les zones de stockage peuvent également être utilisées pour grouper les caméras et les systèmes de stockage selon un critère d'affichage important. Prenons l'exemple d'un système qui comporte à la fois quelques caméras très importantes et de nombreuses caméras beaucoup moins importantes. Il est alors possible de les regrouper en deux zones de stockage, l'une équipée de nombreuses fonctions de redondance, l'autre dotée de moins de fonctions de redondance.

Vous pouvez configurer les propriétés d'équilibrage de charge suivantes pour une zone de stockage :

- Préférences d'enregistrement (**Automatique** ou **Basculement**)
- Utilisation d'une cible secondaire

Une cible secondaire est utilisée en mode **Basculement** lorsque la cible principale affectée échoue. Si cette option est désactivée, l'enregistrement s'arrête sur tous les périphériques affectés à cette cible principale en échec.

Mode **Automatique** : si une cible échoue, VRM Server réaffecte automatiquement les périphériques concernés à d'autres équipements de stockage. Si le VRM Server tombe en panne alors qu'une cible est défaillante, l'enregistrement est arrêté sur les dispositifs en cours d'enregistrement sur la cible défaillante.

- Réserve du bloc pour les temps d'arrêt
- Intervalle des contrôles d'intégrité

Pour chaque pool, vous pouvez configurer que ce pool autorise les unités logiques (LUN) d'une taille supérieure à 2 To.

Les LUN d'une taille supérieure à 2 To (« LUN de grande taille ») ne sont pas prises en charge par les périphériques suivants :

- Périphériques VRM antérieurs à la version 3.60
- Périphériques VSG avec une version de firmware antérieure à la version 6.30
- Encodeurs avec une version de firmware antérieure à la version 6.30

BVMS vous empêche d'effectuer les procédures suivantes :

- Ajouter ou déplacer des périphériques avec une version de firmware antérieure à la version 6.30 vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer des périphériques qui ne sont pas actuellement connectés au réseau, vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer un périphérique iSCSI qui contient des LUN de grande taille, vers un pool qui n'autorise pas les LUN de grande taille.
- Autoriser les LUN de grande taille sur un pool contenant des périphériques avec un firmware dont la version est antérieure à la version 6.30.
- Désactiver les LUN de grande taille sur un pool avec un périphérique iSCSI contenant des LUN de grande taille.

Veillez déplacer les périphériques dont le firmware est d'une version antérieure à la version 6.30 vers un pool qui n'autorise pas les LUN de grande taille.

Si un VRM primaire comporte un pool qui autorise les LUN de grande taille, le VRM en miroir correspondant hérite de ce paramètre et vous ne pouvez pas sélectionner or désélectionner la case à cocher **Autoriser les LUN de plus de 2 To** sur le pool correspondant du VRM en miroir. Si vous avez ajouté un périphérique iSCSI avec des LUN de grande taille dans un VRM en miroir, vous ne pouvez pas désélectionner la case à cocher **Autoriser les LUN de plus de 2 To** sur le pool correspondant du VRM primaire.

Se reporter à

– Page Zone, page 185

14.25.2

Ajout manuel d'un dispositif iSCSI

Fenêtre principale > **Périphériques** >  > Développez  > Cliquez avec le bouton

droit de la souris sur  > **Ajouter un périphérique iSCSI** > Boîte de dialogue **Ajouter un périphérique iSCSI**

Permet d'ajouter un dispositif iSCSI à un VRM.

Pour ajouter un dispositif iSCSI :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Ajouter un périphérique iSCSI**.
La boîte de dialogue **Ajouter un périphérique iSCSI** s'affiche.
2. Saisissez le nom d'affichage souhaité, l'adresse réseau d'un dispositif iSCSI et le type de dispositif, puis cliquez sur **OK**.
Le dispositif iSCSI est ajouté au pool VRM sélectionné.
Si nécessaire, ajoutez des cibles et des LUN.

Boîte de dialogue Ajouter un périphérique iSCSI

Nom

Saisissez un nom d'affichage pour le dispositif.

Adresse réseau

Saisissez une adresse réseau valide pour le dispositif.

Type de périphérique iSCSI

Sélectionnez le type de dispositif approprié.

Nom d'utilisateur

Saisissez un nom d'utilisateur pour l'authentification.

Mot de passe

Saisissez le mot de passe pour l'authentification.

Activer la surveillance

Si un dispositif DIVAR IP est sélectionné comme type de dispositif iSCSI et qu'une surveillance SNMP (Simple Network Management Protocol) est prise en charge pour ce type de dispositif DIVAR IP, la case à cocher **Activer la surveillance** est activée.

Cochez la case pour activer la surveillance de l'état d'état du dispositif DIVAR IP. BVMS reçoit et analyse désormais automatiquement les traps SNMP du dispositif DIVAR IP et active les événements et les alarmes de surveillance de l'état (par exemple, unité centrale, stockage, ventilateur,...). Par défaut, seules les alarmes critiques sont déclenchées.

Remarque : Assurez-vous de d'abord configurer SNMP sur le dispositif DIVAR IP.

Remarque : Ce paramètre est disponible uniquement pour les dispositifs pris en charge. Pour plus d'informations sur la configuration de SNMP sur un dispositif DIVAR IP, consultez la documentation DIVAR IP respective.

Rubriques connexes




- *Ajout de dispositifs VRM via un balayage, page 174*

Se reporter à

- *Page RMon et Snmp, page 157*
- *Configuration de la surveillance SNMP, page 96*

14.25.3

Ajout manuel d'un dispositif iSCSI DSA E-Series

Fenêtre principale > **Périphériques** > Développez  > Développer  >  > ajoutez un dispositif iSCSI E-Series non initialisé.

Vous pouvez ajouter des LUN d'une taille supérieure à 2 To si le pool est activé pour les LUN de grande taille.

Les LUN d'une taille supérieure à 2 To (« LUN de grande taille ») ne sont pas prises en charge par les périphériques suivants :


- Périphériques VRM antérieurs à la version 3.60
- Périphériques VSG avec une version de firmware antérieure à la version 6.30
- Encodeurs avec une version de firmware antérieure à la version 6.30

BVMS vous empêche d'effectuer les procédures suivantes :

- Ajouter ou déplacer des périphériques avec une version de firmware antérieure à la version 6.30 vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer des périphériques qui ne sont pas actuellement connectés au réseau, vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer un périphérique iSCSI qui contient des LUN de grande taille, vers un pool qui n'autorise pas les LUN de grande taille.
- Autoriser les LUN de grande taille sur un pool contenant des périphériques avec un firmware dont la version est antérieure à la version 6.30.
- Désactiver les LUN de grande taille sur un pool avec un périphérique iSCSI contenant des LUN de grande taille.




Veuillez déplacer les périphériques dont le firmware est d'une version antérieure à la version 6.30 vers un pool qui n'autorise pas les LUN de grande taille.

Pour ajouter un dispositif iSCSI initialisé :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Ajouter périphérique DSA E-Series**.
La boîte de dialogue **Ajouter périphérique DSA E-Series** s'affiche.
2. Saisissez l'adresse IP de gestion et le mot de passe.
3. Cliquez sur **Connecter**.
Si la connexion est établie, les champs dans les groupes **Contrôleur** et/ou **2ème contrôleur** sont remplis.
4. Cliquez sur **OK**.
Le dispositif est ajouté au système.
Les cibles disponibles sont automatiquement analysées et les LUN sont affichés.
Vous pouvez utiliser le dispositif iSCSI.

Si le pool est activé pour les LUN de grande taille, et si le dispositif iSCSI comporte des LUN de grande taille configurés, la colonne **LUN volumineux** affiche une coche pour les LUN concernés.

Pour ajouter un dispositif iSCSI non initialisé :

1. Cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Ajouter périphérique DSA E-Series**.
La boîte de dialogue **Ajouter périphérique DSA E-Series** s'affiche.
2. Saisissez l'adresse IP de gestion et le mot de passe.
3. Cliquez sur **Connecter**
Si la connexion est établie, les champs dans les groupes **Contrôleur** et/ou **2ème contrôleur** sont remplis.
4. Cliquez sur **OK**.
Le dispositif est ajouté au système.
5. Cliquez sur  , puis sur  .
6. Cliquez sur l'onglet **Configuration de base**.
7. Saisissez la capacité de LUN souhaitée.
Si vous saisissez une valeur supérieure à 2 To, vous devez activer votre pool pour des LUN d'une taille supérieure à 2 To.
8. Cliquez sur **Initialiser**.
Les LUN sont créés.
9. Cliquez sur **Fermer**.
10. Cliquez avec le bouton droit de la souris sur le dispositif iSCSI, puis cliquez sur **Rechercher cible**.
Les LUN sont affichés avec un état inconnu.
11. Enregistrez et activez la configuration.
12. Formatez tous les LUN.
13. Si vous avez ajouté un dispositif iSCSI avec double contrôleur, supprimez les LUN souhaités du premier contrôleur, cliquez avec le bouton droit de la souris sur le deuxième contrôleur, puis cliquez sur **Rechercher cible** pour ajouter ces LUN.

Boîte de dialogue Ajouter périphérique DSA E-Series

Fenêtre principale > **Périphériques** >  > Développez  > Cliquez avec le bouton

droit de la souris sur  > **Ajouter périphérique DSA E-Series** > Boîte de dialogue **Ajouter périphérique DSA E-Series**

Permet d'ajouter un dispositif iSCSI DSA E-Series. Ce type de dispositif comporte une adresse IP de gestion différente de l'adresse IP du stockage iSCSI. Via cette adresse IP de gestion, le dispositif est automatiquement détecté et configuré.

Nom

Saisissez un nom d'affichage pour le dispositif.

Adresse de gestion

Saisissez l'adresse IP pour la configuration automatique du dispositif.

Mot de passe :

Entrez le mot de passe de ce dispositif.

Type DSA E-Series

Affiche le type du dispositif.

Adresse réseau iSCSI Ch

Affiche l'adresse IP du port iSCSI du dispositif. Si cette fonction est disponible, vous pouvez sélectionner une autre adresse IP.

Adresse de gestion

Affiche l'adresse IP pour une configuration automatique du deuxième contrôleur, si disponible. Si cette fonction est disponible, vous pouvez sélectionner une autre adresse IP.

Adresse réseau iSCSI Ch

Affiche l'adresse IP du port iSCSI du deuxième contrôleur, si disponible. Si cette fonction est disponible, vous pouvez sélectionner une autre adresse IP.

Connecter




Cliquez pour détecter les paramètres du dispositif.

Si la connexion est établie, les champs des groupes **Contrôleur** et **2ème contrôleur** sont remplis.

Se reporter à

- *Page Configuration de base, page 200*
- *Formatage d'un LUN, page 204*

14.25.4**Configuration d'un périphérique iSCSI**

Fenêtre principale > **Périphériques** > Développez  > Développez  > 
 Après avoir ajouté des périphériques VRM, des périphériques iSCSI et des encodeurs, effectuez les opérations suivantes pour vous assurer que les données vidéo des encodeurs seront stockées sur les périphériques iSCSI ou qu'elles pourront être récupérées à partir de ces périphériques iSCSI :

- Exécutez la configuration par défaut pour créer des LUNs sur chaque cible du périphérique iSCSI.
 Cette étape est facultative. Vous n'êtes pas tenu de l'effectuer sur un périphérique iSCSI comportant des LUNs préconfigurés.
- Recherchez le périphérique iSCSI de manière à ajouter les cibles et les LUNs à l'Arborescence des Périphériques après une configuration par défaut.




Remarque :

La configuration par défaut et le mappage automatique des IQN ne sont pas reconnus par tous les périphériques iSCSI.

Prérequis :

Le dispositif iSCSI doit être configuré avec des adresses IP valides.

Pour effectuer la configuration de base d'un dispositif iSCSI DSA E-Series :







- ▶ Développez le périphérique VRM approprié  et  et cliquez sur le périphérique iSCSI  souhaité.
 1. Cliquez sur l'onglet **Configuration de base**.
 2. Saisissez la capacité de LUN souhaitée.
 Si vous saisissez une valeur supérieure à 2 To, vous devez activer votre pool pour des LUN d'une taille supérieure à 2 To.

3. Cliquez sur **Initialiser**.
Les LUN sont créés.
4. Cliquez sur **Fermer**.
5. Cliquez avec le bouton droit de la souris sur le dispositif iSCSI, puis cliquez sur **Rechercher cible**.
Les LUN sont affichés avec un état inconnu.
6. Enregistrez et activez la configuration.
7. Formatez tous les LUN.
8. Si vous avez ajouté un dispositif iSCSI avec double contrôleur, supprimez les LUN souhaités du premier contrôleur, cliquez avec le bouton droit de la souris sur le deuxième contrôleur, puis cliquez sur **Rechercher cible** pour ajouter ces LUN.

Pour effectuer la configuration de base sur d'autres dispositifs iSCSI :

1. Cliquez sur l'onglet **Configuration de base**.
2. Saisissez le nombre de LUN souhaités.
3. Cliquez sur **Définir**.
Les LUN sont créés.
4. Cliquez sur **Fermer**.
5. Cliquez avec le bouton droit de la souris sur le dispositif iSCSI, puis cliquez sur **Rechercher cible**.
Les LUN sont affichés avec un état inconnu.
6. Enregistrez et activez la configuration.
7. Formatez tous les LUN.

Pour effectuer le mappage IQN des autres dispositifs iSCSI :

1. Développez le périphérique VRM approprié  et  et cliquez sur le périphérique iSCSI  souhaité.
2. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Cartographier les IQN**.
La boîte de dialogue iqn-Mapper s'affiche et le processus démarre.
Les encodeurs affectés au périphérique VRM sélectionné sont évalués et leurs IQN sont ajoutés à ce périphérique iSCSI.
3. Cliquez sur  pour enregistrer les paramètres.
4. Cliquez sur  pour activer la configuration.

Se reporter à

- Page Configuration de base, page 200
- Boîte de dialogue Équilibrage de charge, page 202
- Boîte de dialogue iqn-Mapper, page 205
- Formatage d'un LUN, page 204

14.25.5

Page Configuration de base

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Cliquez sur  > Onglet **Configuration de base**

Les options affichées peuvent différer selon le type de système de stockage iSCSI utilisé. Permet de procéder à la configuration de base de votre périphérique iSCSI. Vous devez créer des LUNs sur le disque dur iSCSI et formater ces LUNs. Cet onglet s'affiche uniquement si le périphérique correspond à l'un des systèmes de stockage iSCSI pris en charge par Bosch, par exemple DSA ou DLS 1x00.

**Remarque!**

Après la configuration de base d'un modèle E-Series, le système a besoin de nombreuses heures (voire de jours) pour s'initialiser. Pendant cette phase, les performances ne sont pas optimales. En phase 1.5, le formatage peut échouer.

Capacité physique (Go)

Informations sur la capacité totale du système de stockage.

Nombre de LUN

Vous pouvez modifier le nombre de LUN.

**Remarque!**

Si vous modifiez le nombre de LUN, tout le système iSCSI est réorganisé et les séquences enregistrées sur le système sont perdues.

Par conséquent, avant d'apporter des modifications, vérifiez les enregistrements et sauvegardez les séquences importantes.

Capacité pour des LUN supplémentaires (Go)

Le nombre maximal de LUN par matrice de stockage étant de 256, la taille du LUN ne doit pas être définie sur une trop petite valeur. Dans le cas contraire plus aucun LUN ne pourra être créé à l'avenir si une extension de logement supplémentaire est installée.

Disques de réserve cible

Nombre de disques de réserve dont l'utilisateur souhaite disposer dans le système.

Disques de réserve actuels

Nombre de disques de réserve actuellement disponibles dans le système. Ce chiffre peut être différent du chiffre ci-dessus, par exemple, si le système de stockage est reconfiguré manuellement ou si les disques sont hors service.

État de l'initialisation (%)

Des informations supplémentaires s'affichent au cours de l'initialisation. Une fois l'initialisation terminée (100 %), vous pouvez à nouveau effacer tous les LUN.

RAID-DP (fiabilité)

Activez cette option si vous ne souhaitez pas utiliser le type de protection RAID spécifié, à savoir RAID-4, mais plutôt le type de protection RAID-DP offrant une fiabilité supérieure.

RAID 6 (fiabilité)

Sélectionnez cette option si vous ne souhaitez pas utiliser le type de protection RAID spécifié, à savoir RAID 5, mais plutôt le type de protection RAID 6 offrant une fiabilité supérieure.





Informations supplémentaires

Affiche des informations supplémentaires, par exemple pour indiquer que le système de stockage n'est pas configuré correctement, ce qui empêche toute configuration.

Se reporter à

– *Ajout manuel d'un dispositif iSCSI DSA E-Series, page 197*

14.25.6**Boîte de dialogue Équilibrage de charge**





Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Commande **Équilibrage de la charge...** > Boîte de dialogue **Équilibrage de la charge**

Prérequis : Configuration du mode d'enregistrement **Automatique**.

Définissez le débit maximal autorisé ainsi que le nombre maximal de connexions iSCSI simultanées pour chaque système iSCSI. Si ces valeurs maximales sont dépassées, les données ne sont plus écrites sur le système iSCSI et sont alors perdues.




Pour les systèmes pris en charge (par exemple Bosch RAID, NetApp, DLA), utilisez les valeurs par défaut. Pour les autres périphériques, reportez-vous à la documentation correspondante. Essayez des petites valeurs pour commencer.

14.25.7**Déplacement d'un système iSCSI vers une autre zone de stockage (Modifier la zone de stockage)**






Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > 

Vous pouvez déplacer un dispositif d'une zone de stockage vers une autre à l'intérieur du même dispositif VRM sans perdre d'enregistrements.

Pour effectuer un déplacement :

1. Cliquez avec le bouton droit de la souris sur  /  / , puis cliquez sur **Modification du groupe ...**
La boîte de dialogue **Modifier le groupe** s'affiche.
2. Dans la liste **Nouveau groupe :**, sélectionnez la zone de stockage souhaitée.
3. Cliquez sur **OK**.
Le périphérique est déplacé vers la zone de stockage sélectionnée.

14.25.8**Page LUN**

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > 

Vous pouvez ajouter, supprimer ou formater des LUN, et afficher des informations sur les LUN.

Ajouter

Cliquez sur ce bouton pour afficher la boîte de dialogue **Ajouter LUN**.

Supprimer

Cliquez pour supprimer les lignes sélectionnées. Pour sélectionner une ligne, cliquez sur l'en-tête de ligne sur le côté gauche. Chaque ligne représente un LUN.

Une boîte de message s'affiche.

Formater LUN

Cliquez sur ce bouton pour formater le LUN sélectionné. Une boîte de message s'affiche.

Format

Cliquez sur la case pour sélectionner le LUN, puis cliquez sur **Formater LUN**.

LUN

Affiche le nom du LUN.

Taille [Go]

Affiche la capacité maximale du LUN.

LUN volumineux

Chaque cellule indique s'il s'agit ou non d'un LUN d'une taille supérieure à 2 To.

État

Affiche l'état du LUN.

Avancement

Affiche la progression du processus de formatage.

Se reporter à

- *Page Zone, page 185*
- *Ajout d'un LUN, page 203*
- *Ajout de dispositifs VRM via un balayage, page 174*

14.25.9**Ajout d'un LUN**

Fenêtre principale > **Périphériques** > Développez  > Développez  > 

En règle générale, le balayage du réseau ajoute automatiquement les périphériques iSCSI voulus avec leur cible et leurs LUN. Si le balayage du réseau n'a pas fonctionné correctement ou que vous souhaitez configurer votre périphérique iSCSI hors ligne avant qu'il ne soit effectivement intégré dans votre réseau, vous pouvez configurer une cible dans votre périphérique iSCSI, et sur cette cible, configurer un ou plusieurs LUN.

Vous pouvez ajouter des LUN d'une taille supérieure à 2 To si le pool est activé pour les LUN de grande taille.

Les LUN d'une taille supérieure à 2 To (« LUN de grande taille ») ne sont pas prises en charge par les périphériques suivants :

- Périphériques VRM antérieurs à la version 3.60
- Périphériques VSG avec une version de firmware antérieure à la version 6.30
- Encodeurs avec une version de firmware antérieure à la version 6.30



BVMS vous empêche d'effectuer les procédures suivantes :

- Ajouter ou déplacer des périphériques avec une version de firmware antérieure à la version 6.30 vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer des périphériques qui ne sont pas actuellement connectés au réseau, vers un pool qui autorise les LUN de grande taille.
- Ajouter ou déplacer un périphérique iSCSI qui contient des LUN de grande taille, vers un pool qui n'autorise pas les LUN de grande taille.
- Autoriser les LUN de grande taille sur un pool contenant des périphériques avec un firmware dont la version est antérieure à la version 6.30.
- Désactiver les LUN de grande taille sur un pool avec un périphérique iSCSI contenant des LUN de grande taille.

Veillez déplacer les périphériques dont le firmware est d'une version antérieure à la version 6.30 vers un pool qui n'autorise pas les LUN de grande taille.

Pour effectuer un ajout :






1. Si nécessaire, cliquez pour sélectionner **Autoriser les LUN de plus de 2 To**.

2. Cliquez avec le bouton droit de la souris sur  et cliquez sur **Rechercher cible**.
 La cible  est ajoutée.
3. Cliquez sur la cible.
 La page **LUN** s'affiche.
4. Cliquez sur **Ajouter**.
 La boîte de dialogue **Ajouter LUN** s'affiche.
5. Saisissez le nombre de LUN souhaité et cliquez sur **OK**.
 Le LUN est ajouté en tant que nouvelle ligne dans le tableau.
 Répétez cette étape pour chaque LUN souhaité.

Remarques :

- Pour supprimer un LUN, cliquez sur **Supprimer**.
 Les données vidéo restent sur ce LUN.
- Pour formater un LUN, cliquez sur **Formater LUN**.
 Toutes les données de ce LUN sont supprimées.

Boîte de dialogue Ajouter LUN

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  >  > Cliquez sur **Ajouter**
 Permet d'ajouter un LUN.






Id

Saisissez l'identifiant du LUN souhaité.

Se reporter à

- *Page Zone, page 185*
- *Page LUN, page 202*

14.25.10**Formatage d'un LUN**

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > 
 Vous devez formater un LUN pour le préparer à sa première utilisation.

**Remarque!**

Après un formatage, toutes les données du LUN sont perdues.





Pour procéder à une configuration :

1. Sélectionnez le LUN souhaité et cliquez dans la colonne **Format** pour le cocher.
2. Cliquez sur **Formater LUN**.
3. Lisez attentivement le message affiché et confirmez-le si vous le souhaitez.
 Le LUN sélectionné est formaté. Toutes les données de ce LUN sont perdues.

Se reporter à

- *Page LUN, page 202*

14.25.11 Boîte de dialogue iqn-Mapper





Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  >  > **Cartographier les IQN**

Vous permet de débiter le processus de cartographie IQN.

Se reporter à

- *Ajout de dispositifs VRM via un balayage, page 174*
- *Configuration d'un périphérique iSCSI, page 199*




14.26 Page du dispositif Video Streaming Gateway

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > 

Ce chapitre explique comment configurer le dispositif VSG de votre système. Permet d'ajouter et de configurer les types d'encodeurs suivants :

- Encodeurs Bosch
- Encodeurs ONVIF
- Encodeurs JPEG
- Encodeurs RTSP

Pour ajouter des dispositifs VSG via un balayage :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Rechercher les passerelles de diffusion de flux**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
 2. Sélectionnez les dispositifs VSG appropriés, sélectionnez la zone de stockage VRM souhaitée, puis cliquez sur **Affecter** pour les affecter à la zone de stockage VRM.
 3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
 4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit sur ce champ et sélectionnez **Copier la cellule dans la colonne**.
Dans la colonne **État**, les connexions qui ont abouti sont indiquées par le symbole .
les connexions qui ont échoué sont indiquées par le symbole .
 5. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.
- Si vous ajoutez une nouvelle passerelle VSG version 7.0 ou supérieure, la case **Connexion sécurisée** est sélectionnée par défaut.



Pour modifier une connexion sécurisée ou non sécurisée, utilisez la commande **Modifier la passerelle de diffusion de flux**, puis sélectionnez ou désélectionnez la case **Connexion sécurisée**.

Se reporter à


- *Modification d'une passerelle Video Streaming Gateway, page 207*
- *Page ONVIF, page 243*

14.26.1


Ajout manuel d'un composant Video Streaming Gateway

Fenêtre principale > **Périphériques** > Développez  > 
 Vous pouvez ajouter des dispositifs VSG à une zone de stockage VRM.

Pour ajouter un dispositif VSG manuellement :

1. Cliquez avec le bouton droit de la souris sur  et cliquez sur **Ajouter une passerelle de diffusion de flux**.
 La boîte de dialogue **Ajouter une passerelle de diffusion de flux** s'affiche.
2. Définissez les paramètres requis pour votre dispositif VSG.
3. Cliquez sur **Ajouter**.
 ⇒ Le périphérique VSG est ajouté au système. Les caméras affectées à ce périphérique VSG sont enregistrées.

Boîte de dialogue Ajouter une passerelle de diffusion de flux

Cliquez avec le bouton droit de la souris sur la boîte de dialogue  > **Ajouter une passerelle de diffusion de flux** > **Ajouter une passerelle de diffusion de flux**

Nom

Saisissez le nom d'affichage souhaité pour le périphérique.

Nom d'utilisateur

Saisissez le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Généralement : service

Adresse réseau/Port

Saisissez l'adresse IP de votre dispositif.

Si la case **Connexion sécurisée** est sélectionnée, le port bascule automatiquement sur le port HTTPS.

Vous pouvez modifier le numéro de port, si aucun port par défaut n'est utilisé ou si les instances VSG sont configurées dans un ordre différent.

Ports par défaut

Instance VSG	Port rcpp	Port HTTPS
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448

Instance VSG	Port rcpp	Port HTTPS
7	8762	8449

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le périphérique.

Show password

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Sécurité

La case **Connexion sécurisée** est sélectionnée par défaut si le protocole HTTPS est pris en charge.

À compter de VSG version 7.0, VSG prend en charge une connexion sécurisée.

**Remarque!**

Si vous effectuez une migration vers BVMS version 10,0 ou supérieure, la case **Connexion sécurisée** n'est pas sélectionnée par défaut et la connexion n'est pas sécurisée (rcpp).

Pour modifier une connexion sécurisée ou non sécurisée, utilisez la commande **Modifier la passerelle de diffusion de flux**, puis sélectionnez ou désélectionnez la case **Connexion sécurisée**.


Test

Permet de vous authentifier sur le périphérique avec les identifiants saisis précédemment.


Se reporter à

– *Modification d'une passerelle Video Streaming Gateway, page 207*

14.26.2**Modification d'une passerelle Video Streaming Gateway**

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > 

Pour modifier une connexion sécurisée/non sécurisée :

1. Cliquez avec le bouton droit de la souris sur .
2. Cliquez sur **Modifier la passerelle de diffusion de flux**.
La boîte de dialogue **Modifier la passerelle de diffusion de flux** s'affiche.
3. Sélectionnez la case **Connexion sécurisée**.
Le port utilisé change automatiquement sur le port HTTPS.
Ou bien
désélectionnez la case **Connexion sécurisée**.
Le port utilisé change automatiquement sur le port rcpp.





**Remarque!**

Après une mise à niveau vers une version plus récente, nous vous recommandons de changer pour une connexion sécurisée.

Se reporter à

– *Ajout manuel d'un composant Video Streaming Gateway, page 206*

14.26.3 Ajout d'une caméra à un VSG


Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > 

Vous pouvez ajouter les dispositifs suivants à votre VSG :

- Encodeurs de Bosch
- Caméras ONVIF
- Caméras JPEG
- Encodeurs RTSP

Si vous avez ajouté des encodeurs VGS hors ligne, vous pouvez actualiser leur état.

Pour effectuer un ajout :

1. Cliquez avec le bouton droit de la souris sur , pointez sur **Ajouter un encodeur/une caméra**, puis cliquez sur la commande souhaitée.
2. Dans la boîte de dialogue, définissez les paramètres appropriés pour ajouter le périphérique.
3. Cliquez sur **OK**.

Le périphérique est ajouté.

Pour actualiser :





- ▶ Cliquez avec le bouton droit de la souris sur l'encodeur souhaité, puis cliquez sur **Actualiser l'état**.

Les propriétés du dispositif sont extraites.

Se reporter à

- Boîte de dialogue Ajouter un encodeur Bosch, page 208
- Boîte de dialogue Ajouter un encodeur ONVIF, page 209
- Boîte de dialogue Ajouter une caméra JPEG, page 211
- Boîte de dialogue Ajouter un encodeur RTSP, page 212

14.26.4 Boîte de dialogue Ajouter un encodeur Bosch

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > **Ajouter un encodeur/une caméra** > Commande **Encodeur Bosch**

Vous pouvez ajouter un encodeur de Bosch à votre périphérique VSG.

Nom

Saisissez le nom d'affichage souhaité pour le périphérique.

Adresse réseau

Saisissez l'adresse réseau du dispositif.

Type

Affiche le type de périphérique détecté, s'il est pris en charge.

Nom d'utilisateur

Saisissez le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Généralement : service

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le périphérique.

Show password

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Test

Permet de vous authentifier sur le périphérique avec les identifiants saisis précédemment.

Propriétés

Cliquez sur ce bouton pour activer les fonctionnalités souhaitées disponibles pour ce dispositif.

Audio	Cliquez sur ce bouton pour activer le son s'il est disponible sur ce dispositif.
PTZ	Cliquez sur ce bouton pour activer la fonctionnalité PTZ si elle est disponible sur ce dispositif.
Protocole de la caméra	TCP Utilisé pour la transmission sur Internet et/ou la transmission de données sans perte. Garantit qu'aucun paquet de données ne se perd. Les besoins en bande passante peuvent être élevés. Utilisez ce paramètre si le dispositif se trouve derrière un pare-feu. Ne prend pas en charge le multicast. UDP Utilisé pour la transmission de données statique et légère dans des réseaux privés. Il est possible de perdre des paquets de données. Les besoins en bande passante peuvent être faibles. Prend en charge le multicast.
Utiliser l'entrée vidéo 1 - Utiliser l'entrée vidéo 4	Cliquez sur cette option pour sélectionner les entrées vidéo si vous configurez un dispositif multicanal.


Se reporter à

- Ajout d'une caméra à un VSG, page 208

14.26.5

Boîte de dialogue Ajouter un encodeur ONVIF

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > **Ajouter un encodeur/une caméra** > Commande **Ajouter un encodeur ONVIF**
ou

Fenêtre principale > **Périphériques** > Cliquer avec le bouton droit de la souris sur  > Commande **Ajouter un encodeur ONVIF**

Vous pouvez ajouter un encodeur ONVIF au dispositif VSG ou en tant qu'encodeur en temps réel uniquement.

Vous devez configurer le profil utilisé pour l'enregistrement et l'utilisation en temps réel dans le Tableau des caméras.

À partir de BVMS 10,0, les événements d'encodeur ONVIF peuvent être récupérés directement à partir de l'encodeur VSG ou ONVIF. Si vous ajoutez un nouvel encodeur ONVIF, la case **extraire les événements ONVIF de VSG (Profil S, T)** est sélectionnée par défaut et le profil T est pris en charge.

Les fonctions suivantes ne sont prises en charge que si un encodeur ONVIF est ajouté à votre système via un dispositif VSG :

- Si des événements d'encodeur ONVIF sont récupérés de VSG, les événements ONVIF par défaut sont déjà mappés.
- L'opérateur peut activer ou désactiver des relais dans Operator Client.



Remarque!

La récupération des événements ONVIF à partir de VSG est uniquement disponible à partir de la version 7.0 de VSG. Si vous effectuez une migration vers BVMS version 10.0, les événements d'encodeur ONVIF existants sont récupérés directement à partir de l'encodeur ONVIF. Vous devez mettre à jour VSG vers la version 7.0.

Nom

Saisissez le nom d'affichage souhaité pour le périphérique.

Adresse réseau

Saisissez l'adresse réseau du dispositif. Si nécessaire, modifiez le numéro de port.

Nom d'utilisateur

Saisissez le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Généralement : service

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le périphérique.

Show password

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Test

Permet de vous authentifier sur le périphérique avec les identifiants saisis précédemment.

Connexion sécurisée

Vous pouvez activer la connexion sécurisée des vidéos en temps réel transférées à partir d'un encodeur ONVIF vers le dispositif VSG.

Remarque :

Lors de l'activation, l'utilisateur d'Operator Client ne peut pas basculer un flux sur UDP et sur UDP multicast.

Lors de l'activation, ANR ne fonctionne pas pour le dispositif concerné.

Lors de l'activation, la relecture de l'encodeur ne fonctionne pas sur les encodeurs avec un firmware d'une version antérieure à 6.30.

**Remarque!**

Le port 443 est défini par défaut. Vous pouvez modifier le numéro de port de manière à le faire correspondre au port HTTPS configuré sur l'encodeur.

Le numéro de port configuré ne sera pas enregistré.

Propriétés

Type de périphérique	Affiche le type de dispositif récupéré.
Fabricant	Affiche le nom de fabricant récupéré.
Modèle	Affiche le nom de modèle récupéré.
Version du firmware	Affiche la version de firmware récupérée.
Commandes auxiliaires	Si la case est sélectionnée, les commandes auxiliaires sont prises en charge.
Nombre de canaux d'entrées vidéo	Saisissez le nombre d'entrées vidéo souhaité.
Nombre de canaux d'entrées audio	Saisissez le nombre d'entrées audio souhaité.
Nombre d'entrées d'alarme	Saisissez le nombre d'entrées d'alarme souhaité.
Nombre de relais	Saisissez le nombre de relais souhaité.
Canaux de passerelle affectés	Saisissez le nombre de canaux de passerelle souhaité.
Protocole de la caméra	Sélectionnez le protocole de caméra souhaité.
Utiliser l'entrée vidéo {0}	Cochez cette case pour utiliser l'entrée vidéo appropriée.
Profil ONVIF	Si cela est pris en charge, sélectionnez le profil que vous souhaitez configurer.



Remarque!

Les options **Paramètres Video Streaming Gateway** ne sont pas disponibles pour les encodeurs ONVIF qui sont ajoutés en tant qu'encodeur temps réel uniquement.



Se reporter à

– *Ajout d'une caméra à un VSG, page 208*

14.26.6

Boîte de dialogue Ajouter une caméra JPEG

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez

 > Cliquez avec le bouton droit de la souris sur  > **Ajouter un encodeur/une caméra** > Commande **Caméra JPEG**

Vous pouvez ajouter une caméra JPEG à votre dispositif VSG.

Nom

Saisissez le nom d'affichage souhaité pour le périphérique.

URL

Saisissez l'URL de la caméra JPEG ou de la caméra RTSP.

Pour une caméra JPEG de Bosch, saisissez la chaîne suivante :

`http://<ip-address>/snap.jpg?jpegCam=<channel_no.>`

Pour une caméra RTSP de Bosch, saisissez la chaîne suivante :

rtsp://<ip-address>/rtsp_tunnel

Nom d'utilisateur

Saisissez le nom d'utilisateur utilisé pour l'authentification sur le périphérique.
Généralement : service

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le périphérique.

Show password

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Test

Permet de vous authentifier sur le périphérique avec les identifiants saisis précédemment.

Propriétés

Nombre de canaux d'entrées vidéo	Saisissez le nombre d'entrées vidéo disponibles le cas échéant.
Cadence d'images [ips]	Saisissez la cadence d'images souhaitée.

Se reporter à


– *Ajout d'une caméra à un VSG, page 208*

14.26.7

Boîte de dialogue Ajouter un encodeur RTSP

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez



> Cliquez avec le bouton droit de la souris sur  > **Ajouter un encodeur/une caméra** > Commande **Caméra RTSP**

Vous pouvez ajouter un encodeur RTSP à votre dispositif VSG.

Nom

Saisissez le nom d'affichage souhaité pour le périphérique.

URL

Saisissez l'URL de la caméra JPEG ou de la caméra RTSP.

Pour une caméra JPEG de Bosch, saisissez la chaîne suivante :

http://<ip-address>/snap.jpg?jpegCam=<channel_no.>

Pour une caméra RTSP de Bosch, saisissez la chaîne suivante :

rtsp://<ip-address>/rtsp_tunnel

Nom d'utilisateur

Saisissez le nom d'utilisateur utilisé pour l'authentification sur le périphérique.
Généralement : service

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le périphérique.

Show password

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Test

Permet de vous authentifier sur le périphérique avec les identifiants saisis précédemment.

Propriétés





Nombre de canaux d'entrées vidéo	Saisissez le nombre d'entrées vidéo disponibles le cas échéant.
---	---

Se reporter à




- Ajout d'une caméra à un VSG, page 208

14.26.8

Déplacement d'un VSG vers une autre zone de stockage (Modifier la zone de stockage)





Fenêtre principale > **Périphériques** > Développez  > Développez  >  > 
 Vous pouvez déplacer un dispositif d'une zone de stockage vers une autre à l'intérieur du même dispositif VRM sans perdre d'enregistrements.

Pour effectuer un déplacement :

1. Cliquez avec le bouton droit de la souris sur  /  /  , puis cliquez sur **Modification du groupe ...**
 La boîte de dialogue **Modifier le groupe** s'affiche.
2. Dans la liste **Nouveau groupe :**, sélectionnez la zone de stockage souhaitée.
3. Cliquez sur **OK**.
 Le périphérique est déplacé vers la zone de stockage sélectionnée.

14.26.9

Configuration du multicast (onglet Multicast)

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > 

Pour chaque caméra affectée à un dispositif Video Streaming Gateway, vous pouvez configurer une adresse multicast et un port.

Pour configurer le multicast :

1. Cochez la case appropriée pour activer le multicast.
2. Saisissez une adresse multicast valide et un numéro de port.
3. Si nécessaire, configurez une diffusion multicast en continu.

Onglet Multicast

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  >  > Onglet **Réseau** > Onglet **Multicast**

Permet de configurer le mode multicast pour les caméras affectées.

Permettre

Cliquez sur ce bouton pour activer le multicast pour cette caméra.

Adresse multicast

Insérez une adresse multicast valide (comprise dans la plage 224.0.0.0 - 239.255.255.255). Entrez 1.0.0.0. Une adresse multicast unique est automatiquement insérée en fonction de l'adresse MAC du périphérique.

Port



Lorsqu'un pare-feu est utilisé, saisissez la valeur d'un port configuré en tant que port non bloqué dans le pare-feu.

Diffusion

Cliquez sur ce bouton pour activer la diffusion multicast en continu sur le commutateur. Cela signifie que la connexion multicast n'est pas précédée d'une inscription RCP+. L'encodeur diffuse toujours toutes les données vers le commutateur. En retour, le commutateur (si aucun filtrage multicast IGMP n'est pris en charge ni configuré) envoie ces données à tous les ports, ce qui surcharge le commutateur. Vous avez besoin de la diffusion pour pouvoir recevoir un flux multicast avec un périphérique non fabriqué par Bosch.

14.26.10

Configuration de la journalisation (onglet Avancé)

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  >  > Onglet **Administration** > Onglet **Avancé**

Permet d'activer la journalisation pour la passerelle de flux vidéo.

Les fichiers journaux sont généralement stockés dans l'emplacement suivant :

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

À compter de VSG version 7.0, les fichiers journaux sont généralement stockés dans l'emplacement suivant :

```
C:\ProgramData\Bosch\VSG\log
```

Remarque : Si vous effectuez une mise à niveau vers VSG 7.0 ou version ultérieure, les fichiers journaux précédents sont automatiquement déplacés vers cet emplacement. Les fichiers journaux des versions antérieures de VSG sont généralement stockés dans le chemin suivant :

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

Onglet Avancé

Journalisation RCP+

Cliquez sur cette option pour activer la journalisation RCP+.

Débogage journalisation

Cliquez sur cette option pour activer la journalisation du débogage.

Journalisation RTP

Cliquez sur cette option pour activer la journalisation RTP.

Durée de conservation (en jours)

Sélectionnez le nombre de jours souhaité.

Fichier de vidage de mémoire complet

N'activez cette case qu'en cas de besoin, par exemple, si l'équipe technique du Service clientèle vous demande un historique complet de la mémoire principale.

Prise en charge Telnet

Activez cette case si l'accès avec le protocole Telnet doit être pris en charge. N'activez cette case qu'en cas de besoin.







Remarque!

Une journalisation étendue nécessite un processeur extrêmement puissant, ainsi qu'un disque dur doté d'une capacité importante.

N'utilisez pas la journalisation étendue en fonctionnement continu.

14.26.11 Démarrage de ONVIF Camera Event Driver Tool à partir de Configuration Client

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > 

Vous pouvez démarrer ONVIF Camera Event Driver Tool directement à partir de Configuration Client pour certaines passerelles VSG.

Remarque : vous pouvez également démarrer l'outil à partir du menu de démarrage Windows.

ONVIF Camera Event Driver Tool vous permet de mapper des événements ONVIF aux événements BVIP de la passerelle VSG. Vous pouvez vous connecter à des caméras ONVIF et extraire les événements ONVIF en vue d'un mappage.

Pour démarrer ONVIF Camera Event Driver Tool à partir de Configuration Client :

1. Cliquez avec le bouton droit sur la passerelle VSG appropriée.
2. Cliquez sur **Démarrer ONVIF Camera Event Driver Tool**.
ONVIF Camera Event Driver Tool s'affiche.



Remarque!

ONVIF Camera Event Driver Tool prend uniquement en charge une connexion sécurisée à la passerelle VSG.

Pour utiliser ONVIF Camera Event Driver Tool :

Regardez la [vidéo de procédure](#).

14.27 Page Temps Réel Uniquement

Fenêtre principale > **Périphériques** > Développez  > 

Permet d'ajouter et de configurer les encodeurs pour le temps réel uniquement. Vous pouvez ajouter des encodeurs Bosch et des émetteurs vidéo de réseau ONVIF.


Pour ajouter, modifier et configurer un encodeur ONVIF temps réel uniquement, reportez-vous à la [Page ONVIF, page 243](#).

Se reporter à

- *Ajout d'un encodeur temps réel uniquement, page 225*
- *Recherche de périphériques, page 74*
- *Page Encodeur / Décodeur / Caméra Bosch, page 222*
- *Page ONVIF, page 243*
- *Configuration du multicast, page 242*

14.27.1 Ajout de dispositifs temps réel uniquement via un balayage

Pour ajouter des dispositifs Bosch en temps réel uniquement via un balayage :


1. Cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Rechercher des encodeurs en temps réel uniquement**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Cochez les boîtes de dialogue des dispositifs que vous souhaitez ajouter.

3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit de la souris sur ce champ, puis cliquez sur **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions réussies sont indiquées par .

Les connexions qui ont échoué sont indiquées par .


5. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.


L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

14.27.2

Ajout manuel d'un encodeur

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**
ou

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**
ou

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**
ou




Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter décodeur** > Boîte de dialogue **Ajouter encodeur**

Vous permet d'ajouter un encodeur manuellement. Cette fonction s'avère très utile lorsque vous souhaitez ajouter un périphérique vidéo IP de Bosch (uniquement pour VRM).

Remarque :


Si vous ajoutez un encodeur vidéo IP de Bosch avec l'option **<Détection automatique>**, ce dispositif doit être disponible sur le réseau.

Pour ajouter un dispositif vidéo IP Bosch :

1. Développez , puis , cliquez avec le bouton droit de la souris sur .
Ou

cliquez avec le bouton droit de la souris sur .

Ou


cliquez avec le bouton droit de la souris sur  .

2. Cliquez sur **Ajouter encodeur**.
La boîte de dialogue **Ajouter un encodeur** s'affiche.
3. Saisissez l'adresse IP correspondante.
4. Dans la liste, sélectionnez **<Détection automatique>**, saisissez le mot de passe du dispositif et cliquez sur **Authentifier**.

Ou

Dans la liste, sélectionnez un type d'encodeur concret ou **<Caméra avec un seul espace réservé>**.

5. Cliquez sur **OK**.
Le dispositif est ajouté au système.

L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

Boîte de dialogue Ajouter encodeur

Adresse réseau

Saisissez une adresse IP valide.

Type d'encodeur

Pour les dispositifs dont le type est connu, sélectionnez l'entrée correspondante. Le périphérique ne doit pas obligatoirement être disponible sur le réseau.

Si vous souhaitez ajouter un dispositif vidéo IP de Bosch, sélectionnez **<Détection automatique>**. Le dispositif doit être disponible sur le réseau.

Si vous souhaitez ajouter une caméra pour une configuration hors ligne, sélectionnez **<Caméra avec un seul espace réservé>**.

Nom d'utilisateur

Affiche le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le dispositif.

Afficher le mot de passe

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.


Authentifier

Permet de vous authentifier sur le dispositif avec les identifiants saisis précédemment.

14.27.3

Indication du mot de passe de destination d'un décodeur (Authentifier...)

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec

le bouton droit de la souris sur  > Cliquez sur **Authentifier...** > Boîte de dialogue **Entrer le mot de passe**

Pour activer l'accès d'un encodeur protégé par mot de passe à un décodeur, vous devez saisir le mot de passe de niveau d'autorisation Utilisateur de l'encodeur comme mot de passe de destination du décodeur.

Pour fournir un mot de passe :

1. Dans la liste **Entrez le nom de l'utilisateur**, sélectionnez destination password.
 2. Dans le champ **Entrez le mot de passe de l'utilisateur**, saisissez le nouveau mot de passe.
 3. Cliquez sur **OK**.
- ⇒ Le mot de passe est immédiatement modifié sur le dispositif.

Se reporter à


- *Modification du mot de passe d'un encodeur / décodeur (modifier mot de passe / entrer mot de passe), page 146*

14.28**Page Stockage local**

Fenêtre principale > **Périphériques** > Développez  > 

Permet d'ajouter et de configurer des encodeurs à stockage local.


Pour ajouter des encodeurs à stockage local via un balayage :

1. Dans l'arborescence des dispositifs, cliquez avec le bouton droit de la souris sur  et cliquez sur **Rechercher les encodeurs à stockage local**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Cochez les boîtes de dialogue des dispositifs que vous souhaitez ajouter.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit de la souris sur ce champ, puis cliquez sur **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions réussies sont indiquées par .

Les connexions qui ont échoué sont indiquées par .

5. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.

L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

Se reporter à

- *Configuration du multicast, page 242*
- *Ajout d'un encodeur pour stockage local, page 225*
- *Page Encodeur / Décodeur / Caméra Bosch, page 222*
- *Recherche de périphériques, page 74*

14.29**Page Unmanaged Site**

Fenêtre principale > **Périphériques** > Développez  > 

Vous pouvez ajouter un dispositif vidéo réseau à l'élément **Unmanaged Sites** de l'arborescence des dispositifs.

On suppose que tous les dispositifs réseau non gérés d'un unmanaged site se trouvent dans la même fuseau horaire.

Nom du site

Affiche le nom du site qui a été saisi lors de la création de cet élément.

Description

Saisissez une description pour ce site.

Fuseau horaire


Sélectionnez le fuseau horaire de ce unmanaged site.

Se reporter à


- *Unmanaged site, page 26*
- *Ajout manuel d'un élément unmanaged site, page 219*
- *Importation de sites non gérés, page 219*
- *Configuration du fuseau horaire, page 221*

14.29.1

Ajout manuel d'un élément unmanaged site

Fenêtre principale > **Périphériques** > 

Pour procéder à une création :


1. Cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Ajouter un Unmanaged Site**.
La boîte de dialogue **Ajouter un Unmanaged Site** s'affiche.
2. Tapez un nom de site et une description.
3. Dans la liste **Fuseau horaire**, sélectionnez l'entrée appropriée.
4. Cliquez sur **OK**.
Un nouvel élément unmanaged site est ajouté au système.

Se reporter à

- *Unmanaged site, page 26*
- *Page Unmanaged Site, page 218*


14.29.2

Importation de sites non gérés

Fenêtre principale > **Périphériques** > 

Vous pouvez importer un fichier CSV contenant la configuration d'un enregistreur numérique ou un autre BVMS que vous souhaitez importer dans votre système BVMS comme un élément unmanaged site.

Pour effectuer une importation :

1. Cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Importer les Unmanaged Sites**.
2. Cliquez sur le fichier que vous souhaitez importer, puis cliquez sur **Ouvrir**.
Un nouveau unmanaged site (ou plusieurs) est ajouté au système.
Vous pouvez désormais ajouter cet élément unmanaged sites à l'arborescence logique.

Remarque : Si une erreur se produit et que le fichier ne peut pas être importé, un message d'erreur vous en informe.

14.29.3 Page Unmanaged Site

Nom du site

Affiche le nom du site qui a été saisi lors de la création de cet élément.

Description

Saisissez une description pour ce site.

Fuseau horaire

Sélectionnez le fuseau horaire de ce unmanaged site.

14.29.4 Ajout d'un dispositif réseau non géré

Fenêtre principale > **Périphériques** >  > 

1. Cliquez avec le bouton droit de la souris sur cet élément, puis cliquez sur **Ajouter un périphérique réseau Unmanaged**.

La boîte de dialogue **Ajouter un périphérique réseau Unmanaged** s'affiche.

2. Sélectionnez le type de dispositif souhaité.
3. Saisissez une adresse IP ou un nom d'hôte valide et les identifiants pour ce dispositif.
4. Cliquez sur **OK**.

Un nouvel élément **Périphérique réseau unmanaged** est ajouté au système.

Vous pouvez désormais ajouter cet élément unmanaged site à l'arborescence logique.

Veillez noter que seul le site est visible dans l'arborescence logique, mais pas les dispositifs réseau appartenant à ce site.

5. Saisissez le nom d'utilisateur valide pour ce dispositif réseau, le cas échéant.
6. Saisissez le mot de passe valide, si disponible.

Boîte de dialogue Ajouter un périphérique réseau Unmanaged

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la

souris sur  > Cliquez sur **Ajouter un périphérique réseau Unmanaged**

Type périphérique :

Sélectionnez l'entrée qui s'applique à ce dispositif.

Entrées disponibles :

- **DIVAR AN / DVR**
- **DIVAR IP (AiO), BVMS**
- **Caméra IP / encodeur Bosch**

Adresse réseau:

Saisissez une adresse IP ou un nom d'hôte. Si nécessaire, modifiez le numéro de port.

Remarque : si vous utilisez une connexion SSH, saisissez l'adresse au format suivant : **ssh://IP ou nomserveur:5322**

Sécurité

La case **HTTPS** est cochée par défaut.



Remarque!

Si vous ajoutez un enregistreur numérique et que la case **HTTPS** est cochée, les connexions de commande et de contrôle sont sécurisées. Le flux de données vidéo n'est pas sécurisé.

Nom d'utilisateur:

Saisissez le nom d'utilisateur valide pour ce dispositif réseau, le cas échéant. Pour plus d'informations, voir *Unmanaged site*, page 26.

Mot de passe:

Saisissez le mot de passe valide, le cas échéant. Consultez *Unmanaged site*, page 26 pour plus d'informations sur les identifiants d'utilisateur.

Se reporter à

– *Unmanaged site*, page 26

14.29.5**Configuration du fuseau horaire**

Fenêtre principale > **Périphériques** > Développer

Vous pouvez configurer le fuseau horaire d'un unmanaged site. Cela est utilisé lorsqu'un utilisateur d'Operator Client veut accéder à un unmanaged site à l'aide d'un ordinateur doté d'Operator Client situé dans un fuseau horaire différent de celui de ce unmanaged site.

Pour configurer le fuseau horaire :

- ▶ Dans la liste **Fuseau horaire**, sélectionnez l'entrée appropriée.

Se reporter à

– *Page Unmanaged Site*, page 218

15 Page Encodeur / Décodeur / Caméra Bosch

Ce chapitre explique comment configurer les encodeurs et les décodeurs de votre système.







Remarque!






BVMS Viewer ne prend pas en charge les décodeurs.

Pour obtenir des informations détaillées sur les paramètres de l'encodeur, du décodeur ou de la caméra, par exemple Video Content Analysis (VCA) ou les paramètres réseau, reportez-vous au manuel du dispositif correspondant.

Le nombre d'éléments au-dessous d'une entrée est affiché entre crochets.

Pour configurer un encodeur :

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > 

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  >  > 


ou

Fenêtre principale > **Périphériques** >  > 

Fenêtre principale > **Périphériques** >  > 

Pour configurer un décodeur :

Fenêtre principale > **Périphériques** > Développez  > Développez  > 

Pour plus de détails, reportez-vous à l'aide en ligne des pages  .

Pour configurer une caméra :

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > 

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > 

> 

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez 




 >  > 

ou


Fenêtre principale > **Périphériques** >  >  > 


ou

Fenêtre principale > **Périphériques** >  >  > 

- Cliquez sur  pour enregistrer les paramètres.
- Cliquez sur  pour annuler le dernier paramètre.
- Cliquez sur  pour activer la configuration.

La plupart des paramètres des pages relatives aux encodeurs / décodeurs / caméras

deviennent immédiatement effectifs lorsque vous cliquez sur . Si vous cliquez sur un

autre onglet, en omettant de cliquer sur  alors que des modifications ont été opérées, deux messages s'affichent. Confirmez-les tous les deux si vous souhaitez conserver les modifications.

Pour modifier les mots de passe d'un encodeur, cliquez avec le bouton droit de la souris sur l'icône du dispositif, puis cliquez sur **Modifier le mot de passe...**


Pour afficher le dispositif dans un navigateur Web, cliquez avec le bouton droit de la souris sur l'icône du dispositif, puis cliquez sur **Afficher la page Web dans le navigateur**.

Remarque :

Selon l'encodeur ou la caméra sélectionné(e), il se peut que toutes les pages décrites ici ne soient pas disponibles pour chaque dispositif. Les termes utilisés ici pour décrire les noms des champs peuvent être différents de ceux de votre logiciel.

- ▶ Cliquez sur un onglet pour afficher la page de propriété correspondante.


Pour ajouter un encodeur via un balayage :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Rechercher des encodeurs**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Sélectionnez les encodeurs appropriés, sélectionnez la zone de stockage VRM souhaitée, puis cliquez sur **Affecter** pour les affecter à la zone de stockage VRM.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit de la souris sur ce champ, puis cliquez sur **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions réussies sont indiquées par .

Les connexions qui ont échoué sont indiquées par .

5. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.

L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.


Se reporter à


– Recherche de périphériques, page 74


15.1

Ajout manuel d'un encodeur

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec

le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**
ou

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**
ou

Fenêtre principale > **Périphériques** > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter encodeur** > Boîte de dialogue **Ajouter encodeur**
ou




Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Ajouter décodeur** > Boîte de dialogue **Ajouter encodeur**

Vous permet d'ajouter un encodeur manuellement. Cette fonction s'avère très utile lorsque vous souhaitez ajouter un périphérique vidéo IP de Bosch (uniquement pour VRM).


Remarque :

Si vous ajoutez un encodeur vidéo IP de Bosch avec l'option **<Détection automatique>**, ce dispositif doit être disponible sur le réseau.

Pour ajouter un dispositif vidéo IP Bosch :

1. Développez , puis , cliquez avec le bouton droit de la souris sur .
Ou

cliquez avec le bouton droit de la souris sur .
Ou

cliquez avec le bouton droit de la souris sur .

2. Cliquez sur **Ajouter encodeur**.

La boîte de dialogue **Ajouter un encodeur** s'affiche.


3. Saisissez l'adresse IP correspondante.

4. Dans la liste, sélectionnez **<Détection automatique>**, saisissez le mot de passe du dispositif et cliquez sur **Authentifier**.

Ou

Dans la liste, sélectionnez un type d'encodeur concret ou **<Caméra avec un seul espace réservé>**.

5. Cliquez sur **OK**.
Le dispositif est ajouté au système.

L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

Boîte de dialogue Ajouter encodeur

Adresse réseau

Saisissez une adresse IP valide.

Type d'encodeur

Pour les dispositifs dont le type est connu, sélectionnez l'entrée correspondante. Le périphérique ne doit pas obligatoirement être disponible sur le réseau.

Si vous souhaitez ajouter un dispositif vidéo IP de Bosch, sélectionnez **<Détection automatique>**. Le dispositif doit être disponible sur le réseau.

Si vous souhaitez ajouter une caméra pour une configuration hors ligne, sélectionnez **<Caméra avec un seul espace réservé>**.

Nom d'utilisateur

Affiche le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le dispositif.

Afficher le mot de passe

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Authentifier

Permet de vous authentifier sur le dispositif avec les identifiants saisis précédemment.

15.2 Ajout d'un encodeur à une zone de stockage VRM

Pour ajouter des encodeurs à une zone de stockage VRM, voir *Ajout d'encodeurs via un balayage*, page 183.

Se reporter à

- *Ajout d'un dispositif*, page 127

15.3 Ajout d'un encodeur temps réel uniquement

Pour ajouter un encodeur temps réel uniquement via un balayage, voir *Ajout de dispositifs temps réel uniquement via un balayage*, page 215.

Se reporter à

- *Ajout d'un dispositif*, page 127
- *Page Temps Réel Uniquement*, page 215

15.4 Ajout d'un encodeur pour stockage local

Pour ajouter des encodeurs à stockage local via un balayage, voir *Page Stockage local*, page 218.

Se reporter à

- *Ajout d'un dispositif*, page 127

– Page Stockage local, page 218

15.5 Ajout d'une caméra avec un seul espace réservé

Si vous souhaitez ajouter et configurer une caméra qui est actuellement hors ligne, vous pouvez ajouter une caméra avec un seul espace réservé à la place. Vous pouvez ajouter la caméra avec un seul espace réservé à l'arborescence logique et aux cartes, et également configurer des événements et des alarmes.

Pour ajouter une caméra avec un seul espace réservé

1. Cliquez avec le bouton droit de la souris sur l'élément de l'arborescence de dispositifs dans lequel vous souhaitez ajouter la caméra avec espace réservé.
2. Cliquez sur **Ajouter encodeur**.
La boîte de dialogue **Ajouter encodeur** s'affiche.
3. Saisissez une adresse IP correspondante qui est actuellement hors ligne.
4. Sélectionnez le type d'encodeur **<Caméra avec un seul espace réservé>**.
5. Configurez tous les paramètres adéquats pour la caméra avec espace réservé.

Pour remplacer une caméra avec espace réservé

1. Cliquez avec le bouton droit de la souris sur la caméra avec espace réservé correspondante.
2. Cliquez sur **Modifier l'encodeur**.
La boîte de dialogue **Modifier l'encodeur** s'affiche.
3. Saisissez l'adresse réseau de la caméra de remplacement.
4. Saisissez le mot de passe correct de la caméra de remplacement.
5. Cliquez sur **OK**.
La boîte de dialogue **Mise à jour des noms de périphérique** s'affiche.
6. Cliquez sur **OK**.

Remarque : lorsque les fonctions de la caméra de remplacement sont à jour, vous devez vérifier les paramètres créés dans le tableau des caméras et des enregistrements.

15.6 Importation de caméras à partir d'un fichier CSV

Fenêtre principale > **Périphériques** > Développer  > Développer 

Vous pouvez importer un plus grand nombre de caméras à partir d'un fichier CSV. Vous pouvez spécifier le nom de l'encodeur ou de la caméra, les arborescences logiques et les groupes d'utilisateurs qui ont accès aux caméras nouvellement ajoutées.

Modèle CSV

Vous pouvez utiliser le modèle MassConfigurationTemplate.csv sous : C:\Program Files\Bosch\VMS\Samples.

Remarque : utilisez la virgule comme délimiteur de colonnes CSV.

Colonne	Information
NetworkAddress	Adresse IP de l'encodeur. Cette valeur ne peut pas être vide et ne peut pas être dupliquée.
EncoderName	Nom de l'encodeur. Cette valeur ne peut pas être vide.

Colonne	Information
CameraNames	Nom des caméras de l'encodeur en cours. Cette valeur ne peut pas être vide. Séparez les différentes caméras par un point-virgule.
UserName	Nom de l'utilisateur pour l'authentification sur l'encodeur. Cette valeur peut être vide.
Password	Mot de passe pour l'authentification sur l'encodeur. Cette valeur peut être vide.
LogicalTree	Chemins de l'arborescence logique dans laquelle vous ajoutez les caméras. Séparez les différents chemins par un point-virgule. Si la valeur est vide, les caméras ne sont pas ajoutées à l'arborescence logique et vous ne pouvez affecter aucun groupe d'utilisateurs. Les chemins de l'arborescence logique commencent par « / ». Le signe « / » est uniquement obligatoire pour le nœud racine ; il est facultatif pour les autres dossiers. Il n'est pas nécessaire d'ajouter le nom du nœud racine au chemin du dossier. Si un chemin d'accès n'existe pas, il est créé.
Permissions	Groupes d'utilisateurs autorisés. Séparez les différents groupes d'utilisateurs par un point-virgule. Si la valeur est vide, les caméras doivent être accessibles par tous les groupes. Le groupe admin est autorisé à accéder à toutes les caméras. Si vous ne souhaitez pas donner accès à un groupe, vous devez tout de même ajouter le groupe admin. Si le groupe d'utilisateurs n'existe pas, la caméra ne sera pas importée. Remarque : Les Enterprise User Groups ne ont pas pris en charge, uniquement les Enterprise Accounts.

Exemples :


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

Les trois autorisations suivantes sont requises avant de commencer l'importation :

- **Modifier les propriétés de périphérique**
- **Modifier l'arborescence logique**
- **Configurer les groupes d'utilisateurs/comptes Enterprise Accounts**

Remarque : Un utilisateur admin peut toujours procéder à l'importation.

Pour importer des caméras à partir d'un fichier CSV :





1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Importer des caméras depuis un fichier CSV...**
L'explorateur de fichiers s'ouvre.
2. Sélectionnez le fichier CSV approprié et cliquez sur **Ouvrir**.
Remarque : Le traitement du fichier CSV peut prendre un certain temps. Le nombre maximal de caméras pouvant être importées est de 250.
3. La boîte de dialogue **Importation de caméras depuis un fichier CSV** affiche toutes les informations pertinentes sur les importations de caméras, qu'elles aient réussi ou échoué.
Cliquez sur **Afficher uniquement les pannes** pour voir toutes les caméras importées.
4. Cliquez sur **Fermer** pour fermer la boîte de dialogue ou sur **Exporter un fichier** pour exporter et enregistrer un fichier journal.

15.7



Modification d'un encodeur

15.7.1

Chiffrement de vidéo en temps réel (Modifier l'encodeur)

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Cliquez sur  > Boîte de dialogue **Modifier l'encodeur**

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Boîte de dialogue **Modifier l'encodeur**

Fenêtre principale > **Périphériques** > Développez  > Cliquez sur  > Boîte de dialogue **Modifier l'encodeur**

Vous pouvez activer la connexion sécurisée des vidéos en temps réel transférées à partir d'un encodeur vers les dispositifs suivants si le port 443 HTTPS est configuré sur l'encodeur :

- Ordinateur Operator Client
- Ordinateur Management Server
- Ordinateur Configuration Client
- Ordinateur VRM
- Décodeur

Remarque :

Lors de l'activation, ANR ne fonctionne pas pour le dispositif concerné.

Lors de l'activation, la relecture de l'encodeur ne fonctionne pas sur les encodeurs avec un firmware d'une version antérieure à 6.30.

Seul l'encodeur doté de la version 7,0 ou supérieure du firmware prend en charge Secure UDP. Lorsque la connexion sécurisée est activée dans ce cas, l'utilisateur d'Operator Client peut basculer un flux vers UDP et UDP multicast.

Pour activer :

1. Cochez la case **Connexion sécurisée**.
2. Cliquez sur **OK**.
La connexion sécurisée est activée pour cet encodeur.



Se reporter à

- *Configuration du multicast, page 242*
- *Boîte de dialogue Modifier encodeur / décodeur, page 229*

15.7.2**Mise à jour des fonctions du dispositif (Modifier l'encodeur)**

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier l'encodeur** > Boîte de dialogue **Modifier l'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier l'encodeur** > Boîte de dialogue **Modifier l'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier l'encodeur** > Boîte de dialogue **Modifier l'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier le décodeur** > Boîte de dialogue **Modifier le décodeur**

Après une mise à niveau du périphérique, vous pouvez mettre à jour les fonctions du périphérique. Un message vous informe si les fonctions récupérées du périphérique correspondent à celles enregistrées dans BVMS.

Pour mettre à jour :



1. Cliquez sur **OK**.
Une boîte de message s'affiche avec le texte suivant :
Si vous appliquez les fonctions du périphérique, il se peut que les paramètres d'enregistrement soient modifiés. Vérifiez ces paramètres pour ce périphérique.
2. Cliquez sur **OK**.
Les fonctions du périphérique sont mises à jour.



Se reporter à

- *Boîte de dialogue Modifier encodeur / décodeur, page 229*

15.7.3**Boîte de dialogue Modifier encodeur / décodeur**

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier l'encodeur** > Boîte de dialogue **Modifier l'encodeur**
ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier l'encodeur** > Boîte de dialogue **Modifier l'encodeur** ou

Fenêtre principale > **Périphériques** > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier l'encodeur** > Boîte de dialogue **Modifier l'encodeur** ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Modifier le décodeur** > Boîte de dialogue **Modifier le décodeur**

Permet de vérifier et de mettre à jour les fonctionnalités d'un dispositif. À l'ouverture de cette boîte de dialogue, le périphérique est connecté. Le mot de passe est vérifié et les fonctions de ce périphérique sont comparées à celles enregistrées dans BVMS.

Nom

Affiche le nom du dispositif. Lorsque vous ajoutez un dispositif vidéo IP de Bosch, son nom est généré. Modifiez les valeurs si nécessaire.

Adresse réseau

Saisissez l'adresse réseau du dispositif. Si nécessaire, modifiez le numéro de port.

Nom d'utilisateur

Affiche le nom d'utilisateur utilisé pour l'authentification sur le périphérique.

Mot de passe

Saisissez un mot de passe valide pour vous authentifier sur le dispositif.

Afficher le mot de passe

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Authentifier

Permet de vous authentifier sur le dispositif avec les identifiants saisis précédemment.

Sécurité

La case **Connexion sécurisée** est cochée par défaut.

Si aucune connexion sécurisée n'est possible, un message s'affiche. Cliquez sur ce bouton pour effacer la sélection.

Les décodeurs suivants prennent en charge une connexion sécurisée :

- VJD 7000
- VJD 8000
- VIP XD HD



Remarque!

La connexion entre un décodeur et un encodeur est uniquement sécurisée, si les deux sont configurés avec une connexion sécurisée.

Flux vidéo

UDP : permet la diffusion multidiffusion chiffrée pour les décodeurs pris en charge.

TCP : permet la diffusion monodiffusion chiffrée pour les décodeurs pris en charge.

Remarque : si aucune adresse multidiffusion n'est configurée pour un encodeur, le décodeur récupère le flux par monodiffusion.



Remarque!

BVMS ne prend pas en charge les caméras Bosch connectées à un VSG.

BVMS ne prend en charge que le chiffrement UDP pour les plates-formes plus anciennes que CPP13.

Fonctions du périphérique

Permet de trier les fonctions affichées par catégorie ou par ordre alphabétique.

Un message vous informe si les fonctions détectées correspondent aux fonctions actuelles du périphérique.

Cliquez sur **OK** pour appliquer les modifications des fonctions après une mise à niveau du périphérique.

Se reporter à

- *Chiffrement de vidéo en temps réel (Modifier l'encodeur), page 228*
- *Mise à jour des fonctions du dispositif (Modifier l'encodeur), page 229*

15.8

Gestion de la vérification d'authenticité

Pour activer la vérification d'authenticité sur un encodeur, vous devez effectuer les opérations suivantes :

- Configurez l'authentification sur l'encodeur.
- Téléchargez un certificat à partir de l'encodeur.
- Installez ce certificat d'encodeur sur le poste de travail utilisé pour la vérification d'authenticité.

Se reporter à

- *Vérification d'authenticité , page 231*

15.8.1

Vérification d'authenticité

L'utilisateur d'Operator Client peut vérifier l'authenticité des enregistrements. L'authenticité des exportations est vérifiée automatiquement.

L'administrateur peut procéder comme suit pour garantir une chaîne de certificat non rompue. Pour les systèmes de grande taille (>30 caméras), nous recommandons la procédure suivante :

- Laissez votre autorité de certificat (CA) émettre un certificat pour chaque encodeur.
- Chargez le certificat émis (y compris la clé privée) de manière sécurisée sur chaque encodeur.
- Installez le certificat CA sur les postes de commande Operator Client sur lesquels vous souhaitez effectuer la vérification d'authenticité ou sur d'autres ordinateurs sur lesquels vous souhaitez effectuer les exportations.

Pour les systèmes de petite taille (< 30 caméras), nous recommandons la procédure suivante :

- Téléchargez le certificat `HTTPS Server` de chaque encodeur.
- Installez ces certificats sur les postes de travail d'Operator Client où vous voulez effectuer la vérification d'authenticité.

Renseignez-vous auprès du support informatique de votre entreprise.

Pour activer la vérification sécurisée de l'authenticité, l'administrateur doit procéder comme suit :

- Activez l'authentification sur chaque caméra souhaitée.
- Pour les systèmes de grande taille : Chargez et affectez le certificat approprié sur chaque caméra souhaitée.
- Pour les systèmes de petite taille : téléchargez un certificat de chaque encodeur. Installez les certificats autorisant la vérification sur un poste de travail.

Limitations

Le firmware version 6.30 ou suivante est requis.

Nous vous recommandons de vérifier l'authenticité d'au maximum 4 caméras en même temps.

L'utilisateur d'Operator Client ne peut pas vérifier l'authenticité de la vidéo en temps réel.

Remarque : Ne modifiez pas le certificat lorsqu'un enregistrement est en cours. Si vous devez modifier le certificat, arrêtez d'abord l'enregistrement, modifiez le certificat, et redémarrez l'enregistrement.

Pour vérifier l'authenticité d'un enregistrement, ce dernier est relu en processus d'arrière-plan à vitesse maximale. Sur les réseaux à faible bande passante, la lecture peut être lente. Le processus de vérification peut être aussi long que la période sélectionnée pour la vérification. Exemple : Vous sélectionnez une période de 1 heure. Le processus de vérification peut prendre jusqu'à 1 heure.

L'utilisateur peut uniquement vérifier qu'un enregistrement est authentique. Si le processus de vérification échoue, cela ne signifie pas nécessairement que la vidéo a été trafiquée. De nombreuses autres raisons peuvent être responsables de cet échec, par exemple une suppression manuelle. L'utilisateur d'Operator Client ne peut pas faire de distinction entre une modification intentionnelle de l'enregistrement et une manipulation frauduleuse.

L'authentification vidéo utilise seulement des méthodes de validation de l'authenticité d'une vidéo. L'authentification vidéo ne vérifie en aucun cas la transmission de vidéo, ou de données.

La fonction de filigrane pour la vérification de l'authenticité dans les versions antérieures de BVMS est remplacée. La nouvelle vérification d'authenticité est automatiquement disponible après une mise à niveau vers la dernière version de BVMS. Les vérifications d'authenticité qui réussissaient par le passé ne peuvent plus désormais être effectuées car ces enregistrements ne comportent pas les informations étendues requises.

La vérification de l'authenticité n'est pas prise en charge dans les cas suivants :





- Transcodage
- Enregistrement local
- VSG
- Enregistreur vidéo numérique
- Bosch Recording Station
- ANR

Se reporter à



- *Configuration de l'authentification, page 232*
- *Chargement d'un certificat, page 233*
- *Téléchargement d'un certificat, page 233*
- *Installation d'un certificat sur un poste de travail, page 234*

15.8.2

Configuration de l'authentification

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > 

ou





Fenêtre principale > **Périphériques** > Développez  >  >
vous pouvez activer la vérification d'authenticité sur un encodeur.

Pour procéder à une configuration :



1. Cliquez sur **Caméra**, puis sur **Entrée vidéo**.
2. Dans la liste **Authentification vidéo**, sélectionnez **SHA-256**.
3. Dans la liste **Intervalles de signature**, sélectionnez la valeur souhaitée.
Une petite valeur améliore la sécurité, une valeur élevée réduit la charge de l'encodeur.

4. Cliquez sur  .

15.8.3 Chargement d'un certificat

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  >  >

ou





Fenêtre principale > **Périphériques** > Développez  >  >
Vous pouvez charger un certificat dérivé vers un encodeur.

Pour effectuer le chargement :



1. Cliquez sur **Administration**, puis sur **Certificats**.
2. Cliquez sur **Charger certificat**.
3. Sélectionnez le fichier approprié contenant le certificat de cet encodeur. Ce fichier doit contenir la clé privée, par exemple, *.pem.
Garantissez une transmission de données sécurisée.
4. Cliquez sur **Ouvrir**.
5. Dans la liste **Utilisation**, sélectionnez **Serveur HTTPS** pour affecter le certificat chargé à l'entrée **Serveur HTTPS**.

6. Cliquez sur  .

15.8.4 Téléchargement d'un certificat

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  >  >

ou

Fenêtre principale > **Périphériques** > Développez  >  >
Vous pouvez télécharger un certificat à partir d'un encodeur.

Pour effectuer le téléchargement :

1. Cliquez sur **Administration**, puis sur **Certificats**.
2. Sélectionnez le certificat souhaité, puis cliquez sur l'icône *Save*.
3. Sélectionnez le répertoire approprié pour l'enregistrement du fichier de certificat.
4. Renommez l'extension de fichier du fichier de certificat en *.cer.


Vous pouvez désormais installer ce certificat sur le poste de travail où vous souhaitez vérifier l'authenticité.

15.8.5 Installation d'un certificat sur un poste de travail

Vous pouvez installer le certificat que vous avez téléchargé à partir d'un encodeur, sur un poste de travail où vous souhaitez effectuer la vérification d'authenticité.

1. Sur le poste de travail, démarrez la `Microsoft Management Console`.
2. Ajoutez le code enfichable `Certificates` sur cet ordinateur avec l'option `Computer account` sélectionnée.
3. Développez `Certificates (Local computer)`, puis `Trusted Root Certification Authorities`.
4. Cliquez avec le bouton droit de la souris sur `Certificates`, pointez sur `All Tasks`, puis cliquez sur `Import...`
L'`Certificate Import Wizard` s'affiche.
L'option `Local Machine` est présélectionnée et ne peut pas être modifiée.
5. Cliquez sur `Next`.
6. Sélectionnez le fichier de certificat téléchargé depuis l'encodeur.
7. Cliquez sur `Next`.
8. Conservez les paramètres, puis cliquez sur `Next`.
9. Conservez les paramètres, puis cliquez sur `Finish`.

15.9 Indication du mot de passe de destination d'un décodeur (Authentifier...)

Fenêtre principale > **Périphériques** > Développez  > Développez  > Cliquez avec le bouton droit de la souris sur  > Cliquez sur **Authentifier...** > Boîte de dialogue **Entrer le mot de passe**

Pour activer l'accès d'un encodeur protégé par mot de passe à un décodeur, vous devez saisir le mot de passe de niveau d'autorisation Utilisateur de l'encodeur comme mot de passe de destination du décodeur.





Pour fournir un mot de passe :

1. Dans la liste **Entrez le nom de l'utilisateur**, sélectionnez destination password.
 2. Dans le champ **Entrez le mot de passe de l'utilisateur**, saisissez le nouveau mot de passe.
 3. Cliquez sur **OK**.
- ⇒ Le mot de passe est immédiatement modifié sur le dispositif.

Se reporter à

- *Modification du mot de passe d'un encodeur / décodeur (modifier mot de passe / entrer mot de passe), page 234*

15.10 Modification du mot de passe d'un encodeur / décodeur (modifier mot de passe / entrer mot de passe)

Fenêtre principale > **Périphériques** > Développez  > Développez  >  >  >




ou

Fenêtre principale > **Périphériques** >  >  >


ou

Fenêtre principale > **Périphériques** >  >  >

ou

Fenêtre principale > **Périphériques** > Développez  > Développez  >  >
 Définissez ou modifiez le mot de passe pour chaque niveau. Saisissez le mot de passe (19 caractères maximum ; aucun caractère spécial) correspondant au niveau sélectionné.

Pour modifier le mot de passe :

1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Modifier le mot de passe...**
 La boîte de dialogue **Entrer le mot de passe** s'affiche.
 2. Dans la liste **Entrez le nom de l'utilisateur**, sélectionnez l'utilisateur pour lequel vous souhaitez modifier le mot de passe.
 3. Dans le champ **Entrez le mot de passe de l'utilisateur**, saisissez le nouveau mot de passe.
 4. Cliquez sur **OK**.
- ⇒ Le mot de passe est immédiatement modifié sur le dispositif.

Un mot de passe empêche tout accès non autorisé à l'unité. Vous pouvez utiliser différents niveaux d'autorisation pour restreindre l'accès.

Une protection par mot de passe n'est valide que si tous les niveaux d'autorisation supérieurs sont également protégés par un mot de passe. Par conséquent, vous devez toujours commencer par le niveau d'autorisation le plus élevé lorsque vous attribuez des mots de passe.

Vous pouvez définir et modifier un mot de passe pour chaque niveau d'autorisation si vous êtes connecté au compte utilisateur « service ».

L'appareil reconnaît trois niveaux d'autorisation : service, user et live.

- service représente le niveau d'autorisation le plus élevé. Après avoir saisi le mot de passe approprié, vous pouvez accéder à toutes les fonctions et modifier tous les paramètres de configuration.
- user représente le niveau d'autorisation intermédiaire. À ce niveau, vous pouvez faire fonctionner le périphérique, lire les enregistrements et commander une caméra, mais pas modifier la configuration.
- live représente le niveau d'autorisation le plus bas. À ce niveau, vous pouvez uniquement visualiser l'image vidéo en temps réel et passer d'une image en temps réel à une autre.

Pour un décodeur, le niveau d'autorisation suivant remplace le niveau d'autorisation live :




- destination password (disponible uniquement pour les décodeurs)
 Utilisé pour accéder à un encodeur.





Se reporter à





- *Indication du mot de passe de destination d'un décodeur (Authentifier...), page 234*

15.11

Déplacement d'un encodeur vers une autre zone de stockage (Modifier la zone de stockage)




Fenêtre principale > **Périphériques** > Développez  > Développez  >  > 

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez 

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > 

Vous pouvez déplacer un dispositif d'une zone de stockage vers une autre à l'intérieur du même dispositif VRM sans perdre d'enregistrements.

Pour effectuer un déplacement :

1. Cliquez avec le bouton droit de la souris sur  /  /  , puis cliquez sur **Modification du groupe ...**
La boîte de dialogue **Modifier le groupe** s'affiche.
2. Dans la liste **Nouveau groupe :**, sélectionnez la zone de stockage souhaitée.
3. Cliquez sur **OK**.
Le périphérique est déplacé vers la zone de stockage sélectionnée.

Boîte de dialogue Modifier le groupe

Permet de modifier l'affectation de la zone de stockage d'un dispositif.

Groupe actuel :





Affiche le numéro du pool auquel est affecté le dispositif sélectionné.

Nouveau groupe :

Sélectionnez le numéro du pool souhaité.

15.12

Récupération des enregistrements à partir d'un encodeur remplacé (Associer avec les enregistrements du prédécesseur)

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > 

Si vous remplacez un encodeur défectueux, les enregistrements de l'encodeur remplacé sont disponibles pour le nouvel encodeur lorsque vous sélectionnez le nouvel encodeur dans Operator Client.



Remarque!


Un encodeur ne peut être remplacé que par un encodeur doté du même nombre de canaux.



Récupération des enregistrements à partir d'un encodeur remplacé



Remarque!

N'utilisez pas la commande **Modifier l'encodeur**.

1. Cliquez avec le bouton droit de la souris sur la commande  > **Associer avec les enregistrements du prédécesseur...**
2. La boîte de dialogue **Associer avec les enregistrements du prédécesseur...** s'affiche.
3. Saisissez l'adresse réseau et un mot de passe valide pour le nouveau dispositif.
4. Cliquez sur **OK**.

5. Cliquez sur  pour enregistrer les paramètres.
6. Cliquez sur  pour activer la configuration.

Boîte de dialogue Associer avec les enregistrements du prédécesseur...

Vous permet de récupérer les enregistrements à partir d'un encodeur remplacé. Une fois les paramètres configurés dans la boîte de dialogue, les enregistrements de l'encodeur remplacé sont disponibles pour le nouvel encodeur lorsque vous le sélectionnez dans Operator Client.

Adresse réseau/Port

Saisissez l'adresse réseau du dispositif.

Nom d'utilisateur

Affiche le nom d'utilisateur utilisé pour l'authentification sur le dispositif.

Mot de passe





Saisissez un mot de passe valide pour vous authentifier sur le dispositif.

Authentifier

Permet de vous authentifier sur le dispositif avec les identifiants saisis précédemment.

15.13 Configuration des encodeurs / décodeurs

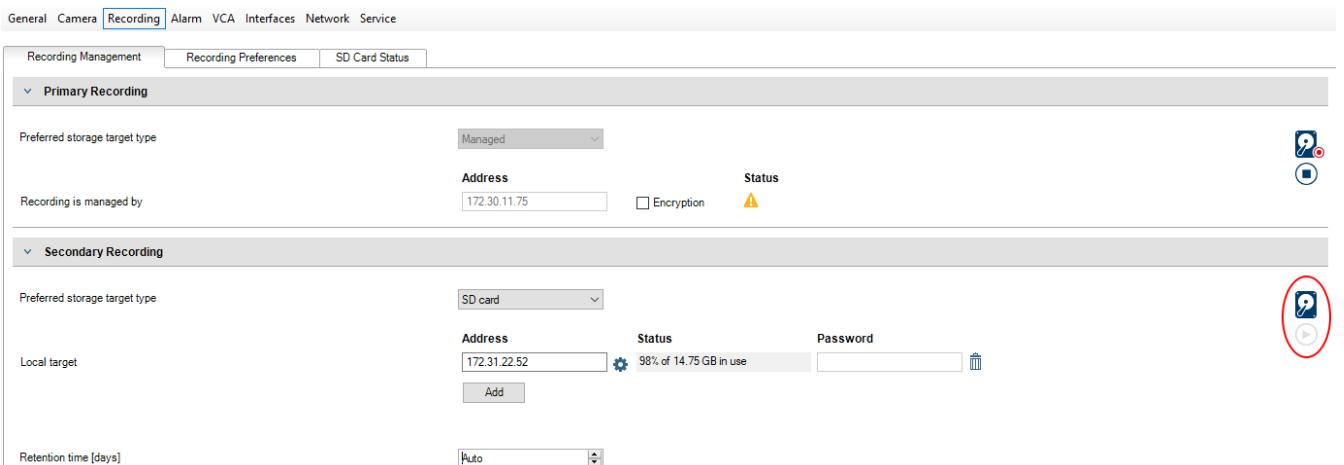
15.13.1 Configuration du support de stockage d'un encodeur

Fenêtre principale > **Périphériques** > Développez  > Développez  >  >  > **Paramètres avancés** > **Gestion des enregistrements**

Remarque : vérifiez que les caméras souhaitées de cet encodeur sont ajoutées à Arborecence logique.

Vous devez configurer le support de stockage d'un encodeur pour utiliser la fonction ANR.

Remarque : Si vous voulez configurer le support de stockage d'un encodeur qui a déjà été ajouté à votre système et qui est enregistré via VRM, assurez-vous que l'enregistrement secondaire est arrêté.



La fonction ANR ne peut fonctionner que sur les encodeurs dotés de la version 5.90 (ou ultérieure) du firmware. Tous les types d'encodeurs ne prennent pas en charge ANR même si la version de firmware correcte est installée.

Pour configurer le support de stockage d'un encodeur :

1. Sous **Enregistrement secondaire**, dans la liste **Types cible de stockage préférés**, sélectionnez les supports de stockage. En fonction du type de dispositif, différents supports sont disponibles.
2. Si nécessaire, cliquez sur le bouton ... pour formater le support de stockage. Une fois le processus de formatage terminé, le support de stockage est prêt pour être utilisé avec la fonction ANR.
3. Configurez la ANR de cet encodeur dans la page **Caméras et enregistrement**.

Se reporter à

- Page *Gestion des enregistrements*, page 240
- *Configuration de la fonction ANR*, page 314

15.13.2**Configuration de plusieurs encodeurs et décodeurs**

Fenêtre principale

Vous pouvez modifier simultanément les propriétés suivantes de plusieurs encodeurs et décodeurs :

- Mots de passe de dispositif
- Adresses IP
- Noms affichés
- Masque de sous-réseau
- ID de la passerelle
- Versions de micrologiciel


Pour sélectionner plusieurs dispositifs :

- ▶ Sélectionnez les dispositifs requis en appuyant sur la touche CTRL ou MAJ.

Pour sélectionner tous les dispositifs disponibles :

- ▶ Cliquez sur la commande  **Sélectionner tout**.

Pour modifier le mot de passe de plusieurs dispositifs :

1. Dans la fenêtre principale **Périphériques**, cliquez sur la commande  **Changer les mots de passe du périphérique**.
Ou
dans le menu **Matériel**, cliquez sur **Changer les mots de passe du périphérique...**
La boîte de dialogue **Changer les mots de passe du périphérique** s'affiche.
2. Sélectionnez les dispositifs requis.
3. Cliquez avec le bouton droit de la souris sur les dispositifs sélectionnés.
4. Cliquez sur **Modifier le mot de passe...** La boîte de dialogue **Modification des mots de passe** s'affiche.
5. Définissez les paramètres appropriés.

**Remarque!**

Vous pouvez sélectionner uniquement les types de mots de passe disponibles pour tous les dispositifs sélectionnés.

Pour configurer plusieurs noms affichés :

1. Dans le menu **Matériel**, cliquez sur **Changer l'IP du périphérique et les paramètres réseau...**
La boîte de dialogue **Changer les paramètres IP du périphérique et réseau** s'affiche.
2. Sélectionnez les dispositifs requis.
3. Cliquez avec le bouton droit de la souris sur les dispositifs sélectionnés.
4. Cliquez sur **Définir les noms affichés...**
La boîte de dialogue **Définir les noms affichés** s'affiche.
5. Définissez les paramètres appropriés.

Pour configurer plusieurs adresses IP :**Remarque!**

En modifiant l'adresse IP d'un périphérique IP, vous risquez de le rendre inaccessible.

1. Dans le menu **Matériel**, cliquez sur **Changer l'IP du périphérique et les paramètres réseau...**
La boîte de dialogue **Changer les paramètres IP du périphérique et réseau** s'affiche.
2. Sélectionnez les dispositifs requis.
3. Cliquez avec le bouton droit de la souris sur les dispositifs sélectionnés.
4. Cliquez sur **Définir les adresses IP...**
La boîte de dialogue **Définir les adresses IP** s'affiche.
5. Définissez les paramètres appropriés.

Pour modifier le masque de sous-réseau/l'ID passerelle pour plusieurs dispositifs :

1. Cliquez dans le champ requis de l'un des dispositifs dont vous souhaitez modifier la valeur.
2. Saisissez la valeur appropriée.
3. Sélectionnez tous les dispositifs requis.
4. Cliquez avec le bouton droit de la souris sur le champ requis du dispositif sur lequel vous avez déjà modifié la valeur.
5. Cliquez sur la commande **Copier la cellule dans** et la commande **Sélection dans colonne** .
Ou bien cliquez sur la commande **Colonne entière**, si nécessaire.

**Remarque!**

Vous pouvez également copier des lignes complètes pour modifier des adresses IP, des noms affichés, des masques de sous-réseau et des ID passerelle pour plusieurs dispositifs.

Pour mettre à jour le firmware de plusieurs dispositifs :

1. Dans le menu **Matériel**, cliquez sur **Mettre à jour le firmware du périphérique...**
La boîte de dialogue **Mettre à jour le firmware du périphérique** s'affiche.
2. Sélectionnez les dispositifs requis.
3. Cliquez sur la commande **Mettre à jour le firmware**.
4. Sélectionnez le fichier contenant la mise à jour.

5. Cliquez sur **OK**.

Résultat de l'opération

Affiche l'état approprié des dispositifs concernés.

15.13.3

Configuration du mode d'enregistrement de basculement sur un encodeur

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > 

Exigences préalables : Sur la page **Groupe**, dans la liste **Enregistrement du mode préférences**, sélectionnez **Basculement**. Si vous sélectionnez **Automatique**, les paramètres sont appliqués automatiquement et ne peuvent pas être configurés.

Pour utiliser une cible secondaire pour le mode de basculement ou le mode automatique : sur la page **Groupe**, dans la liste **Utilisation d'une cible secondaire**, sélectionnez **Activé**.

Il est recommandé de configurer au moins deux périphériques iSCSI pour le mode de basculement.

Pour configurer :

1. Cliquez sur **Paramètres avancés**.
2. Cliquez sur **Préférences d'enregistrement**.
3. Sous **Cible principale**, sélectionnez l'entrée correspondant à la cible de votre choix. Tous les systèmes de stockage saisis sous **Systèmes de stockage** figurent dans la liste.
4. Sous **Cible secondaire**, sélectionnez l'entrée correspondant à la cible de votre choix. Tous les systèmes de stockage saisis sous **Systèmes de stockage** s'affichent dans la liste.
Les modifications sont immédiatement appliquées. Aucune activation n'est nécessaire.

Rubriques connexes

- *Configuration du mode d'enregistrement automatique sur une zone de stockage, page 186*

15.13.4

Page Gestion des enregistrements



Les enregistrements actifs sont indiqués par

Pointez sur l'icône. Des informations détaillées concernant les enregistrements actifs s'affichent.

Gestion manuelle des enregistrements

Les enregistrements sont gérés localement sur cet encodeur. Tous les paramètres correspondants doivent être définis manuellement. L'encodeur / la caméra IP agit uniquement comme un périphérique en temps réel. Il / elle ne doit pas être supprimé(e) automatiquement de VRM.

Enregistrement 1 géré par VRM

Les enregistrements de cet encodeur sont gérés par le système VRM.

VRM double

L'enregistrement 2 de cet encodeur est géré par un VRM secondaire.

Onglet Supports iSCSI

Cliquez sur cet onglet pour afficher le stockage iSCSI disponible connecté à cet encodeur.

Onglet Supports locaux

Cliquez sur cet onglet pour afficher le stockage local sur cet encodeur.

Ajouter

Cliquez sur cet onglet pour ajouter un périphérique de stockage à la liste des supports de stockage pris en charge.

Supprimer

Cliquez sur ce bouton pour supprimer un périphérique de stockage de la liste des supports de stockage pris en charge.

Se reporter à

- *Configuration du support de stockage d'un encodeur, page 237*

15.13.5**Page Recording preferences (Préférences d'enregistrement)**

La page **Préférences d'enregistrement** s'affiche pour chaque encodeur. Cette page n'apparaît que si un périphérique est dédié à un système VRM.

Cible principale

Visible uniquement si la liste **Mode Préférences d'enregistrement** de la page **Groupe** est définie sur **Basculement**.

Sélectionnez l'entrée correspondant à la cible requise.

Cible secondaire

Visible uniquement si la liste **Mode Préférences d'enregistrement** de la page **Groupe** est définie sur **Basculement** et si la liste **Utilisation de cible secondaire** est définie sur **Activé**. Sélectionnez l'entrée correspondant à la cible requise pour la configuration du mode de basculement.




Se reporter à

- *Page Zone, page 185*

15.13.6**Configuration des décodeurs pour l'affichage à l'écran (OSD)**

Pour activer l'affichage à l'écran (OSD) pour les décodeurs, vous devez configurer les paramètres de décodeur respectifs.




Configuration de VIDEOJET decoder 8000

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > **Avancé** > **Affichage**

Dans la section **Affichage à l'écran**, configurez les paramètres suivants :

- **Affichage du mode d'alarme** : sélectionnez **Personnalisé**
- Entrez les coordonnées **X** et **Y** pour déterminer la position de l'étiquette OSD.
- Réglez la hauteur, la couleur et la couleur de fond souhaités pour le texte de l'alarme.

Configuration de VIDEOJET decoder 7513, VIDEOJET decoder 7523

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > **Avancé** > **Affichage**

Dans la section **Affichage à l'écran**, configurez les paramètres suivants :

- **Affichage du mode d'alarme** : sélectionnez **Personnalisé**
- Entrez les coordonnées **X** et **Y** pour déterminer la position de l'étiquette OSD.
- Réglez la hauteur, la couleur et la couleur de fond souhaités pour le texte de l'alarme.

Dans la section **Mode d'affichage**, configurez le paramètre suivant :

- **Mode d'affichage** : sélectionnez **Texte**

15.14 Configuration du multicast

Pour chaque caméra affectée, vous pouvez configurer une adresse multicast avec port.

Pour configurer le multicast :

1. Cochez la case appropriée pour activer le multicast.
2. Saisissez une adresse multicast valide et un numéro de port.
3. Si nécessaire, configurez une diffusion multicast en continu.





Onglet Multicast

Fenêtre principale > **Périphériques** >  >  > 

ou

Fenêtre principale > **Périphériques** >  >  > 

ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > 

> Onglet **Réseau** > Onglet **Multicast**

Permet de configurer le mode multicast pour les caméras affectées.

Permettre

Cliquez sur ce bouton pour activer le multicast pour cette caméra.

Adresse multicast

Insérez une adresse multicast valide (comprise dans la plage 224.0.0.0 - 239.255.255.255). Entrez 1.0.0.0. Une adresse multicast unique est automatiquement insérée en fonction de l'adresse MAC du périphérique.

Port

Lorsqu'un pare-feu est utilisé, saisissez la valeur d'un port configuré en tant que port non bloqué dans le pare-feu.

Diffusion

Cliquez sur ce bouton pour activer la diffusion multicast en continu sur le commutateur.

Cela signifie que la connexion multicast n'est pas précédée d'une inscription RCP+.

L'encodeur diffuse toujours toutes les données vers le commutateur. En retour, le commutateur (si aucun filtrage multicast IGMP n'est pris en charge ni configuré) envoie ces données à tous les ports, ce qui surcharge le commutateur.

Vous avez besoin de la diffusion pour pouvoir recevoir un flux multicast avec un périphérique non fabriqué par Bosch.



Remarque!






Les flux multicast sont sécurisés uniquement si l'encodeur dispose du firmware version 7.0 ou supérieure et si la case **Connexion sécurisée** est sélectionnée.

Se reporter à

- *Chiffrement de vidéo en temps réel (Modifier l'encodeur), page 228*

16 Page ONVIF

Fenêtre principale > **Périphériques** > Développez  > 




Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > Développez 

Se reporter à





- Page du dispositif Video Streaming Gateway, page 205
- Page Temps Réel Uniquement, page 215

16.1 Ajout d'un dispositif ONVIF en temps réel par balayage

Pour ajouter des dispositifs ONVIF en temps réel uniquement via un balayage :

1. Cliquez avec le bouton droit sur  et cliquez sur **Rechercher les encodeurs ONVIF en temps réel uniquement**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Cochez les boîtes de dialogue des dispositifs que vous souhaitez ajouter.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit sur ce champ et sélectionnez **Copier la cellule dans la colonne**.
Dans la colonne **État**, les connexions qui ont abouti sont indiquées par le symbole .
les connexions qui ont échoué sont indiquées par le symbole .
5. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.

16.2 Page Encodeur ONVIF

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > Onglet **Encodeur ONVIF**

ou
Fenêtre principale > **Périphériques** > Développez  >  > onglet **Encodeur ONVIF**
Affiche des informations sur un encodeur ONVIF temps réel uniquement, ajouté à votre BVMS.

Nom

Affiche le nom du dispositif ONVIF. Vous pouvez le renommer directement dans l'arborescence des dispositifs.

Adresse réseau

Affiche l'adresse IP du dispositif.

Fabricant

Affiche le nom du fabricant.

Modèle

Affiche le nom du modèle.

Entrées vidéo

Saisissez le nombre de caméras connectées à cet encodeur.

Entrées audio

Saisissez le nombre d'entrées audio connectées à cet encodeur.

Entrées d'alarme

Saisissez le nombre d'entrées d'alarme connectées à cet encodeur.

Relais

Saisissez le nombre de relais connectés à cet encodeur.

Se reporter à

- Page *Événements d'encodeur ONVIF*, page 244
- *Ajout d'un encodeur temps réel uniquement*, page 225
- *Configuration d'un tableau de mappage ONVIF*, page 248

16.3**Page Événements d'encodeur ONVIF**

À partir de BVMS 10,0, les événements d'encodeur ONVIF peuvent être récupérés directement à partir de l'encodeur VSG ou ONVIF. Si vous ajoutez un nouvel encodeur ONVIF, la case **extraire les événements ONVIF de VSG (Profil S, T)** est sélectionnée par défaut et le profil T est pris en charge.

Les fonctions suivantes ne sont prises en charge que si un encodeur ONVIF est ajouté à votre système via un dispositif VSG :



- Si des événements d'encodeur ONVIF sont récupérés de VSG, les événements ONVIF par défaut sont déjà mappés.
- L'opérateur peut activer ou désactiver des relais dans Operator Client.

Remarque!

La récupération des événements ONVIF à partir de VSG est uniquement disponible à partir de la version 7.0 de VSG. Si vous effectuez une migration vers BVMS version 10.0, les événements d'encodeur ONVIF existants sont récupérés directement à partir de l'encodeur ONVIF. Vous devez mettre à jour VSG vers la version 7.0.

Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  >  > Onglet **Événements d'encodeur ONVIF**

ou

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Événements d'encodeur ONVIF**

Vous devez mapper les événements ONVIF aux événements BVMS, si les événements d'encodeur ONVIF sont récupérés directement à partir de l'encodeur ONVIF. Vous êtes ainsi certain de pouvoir configurer ultérieurement des événements ONVIF en tant qu'alarmes BVMS.

**Remarque!**


Si des événements d'encodeur ONVIF sont récupérés de VSG, les événements ONVIF par défaut sont déjà mappés.

Tableau de mappage



Vous pouvez créer ou modifier un tableau de mappage



Cliquez sur  pour afficher la boîte de dialogue **Ajouter un tableau de mappage**.

Cliquez sur  pour afficher la boîte de dialogue **Renommer le tableau de mappage**.

Cliquez sur  pour supprimer le tableau de mappage avec toutes ses lignes.

Cliquez sur  ou sur  pour importer ou exporter un tableau de mappage ONVIF.

Événements et alarmes

Sélectionnez un événement BVMS pour le mapper à un événement ONVIF.

Ajouter une ligne

Cliquez sur cette option pour ajouter une ligne au tableau de mappage.

Lorsqu'il existe plusieurs lignes, un événement se produit si une ligne est vérifiée.

Supprimer une ligne

Cliquez sur cette option pour supprimer la ligne sélectionnée du tableau de mappage.

Rubrique ONVIF

Saisissez ou sélectionnez une chaîne, par exemple :

`tns1:VideoAnalytics/tnsaxis:MotionDetection`

Nom des données ONVIF

Saisissez ou sélectionnez une chaîne.

Type de données ONVIF

Saisissez ou sélectionnez une chaîne.

Valeur des données ONVIF

Saisissez ou sélectionnez une chaîne ou un nombre.

Si les événements ONVIF sont récupérés de VSG, les événements suivants sont mappés à VSG par défaut :

- **Changement global - Détecté**
- **Changement global - Non détecté**
- **Détection de mouvements - Mouvement détecté**
- **Détection de mouvements - Mouvement arrêté**
- **Vérification de l'image de référence - Dérégulé**
- **Vérification de l'image de référence - Régulé**
- **Perte de vidéo - Signal vidéo perdu**


- **Perte de vidéo - Signal vidéo OK**
- **Perte de vidéo - État du signal vidéo inconnu**
- **Signal vidéo trop flou - Signal vidéo OK**
- **Signal vidéo trop flou - Signal vidéo pas OK**
- **Signal vidéo trop lumineux - Signal vidéo OK**
- **Signal vidéo trop lumineux - Anomalie signal vidéo**
- **Signal vidéo trop sombre - Signal vidéo OK**
- **Signal vidéo trop sombre - Anomalie signal vidéo**
- **Signal vidéo trop bruyant - Signal vidéo OK Anomalie signal vidéo**
- **État du relais - Relais ouvert**
- **État du relais - Relais fermé**
- **État du relais - Erreur de relais**
- **État d'entrée - Entrée ouverte**
- **État d'entrée - Entrée fermée**
- **État d'entrée - Erreur d'entrée**

Se reporter à


- *Démarrage de ONVIF Camera Event Driver Tool à partir de Configuration Client, page 215*
- *Mappage des événements ONVIF, page 41*
- *Configuration d'un tableau de mappage ONVIF, page 248*

16.3.1

Ajout et suppression d'un profil ONVIF

Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  >  > Onglet **Événements d'encodeur ONVIF**

ou

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Événements d'encodeur ONVIF**

Vous pouvez ajouter, supprimer ou modifier les profils ONVIF pour un encodeur sélectionné.

Pour effectuer un ajout :

1. Cliquez sur **Ajouter...**
2. Dans la boîte de dialogue **Ajouter un profil**, entrez un nom pour le profil.
3. Cliquez sur **Suivant >**.
4. Dans la boîte de dialogue suivante, sélectionnez la caméra souhaitée.
5. Cliquez sur **Suivant >**.
6. Dans la boîte de dialogue suivante, sélectionnez le profil d'encodeur sans enregistrement souhaité.
7. Cliquez sur **Enregistrer**.
Le nouveau profil est enregistré.
Les paramètres de ce profil sont remplis avec les valeurs du profil d'encodeur sélectionné. Vous pouvez modifier ces valeurs si nécessaire.

Pour effectuer une suppression :

- ▶ Dans la liste, sélectionnez un profil, puis cliquez sur **Supprimer**.


Pour effectuer une modification :

1. Sélectionnez un profil dans la liste.
2. Modifiez les paramètres si nécessaire.

16.3.2 Exportation d'un fichier de tableau de mappage ONVIF


Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  >  > Onglet **Événements d'encodeur ONVIF**

ou

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Événements d'encodeur ONVIF**

Vous pouvez exporter un tableau de mappage ONVIF sous forme de fichier (OMF). Le tableau de mappage est enregistré pour le modèle d'encodeur sélectionné.

Pour effectuer une exportation :

1. Cliquez sur .
2. Saisissez un nom de fichier, puis cliquez sur **Enregistrer**.
Le tableau de mappage ONVIF est exporté en tant que fichier OMF pour le modèle de l'encodeur sélectionné.



Se reporter à

– Page *Événements d'encodeur ONVIF*, page 244

16.3.3 Importation d'un fichier de tableau de mappage ONVIF

Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  >  > Onglet **Événements d'encodeur ONVIF**

ou

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Événements d'encodeur ONVIF**

Vous pouvez importer un tableau de mappage ONVIF disponible sous forme de fichier (OMF).

Les fichiers de mappage ONVIF publiés sont stockés dans le répertoire suivant de Configuration Client :


– %programdata%\Bosch\VMS\ONVIF

Si le même nom de tableau de mappage est déjà importé, un message d'erreur s'affiche.







Si une version plus récente de ce fichier est importée, un message d'avertissement s'affiche.

Cliquez sur **OK** si vous voulez importer ce fichier. Sinon, cliquez sur **Annuler**.

Pour effectuer une importation :

1. Cliquez sur .
2. Sélectionnez le fichier souhaité, puis cliquez sur **Ouvrir**.
La boîte de dialogue **Importer un tableau de mappage** s'affiche.
3. Définissez les paramètres appropriés.
4. Cliquez sur **OK**.

Boîte de dialogue Importer un tableau de mappage

Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  >  > Onglet **Événements d'encodeur ONVIF** > 

ou

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Événements d'encodeur ONVIF** > 

Fabricant

Affiche le nom du fabricant pour lequel ce tableau de mappage est valide.

Modèle

Affiche le nom de modèle pour lequel ce tableau de mappage est valide.

Description

Affiche des informations supplémentaires, par exemple sur les modèles de caméra testés.

Nom du tableau de mappage

Affiche le nom du tableau de mappage. Modifiez ce nom s'il est déjà utilisé dans BVMS. Vous pouvez sélectionner l'une des options suivantes pour choisir les encodeurs ONVIF auxquels appliquer le tableau de mappage.


Appliquer uniquement à l'encodeur ONVIF sélectionné**Appliquer à tous les encodeurs ONVIF des modèles répertoriés****Appliquer à tous les encodeurs ONVIF du fabricant**

Le mappage des événements ONVIF existants se poursuit. Vous ne pouvez pas importer des fichiers OMT de versions précédentes de BVMS.

16.3.4**Configuration d'un tableau de mappage ONVIF**


Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  >  > Onglet **Événements d'encodeur ONVIF**

ou

Fenêtre principale > **Périphériques** > Développer  >  > Onglet **Événements d'encodeur ONVIF**


Vous configurez des tableaux de mappage pour mapper des événements ONVIF aux événements BVMS.

Vous configurez un tableau de mappage pour tous les encodeurs ONVIF de même modèle ou tous les encodeurs ONVIF du même fabricant.


Cliquez sur  pour mettre à jour les encodeurs ONVIF ajoutés hors ligne avec le mappage des événements d'un encodeur ONVIF déjà ajouté, ayant le même fabricant et/ou de modèle identique.

Pour les encodeurs multicanaux, vous pouvez configurer les sources des événements, par exemple une caméra ou un relais spécifique.

Pour créer un tableau de mappage :

1. Cliquez sur  .
La boîte de dialogue **Ajouter un tableau de mappage** s'affiche.
2. Saisissez un nom pour le tableau de mappage.
3. Dans les listes **Fabricant** et **Modèle**, sélectionnez les entrées de votre choix.
Lorsque vous sélectionnez **<aucun>** dans les deux listes, le mappage d'événement n'est valide que pour ce dispositif.
Lorsque vous sélectionnez **<aucun>** dans la liste **Modèle** et le nom du fabricant dans la liste **Fabricant**, le mappage d'événement est valide pour tous les dispositifs du même fabricant.
Lorsque vous sélectionnez les entrées disponibles dans les deux listes, le mappage d'événement est valide pour tous les dispositifs du même fabricant et modèle.
4. Cliquez sur **OK**.
Vous pouvez à présent modifier le tableau de mappage, par exemple en ajoutant une ligne à l'événement **Mouvement détecté**.


Pour modifier un tableau de mappage :

1. Cliquez sur  .
La boîte de dialogue **Renommer le tableau de mappage** s'affiche.
2. Modifiez les entrées de votre choix.





Pour ajouter ou supprimer des mappages d'événements :

1. Dans la liste **Tableau de mappage**, sélectionnez le nom souhaité.
2. Pour ajouter une ligne : cliquez sur **Ajouter une ligne**.
3. Sur la ligne, sélectionnez les entrées souhaitées.
Si plusieurs lignes sont disponibles, un événement est déclenché lorsqu'une seule des lignes est vérifiée.
4. Pour supprimer une ligne : cliquez sur **Supprimer une ligne**.

Pour supprimer un tableau de mappage :

1. Dans la liste **Tableau de mappage**, cliquez sur le nom des mappages d'événements à supprimer.
2. Cliquez sur  .

Pour configurer une source d'événement :

1. Développez  , puis cliquez sur  ,  ou  .
2. Cliquez sur l'onglet **Source d'événement ONVIF**.
3. Dans la colonne **Déclencher un événement**, activez l'événement configuré sur cette ligne.
4. Sélectionnez les définitions d'événements souhaitées.

Boîte de dialogue Ajouter/Renommer un tableau de mappage ONVIF

Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  > Onglet **Événements d'encodeur ONVIF** >  ou 

ou

Fenêtre principale > **Périphériques** > Développer  > Onglet  > **Événements**

d'encodeur ONVIF >  ou 

Permet d'ajouter un tableau de mappage. Si ce tableau de mappage doit servir de modèle pour les prochains encodeurs ONVIF provenant du même fabricant et de même modèle, sélectionnez les entrées correctes.

Nom du tableau de mappage

Saisissez un nom facilitant l'identification.

Fabricant

Sélectionnez une entrée si nécessaire.

Modèle

Sélectionnez une entrée si nécessaire.

Se reporter à



- *Activation de la journalisation des événements ONVIF, page 392*
- *Mappage des événements ONVIF, page 41*
- *Page Événements d'encodeur ONVIF, page 244*
- *Page Source d'événement ONVIF, page 264*

16.4

Page Configuration ONVIF

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > Onglet  > **Configuration ONVIF**

ou

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF**

Vous pouvez sélectionner plusieurs encodeurs ONVIF et modifier les paramètres dans la page **Profil d'encodeur vidéo**. Les paramètres modifiés sont valides pour tous les dispositifs sélectionnés.

Cette page est uniquement disponible pour les encodeurs ONVIF.



Remarque!

Restrictions de la configuration ONVIF

Les paramètres que vous effectuez sur ces pages peuvent ne pas être exécutés correctement car ils ne sont pas pris en charge par votre caméra. Les caméras ONVIF prises en charge ont été testées uniquement avec les paramètres par défaut.

16.4.1

Accès à l'appareil

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Accès à l'appareil**

ou

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Accès à l'appareil**

Fabricant

Affiche le nom du fabricant de l'encodeur sélectionné.

Modèle

Affiche le nom du modèle de l'encodeur sélectionné.

Remarque : si vous souhaitez exporter des mappages d'événements dans un fichier de mappage ONVIF, sélectionnez ce nom de modèle comme nom de fichier.

ID du matériel

Affiche l'identifiant matériel de l'encodeur sélectionné.

Version du firmware

Affiche la version de firmware de l'encodeur sélectionné.

Remarque : vérifiez que la version du firmware est correcte auprès de la liste de compatibilité BVMS.

Numéro de série

Affiche le numéro de série de l'encodeur sélectionné.

Adresse MAC

Affiche l'adresse MAC de l'encodeur sélectionné.





Version ONVIF

Affiche la version ONVIF de l'encodeur sélectionné.

Pour BVMS, la version 2.0 d'ONVIF est requise.

16.4.2

Date / Heure

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > Onglet  > **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Date/Heure**

ou

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Date/Heure**

Fuseau horaire

Sélectionnez le fuseau horaire du système.

Si votre système ou réseau comprend plusieurs périphériques, il est important de synchroniser leurs horloges internes. Vous ne pouvez, par exemple, effectuer une identification et une évaluation correcte des enregistrements simultanés que si tous les appareils sont à la même heure.

1. Saisissez la date du jour. L'heure de l'appareil étant commandée par l'horloge interne, il n'est pas nécessaire de saisir le jour de la semaine. Il s'ajoute automatiquement.
2. Pour appliquer l'heure système de votre ordinateur au périphérique, saisissez l'heure actuelle ou cliquez sur **Synchr. PC**.

Remarque :

Il est essentiel de vérifier la date et l'heure pour l'enregistrement. Un réglage incorrect pourrait entraîner des perturbations.

16.4.3 Gestion des utilisateurs

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Gestion des utilisateurs**
ou

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Gestion des utilisateurs**

Ces paramètres utilisateur sont utilisés pour les applications tierces telles que l'accès direct du Client Web aux encodeurs.

Les rôles utilisateur suivants pour l'accès aux applications tierces sont pris en charge :

- **Anonyme** : ce rôle dispose d'un accès illimité aux dispositifs où aucun utilisateur possédant un autre rôle (**Utilisateur**, **Opérateur**, **Administrateur**) n'est enregistré. Sur les dispositifs possédant au moins un des utilisateurs mentionnés ci-dessus, l'utilisateur anonyme n'a le droit que d'afficher les paramètres d'heure.
- **Administrateur** (non pris en charge par Configuration Client) : ce rôle a accès à toutes les sections et fonctionnalités de l'application, les droits de relancer le dispositif, de réinitialiser les paramètres et de mettre à jour le firmware ainsi que de créer d'autres utilisateurs dotés de droits d'accès différents.

Le premier utilisateur créé sur le dispositif doit être **Administrateur**.

Pour connaître les différences de droits d'accès par défaut entre les rôles **Opérateur** et **Utilisateur**, reportez-vous au tableau ci-dessous.

Section ou Fonctionnalité de Configuration ONVIF	Opérateur	Utilisateur
Identification	VIEW	HIDDEN
Paramètres d'heure	VIEW	VIEW
Paramètres réseau	VIEW	VIEW
Utilisateurs	HIDDEN	HIDDEN
Paramètres du relais	CHANGE	VIEW
Vidéo en temps réel (y compris rtsp-link)	CHANGE	CHANGE
Vidéo en continu	CHANGE	VIEW
Profils	CHANGE	VIEW

CHANGE - Modification des paramètres existants et création de nouveaux paramètres.

VIEW - Les paramètres ne sont pas masqués, mais il n'est pas possible de les modifier ni de les créer.

HIDDEN - Certains paramètres ou les sections sont masqués.

Utilisateurs

Répertorie les utilisateurs disponibles du dispositif.

Mot de passe

Saisissez un mot de passe valide.

Confirmer le mot de passe

Confirmez le mot de passe saisi.

Rôle

Sélectionnez le rôle souhaité pour l'utilisateur sélectionné. Les droits d'accès sont adaptés en conséquence.

16.4.4

Page Profil d'encodeur vidéo

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > Onglet **Configuration ONVIF** > Onglet **Caméra** > Onglet

Profil d'encodeur vidéo

ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > Onglet **Configuration ONVIF** > Onglet **Caméra** > Onglet **Profil d'encodeur vidéo**

Les profils sont relativement complexes et comprennent un certain nombre de paramètres interagissant les uns avec les autres. Il est donc généralement préférable d'utiliser les profils prédéfinis. Ne modifiez un profil que si vous êtes familiarisé avec toutes les options de configuration.

Profils

Cliquez sur le nom voulu.

Remarque!

Les profils configurés ici peuvent être sélectionnés dans le Client de configuration.

Dans la fenêtre principale, cliquez sur **Caméras et enregistrement**, puis cliquez sur 

ou  .

Le paramètre par défaut '<Automatic>' peut être modifié dans l'un des profils répertoriés et configurés.

Remarque : assurez-vous, lorsque vous utilisez plus d'un profil d'un dispositif unique, que certaines restrictions de performances s'appliquent et, éventuellement, que la caméra limite automatiquement la qualité d'un flux dans les situations de surcharge.



Nom

Vous pouvez attribuer un nouveau nom au profil dans ce champ. Le nom est alors affiché dans la liste des profils disponibles dans le champ Profil actif.

Encodage

Sélectionnez le CODEC souhaité.

Résolution

Sélectionnez la résolution souhaitée pour l'image vidéo.

Qualité

Ce paramètre vous permet de réduire la charge sur le canal en réduisant la définition d'image. Le paramètre est défini à l'aide du curseur : la position la plus à gauche correspond à la définition d'image la plus élevée, la position la plus à droite correspond à la charge la plus basse sur le canal vidéo.

Limite de la cadence d'images

Cadence d'images (images par seconde) qui indique le nombre d'images par seconde capturées par la caméra vidéo connectée au dispositif. Ce paramètre s'affiche uniquement pour information.

Si un intervalle d'encodage est fourni, la cadence d'images résultante est réduite selon le facteur donné.

Limite du débit

Plus le débit est faible, plus la taille du fichier vidéo est petite. Mais lorsque le débit binaire est très réduit, le programme doit utiliser des algorithmes de compression renforcés, ce qui réduit également la qualité vidéo.

Sélectionnez le débit de sortie maximal en kbits/s. Le débit de données maximal ne doit être dépassé en aucune circonstance. En effet, selon les paramètres de qualité vidéo des images I et P, tout dépassement peut provoquer une instabilité des images individuelles. La valeur saisie ici doit être supérieure de 10 %, au moins, au débit de données cible standard.

Intervalle d'encodage

L'intervalle d'encodage (nombre d'images) désigne à quelle cadence les images en provenance de la caméra sont encodées. Par exemple, lorsque l'intervalle d'encodage comprend la valeur 25, cela signifie qu'1 image sur 25 images capturées par seconde est codée et transmise à l'utilisateur. La valeur maximale réduit la charge sur le canal, mais peut provoquer la perte d'informations dans les images non codées. Réduire l'intervalle d'encodage augmente la fréquence de mise à jour des images, ainsi que la charge sur le canal.

Longueur du GOP

Il est possible de modifier la longueur du GOP uniquement si l'encodeur est H.264 ou H.265. Ce paramètre désigne la longueur du groupe d'images entre deux images clés. Plus cette valeur est élevée, plus la charge du réseau est faible, mais la qualité vidéo est affectée.

La valeur 1 indique que les images I sont générées en continu. La valeur 2 indique qu'une image sur deux est une image I, la valeur 3 indique qu'une image sur 3 est une image I, etc. Les images intermédiaires sont codées comme images P ou images B.

Délai d'attente de la session

Délai d'attente de la session RTSP pour le flux vidéo associé.

Le délai d'attente de la session est fourni en tant qu'un indice pour que la session RTSP soit conservée par un dispositif.

Multicast - Adresse IP

Saisissez une adresse multicast valide à exploiter en mode multicast (répétition des flux de données sur le réseau).

Avec le réglage 0.0.0.0, l'encodeur du flux fonctionne en mode multicast unique (copie des flux de données de l'appareil). La caméra prend en charge les connexions multicast unique pour cinq récepteurs connectés simultanément au maximum.

La répétition des données crée une lourde charge sur l'unité centrale et peut provoquer une baisse de la qualité de l'image dans certaines circonstances.

Multicast - Port

Sélectionnez le port de destination RTP multicast. Un dispositif peut prendre en charge RTCP. Dans ce cas, la valeur du port doit être paire pour permettre au flux RTCP correspondant d'être mappé sur le numéro de port de destination (impair) supérieur suivant comme indiqué dans la spécification RTSP.

Multicast - TTL

Vous pouvez entrer une valeur pour indiquer combien de temps les paquets de données multicast restent actifs sur le réseau. Si le multicast doit être effectué via un routeur, la valeur doit être supérieure à 1.

**Remarque!**

Le fonctionnement multicast n'est possible qu'avec le protocole UDP. Le protocole TCP ne prend pas en charge les connexions multicast.

Si le dispositif est utilisé avec un pare-feu, sélectionnez le protocole de transmission TCP (port HTTP). Si vous l'utilisez sur un réseau local, sélectionnez UDP.

16.4.5**Profil d'encodeur audio**

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > **Onglet Configuration ONVIF** > **Onglet Caméra** > **Onglet**

Profil d'encodeur audio

ou

Fenêtre principale > **Périphériques** > Développez  >  > **Onglet Configuration ONVIF** > **Onglet Caméra** > **Onglet Profil d'encodeur audio**

Les profils sont relativement complexes et comprennent un certain nombre de paramètres interagissant les uns avec les autres. Il est donc généralement préférable d'utiliser les profils prédéfinis. Ne modifiez un profil que si vous êtes familiarisé avec toutes les options de configuration.

Encodage

Sélectionnez l'encodage souhaité pour la source audio, le cas échéant :

- **G.711 [ITU-T G.711]**
- **G.726 [ITU-T G.726]**
- **AAC [ISO 14493-3]**

Débit

Sélectionnez le débit souhaité, par exemple 64 kbits/s, pour la transmission du signal audio.

Fréquence d'échantillonnage

Saisissez le taux d'échantillonnage de sortie en kHz, par exemple, 8 kbits/s.

Délai d'attente de la session

Délai d'attente de la session RTSP pour le flux audio associé.

Le délai d'attente de la session est fourni en tant qu'un indice pour que la session RTSP soit conservée par un dispositif.

16.4.6 Imagerie - Généralités

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Caméra** > Onglet **Imagerie - généralités**

ou

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Caméra** > Onglet **Imagerie - généralités**

Luminosité

Permet de régler la luminosité des images pour votre environnement de travail.

Saturation des couleurs

Permet de régler la saturation des couleurs de l'image pour rendre la reproduction des couleurs sur le moniteur la plus réaliste possible.

Contraste

Vous pouvez adapter le contraste de l'image vidéo pour votre environnement de travail.

Netteté

Permet de régler la netteté des images.

Une valeur faible rend l'image moins nette. L'augmentation de la netteté fait ressortir davantage de détails. Le supplément de netteté permet d'accentuer les détails des plaques d'immatriculation, des caractéristiques du visage et des bords de certaines surfaces, mais peut accroître les besoins de bande passante.

Filtre anti-IR

Sélectionnez l'état du filtre de coupure IR.

L'état AUTO permet à l'algorithme d'exposition de gérer l'activation du filtre de coupure IR.

16.4.7 Compensation de contre-jour

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Compensation de contre-jour**

ou

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Compensation de contre-jour**

Selon le modèle de dispositif, vous pouvez configurer ici les paramètres relatifs à la compensation de contre-jour.

Mode

Sélectionnez **Désactivé** pour désactiver la compensation de contre-jour.

Sélectionnez **Activé** pour capter les détails dans des conditions caractérisées par un fort contraste et une luminosité extrêmement forte/faible.

Niveau

Saisissez ou sélectionnez la valeur souhaitée.

16.4.8

Exposition

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez

 > Développez  > Onglet  > **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Exposition**

ou

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Exposition**

Selon le modèle de dispositif, vous pouvez configurer ici les paramètres relatifs à l'exposition.

Mode

Sélectionnez **Auto** pour activer l'algorithme d'exposition sur le dispositif. Les valeurs des champs suivants sont utilisées par l'algorithme :

- **Priorité**
- **Fenêtre**
- **Temps d'exposition min.**
- **Temps d'exposition max.**
- **Gain min.**
- **Gain max.**
- **Diaphragme min.**

Sélectionnez **Manuel** pour désactiver l'algorithme d'exposition sur le dispositif. Les valeurs des champs suivants sont utilisées par l'algorithme :

- **Temps d'exposition**
- **Gain**
- **Diaphragme**

Priorité

Configurer le mode de priorité d'exposition (faible bruit/cadence d'images).

Fenêtre

Définir un masque d'exposition rectangulaire.

Temps d'exposition min.

Configurer la période d'exposition minimale [μ s].

Temps d'exposition max.

Configurer la période d'exposition maximale [μ s].

Gain min.

Configurer la plage minimale de gain du capteur [dB].

Gain max.

Configurer la plage maximale de gain du capteur [dB].

Diaphragme min.

Configurer l'atténuation minimale de la lumière en entrée affectée par l'iris [dB]. 0 dB correspond à un iris entièrement ouvert.

Diaphragme max.

Configurer l'atténuation maximale de la lumière en entrée affectée par l'iris [dB]. 0 dB correspond à un iris entièrement ouvert.

Temps d'exposition

Configurer la durée d'exposition fixe [μ s].

Gain

Configurer le gain fixe [dB].

Diaphragme

Configurer l'atténuation fixe de la lumière en entrée affectée par l'iris [dB]. 0 dB correspond à un iris entièrement ouvert.

16.4.9**Mise au point**

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez

 > Expand  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Mise au point**

ou

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Paramètres principaux** > Onglet **Mise au point**

Selon le modèle de dispositif, vous pouvez configurer ici les paramètres relatifs à la mise au point.

Cette page permet de déplacer l'objectif de manière absolue, relative ou continue. Les réglages de la mise au point via cette opération désactivent la mise au point automatique (focus). Un dispositif prenant en charge la mise au point à distance prend généralement en charge cette opération de déplacement. La position de la mise au point est représentée par une certaine valeur numérique. L'état de la mise au point peut avoir l'une des valeurs suivantes :

MOVING

OK

UNKNOWN

En outre, les informations d'erreur peuvent être affichées, par exemple, une erreur de positionnement indiquée par le matériel.

Mode

Sélectionnez **Auto** pour permettre la mise au point automatique de l'objectif à tout moment en fonction des objets de la scène. Les valeurs des champs suivants sont utilisées par l'algorithme :

- **Limite proche**
- **Limite éloignée**

Sélectionnez **Manuel** pour régler la mise au point manuellement. Les valeurs des champs suivants sont utilisées par l'algorithme :

- **Vitesse par défaut**

Vitesse par défaut

Configurer la vitesse par défaut pour le déplacement de la mise au point (lorsque le paramètre de vitesse n'est pas présent).





Limite éloignée

Configurer la limite proche de l'objectif à focale [m].

Limite éloignée

Configurer la limite éloignée de l'objectif à focale [m].

16.4.10 Plage dynamique étendue (WDR)

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > **Onglet Configuration ONVIF** > **Onglet Paramètres principaux** > **Onglet Plage dynamique étendue**
ou

Fenêtre principale > **Périphériques** > Développez  >  > **Onglet Configuration ONVIF** > **Onglet Paramètres principaux** > **Onglet Plage dynamique étendue**
Selon le modèle de dispositif, vous pouvez configurer ici les paramètres relatifs à la plage dynamique étendue.





Mode

Saisissez ou sélectionnez la valeur souhaitée.

Niveau

Saisissez ou sélectionnez la valeur souhaitée.

16.4.11 Balance des blancs

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > **Onglet Configuration ONVIF** > **Onglet Paramètres principaux** > **Onglet Balance des blancs**
ou

Fenêtre principale > **Périphériques** > Développez  >  > **Onglet Configuration ONVIF** > **Onglet Paramètres principaux** > **Onglet Balance des blancs**
Selon le modèle de dispositif, vous pouvez configurer ici les paramètres relatifs à la balance des blancs.

Mode

Le mode Auto permet à la caméra d'ajuster en permanence la reproduction optimale des couleurs à l'aide d'une méthode de réflexion moyenne ou dans un environnement doté de sources de lumière naturelle.

En mode Manuel, les gains Rouge, Vert et Bleu peuvent être réglés manuellement sur la position de votre choix.

Il n'est pas nécessaire de modifier le décalage du point blanc pour les conditions de prise de vue spéciales :

- sources de lumière intérieures et éclairages obtenus avec des LED colorées
- lampes à vapeur de sodium (éclairage public)
- n'importe quelle couleur dominante de l'image, par exemple, le vert d'un terrain de football ou d'une table de jeux

Gain Rouge

En mode de balance des blancs Manuel, réglez le curseur de gain du rouge pour décaler l'alignement du point blanc par défaut (en réduisant le rouge et en augmentant le cyan).

Gain Bleu

En mode de balance des blancs Manuel, réglez le curseur de gain du bleu pour décaler l'alignement du point blanc par défaut (en réduisant le bleu et en augmentant le jaune).

16.4.12

Accès réseau

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Expand  > Onglet  > **Configuration ONVIF** > Onglet **Réseau** > Onglet **Accès réseau**

ou

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Réseau** > Onglet **Accès réseau**

Ici, vous pouvez configurer différents paramètres réseau.

Ethernet IPv4

DHCP

Si un serveur DHCP est utilisé sur le réseau pour l'affectation dynamique des adresses IP, vous pouvez activer l'acceptation des adresses IP automatiquement attribuées à l'encodeur. BVMS utilise l'adresse IP pour l'affectation unique de l'encodeur. Le serveur DHCP doit prendre en charge l'affectation fixe entre l'adresse IP et l'adresse MAC et être configuré de telle sorte que lorsqu'une adresse IP est affectée, elle reste en mémoire lors de chaque redémarrage de l'ordinateur.

Masque de sous-réseau

Saisissez le masque de sous-réseau approprié pour l'adresse IP définie.

Si le serveur DHCP est activé, le masque de sous-réseau est automatiquement affecté.

Passerelle par défaut

Si vous souhaitez que le module établisse une connexion avec un emplacement distant dans un autre sous-réseau, saisissez l'adresse IP de la passerelle ici. Si ce n'est pas le cas, laissez ce champ vide (0.0.0.0).

Ethernet IPv6

DHCP

Saisissez ou sélectionnez la valeur souhaitée.

Adresse IP

Affiche l'adresse IPv6 du dispositif, fournie par le serveur DHCP.

Longueur du préfixe

Affiche la longueur de préfixe du dispositif, fournie par le serveur DHCP.

Passerelle par défaut

Affiche la passerelle par défaut du dispositif, fournie par le serveur DHCP.

Nom de l'hôte

Saisissez ou sélectionnez la valeur souhaitée.

DNS

À l'aide d'un serveur DNS, le dispositif peut résoudre une adresse indiquée sous forme de nom. Saisissez l'adresse IP du serveur DNS ici.

Serveurs NTP

Saisissez l'adresse IP du serveur de temps de votre choix ou laissez le serveur DHCP le faire pour vous.

L'encodeur peut recevoir le signal d'heure d'un serveur de synchronisation utilisant différents protocoles de serveur de synchronisation et s'en servir pour régler l'horloge interne. Le module interroge automatiquement le signal d'heure toutes les minutes. Saisissez l'adresse IP d'un serveur de synchronisation ici. Ce paramètre accepte un degré de précision élevé et est nécessaire pour certaines applications.

Ports HTTP

Si nécessaire, sélectionnez un port HTTP différent pour le navigateur. Le port HTTP par défaut est 80. Si vous souhaitez autoriser uniquement des connexions sécurisées par le port HTTPS, vous devez désactiver le port HTTP.

Remarque : non pris en charge par BVMS.

Ports HTTPS

Remarque : non pris en charge par BVMS.

Si vous souhaitez accorder l'accès du réseau via une connexion sécurisée, sélectionnez un port HTTPS, si nécessaire. Le port HTTP par défaut est 443. Sélectionnez l'option **Désactivé** pour désactiver les ports HTTPS. Seules des connexions non sécurisées seront alors possibles.

Passerelle par défaut

Saisissez ou sélectionnez la valeur souhaitée.

Ports RTSP

Si nécessaire, sélectionnez un autre port pour l'échange de données RTSP. Le port RTSP standard est 554. Sélectionnez **Désactivé** pour désactiver la fonction RTSP.

Adresse sans configuration

Activer ou désactiver la détection de configuration zéro de la caméra sélectionnée.

La configuration zéro est une autre méthode pour DHCP et DNS d'affectation des adresses IP aux caméras. Elle crée automatiquement une adresse IP de réseau utilisable sans configuration ni serveurs spéciaux.

Remarque : dans la norme ONVIF, seule la détection de service de la configuration zéro est utilisée.

Sans configuration zéro, le réseau doit fournir des services, tels que DHCP ou DNS.

Dans le cas contraire, configurez les paramètres réseau de chaque caméra IP manuellement.

Mode découverte ONVIF

Si elle est activée, la caméra peut être analysée sur le réseau. Cette opération inclut ses fonctions.

Si elle est désactivée, la caméra n'envoie pas de messages de détection afin d'éviter les attaques de refus de service.

Il est recommandé de désactiver la détection après l'ajout de la caméra à la configuration.

Saisissez ou sélectionnez la valeur souhaitée.

Activer DynDNS

Permet d'activer DynDNS.

Un service de noms de domaines (DNS) dynamique permet de sélectionner l'unité via Internet à l'aide d'un nom d'hôte, sans avoir à connaître l'adresse IP actuelle de l'unité. Pour cela, vous devez disposer d'un compte auprès d'un fournisseur DNS dynamique et vous devez enregistrer le nom d'hôte requis pour l'unité sur ce site.

Remarque :

Pour plus d'informations relatives au service, à la procédure d'enregistrement et aux noms d'hôte disponibles, prenez contact avec le fournisseur DynDNS sur le site dyndns.org.

Type

Saisissez ou sélectionnez la valeur souhaitée.

Nom

Saisissez le nom de votre compte utilisateur DynDNS.

TTL

Saisissez ou sélectionnez la valeur souhaitée.

16.4.13**Portées**

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > Onglet **Configuration ONVIF** > Onglet **Réseau** > Onglet

Portées

ou

Fenêtre principale > **Périphériques** > Développez  > Onglet **Configuration ONVIF** > Onglet **Réseau** > Onglet **Portées**

Vous pouvez ajouter ou supprimer des portées sur votre dispositif ONVIF avec URI au format suivant :

onvif://www.onvif.org/<path>

L'exemple ci-dessous illustre l'utilisation de la valeur de la portée. Il ne s'agit que d'un exemple et non d'une indication sur le type de paramètre de portée devant faire partie d'une configuration d'encodeur. Dans cet exemple, nous supposons que l'encodeur est configuré avec les portées suivantes :

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

Vous pouvez attribuer au dispositif un nom et un emplacement détaillés pour l'identifier dans la liste des dispositifs.

Le tableau indique les fonctions de base et d'autres propriétés du dispositif, qui sont normalisées :

Catégorie	Valeurs définies	Description
type	video_encoder	Le dispositif est un encodeur vidéo réseau.
	Ptz	Le dispositif est un dispositif mobile (PTZ).
	audio_encoder	Le dispositif prend en charge de l'encodeur audio.
	video_analytics	Le dispositif prend en charge Video Analytics.
	Network_Video_Transmitter	Le dispositif est un émetteur vidéo réseau.
	Network_Video_Decoder	Le dispositif est un décodeur vidéo réseau.
	Network_Video_Storage	Le dispositif est un dispositif de stockage vidéo réseau.



Catégorie	Valeurs définies	Description
	Network_Video_Analytic	Le dispositif est un dispositif Video Analytics réseau.
location	Toute valeur de chemin ou chaîne de caractères.	Non pris en charge par BVMS.
hardware	Toute valeur de chemin ou chaîne de caractères.	Une valeur de chaîne ou de chemin qui décrit le matériel du dispositif. Un dispositif doit inclure au moins une entrée de matériel dans la liste de portées.
name	Toute valeur de chemin ou chaîne de caractères.	Nom de recherche du dispositif. Ce nom s'affiche dans l'arborescence logique et de dispositifs.

Le nom de la portée, le modèle et le fabricant déterminent la manière dont le dispositif s'affiche dans l'arborescence des dispositifs et dans les paramètres principaux et l'identification de l'encodeur ONVIF.

16.4.14

Relais

Fenêtre principale > **Périphériques** > Développez  > Développez  > Développez  > Développez  > Onglet **Configuration ONVIF** > Onglet **Interfaces** > Onglet **Relais**

Fenêtre principale > **Périphériques** > Développez  >  > Onglet **Configuration ONVIF** > Onglet **Interfaces** > Onglet **Relais**

L'état inactif physique d'une sortie de relais peut être configuré en définissant l'état inactif sur **ouvert** ou **fermé** (inversion du comportement du relais).

Les sorties numériques disponibles du dispositif sont répertoriés par leur nom, par exemple :

- **AlarmOut_0**
- **AlarmOut_1**

Pour tout mappage d'événements des relais dans BVMS, utilisez les noms répertoriés ici.

Mode

Le relais peut fonctionner selon deux modes :

- **Bistable** : une fois l'état défini, le relais reste dans cet état.
- **Monostable** : une fois l'état défini, le relais revient à l'état inactif une fois le délai de retard spécifié écoulé.

État inactif

Sélectionnez **Ouvert** pour que le relais fonctionne comme un contact normalement ouvert, ou **Fermé** s'il doit fonctionner comme un contact normalement fermé.

Durée de temporisation

Définissez le délai de retard. Après ce délai, le relais repasse à l'état inactif s'il est configuré en mode **Monostable**.

Si vous souhaitez tester des configurations liées à une modification de l'état du relais, cliquez sur **Activer** ou sur **Désactiver** pour commuter le relais. Vous pouvez consulter les événements de relais de la caméra configurée pour vérifier le fonctionnement correct : affichage de l'état de l'icône du relais dans l'arborescence logique, événements dans la liste des alarmes ou journal des événements.

Activer






Cliquez sur ce bouton pour faire passer le relais à l'état inactif configuré.

Désactiver





Cliquez sur ce bouton pour faire passer le relais à l'état non inactif configuré.

16.5





Page Source d'événement ONVIF



Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  > Développer  > Onglet **Source d'événement ONVIF**
ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > onglet **Source d'événement ONVIF**
ou

Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  > Onglet **Source d'événement ONVIF**
ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > onglet **Source d'événement ONVIF**
ou

Fenêtre principale > **Périphériques** > Développer  > Développer  > Développer  > Développer  > Onglet **Source d'événement ONVIF**
ou

Fenêtre principale > **Périphériques** > Développez  > Développez  > onglet **Source d'événement ONVIF**

Vous pouvez configurer les événements ONVIF d'une source (canal vidéo, entrée ou relais). Une définition d'événement activé est ajoutée au tableau de mappage de l'encodeur. Par exemple, dans le cas d'un encodeur multicanal, vous configurez pour quelle caméra un événement **Mouvement détecté** se déclenche.

Déclencher un événement

Activez cet événement.

Rubrique ONVIF

Saisissez ou sélectionnez une chaîne.

Nom de la source ONVIF

Saisissez ou sélectionnez une chaîne.

Type de la source ONVIF

Saisissez ou sélectionnez une chaîne.

Valeur de la source ONVIF

Saisissez ou sélectionnez une chaîne.

Se reporter à

- *Mappage des événements ONVIF, page 41*
- *Configuration d'un tableau de mappage ONVIF, page 248*

16.6**Affectation d'un profil ONVIF**

Fenêtre principale > **Caméras et enregistrement** >

Vous pouvez affecter un jeton de profil de support ONVIF à une caméra ONVIF.

Ce peut être pour la vidéo en temps réel ou pour l'enregistrement.

Pour affecter un jeton de vidéo en temps réel :

- ▶ Dans la colonne **Vidéo en temps réel - Profil**, sélectionnez l'entrée souhaitée.

Pour affecter un jeton d'enregistrement :

- ▶ Dans la colonne **Enregistrement - Profil**, sélectionnez l'entrée souhaitée.

Se reporter à

- *Page Caméras, page 297*

17 Page Cartes et structure



Remarque!

BVMS Viewer offre uniquement des fonctionnalités de base. Les fonctionnalités avancées sont incluses dans BVMS Professional. Pour de plus amples informations sur les différentes éditions BVMS, consultez le site www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Le nombre d'éléments au-dessous d'une entrée est affiché entre crochets.

Fenêtre principale > **Cartes et structure**

Il est possible de perdre des autorisations. Si vous déplacez un groupe de dispositifs, ces dispositifs perdent leurs autorisations. Vous devez de nouveau les définir sur la page

Groupes d'utilisateurs.

Affiche l'arborescence des périphériques, l'arborescence logique et la fenêtre **Carte globale**.

Permet d'ajouter une structure pour tous les périphériques de BVMS. Cette structure s'affiche dans l'arborescence logique.

Permet d'effectuer les tâches suivantes :

- Configuration de l'arborescence logique Complète
- Gestion des ressources
- Création des Scripts de Commande
- Création de séquences
- Création de zones de visualisation de carte
- Création de relais de dysfonctionnement
- Ajout de cartes de site et création de zones réactives

Les zones réactives sur les cartes peuvent être des :

- Caméras
- Entrées
- Relais
- Scripts de commande
- Séquences
- Documents
- Liens vers d'autres cartes de site
- VRM
- iSCSI
- Lecteurs d'un système de contrôle d'accès
- Centrales de détection d'intrusion
- Serveur de gestion d'Enterprise Systems









Les fichiers ressource peuvent être de type suivant :

- Fichiers de carte
- Fichiers de document
- Liens vers des URL externes
- Fichiers audio
- Liens vers des applications externes


Icônes




Affiche une boîte de dialogue permettant de gérer les fichiers de ressource.

	Affiche une boîte de dialogue permettant d'ajouter des scripts de commande à l'arborescence logique ou de gérer ceux-ci.
	Affiche une boîte de dialogue permettant d'ajouter ou de modifier un fichier de séquence de caméras.
	Permet de créer un dossier dans l'arborescence logique.
	Affiche une boîte de dialogue permettant d'ajouter des fichiers ressource Carte.
	Permet de créer une zone de visualisation de carte dans l'arborescence logique.
	Affiche une boîte de dialogue permettant d'ajouter un fichier document.
	Affiche une boîte de dialogue permettant d'ajouter un lien vers une application externe.
	Affiche une boîte de dialogue permettant d'ajouter un relais de dysfonctionnement.

Symboles

	Le dispositif a été ajouté à l'arborescence logique.
---	--

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.




18 Configuration de cartes et de l'arborescence logique

Ce chapitre explique comment configurer l'Arborescence Logique et comment gérer les fichiers ressource, tels que les cartes.



Remarque!

Si vous déplacez un groupe de périphériques dans l'Arborescence Logique, ces périphériques perdent leurs autorisations. Vous devez de nouveau les définir sur la page **Groupes d'utilisateurs**.

- Cliquez sur  pour enregistrer les paramètres.
- Cliquez sur  pour annuler le dernier paramètre.
- Cliquez sur  pour activer la configuration.

Se reporter à

- *Boîte de dialogue Gestionnaire de ressources, page 271*
- *Boîte de dialogue Sélectionner une ressource, page 272*
- *Boîte de dialogue Générateur de séquence, page 274*
- *Boîte de dialogue Ajouter une séquence, page 277*
- *Boîte de dialogue Ajouter un pas de séquence, page 277*
- *Boîte de dialogue Ajouter URL, page 273*
- *Boîte de dialogue Sélectionner une carte pour le lien, page 278*
- *Boîte de dialogue Relais de dysfonctionnement, page 286*
- *Lien vers la boîte de dialogue Application externe, page 273*

18.1 Configuration de l'Arborescence Logique

Fenêtre principale > **Cartes et structure** > onglet **Arborescence Logique**

Vous pouvez ajouter des dispositifs, des fichiers de ressources, des zones de visualisation de carte, des séquences, des scripts de commande client et des dossiers à l'arborescence logique. Les dispositifs sont répertoriés dans l'arborescence des dispositifs et vous pouvez faire glisser n'importe quel niveau de l'arborescence des dispositifs vers l'arborescence Logique.

Un fichier de ressource peut être, par exemple; une carte de site, un document, un fichier Web, un fichier audio ou un script de commande.

- Une carte de site est un fichier que vous pouvez ajouter à l'arborescence Logique. L'ajout d'une carte de site à l'arborescence logique engendre la création d'un dossier de carte, dans lequel vous pouvez classer les dispositifs logiques spécifiques à la carte.
- Une zone de visualisation de carte est une zone d'une carte globale avec un centre et un niveau de zoom spécifiques.
- Ce type de dossier vous offre une meilleure organisation des dispositifs dans l'arborescence logique.

Lorsque vous démarrez Configuration Client pour la première fois, l'arborescence logique est vide.

Si un groupe d'utilisateurs n'est pas autorisé à accéder à un dispositif (une caméra, par exemple), il n'apparaît ni sur la carte de site, ni dans la zone de visualisation de carte, ni dans l'arborescence logique.

Vous pouvez ajouter les éléments suivants de l'arborescence des dispositifs ou de l'arborescence logique en tant que zones réactives dans une carte de site :

- Caméras
- Entrées
- Relais
- Scripts de commande
- Séquences
- Documents
- Liens vers d'autres cartes de site
- VRM
- iSCSI
- Lecteurs d'un système de contrôle d'accès
- Centrales de détection d'intrusion
- Serveur de gestion d'Enterprise Systems

Lorsque vous ajoutez un élément à une carte de site, une zone réactive est créée sur la carte.

Lorsque vous ajoutez un élément au dossier d'une carte dans l'arborescence logique, cet élément s'affiche également dans le coin supérieur gauche de la carte. Lorsque vous ajoutez un élément à une carte, cet élément s'ajoute également sous le nœud correspondant de la carte dans l'arborescence logique d'Operator Client.

Vous pouvez ajouter les éléments suivants de l'arborescence des dispositifs ou de l'arborescence logique à la carte globale :

- Caméras

Pour configurer l'arborescence logique, vous devez suivre partiellement ou intégralement la procédure ci-dessous et, au besoin, la répéter.

Pour renommer l'arborescence logique :

1. Sélectionnez l'élément racine de l'arborescence logique.

2. Cliquez sur  .

3. Saisissez le nouveau nom.

Ce nom est visible pour tous les utilisateurs dans l'arborescence logique de l'Operator Client.

Se reporter à

- *Page Cartes et structure , page 266*

18.2

Ajout d'un périphérique à l'Arborescence Logique

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Pour ajouter un dispositif :

- ▶ Faites glisser un élément de l'arborescence des dispositifs à l'endroit requis dans l'arborescence logique.

Vous pouvez faire glisser un nœud entier avec tous ses sous-éléments de l'arborescence des dispositifs vers l'arborescence logique. Vous pouvez sélectionner plusieurs dispositifs en appuyant sur la touche CTRL ou MAJ.

Se reporter à

- *Page Cartes et structure , page 266*

18.3 Suppression d'un élément de l'arborescence

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Pour supprimer un élément de l'arborescence logique :

- ▶ Cliquez avec le bouton droit de la souris sur un élément dans l'arborescence logique, puis cliquez sur **Supprimer**. Si l'élément sélectionné comporte des sous-éléments, une boîte de message s'affiche. Pour confirmer, cliquez sur **OK**. L'élément est supprimé. Lorsque vous supprimez un élément du dossier d'une carte dans l'arborescence logique, cet élément est également supprimé de la carte.

Se reporter à

- Page *Cartes et structure* , page 266

18.4 Gestion des fichiers ressources

Fenêtre principale > **Cartes et structure** > > onglet **Arborescence Logique** > 
ou

Fenêtre principale > **Alarmes** > 

Vous pouvez importer des fichiers de ressource dans les formats suivants :


- Fichiers DWF (2D, fichiers de ressource Carte)
- PDF
- JPG
- PNG
- Fichiers HTML
- Fichiers MP3 (fichiers audio)
- Fichiers TXT (Scripts de commande ou séquences de caméras)
- Fichiers MHT (archives Web)
- Fichiers d'URL (liens vers des pages Web)
- Fichiers d'URL HTTPS (liens vers les widgets Intelligent Insights)
- Fichiers WAV (fichiers audio)

Les fichiers de ressource importés sont ajoutés à une base de données. Ils ne sont pas liés aux fichiers d'origine.




Remarque!


Après chacune des tâches suivantes :

Cliquez sur  pour enregistrer les paramètres.


Pour importer un fichier de ressource :

1. Cliquez sur  .
La boîte de dialogue **Importer ressource** s'affiche.
2. Sélectionnez un ou plusieurs fichiers.
3. Cliquez sur **Ouvrir**.
Les fichiers sélectionnés sont ajoutés à la liste.
Si un fichier a déjà été importé, un message s'affiche.
Si vous décidez d'importer à nouveau un fichier déjà importé, une nouvelle entrée est ajoutée à la liste.


Pour supprimer un fichier de ressource :

1. Sélectionnez le fichier de ressource souhaité.
2. Cliquez sur  .
Le fichier de ressource sélectionné est supprimé de la liste.


Pour renommer un fichier de ressource :

1. Sélectionnez le fichier de ressource souhaité.
2. Cliquez sur  .
3. Saisissez le nouveau nom.
Le nom d'origine et la date de création sont conservés.

Pour remplacer le contenu d'un fichier de ressource :

1. Sélectionnez le fichier de ressource souhaité.
2. Cliquez sur  .
La boîte de dialogue **Remplacer ressource** s'affiche.
3. Sélectionnez un fichier dont le contenu est approprié, puis cliquez sur **Ouvrir**.
Le nom de ressource est conservé, le nom d'origine du fichier est remplacé par le nouveau nom de fichier.

Pour exporter un fichier de ressource :

1. Sélectionnez le fichier de ressource souhaité.
2. Cliquez sur  .
Une boîte de dialogue permettant de sélectionner un répertoire s'affiche.
3. Sélectionnez le répertoire approprié, puis cliquez sur **OK**.
Le fichier d'origine est exporté.

Se reporter à

- *Boîte de dialogue Sélectionner une ressource, page 272*

18.4.1**Boîte de dialogue Gestionnaire de ressources**

Fenêtre principale > **Cartes et structure** >  > Boîte de dialogue **Gestionnaire de ressources**

Permet de gérer les fichiers ressource.

Vous pouvez gérer les formats de fichier suivants :

- Fichiers DWF (fichiers ressource Carte)
Ces fichiers sont convertis au format bitmap pour pouvoir être utilisés avec Operator Client.
- PDF
- JPG
- PNG
- Fichiers HTML (documents HTML, tels que les plans d'action)
- Fichiers MP3 (fichiers audio)
- Fichiers TXT (fichiers texte)
- Fichiers d'URL (contiennent des liens vers des pages Web ou des widgets Intelligent Insights)
- Fichiers MHT (archives Web)
- Fichiers WAV (fichiers audio)

– EXE



Cliquez pour afficher une boîte de dialogue permettant d'importer un fichier ressource.



Cliquez sur ce bouton pour afficher la boîte de dialogue **Ajouter l'URL**.



Cliquez sur ce bouton pour afficher la boîte de dialogue **Lien vers l'application externe**.



Cliquez pour supprimer le fichier ressource sélectionné.



Cliquez pour renommer le fichier ressource sélectionné.



Cliquez pour afficher une boîte de dialogue permettant de remplacer le fichier ressource sélectionné par un autre.



Cliquez pour afficher une boîte de dialogue permettant d'exporter le fichier ressource sélectionné.

18.4.2

Boîte de dialogue Sélectionner une ressource



Fenêtre principale > **Cartes et structure** >

Permet d'ajouter un fichier Carte au format DWF, PDF, JPG ou PNG dans l'Arborescence Logique .

Sélectionner un fichier de ressource :

Cliquez sur un nom de fichier pour sélectionner un fichier Carte. Le contenu du fichier sélectionné s'affiche dans le volet d'aperçu.

Gérer...

Cliquez sur ce bouton pour afficher la boîte de dialogue **Gestionnaire de ressources**.

Se reporter à

- *Ajout d'une carte, page 277*
- *Affectation d'une carte à un dossier, page 278*
- *Ajout d'un document, page 272*

18.5

Ajout d'un document

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**


Vous pouvez ajouter des fichiers texte, des fichiers HTML (y compris des fichiers MHT), des fichiers d'URL (contenant une adresse Internet) ou des fichiers d'URL HTTPS (contenant par exemple un widget Intelligent Insights) en tant que documents. Vous pouvez également ajouter un lien vers une autre application.

Pour pouvoir ajouter un document, vous devez avoir importé des fichiers de document.

Pour plus d'informations sur l'importation de fichiers de document, reportez-vous à la rubrique *Gestion des fichiers ressources, page 270*.

Pour ajouter un fichier de document de carte / pour ajouter un widget Intelligent Insights :

1. Assurez-vous que le fichier de document que vous souhaitez ajouter a déjà été importé.
2. Sélectionnez le dossier dans lequel ajouter le nouveau document.



3. Cliquez sur . La boîte de dialogue **Sélectionner une ressource** s'affiche.
4. Sélectionnez un fichier dans la liste. Si les fichiers requis n'apparaissent pas dans la liste, cliquez sur **Gérer...** pour afficher la boîte de dialogue **Gestionnaire de ressources** et importer les fichiers.
5. Cliquez sur **OK**. Un nouveau document est ajouté au dossier sélectionné.

Se reporter à

- *Boîte de dialogue Sélectionner une ressource, page 272*
- *Gestion des fichiers ressources, page 270*

18.5.1

Boîte de dialogue Ajouter URL

Fenêtre principale > **Cartes et structure** >  > 
 Permet d'ajouter une adresse Internet HTTP (URL) ou une adresse HTTPS, comme des widgets Intelligent Insights à votre système. Vous pouvez ajouter cette URL à l'Arborescence Logique en tant que document. L'utilisateur peut afficher une page Internet ou un widget Intelligent Insights dans son Operator Client.

Nom

Saisissez le nom d'affichage de l'URL.

URL

Saisissez l'URL.

Pour une connexion sécurisée uniquement

Utilisateur

Saisissez le nom d'utilisateur pour l'URL HTTPS.

Mot de passe :

Indiquez le mot de passe pour l'URL HTTPS.

Afficher le mot de passe

Permet d'activer l'affichage du mot de passe saisi. Veillez à garder ce mot de passe à l'abri des regards.

Se reporter à

- *Ajout d'un document, page 272*

18.6

Lien vers la boîte de dialogue Application externe

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique** >  > Boîte de dialogue **Gestionnaire de ressources** >  > Boîte de dialogue **Lien vers l'application externe**

Vous permet d'ajouter un lien vers une application externe. Le lien doit être valide sur le poste de travail où ce lien est utilisé.

Remarque!



Une application externe qui commence par un écran d'accueil ne fonctionnera pas comme prévu.

Une application externe qui partage des fonctions avec Operator Client, ne fonctionnera pas comme prévu et peut, dans de rares cas, provoquer un plantage d'Operator Client.

Nom

Saisissez un nom pour le lien qui s'affiche dans l'arborescence logique.

Chemin

Saisissez ou sélectionnez le chemin d'accès à l'application externe. Ce chemin d'accès doit être valide sur le poste de travail où l'utilisateur d'Operator Client utilise ce lien.

Arguments :

Si nécessaire, saisissez des arguments pour la commande qui exécute l'application externe.

18.7


Ajout d'un Script de Commande

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Pour pouvoir ajouter un script de commande, vous devez avoir importé ou créé des fichiers de script de commande.

Si nécessaire, reportez-vous à *Configuration de Scripts de Commande, page 90* pour plus d'informations.

Pour ajouter un fichier de script de commande :

1. Sélectionnez le dossier dans lequel ajouter le nouveau script de commande.
2. Cliquez sur . La boîte de dialogue **Sélectionner un script de client** s'affiche.
3. Sélectionnez un fichier dans la liste.
4. Cliquez sur OK. **OK.**

Un nouveau script de commande est ajouté dans le dossier sélectionné.

Se reporter à

- *Boîte de dialogue Sélectionner une ressource, page 272*



18.8

Ajout d'une séquence de caméras

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Vous pouvez ajouter une séquence de caméras dans le répertoire racine ou dans un dossier de l'arborescence logique.

Pour ajouter une séquence de caméras :

1. Dans l'arborescence logique, sélectionnez le dossier dans lequel ajouter la nouvelle séquence de caméras.
2. Cliquez sur . La boîte de dialogue **Générateur de séquence** s'affiche.
3. Dans la liste, sélectionnez une séquence de caméras.
4. Cliquez sur **Ajouter à l'Arborescence Logique**. Une nouvelle séquence  est ajoutée dans le dossier sélectionné.

Se reporter à

- *Boîte de dialogue Générateur de séquence, page 274*




18.8.1

Boîte de dialogue Générateur de séquence

Fenêtre principale > **Cartes et structure** > 

Permet de gérer les séquences de caméras.

Icônes

	Cliquez sur ce bouton pour afficher la boîte de dialogue Ajouter une séquence .
	Cliquez sur ce bouton pour renommer une séquence de caméras.
	Cliquez sur ce bouton pour supprimer la séquence de caméras sélectionnée.

Ajouter un pas

Cliquez sur ce bouton pour afficher la boîte de dialogue **Ajouter un pas de séquence**.

Supprimer le pas

Cliquez sur ce bouton pour supprimer les pas sélectionnés.

Pas

Affiche le numéro du pas. Toutes les caméras d'un pas particulier possèdent la même durée de temporisation.

Temporisation

Permet de modifier la durée de temporisation (en secondes).

Numéro de caméra

Cliquez sur une cellule pour sélectionner une caméra d'après son numéro logique.

Caméra

Cliquez sur une cellule pour sélectionner une caméra d'après son nom.

Fonction de la caméra

Cliquez sur une cellule pour changer la fonction de la caméra dans cette ligne.

Données

Entrez la durée de la fonction de caméra sélectionnée. Pour pouvoir configurer ceci, vous devez avoir sélectionné une entrée de la colonne **Caméra** et une entrée de la colonne

Fonction de la caméra.

Unité de données

Sélectionnez l'unité de la durée sélectionnée, telle que les secondes. Pour pouvoir configurer ceci, vous devez avoir sélectionné une entrée de la colonne **Caméra** et une entrée de la colonne **Fonction de la caméra**.

Ajouter à l'Arborescence Logique

Cliquez sur ce bouton pour ajouter la séquence de caméras sélectionnée à l'Arborescence Logique et fermer la boîte de dialogue.

Se reporter à

- *Gestion des séquences de caméra préconfigurées, page 275*

18.9

Gestion des séquences de caméra préconfigurées

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Vous pouvez effectuer les tâches suivantes pour gérer les séquences de caméra :

- Créer une séquence de caméras
- Ajouter une étape utilisant une nouvelle durée de temporisation à une séquence de caméras existante
- Supprimer une étape d'une séquence de caméras
- Supprimer une séquence de caméras

**Remarque!**

Lorsque la configuration est modifiée et activée, une séquence de caméras (préconfigurée ou automatique) se poursuit généralement après le redémarrage d'Operator Client.

En revanche, les séquences sont interrompues dans les cas suivants :


Suppression d'un moniteur sur lequel la séquence est configurée pour être affichée.

Modification du mode d'un moniteur (vue unique/mode quadravision) sur lequel la séquence est configurée pour être affichée.



Le numéro logique d'un moniteur sur lequel la séquence est configurée pour être affichée a changé.

**Remarque!**

Après chacune des tâches suivantes :

Cliquez sur  pour enregistrer les paramètres.

Pour créer une séquence de caméras :

1. Dans l'arborescence logique, sélectionnez le dossier dans lequel vous voulez créer la nouvelle séquence de caméras.
2. Cliquez sur .
La boîte de dialogue **Générateur de séquence** s'affiche.
3. Dans la boîte de dialogue **Générateur de séquence**, cliquez sur .
La boîte de dialogue **Ajouter une séquence** s'affiche.
4. Entrez les valeurs appropriées.
5. Cliquez sur **OK**.

Une nouvelle séquence de caméras  est ajoutée.

Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.


Pour ajouter un pas utilisant une nouvelle durée de temporisation à une séquence de caméras :

1. Sélectionnez la séquence de caméras qui vous intéresse.
2. Cliquez sur **Ajouter un pas**.
La boîte de dialogue **Ajouter un pas de séquence** s'affiche.
3. Définissez les paramètres appropriés.
4. Cliquez sur **OK**.
Un nouveau pas est ajouté à la séquence de caméras.

Pour supprimer un pas d'une séquence de caméras :

- ▶ Cliquez avec le bouton droit de la souris sur la séquence de caméras voulue, puis cliquez sur **Supprimer le pas**.
Le pas portant le numéro le plus élevé est supprimé.



Pour supprimer une séquence de caméras :

1. Sélectionnez la séquence de caméras qui vous intéresse.
2. Cliquez sur . La séquence de caméras sélectionnée est supprimée.

Se reporter à

- Boîte de dialogue *Générateur de séquence*, page 274

18.9.1 Boîte de dialogue Ajouter une séquence

Fenêtre principale > **Cartes et structure** >  > Boîte de dialogue **Générateur de séquence** > 

Permet de configurer les propriétés d'une séquence de caméras.

Nom de la séquence :

Saisissez le nom de la nouvelle séquence de caméras.

N° logique :

Pour une utilisation avec un clavier numérique IntuiKey de Bosch, saisissez un numéro logique pour la séquence.

Durée de temporisation :

Entrez la durée de temporisation appropriée.

Caméras par pas :

Entrez le nombre de caméras à chaque pas.

Pas :

Entrez le nombre de pas approprié.

18.9.2 Boîte de dialogue Ajouter un pas de séquence

Fenêtre principale > **Cartes et structure** >  > Bouton **Ajouter un pas**
Permet d'ajouter un pas ayant une nouvelle durée de temporisation à une séquence de caméras existante.

Durée de temporisation :


Entrez la durée de temporisation appropriée.

18.10 Ajout d'un dossier

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Pour ajouter un dossier :

1. Sélectionnez le dossier dans lequel vous voulez en ajouter un autre.

2. Cliquez sur . Un nouveau dossier est ajouté dans le dossier sélectionné.

3. Cliquez sur  pour renommer le dossier.

4. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.

Se reporter à

– Page *Cartes et structure*, page 266


18.11 Ajout d'une carte


Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Pour pouvoir ajouter une carte, vous devez avoir importé des fichiers de ressource Carte. Pour plus d'informations sur l'importation d'un fichier de ressource Carte, reportez-vous à *Gestion des fichiers ressources*, page 270.

Pour ajouter une carte :

1. Assurez-vous que le fichier de ressource Carte que vous souhaitez ajouter a déjà été importé.
2. Sélectionnez le dossier dans lequel vous voulez ajouter la nouvelle carte.

3. Cliquez sur . La boîte de dialogue **Sélectionner une ressource** s'affiche.
4. Sélectionnez un fichier dans la liste.
Si les fichiers requis n'y figurent pas, cliquez sur **Gérer...** pour afficher la boîte de dialogue **Gestionnaire de ressources** et importer des fichiers.
5. Cliquez sur **OK**.

Une nouvelle carte  est ajoutée sous le dossier sélectionné.
La carte s'affiche.

Tous les dispositifs contenus dans ce dossier s'affichent dans l'angle supérieur gauche de la carte.

Se reporter à

- *Boîte de dialogue Sélectionner une ressource, page 272*



18.12

Ajout d'un lien vers une autre carte

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**


Lorsque vous avez ajouté au moins deux cartes, vous pouvez ajouter sur l'une d'elles un lien pointant vers l'autre ; ceci permet à l'utilisateur de passer facilement d'une carte à une autre.

Pour ajouter un lien :

1. Cliquez sur le dossier d'une carte  dans l'arborescence logique.
2. Cliquez avec le bouton droit de la souris sur la carte, puis cliquez sur **Créer un lien**.
La boîte de dialogue **Sélectionner une carte pour le lien** s'affiche.
3. Dans la boîte de dialogue, cliquez sur une carte .
4. Cliquez sur **Sélectionner**.
5. Faites glisser l'élément à l'endroit approprié de la carte.

18.12.1

Boîte de dialogue Sélectionner une carte pour le lien

Fenêtre principale > **Cartes et structure** > sélectionnez le dossier d'une carte  dans l'Arborescence Logique > Cliquez avec le bouton droit sur la carte et cliquez sur **Créer un lien**

Permet de sélectionner une carte pour créer un lien vers une autre carte.



Cliquez sur la carte à sélectionner.

Sélectionner

Cliquez sur ce bouton pour insérer le lien vers la carte sélectionnée.


18.13

Affectation d'une carte à un dossier

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Pour pouvoir affecter des cartes, vous devez avoir importé des fichiers de ressource Carte.
Si nécessaire, reportez-vous à *Gestion des fichiers ressources, page 270* pour plus d'informations.

Pour affecter un fichier de ressource Carte :

1. Cliquez avec le bouton droit de la souris sur un dossier, puis cliquez sur **Affecter une carte**.
La boîte de dialogue **Sélectionner une ressource** s'affiche.
2. Sélectionnez un fichier de ressource Carte dans la liste.
3. Cliquez sur **OK**. Le dossier sélectionné apparaît sous la forme .
La carte est affichée dans la fenêtre de plans.
Tous les éléments contenus dans ce dossier s'affichent dans l'angle supérieur gauche de la carte.

Se reporter à

- Page *Cartes et structure*, page 266
- Boîte de dialogue *Sélectionner une ressource*, page 272


18.14**Gérer des dispositifs sur une carte de site**

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Pour pouvoir gérer des dispositifs sur une carte de site, vous devez ajouter ou affecter une carte à un dossier, puis ajouter des dispositifs à ce dossier.

**Remarque!**

Après chacune des tâches suivantes :

Cliquez sur  pour enregistrer les paramètres.

Pour placer des éléments sur une carte de site :

1. Sélectionnez le dossier d'une carte.
2. Faites-y glisser des dispositifs de l'arborescence des dispositifs.
Les dispositifs figurant dans ce dossier se trouvent dans le coin supérieur gauche de la carte de site.
3. Faites glisser les éléments à l'endroit approprié de la carte de site.

Pour supprimer uniquement de la carte de site un élément figurant dans l'arborescence logique :

1. Cliquez avec le bouton droit de la souris sur la carte, puis cliquez sur **Invisible**.
L'élément est supprimé de la carte de site.
Il reste toutefois dans l'arborescence logique.
2. Pour le faire réapparaître, cliquez avec le bouton droit de la souris sur le dispositif dans l'arborescence logique et sélectionnez l'option **Visible sur la carte**.

Pour supprimer un élément de la carte de site et de l'arborescence logique complète :

- ▶ Cliquez avec le bouton droit de la souris sur l'élément dans l'arborescence logique, puis cliquez sur **Supprimer**.
L'élément est supprimé de la carte de site et de l'arborescence logique.

Pour modifier l'icône représentant l'orientation d'une caméra :

- ▶ Cliquez avec le bouton droit de la souris sur l'élément, pointez sur **Modifier l'image**, puis cliquez sur l'icône appropriée.
L'icône change en conséquence.

Pour modifier la couleur d'un élément :

- ▶ Cliquez avec le bouton droit de la souris sur l'élément, puis cliquez sur **Modifier la couleur**. Sélectionnez la couleur appropriée.
L'icône change en conséquence.

Pour exclure / rétablir un dispositif sur une carte de site :

1. Cliquez avec le bouton droit de la souris sur le dispositif, sur la carte de site.
2. Cliquez sur **Ignorer / Arrêter d'ignorer**.

**Remarque!**

Il est possible de filtrer des dispositifs exclus dans le champ de recherche.

Se reporter à

- *Configuration de l'exclusion de dispositifs, page 286*
- *Page Cartes et structure , page 266*

18.15**Configurer la carte globale et les zones de visualisation de carte**

Fenêtre principale > **Cartes et structure** > Onglet **Carte globale**

Pour utiliser des cartes en ligne ou le Map-based tracking assistant dans Operator Client, vous devez ajouter et configurer des caméras sur la carte globale.

Vous pouvez configurer des zones de visualisation de carte à partir d'une carte globale. Une zone de visualisation de carte est une zone de la carte globale avec un centre et un niveau de zoom spécifiques. Une zone de visualisation de carte peut être affichée dans le volet des images d'Operator Client.

Si vous souhaitez créer une zone de visualisation de carte ou utiliser le Map-based tracking assistant dans Operator Client, procédez comme suite la première fois :

1. Sélectionnez le type de plan d'arrière-plan de la carte globale.
2. Faites glisser vos caméras vers la carte globale.
3. Configurez la direction et le cône de vue de vos caméras sur la carte globale.

Si vous souhaitez créer des zones de visualisation de carte ou utiliser le Map-based tracking assistant dans l'Operator Client **sur plusieurs étages**, commencez par procéder comme suit :

1. Sélectionnez le type de plan d'arrière-plan de la carte globale.
2. Ajoutez une carte à la carte globale.

Remarque : la première carte à ajouter sera le rez-de-chaussée. Si vous sélectionnez le type de carte d'arrière-plan hors ligne **Aucun**, la première carte que vous ajoutez est la carte d'arrière-plan.

3. Ajoutez des étages au rez-de-chaussée ou à la carte d'arrière-plan.
4. Sélectionnez l'étage approprié.
5. Faites glisser vos caméras vers la carte de l'étage.
6. Configurez la direction et le cône de vue de vos caméras.

18.15.1**Configurer la carte globale**

Vous pouvez définir des types de plan d'arrière-plan pour la carte globale et rechercher des caméras, des emplacements et des adresses.

Pour modifier le type de carte d'arrière-plan de la carte globale :

1. Accédez à la fenêtre principale et sélectionnez le menu **Paramètres** > commande **Options**.

2. Sélectionnez l'option appropriée.
Remarque : Si vous avez accès à Internet, vous pouvez sélectionner un type de carte d'arrière-plan en ligne (cartes Here). Si vous n'avez pas accès à Internet, sélectionnez le type de carte d'arrière-plan hors ligne **Aucun**.
Vous devez acheter une licence pour utiliser des cartes en ligne.
3. Si vous avez sélectionné un type de carte d'arrière-plan en ligne, saisissez votre clé API spécifique au client.
4. Cliquez sur **Test** pour vérifier la connexion d'API.
5. Cliquez sur **OK**.




Remarque!

Si vous passez le type de carte d'arrière-plan du mode en ligne (cartes Here) au mode hors ligne (**Aucun**) ou l'inverse, vous perdez toutes les zones réactives de la caméra positionnés et les zones de visualisation de carte.

Vous ne pouvez définir qu'un seul arrière-plan pour la carte globale. Cet arrière-plan s'applique à toutes les zones de visualisation de la carte.

Pour rechercher des caméras ou des emplacements sur la carte globale :

1. Dans le champ de recherche, saisissez le nom d'une caméra, d'un emplacement ou d'une adresse.
 Dès que vous commencez la saisie, un menu déroulant affiche une liste d'options pertinentes.
2. Sélectionnez l'option respective dans la liste
 La caméra, l'emplacement ou l'adresse s'affichent et sont indiquées par un indicateur  pendant quelques secondes.

Se reporter à

- Boîte de dialogue Options (menu Paramètres), page 122


18.15.2

Configuration des caméras sur la carte globale

Pour configurer une caméra sur la carte globale :

Remarque : si vous avez configuré plusieurs étages sur des cartes, assurez-vous de sélectionner l'étage où vous souhaitez configurer vos caméras.



1. Sélectionnez l'onglet **Carte globale**.
2. Pour accéder à la position, où placer la caméra, saisissez une adresse ou un emplacement dans le champ de recherche.

Vous pouvez également effectuer un zoom avant ou arrière à l'aide des bouton  et

 à l'aide de la molette de la souris.

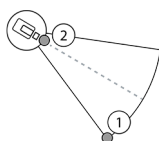
3. Faites glisser une caméra de l'arborescence des dispositifs vers la zone respective de la carte globale.
4. Cliquez sur la caméra pour la sélectionner.
5. Configurez la direction et le cône de vue de la caméra.

Remarque : Lorsque vous sélectionnez une caméra dôme, vous pouvez visualiser le cône de vue accessible et le cône de vue réel. Un symbole d'avertissement signifie que le cône de vue réel de la caméra dôme doit être étalonné horizontalement et verticalement. Pour étalonner la caméra dôme, ouvrez la prévisualisation de la vidéo en temps réel.

6. Cliquez sur  pour voir la prévisualisation de la vidéo en temps réel de la caméra sélectionnée.
La prévisualisation de la vidéo peut vous aider à configurer la direction et le cône de vue.
7. Cliquez sur  pour masquer la prévisualisation de la vidéo de la caméra sélectionnée.

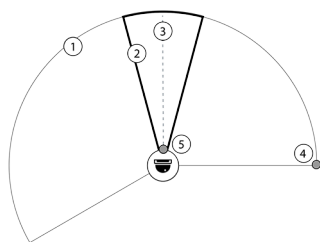
Remarque : Si vous ajoutez une caméra à la carte globale et que vous n'avez pas déjà ajouté cette caméra à l'arborescence logique, elle sera ajoutée automatiquement à la fin de l'arborescence logique.

Pour configurer la direction et le cône de vue d'une caméra :



1. Faites glisser le cône de vue afin de le configurer.
2. Faites glisser le cône pour lui faire effectuer une rotation et configurer la direction.

Pour configurer la direction horizontale et le cône de vue d'une caméra PTZ (plate-forme CPP4ou supérieure) :




1. Le cône de vue accessible indique la zone de vue en théorie accessible.
2. Le cône de vue réel indique la position de balayage horizontal/vertical et de zoom (PTZ) réelle de la caméra.
3. Angle d'orientation 0.
4. Faites glisser le cône de vue afin de le configurer.
5. Faites glisser le cône pour lui faire effectuer une rotation et configurer la direction.


Remarque!

Pour garantir une utilisation optimale du Map-based tracking assistant, vous devez également régler la position verticale de la caméra PTZ. Nous vous recommandons de régler la position verticale dans la prévisualisation de la vidéo en temps réel en vous basant sur une position bien connue de la zone, par exemple en vous basant sur un monument distinctif. Le Map-based tracking assistant utilisera toujours ultérieurement cette position verticale configurée.



Pour afficher ou masquer les aperçus de caméra :

1. Cliquez sur  pour voir la prévisualisation de la vidéo en temps réel de la caméra sélectionnée.
Ou
Cliquez avec le bouton droit de la souris sur la caméra et sélectionnez **Afficher les aperçus**.
L'aperçu vidéo peut vous aider à configurer la direction et le cône de vue.

2. Cliquez sur  pour masquer l'aperçu vidéo de la caméra sélectionnée.
Ou
Cliquez avec le bouton droit de la souris sur la caméra et sélectionnez **Masquer les aperçus**.

Pour supprimer une caméra de la carte globale :

- ▶ Cliquez avec le bouton droit de la souris sur la caméra et sélectionnez **Supprimer**.

Pour rendre une caméra visible à tous les étages :

- ▶ Cliquez avec le bouton droit de la souris sur la caméra et sélectionnez **Visible à tous les étages**.

La caméra est à présent toujours visible lorsque vous sélectionnez un autre étage.

Regrouper les zones réactives d'une caméra

Si vous avez déjà configuré plusieurs caméras sur la carte globale et la fonction de zoom arrière, les zones réactives de la caméra sont regroupées dans des groupes de zones réactives. Le nombre de zones réactives d'un groupe de zones réactives est affiché. Une caméra sélectionnée ne s'affiche pas dans le cadre d'un groupe.


18.15.3


Ajouter des cartes sur la carte globale





Vous pouvez ajouter vos propres fichiers de carte de construction sur la carte globale. Les opérateurs BVMS peuvent alors obtenir une vue plus détaillée de certains emplacements de caméras.

Pour ajouter une carte sur la carte globale :


1. Sélectionnez l'onglet **Carte globale**.
2. Pour accéder à la position, où placer votre carte, saisissez une adresse ou un emplacement dans le champ de recherche.

Vous pouvez également effectuer un zoom avant ou arrière à l'aide des boutons  et


 à l'aide de la molette de la souris.

3. Cliquez sur .
La fenêtre **Sélectionner une ressource** s'affiche.
4. Sélectionnez une carte et cliquez sur **OK**.
5. Cliquez sur  et faites-le glisser pour faire pivoter la carte.
6. Cliquez sur  et faites-le glisser pour déplacer la carte.
7. Utilisez les points de glisser-déposer pour régler la taille de votre carte.
8. Cliquez sur  pour supprimer la carte.

Remarque : si vous souhaitez ajouter plusieurs étages, la première carte à ajouter est le rez-

de-chaussée. Le rez-de-chaussée est indiqué par le chiffre 0 dans le champ .


Pour ajouter des étages au rez-de-chaussée :

1. Cliquez sur le chiffre 0 dans le champ .



Le champ  s'ouvre.

2. Sélectionnez l'étage où vous souhaitez ajouter une carte.
3. **Remarque :** vous pouvez uniquement sélectionner l'étage supérieur ou inférieur suivant pour ajouter une carte.

4. Cliquez sur .

La fenêtre **Sélectionner une ressource** s'affiche.

5. Sélectionnez une carte et cliquez sur **OK**.
6. Modifiez la carte d'étage ajoutée pour adapter la position à celle de la carte du rez-de-chaussée.

Pour rendre un étage visible à tous les étages :

1. Cliquez avec le bouton droit de la souris sur n'importe laquelle des icônes de réglage de la carte d'étage correspondante, \cup , + ou \times .
2. Sélectionnez **Visible à tous les étages**.


Cet étage est désormais toujours visible lorsque vous sélectionnez un autre étage.

Remarque : si vous n'avez pas accès à Internet et que vous avez sélectionné le type de carte d'arrière-plan hors ligne **Aucun**, vous pouvez ajouter une carte comme carte d'arrière-plan. Nous recommandons de rendre cette carte d'arrière-plan visible à tous les étages. La carte d'arrière-plan sera ensuite toujours visible si vous sélectionnez un autre étage.

18.16**Ajouter une zone de visualisation de carte**


Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Pour ajouter une zone de visualisation de carte :

1. Cliquez sur  pour ajouter une zone de visualisation de carte.
2. Saisissez le nom de votre zone de visualisation de carte.
3. Pour accéder à l'emplacement où vous souhaitez créer votre zone de visualisation de carte, saisissez une adresse ou un emplacement dans le champ de recherche de la carte globale.

Si vous ne connaissez pas l'adresse ou l'emplacement, vous pouvez effectuer un zoom

avant ou arrière à l'aide des boutons  et  de la molette de la souris.

4. Cliquez sur  pour enregistrer votre configuration.

Remarque!

Si une zone de visualisation de carte contient différents étages, l'étage qui est sélectionné lors de l'enregistrement de la configuration est celui qui s'affiche dans l'Operator Client lorsque l'opérateur ouvre la zone de visualisation de carte. L'opérateur peut ensuite changer l'étage de la zone de visualisation de carte dans le volet des images.



18.17 Activer le Map-based tracking assistant

Le Map-based tracking assistant vous permet de suivre les objets en déplacement sur plusieurs caméras. Les caméras respectives doivent être configurées sur la carte globale. Si un objet en mouvement d'intérêt apparaît en temps réel, en lecture ou dans le volet d'images d'alarme, l'utilisateur peut lancer automatiquement le Map-based tracking assistant qui affiche automatiquement toutes les caméras situées à proximité.

Pour activer le Map-based tracking assistant :

1. Accédez à la fenêtre principale et sélectionnez le menu **Paramètres** > commande **Options**.
2. Cochez la case **Activer la fonction système**.
3. Cliquez sur **OK**.

18.18 Ajout d'un relais de dysfonctionnement

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique** > Boîte de

dialogue  > **Relais de dysfonctionnement**

Utilisation prévue

Un relais de dysfonctionnement est destiné à s'activer en cas d'erreur système grave pour déclencher une alerte externe (flash, sirène, etc.).

L'utilisateur doit réinitialiser le relais manuellement.

Le relais de dysfonctionnement peut être l'un des relais de la liste suivante :

- Relais de décodeur ou d'encodeur BVIP
- Relais ADAM
- Sortie de la centrale d'intrusion

Exemple

S'il se produit un événement affectant fortement le fonctionnement du système (par exemple, une défaillance de disque dur) ou un incident mettant en danger la sécurité d'un site (par exemple, une vérification des images de référence défaillante), le relais de dysfonctionnement est activé. Cela peut, par exemple, déclencher une alarme sonore ou fermer automatiquement des portes.

Fonctions

Vous pouvez configurer un seul relais pour jouer le rôle de relais de dysfonctionnement. Le relais de dysfonctionnement est activé automatiquement en cas de déclenchement d'un événement figurant dans un ensemble d'événements définis par l'utilisateur. L'activation d'un relais signifie qu'une commande sera envoyée au relais pour le fermer. L'événement « Relais fermé » suivant est découplé de la commande ; il ne sera généré et reçu que si l'état du relais est modifié physiquement. Par exemple, un relais dont la fermeture a lieu avant n'enverra pas cet événement.

Outre le fait qu'il est déclenché automatiquement par l'ensemble des événements définis par l'utilisateur, le relais de dysfonctionnement est traité comme tout autre relais.

Par conséquent, l'utilisateur peut le désactiver dans l'Operator Client. Le client Web permet également de désactiver le relais de dysfonctionnement. Étant donné que les autorisations d'accès classiques s'appliquent également au relais de dysfonctionnement, tous les clients doivent tenir compte des autorisations de l'utilisateur connecté.

Pour effectuer un ajout :

1. Dans la liste **Relais de dysfonctionnement**, sélectionnez le relais souhaité.

2. Cliquez sur **Événements...**
La boîte de dialogue **Sélection d'événements pour le relais de dysfonctionnement** s'affiche.
3. Cliquez pour sélectionner les événements souhaités susceptibles de déclencher le relais de dysfonctionnement.
4. Cliquez sur **OK**.
Le relais de dysfonctionnement est ajouté au système.

18.18.1

Boîte de dialogue Relais de dysfonctionnement

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique** > Boîte de

dialogue  > **Relais de dysfonctionnement**

Vous pouvez ajouter un relais de dysfonctionnement au système. Vous définissez le relais qui doit être utilisé comme relais de dysfonctionnement et vous configurez les événements qui déclenchent ce dernier.

Le relais doit déjà être configuré dans l'Arborescence logique.

Relais de dysfonctionnement

Dans la liste, sélectionnez le relais souhaité.

Événements...

Cliquez sur ce bouton pour afficher la boîte de dialogue **Sélection d'événements pour le relais de dysfonctionnement**.

18.19

Configuration de l'exclusion de dispositifs

Fenêtre principale > **Cartes et structure** > Onglet **Arborescence Logique**

Il est possible d'exclure des encodeurs, des caméras, des entrées et des relais, par exemple, pendant des travaux de construction. Si un encodeur, une caméra, une entrée ou un relais est exclu, l'enregistrement s'arrête, le BVMS Operator Client n'affiche pas d'événement ni d'alarme et les alarmes ne sont pas enregistrées dans le journal des connexions.

Les caméras exclues continuent d'afficher la vidéo en temps réel dans l'Operator Client et l'opérateur a toujours accès aux anciens enregistrements.

Remarque!



Si l'encodeur est exclu, aucune alarme ni aucun événement n'est généré pour l'ensemble des caméras, relais et entrées de cet encodeur. En cas d'exclusion d'une caméra, d'un relais ou d'une entrée, et si un dispositif est déconnecté de l'encodeur, ces alarmes sont toujours générées.

Pour exclure / rétablir un dispositif dans l'arborescence logique ou dans l'arborescence des dispositifs :

1. Dans l'arborescence logique ou dans l'arborescence des dispositifs, cliquez avec le bouton droit de la souris sur le dispositif.
2. Cliquez sur **Ignorer / Arrêter d'ignorer**.

Pour exclure / rétablir un dispositif sur une carte :

Voir *Gérer des dispositifs sur une carte de site*, page 279



Remarque!

Il est possible de filtrer des dispositifs exclus dans le champ de recherche.

Se reporter à

- *Gérer des dispositifs sur une carte de site, page 279*

19 Page Planifications

Fenêtre principale >

Permet de configurer des Planifications d'Enregistrement et des Planifications de Tâches.



Cliquez sur ce bouton pour renommer la Planification d'Enregistrement ou la Planification des Tâches sélectionnée.

Planifications d'Enregistrement

Affiche l'arborescence des Planifications d'Enregistrement. Sélectionnez l'entrée à configurer.

Planifications de Tâches

Affiche l'arborescence des Planifications de Tâches. Sélectionnez l'entrée à configurer.

Ajouter

Cliquez sur ce bouton pour ajouter une nouvelle Planification de Tâches.

Supprimer

Cliquez sur ce bouton pour supprimer la Planification des Tâches sélectionnée.

Se reporter à

– *Configuration des planifications, page 291*

19.1 Page Planifications d'Enregistrement

Fenêtre principale > > sélectionner un élément dans l'arborescence Planifications d'Enregistrement

Permet de configurer les Planifications d'Enregistrement.

Jours de semaine

Cliquez sur ce bouton pour afficher le Tableau de Planification pour les jours de la semaine.

Les périodes de toutes les Planifications d'Enregistrement configurées s'affichent.

Faites glisser le pointeur pour sélectionner les périodes de la planification sélectionnée.

Toutes les cellules sélectionnées adoptent la couleur de la planification sélectionnée.

Les 24 heures de la journée s'affichent horizontalement. Chaque tranche horaire est divisée en 4 cellules, représentant chacune 15 minutes.

Jours fériés

Cliquez sur ce bouton pour afficher le Tableau de Planification pour les jours fériés.

Jours d'exception

Cliquez sur ce bouton pour afficher le Tableau de Planification pour les Jours d'Exception.

Ajouter

Cliquez sur ce bouton pour afficher une boîte de dialogue permettant d'ajouter des jours fériés et des Jours d'Exception.

Supprimer

Cliquez sur ce bouton pour afficher une boîte de dialogue permettant de supprimer des jours fériés ou des Jours d'Exception.

Se reporter à

- *Configuration d'une Planification d'Enregistrement, page 291*
- *Ajout de jours fériés et de jours d'exception, page 293*
- *Suppression de jours fériés et de jours d'exception, page 294*
- *Modification du nom d'une planification, page 294*

19.2 Page Planifications de Tâches

Fenêtre principale > > sélectionner un élément dans l'arborescence des Planifications de Tâches

Permet de configurer les Planifications de Tâches disponibles. Vous pouvez configurer un modèle standard ou récurrent.

Standard

Cliquez sur ce bouton pour afficher le Tableau de Planification en vue de configurer des Planifications de Tâches standard. Si vous configurez un modèle standard, aucun modèle récurrent n'est valide pour la planification sélectionnée.

Récurrent

Cliquez sur ce bouton pour afficher le Tableau de Planification en vue de configurer un modèle récurrent pour la Planification des Tâches sélectionnée. Par exemple, vous pouvez configurer une planification pour un mardi sur deux tous les mois ou pour le 14 juillet tous les ans. Si vous configurez un modèle récurrent, aucun modèle standard n'est valide pour la Planification des Tâches sélectionnée.

Jours de semaine

Cliquez sur ce bouton pour afficher le Tableau de Planification pour les jours de la semaine. Faites glisser le pointeur pour sélectionner les périodes de la planification sélectionnée. Les cellules sélectionnées s'affichent dans la couleur de la planification sélectionnée. Les 24 heures de la journée s'affichent horizontalement. Chaque tranche horaire est divisée en 4 cellules, représentant chacune 15 minutes.

Jours fériés

Cliquez sur ce bouton pour afficher le Tableau de Planification pour les jours fériés.

Jours d'exception

Cliquez sur ce bouton pour afficher le Tableau de Planification pour les Jours d'Exception.

Tout décocher

Cliquez sur ce bouton pour effacer les périodes de tous les jours disponibles (jours de la semaine, jours fériés, Jours d'Exception).

Sélectionner tout

Cliquez sur ce bouton pour sélectionner les périodes de tous les jours disponibles (jours de la semaine, jours fériés, Jours d'Exception).

Ajouter...

Cliquez sur ce bouton pour afficher une boîte de dialogue permettant d'ajouter des jours fériés et des Jours d'Exception.

Supprimer...

Cliquez sur ce bouton pour afficher une boîte de dialogue permettant de supprimer les jours fériés ou les Jours d'Exception.

Périodicité

Cliquez sur la fréquence à laquelle répéter la Planification des Tâches (Quotidien, Hebdomadaire, Mensuel, Annuel), puis sélectionnez les options correspondantes.

Modèle des jours

Faites glisser le pointeur pour sélectionner les périodes du modèle récurrent.

Se reporter à

- *Ajout d'une Planification des Tâches, page 292*
- *Configuration d'une Planification des Tâches standard, page 292*

- *Configuration d'une Planification des Tâches récurrente, page 292*
- *Suppression d'une Planification des Tâches, page 293*
- *Ajout de jours fériés et de jours d'exception, page 293*
- *Suppression de jours fériés et de jours d'exception, page 294*
- *Modification du nom d'une planification, page 294*

20

Configuration des planifications

Fenêtre principale > **Planifications**

Il existe deux types de planifications :




- Planifications d'Enregistrement
- Planifications des Tâches

Vous pouvez configurer un maximum de 10 Planifications d'Enregistrement différentes dans le Tableau des Planifications d'Enregistrement. Dans ces segments, les caméras peuvent se comporter différemment. Elles peuvent par exemple avoir des paramètres de cadence d'images et de résolution différents (à configurer sur la page **Caméras et enregistrement**). Il existe à tout moment une Planification d'Enregistrement valide. Il n'y a aucun temps mort ni chevauchement.

Vous pouvez configurer des Planifications de Tâches pour planifier divers événements susceptibles de se produire dans le système (à configurer sur la page **Événements**).

Voir le glossaire pour la définition des termes Planifications d'Enregistrement et Planifications de Tâches.

Les planifications sont utilisées dans d'autres pages de Configuration Client :

- Page **Caméras et enregistrement**
Permet de configurer un enregistrement.
- Page **Événements**
Permet de déterminer le moment où les événements doivent être consignés ou le moment où ils doivent déclencher des alarmes ou l'exécution de Scripts de Commande.
- Page **Groupes d'utilisateurs**
Permet de déterminer le moment où les membres d'un groupe d'utilisateurs peuvent ouvrir une session.
- Cliquez sur  pour enregistrer les paramètres.
- Cliquez sur  pour annuler le dernier paramètre.
- Cliquez sur  pour activer la configuration.

Se reporter à

- Page *Planifications d'Enregistrement*, page 288
- Page *Planifications de Tâches*, page 289

20.1

Configuration d'une Planification d'Enregistrement

Fenêtre principale > **Planifications**

Vous pouvez ajouter des Jours d'Exception et des jours fériés aux Planifications d'Enregistrement. Ces paramètres sont prioritaires par rapport aux paramètres hebdomadaires standard.

La séquence par priorité décroissante est la suivante : jours d'exception, jours fériés, jours de semaine.

Le nombre maximal de Profils d'Enregistrement est de 10. Les trois premières entrées sont configurées par défaut. Vous pouvez toutefois modifier ces paramètres. Les entrées

accompagnées de l'icône grise  ne comportent pas de période.

Les Planifications d'Enregistrement partagent les mêmes jours de semaine.

Chaque Planification des Tâches standard présente ses propres schémas de jours de semaine.

Pour configurer une Planification d'Enregistrement :

1. Dans l'arborescence **Planifications d'Enregistrement**, sélectionnez une planification.
2. Cliquez sur l'onglet **Jours de semaine**.
3. Dans le champ **Tableau de Planification**, faites glisser le pointeur pour sélectionner les périodes applicables à la planification sélectionnée. Les cellules sélectionnées s'affichent dans la couleur de la planification sélectionnée.

Remarques :

- vous pouvez repérer une période d'un jour de semaine d'une Planification d'Enregistrement dans la couleur d'une autre Planification d'Enregistrement.

Se reporter à

- *Page Planifications d'Enregistrement, page 288*

20.2

Ajout d'une Planification des Tâches

Fenêtre principale > **Planifications**

Pour ajouter une Planification des Tâches :

1. Cliquez sur **Ajouter**.
Une nouvelle entrée est ajoutée.
2. Saisissez un nom.
3. Cliquez sur **Standard** pour une Planification des Tâches ou sur **Récurrent** pour une Planification des Tâches récurrente.
Si vous modifiez ce paramètre, une boîte de message s'affiche. Cliquez sur **OK** si vous voulez modifier le type de planification.

Une Planification des Tâches standard est affichée en tant que  , une Planification des Tâches récurrente en tant que 

4. Paramétrez la planification sélectionnée comme vous le souhaitez.

Se reporter à

- *Page Planifications de Tâches, page 289*

20.3

Configuration d'une Planification des Tâches standard

Fenêtre principale > **Planifications**

Chaque Planification des Tâches standard présente ses propres schémas de jours de semaine.

Pour configurer un Profil de Tâches standard :

1. Dans l'arborescence **Planifications de Tâches**, sélectionnez une Planification des Tâches standard.
2. Cliquez sur l'onglet **Jours de semaine**.
3. Dans le champ **Tableau de Planification**, faites glisser le pointeur pour sélectionner les périodes applicables à la planification sélectionnée.

Se reporter à

- *Page Planifications de Tâches, page 289*


20.4

Configuration d'une Planification des Tâches récurrente

Fenêtre principale > **Planifications**

Chaque Planification des Tâches récurrente présente son propre modèle des jours.

Pour configurer une Planification des Tâches récurrente :

1. Dans l'arborescence **Planifications de Tâches**, sélectionnez une Planification des Tâches  récurrente.
2. Dans le champ **Périodicité**, cliquez sur la fréquence à laquelle la Planification des Tâches doit se répéter (**Chaque jour**, **Chaque semaine**, **Chaque mois**, **Annuel**), puis sélectionnez les paramètres correspondants.
3. Dans la liste **Date début** :, sélectionnez la date de début appropriée.
4. Dans le champ **Modèle des jours**, faites glisser le pointeur pour sélectionner la période appropriée.

Se reporter à

- *Page Planifications de Tâches, page 289*

20.5**Suppression d'une Planification des Tâches**

Fenêtre principale > > sélectionner un élément dans l'arborescence **Planifications de Tâches**

Pour supprimer une Planification des Tâches :

1. Dans l'arborescence **Planifications de Tâches**, sélectionnez un élément.
2. Cliquez sur **Supprimer**.
La Planification des Tâches est supprimée. Aucun des éléments affectés à cette planification n'est planifié.

Se reporter à

- *Page Planifications de Tâches, page 289*

20.6**Ajout de jours fériés et de jours d'exception**

Fenêtre principale > **Planifications**

**Remarque!**

Vous pouvez configurer des jours d'exception et des jours fériés vides. Les jours d'exception et les jours fériés remplacent la planification du jour de semaine correspondant.

Exemple :

Configuration précédente :

Planification de jour de semaine configurée pour être active de 9:00 à 10:00

Planification de jour d'exception configurée pour être active de 10:00 à 11:00

Résultat : activité de 10:00 à 11:00

Ce comportement est le même pour les jours fériés.

Vous pouvez ajouter des jours fériés et des Jours d'Exception à une Planification d'Enregistrement ou à une Planification des Tâches.

Les Planifications d'Enregistrement partagent les mêmes jours fériés et jours d'exception. Chaque Planification des Tâches standard présente ses propres schémas de jours fériés et de jours d'exception.

Pour ajouter des jours fériés et des jours d'exception à une planification :

1. Dans l'arborescence **Planifications d'Enregistrement** ou **Planifications de Tâches**, sélectionnez une planification.
2. Cliquez sur l'onglet **Jours fériés**.

3. Cliquez sur **Ajouter**.
La boîte de dialogue **Ajouter jour(s) férié(s)** s'affiche.
4. Sélectionnez un ou plusieurs jours fériés, puis cliquez sur **OK**.
Les jours fériés sélectionnés sont ajoutés au Tableau de Planification.
5. Faites glisser le pointeur pour sélectionner la période appropriée (impossible pour les Planifications d'enregistrement).
Les cellules sélectionnées sont effacées et inversement.
6. Cliquez sur l'onglet **Jours d'exception**.
7. Cliquez sur **Ajouter**.
La boîte de dialogue **Ajouter Jour(s) d'Exception** s'affiche.
8. Sélectionnez un ou plusieurs jours spéciaux, puis cliquez sur **OK**.
Les jours d'exception sélectionnés sont ajoutés au Tableau de planification.
9. Faites glisser le pointeur pour sélectionner la période appropriée (impossible pour les Planifications d'enregistrement).
Les cellules sélectionnées sont effacées et inversement.
Les jours fériés et les jours d'exception ajoutés sont classés par ordre chronologique.

Remarques :

- vous pouvez repérer une période d'un jour férié ou d'un jour d'exception d'une Planification d'Enregistrement dans la couleur d'une autre Planification d'Enregistrement.

Se reporter à

- *Page Planifications d'Enregistrement, page 288*
- *Page Planifications de Tâches, page 289*

20.7

Suppression de jours fériés et de jours d'exception

Fenêtre principale > **Planifications**

Vous pouvez supprimer des jours fériés et des Jours d'Exception d'une Planification d'Enregistrement ou d'une Planification des Tâches.

Pour supprimer des jours fériés et des jours d'exception d'une Planification des Tâches :

1. Dans l'arborescence **Planifications d'Enregistrement** ou **Planifications de Tâches**, sélectionnez une planification.
2. Cliquez sur l'onglet **Jours fériés**.
3. Cliquez sur **Supprimer**.
La boîte de dialogue **Sélectionner les jours fériés à supprimer** s'affiche.
4. Sélectionnez un ou plusieurs jours fériés, puis cliquez sur **OK**.
Les jours fériés sélectionnés sont retirés du Tableau de Planification.
5. Cliquez sur l'onglet **Jours d'exception**.
6. Cliquez sur **Supprimer**.
La boîte de dialogue **Sélectionnez les Jours d'Exception à supprimer** s'affiche.
7. Sélectionnez un ou plusieurs jours spéciaux, puis cliquez sur **OK**.
Les jours d'exception sélectionnés sont retirés du Tableau de planification.

Se reporter à


- *Page Planifications d'Enregistrement, page 288*
- *Page Planifications de Tâches, page 289*

20.8

Modification du nom d'une planification

Fenêtre principale >

Pour renommer une planification :

1. Dans l'arborescence **Planifications d'Enregistrement** ou **Planifications de Tâches**, sélectionnez un élément.
2. Cliquez sur  .
3. Saisissez le nouveau nom, puis appuyez sur ENTRÉE. L'entrée change de nom.

Se reporter à

- *Page Planifications d'Enregistrement, page 288*
- *Page Planifications de Tâches, page 289*

21 Page Caméras et enregistrement



Remarque!

BVMS Viewer offre uniquement des fonctionnalités de base. Les fonctionnalités avancées sont incluses dans BVMS Professional. Pour de plus amples informations sur les différentes éditions BVMS, consultez le site www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Fenêtre principale > Caméras et enregistrement

Affiche la page Tableau des caméras ou Tableau d'enregistrement.

Permet de configurer les propriétés des caméras et les paramètres d'enregistrement.

Permet de filtrer les caméras affichées d'après leur type.

Icônes

	Cliquez sur ce bouton pour copier les paramètres d'enregistrement d'une Planification d'Enregistrement à une autre.
	Cliquez sur ce bouton pour afficher la boîte de dialogue Paramètres de qualité du flux .
	Cliquez sur ce bouton pour afficher la boîte de dialogue Paramètres d'enregistrement planifié .
	Cliquez sur ce bouton pour afficher la boîte de dialogue permettant de configurer une caméra mobile sélectionnée.
	Affiche toutes les caméras disponibles, indépendamment de leur périphérique de stockage.
	Cliquez sur ce bouton pour changer le Tableau des caméras en fonction du périphérique de stockage sélectionné.
	Affiche le Tableau des caméras correspondant. Aucun enregistrement de paramètres n'est disponible, car ces caméras ne sont pas enregistrées dans BVMS.
	Cliquez pour sélectionner les colonnes qui doivent être visibles dans le tableau Caméras .

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.

21.1

Page Caméras

Fenêtre principale > **Caméras et enregistrement** > Cliquez sur une icône pour modifier la


page Caméras en fonction du périphérique de stockage souhaité ; par exemple 

Affiche diverses informations sur les caméras disponibles dans votre BVMS.

Permet de modifier les propriétés suivantes des caméras :

- Nom de la caméra
- Affectation d'une source audio
- Numéro logique
- Commande de balayage horizontal/vertical et de zoom, le cas échéant
- Qualité temps réel (VRM et Temps réel/Stockage local)
- Configuration du profil d'enregistrement
- Durée de stockage minimale et maximale
- Zone d'intérêt (ROI)
- Automated Network Replenishment
- Double enregistrement

Pour personnaliser le tableau Caméras :

1. Cliquez  pour sélectionner les colonnes qui doivent être visibles dans le tableau **Caméras**.
2. Cliquez sur le titre d'une colonne pour trier le tableau en conséquence.

Caméra - Encodeur

Affiche le type de périphérique.

Caméra - Caméra

Affiche le nom de la caméra.

Caméra - Adresse réseau

Affiche l'adresse IP de la caméra.

Caméra - Emplacement

Affiche la position de la caméra. Si la caméra n'est pas encore affectée à une arborescence logique, la mention **Emplacement non affecté** apparaît.

Caméra - Famille de périphériques

Affiche le nom de la famille de périphériques de la caméra sélectionnée.

Caméra - Numéro

Cliquez sur une cellule pour modifier le numéro logique attribué automatiquement à la caméra au moment de sa détection. Si vous indiquez un numéro déjà utilisé, un message d'erreur s'affiche.

Le numéro logique se libère de nouveau une fois la caméra supprimée.

Son

Cliquez sur une cellule pour affecter une source audio à la caméra.

Si une alarme de faible priorité se produit sur une caméra dont le son est configuré, le signal audio est lu même lorsqu'une alarme de priorité plus élevée est déjà affichée (à condition que le son de cette alarme ne soit pas configuré).

Liaison Son entre les caméras

La liaison audio permet à un configurateur d'affecter à une caméra l'entrée et la sortie audio d'une autre caméra.

Cette fonctionnalité est avantageuse dans des scénarios tels que l'attribution de l'entrée et de la sortie audio d'une autre caméra à une caméra qui ne dispose pas de microphone ni de haut-parleur. Cela permet aux opérateurs de communiquer avec des personnes à proximité de l'une ou l'autre des caméras tout en visualisant le flux en direct de n'importe quelle caméra.

Le menu déroulant **Son** contient plusieurs options de liaison audio entre les dispositifs. Le menu présente les options dans l'ordre suivant :

1. Aucun **Son**
2. Audio pour certains dispositifs
3. Audio provenant de dispositifs situés au même emplacement dans l'arborescence de dispositifs
4. Audio de tous les autres dispositifs disponibles

Flux / Limites de flux

Cette colonne est en lecture seule et indique les limites de flux de la caméra correspondante.

Remarque : les limites de flux ne sont affichées que pour les caméras CPP13 et CPP14.

Remarque!



Vous ne pouvez pas modifier les limites du flux dans BVMS. Vous pouvez les modifier sur le site Web de l'encodeur ou dans le Configuration Manager. Après avoir modifié les limites de flux sur le site Web ou dans le Configuration Manager, vous devez mettre à jour les fonctions du périphérique dans BVMS. Si vous ne mettez pas à jour les fonctions du périphérique, BVMS écrasera les limites de flux mises à jour avec les anciens paramètres affichés lors de la dernière mise à jour des fonctions du périphérique.

Flux 1 - Codec 1 / Flux 2 - Codec 1

Cliquez sur une cellule pour sélectionner le codec d'encodage du flux souhaité.

Flux 3 - Codec 1

Cliquez sur une cellule pour sélectionner la résolution vidéo souhaitée.

Les valeurs correspondant à la résolution vidéo sont chargées à partir de l'encodeur.

L'affichage de ces valeurs peut prendre un certain temps.

Remarque : seules les caméras CPP13 et CPP14 prennent en charge un troisième flux. Cette colonne s'affiche uniquement si au moins une caméra configurée prend en charge un troisième flux.

Flux 1 - Qualité / Flux 2 - Qualité / Flux 3 - Qualité

Sélectionnez le niveau de qualité souhaité pour le flux utilisé pour l'affichage en temps réel ou pour l'enregistrement. Vous pouvez configurer les paramètres de qualité dans la boîte de dialogue **Paramètres de qualité du flux**.

Flux 1 - Plate-forme active / Flux 2 - Plate-forme active / Flux 3 - Plate-forme active

Affiche le nom des paramètres de la plate-forme dans la boîte de dialogue **Paramètres de qualité du flux**. Cette colonne est en lecture seule et indique les paramètres du profil devant être consignés sur encodeur.

Remarque!



Vous pouvez utiliser le troisième flux uniquement pour l'affichage en temps réel. L'enregistrement est impossible.

Vidéo en temps réel - Flux (uniquement VRM et Temps réel uniquement/Stockage local)

Cliquez sur une cellule pour sélectionner un flux pour un VRM ou un encodeur temps réel uniquement / à stockage local.

Vidéo en temps réel - Profil (disponible uniquement pour les caméras ONVIF)

Cliquez sur une cellule pour rechercher les jetons de profil en temps réel de cette caméra ONVIF disponibles.

Si vous sélectionnez l'entrée **<Automatique>**, le flux ayant la meilleure qualité est automatiquement utilisé.

Remarque : si vous sélectionnez un dispositif Video Streaming Gateway pour récupérer la vidéo en temps réel sur un poste de travail, le paramètre **Vidéo en temps réel - Profil** est obsolète. Au lieu de cela, le paramètre **Enregistrement - Profil** est également utilisé pour la vidéo en temps réel.

Vidéo en temps réel - ROI

Cliquez pour activer Region of Interest (ROI). Cela n'est possible que si l'élément sélectionné pour le flux 2 dans la colonne **Qualité** est H.264 MP SD ROI ou H.265 MP SD ROI et que le flux 2 est affecté à la vidéo en temps réel.

Remarque : Si le flux 1 est utilisé pour le fonctionnement en temps réel pour un poste de commande spécifique, l'Operator Client en cours d'exécution sur ce poste de commande active la fonction ROI pour cette caméra.



est automatiquement activé dans le tableau .

Enregistrement - Paramètre

Cliquez sur une cellule pour sélectionner le paramètre d'enregistrement requis. Vous pouvez configurer les paramètres d'enregistrement disponibles dans la boîte de dialogue

Paramètres d'enregistrement planifié.**Enregistrement - Profil (disponible uniquement pour les caméras ONVIF)**

Cliquez sur une cellule pour rechercher les jetons de profil d'enregistrement de cette caméra ONVIF disponibles. Sélectionnez l'entrée de votre choix.

Enregistrement - ANR

Cochez une case pour activer la fonction ANR. Vous ne pouvez activer cette fonction que si l'encodeur dispose d'une version de firmware et d'un type de périphérique appropriés.

Enregistrement - Durée de pré-alarme maximale

Affiche la durée de pré-alarme maximale calculée pour cette caméra. Cette valeur vous permet de calculer les besoins en capacité de stockage du support de stockage local.

**Remarque!**

Si un VRM redondant est déjà configuré pour un encodeur, vous ne pouvez modifier aucun paramètre de cet encodeur dans les colonnes **Enregistrement secondaire**.

Enregistrement secondaire - Paramètre (disponible uniquement si un VRM secondaire est configuré)

Cliquez sur une cellule pour affecter un paramètre d'enregistrement planifié à l'enregistrement double de cet encodeur.

En fonction de votre configuration, il peut arriver que la qualité de flux configurée pour l'enregistrement secondaire ne soit pas valide. Dans ce cas, la qualité de flux configurée pour l'enregistrement principal est utilisée à la place.

Enregistrement secondaire - Profil (disponible uniquement pour les caméras ONVIF)

Cliquez sur une cellule pour rechercher les jetons de profil d'enregistrement de cette caméra ONVIF disponibles.



(uniquement visible lorsque vous cliquez sur  Tous)

Cochez une case pour activer les commandes de balayage horizontal/vertical et de zoom.

Remarque :

Pour les paramètres de port, reportez-vous à la section COM1.

Port (uniquement visible lorsque vous cliquez sur  Tous)

Cliquez sur une cellule pour indiquer le port série de l'encodeur nécessaire aux commandes de balayage horizontal/vertical et de zoom. Pour une caméra mobile reliée à un système Bosch Allegiant, vous pouvez sélectionner **Allegiant**. Une ligne de jonction n'est pas nécessaire pour ce type de caméra.

Protocole (uniquement visible lorsque vous cliquez sur  Tous)

Cliquez sur une cellule pour sélectionner le protocole nécessaire aux commandes de balayage horizontal/vertical et de zoom.

Adresse de la caméra PTZ (uniquement visible lorsque vous cliquez sur  Tous)

Entrez l'adresse nécessaire aux commandes de balayage horizontal/vertical et de zoom.

Enregistrement - Durée minimale de stockage [jours]**Enregistrement secondaire - Durée minimale de stockage [jours] (uniquement VRM et stockage local)**

Cliquez sur une cellule pour modifier le nombre minimum de jours pendant lesquels les données vidéo de cette caméra doivent être conservées. Les enregistrements pour lesquels cette durée n'a pas encore été dépassée ne sont pas supprimés automatiquement.

Enregistrement - Durée maximale de stockage [jours]**Enregistrement secondaire - Durée maximale de stockage [jours] (uniquement VRM et stockage local)**


Cliquez sur une cellule pour modifier le nombre maximum de jours pendant lesquels les données vidéo de cette caméra doivent être conservées. Seuls les enregistrements pour lesquels cette durée a été dépassée sont supprimés automatiquement. 0 = illimité.

Se reporter à

- Configuration de l'enregistrement double dans le Tableau des caméras, page 314
- Configuration de positions prédéfinies et de commandes auxiliaires, page 311
- Configuration des paramètres de port PTZ, page 311
- Configuration des paramètres de qualité du flux, page 304
- Copier et coller une sélection dans les tableaux, page 302
- Configuration de la fonction ANR, page 314
- Exportation du Tableau des caméras, page 303
- Affectation d'un profil ONVIF, page 315
- Configuration de la fonction ROI, page 313

21.2 Pages des paramètres d'enregistrement

Fenêtre principale > **Caméras et enregistrement** >  > Cliquez sur un onglet

Planification d'enregistrement (par exemple )

Permet de configurer les paramètres d'enregistrement.


Pour configurer les Planifications d'Enregistrement affichées, accédez à **Planifications**.

Seules les colonnes n'appartenant pas à un Tableau des caméras sont décrites.

- ▶ Cliquez sur le titre d'une colonne pour trier le tableau en conséquence.


Enregistrement continu

Dans la colonne **Qualité**, cliquez sur une cellule pour désactiver l'enregistrement ou pour sélectionner la qualité du flux 1.

Dans la colonne , cochez une case pour activer le son.


Temps Réel/Enregistrement pré-événement

Dans la colonne **Qualité**, cliquez sur une cellule pour sélectionner la qualité de flux de l'affichage en temps réel (requis pour la lecture instantanée) et du mode d'enregistrement pré-événement (requis pour l'enregistrement de mouvement et d'alarme) du flux 2. Si la double diffusion est active sur cet encodeur, vous pouvez sélectionner le flux 1 pour l'enregistrement en temps réel ou de pré-événement.

Dans la colonne , cochez une case pour activer le son.

Enregistrement de mouvement

Dans la colonne **Qualité**, cliquez sur une cellule pour désactiver l'enregistrement ou pour sélectionner la qualité du flux 1.


Dans la colonne , cliquez sur une cellule pour activer le son.

Dans la colonne **Pré-événement**, cliquez sur une cellule pour sélectionner la durée d'enregistrement (en secondes) avant l'événement de détection de mouvement.

Dans la colonne **Post-événement**, cliquez sur une cellule pour sélectionner la durée d'enregistrement (en secondes) après l'événement de détection de mouvement.

Enregistrement d'alarme

Dans la colonne **Qualité**, cliquez sur une cellule pour sélectionner la qualité du flux 1. Pour activer l'enregistrement d'alarme, configurez une alarme correspondante.

Dans la colonne , cochez une case pour activer le son.

Dans la colonne **Pré-événement**, cliquez sur une cellule pour sélectionner la durée (en secondes) avant l'alarme.

Dans la colonne **Post-événement**, cliquez sur une cellule pour sélectionner la durée (en secondes) après l'alarme.

Se reporter à

- *Copier et coller une sélection dans les tableaux, page 302*

22

Configuration des caméras et des paramètres d'enregistrement



Remarque!

Ce document décrit certaines fonctions non disponibles pour BVMS Viewer.




Pour plus de détails sur les différentes versions BVMS, consultez le site

www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Fenêtre principale > **Caméras et enregistrement**

Ce chapitre explique comment configurer les caméras de BVMS.

Vous pouvez configurer les paramètres d'enregistrement et diverses propriétés des caméras.

- Cliquez sur  pour enregistrer les paramètres.
- Cliquez sur  pour annuler le dernier paramètre.
- Cliquez sur  pour activer la configuration.

Se reporter à

- *Page Caméras, page 297*
- *Boîte de dialogue Paramètres d'enregistrement planifié (uniquement VRM et stockage local), page 308*
- *Boîte de dialogue Paramètres de qualité du flux, page 304*
- *boîte de dialogue des positions prédéfinies et des commandes auxiliaires, page 313*

22.1

Copier et coller une sélection dans les tableaux

Vous pouvez configurer simultanément plusieurs objets dans un tableau de caméras, un tableau de configuration d'événements ou un tableau de configuration d'alarmes.

Vous pouvez copier les valeurs configurables d'une ligne dans d'autres lignes :

- Copie de toutes les valeurs d'une ligne dans d'autres lignes
- Copie d'une seule valeur d'une ligne dans une autre ligne
- Copie de la valeur d'une cellule dans une colonne entière

Pour ce faire, deux méthodes sont à votre disposition :

- Copier la sélection dans le Presse-papiers, puis coller.
- Copier/Coller une sélection

Vous pouvez déterminer les lignes dans lesquelles coller les données :

- Copie de la sélection dans toutes les lignes.
- Copie de la sélection dans des lignes sélectionnées.

Pour copier et coller toutes les valeurs configurables d'une ligne dans une autre :

1. Cliquez avec le bouton droit de la souris sur la ligne contenant les valeurs à copier, puis cliquez sur **Copier ligne**.
2. Cliquez sur le titre de la ligne à modifier.
Pour sélectionner plusieurs lignes, maintenez la touche CTRL enfoncée et pointez sur le titre des autres lignes.
3. Cliquez avec le bouton droit de la souris sur le tableau et cliquez sur **Coller**.
Les valeurs sont copiées.

Pour copier et coller une valeur d'une ligne à une autre :

1. Cliquez avec le bouton droit de la souris sur la ligne contenant les valeurs à copier, puis cliquez sur **Copier ligne**.
2. Cliquez avec le bouton droit de la souris sur la cellule à modifier, pointez sur **Coller la cellule dans** et cliquez sur **Cellule active**.
La valeur est copiée.

Pour copier directement toutes les valeurs configurables :

1. Cliquez sur le titre de la ligne à modifier.
Pour sélectionner plusieurs lignes, maintenez la touche CTRL enfoncée et pointez sur le titre des autres lignes.
2. Cliquez avec le bouton droit de la souris sur la ligne contenant les valeurs souhaitées, pointez sur **Copier la ligne dans** puis cliquez sur **Lignes sélectionnées**.
Les valeurs sont copiées.

Pour copier une valeur directement :

1. Cliquez sur le titre de la ligne à modifier.
Pour sélectionner plusieurs lignes, maintenez la touche CTRL enfoncée et pointez sur le titre des autres lignes.
2. Cliquez avec le bouton droit de la souris sur la cellule contenant la valeur souhaitée, pointez sur **Copier la cellule dans** puis cliquez sur **Sélection dans colonne**.
La valeur est copiée.

Pour copier la valeur d'une cellule dans toutes les autres cellules de la colonne :

- ▶ Cliquez avec le bouton droit de la souris sur la cellule contenant la valeur souhaitée, pointez sur **Copier la cellule dans** puis cliquez sur **Colonne entière**.
La valeur est copiée.

Pour dupliquer une ligne :

- ▶ Cliquez avec le bouton droit de la souris sur la ligne et cliquez sur **Ajouter la ligne dupliquée**.
La ligne dupliquée est insérée juste en dessous, avec un nouveau nom.

Se reporter à

- *Page Caméras, page 297*
- *Boîte de dialogue Paramètres d'enregistrement planifié (uniquement VRM et stockage local), page 308*
- *Page Événements, page 316*
- *Page Alarmes, page 322*

22.2

Exportation du Tableau des caméras

Fenêtre principale > **Caméras et enregistrement**

Or

Fenêtre principale > **Caméras et enregistrement** > Cliquez sur une icône pour modifier la



page Caméras en fonction du périphérique de stockage souhaité ; par exemple

Affiche diverses informations sur les caméras disponibles dans votre BVMS.

Vous pouvez exporter le Tableau des caméras vers un fichier CSV.

Pour exporter :

1. Cliquez n'importe où avec le bouton droit de la souris dans le Tableau des caméras, puis cliquez sur **Exporter la table...**
2. Dans la boîte de dialogue, saisissez un nom de fichier approprié.

3. Cliquez sur **Enregistrer**.
Le Tableau des caméras sélectionné est exporté vers un fichier CSV.


22.3

Configuration des paramètres de qualité du flux

Pour ajouter une entrée dans les paramètres de qualité du flux :

1. Cliquez sur  pour ajouter une nouvelle entrée à la liste.
2. Saisissez un nom.

Pour supprimer une entrée des paramètres de qualité du flux :

- ▶ Sélectionnez une entrée dans la liste, puis cliquez sur  pour la supprimer.
Il est impossible de supprimer les entrées par défaut.

Pour renommer une entrée dans les paramètres de qualité du flux :

1. Sélectionnez une entrée dans la liste.
2. Saisissez un nouveau nom dans le champ **Nom**.
Vous ne pouvez pas renommer les entrées par défaut.
3. Cliquez sur **OK**.

Pour configurer des paramètres de qualité du flux :

1. Sélectionnez une entrée dans la liste.
2. Définissez les paramètres appropriés.



22.3.1


Boîte de dialogue Paramètres de qualité du flux


Fenêtre principale > **Caméras et enregistrement**  >
Permet de configurer les profils de qualité du flux à affecter par la suite aux caméras sur la page **Caméras et enregistrement** ou dans la boîte de dialogue **Paramètres d'enregistrement planifié**.

Une qualité de flux associe les paramètres suivants : résolution vidéo, cadence d'images, bande passante maximale et compression vidéo.

Qualités du flux

 Sélectionnez une qualité de flux prédéfinie, puis cliquez sur  pour ajouter une nouvelle qualité de flux sur la base de la qualité de flux prédéfinie. Lorsque vous

sélectionnez un seul flux et que vous cliquez sur , ce paramètre de qualité de flux est copié en tant que nœud de niveau supérieur sans enfant.

 Cliquez sur ce bouton pour supprimer la qualité de flux sélectionnée. Il est impossible de supprimer les paramètres de qualité de flux.

La liste affiche tous les paramètres de qualité de flux prédéfinie. Il est recommandé d'affecter une qualité de flux portant le même nom que la plate-forme de la caméra.

Les profils disponibles pour les qualités de flux sont les suivants :

Image optimized : Les paramètres sont optimisés pour la qualité d'image. Cela peut charger le réseau.

Bit rate optimized : Les paramètres sont optimisés pour une faible bande passante. Cela peut diminuer la qualité d'image.

Balanced : Les paramètres offrent un compromis entre une qualité d'image optimale et une utilisation de la bande passante optimale.

Les profils suivants des qualités de flux sont disponibles depuis BVMS 9.0 pour prendre en charge la fonctionnalité Intelligent Streaming des caméras Bosch :

Cloud optimized 1/8 FR : Les paramètres sont optimisés pour une faible bande passante et de manière identique pour tous les types de caméras.

PTZ optimized : Les paramètres sont optimisés pour les caméras mobiles.

Image optimized quiet / standard / busy

Bit rate optimized quiet / standard / busy

Balanced quiet / standard / busy

Catégories de types de scènes :

quiet : Les paramètres sont optimisés pour des images avec une faible activité. Scène statique (89 %), scène normale (10 %), scène active (1 %).

standard : Les paramètres sont optimisés pour des images avec un niveau d'activité moyen. Scène statique (54 %), scène normale (35 %), scène active (11 %).

busy : Les paramètres sont optimisés pour des images avec une activité élevée. Scène statique (30 %), scène active (55 %), scène encombrée (15 %).

Les valeurs de pourcentage sont associées à une distribution pendant une journée.

Par défaut, le profil Balanced standard est affecté.

**Remarque!**

Pour chaque combinaison de plate-forme de caméra (CPP3-CPP7.3) et pour chacune des résolutions disponibles, il existe un réglage spécifique pour pouvoir définir les débits corrects pour les caméras.

Le profil doit être sélectionné manuellement avec le type de scène correspondant à la caméra.

**Remarque!**

Si vous installez une mise à jour, les nouveaux profils doivent être sélectionnés manuellement pour être activés. Les anciens profils sont conservés.

Nom

Affiche le nom de la qualité du flux. Vous pouvez changer le nom d'une nouvelle qualité de flux au moment où vous l'ajoutez.

Résolution de vidéo SD

Ce paramètre s'applique uniquement lorsque le codec du flux est défini sur une résolution SD.

Sélectionnez la résolution vidéo souhaitée. Pour une qualité HD, vous pouvez configurer la qualité SD du flux 2.

Remarque : Il n'existe pas d'incidence sur la résolution lorsque le codec est configuré en résolution HD ou UHD (toute résolution supérieure à un codec SD) La résolution d'une caméra HD, par exemple, ne peut pas être réduite à SD avec ce paramètre.

Intervalle de codage d'image

Faites glisser le curseur ou entrez la valeur souhaitée.

Le système vous permet de calculer la valeur correspondante pour IPS.

L'**Intervalle de codage d'image** correspond à la fréquence à laquelle les images sont codées et transmises. Si vous choisissez la valeur 1, toutes les images sont codées. Par exemple, si vous entrez la valeur 4, cela signifie qu'une image sur quatre sera codée et que les trois images suivantes seront ignorées. Cette fonction est particulièrement intéressante pour les faibles bandes passantes. Pour obtenir une qualité vidéo optimale, il est conseillé de choisir une valeur d'autant plus élevée que la bande passante est faible.

Le moteur de codage obtient par exemple 30 images du capteur comme entrée. La sortie requise pour l'affichage en temps direct ou l'enregistrement est de 15 images.

Pour réaliser cet objectif :

- ▶ Réglez l'**Intervalle de codage d'image** sur 2.
L'encodeur ignorera un cadre sur deux du capteur et diffusera un flux encodeur H.264 à 15 images uniquement.

Intervalle de codage d'image:

- 1= cadence d'images intégrale comme indiqué dans les paramètres du codec
- 2= 50 % des ips fournies dans les paramètres du codec

Pour calculer rapidement la cadence d'images, la formule est la suivante : $IPS = \text{mode capteur} / \text{intervalle de codage d'images}$

Structure GoP

Sélectionnez la structure dont vous avez besoin pour le groupe d'images ou Group-of-Pictures (GOP). Selon que vous privilégiez les délais les plus faibles (images IP uniquement) ou l'utilisation minimale de la bande passante, vous avez le choix entre IP, IBP et IBBP. (GOP n'est pas un choix disponible sur certaines caméras).

Remarque :

Les B-frames sont uniquement prise en charge par les caméras jusqu'à une résolution de 1 080 p et du firmware 6.40.

Évitez les B-frames en affichage en temps direct et pour les caméras PTZ en raison d'un temps de latence vidéo en temps direct.

Optimisation du débit binaire

L'optimisation du débit binaire se rapporte à la priorité accordée à la réduction de la qualité de l'image ou du débit binaire.

Haute qualité ou **Qualité maximum** fournit une économie de débit binaire inférieure ou nulle, mais une qualité d'image bonne à excellente.

Le **Débit binaire bas** et le débit binaire **Moyen** permettent d'économiser de la bande passante, mais l'image qui en résulte peut fournir moins de détails.

Si l'optimisation du débit binaire est désactivée, un débit binaire moyen de 24 h est attendu (supérieur au débit binaire cible).

Débit cible [kbits/s]

Faites glisser le curseur ou entrez la valeur souhaitée.

Vous pouvez optimiser l'utilisation de la bande passante de votre réseau en limitant le débit de données de l'encoder. Le débit de données cible doit être réglé en fonction de la qualité d'image souhaitée pour des scènes types sans mouvement excessif.

Pour des images complexes ou en cas de changements fréquents du contenu de l'image en raison de mouvements répétés, cette limite peut être momentanément dépassée jusqu'à la valeur indiquée dans le champ **Débit maximal [kbits/s]**.

Débit maximal [kbits/s]

Faites glisser le curseur ou entrez la valeur souhaitée.

Le débit maximum permet de configurer la vitesse de transmission maximale autorisée. Vous pouvez configurer un débit limite pour pouvoir déterminer précisément l'espace disque nécessaire au stockage des données vidéo.

En effet, selon les paramètres de qualité vidéo des images I et P, tout dépassement peut provoquer une instabilité des images individuelles.

La valeur saisie ici doit être supérieure d'au moins 10 % à celle du champ **Débit cible [kbits/s]**. Si la valeur saisie ici est trop basse, elle est automatiquement corrigée.

Intervalle des images I

Ce paramètre sert à définir l'intervalle de codage des I-frames.

La valeur 1 indique que les I-frames sont générées en continu. Avec la valeur 10, une image sur dix seulement est une I-frame et, avec la valeur 60, une image sur soixante. Les I-frames sont codées comme des P-frames.

Remarque : Si vous utilisez un GOP très long (jusqu'à 255), associé à une faible cadence d'images (1 ips), la distance entre les I-frames est trop importante et la lecture ne peut s'afficher. Nous recommandons de réduire la longueur de GOP à 30.

Niveau de qualité d'image

Cette boîte de dialogue permet de définir la valeur 0 ou 100 à la fois pour les images I et les images P. La valeur la plus faible offre la meilleure qualité et le taux d'actualisation d'image le plus faible. La valeur la plus élevée donne le taux d'actualisation d'image le plus élevé et la qualité d'image la plus faible.

Plus la bande passante de transmission disponible est faible, plus il faut augmenter le niveau de qualité pour conserver une bonne qualité vidéo.

Remarque :

Si le support technique ne vous y invite pas, nous vous recommandons vivement de cocher les cases **Automatique**. La relation optimale entre le mouvement et la définition d'image est alors automatiquement ajustée.

Paramètres VIP X1600 XFM4

Permet de configurer les paramètres H.264 suivants pour le module encodeur VIP X 1600 XFM4.

Filtre de déblocage H.264 : Sélectionnez cette option pour améliorer la qualité visuelle et les performances de prédiction en lissant les bords vifs.

CABAC : Sélectionnez cette option pour activer une compression hautement efficace. Utilisez une grande quantité de puissance de traitement.

Se reporter à

– *Configuration des paramètres de qualité du flux, page 304*

22.4

Configuration des propriétés d'une caméra

Fenêtre principale > **Caméras et enregistrement** > 

Pour modifier les propriétés d'une caméra :

1. Dans la colonne **Caméra**, cliquez sur une cellule et saisissez le nouveau nom de la caméra.

Ce nom s'affiche à tous les endroits où les caméras sont répertoriées.

2. Effectuez les réglages appropriés dans les autres colonnes.

Pour de plus amples informations sur les différents champs, cliquez ci-dessous sur le lien de la fenêtre concernée.

Se reporter à

– Page *Caméras*, page 297

22.5**Configuration des paramètres d'enregistrement (uniquement VRM et stockage local)**

Fenêtre principale > **Caméras et enregistrement** > 


Vous pouvez configurer les paramètres d'enregistrement de tous les périphériques ajoutés à l'élément Périphériques VRM dans l'Arborescence des Périphériques.

Remarque : pour pouvoir enregistrer, assurez-vous que le VRM ou le stockage local correspondant est correctement configuré.


VRM : **Périphériques** > Développer  > 

Stockage local : >**Périphériques** Développer  > 

Pour ajouter une entrée dans les paramètres d'enregistrement :

1. Cliquez sur  pour ajouter une nouvelle entrée à la liste.
2. Saisissez un nom.



Pour supprimer une entrée dans les paramètres d'enregistrement :

- ▶ Sélectionnez une entrée dans la liste, puis cliquez sur  pour la supprimer.
Il est impossible de supprimer les entrées par défaut.

Pour renommer une entrée dans les paramètres d'enregistrement :

1. Sélectionnez une entrée dans la liste.
2. Saisissez un nouveau nom dans le champ **Nom** :
Vous ne pouvez pas renommer les entrées par défaut.
3. Cliquez sur **OK**.

Pour configurer les paramètres d'enregistrement :

1. Sélectionnez une entrée dans la liste.
2. Définissez les paramètres appropriés, puis cliquez sur **OK**.
3. Cliquez sur  ou sur .
4. Dans la colonne **Enregistrement**, sélectionnez le paramètre d'enregistrement souhaité pour chaque encodeur.

Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Se reporter à

– Boîte de dialogue *Paramètres d'enregistrement planifié (uniquement VRM et stockage local)*, page 308

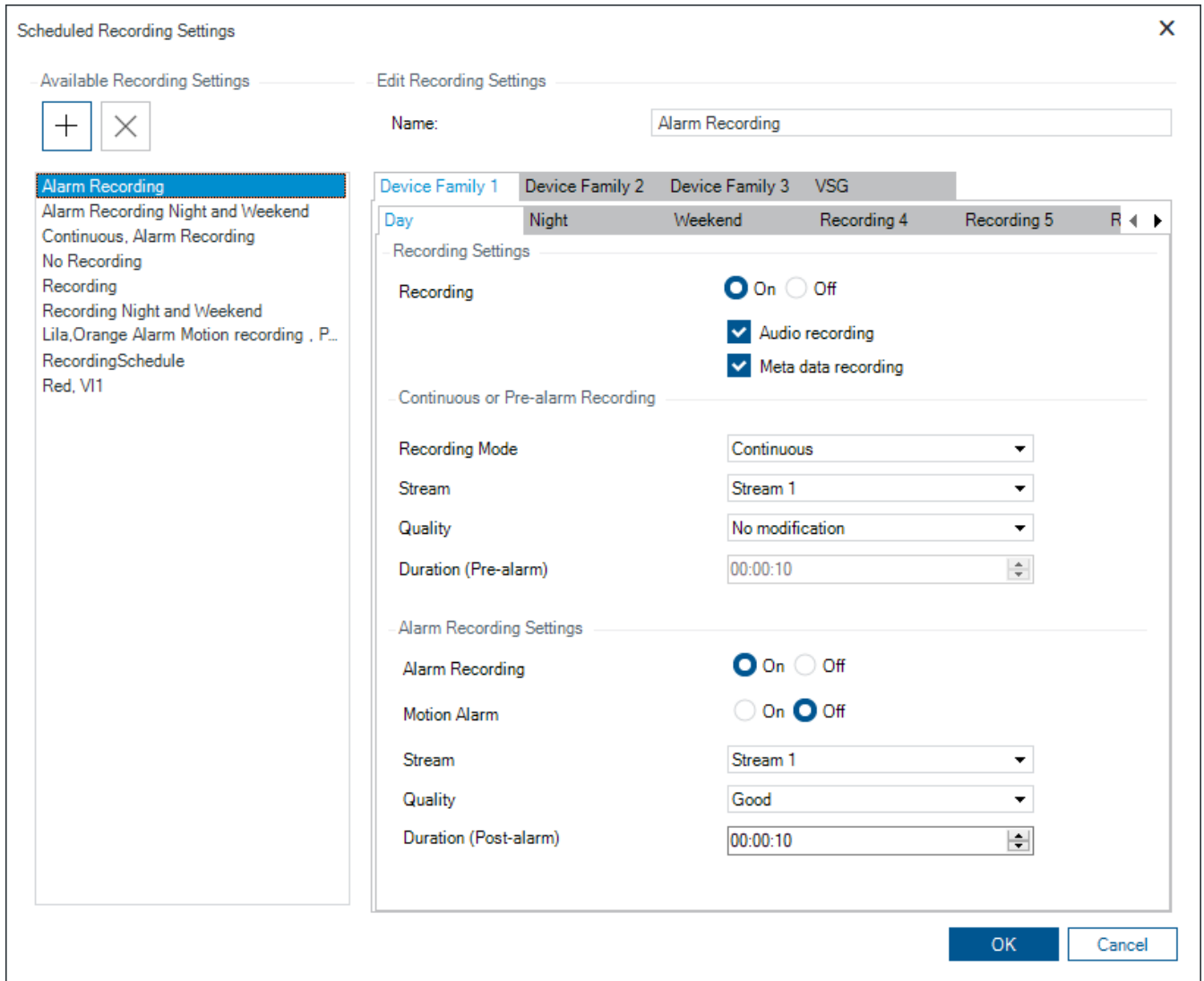
22.6**Boîte de dialogue Paramètres d'enregistrement planifié (uniquement VRM et stockage local)**

Fenêtre principale > **Caméras et enregistrement** > 

Permet de configurer des paramètres d'enregistrement relatifs à une planification pour chaque famille de périphériques disponible. Une famille de périphériques est disponible lorsqu'au moins un encodeur de cette famille de périphériques a été ajouté à l'Arborescence des Périphériques. Dans le tableau **Caméras**, vous pouvez affecter un paramètre d'enregistrement à chaque caméra.

Vous pouvez utiliser les Planifications d'Enregistrement configurées sur la page **Planifications**.

Remarque : lors de l'allumage ou de l'extinction, l'enregistrement normal est valide pour toutes les familles de périphériques.



Paramètres d'enregistrement disponibles

Sélectionnez un paramètre d'enregistrement prédéfini pour en changer les propriétés. Vous pouvez ajouter ou supprimer un paramètre défini par l'utilisateur.

Nom :

Saisissez un nom pour le nouveau paramètre de l'enregistrement.

Onglet Famille de périphériques

Sélectionnez la famille de périphériques de votre choix pour configurer les paramètres d'enregistrement.

Onglet Planification d'Enregistrement

Pour la famille de périphériques choisie, sélectionnez un calendrier d'enregistrements pour configurer les paramètres d'enregistrement.

Enregistrement

Activez ou désactivez l'enregistrement normal (continu et de pré-alarme).

Enregistrement audio

Indiquez si vous voulez effectuer un enregistrement audio.

Enregistrement de métadonnées

Indiquez si vous voulez effectuer un enregistrement de métadonnées.

Mode enregistrement

Sélectionnez le mode d'enregistrement souhaité.

Les éléments suivants sont disponibles :

- **Enregistrement continu**
- **Pré-alarme**

Flux

Sélectionnez le flux souhaité pour l'enregistrement normal.

Remarque : il varie en fonction de la famille de périphériques et de la disponibilité de leur flux.

Qualité

Sélectionnez la qualité de flux souhaitée pour l'enregistrement normal. Les paramètres de qualité disponibles sont configurés dans la boîte de dialogue **Paramètres de qualité du flux**.

Durée (pré-alarme)

Sélectionnez la durée d'enregistrement souhaitée (en secondes) avant l'alarme. Saisissez l'heure indiquée au format hh.mm.ss.

Remarque : activé uniquement lorsque **Pré-alarme** est sélectionné.



Remarque!

Pour les paramètres de pré-alarme entre 1 et 10 s, les pré-alarmes sont automatiquement stockées dans la RAM de l'encodeur si la mémoire RAM disponible est suffisante, sinon sur le support de stockage.

Pour les paramètres de pré-alarme supérieurs à 10 s, les pré-alarmes sont stockées sur le support de stockage.

Le stockage des pré-alarmes sur la mémoire RAM de l'encodeur est uniquement disponible pour la version de firmware 5.0 ou ultérieure.

Paramètres d'enregistrement d'alarme

Permet d'activer ou de désactiver l'enregistrement d'alarme pour cette caméra.

Alarme d'activité

Permet d'activer ou de désactiver l'enregistrement d'alarme déclenché par un mouvement.

Flux

Sélectionnez le flux à utiliser pour l'enregistrement d'alarme.

Remarque : il varie en fonction de la famille de périphériques et de la disponibilité de leur flux.

Qualité

Sélectionnez la qualité de flux souhaitée pour l'enregistrement d'alarme. Les paramètres de qualité disponibles sont configurés dans la boîte de dialogue **Paramètres de qualité du flux**.

Uniquement pour les périphériques appartenant à la famille de périphériques 2 ou 3 : lorsque vous sélectionnez l'entrée **Aucune modification**, l'enregistrement d'alarme utilise la même qualité que pour l'enregistrement continu/de pré-alarme. Nous vous conseillons d'utiliser l'entrée **Aucune modification**. Lorsque vous sélectionnez une qualité de flux pour l'enregistrement d'alarme, seules les valeurs de l'intervalle de codage d'image et le débit cible sont modifiées selon les paramètres dans cette qualité de flux. Les autres paramètres de qualité qui sont utilisés sont configurés dans le paramètre de qualité affecté à l'enregistrement continu/de pré-alarme.

Durée (post-alarme)




Sélectionnez la durée d'enregistrement souhaitée. Saisissez l'heure indiquée au format hh.mm.ss.

Se reporter à

- Copier et coller une sélection dans les tableaux, page 302
- Configuration des paramètres d'enregistrement (uniquement VRM et stockage local), page 308

22.7

Configuration des paramètres de port PTZ

Fenêtre principale > **Périphériques** > Développez  > Développez  >  > onglet **Interfaces** > onglet **Périphériques**

Fenêtre principale > **Périphériques** >  >  > onglet **Interfaces** > onglet **Périphériques**

Pour pouvoir configurer les paramètres de port d'un encodeur, la commande de la caméra de l'encodeur doit être disponible et activée.

Lorsque l'encodeur ou la caméra mobile est échangé, les paramètres port ne sont pas conservés. Vous devez à nouveau les configurer.

Après une mise à jour du firmware, contrôlez les paramètres port.

Pour configurer les paramètres de port d'un encodeur :

- ▶ Définissez les paramètres appropriés.
Les paramètres sont valides immédiatement après la sauvegarde. Vous n'avez pas besoin d'activer la configuration.

Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

22.8

Configuration de positions prédéfinies et de commandes auxiliaires



Fenêtre principale > **Caméras et enregistrement** > 


Vous pouvez prédéfinir et enregistrer des positions de la caméra pour les caméras PTZ, ROI et panoramiques. Pour les caméras PTZ, vous pouvez également définir des commandes auxiliaires.


Remarque : Vous devez d'abord configurer les paramètres de port de votre caméra PTZ avant de pouvoir configurer les autres paramètres correspondants. Dans le cas contraire, la commande PTZ ne fonctionne pas dans cette boîte de dialogue.

Pour configurer une position prédéfinie :

1. Dans le tableau **Caméras**, sélectionnez l'encodeur souhaité.



2. Uniquement pour les caméras PTZ : pour activer la commande d'une caméra PTZ, cochez la case dans la colonne  .
3. Cliquez sur le bouton  .
La boîte de dialogue **Positions prédéfinies et commandes AUX** s'affiche.
4. Vous pouvez définir le nombre de positions prédéfinies que vous souhaitez utiliser.
5. Sélectionnez la position que vous souhaitez définir.
6. Dans la fenêtre de prévisualisation, utilisez la souris pour accéder à la position que vous souhaitez configurer.
Faites défiler pour effectuer un zoom avant et arrière et faites glisser pour déplacer la section d'image.
7. Si nécessaire, saisissez un nom pour la position configurée.

8. Cliquez sur  pour enregistrer la position prédéfinie.

Remarque : Cliquez sur  pour chaque position définie. Sinon, la position n'est pas enregistrée.

9. Cliquez sur **OK**.

Pour afficher les positions prédéfinies déjà configurées :


1. Dans le tableau **Caméras**, sélectionnez l'encodeur souhaité.
2. Cliquez sur le bouton  .
La boîte de dialogue **Positions prédéfinies et commandes AUX** s'affiche.
3. Sélectionnez la position appropriée.
4. Cliquez sur  .
La position de la caméra prédéfinie s'affiche dans la fenêtre de prévisualisation.


Remarque :

Les positions prédéfinies pour les caméras PTZ et ROI sont stockées directement sur la caméra. Les positions prédéfinies pour les caméras panoramiques sont stockées dans BVMS.

Les caméras PTZ se déplacent physiquement vers la position prédéfinie. Les caméras panoramiques et ROI n'affichent qu'une section d'image de la vue complète de la caméra.

Pour configurer des commandes auxiliaires pour les caméras PTZ :

1. Dans le tableau **Caméras**, sélectionnez l'encodeur souhaité.
2. Cliquez sur le bouton  .
La boîte de dialogue **Positions prédéfinies et commandes AUX** s'affiche.
3. Sélectionnez l'onglet **Commandes AUX**.
4. Définissez les paramètres appropriés.

5. Cliquez sur  pour enregistrer les commandes prédéfinies.

Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Se reporter à

- *boîte de dialogue des positions prédéfinies et des commandes auxiliaires, page 313*

- Configuration des paramètres de port PTZ, page 311
- Configuration d'une alarme, page 336
- Boîte de dialogue Sélectionner le contenu du volet des Images, page 324
- Boîte de dialogue Options d'alarmes, page 325
- Boîte de dialogue Sélectionner le contenu du volet des Images (MG), page 325

22.9

boîte de dialogue des positions prédéfinies et des commandes auxiliaires

Fenêtre principale > **Caméras et enregistrement** >  > Sélectionnez une caméra PTZ, ROI



ou panoramique > 

Permet de configurer une caméra PTZ, ROI ou panoramique.

Pour les caméras ROI et panoramiques, aucune commande auxiliaire n'est disponible.

Remarque : Vous devez d'abord configurer les paramètres de port de votre caméra PTZ avant de pouvoir configurer les autres paramètres correspondants. Dans le cas contraire, la commande PTZ ne fonctionne pas dans cette boîte de dialogue.

Icônes

	Cliquez sur ce bouton pour placer la caméra dans la position prédéfinie ou pour exécuter la commande.
	Cliquez sur ce bouton pour enregistrer la position prédéfinie ou la commande.

Onglet Positions prédéfinies

Cliquez sur cet onglet pour afficher le tableau des positions prédéfinies.

Num.

Affiche le numéro de la position prédéfinie.

Nom

Cliquez sur une cellule pour modifier le nom de la position prédéfinie.

Onglet Commandes AUX (uniquement pour les caméras PTZ)

Cliquez sur cet onglet pour afficher le tableau des commandes auxiliaires.

Remarque : Si un encodeur ONVIF prend en charge les commandes auxiliaires, celles-ci sont fournies directement à partir de l'encodeur ONVIF.

Num.

Affiche le numéro de la commande auxiliaire.

Nom

Cliquez sur une cellule pour modifier le nom de la commande.

Code

Cliquez sur une cellule pour modifier le code de la commande.

Se reporter à

- Configuration des paramètres de port PTZ, page 311
- Configuration de positions prédéfinies et de commandes auxiliaires, page 311

22.10

Configuration de la fonction ROI

Fenêtre principale > **Caméras et enregistrement** > 

Vous pouvez activer la fonction ROI d'une caméra HD fixe.

Vous devez configurer le flux 2 pour la vidéo en temps réel et vous devez configurer le CODEC H.264 MP SD ROI ou H.265 MP SD ROI pour le flux 2.

Assurez-vous que le flux 2 est utilisé pour la vidéo en temps réel sur chaque poste de commande où la fonction ROI doit être utilisée.

Pour activer ROI :

1. Dans la colonne **Flux 2 - Codec 1**, sélectionnez le CODEC H.264 MP SD ROI ou H.265 MP SD ROI.
2. Dans la colonne **Vidéo en temps réel - Flux**, sélectionnez **Flux 2**.
3. Dans la colonne **Vidéo en temps réel - ROI**, cliquez pour cocher la case.

Pour désactiver la fonction ROI :

1. Dans la colonne **Vidéo en temps réel - ROI**, cliquez pour décocher la case.
2. Dans la colonne **Flux 2 - Codec 1**, sélectionnez le CODEC souhaité.

Se reporter à

- *Page Caméras, page 297*

22.11

Configuration de la fonction ANR

Fenêtre principale > **Caméras et enregistrement** > 

Avant d'activer la fonction ANR, vous devez ajouter le support de stockage d'un encodeur à l'encodeur souhaité et configurer ce support de stockage.

Pour configurer la fonction ANR, vous devez désactiver l'enregistrement double pour l'encodeur.

La fonction ANR ne peut fonctionner que sur les encodeurs dotés de la version 5.90 (ou ultérieure) du firmware. Tous les types d'encodeurs ne prennent pas en charge ANR même si la version de firmware correcte est installée.

Pour l'activer :

- ▶ Sur la ligne de la caméra souhaitée, dans la colonne **ANR**, cochez la case.

Se reporter à

- *Configuration de l'enregistrement double dans le Tableau des caméras, page 314*
- *Page Caméras, page 297*
- *Configuration du support de stockage d'un encodeur, page 237*

22.12

Configuration de l'enregistrement double dans le Tableau des caméras

Fenêtre principale > **Caméras et enregistrement** > 

Vous devez désactiver la fonction ANR pour configurer l'enregistrement double.

Si vous configurez l'enregistrement double pour une caméra d'un encodeur multivoie, le système s'assure que la même cible d'enregistrement est configurée pour toutes les caméras de cet encodeur.

Pour configurer :

1. Dans la colonne **Enregistrement secondaire - Cible**, cliquez sur une cellule de l'encodeur de votre choix, puis sur la zone de stockage souhaitée d'un VRM secondaire. Toutes les caméras de l'encodeur affecté sont automatiquement configurées pour être enregistrées sur le VRM secondaire sélectionné.
2. Dans la colonne **Paramètre**, sélectionnez le paramètre d'enregistrement souhaité.

Se reporter à

- *Configuration de l'enregistrement double dans l'Arborescence des périphériques, page 194*
- *Configuration de la fonction ANR, page 314*
- *Enregistrement double/de basculement, page 29*
- *Page Caméras, page 297*

22.13**Gestion de Video Streaming Gateway****Se reporter à**

- *Page du dispositif Video Streaming Gateway, page 205*
- *Boîte de dialogue Ajouter un encodeur Bosch, page 208*
- *Boîte de dialogue Ajouter un encodeur ONVIF, page 209*
- *Boîte de dialogue Ajouter une caméra JPEG, page 211*
- *Boîte de dialogue Ajouter un encodeur RTSP, page 212*

22.13.1**Affectation d'un profil ONVIF**

Fenêtre principale > **Caméras et enregistrement** >

Vous pouvez affecter un jeton de profil de support ONVIF à une caméra ONVIF. Ce peut être pour la vidéo en temps réel ou pour l'enregistrement.

Pour affecter un jeton de vidéo en temps réel :

- ▶ Dans la colonne **Vidéo en temps réel - Profil**, sélectionnez l'entrée souhaitée.

Pour affecter un jeton d'enregistrement :

- ▶ Dans la colonne **Enregistrement - Profil**, sélectionnez l'entrée souhaitée.

Se reporter à



- *Page Caméras, page 297*


23 Page Événements

Fenêtre principale > **Événements**

Affiche l'Arborescence des événements avec tous les événements disponibles, ainsi qu'un Tableau de configuration des événements pour chaque événement. Les événements sont organisés par type. Par exemple, les événements d'enregistrement de caméra, tels que les enregistrements continus ou d'alarme, figurent tous sous Mode enregistrement.


Les événements disponibles sont placés en regard des dispositifs correspondants. Un

changement d'état d'un dispositif est indiqué après  par le symbole . Les autres

événements s'affichent dans des groupes classés par dispositifs, avec le symbole .

Vous pouvez configurer les opérations suivantes pour chaque événement :

- Déclenchement d'une alarme en fonction d'une planification (opération impossible pour certains événements).
- Consignation de l'événement en fonction d'une planification. Les événements consignés s'affichent dans la Liste d'Événements de Operator Client.
- Exécution d'un Script de commande en fonction d'une planification (opération impossible pour certains événements).

- Pour les événements de type  : ajout de données texte à l'enregistrement.

Si l'événement se produit, vos paramètres sont exécutés.

Vous pouvez créer un Événement Combiné qui associe plusieurs événements au moyen d'expressions booléennes.

- ▶ Cliquez sur un élément de l'arborescence pour afficher le Tableau de Configuration des Événements correspondant.



Cliquez sur ce bouton pour dupliquer un événement. Utilisez ce bouton pour générer plusieurs alarmes pour un événement particulier.



Cliquez sur ce bouton pour supprimer un Événement Combiné ou dupliqué.



Cliquez sur ce bouton pour renommer l'Événement Combiné sélectionné.



Cliquez sur ce bouton pour afficher une boîte de dialogue permettant de créer des Événements Combinés à l'aide d'expressions booléennes. Les Événements Combinés peuvent inclure 10 événements maximum.

Les Événements Combinés sont ajoutés au Tableau de Configuration des Événements.



Cliquez sur ce bouton pour modifier l'Événement Combiné sélectionné.



Cliquez sur ce bouton pour afficher une boîte de dialogue permettant de créer et de modifier des Scripts de Commande.

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.

Se reporter à

- *Configuration des événements et des alarmes, page 331*
- *Configuration de Scripts de Commande, page 90*
- *Boîte de dialogue Options (menu Paramètres), page 122*
- *Configuration de zones réactives clignotantes, page 339*

23.1

Onglet Paramètres de réponse

Remarque : en raison de restrictions d'ordre technique, l'onglet Debounce Settings (Paramètres de réponse) n'est pas disponible pour certains événements. Permet de configurer les paramètres de réponse de l'événement sélectionné.

Temps de réponse

Pendant la période indiquée, tous les événements ultérieurs sont ignorés.

Priorité de l'état de l'événement

Pour un état d'événement, vous pouvez affecter un paramètre de priorité.

Modifier les priorités

Cliquez sur ce bouton pour afficher une boîte de dialogue permettant de configurer un paramètre de priorité.

Ajouter un paramètre

Cliquez sur ce bouton pour ajouter une ligne et configurer un paramètre de réponse issu des paramètres de réponse de tous les périphériques.


Supprimer le paramètre


Cliquez sur ce bouton pour supprimer une ligne sélectionnée. Pour sélectionner une ligne, cliquez sur le titre de colonne de gauche.

23.2



Onglet Paramètres pour l'affichage de carte avancé

La configuration des états de couleur sur les cartes n'est possible que lorsque vous cliquez pour sélectionner l'option **Affichage d'état avancé activé (coloration des points chauds sur les cartes en fonction de l'état)** ou l'option **Affichage d'état avancé activé (coloration des points chauds sur les cartes en fonction de l'alarme)** dans la boîte de dialogue **Options**.

Pour chaque événement ou alarme  , vous pouvez configurer la couleur d'arrière-plan et le comportement (avec ou sans clignotement) pour les zones réactives. Par exemple, vous

pouvez configurer pour un événement ou une alarme  d'un dispositif le clignotement de son icône de dispositif sur une carte lorsque l'état de ce dispositif change.

En outre, vous pouvez configurer la priorité d'affichage pour toutes les zones réactives. Cette opération est obligatoire lorsque différents événements se produisent pour le même dispositif. (1 = niveau de priorité le plus élevé)

La couleur configurée est valide pour toutes les zones réactives avec la même priorité d'affichage. Vous pouvez modifier la couleur, le comportement et la priorité de n'importe quel événement ou alarme  : la couleur modifiée et le comportement sont utilisés pour toutes les zones réactives de tous les autres événements ou alarmes  qui ont la même priorité.

Activer sur cartes couleur états

Cliquez sur cette option pour permettre que les zones réactives des dispositifs appartenant à cet événement s'affichent avec un arrière-plan coloré et qu'elles puissent clignoter sur les cartes.

Afficher priorité sur carte :

Cliquez sur les flèches pour modifier la priorité des zones réactives des dispositifs appartenant à cet événement.

Couleur arrière-pl sur carte :

Cliquez sur le champ de couleur afin de choisir la couleur d'arrière-plan utilisée pour les zones réactives des dispositifs appartenant à cet événement.

Remarque : Tous les événements d'état de tous les dispositifs de même priorité ont la même couleur.

Clignotant

Cliquez sur cette option pour permettre le clignotement des zones réactives des dispositifs appartenant à cet événement.

23.3

Onglet Paramètres pour la configuration des événements

Périphérique

Affiche le nom du périphérique ou de la planification.

Réseau

Affiche l'adresse IP du périphérique IP correspondant.

Déclencher l'alarme

Cliquez sur une cellule pour sélectionner une Planification d'Enregistrement ou une Planification des Tâches afin de déclencher une alarme.

Sélectionnez **Toujours** pour que l'alarme se déclenche indépendamment de l'instant précis. Sélectionnez **Jamais** pour que l'alarme ne se déclenche pas.

Fichier

Dans la colonne **Planification**, cliquez sur une cellule pour sélectionner la Planification d'Enregistrement ou la Planification des Tâches à consigner.

Sélectionnez **Toujours** pour que l'événement soit consigné indépendamment de l'instant précis.

Sélectionnez **Jamais** pour que l'événement ne soit pas consigné.

Script

Dans la colonne **Script**, cliquez sur une cellule pour sélectionner un Script de Commande.

Dans la colonne **Planification**, cliquez sur une cellule pour sélectionner la Planification d'Enregistrement ou la Planification des Tâches à utiliser pour exécuter un Script de Commande.

Sélectionnez **Toujours** pour que le Script de Commande soit exécuté indépendamment de l'instant précis.


Sélectionnez **Jamais** pour que le Script de Commande ne soit pas exécuté.

Enregistrement de données de texte

Vous pouvez configurer l'ajout de données texte à l'enregistrement continu d'une caméra.

Remarque : cette colonne est disponible uniquement pour les événements qui contiennent des données texte. Par exemple : **Périphériques ATM/POS-Bridge > Entrée ATM > Entrée de données**

23.4 Boîte de dialogue Éditeur de Script de Commande

Fenêtre principale > **Événements** > 

Permet de créer et de modifier des Scripts de Commande.



Cliquez sur ce bouton pour enregistrer les paramètres modifiés.



Cliquez sur ce bouton pour rétablir les paramètres enregistrés.



Cliquez sur ce bouton pour vérifier le code d'un script.



Cliquez sur ce bouton pour créer un fichier de script.



Cliquez sur ce bouton pour supprimer un fichier de script.



Cliquez sur ce bouton pour afficher une boîte de dialogue permettant d'importer un fichier de script.



Cliquez sur ce bouton pour afficher une boîte de dialogue permettant d'exporter un fichier de script.



Cliquez pour convertir un script dans l'autre langage de script disponible. Tout le texte de script existant est supprimé.



Cliquez sur ce bouton pour afficher l'aide en ligne du script de l'interface API de BVMS.



Cliquez sur ce bouton pour afficher l'aide en ligne de BVMS.



Cliquez sur ce bouton pour fermer la boîte de dialogue **Éditeur de Script de Commande**.

Se reporter à

– *Configuration de Scripts de Commande, page 90*

23.5 Créer un Événement Combiné / Boîte de dialogue Modifier l'Événement Combiné

Fenêtre principale > **Événements** > 

Permet de créer ou de modifier un Événement Combiné.

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.

Nom de l'événement :

Saisissez le nom de l'Événement Combiné.

États d'événement :

Sélectionnez le changement d'état à inclure dans un Événement Combiné.

Objets :

Sélectionnez un ou plusieurs objets disponibles de l'état d'événement sélectionné. Cet état et l'objet sélectionné s'affichent dans l'arborescence des événements combinés, comme enfant immédiat de l'opérateur racine.

Événement combiné:


Vous pouvez générer les événements combinés dans l'arborescence des événements combinés. Tous les enfants immédiats d'un opérateur booléen (AND, OR) sont combinés par cet opérateur.

Se reporter à

- *Création d'un Événement Combiné, page 334*
- *Modification d'un Événement Combiné, page 335*

23.6

Boîte de dialogue Sélectionner un langage de script

Fenêtre principale > **Événements** > 

Permet de définir le langage de script des Scripts de Commande.

Il est impossible de modifier le langage de script des Scripts de Commande existants.

Langage de script :

Sélectionnez le langage de script approprié.

Se reporter à

- *Configuration de Scripts de Commande, page 90*

23.7

Boîte de dialogue Modifier les priorités du type d'événement

Fenêtre principale > **Événements** > onglet **Paramètres de réponse** > bouton **Modifier les priorités**

Vous pouvez, le cas échéant, configurer les priorités pour les divers changements d'état d'un type d'événement, par exemple entrée virtuelle fermée et entrée virtuelle ouverte. Un changement d'état avec une priorité plus élevée prend le pas sur le temps de réponse d'un autre changement d'état de priorité inférieure.

Nom de la priorité :

Saisissez un nom pour le paramètre de priorité.

Valeur de l'état

Affiche les noms des états de l'événement choisi.

Priorité de l'état

Saisissez la priorité souhaitée. 1 = priorité est la plus élevée, 10 = priorité la plus basse.


23.8 Boîte de dialogue Sélectionner les périphériques

Fenêtre principale > **Événements** >  ou  > Onglet **Paramètres de réponse** > Bouton **Ajouter un paramètre**

Sélectionner

Cochez la case correspondant à l'entrée de votre choix, puis cliquez sur **OK** pour ajouter une ligne dans le tableau **Périphériques avec des paramètres de réponse différents**.

23.9 Boîte de dialogue Enregistrement de données texte

Fenêtre principale > **Événements** > Dans l'arborescence des événements, sélectionnez  **Entrée de données** (des données texte doivent être disponibles, par exemple : **Lecteurs de carte foyer** > **Lecteur de carte foyer** > **Carte refusée**) > Colonne **Enregistrement de données de texte** > ...

Vous pouvez configurer les caméras pour lesquelles des données texte sont ajoutées à l'enregistrement continu.

Se reporter à

- *Déclenchement de l'enregistrement d'alarme avec des données texte, page 337*

24 Page Alarmes

Fenêtre principale > **Alarmes**

Affiche l'Arborescence des Événements et un Tableau de Configuration des Alarmes pour chaque événement. Seuls les événements configurés sur la page **Événements** s'affichent. Les tableaux vous permettent de configurer pour chaque événement le mode d'affichage d'une alarme déclenchée par cet événement et les caméras à enregistrer et à afficher lorsque cette alarme se produit.

Certains événements sont configurés en tant qu'alarmes par défaut. C'est notamment le cas des erreurs système.

Il est impossible de configurer une alarme pour les événements suivants :

- Changement du mode d'enregistrement
- Changement d'un état d'alarme
- La majorité des actions utilisateur (sur une caméra mobile, par exemple)



Cliquez sur ce bouton pour afficher la boîte de dialogue **Gestionnaire de ressources**.



Affiche une boîte de dialogue permettant de définir les paramètres d'alarme valide pour ce Management Server.

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.

- ▶ Cliquez sur un élément de l'arborescence pour afficher le Tableau de Configuration des Alarmes correspondant.

Périphérique

Affiche le périphérique associé à l'événement sélectionné dans l'Arborescence des Événements.

Adresse réseau

Affiche l'adresse IP du périphérique IP correspondant.

Identité de l'alarme

Dans la colonne **Priorité**, cliquez sur une cellule pour entrer le niveau de priorité de l'alarme sélectionnée (**100** étant un niveau faible et **1** un niveau élevé). Dans la colonne **Titre**, cliquez dans une cellule pour saisir le titre de l'alarme à afficher dans BVMS, par exemple dans la Liste des Alarmes. Dans la colonne **Couleur**, cliquez dans une cellule pour afficher une boîte de dialogue permettant de sélectionner la couleur dans laquelle afficher l'alarme dans Operator Client, par exemple dans la Liste des Alarmes.

Volets des Images d'Alarme

...Dans l'une des colonnes **1 à 5**, cliquez sur une cellule pour afficher une boîte de dialogue permettant de sélectionner une caméra.

Vous ne pouvez sélectionner qu'une caméra ajoutée à l'arborescence logique dans **Cartes et structure**.

Vous pouvez configurer le nombre de volets des images d'Alarme disponibles dans la boîte de dialogue **Paramètres de l'alarme**.

Dans la colonne **Fichier audio**, cliquez sur ... dans une cellule pour afficher une boîte de dialogue permettant de sélectionner un fichier audio à lire en cas d'alarme.

Options d'alarmes


Cliquez sur ... dans une cellule pour afficher la boîte de dialogue **Options d'alarmes**.

Se reporter à

– *Gestion des alarmes, page 39*

24.1

Boîte de dialogue Paramètres d'alarme

Fenêtre principale > **Alarmes** > 

Onglet Paramètres de l'alarme

Nombre max. de volets des images par alarme :

Entrez le nombre maximum de volets des images d'alarme à afficher en cas d'alarme.

Remarque : Si vous utilisez un Enterprise System, le décompte maximum le plus élevé est configuré sur les Management Servers en ligne s'applique.

Durée de l'effacement automatique :

Entrez la durée en secondes après laquelle une alarme doit s'effacer automatiquement.

Ce paramètre ne s'applique qu'aux alarmes définies sur **Effac. auto. alarme après durée config. (boîte de dialogue « Paramètres de l'alarme »)** dans la page **Alarmes**.

Affichage alarme plusieurs lignes dans fenêtre image alarme

Cochez cette case pour autoriser l'affichage d'alarme sur plusieurs lignes de la fenêtre d'image d'alarme.



Remarque!

Pour les configurations d'alarme existantes, l'affichage d'alarme sur plusieurs lignes est activé ; pour les nouvelles configurations d'alarme, la valeur par défaut est désactivée et le mode affichage simple est actif.

Définir la limite de durée pour les enregistrements d'alarme déclenchée par un état :

Cochez cette case pour activer une durée maximale pour les enregistrements d'alarme déclenchée par un état. Saisissez le nombre de minutes correspondant à la durée de l'enregistrement d'alarme. L'enregistrement s'arrête automatiquement à la fin du temps défini.

L'utilisateur peut entrer une durée comprise entre 1 et 1 440 minutes.

Lorsqu'une alarme déclenche un enregistrement avec une durée maximale configurée :

- Si l'alarme est redéclenchée avant la fin du délai imparti, l'enregistrement continue et le délai redémarre à 0.
- Si l'alarme est annulée avant la fin du délai imparti, l'enregistrement continue jusqu'à la fin de la durée post-alarme configurée.

Onglet Groupes de moniteurs

Ordre affichage si priorité alarme identique

Sélectionnez l'entrée de votre choix pour le tri d'alarmes du même niveau de priorité en fonction de leur horodatage.

Afficher un écran vierge

Cliquez sur ce bouton pour que les moniteurs non utilisés pour l'affichage des alarmes n'affichent rien.



Affichage en temps réel continu

Cliquez sur ce bouton pour qu'un affichage en temps réel apparaisse sur les moniteurs non utilisés pour l'affichage des alarmes.

Se reporter à

– *Configuration de paramètres pour toutes les alarmes, page 336*

24.2**Boîte de dialogue Sélectionner le contenu du volet des Images**

Fenêtre principale > **Alarmes** >  ou  > colonne **Volets des images d'alarme** > Cliquez sur ... dans l'une des colonnes **1-5**

Permet de sélectionner un élément de l'Arborescence Logique qui est affiché et enregistré (si l'élément est une caméra) dans le cas de l'alarme sélectionnée.

**Remarque!**

Une carte de site affichée dans un volet des images d'alarme est optimisée pour l'affichage ; elle contient uniquement la vue initiale du fichier de carte d'origine.

Rechercher l'élément

Saisissez du texte pour rechercher un élément dans l'arborescence logique.

Rechercher

Cliquez sur ce bouton pour rechercher les caméras dont la description inclut le texte saisi.

Temps réel

Cliquez sur ce bouton pour que l'image en temps réel de la caméra s'affiche en cas d'alarme.

Lecture instantanée

Cliquez sur ce bouton pour que la lecture instantanée de la caméra s'affiche.

Vous pouvez configurer la durée de rembobinage pour la lecture instantanée d'alarme sur la page **Fonctions de l'opérateur**, voir *Page des fonctionnalités d'Operator, page 350*.

Pauser la lecture

Cochez cette case pour afficher la caméra d'alarme à lecture instantanée avec lecture instantanée interrompue. L'utilisateur peut lancer la lecture instantanée si nécessaire.

Lecture en boucle

Cochez cette case pour afficher la caméra d'alarme à lecture instantanée avec lecture instantanée en boucle.

La durée de la lecture instantanée en boucle dans le volet des images d'alarme correspond au temps de rembobinage plus la durée de l'alarme plus les durées de rembobinage.

Enregistrer cette caméra

Cochez une case pour activer l'enregistrement de cette caméra en cas d'alarme. Si une alarme se déclenche, les images de cette caméra sont enregistrées en qualité Alarme. La durée de l'enregistrement correspond à la durée de l'alarme plus les durées pré- et post-alarme. Ce paramètre modifie directement les paramètres d'enregistrement sur alarme dans la boîte de dialogue **Options d'alarmes** et inversement.

Remarque : Si une position prédéfinie est sélectionnée pour une caméra panoramique, non seulement cette section d'image est stockée, mais également la vue en cercle complète.

Position prédéfinie panoramique

Si vous avez sélectionné une caméra panoramique, vous pouvez sélectionner une position de caméra prédéfinie. Lorsqu'un utilisateur d'Operator Client accepte cette alarme, l'image d'alarme s'affiche dans la position prédéfinie dans la vue recadrée.

Si **<aucun>** est sélectionné, l'image d'alarme s'affiche dans la vue panoramique.

Se reporter à

- Page des fonctionnalités d'Operator, page 350
- Configuration d'une alarme, page 336

24.3

Boîte de dialogue Sélectionner le contenu du volet des Images (MG)

Fenêtre principale >

Alarmes > Colonne  ou  > **Options d'alarmes** > Cliquez sur ... > Boîte de dialogue **Options d'alarmes** > Onglet **Groupe de moniteurs** > Cliquez sur ... dans l'une des colonnes 1 à 10

Permet de sélectionner une caméra dans l'arborescence logique. Cette caméra sera affichée sur le moniteur affecté au cas en cas de déclenchement de l'alarme sélectionnée.

Rechercher l'élément

Saisissez du texte pour rechercher un élément dans l'arborescence logique.

Rechercher

Cliquez sur ce bouton pour rechercher les caméras dont la description inclut le texte saisi.

Position prédéfinie panoramique

Si vous avez sélectionné une caméra panoramique, vous pouvez sélectionner une position de caméra prédéfinie. Lorsqu'un utilisateur d'Operator Client accepte cette alarme, l'image d'alarme s'affiche dans la position prédéfinie dans la vue recadrée.

Si vous sélectionnez **<aucun>**, le décodeur affiche l'image d'alarme dans la vue en cercle.

Aucune caméra

Cliquez pour effacer une caméra de la colonne de groupe de moniteurs.

Remarque :

Le champ de vision d'une position de caméra panoramique prédéfinie diffère entre Operator Client ou Configuration Client et le décodeur.





Remarque!

Pour utiliser des positions prédéfinies pour les caméras panoramiques, la **Position de montage** de la caméra panoramique doit être **Mur** ou **Plafond**.

24.4

Boîte de dialogue Options d'alarmes

Fenêtre principale > **Alarmes** >  ou  > colonne **Options d'alarmes** > ...
Permet de configurer les paramètres suivants pour les alarmes :

- Caméras dont il faut démarrer l'enregistrement en cas d'alarme.
- Activation de la protection de ces enregistrements d'alarme.
- Activation et configuration de paramètres de durées d'alarme différentes.
- Déclenchement de commandes de balayage horizontal/vertical et de zoom en cas d'alarme.
- Notifications à envoyer en cas d'alarme.
- Flux de travail à suivre en cas d'alarme.
- Affectation des caméras affichées dans les groupes de moniteurs en cas d'alarme.

Onglet Caméras

Num.	Affiche le numéro de la caméra tel qu'il est configuré sur la page Caméras et enregistrement .
Nom	Affiche le nom de la caméra tel qu'il est configuré sur la page Caméras et enregistrement .
Emplacement	Affiche l'emplacement tel qu'il est configuré sur la page Cartes et structure .
Enregistrer	Cochez une case pour activer l'enregistrement de cette caméra en cas d'alarme. Si une alarme se déclenche, les images de cette caméra sont enregistrées en qualité Alarme. La durée de l'enregistrement correspond à la durée de l'alarme plus les durées pré- et post-alarme. Ce paramètre modifie directement les paramètres d'enregistrement sur alarme dans la boîte de dialogue Sélectionner le contenu du volet Image et inversement.
Protéger l'enregistrement	Cochez une case pour protéger l'enregistrement d'alarme de cette caméra. Remarque : Le système VRM ne supprimera jamais les données vidéo protégées. Notez que trop de blocs protégés peuvent saturer le stockage et la caméra risque de ne plus enregistrer.
Déviatation des paramètres de durée d'alarme	La case est automatiquement cochée lorsque vous cochez la case Enregistrer et que la caméra prend en charge la fonction ANR.
Commandes AUX	Cliquez sur une cellule pour sélectionner une commande auxiliaire à exécuter en cas d'alarme. Les entrées de cette liste ne sont disponibles que pour les caméras mobiles.
Position prédéfinie	Cliquez sur une cellule pour sélectionner une position prédéfinie à définir en cas d'alarme. Les entrées de cette liste ne sont disponibles que pour les caméras mobiles.

Remarque : Vous ne pouvez pas configurer les deux, **Commandes AUX** et **Position prédéfinie**, pour la même caméra et l'alarme.

Onglet Notifications

E-mail	Cochez cette case pour envoyer un e-mail en cas d'alarme.
Serveur :	Sélectionnez un serveur de messagerie.
Destinataires :	Saisissez les adresses e-mail des destinataires en veillant à les séparer par des virgules (exemple : nom@fournisseur.fr).
Texte :	Saisissez le texte de la notification.
Informations :	Cochez les cases des informations à ajouter au texte de la notification. Remarque : pour un e-mail, la date du fuseau horaire de Management Server est utilisée.

Onglet Flux de travail

Alarme Enregistrement seul	Cochez cette case si vous souhaitez que la caméra soit uniquement enregistrée et non affichée en cas d'alarme. Cette case est active uniquement si la case Enregistrer de l'onglet Caméras est cochée.
Effac. auto. alarme après durée config. (boîte de dialogue « Paramètres de l'alarme »)	Cochez cette case pour que l'alarme s'efface automatiquement.
Effacement automatique de l'alarme quand l'état d'événement revient à l'état normal	Cochez cette case pour que l'alarme s'efface automatiquement quand l'événement qui déclenche cette alarme change d'état. L'alarme ne sera pas automatiquement effacée si elle est acceptée et non acceptée.
Empêcher l'effacement d'alarme tant que l'état de déclenchement perdure	Cochez cette case afin d'éviter que cette alarme soit supprimée tant que la cause de l'alarme est présente.
Supprimer les alarmes en double dans la liste d'alarme	Cochez cette case afin d'éviter la duplication des alarmes pour le même type d'événement et de dispositif dans la liste des alarmes de BVMS Operator Client. Tant qu'une alarme est active (à l'état d'alarme Active ou Acceptée), aucune autre alarme pour le même type d'événement et de dispositif ne s'affiche dans la liste des alarmes. Remarque : <ul style="list-style-type: none"> - Les événements sont toujours enregistrés dans le journal des connexions. - Sachez que toutes les actions Alarme déclenchées par cette alarme (par exemple, le démarrage d'un enregistrement d'alarme, etc.) ne sont pas redéclenchées.

	<p>Après que l'alarme a été effacée et qu'une nouvelle alarme a été déclenchée pour le même dispositif et par le même type d'événement, la nouvelle alarme s'affiche à nouveau dans la liste des alarmes et toutes les actions Alarme définies pour cette alarme sont à nouveau déclenchées.</p> <ul style="list-style-type: none"> - Cette case est présélectionnée pour les alarmes Person Identification.
Afficher le plan d'action	Cochez cette case pour activer le flux de travail à suivre en cas d'alarme.
Ressources...	Cliquez sur ce bouton pour afficher la boîte de dialogue Gestionnaire de ressources . Sélectionnez un document portant la description du flux de travail correspondant.
Afficher une zone de commentaire	Cochez cette case pour activer l'affichage d'une zone de commentaire en cas d'alarme. Cette zone de texte permet à l'utilisateur d'entrer des commentaires sur l'alarme.
Obliger l'opérateur à traiter le flux de travail	Cochez cette case pour obliger l'utilisateur à suivre le flux de travail. Lorsque cette case est cochée, l'utilisateur est obligé d'entrer un commentaire avant d'effacer l'alarme.
Lorsque l'alarme est acceptée, exécutez le script de client suivant :	Sélectionnez un script de commande client exécuté automatiquement dès l'acceptation d'une alarme par l'utilisateur.


Onglet Groupe de moniteurs

1...10	Dans une colonne numérotée, cliquez sur une cellule. La boîte de dialogue Sélectionner le contenu du volet Image s'affiche. Sélectionnez une caméra dans l'arborescence logique. En cas d'alarme, cette caméra sera affichée dans le moniteur à laquelle elle a été affectée. Sélectionnez les positions de la caméra prédéfinies, si elles sont configurées. Pour plus d'informations, consultez la boîte de dialogue d'aide en ligne pour Sélectionner le contenu du volet Image (MG).
Effacer le tableau	Cliquez sur ce bouton pour supprimer toutes les affectations de caméras aux groupes de moniteurs
Affichage à l'écran (OSD) Paramètres	
Titre d'alarme	Cochez cette case pour que le titre de l'alarme soit affiché à l'écran sur les moniteurs.
Durée d'alarme	Cochez cette case pour que l'heure de l'alarme soit affichée à l'écran sur les moniteurs.
Date d'alarme	Cochez cette case pour que la date de l'alarme s'affiche à l'écran sur les moniteurs.

Nom de la caméra d'alarme	Cochez cette case pour que le nom de la caméra d'alarme s'affiche à l'écran sur les moniteurs.
Numéro de caméra d'alarme	Cochez cette case pour que le numéro de la caméra d'alarme s'affiche à l'écran sur les moniteurs.
Sur le 1er moniteur uniquement	Cochez cette case pour que le titre et l'heure de l'alarme soient affichés à l'écran uniquement sur le premier moniteur du groupe de moniteurs.

Onglet Déviation des paramètres de durée d'alarme

Les paramètres affichés sous cet onglet sont disponibles uniquement si la fonction ANR est activée pour cette caméra.

Utiliser les paramètres de profil	Cliquez sur cette option pour activer ce paramètre. Pour cette caméra, les paramètres des durées pré-alarme et post-alarme configurés dans la boîte de dialogue Paramètres d'enregistrement planifié sont utilisés.
Remplacer les paramètres	Cliquez sur ce bouton pour activer les paramètres suivants pour les durées pré-alarme et post-alarme.
Durée (pré-alarme)	Disponible pour tous les événements.
Durée (post-alarme)	Disponible uniquement pour les événements  .

Onglet **Niveau de menace**

Augmentez le niveau de menace à	Sélectionnez le niveau de menace déclenché par cette alarme. Sélectionnez l'entrée Réinitialiser le niveau de menace si cette alarme doit mettre fin à un niveau de menace actif. L'Operator Client se déconnecte ensuite et l'utilisateur peut se reconnecter.
--	--

Se reporter à

- Configuration des décodeurs pour l'affichage à l'écran (OSD), page 241
- Boîte de dialogue Sélectionner le contenu du volet des Images (MG), page 325
- Déclenchement de l'enregistrement d'alarme avec des données texte, page 337
- Configuration d'une alarme, page 336
- Configuration des durées pré-alarme et post-alarme d'une alarme, page 337

24.5

Boîte de dialogue Sélectionner une ressource

Fenêtre principale > **Alarmes** >  ou colonne  > **Identité de l'alarme** > colonne **Fichier audio** > Cliquez sur ...

Permet de sélectionner un fichier audio à lire en cas d'alarme.

Lecture

Cliquez sur ce bouton pour lire le fichier audio sélectionné.

Pause

Cliquez sur ce bouton pour interrompre la lecture du fichier audio sélectionné.

Arrêter

Cliquez sur ce bouton pour arrêter la lecture du fichier audio sélectionné.

Gérer...

Cliquez sur ce bouton pour afficher la boîte de dialogue **Gestionnaire de ressources**.

Se reporter à

- *Configuration d'une alarme, page 336*
- *Gestion des fichiers ressources, page 332*

25 Configuration des événements et des alarmes

Fenêtre principale > **Événements**

ou

Fenêtre principale > **Alarmes**

Ce chapitre explique comment configurer les événements et les alarmes dans le système.

Les événements disponibles sont placés en regard des dispositifs correspondants.

La page **Événements** permet de définir à quel moment un événement de BVMS doit déclencher une alarme, exécuter un Script de Commande ou être consigné.

Exemple (extrait d'un Tableau de Configuration des Événements) :




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>

Explications de l'exemple :

En cas de perte du signal vidéo de la caméra sélectionnée, l'alarme se déclenche, l'événement est consigné et aucun script n'est exécuté.

La page **Alarmes** permet de définir le mode d'affichage d'une alarme, ainsi que les caméras à afficher et à enregistrer en cas d'alarme.

Certains événements système sont configurés par défaut en tant qu'alarmes.

- Cliquez sur  pour enregistrer les paramètres.
- Cliquez sur  pour annuler le dernier paramètre.
- Cliquez sur  pour activer la configuration.

Se reporter à

- Onglet Paramètres de réponse, page 317
- Onglet Paramètres pour l'affichage de carte avancé, page 317
- Onglet Paramètres pour la configuration des événements, page 318
- Boîte de dialogue Éditeur de Script de Commande, page 319
- Créer un Événement Combiné / Boîte de dialogue Modifier l'Événement Combiné, page 319
- Boîte de dialogue Sélectionner un langage de script, page 320
- Boîte de dialogue Modifier les priorités du type d'événement, page 320
- Boîte de dialogue Sélectionner les périphériques, page 321
- Boîte de dialogue Enregistrement de données texte, page 321
- Boîte de dialogue Paramètres d'alarme, page 323
- Boîte de dialogue Sélectionner le contenu du volet des Images, page 324
- Boîte de dialogue Options d'alarmes, page 325

25.1 Copier et coller une sélection dans les tableaux

Vous pouvez configurer en quelques clics plusieurs objets simultanément dans un tableau de caméras, un tableau de configuration d'événements ou un tableau de configuration d'alarmes.

Pour plus d'informations, voir *Copier et coller une sélection dans les tableaux*, page 302.

25.2 Suppression d'une ligne de tableau

Fenêtre principale > **Alarmes**

Vous pouvez uniquement supprimer une ligne que vous ou un autre utilisateur avez ajoutée.


Cela signifie que vous pouvez supprimer les événements dupliqués ou combinés.

Les Événements Combinés sont situés dans l'Arborescence des Événements sous

Périphériques système > Événements Combinés.

Pour supprimer une ligne dans un tableau :

1. Sélectionnez la ligne.

2. Cliquez sur  .

Se reporter à

– *Page Événements*, page 316

25.3 Gestion des fichiers ressources

Pour plus d'informations, voir :

– *Gestion des fichiers ressources*, page 270.

25.4 Configuration d'un événement

Fenêtre principale > **Événements**

Pour configurer un événement :

1. Dans l'arborescence, sélectionnez un événement ou un état d'événement, par exemple **Périphériques système > Authentification > Authentification de l'opérateur rejetée.**

Le tableau de configuration d'événement correspondant s'affiche.

2. Dans la colonne **Déclencher l'alarme- Planification**, cliquez sur une cellule, puis sélectionnez la planification appropriée.

La planification détermine le moment où l'alarme est déclenchée.

Sélectionnez l'une des Planifications d'Enregistrement ou Planifications des Tâches que vous avez configurées dans la page **Planifications**.

3. Dans la colonne **Fichier - Planification**, cliquez sur une cellule, puis sélectionnez la planification qui convient.

La planification détermine le moment où l'événement est consigné.

4. Dans la colonne **Script - Script**, cliquez sur une cellule, puis sélectionnez un Script de Commande.

5. Dans la colonne **Script- Planification**, cliquez sur une cellule, puis sélectionnez la planification appropriée.

La planification détermine le moment où l'événement déclenche le démarrage du script de Commande.

Se reporter à


– *Page Événements*, page 316

25.5 Duplication d'un événement

Fenêtre principale > **Événements**

Vous pouvez dupliquer un événement pour déclencher plusieurs alarmes lorsqu'un événement particulier se produit.

Pour dupliquer un événement :

1. Dans l'arborescence, sélectionnez une condition événementielle. Le Tableau de Configuration des Événements correspondant s'affiche.
2. Sélectionnez une ligne dans le tableau.
3. Cliquez sur . Une nouvelle ligne est ajoutée en dessous de la position actuelle dans le tableau. Elle comporte les paramètres par défaut.

Se reporter à

– Page *Événements*, page 316

25.6 Consignation des événements utilisateur

Fenêtre principale > **Événements** > Développez **Périphériques système** > **Actions utilisateur**

Vous pouvez configurer individuellement le mode de consignation de plusieurs actions utilisateur pour chaque groupe d'utilisateurs disponible.

Exemple :

Pour consigner les événements utilisateur :

1. Sélectionnez un événement utilisateur pour configurer son mode de consignation, par exemple **Connexion de l'opérateur**.
Le Tableau de Configuration des Événements correspondant s'affiche.
Chaque groupe d'utilisateurs figure dans la colonne **Périphérique**.
2. Le cas échéant : dans la colonne **Déclencher l'alarme - Planification**, cliquez sur une cellule, puis sélectionnez la planification appropriée.
La planification détermine le moment de déclenchement de l'alarme devant avertir l'utilisateur de l'événement.
Vous pouvez sélectionner l'une des Planifications d'Enregistrement ou Planifications des Tâches que vous avez configurées dans **Planifications**.
3. Dans la colonne **Fichier - Planification**, cliquez sur une cellule, puis sélectionnez la planification qui convient.
La planification détermine le moment où l'événement est consigné.
Dans l'exemple, l'événement Connexion de l'Opérateur n'est pas consigné pour le groupe administratif ni pour le groupe d'utilisateurs expérimentés. Il l'est en revanche pour le groupe d'utilisateurs en temps réel au cours de la planification **Jour**.

Se reporter à

– Page *Événements*, page 316

25.7 Configuration des boutons d'événement utilisateur

Fenêtre principale > **Événements**

Vous pouvez configurer les boutons d'événement utilisateur disponibles dans le Operator Client. Vous pouvez choisir de ne pas tous les afficher dans le Operator Client.

La page **Groupes d'utilisateurs** permet de configurer les boutons d'événement utilisateur de façon à ce qu'ils soient uniquement disponibles dans le Operator Client du groupe d'utilisateurs correspondant.

Pour configurer des boutons d'événement utilisateur :

1. Dans l'arborescence, sélectionnez **Périphériques système > Boutons événement Operator Client > Bouton événement enfoncé**.
Le Tableau de Configuration des Événements correspondant s'affiche.
2. Sélectionnez un bouton d'événement utilisateur pour configurer son comportement.
3. Dans la colonne **Déclencher l'alarme - Planification**, cliquez sur une cellule, puis sélectionnez la planification appropriée.
La planification détermine le moment de déclenchement de l'alarme devant avertir l'utilisateur de l'événement.
4. Dans la colonne **Fichier - Planification**, cliquez sur une cellule, puis sélectionnez la planification qui convient.
La planification détermine le moment où l'événement est consigné.
Si vous sélectionnez **Jamais**, le bouton d'événement utilisateur n'est pas disponible dans le Operator Client des groupes d'utilisateurs autorisés à accéder à ce type de bouton.
5. Dans la colonne **Script - Script**, cliquez sur une cellule, puis sélectionnez un Script de Commande.
6. Dans la colonne **Script- Planification**, cliquez sur une cellule, puis sélectionnez la planification appropriée.
La planification détermine le moment où le script de Commande est exécuté.

Se reporter à

– Page *Événements*, page 316

25.8

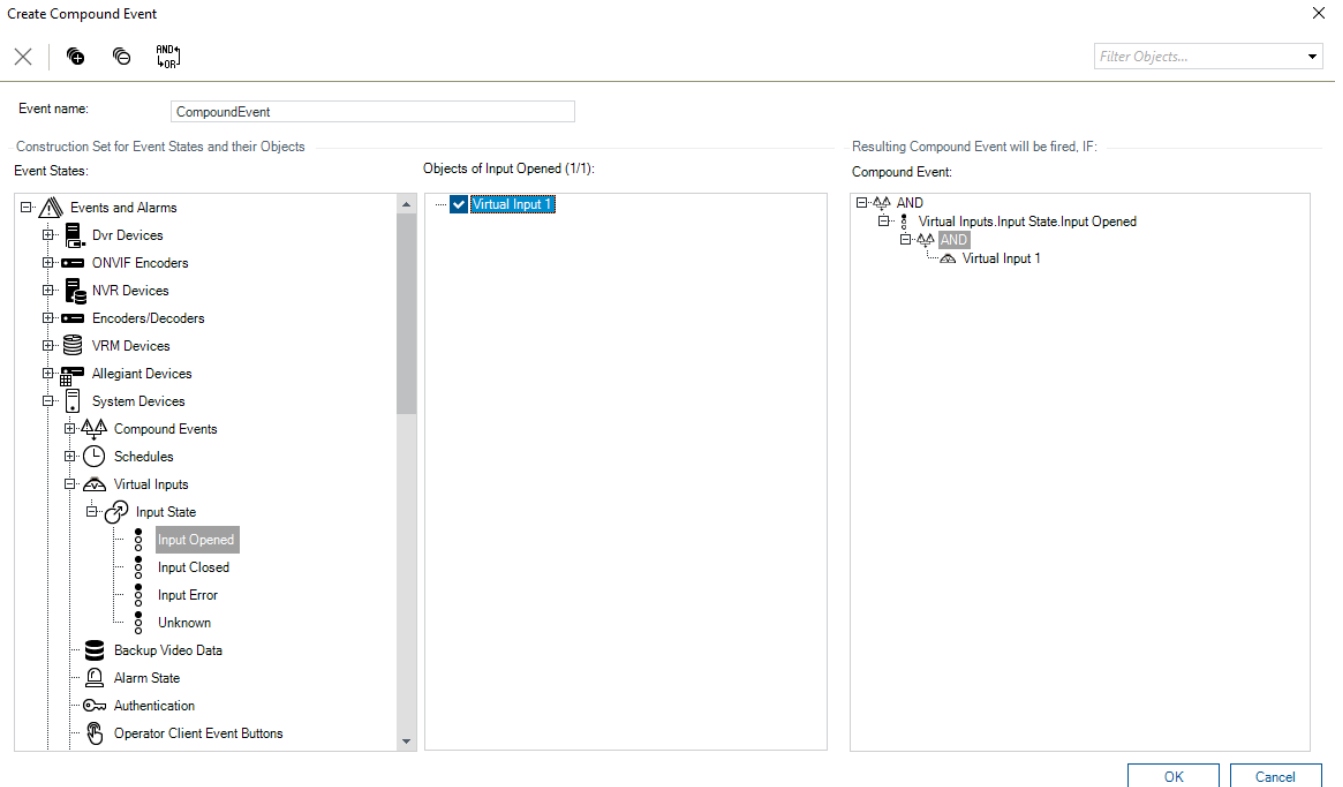
Création d'un Événement Combiné



Fenêtre principale > **Événements** >

Vous créez un Événement Combiné. Vous pouvez uniquement combiner des changements d'état et leurs objets. Les objets correspondent par exemple à des planifications ou des périphériques. Vous pouvez combiner à la fois des changements d'état et des objets à l'aide des expressions booléennes ET et OU.

Exemple : supposons que vous combiniez les états de connexion d'une caméra IP et d'un décodeur. L'Événement Combiné ne doit se produire que lorsque les deux périphériques perdent leur connexion. Dans ce cas, utilisez l'opérateur ET pour les deux objets (la caméra IP et le décodeur) et pour les deux états de connexion **Signal vidéo perdu** et **Déconnecté**.



Pour créer un Événement Combiné :

1. Dans le champ **Nom de l'événement** :, saisissez un nom pour l'Événement Combiné.
2. Dans le champ **États d'événement** :, sélectionnez un état d'événement.
Les objets disponibles s'affichent dans le champ **Objets** :.
3. Dans le champ **Objets** :, sélectionnez le périphérique requis.
L'événement correspondant et les périphériques sélectionnés sont ajoutés au volet Événement Combiné.
4. Dans le champ **Événement combiné**:, cliquez avec le bouton droit de la souris sur une opération booléenne et effectuez les modifications nécessaires.
Une opération booléenne définit la combinaison de ses éléments enfants immédiats.
5. Cliquez sur **OK**.
Le nouvel Événement Combiné est ajouté au Tableau de Configuration des Événements.
Pour consulter ce tableau, accédez à l'Arborescence des Événements sous **Périphériques système**.

Se reporter à

– Page *Événements*, page 316

25.9

Modification d'un Événement Combiné

Fenêtre principale > **Événements**

Vous pouvez modifier un Événement Combiné existant.

Pour modifier un Événement Combiné :

1. Dans l'Arborescence des Événements, développez **Périphériques système** > **État de l'Événement Combiné** > **L'Événement Combiné est vrai**.

2. Dans la colonne **Périphérique** du Tableau de Configuration des Événements, cliquez avec le bouton droit de la souris sur l'Événement Combiné à modifier, puis cliquez sur **Modifier**.
La boîte de dialogue **Modifier l'Événement Combiné** s'affiche.
3. Effectuez les modifications nécessaires.
4. Cliquez sur **OK**.
L'Événement Combiné est modifié.

Se reporter à

- *Page Événements, page 316*

25.10 Configuration d'une alarme

Fenêtre principale > **Alarmes**

Avant de configurer une alarme, vous devez configurer l'événement déclencheur sur la page **Événements**.

Pour configurer une alarme :

1. Dans l'arborescence, sélectionnez une alarme, par exemple **Périphériques système > Authentification > Authentification de l'opérateur rejetée**.
Le Tableau de Configuration des Alarmes correspondant s'affiche.
 2. Dans la colonne **Priorité**, cliquez sur ... dans une cellule pour entrer le niveau de priorité de l'alarme sélectionnée (100 étant un niveau de priorité faible et 1 un niveau de priorité élevé).
Dans la colonne **Titre**, cliquez sur ... dans une cellule pour saisir le titre de l'alarme à afficher dans BVMS, par exemple dans la Liste des Alarmes.
Dans la colonne **Couleur**, cliquez sur ... dans une cellule pour afficher une boîte de dialogue permettant de sélectionner la couleur dans laquelle afficher l'alarme dans Operator Client, par exemple dans la Liste des Alarmes.
 3. Dans les colonnes 1-5, cliquez sur ... dans une cellule pour afficher la boîte de dialogue **Sélectionner le contenu du volet Image**.
Sélectionnez les paramètres appropriés.
 4. Dans la colonne **Fichier audio**, cliquez sur ... dans une cellule pour afficher une boîte de dialogue permettant de sélectionner un fichier audio à lire en cas d'alarme.
 5. Dans la colonne **Options d'alarme**, cliquez sur ... dans une cellule pour afficher la boîte de dialogue **Options d'alarme**.
 6. Sélectionnez les paramètres appropriés.
- Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Se reporter à

- *Configuration d'un événement, page 332*
- *Page Alarmes, page 322*
- *Boîte de dialogue Sélectionner le contenu du volet des Images, page 324*
- *Boîte de dialogue Options d'alarmes, page 325*

25.11 Configuration de paramètres pour toutes les alarmes

Fenêtre principale > **Alarmes**

Vous pouvez définir les paramètres d'alarme suivants, valides pour ce Management Server :

- Nombre de volets des images par alarme
- Durée de l'effacement automatique
- Durée d'enregistrement d'alarme manuelle

- Affichage des alarmes sur plusieurs lignes dans la fenêtre d'image d'alarme
- Durée maximale des enregistrements d'alarme déclenchés par un état
- Configuration du comportement de tous les groupes de moniteurs

Pour configurer toutes les alarmes :

1. Cliquez sur .
La boîte de dialogue **Paramètres de l'alarme** s'affiche.
2. Définissez les paramètres appropriés.
 - ▶ Cliquez sur **OK**.

Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Se reporter à

- *Boîte de dialogue Paramètres d'alarme, page 323*

25.12

Configuration des durées pré-alarme et post-alarme d'une alarme

Pour configurer les paramètres des durées pré-alarme et post-alarme, vous devez disposer d'une caméra prenant en charge la fonction ANR, et le firmware 5.90 ou version ultérieure doit être installé.



Fenêtre principale > **Caméras et enregistrement** > 

- ▶ Pour la caméra souhaitée, cliquez pour activer **ANR**.

Fenêtre principale > **Événements**

- ▶ Configurez l'événement souhaité pour la caméra pour laquelle ANR est activé.

Fenêtre principale > **Alarmes**

1. Configurez une alarme pour cet événement.
2. Sélectionnez  ou .
3. Dans la colonne **Options d'alarmes**, cliquez sur ...
La boîte de dialogue **Options d'alarmes** s'affiche.
4. Dans la colonne **Enregistrer**, cochez la case de la caméra pour laquelle ANR est activé afin d'activer l'enregistrement d'alarme.
La case située dans la colonne **Déviations des paramètres de durée d'alarme** est automatiquement cochée.
5. Cliquez sur l'onglet **Déviations des paramètres de durée d'alarme**.
6. Configurez les paramètres de durée d'alarme comme il convient.

Se reporter à

- *Boîte de dialogue Options d'alarmes, page 325*


25.13

Déclenchement de l'enregistrement d'alarme avec des données texte

Fenêtre principale > **Alarmes**

Vous pouvez déclencher l'enregistrement d'alarme avec des données texte.

Avant de configurer une alarme, vous devez configurer un événement contenant des données texte.

Exemple : **Événements** > Dans l'arborescence des événements, sélectionnez  (des données texte doivent être disponibles, par exemple : **Lecteurs de carte foyer** > **Lecteur de carte foyer** > **Carte refusée**)



Remarque!

Affectez la valeur 0 au temps de réponse pour l'événement sélectionné. Cela garantit qu'aucune donnée texte n'est perdue.

Pour configurer un enregistrement d'alarme :


1. Dans l'arborescence, sélectionnez une alarme, par exemple **Périphériques ATM/POS-Bridge** > **Entrée ATM** > **Entrée de données**.
Le Tableau de Configuration des Alarmes correspondant s'affiche.
2. Sélectionnez les paramètres appropriés.
3. Dans la colonne **Options d'alarmes**, cliquez sur ... dans une cellule pour afficher la boîte de dialogue **Options d'alarmes**.
4. Cliquez sur l'onglet **Caméras**, puis cochez la case **Enregistrer**.

Se reporter à

- *Boîte de dialogue Options d'alarmes, page 325*
- *Boîte de dialogue Enregistrement de données texte, page 321*

25.14

Ajout de données texte à l'enregistrement continu

Fenêtre principale > **Événements** > Dans l'arborescence des événements, sélectionnez  **Entrée de données** (des données texte doivent être disponibles, par exemple : **Lecteurs de carte foyer** > **Lecteur de carte foyer** > **Carte refusée**) > Colonne **Enregistrement de données de texte** > ...

Vous pouvez ajouter des données texte pour l'enregistrement continu.

25.15

Protection de l'enregistrement d'alarme

Fenêtre principale > **Alarmes**

Avant de configurer une alarme, vous devez configurer un événement dans **Événements**.



Remarque!

Si vous protégez l'enregistrement d'alarme d'une caméra, les données vidéo protégées ne seront jamais supprimées automatiquement par VRM. Notez que trop de blocs protégés peuvent saturer le stockage et la caméra risque de ne plus enregistrer. Vous devez déprotéger manuellement les données vidéo dans Operator Client.

Pour configurer un enregistrement d'alarme :

1. Dans l'arborescence, sélectionnez une alarme, par exemple **Périphériques ATM/POS-Bridge** > **Entrée ATM** > **Entrée de données**.
Le Tableau de Configuration des Alarmes correspondant s'affiche.
2. Sélectionnez les paramètres appropriés.
3. Dans la colonne **Options d'alarmes**, cliquez sur ... dans une cellule pour afficher la boîte de dialogue **Options d'alarmes**.
4. Cliquez sur l'onglet **Caméras**, puis cochez la case **Enregistrer**.
1. Cochez la case **Protéger l'enregistrement**.

Se reporter à

– Boîte de dialogue *Options d'alarmes*, page 325


25.16**Configuration de zones réactives clignotantes****Remarque!**


Une zone réactive clignotante ne peut être configurée que pour un événement ou une alarme.

Fenêtre principale > **Événements**

ou


Fenêtre principale > **Alarmes**


Pour chaque événement ou alarme  , vous pouvez configurer la couleur d'arrière-plan et le comportement (avec ou sans clignotement) pour les zones réactives. Par exemple, vous

pouvez configurer pour un événement ou une alarme  d'un dispositif le clignotement de son icône de dispositif sur une carte lorsque l'état de ce dispositif change.

En outre, vous pouvez configurer la priorité d'affichage pour toutes les zones réactives. Cette opération est obligatoire lorsque différents événements se produisent pour le même dispositif. (1 = niveau de priorité le plus élevé)


La couleur configurée est valide pour toutes les zones réactives avec la même priorité d'affichage. Vous pouvez modifier la couleur, le comportement et la priorité de n'importe

quel événement ou alarme  : la couleur modifiée et le comportement sont utilisés pour

toutes les zones réactives de tous les autres événements ou alarmes  qui ont la même priorité.

La configuration des états de couleur sur les cartes n'est possible que lorsque vous cliquez pour sélectionner l'option **Affichage d'état avancé activé (coloration des points chauds sur les cartes en fonction de l'état)** ou l'option **Affichage d'état avancé activé (coloration des points chauds sur les cartes en fonction de l'alarme)** dans la boîte de dialogue **Options**.

Pour configurer une zone réactive clignotante pour un événement :

1. Dans l'arborescence, sélectionnez un état d'événement (), par exemple **Encodeurs/décodeurs > Relais d'encodeur > État du relais > Relais ouvert**.
Le tableau de configuration d'événement correspondant s'affiche.
2. Cliquez sur **Activer sur cartes couleur états**.
3. Dans le champ **Afficher priorité sur carte :**, saisissez la priorité souhaitée.
4. Cliquez sur le champ **Couleur arrière-pl sur carte :** pour sélectionner la couleur souhaitée.
5. Si vous le souhaitez, cliquez sur l'option **Clignotant** pour l'activer.

Pour configurer une zone réactive clignotante pour une alarme :

Reportez-vous au chapitre *Identité de l'alarme* , page 322 de la *Page Alarmes*, page 322.

**Remarque!**

La zone réactive se met à clignoter uniquement si l'alarme figure dans la liste des alarmes.

Les icônes de dispositif sur une carte clignotent dans la couleur configurée pour l'alarme ou l'événement.

Se reporter à

- Page *Événements*, page 316
- Boîte de dialogue *Options (menu Paramètres)*, page 122

25.17

Événements et alarmes pour les systèmes de contrôle d'accès

Informations supplémentaires sur les événements et les alarmes des systèmes de contrôle d'accès.

Événement d'accès demandé

L'événement permet à un opérateur BVMS d'accorder ou de refuser manuellement l'accès à une personne via un système de contrôle d'accès. Vous pouvez configurer l'enregistrement d'alarme, l'enregistrement de données texte ou des informations supplémentaires pour cet événement.

Les événements d'accès demandé sont uniquement envoyés à BVMS si l'option **Vérification supplémentaire** est définie sur chaque lecteur du système de contrôle d'accès. Dans la configuration des événements BVMS, les événements **Accès requis** envoyés par les lecteurs déclenchent toujours une alarme dans BVMS.



Remarque!

Nous vous recommandons de définir le niveau de priorité le plus élevé (1) pour les alarmes **Accès requis**. Vous êtes ainsi certain que les alarmes apparaîtront automatiquement et qu'elles recevront l'attention nécessaire de la part de l'opérateur.

25.18

Événements et alarmes pour l'identification d'une personne

Fenêtre principale > **Événements**

Informations supplémentaires sur les événements et les alarmes pour Person Identification.

Personne non autorisée détectée

Pour chaque caméra, vous pouvez configurer quel groupe de personnes est autorisé ou non à accéder à une certaine zone.

Remarque : la configuration des groupes de personnes autorisés et non autorisés n'est possible que si vous disposez de l'autorisation **Modifier les paramètres d'événement**.

Pour configurer Personne non autorisée détectée

1. Sélectionnez la caméra correspondante sous **Video Analytics**.
2. Sélectionnez l'événement **Personne non autorisée détectée**.
3. Sélectionnez l'onglet **Personne non autorisée détectée**.
4. Cliquez ... dans la cellule **Non autorisé** ou **Autorisé**.

La boîte de dialogue **Authorization for camera** (Autorisation pour la caméra) s'affiche.

5. Par glisser-déposer, déplacez les groupes de personnes configurés dans les champs correspondants.
6. Cliquez sur **OK**.

Les groupes de personnes configurés sont à présent autorisés ou non autorisés pour la caméra correspondante.

26 Page Groupes d'utilisateurs



Remarque!

BVMS Viewer offre uniquement des fonctionnalités de base. Les fonctionnalités avancées sont incluses dans BVMS Professional. Pour de plus amples informations sur les différentes éditions BVMS, consultez le site www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Fenêtre principale > **Groupes d'utilisateurs**

Vous permet de configurer des groupes d'utilisateurs , Enterprise User Groups et Accès Enterprise.

Le groupe d'utilisateurs suivant est disponible par défaut :

- Groupe Admin (avec un seul utilisateur Admin).

Mappage **Fournisseur d'identité (IdP)**

Vous permet de mapper des groupes IdP à des groupes d'utilisateurs BVMS.

Certains des groupes ne s'affichent pas. Les groupes suivants sont filtrés :

- Groupes de vérification multiple
- Partie de groupes d'un groupe de vérification multiple
- Accès Enterprise

Remarque : le même groupe IdP ne peut pas être mappé plusieurs fois.

1. Cliquez sur **+ Ajouter** sur la ligne du groupe d'utilisateurs BVMS que vous souhaitez mapper à un groupe IdP.
2. Dans la fenêtre qui s'affiche, remplissez les champs **Nom de la demande** et **Valeur de la demande**. Vous pouvez obtenir les informations nécessaires pour remplir ces champs auprès de votre fournisseur d'identité externe. **Remarque** : le champ Nom de la demande est sensible à la casse.
3. Cliquez sur **Ajouter**.
4. Cliquez sur **OK**, puis sur **Enregistrer les modifications**.

Si un utilisateur appartient à plusieurs groupes mappés, l'ordre de la liste définit la priorité selon laquelle le groupe BVMS est sélectionné. Vous pouvez modifier cet ordre à l'aide des boutons haut et bas.

Assurez-vous de cliquer sur **Activer la copie de configuration à utiliser** pour activer les modifications apportées à la configuration.

Onglet Groupes d'utilisateurs

Cliquez sur ce bouton pour afficher les pages permettant de configurer les droits d'accès de ce groupe d'utilisateurs standard.

Onglet Enterprise User Groups









Cliquez sur ce bouton pour afficher les pages permettant de configurer les autorisations d'un Enterprise User Group.

Onglet Accès Enterprise

Cliquez sur ce bouton pour afficher les pages permettant d'ajouter et de configurer Enterprise Access.

Options utilisateur/groupe d'utilisateurs

Icône	Description
	Cliquez sur ce bouton pour supprimer une entrée sélectionnée.

Icône	Description
	Cliquez sur ce bouton pour ajouter un nouveau groupe ou compte.
	Cliquez sur cette icône pour ajouter un nouvel utilisateur au groupe d'utilisateurs sélectionné. Si vous le souhaitez, vous pouvez modifier le nom d'utilisateur par défaut.
	Cliquez sur ce bouton pour ajouter un nouveau groupe de double autorisation.
	Cliquez sur ce bouton pour ajouter une nouvelle combinaison de connexion pour la double autorisation
	Affiche une boîte de dialogue permettant de copier des autorisations d'un groupe d'utilisateurs sélectionné vers un autre.
	Cliquez sur ce bouton pour afficher la page permettant de configurer les propriétés de cet utilisateur.
	Cliquez sur ce bouton pour afficher la page permettant de configurer les propriétés de cette combinaison de connexion.
	Cliquez sur ce bouton pour afficher les pages permettant de configurer les droits d'accès de ce groupe de double autorisation.

Activation de la modification du nom d'utilisateur et du mot de passe



Cliquez pour activer les modifications de mot de passe.



Cliquez pour activer les modifications de nom d'utilisateur.



Remarque!

Les modifications de nom d'utilisateur et de mot de passe sont annulées après un rétablissement de configuration.

Autorisations sur un Enterprise System

Pour un Enterprise System, vous pouvez configurer les autorisations suivantes :

- Autorisations d'exploitation pour Operator Client définissant l'interface utilisateur pour l'exploitation dans Enterprise System, par exemple l'interface utilisateur du moniteur d'alarme.
Utilisez un groupe Enterprise User Group. Configurez-le sur Enterprise Management Server.
- Les autorisations de dispositifs devant être disponibles pour l'exploitation sur un Enterprise Management Server sont définies sur chaque Management Server.
Utilisez des comptes Enterprise Account. Configurez-les sur chaque Management Server.

Autorisations pour un seul Management Server

Pour gérer l'accès à l'un des Management Servers, utilisez le groupe d'utilisateurs standard. Vous pouvez configurer toutes les autorisations relatives à ce Management Server dans ce groupe d'utilisateurs.

Vous pouvez configurer des groupes d'utilisateurs à double autorisation pour les groupes d'utilisateurs standard et pour les Enterprise User Groups.

Type	Contient	Paramètres de configuration disponibles	Quel est l'élément à configurer ?
Groupe d'utilisateurs	Utilisateurs	<ul style="list-style-type: none"> - Autorisations d'exploitation et d'utilisation de dispositifs 	<ul style="list-style-type: none"> - Management Server
Enterprise User Group	Utilisateurs	<ul style="list-style-type: none"> - Autorisations d'exploitation - Par Management Server : nom des comptes d'accès Enterprise correspondants avec identifiants de connexion 	<ul style="list-style-type: none"> - Enterprise Management Server
Enterprise Account	-	<ul style="list-style-type: none"> - Autorisations d'utilisation de dispositifs - Clé de compte 	<ul style="list-style-type: none"> - Management Server
Groupe d'utilisateurs avec autorisation double	Groupes d'utilisateurs	<ul style="list-style-type: none"> - Voir les groupes d'utilisateurs 	<ul style="list-style-type: none"> - Voir les groupes d'utilisateurs
Enterprise double autorisation	Enterprise User Groups	<ul style="list-style-type: none"> - Voir Enterprise User Groups 	<ul style="list-style-type: none"> - Voir Enterprise User Groups

Pour rechercher des éléments :

- ▶ Dans le champ de recherche , saisissez une chaîne et appuyez sur la touche ENTER de votre clavier pour filtrer les options affichées. Seuls les éléments contenant la chaîne et leurs éléments parents correspondants (uniquement dans des arborescences) sont affichés. Le nombre d'éléments filtrés et le nombre total d'articles sont fournis.

Remarque : Pour effectuer une recherche exacte sur des chaînes de caractères, placez-les entre guillemets. Par exemple, la recherche "Camera 1" ne filtrera que les caméras portant ce nom exact, et non pas camera 201.

26.1

Page Propriétés du groupe d'utilisateurs

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
 Onglet **Autorisations d'utilisation** > Onglet **Propriétés du groupe d'utilisateurs**
 ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
 Onglet **Autorisations d'utilisation** > Onglet **Propriétés du groupe d'utilisateurs**
 Permet de configurer les paramètres suivants pour le groupe d'utilisateurs sélectionné :

- Planification de connexion
- Sélection du groupe d'utilisateurs LDAP associé

Propriétés du groupe d'utilisateurs

Description :

Entrez une brève description du groupe d'utilisateurs.

Langue

Sélectionnez la langue de l'Operator Client.

Planification de connexion

Sélectionnez une Planification des Tâches ou une Planification d'Enregistrement. Les utilisateurs du groupe sélectionné peuvent uniquement se connecter au système au cours des tranches horaires définies dans cette planification.

Propriétés LDAP

Rechercher des groupes

Cliquez sur ce bouton pour afficher les groupes LDAP associés disponibles dans la liste **Groupe LDAP associé**. Pour sélectionner un groupe LDAP associé, vous devez définir les paramètres appropriés dans la boîte de dialogue **Paramètres du serveur LDAP**.

Groupe LDAP associé



Sélectionnez un groupe LDAP dans la liste **Groupe LDAP associé** à utiliser pour votre système.

Se reporter à



- *Sélectionner un groupe LDAP associé, page 371*
- *Association d'un groupe LDAP, page 119*
- *Planification des autorisations de connexion utilisateur, page 372*

26.2

Page Propriétés de l'utilisateur

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs**  > 

ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  > 

Permet de configurer un nouvel utilisateur dans un groupe d'utilisateurs standard ou dans un groupe Enterprise User Group.

Si vous modifiez le mot de passe pour un utilisateur ou si vous le supprimez alors qu'il est connecté, il peut continuer à travailler avec Operator Client, même après la modification ou la suppression. Si, après la modification ou la suppression, la connexion à Management Server est interrompue (par exemple après l'activation de la configuration), l'utilisateur ne peut pas se reconnecter automatiquement à la Management Server sans se déconnecter/ connecter à Operator Client.

Le compte est activé

Cochez cette case pour activer un compte utilisateur.

Remarque : Chaque nouveau compte d'utilisateur est désactivé par défaut. Vous devez d'abord définir un mot de passe, puis activer le compte d'utilisateur.

Nom complet

Saisissez le nom de l'utilisateur en entier.

Description

Entrez une brève description de l'utilisateur.

L'utilisateur doit changer le mot de passe lors de la prochaine connexion

Cochez cette case pour obliger les utilisateurs à définir un nouveau mot de passe au moment de la prochaine connexion.


Entrer le nouveau mot de passe

Saisissez le mot de passe du nouvel utilisateur.

Confirmer le mot de passe

Saisissez à nouveau le mot de passe.

**Remarque!**

Pour activer les modifications de cette boîte de dialogue, cliquez sur  .

**Remarque!**


Il est fortement recommandé d'affecter un mot de passe spécifique à tous les nouveaux utilisateurs et de demander à chaque utilisateur de le modifier au moment de la connexion.

**Remarque!**

Les clients de Mobile Video Service, Web Client, Bosch iOS App et SDK ne sont pas en mesure de modifier le mot de passe au moment de la connexion.

Appliquer

Cliquez sur ce bouton pour appliquer les paramètres.

Cliquez sur  pour activer le mot de passe.

Informations supplémentaires

Après la mise à niveau vers BVMS 9.0.0.x, les paramètres **Propriétés de l'utilisateur** sont les suivants :

- **Le compte est activé** est défini.
- **L'utilisateur doit changer le mot de passe lors de la prochaine connexion** n'est pas défini.

26.3

Page Propriétés de combinaison de connexion

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** > 

Nouveau groupe de double autorisation > 

ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** > 

Nouveau groupe de double autorisation Enterprise > 

Permet de convertir une combinaison de groupes d'utilisateurs en un groupe de double autorisation. Les utilisateurs du premier groupe d'utilisateurs doivent se connecter dans la première boîte de dialogue d'ouverture de session ; les utilisateurs du deuxième groupe d'utilisateurs confirment la connexion.

Sélectionner une combinaison de connexion

Sélectionnez un groupe d'utilisateurs dans chacune des listes.


Forcer la double autorisation

Cochez cette option pour imposer que chaque utilisateur ne puisse se connecter que simultanément avec un utilisateur du second groupe.

Se reporter à

– *Ajout d'une combinaison de connexion au groupe de double autorisation, page 370*

26.4**Page Autorisations de caméra**

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations du périphérique** > Onglet **Autorisations de caméra**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Accès Enterprise** >  > Onglet
Autorisations du périphérique > Onglet **Autorisations de caméra**

Permet de configurer les droits d'accès aux fonctions d'une caméra ou d'un groupe de caméras pour le groupe d'utilisateurs sélectionné.

Si de nouveaux composants sont ajoutés, il est nécessaire de reconfigurer les autorisations de caméra.

Vous pouvez interdire l'accès à une caméra sur la page **Caméra**.

Caméra

Affiche le nom de la caméra tel qu'il est configuré sur la page **Caméras et enregistrement**.

Emplacement

Affiche la position de la caméra telle qu'elle est configurée sur la page **Cartes et structure**.

Accès

Cochez cette case pour autoriser l'accès à cette caméra.

Vidéo en Mode Temps Réel

Cochez cette case pour autoriser l'utilisation de la vidéo en Mode Temps Réel.

Son en Mode Temps Réel

Cochez cette case pour autoriser l'utilisation de la vidéo en Mode Temps Réel.

Enregistrement manuel

Cochez cette case pour autoriser l'enregistrement manuel des alarmes (enregistrement d'alarme).

Vous ne pouvez cocher ou décocher cette case que si l'enregistrement sur alarme manuel est activé sur la page **Fonctions de l'opérateur**.

Vidéo en Mode Lecture

Cochez cette case pour autoriser l'utilisation de la vidéo en Mode Temps Réel.

Vous ne pouvez cocher ou décocher cette case que si le mode lecture est activé sur la page **Fonctions de l'opérateur**.

Son en Mode Lecture

Cochez cette case pour autoriser l'utilisation du son en Mode Lecture.

Vous ne pouvez cocher ou décocher cette case que si le mode lecture est activé sur la page **Fonctions de l'opérateur**.

Données texte

Cochez cette case pour autoriser l'affichage des métadonnées.

Vous ne pouvez cocher ou décocher cette case que si l'affichage des métadonnées est activé sur la page **Fonctions de l'opérateur**.

Exporter

Cochez cette case pour autoriser l'exportation de données vidéo.

Vous ne pouvez cocher ou décocher cette case que si l'exportation des données vidéo est activée sur la page **Fonctions de l'opérateur**.

PTZ/ROI

Sélectionnez une case pour permettre l'utilisation de la commande PTZ ou du ROI de cette caméra.

Vous ne pouvez cocher ou décocher cette case que si la commande PTZ (balayage horizontal/vertical et zoom) ou la fonction ROI de cette caméra est activée sur la page **Fonctions de l'opérateur**. Vous devez également configurer PTZ ou ROI dans le Tableau des caméras.

Aux

Cochez cette case pour autoriser l'exécution de commandes auxiliaires.

Vous ne pouvez cocher ou décocher cette case que si les commandes de balayage horizontal/vertical et de zoom d'une caméra sont activées sur la page **Fonctions de l'opérateur**.

Définir des positions prédéfinies

Cochez cette case pour autoriser l'utilisateur à définir des prépositions pour cette caméra mobile.

Vous pouvez également définir des prépositions pour la fonctionnalité Zone d'intérêt, si elle est activée et autorisée.

Vous ne pouvez cocher ou décocher cette case que si les commandes de balayage horizontal/vertical et de zoom d'une caméra sont activées sur la page **Fonctions de l'opérateur**.

Image de référence

Cochez cette case pour permettre la mise à jour de l'image de référence de cette caméra.

Privacy overlay

Cochez une case pour activer ce paramètre Privacy overlay pour cette caméra en mode temps direct et en mode lecture.

26.5**Page Priorité des commandes**

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations du périphérique** > Onglet **Priorités des commandes**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Accès Enterprise** >  > Onglet **Autorisations du périphérique** > Onglet **Priorités des commandes**

Priorités des commandes

Faites glisser le curseur vers la droite pour diminuer le niveau de priorité relatif à la prise de commande du balayage horizontal/vertical et du zoom et des lignes de jonction Allegiant. Un utilisateur bénéficiant d'une priorité élevée peut verrouiller les commandes de balayage horizontal/vertical et de zoom et le contrôle d'une ligne de jonction pour les utilisateurs de

niveau de priorité inférieur. Vous pouvez définir la durée du verrouillage des commandes de balayage horizontal/vertical et de zoom dans le champ **Temps d'attente en min.**. La valeur par défaut est de 1 minute.



Temps d'attente en min.


Indiquez la période en minutes.

Se reporter à

– *Configuration de priorités diverses, page 373*

26.6**Boîte de dialogue Copier les autorisations du groupe d'utilisateurs**

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  > 
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  > 

Permet de sélectionner les autorisations d'un groupe d'utilisateurs à copier vers d'autres groupes.

Copier à partir de :

Affiche le groupe d'utilisateurs sélectionné. Il s'agit du groupe d'utilisateurs dont il faut copier les autorisations.

Paramètres à copier

Cochez la case correspondant aux autorisations du groupe d'utilisateurs à copier.

Copier vers :

Cochez la case des groupes d'utilisateurs vers lesquels copier les autorisations sélectionnées.

Se reporter à

– *Copie des autorisations d'un groupe d'utilisateurs, page 374*

26.7**Page Autorisations de décodeur**

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  > Onglet **Autorisations du périphérique** > Onglet **Autorisations de décodeur**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Accès Enterprise** >  > Onglet **Autorisations du périphérique** > Onglet **Autorisations de décodeur**

Permet de configurer les décodeurs auxquels les utilisateurs de ce groupe ont accès.

Décodeur

Affiche les décodeurs disponibles.

Cochez cette case pour autoriser le groupe d'utilisateurs à accéder à ce décodeur.

Groupe de moniteurs

Cochez cette case pour permettre aux utilisateurs du groupe d'utilisateurs sélectionné d'accéder à ce groupe de moniteurs.

26.8 Page Événements et alarmes

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  > Onglet **Autorisations du périphérique** > Onglet **Événements et alarmes**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Accès Enterprise** >  > Onglet **Autorisations du périphérique** > Onglet **Événements et alarmes**


Permet de configurer les autorisations d'accès dans l'arborescence des événements, par exemple, les événements auxquels le groupe d'utilisateurs peut accéder ou non.

Il est impossible de modifier ces paramètres pour les groupes d'utilisateurs par défaut.

Chaque événement est associé à au moins un dispositif. Par exemple, les caméras disponibles pour l'événement **Perte de vidéo** sont les dispositifs. Pour un événement comme **Sauvegarde terminée**, le dispositif correspondant est **Sauvegarde avec contrôle temporel**. Par conséquent, un dispositif peut être un processus logiciel.

1. Développez un élément de l'arborescence et cochez les cases des événements que vous souhaitez activer. Dans la colonne **Accès**, cochez la case d'un dispositif pour activer les événements associés. L'accès aux dispositifs est configurable sur les pages **Caméra** et **Autorisations de caméra**.
2. Pour activer ou désactiver l'ensemble des événements simultanément, cochez ou décochez la case **Événements et alarmes**.

26.9 Page d'identifiants

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Accès Enterprise** >  > Onglet **Autorisations du périphérique** > Onglet **Identifiants**

Configurez les identifiants d'un Enterprise Account sur un Management Server.

Vous pouvez configurer Accès Enterprise sur chaque Management Server membre de votre Enterprise System. Le Enterprise Management Server utilise cet identifiant pour autoriser l'accès aux dispositifs de ce Management Server pour le Operator Client qui se connecte en tant qu'utilisateur d'un Enterprise User Group.

Description :

Saisissez une description pour le Enterprise Account souhaité.

Politique de clé renforcée

La case à cocher **Politique de clé renforcée** est présélectionnée pour tous les nouveaux groupes d'utilisateurs créés.

Il est fortement recommandé de conserver ce paramètre pour améliorer la protection de votre ordinateur contre tout accès non autorisé.

Les règles suivantes sont applicables :

- Longueur minimale de la clé définie dans la page **Stratégies de compte** pour le groupe d'utilisateurs approprié.
- Ne pas utiliser l'une des clés précédentes.
- Utiliser au moins une lettre majuscule (A à Z).
- Utiliser au moins un chiffre (0 à 9).
- Utiliser au moins un caractère spécial (Exemple : ! \$ # %).

Entrer une nouvelle clé : / Confirmer la clé :

Saisissez et confirmez la clé pour ce Management Server.

Se reporter à

– *Création d'un Enterprise Account, page 367*

26.10 Page Arborescence Logique

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations du périphérique** > Onglet **Arborescence logique**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Accès Enterprise** >  > Onglet **Autorisations du périphérique** > Onglet **Arborescence logique**

Permet de configurer l'arborescence logique de chaque groupe d'utilisateurs.

Pour configurer les autorisations :

- ▶ Cochez ou décochez les cases en fonction de vos besoins.
Lorsque vous sélectionnez un élément dans un nœud, le nœud entier est automatiquement sélectionné.
Lorsque vous sélectionnez un nœud, tous les éléments au-dessous sont automatiquement sélectionnés.

Caméra

Cochez une case pour autoriser les utilisateurs du groupe d'utilisateurs sélectionné à accéder aux dispositifs correspondants.

Vous pouvez interdire l'accès à une caméra sur la page **Autorisations de caméra**.

Groupe de moniteurs

Cochez cette case pour permettre aux utilisateurs du groupe d'utilisateurs sélectionné d'accéder à ce groupe de moniteurs.

Se reporter à

– *Configuration des autorisations d'utilisation des dispositifs, page 372*

26.11 Page des fonctionnalités d'Operator

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations d'utilisation** > Onglet **Fonctions de l'opérateur**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Autorisations d'utilisation** > Onglet **Fonctions de l'opérateur**

Permet de configurer diverses autorisations pour le groupe d'utilisateurs sélectionné.

Commande balayage horizontal/vertical et zoom de dômes

Cochez cette case pour autoriser la commande d'une caméra.

Page **Priorités des commandes** : vous pouvez définir la priorité relative à la prise de commande d'une caméra dans le champ **Priorités des commandes**.

Lignes de jonction Allegiant

Cochez cette case pour autoriser l'accès aux lignes de jonction Bosch Allegiant.

Page **Priorités des commandes** : vous pouvez définir la priorité relative à la prise de commande de lignes de jonction Bosch Allegiant dans le champ **Priorités des commandes**.

Imprimer et enregistrer

Cochez cette case pour autoriser l'impression et l'enregistrement de données vidéo, de cartes et de documents.

Traitement d'alarme

Cochez cette case pour autoriser le traitement des alarmes.

Interrompre l'économiseur d'écran Windows pour les alarmes entrantes

Cochez cette option pour garantir qu'une alarme entrante s'affichera même si l'économiseur d'écran est actif. Ce paramètre reste sans effet si l'interruption de l'économiseur d'écran est conditionnée à la saisie d'un nom d'utilisateur et d'un mot de passe.

Affichage des alarmes

Cochez cette case pour autoriser l'affichage des alarmes. Si vous sélectionnez cette option, l'option **Traitement d'alarme** est désactivée en même temps.

Lecture

Sélectionnez cette case à cocher pour autoriser plusieurs fonctions de lecture.

Exporter la vidéo

Cochez cette case pour autoriser l'exportation de données vidéo.

Exporter dans des formats non natifs

Sélectionnez la case permettant d'exporter des données vidéo dans un format non natif.

Protéger la vidéo

Cochez cette case pour activer la protection des données vidéo.

Désactiver la protection de la vidéo

Cochez cette case pour autoriser la protection et la déprotection des données vidéo.

Restreindre la vidéo (une vidéo restreinte ne peut être vue que par les utilisateurs qui disposent de cette autorisation)

Cochez cette case pour autoriser la restriction des données vidéo.

Désactiver la restriction de la vidéo

Cochez cette case pour autoriser la restriction et la non restriction des données vidéo.

Remarque!

VRM



Configurez les autorisations utilisateur pour restreindre ou non les données vidéo dans BVMS comme il convient.

Seul un utilisateur qui a l'autorisation **Restreindre la vidéo (une vidéo restreinte ne peut être vue que par les utilisateurs qui disposent de cette autorisation)** peut voir des vidéos restreintes sur la chronologie d'Operator Client. La plage de temps restreinte est autrement affichée sous le nom **Aucun enregistrement**.

Remarque!

DIVAR AN



Configurez les autorisations utilisateur définies pour restreindre et ne pas restreindre des données vidéo sur votre dispositif DIVAR AN comme il convient. Créez un utilisateur dans BVMS avec les mêmes informations d'identification et configurez les autorisations pour restreindre et ne pas restreindre en conséquence.

L'affichage d'une vidéo restreinte n'est pas affecté et doit être configuré séparément sur le dispositif DIVAR AN.

Effacer la vidéo

Cochez cette case pour autoriser la suppression de données vidéo.

Accéder aux vidéos enregistrées lorsque le groupe d'utilisateurs n'est pas autorisé à se connecter

Cochez cette case pour autoriser l'accès aux données vidéo indiquées.

Accès au Journal des Connexions

Cochez cette case pour autoriser l'accès au Journal des Connexions.

Effacer les données texte des entrées du journal des connexions (pour effacer des données relatives à une personne)

Sélectionnez cette case pour autoriser l'effacement de données texte des entrées du journal des connexions.

Boutons événement Opérateur

Cochez cette case pour autoriser les boutons d'événements utilisateur dans Operator Client.

Fermer Operator Client

Cochez cette case pour autoriser la fermeture de Operator Client.

Réduire Operator Client

Cochez cette case pour autoriser la réduction de Operator Client.

Intercom audio

Cochez la case de cette option pour autoriser l'utilisateur à parler dans les haut-parleurs d'un encodeur par la fonction entrée audio et sortie audio.

Enregistrement d'alarme manuel

Cochez cette case pour autoriser l'enregistrement manuel des alarmes.

Accès au moniteur VRM

Cochez cette case pour autoriser l'accès au VRM Monitor logiciel.

Définir une image de référence

Cochez la case pour autoriser la mise à jour de l'image de référence dans Operator Client.

Définir la sélection de la zone pour l'Image de référence

Cochez la case pour permettre la sélection de la zone dans l'image de la caméra, pour la mise à jour de l'image de référence dans Operator Client.

Modifier le mot de passe

Cochez la case pour autoriser un utilisateur d'Operator Client à modifier le mot de passe permettant d'ouvrir une session.

Armer les zones du panneau d'intrusion

Activez cette case à cocher pour permettre à un utilisateur d'Operator Client d'armer les zones configurées dans une centrale d'intrusion faisant partie de votre configuration BVMS.

Appliquer l'armement des zones du panneau d'intrusion

Sélectionnez cette case à cocher pour permettre à un utilisateur d'Operator Client de forcer l'armement des zones configurées dans une centrale d'intrusion faisant partie de votre configuration BVMS.

Désarmer les zones du panneau d'intrusion

Sélectionnez cette case à cocher pour permettre à un utilisateur d'Operator Client de désarmer les zones configurées dans une centrale d'intrusion faisant partie de votre configuration BVMS.

Désactiver les sonneries pour les zones du panneau d'intrusion

Sélectionnez cette case à cocher pour permettre à un utilisateur d'Operator Client de désactiver les sirènes des zones configurées dans une centrale d'intrusion faisant partie de votre configuration BVMS.

Exclure les points de panneau d'intrusion

Sélectionnez cette case à cocher pour permettre à un utilisateur d'Operator Client de modifier l'état d'un point configuré dans une centrale d'intrusion à l'état **Point exclu**. Un point exclu ne peut pas envoyer une alarme. Lorsque l'état repasse à **Point non exclu**, une alarme en attente est envoyée le cas échéant

Déverrouiller les portes du panneau d'intrusion

Sélectionnez cette case à cocher pour autoriser un utilisateur d'Operator Client à déverrouiller une porte configurée dans une centrale d'intrusion.

Sécuriser et annuler la sécurisation des portes du panneau d'intrusion

Sélectionnez cette case à cocher pour autoriser un utilisateur d'Operator Client à sécuriser et annuler la sécurisation d'une porte configurée dans une centrale d'intrusion.

Portes cycliques du panneau d'intrusion

Sélectionnez cette case à cocher pour autoriser un utilisateur d'Operator Client à définir le cycle d'une porte configurée dans une centrale d'intrusion.

Faire fonctionner les portes d'accès

Sélectionnez la case à cocher pour permettre à un utilisateur Operator Client de modifier l'état de la porte d'accès (sécuriser, verrouiller, déverrouiller).

Prendre une décision d'accès

Cochez cette case pour permettre à un utilisateur d'Operator Client de prendre une décision d'accès.

Gestion de personne

Sélectionnez cette case à cocher pour permettre à un utilisateur Operator Client de gérer des personnes pour les alarmes d'identification d'une personne.

Réinitialiser le niveau de menace

Cochez cette case pour permettre à un utilisateur d'Operator Client de réinitialiser le niveau d'une menace si l'Operator Client est en mode de niveau de menace.

Importer/Exporter des favoris et des signets

Cochez cette case pour autoriser un utilisateur d'Operator Client d'importer ou exporter des favoris ou des signets.

Ordre affichage si priorité alarme identique

Sélectionnez la valeur appropriée pour configurer l'ordre d'apparition des volets des images d'alarme dans Operator Client.

Durée de rembobinage de lecture instantanée :

Entrez la durée de lecture instantanée d'une alarme en secondes.

Répéter le son de l'alarme :

Cochez cette case et saisissez le nombre de secondes devant s'écouler avant la répétition d'une alarme sonore.

Limiter l'accès à la vidéo enregistrée pendant les n dernières minutes :

Cochez cette case pour restreindre l'accès aux vidéos enregistrées.

Dans la liste, entrez la durée en minutes.

Forcer la déconnexion automatique de l'opérateur après ce délai d'inactivité :


Cochez la case permettant d'activer la déconnexion automatique d'Operator Client au bout de la période configurée.

Se reporter à

– *Déconnexion en cas d'inactivité, page 42*

26.12 Page Priorités

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations d'utilisation** > Onglet **Priorités**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Autorisations d'utilisation** > Onglet **Priorités**

Permet de configurer la durée du verrouillage PTZ explicite. Vous pouvez définir les priorités des commandes de balayage horizontal/vertical et de zoom et de l'affichage des alarmes entrantes.

Comportement contextuel automatique

Faites glisser le curseur pour ajuster le niveau de priorité de la fenêtre Image en Mode Temps Réel ou Lecture. Cette valeur sert à déterminer si les alarmes entrantes doivent automatiquement s'afficher dans la fenêtre Image d'alarme.

Exemple : supposons que le curseur de la fenêtre Image en temps réel est défini sur 50 et celui de l'affichage en Mode Lecture sur 70. Une alarme portant le niveau de priorité 60 s'affiche alors automatiquement si et seulement si l'utilisateur a déjà ouvert l'affichage en Mode Lecture. En revanche, elle ne s'affiche pas automatiquement si l'utilisateur a activé l'affichage en Mode Temps Réel.

Se reporter à

- *Configuration de priorités diverses, page 373*

26.13 Page Interface utilisateur

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations d'utilisation** > Onglet **Interface utilisateur**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Autorisations d'utilisation** > Onglet **Interface utilisateur**

Permet de configurer l'interface utilisateur de 4 moniteurs utilisés par Operator Client. Vous pouvez configurer un mode à plusieurs moniteurs incluant jusqu'à 4 moniteurs. Il est possible de définir ce qui s'affiche sur chaque moniteur ; par exemple, le moniteur 2 peut n'afficher que les volets des images en temps réel, ou le moniteur 1 et le moniteur 2 peuvent utiliser le rapport hauteur/largeur 16:9 pour les caméras HD.

Moniteur de contrôle

Sélectionnez le moniteur qui doit être utilisé comme moniteur de contrôle.

Nombre max de ligne de volets des images en mode lecture

Sélectionnez le nombre maximal de lignes des volets d'images affichées dans la fenêtre Image en mode lecture sur le moniteur de contrôle.

Moniteur d'alarme

Sélectionnez le moniteur d'alarme pouvant afficher des données en temps réel et en mode alarme ou en mode alarme uniquement.

Moniteurs 1 à 4

Dans la liste correspondant à chaque moniteur, sélectionnez l'entrée appropriée.

- Pour le moniteur de contrôle, l'entrée **Contrôle** est présélectionnée et ne peut pas être modifiée.
- Pour le moniteur d'alarme, vous pouvez sélectionner l'une des entrées suivantes :
 - **Vidéo en temps réel et alarmes**
 - **Affichage d'alarmes uniquement**
- Pour les autres moniteurs, vous pouvez sélectionner l'une des entrées suivantes :
 - **Vidéos en temps réel uniquement**
 - **Plans et documents**
 - **Deux plans et documents**
 - **Vidéo en temps réel plein écran**
 - **Un quadravision en temps réel**

Nombre de lignes max de volets des images

Sélectionnez le nombre maximal de lignes des volets d'images affichées dans la fenêtre d'Image sur le moniteur de contrôle.

Remarque : cette option est uniquement disponible pour les modes d'affichage suivants :

- **Contrôle**
- **Affichage d'alarmes uniquement**
- **Vidéo en temps réel et alarmes**
- **Vidéos en temps réel uniquement**

Les vues restantes ont une disposition fixe avec un nombre de lignes du volet d'images fixe, sans modification possible.

Format des volets d'images

Pour chaque moniteur, sélectionnez le rapport hauteur/largeur requis lors du démarrage initial de Operator Client. Utilisez le format 16:9 pour les caméras HD.

Rest. param. par défaut

Cliquez sur ce bouton pour rétablir les paramètres par défaut de cette page. Toutes les listes seront rétablis avec leurs paramètres par défaut.

26.14

Page Accès au serveur

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Accès au serveur**

Vous pouvez configurer l'accès au serveur sur un Enterprise Management Server. Vous saisissez le nom de l'Enterprise Account et son mot de passe pour chaque Management Server de votre Enterprise System. Ce compte est configuré sur chaque Management Server.

Management Server

Affiche le nom du Management Server que vous avez configuré sur ce Enterprise Management Server.

Adresse réseau

Saisissez l'adresse IP ou le nom DNS privé du Management Server.

Numéro du serveur

Affiche le numéro du Management Server. Ce numéro est utilisé par un clavier Bosch IntuiKey pour la sélection du Management Server souhaité.

Accès

Cochez la case lorsque vous souhaitez accorder l'accès au Management Server. Ce Management Server est maintenant un Enterprise Management Server.

Enterprise Account

Saisissez le nom de l'Enterprise Account qui a été configuré sur le Management Server.

Authentification

Sélectionnez l'option d'authentification correspondante dans la boîte de dialogue

Paramètres d'authentification .**Api de config.**

Cochez la case si le jeton d'accès doit autoriser l'accès au service Config API du Management Server.

Description du serveur

Affiche le texte descriptif pour ce serveur.

Les colonnes supplémentaires s'affichent lorsqu'elles ont été ajoutées à la liste des serveurs.

Se reporter à


- *Créer un groupe ou un compte, page 366*
- *Création d'un système d'entreprise, page 86*
- *Configuration de la liste des serveurs pour le système d'entreprise, page 86*
- *Authentification basée sur les jetons, page 88*


26.15**Page Autorisations de configuration****Remarque!**

Ce document décrit certaines fonctions non disponibles pour BVMS Viewer.

Pour plus de détails sur les différentes versions BVMS, consultez le site

www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations d'utilisation** > Onglet **Autorisations de configuration**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Autorisations d'utilisation** > Onglet **Autorisations de configuration**
Permet de configurer diverses autorisations utilisateur pour le Configuration Client.

Arborescence des Périphériques

Dans cette section, vous pouvez indiquer les autorisations dans la page **Périphériques**.

Cochez cette case pour chaque autorisation.

Cartes et structure

Dans cette section, vous pouvez indiquer les autorisations dans la page **Cartes et structure**.

Cochez cette case pour chaque autorisation.

Planifications

Dans cette section, vous pouvez indiquer les autorisations dans la page **Planifications**.

Cochez cette case pour chaque autorisation.

Caméras et enregistrement

Dans cette section, vous pouvez indiquer les autorisations dans la page **Caméras et enregistrement**. Cochez cette case pour chaque autorisation.

Événements

Dans cette section, vous pouvez indiquer les autorisations dans la page **Événements**.
Cochez cette case pour chaque autorisation.

Alarmes

Dans cette section, vous pouvez indiquer les autorisations dans la page **Alarmes**. Cochez cette case pour chaque autorisation.

Groupes d'utilisateurs

Dans cette section, vous pouvez indiquer les autorisations de configuration des groupes d'utilisateurs. Cochez cette case pour chaque autorisation.

**Remarque!**

Pour des raisons de sécurité, la case **Configurer les groupes d'utilisateurs/comptes Enterprise Accounts** et les cases **Configurer les utilisateurs** et **Configurer les utilisateurs Enterprise** ne peuvent pas être cochées simultanément.

**Remarque!**

Une fois les autorisations **Configurer les utilisateurs** et **Configurer les utilisateurs Enterprise** affectées, sur la page **Autorisations du groupe d'utilisateurs**, vous devez affecter les groupes d'utilisateurs dans lesquels il est possible d'ajouter et de configurer de nouveaux utilisateurs.

Audit Trail

Dans cette section, vous pouvez spécifier si un utilisateur peut utiliser cette fonction de Audit Trail et exporter des données de Audit Trail.
Cochez cette case pour chaque autorisation.

Commandes de menu

Dans cette section, vous pouvez indiquer les autorisations de configuration des commandes de menu. Cochez cette case pour chaque autorisation.

Rapports

Dans cette section, vous pouvez indiquer les autorisations de configuration des rapports.
Cochez cette case pour chaque autorisation.

**Remarque!**

Si vous souhaitez utiliser le service Config API du Management Server, vous devez sélectionner les autorisations **Autorisations de configuration** :


- **Modifier les propriétés de périphérique**
- **Appeler le gestionnaire d'activation**

**Remarque!**

Si vous souhaitez configurer les paramètres **Paramètres du certificat autorisé**, vous devez sélectionner l'autorisation **Configurer les groupes d'utilisateurs/comptes Enterprise Accounts**.

26.16**Page Autorisations du groupe d'utilisateurs**

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations d'utilisation** > Onglet **Autorisations du groupe d'utilisateurs**
ou votre

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Autorisations d'utilisation** > Onglet **Autorisations du groupe d'utilisateurs**
Permet d'indiquer dans quels groupes d'utilisateurs les utilisateurs d'un groupe d'utilisateur spécifique peuvent ajouter de nouveaux utilisateurs.

**Remarque!**

Vous ne pouvez affecter des autorisations d'un groupe d'utilisateurs qu'à un groupe d'utilisateurs auquel vous avez préalablement affecté l'autorisation de configurer les utilisateurs. Vous pouvez attribuer cette autorisation dans la page **Autorisations de configuration**.

**Remarque!**


Les utilisateurs d'un groupe d'utilisateurs standard ne sont pas autorisés à ajouter de nouveaux utilisateurs au groupe Admin. Cette case à cocher n'est pas active.

Se reporter à

– *Page Autorisations de configuration, page 356*

26.17

Page Stratégies de compte

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Sécurité** > Onglet **Stratégies de compte**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Sécurité** > Onglet **Stratégies de compte**

Vous permet de configurer les paramètres des utilisateurs et des mots de passe.

Stratégie de mot de passe fort

Cochez cette case pour activer la stratégie de mot de passe.

Pour plus d'informations, reportez-vous à la *Configuration des utilisateurs, des autorisations et de l'accès d'entreprise, page 365*.

**Remarque!**

Le paramètre **Stratégie de mot de passe fort** ne s'applique aux utilisateurs si la case est cochée dans le groupe d'utilisateurs correspondant.

Il est fortement recommandé de conserver ce paramètre pour améliorer la protection de votre ordinateur contre tout accès non autorisé.

Longueur minimum du mot de passe

Ce paramètre détermine le minimum de caractères pouvant constituer un mot de passe pour un compte d'utilisateur.

Cochez cette case pour activer le paramètre et entrez le nombre minimum de caractères.

Âge maximum du mot de passe en jours

Ce paramètre détermine le délai (en jours) d'utilisation du mot de passe avant que le système n'exige sa modification par l'utilisateur.

Cochez cette case pour activer le paramètre et entrez le nombre maximum de jours.

Nombre de mots de passe utilisés dans l'historique

Ce paramètre détermine le nombre de nouveaux mots de passe uniques devant être associés à un compte utilisateur avant qu'un ancien mot de passe puisse être réutilisé. Cochez cette case pour activer le paramètre et entrez le nombre minimum de mots de passe.

Nombre maximum de tentatives de connexion non valides

Ce paramètre détermine la désactivation d'un compte après un certain nombre de tentatives de connexion invalides.

Cochez cette case pour activer le paramètre et entrez le nombre maximum de tentatives.

Si la case à cocher **Nombre maximum de tentatives de connexion non valides** est sélectionnée, vous pouvez spécifier les deux paramètres suivants :

Durée de verrouillage du compte

Ce paramètre détermine le nombre de minutes pendant lesquelles un compte désactivé reste désactivé avant d'être automatiquement activé.

Cochez cette case pour activer le paramètre et entrez le nombre de minutes.

Réinitialiser le compte de verrouillage de compte après

Ce paramètre détermine le nombre de minutes qui doivent s'écouler à partir du moment où un utilisateur ne parvient pas à se connecter avant que le compteur de tentative de connexion en échec ne soit réinitialisé à zéro.

Cochez cette case pour activer le paramètre et entrez le nombre de minutes.

**Remarque!**

Si le nombre maximum de tentatives de connexion non valides est dépassé, le compte est désactivé.

Si la case à cocher **Durée de verrouillage du compte** n'est pas sélectionnée, le compte doit être activé manuellement.

Si la case à cocher **Durée de verrouillage du compte** est sélectionnée, le compte est automatiquement activé au terme du délai défini.

**Remarque!**

Le compteur de tentatives de connexion se remet à zéro :

Après une connexion réussie.

Ou au terme de la durée indiquée, si la case à cocher **Réinitialiser le compte de verrouillage de compte après** est sélectionnée.

Désactiver le client hors ligne

Cochez cette case pour désactiver la connexion à un client hors ligne.

Informations supplémentaires

À partir de BVMS 9.0, les paramètres **Stratégies de compte** suivants s'appliquent par défaut :

- La case **Stratégie de mot de passe fort** est présélectionnée.
- La case **Longueur minimum du mot de passe** est présélectionnée. La valeur par défaut est 10.
- La case **Âge maximum du mot de passe en jours** n'est pas présélectionnée. La valeur par défaut est de 90.
- La case **Nombre de mots de passe utilisés dans l'historique** n'est pas présélectionnée. La valeur par défaut est 10.

- La case **Nombre maximum de tentatives de connexion non valides** n'est pas présélectionnée. La valeur par défaut est de 1.
- La case **Désactiver le client hors ligne** n'est pas présélectionnée.

À compter de la version 10.0.1 de BVMS, les paramètres **Stratégies de compte** suivants sont sélectionnés par défaut pour tous les groupes d'utilisateurs :

- **Nombre maximum de tentatives de connexion non valides**
- **Durée de verrouillage du compte**
- **Réinitialiser le compte de verrouillage de compte après**

26.17.1

Operator Client hors ligne

Lorsque le Operator Client est hors ligne, les cas d'utilisation suivants sont possibles :

- Le Operator Client continue à assurer le fonctionnement de la visualisation en temps réel, de la lecture et de l'exportation sans qu'il soit connecté à l'ordinateur Management Server.
- Si un poste de commande a déjà été connecté à l'ordinateur Management Server, il peut s'y connecter à tout moment avec n'importe quel utilisateur tout en étant hors ligne.

Le mode hors ligne fonctionne uniquement avec BVMS version 3.0 ou ultérieure.

Si un poste de commande Operator Client est déconnecté de l'ordinateur Management Server, il est possible de continuer à travailler. Certaines des fonctions principales restent disponibles, par exemple l'affichage en temps réel et la lecture de vidéos.

À partir de la version BVMS5.5, un poste de commande Operator Client peut fonctionner hors ligne avec une configuration BVMS V5.0.5.

Remarque!

En cas de changement de mot de passe dans Management Server alors que Operator Client est hors ligne, ce changement n'est pas propagé à cet Operator Client.

Lorsque Operator Client est en ligne, l'utilisateur doit se connecter en utilisant le nouveau mot de passe.

Lorsque Operator Client est hors ligne, l'utilisateur doit de nouveau utiliser l'ancien mot de passe pour se connecter. Cela reste ainsi jusqu'à ce qu'une nouvelle configuration soit activée et transférée vers le poste de travail Operator Client.



Remarque!

Si une caméra est appelée pour affichage dans un groupe de moniteurs avec un clavier Bosch Intuikey connecté à un poste de commande, et si ce poste de commande est hors ligne, le clavier n'envoie pas de tonalité d'erreur.



26.17.1.1

Utilisation en mode hors ligne

Quand Operator Client est déconnecté d'un Management Server, l'icône correspondante



s'affiche en superposition dans l'arborescence logique sur le Management Server déconnecté. Vous pouvez continuer à travailler avec Operator Client, même si la déconnexion dure plus longtemps, mais certaines fonctions ne sont pas disponibles.

Si la connexion avec Management Server est rétablie, l'icône correspondante est affichée en superposition.

Si une nouvelle configuration sur Management Server n'a été activée, l'icône correspondante est affichée en superposition dans l'arborescence logique sur l'icône du serveur Management Server affecté, et une boîte de dialogue apparaît pendant quelques secondes. Acceptez ou refusez la nouvelle configuration.

Si votre instance de Operator Client a été paramétrée pour une déconnexion à un instant précis, cette déconnexion se produit même si la connexion à Management Server n'est pas rétablie à cet instant précis.

Si un utilisateur de Operator Client hors ligne se connecte via la Recherche de serveur, la liste des serveurs chargée lors de la dernière connexion s'affiche. L'état hors ligne signifie que le poste de commande Operator Client ne possède aucune connexion réseau au serveur contenant la liste des serveurs.

Fonctions non disponibles en mode déconnexion


Dans le cas d'une déconnexion de Management Server, les fonctions suivantes ne sont pas disponibles dans Operator Client :

- Liste des alarmes :
La gestion des alarmes n'est pas prise en charge. La liste des alarmes est vide et sera automatiquement renseignée lors de la reconnexion.
- Allegiant :
La gestion des lignes de jonction n'est pas possible. Dans les versions antérieures, les caméras Allegiant étaient fermées automatiquement et une boîte de message apparaissait lorsque la gestion d'une ligne de jonction n'était pas possible. Avec BVMS 3.0, le volet des images sera plus convivial et informera l'utilisateur de l'impossibilité d'afficher actuellement cette caméra.
- Groupe de moniteurs :
Il n'est pas possible de faire glisser les caméras vers la commande du groupe de moniteurs. La commande est désactivée et sera automatiquement activée lors de la reconnexion.
- Priorités PTZ :
Sans connexion à Management Server, un client Operator Client hors ligne peut connecter une caméra PTZ si la caméra elle-même n'est pas verrouillée. Les priorités de la caméra mobile sont automatiquement mises à jour lors de la reconnexion.
- Entrée :
L'entrée ne peut pas être commutée.
- Journal des connexions :
Le journal des connexions n'est pas disponible et ne peut pas être ouvert. Les fenêtres de recherche du journal des connexions ne se ferment pas automatiquement. Les résultats de recherche existants sont utilisables et exportables.
- Operator Client SDK :
Les fonctions d'Operator Client SDK avec une API IServer ne peuvent pas être traitées. La création d'une API RemoteClient n'est pas possible.
Certaines méthodes, uniquement disponibles au niveau de l'API du client, ne fonctionnent pas, par exemple ApplicationManager (try GetUserName()).
- Modification du mot de passe :
L'opérateur ne peut pas changer son mot de passe.
- Relais :
Les relais ne peuvent pas être commutés.
- Script de serveur :
Les méthodes de serveur de l'API IServer sont traitées mais ne peuvent pas être transmises au client :

- AlarmManager (gestionnaire d'alarmes)
- AnalogMonitorManager (gestionnaire de moniteurs analogiques)
- CameraManager (gestionnaire de caméra)
- CompoundEventManager (gestionnaire d'événements combinés)
- DecoderManager (gestionnaire de décodeur)
- DeviceManager (gestionnaire du dispositif)
- DomeCameraManager (gestionnaire de caméra mini-dôme)
- EventManager (gestionnaire d'événement)
- InputManager (gestionnaire d'entrée)
- LicenseManager (gestionnaire des licences)
- Logbook (journal des connexions)
- MatrixManager (gestionnaire de matrice)
- RecorderManager (gestionnaire d'enregistreur)
- RelayManager (gestionnaire de relais)
- ScheduleManager (gestionnaire de planification)
- SendManager (gestionnaire d'envoi)
- SequenceManager (gestionnaire de séquence)
- VirtualInputManager (gestionnaire des entrées virtuelles)
- Superpositions des états :
Aucun affichage d'états des caméras, entrées ou relais n'est disponible.

Affichage de l'état des dispositifs

Les états des dispositifs (point d'enregistrement, trop bruyant, trop sombre, ...) sont traités par le Management Server. En cas de déconnexion entre le client et le serveur, les états ne peuvent pas être mis à jour au niveau du client. Un nouvel affichage d'état vous indique visuellement que les états de tous les dispositifs ne sont pas disponibles pour le moment. Si la connexion entre le client et le serveur est rétablie, les états affichés en superposition sont mis à jour automatiquement.

-  État inconnu
Cette icône d'état est affichée au-dessus d'un dispositif dans l'arborescence logique ou sur une carte lorsque le client est déconnecté de l'ordinateur Management Server.


Raisons de déconnexion possibles

Les raisons possibles d'une déconnexion entre un Operator Client et un Management Server sont les suivantes :

- Connexion physique interrompue.
- Le mot de passe de l'utilisateur connecté a été modifié durant la période hors ligne.
- Le Management Server a accordé une licence flottante de poste de commande à un autre Operator Client en ligne pendant que l'Operator Client à présent déconnecté était hors ligne.
- Les versions de l'Operator Client et du Management Server sont différentes (Management Server antérieur à la version 5.5).

26.18

Autorisations de connexion par page de type d'application

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** > Onglet  > **Autorisations de l'application** > Onglet **Autorisations de connexion par type d'application**
ou votre



Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** > Onglet > **Autorisations de l'application** > Onglet **Autorisations de connexion par type d'application**

Permet de configurer diverses autorisations utilisateur pour les différentes applications.

Operator Client ou Cameo SDK (directement vers Management Server)

Cochez la case pour autoriser la connexion directe au Management Server de l'Operator Client ou à l'application Cameo SDK.

Operator Client (vers Unmanaged Site)

Cochez la case pour autoriser la connexion directe à l'application Operator Client en se connectant à un unmanaged site.

Configuration Client

Cochez cette case pour autoriser la connexion à l'application Configuration Client.

API de configuration

Cochez cette case pour autoriser la connexion à l'**API de configuration**.

Accès mobile via un navigateur Web

Cochez cette case pour autoriser l'accès mobile par le navigateur Web.

Accès mobile par Video Security Client

Cochez cette case pour autoriser l'accès mobile par le Video Security Client.

SDK du serveur BVMS / API du serveur

Cochez cette case pour autoriser la connexion à l'application SDK du serveur BVMS.

BVMS Client SDK (permet la connexion à Operator Client)

Cochez cette case pour autoriser la connexion à l'application Client SDK pour certains groupes d'utilisateurs.

26.19

Page des paramètres de gestion des menaces



Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** > Onglet > **Gestion des menaces** > Onglet **Paramètres**

Permet de configurer la modification ou non de l'adhésion à un groupe selon différents niveaux de menaces.

Remarque : En cas d'alarme du niveau de menace, l'utilisateur d'Operator Client actuel est déconnecté et l'Operator Client Operator Client redémarre. L'utilisateur doit se connecter à nouveau à l'Operator Client en mode de niveau de menace. Selon la configuration du groupe d'utilisateurs, l'utilisateur correspondant reçoit alors les autorisations du groupe d'utilisateurs configuré pour le niveau de menace actif.

Pour configurer un niveau de menace pour un groupe d'utilisateurs :

1. Sélectionnez le groupe d'utilisateurs.

2. Dans le menu déroulant du niveau de menace correspondant, sélectionnez le groupe d'utilisateurs qui doit être actif dans ce niveau de menace.

27

Configuration des utilisateurs, des autorisations et de l'accès d'entreprise

**Remarque!**

BVMS Viewer offre uniquement des fonctionnalités de base. Les fonctionnalités avancées sont incluses dans BVMS Professional. Pour de plus amples informations sur les différentes éditions BVMS, consultez le site www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).


Fenêtre principale > **Groupes d'utilisateurs**


Ce chapitre explique comment configurer des groupes d'utilisateurs, des Enterprise User Groups et des accès Enterprise.

Vous devez configurer toutes les autorisations de dispositif et d'exploitation par groupe d'utilisateurs et non par utilisateur.

Les règles suivantes sont applicables :

- Un utilisateur BVMS ne peut appartenir qu'à un seul groupe d'utilisateurs BVMS ou Enterprise User Group. Un utilisateur LDAP peut être membre de plusieurs groupes d'utilisateurs LDAP.
- Il est impossible de modifier les paramètres des groupes d'utilisateurs par défaut.
- Ces groupes d'utilisateurs ont accès à tous les dispositifs de l'arborescence logique complète et se voient affecter la planification **Toujours**.
- Pour accéder aux groupes d'utilisateurs Windows d'un domaine, il faut utiliser des groupes d'utilisateurs LDAP.

- Cliquez sur  pour enregistrer les paramètres.

- Cliquez sur  pour annuler le dernier paramètre.

- Cliquez sur  pour activer la configuration.

Stratégie de mot de passe fort

Pour améliorer la protection de votre ordinateur contre les accès non autorisés, il est recommandé d'utiliser des mots de passe forts pour les comptes utilisateur.

Par conséquent, une stratégie de mot de passe fort est appliquée par défaut pour tous les groupes d'utilisateurs nouvellement créés. Cela inclut le groupe d'utilisateurs admin, ainsi que les groupes d'utilisateurs standard, Enterprise User Group et Accès Enterprise.

Les règles suivantes sont applicables :

- Longueur minimale du mot de passe défini dans la page **Stratégies de compte** pour le groupe d'utilisateurs approprié.
- Ne pas utiliser l'un des mots de passe précédents.
- Utiliser au moins une lettre majuscule (A à Z).
- Utiliser au moins un chiffre (0 à 9).
- Utiliser au moins un caractère spécial (Exemple : ! \$ # %).

Lorsque l'utilisateur Admin démarre Configuration Client pour la première fois, la boîte de dialogue **Violation de la politique de mot de passe** s'affiche et l'invite à définir un mot de passe pour le compte utilisateur Admin. Nous vous recommandons fortement de conserver ce paramètre et de définir un mot de passe sécurisé pour le compte utilisateur Admin, dans le respect des règles de la politique de mot de passe.

Lors de la création de nouveaux groupes d'utilisateurs dans Configuration Client, la stratégie de mot de passe fort est activée par défaut. Si vous ne définissez aucun mot de passe pour les nouveaux comptes utilisateur du groupe d'utilisateurs approprié, vous ne pouvez pas activer la configuration. La boîte de dialogue **Violation de la politique de mot de passe** s'affiche et répertorie tous les utilisateurs pour lesquels aucun mot de passe n'a été défini.

Pour activer la configuration, définissez les mots de passe manquants.

Se reporter à

- Page *Stratégies de compte*, page 358
- Page *Propriétés du groupe d'utilisateurs*, page 343
- Page *Propriétés de l'utilisateur*, page 344
- Page *Propriétés de combinaison de connexion*, page 345
- Page *Autorisations de caméra*, page 346
- Page *Priorité des commandes*, page 347
- Boîte de dialogue *Copier les autorisations du groupe d'utilisateurs*, page 348
- Page *Autorisations de décodeur*, page 348
- Page *Événements et alarmes*, page 349
- Boîte de dialogue *Paramètres du serveur LDAP (menu Paramètres)*, page 117
- Page *d'identifiants*, page 349
- Page *Arborescence Logique*, page 350
- Page *des fonctionnalités d'Operator*, page 350
- Page *Priorités*, page 354
- Page *Interface utilisateur*, page 354
- Page *Accès au serveur*, page 355

27.1 Créer un groupe ou un compte

Fenêtre principale > **Groupes d'utilisateurs**


Vous pouvez créer un groupe d'utilisateurs standard, un Enterprise User Group ou un Enterprise Account.

Pour adapter les autorisations d'un groupe d'utilisateurs à vos besoins, vous devez créer un nouveau groupe d'utilisateurs et modifier ses paramètres.

27.1.1 Création d'un groupe d'utilisateurs standard

Fenêtre principale > **Groupes d'utilisateurs**

Pour créer un groupe d'utilisateurs standard :

1. Cliquez sur l'onglet **Groupes d'utilisateurs**.
2. Cliquez sur .
La boîte de dialogue **Nouveau groupe d'utilisateurs** s'affiche.
3. Tapez le nom et une description.
4. Cliquez sur **OK**.
Un nouveau groupe est ajouté à l'arborescence correspondante.
5. Cliquez avec le bouton droit de la souris sur ce nouveau groupe, puis cliquez sur **Renommer**.
6. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.

Se reporter à

- Page *Propriétés du groupe d'utilisateurs*, page 343
- Page *des fonctionnalités d'Operator*, page 350

- Page *Priorités*, page 354
- Page *Interface utilisateur*, page 354

27.1.2

Création d'un Enterprise User Group

Fenêtre principale > **Groupes d'utilisateurs**

Vous effectuez la tâche suivante : créer un Enterprise User Group pour un Enterprise System sur le Enterprise Management Server.

Vous créez un Enterprise User Group avec les utilisateurs pour configurer leurs autorisations d'exploitation. Ces autorisations d'exploitation sont disponibles sur un Operator Client qui est connecté à l'Enterprise Management Server. L'interface utilisateur du moniteur d'alarme est un exemple d'autorisation d'exploitation.

Pour créer un Enterprise User Group :

1. Cliquez sur l'onglet **Enterprise User Groups**.
Remarque : L'onglet **Enterprise User Groups** est disponible uniquement si la licence appropriée est disponible, et si un ou plusieurs ordinateurs Management Server sont configurés dans **Périphériques > Enterprise System > Liste de serveurs / Carnet d'adresses**.
2. Cliquez sur .
La boîte de dialogue **Nouveau groupe d'utilisateurs Enterprise** s'affiche.
3. Tapez le nom et une description.
4. Cliquez sur **OK**.
Le Enterprise User Group est ajouté à l'arborescence correspondante.
5. Cliquez avec le bouton droit de la souris sur le groupe Enterprise, puis cliquez sur **Renommer**.
6. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.
7. Dans la page **Autorisations d'utilisation**, configurez les autorisations d'exploitation et l'accès aux serveurs des ordinateurs Management Server configurés, comme cela est requis.

Se reporter à

- Page *Propriétés du groupe d'utilisateurs*, page 343
- Page *des fonctionnalités d'Operator*, page 350
- Page *Priorités*, page 354
- Page *Interface utilisateur*, page 354
- Page *Accès au serveur*, page 355

27.1.3

Création d'un Enterprise Account

Fenêtre principale > **Groupes d'utilisateurs**




Remarque!

Au moins un dispositif doit être configuré dans l'arborescence des dispositifs pour que vous puissiez ajouter un Enterprise Account.

Vous effectuez la tâche suivante : créer un Enterprise Account sur un Management Server. Répétez cette tâche sur chaque Management Server membre de votre Enterprise System. Vous pouvez créer un Enterprise Account pour configurer les autorisations du dispositif pour un Operator Client à l'aide de Enterprise System.

Pour créer un Enterprise Account:

1. Cliquez sur l'onglet **Accès Enterprise**.
2. Cliquez sur .
La boîte de dialogue **Nouveau compte Enterprise Account** s'affiche.
3. Tapez le nom et une description.
4. La case **L'utilisateur doit changer le mot de passe lors de la prochaine connexion** est présélectionnée pour tous les nouveaux comptes utilisateur créés.
Saisissez la clé en suivant les règles de clé et confirmez cette clé.
5. Cliquez sur **OK**.
Un nouvel Enterprise Account est ajouté à l'arborescence correspondante.
6. Cliquez avec le bouton droit de la souris sur le nouvel Enterprise Account, puis cliquez sur **Renommer**.
7. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.
8. Dans la page **Autorisations du périphérique**, configurez les identifiants et les autorisations de dispositif comme il convient.

Se reporter à

- *Stratégie de mot de passe fort*, page 365
- *Page d'identifiants*, page 349
- *Page Arborescence Logique*, page 350
- *Page Événements et alarmes*, page 349
- *Page Priorité des commandes*, page 347
- *Page Autorisations de caméra*, page 346
- *Page Autorisations de décodeur*, page 348

27.2

Création d'un utilisateur

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs**
ou


Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups**



Un utilisateur est ajouté en tant que membre d'un groupe d'utilisateurs standard ou d'un Enterprise User Group existant.

**Remarque!**

Un utilisateur souhaitant utiliser un clavier IntuiKey de Bosch connecté à un décodeur doit posséder un nom d'utilisateur et un mot de passe composés de chiffres uniquement. Le nom d'utilisateur peut comporter un maximum de 3 chiffres et le mot de passe, un maximum de 6 chiffres.

Pour créer un utilisateur :

1. Sélectionnez un groupe et cliquez sur  ou cliquez avec le bouton droit sur le groupe souhaité et cliquez sur **Nouvel utilisateur**.
Un nouvel utilisateur est ajouté à l'arborescence **Groupes d'utilisateurs**.
2. Cliquez avec le bouton droit de la souris sur le nouvel utilisateur, puis cliquez sur **Renommer**.
3. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.
4. Sur la page **Propriétés de l'utilisateur**, saisissez le nom d'utilisateur et une description.

5. La case à cocher **L'utilisateur doit changer le mot de passe lors de la prochaine connexion** est présélectionnée pour tous les comptes utilisateur nouvellement créés. Saisissez le mot de passe en fonction des règles de la politique de mot de passe et confirmez ce mot de passe.
6. Cliquez sur **Appliquer** pour appliquer les paramètres.
7. Cochez la case **Le compte est activé** pour activer le compte utilisateur.
8. Cliquez sur  pour activer le mot de passe.
9. Cliquez sur  pour activer la configuration.

Remarque : Après l'ajout d'un nouvel utilisateur, vous devez toujours activer la configuration.

Se reporter à

- Page *Propriétés de l'utilisateur*, page 344
- *Stratégie de mot de passe fort*, page 365
- Page *Groupes d'utilisateurs*, page 341

27.3

Création d'un groupe de double autorisation

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs**
ou


Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups**

Vous pouvez créer une double autorisation pour un groupe d'utilisateurs standard ou un Enterprise User Group.

Pour un accès Enterprise, la double autorisation n'est pas disponible.

Sélectionnez deux groupes d'utilisateurs. Les membres de ces groupes d'utilisateurs sont membres du nouveau groupe de double autorisation.


Pour créer un groupe de double autorisation :

1. Cliquez sur .
La boîte de dialogue **Nouveau groupe de double autorisation** ou **Nouveau groupe de double autorisation Enterprise** s'affiche.
2. Saisissez un nom et une description.
3. Cliquez sur **OK**.
Un nouveau groupe de double autorisation est ajouté à l'arborescence correspondante.
4. Cliquez avec le bouton droit de la souris sur le nouveau groupe de double autorisation, puis cliquez sur **Renommer**.
5. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.

Se reporter à


- *Ajout d'une combinaison de connexion au groupe de double autorisation*, page 370
- Page *Propriétés du groupe d'utilisateurs*, page 343
- Page *des fonctionnalités d'Operator*, page 350
- Page *Priorités*, page 354
- Page *Interface utilisateur*, page 354

27.4 Ajout d'une combinaison de connexion au groupe de double autorisation

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** > 
Nouveau groupe de double autorisation

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** > 
Nouveau groupe de double autorisation Enterprise


Pour ajouter une combinaison de connexion à un groupe de double autorisation :

1. Sélectionnez le groupe de double autorisation souhaité, puis cliquez sur  ou cliquez avec le bouton droit de la souris sur le groupe, puis cliquez sur **Nouvelle combinaison de connexion**.
La boîte de dialogue correspondante s'affiche.
2. Sélectionnez un groupe d'utilisateurs dans chacune des listes.
Les utilisateurs du premier groupe d'utilisateurs doivent se connecter dans la première boîte de dialogue d'ouverture de session ; les utilisateurs du deuxième groupe d'utilisateurs confirment la connexion.
Il est possible de sélectionner le même groupe dans les deux listes.
3. Pour chaque groupe, sélectionnez **Forcer la double autorisation** si nécessaire.
Lorsque la case de cette option est cochée, chaque utilisateur du premier groupe ne peut se connecter que simultanément avec un utilisateur du second groupe.
Lorsque la case de cette option n'est pas cochée, chaque utilisateur du premier groupe peut se connecter individuellement, mais il bénéficiera uniquement des droits d'accès de son groupe.
4. Cliquez sur **OK**.
Une nouvelle combinaison de connexion est ajoutée au groupe de double autorisation approprié.
5. Cliquez avec le bouton droit de la souris sur la nouvelle combinaison de connexion, puis cliquez sur **Renommer**.
6. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.

Se reporter à


- *Création d'un groupe de double autorisation, page 369*
- *Page Propriétés de combinaison de connexion, page 345*

27.5 Configuration du groupe admin.

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs**  Groupe admin.


Permet d'ajouter de nouveaux utilisateurs admin au groupe Admin, de renommer les utilisateurs admin et de retirer des utilisateurs du groupe Admin.

Pour ajouter un nouvel utilisateur admin au groupe Admin :

1. Cliquez sur  ou cliquez avec le bouton droit de la souris sur Groupe admin. et sélectionnez **Ajouter un utilisateur**.
Un nouvel utilisateur admin est ajouté au Groupe admin.
2. Sur la page **Propriétés de l'utilisateur**, saisissez le nom d'utilisateur et une description.


3. La case **L'utilisateur doit changer le mot de passe lors de la prochaine connexion** est présélectionnée pour tous les nouveaux comptes utilisateur créés. Saisissez le mot de passe en suivant les règles de mot de passe et confirmez ce mot de passe.

4. Cliquez sur **Appliquer** pour appliquer les paramètres.

5. Cliquez sur  pour activer le mot de passe.

Pour renommer un utilisateur admin :

1. Cliquez avec le bouton droit de la souris sur l'utilisateur admin de votre choix, puis cliquez sur **Renommer**.
2. Saisissez le nouveau nom, puis appuyez sur ENTRÉE.

3. Cliquez sur  pour activer les modifications de nom d'utilisateur.

Pour retirer un utilisateur admin du groupe Admin :

- ▶ Cliquez avec le bouton droit de la souris sur l'utilisateur admin de votre choix et cliquez sur **Supprimer**.

L'utilisateur admin est retiré du Groupe admin.

Remarque :

Vous pouvez retirer un utilisateur admin du groupe Admin uniquement si d'autres utilisateurs admin existent.

S'il existe un seul utilisateur admin dans le groupe Admin, il ne peut pas être retiré.


Se reporter à

- *Page Groupes d'utilisateurs, page 341*
- *Page Propriétés de l'utilisateur, page 344*
- *Stratégie de mot de passe fort , page 365*

27.6

Sélectionner un groupe LDAP associé

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations d'utilisation** > Onglet **Propriétés du groupe d'utilisateurs**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Autorisations d'utilisation** > Onglet **Propriétés du groupe d'utilisateurs Enterprise**
Vous configurez des groupes LDAP dans des groupes d'utilisateurs standard ou des Enterprise User Groups.

Pour sélectionner un groupe LDAP associé :

1. Cliquez sur le bouton **Rechercher des groupes**.
2. Dans la liste **Groupe LDAP associé**, sélectionnez le groupe LDAP respectif.


Pour de plus amples informations sur les différents champs, cliquez ci-dessous sur le lien de la fenêtre concernée.

Se reporter à

- *Boîte de dialogue Paramètres du serveur LDAP (menu Paramètres), page 117*
- *Page Propriétés du groupe d'utilisateurs, page 343*

27.7 Planification des autorisations de connexion utilisateur

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations d'utilisation** > Onglet **Propriétés du groupe d'utilisateurs**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Autorisations d'utilisation** > Onglet **Propriétés du groupe d'utilisateurs Enterprise**
Vous pouvez limiter les périodes auxquelles les membres d'un groupe d'utilisateurs ou d'un groupe Enterprise User Group peuvent ouvrir une session sur leur ordinateur.
Il est impossible de modifier ces paramètres pour les groupes d'utilisateurs par défaut.

Pour planifier des périodes de connexion :

1. Cliquez sur l'onglet **Propriétés du groupe d'utilisateurs**.
2. Dans la liste **Planification de connexion**, sélectionnez une planification.

27.8 Configuration des autorisations d'exploitation

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** >  >
Onglet **Autorisations d'utilisation** > Onglet **Propriétés du groupe d'utilisateurs**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups** >  >
Onglet **Autorisations d'utilisation** > Onglet **Propriétés du groupe d'utilisateurs Enterprise**

- Vous pouvez configurer des autorisations d'exploitation, telles que l'accès au journal des connexions ou les paramètres de l'interface utilisateur.
- Il est impossible de modifier ces paramètres pour les groupes d'utilisateurs par défaut.
- Vous pouvez configurer les autorisations d'exploitation dans les groupes d'utilisateurs standard ou les Enterprise User Groups.

Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Pour de plus amples informations sur les différents champs, cliquez ci-dessous sur le lien de la fenêtre concernée.

Se reporter à

- *Page Propriétés du groupe d'utilisateurs, page 343*
- *Page des fonctionnalités d'Operator, page 350*
- *Page Priorités, page 354*
- *Page Interface utilisateur, page 354*
- *Page Accès au serveur, page 355*

27.9 Configuration des autorisations d'utilisation des dispositifs

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs** > Onglet **Autorisations du périphérique**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Accès Enterprise** > Onglet **Autorisations du périphérique**

Vous pouvez définir les autorisations des dispositifs de l'arborescence logique indépendamment les uns des autres.

Lorsque des dispositifs autorisés ont été déplacés vers un dossier non accessible à un groupe d'utilisateurs, vous devez définir les autorisations qui permettront d'accéder aux dispositifs de ce dossier.

- Il est impossible de modifier ces paramètres pour les groupes d'utilisateurs par défaut.
- Vous pouvez configurer les autorisations d'utilisation de dispositifs dans les groupes d'utilisateurs standard ou les comptes Entreprise.

Pour de plus amples informations sur les différents champs, consultez la rubrique de l'aide en ligne portant sur la fenêtre concernée de l'application.

Pour de plus amples informations sur les différents champs, cliquez ci-dessous sur le lien de la fenêtre concernée.

Se reporter à

- *Page Arborescence Logique, page 350*
- *Page Événements et alarmes, page 349*
- *Page Priorité des commandes, page 347*
- *Page Autorisations de caméra, page 346*
- *Page Autorisations de décodeur, page 348*

27.10

Configuration de priorités diverses

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups**
ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Accès Entreprise**

Vous pouvez configurer les priorités suivantes :

- Pour les groupes d'utilisateurs standard et **Enterprise User Groups** : vous pouvez configurer les priorités d'alarme pour le Mode Temps Réel et le Mode Lecture.
- Pour les groupes d'utilisateurs standard et **Accès Entreprise** : vous pouvez définir les priorités relatives à la prise des commandes de balayage horizontal/vertical et de zoom et des lignes de jonction Bosch Allegiant.

Vous pouvez configurer un laps de temps pour le verrouillage des commandes de balayage horizontal/vertical et de zoom (un utilisateur bénéficiant d'un niveau de priorité supérieur peut ainsi prendre le contrôle de la caméra d'un utilisateur doté d'un niveau de priorité inférieur et en verrouiller les commandes pendant la durée spécifiée).

Pour configurer les priorités des modes Temps réel et Lecture :

1. Sélectionnez un groupe d'utilisateurs standard Enterprise User Group.
2. Cliquez sur **Autorisations d'utilisation**.
3. Cliquez sur l'onglet **Priorités**.
4. Dans le champ **Comportement contextuel automatique**, déplacez les curseurs comme il convient.

Pour configurer les priorités relatives à la prise des commandes de balayage horizontal/vertical et de zoom et des lignes de jonction Bosch Allegiant :

1. Sélectionnez un groupe d'utilisateurs standard Enterprise Account.
2. Cliquez sur onglet **Autorisations du périphérique**.
3. Cliquez sur l'onglet **Priorités des commandes**.
4. Dans le champ **Priorités des commandes**, déplacez les curseurs comme il convient.
5. Dans la liste **Temps d'attente en min.**, sélectionnez l'entrée appropriée.

Se reporter à

- Page *Priorité des commandes*, page 347
- Page *Priorités*, page 354

27.11

Copie des autorisations d'un groupe d'utilisateurs

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Groupes d'utilisateurs**

ou

Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Enterprise User Groups**

ou


Fenêtre principale > **Groupes d'utilisateurs** > Onglet **Accès Enterprise**

Vous pouvez copier les autorisations d'un groupe ou compte à un autre. Vous devez avoir configuré au moins 2 groupes ou comptes.

Pour copier les autorisations :

1. Dans l'arborescence Groupes d'utilisateurs, sélectionnez un groupe ou un compte.



2. Cliquez sur  .

La boîte de dialogue **Copier les autorisations du groupe d'utilisateurs** s'affiche.

3. Sélectionnez les autorisations appropriées et le groupe ou compte cible approprié.
4. Cliquez sur **OK**. Les permissions de groupe de ce groupe sont copiées dans l'autre groupe ou compte. La boîte de dialogue se ferme.

28 Page Audit Trail



Remarque!

BVMS Viewer offre uniquement des fonctionnalités de base. Les fonctionnalités avancées sont incluses dans BVMS Professional. Pour de plus amples informations sur les différentes éditions BVMS, consultez le site www.boschsecurity.com et le BVMS Guide de sélection rapide : [Guide de sélection rapide de BVMS](#).

Fenêtre principale > **Audit Trail**

Cette fonction de Audit Trail vous permet de suivre toutes les modifications apportées à la configuration du système et d'exporter les données dans un fichier CSV.



Exigences préalables :

1. Installez la base de données Audit Trail en la sélectionnant dans la configuration BVMS (option de configuration en option).
2. Vous disposez de l'autorisation suivante : **Afficher la page Audit Trail**.
3. Audit Trail est activé sous **Paramètres > Options > Paramètres Audit Trail**.

Recommandations :

- N'activez pas la fonction Audit Trail depuis le début car la journalisation est étendue.
- Avant de réaliser la configuration initiale du système, créez des rapports pour la mise en service, puis activez la Audit Trail pour consigner les modifications supplémentaires.
- Pour les importations de configuration, désactivez également la fonction Audit Trail.

Pour étendre/réduire les données de la Audit Trail :

1. Cliquez sur  pour développer un nœud de données.
2. Cliquez sur  pour réduire un nœud de données.
3. Cliquez sur **Développer tout / Tout réduire** pour développer/réduire tous les nœuds de données chargés.

Pour charger les données de la Audit Trail :

- ▶ Cliquez sur **Charger plus**.

Remarque : Lorsque vous cliquez sur le bouton **Charger plus**, vous ne chargez que dix nœuds de données à la fois.

Pour exporter les données de la Audit Trail :

- ▶ Cliquez sur **Exporter** pour enregistrer les données chargées dans un fichier CSV.

Remarque : Seules les données chargées seront exportées.

Se reporter à

- *Boîte de dialogue Options (menu Paramètres), page 122*
- *Page Autorisations de configuration, page 356*

28.1 Détails de la journalisation pour Audit Trail

Remarque : Si l'espace disponible dans la base de données est insuffisant, les données les plus anciennes seront supprimées automatiquement. Lorsque la durée de conservation arrive à expiration, ces entrées sont automatiquement supprimées.

Le tableau de la Audit Trail contient les colonnes suivantes :

Action	La modification qui a été déclenchée par l'utilisateur.
Créé	Un nouvel objet a été ajouté à la configuration BVMS, par exemple une caméra ou un utilisateur.
Modifié	Un objet existant dans la configuration a été modifié, par exemple le nom d'affichage d'une caméra.
Supprimé	Un objet existant dans la configuration a été supprimé.
Élément ajouté à la liste	Un objet a été ajouté à la liste, par exemple une caméra a été ajoutée à un pool VRM.
Élément de liste supprimé	Un objet a été retiré d'une liste, par exemple, une caméra a été retirée d'un pool VRM ou d'un VSG.
Type d'objet	Type de l'objet de configuration qui a été modifié.
Objet	Objet qui a été modifié, par exemple une caméra, un utilisateur, une planification.
Adresse réseau	Adresse réseau de l'objet, le cas échéant.
Contexte objet 1 / Contexte objet 2	Contexte de l'élément modifié, généralement un ancêtre de l'objet. Par exemple : une cible d'un dispositif iSCSI est ajoutée. Le contexte 1 du périphérique est le dispositif iSCSI parent, le contexte 2 est VRM, auquel le dispositif iSCSI appartient.
Propriété	Nom de la propriété qui a été modifiée.
Ancienne valeur	Ancienne valeur avant le déclenchement de la modification.
Nouvelle valeur	Nouvelle valeur définie lors de la modification.
Contexte 1 / Contexte 2	Contexte supplémentaire décrivant la modification. Par exemple, si vous modifiez les paramètres d'une caméra dans les options d'alarme d'une alarme, cette caméra sera ajoutée comme contexte.

28.2

Boîte de dialogue de filtre Audit Trail

La boîte de dialogue de filtre permet de filtrer ou de rechercher des informations spécifiques dans la base de données de la Audit Trail.

La boîte de dialogue comporte les filtres prédéfinis suivants :

- Catégorie
- Action
- Période

Si vous sélectionnez plusieurs catégories ou actions dans la boîte de dialogue de filtre, toutes ces sections sont incluses dans votre recherche.

Il est également possible d'entrer des chaînes en texte libre dans le champ de recherche, ce qui vous permet de filtrer pour des utilisateurs, dispositifs ou paramètres spécifiques, par exemple. Si vous entrez plusieurs termes de recherche, le résultat doit contenir tous les mots entrés dans le champ de recherche.

Vous pouvez utiliser des guillemets pour des termes qui contiennent un blanc, par exemple : "Camera 1".


Exemple :

Vous sélectionnez les catégories **Dispositifs** et **Cartes et structure**, puis vous entrez le nom de la caméra "Cam1" et le nom d'utilisateur "X" dans le champ de texte libre.

Résultat : la base de données Audit Trail recherche toutes les modifications apportées par l'utilisateur "X" aux objets de configuration de la caméra "Cam1", qui figurent dans

Dispositifs ou dans **Cartes et structure**.

Pour utiliser le filtre Audit Trail :

1. Cliquez sur **Filtrer**.
La boîte de dialogue de filtre Audit Trail s'ouvre.
2. Après avoir filtré la configuration, cliquez sur **Appliquer**.
3. Cliquez sur  pour supprimer les objets à un seul filtre.
4. Cliquez sur **Réinitialiser tous les filtres** pour réinitialiser la configuration complète de votre filtre.

29 Configuration de la détection incendie basée sur la vidéo

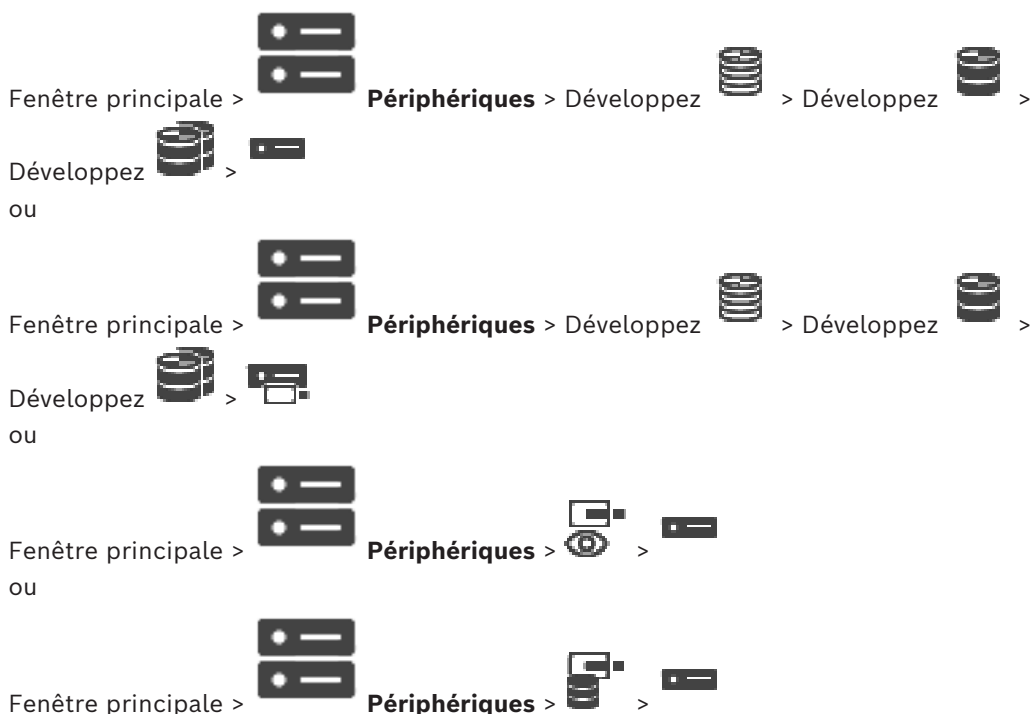
Pour configurer une alarme incendie basée sur la vidéo, vous devez effectuer les opérations suivantes :

1. Configurez une détection incendie sur votre caméra de détection incendie.
Utilisez la page Web de la caméra pour cette configuration.
Pour plus d'informations sur la configuration d'une caméra de détection incendie, reportez-vous à :
 - *Configuration d'une caméra de détection incendie, page 378*
2. Ajoutez cette caméra de détection incendie au système. Vous pouvez ajouter la caméra de détection incendie à une zone de stockage VRM, sous la forme d'un encodeur en temps réel uniquement ou d'un encodeur pour stockage local.
Pour plus d'informations sur l'ajout d'une caméra, reportez-vous à :
 - *Ajout d'un encodeur à une zone de stockage VRM, page 225*
 - *Ajout d'un encodeur temps réel uniquement, page 225*
 - *Ajout d'un encodeur pour stockage local, page 225*
3. Configurez un événement d'incendie pour cette caméra.
 - *Configuration d'un événement d'incendie, page 381*
4. Configurez l'alarme pour l'événement d'incendie.
 - *Configuration d'une alarme incendie, page 381*

Se reporter à

- *Ajout d'un encodeur à une zone de stockage VRM, page 379*
- *Ajout d'un encodeur temps réel uniquement, page 225*
- *Ajout d'un encodeur pour stockage local, page 225*
- *Configuration d'un événement d'incendie, page 381*
- *Configuration d'une alarme incendie, page 381*

29.1 Configuration d'une caméra de détection incendie



Pour configurer une alarme incendie basée sur la vidéo, vous devez d'abord configurer la détection incendie sur la caméra de détection incendie.

Pour plus d'informations, consultez le manuel d'utilisation de votre caméra de détection incendie.

Pour procéder à une configuration :

1. Cliquez avec le bouton droit de la souris sur l'icône du dispositif, puis cliquez sur **Afficher la page Web dans le navigateur**.
2. Cliquez sur **Configuration**.
3. Dans le volet de navigation, développez **Alarme**, puis cliquez sur **Détection d'incendie**.
4. Sélectionnez les différents paramètres.

29.2

Ajout d'un encodeur à une zone de stockage VRM

Pour ajouter des encodeurs à une zone de stockage VRM, voir *Ajout d'encodeurs via un balayage*, page 183.


Se reporter à

- *Ajout d'un dispositif*, page 127


29.3

Ajout d'encodeurs via un balayage

Pour ajouter un encodeur via un balayage :


1. Cliquez avec le bouton droit de la souris sur , puis cliquez sur **Rechercher des encodeurs**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Sélectionnez les encodeurs appropriés, sélectionnez la zone de stockage VRM souhaitée, puis cliquez sur **Affecter** pour les affecter à la zone de stockage VRM.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit de la souris sur ce champ, puis cliquez sur **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions réussies sont indiquées par .

Les connexions qui ont échoué sont indiquées par .


5. Cliquez sur **Terminer**.

L'élément est ajouté dans l'arborescence des dispositifs.

L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

29.4 Ajout de dispositifs temps réel uniquement via un balayage


Pour ajouter des dispositifs Bosch en temps réel uniquement via un balayage :

1. Cliquez avec le bouton droit de la souris sur  , puis cliquez sur **Rechercher des encodeurs en temps réel uniquement**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Cochez les boîtes de dialogue des dispositifs que vous souhaitez ajouter.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit de la souris sur ce champ, puis cliquez sur **Copier la cellule dans la colonne**.

Dans la colonne **État**, les connexions réussies sont indiquées par  .

Les connexions qui ont échoué sont indiquées par  .


5. Cliquez sur **Terminer**.
L'élément est ajouté dans l'arborescence des dispositifs.

L'icône  indique une erreur que vous devez corriger. Consultez l'info-bulle pour obtenir de plus amples informations sur l'erreur en question.

29.5 Ajout d'encodeurs à stockage local via un balayage

Fenêtre principale > **Périphériques** > Développez  >  .
Permet d'ajouter et de configurer des encodeurs à stockage local.

Pour ajouter des encodeurs à stockage local via un balayage :

1. Dans l'arborescence des dispositifs, cliquez avec le bouton droit de la souris sur  et cliquez sur **Rechercher les encodeurs à stockage local**.
La boîte de dialogue **BVMS Scan Wizard** s'affiche.
2. Cochez les boîtes de dialogue des dispositifs que vous souhaitez ajouter.
3. Cliquez sur **Suivant >>**.
La boîte de dialogue **Authentifier les dispositifs** de l'Assistant s'affiche.
4. Saisissez le mot de passe de chaque dispositif protégé par mot de passe.
La vérification du mot de passe est effectuée automatiquement lorsqu'il n'y a pas de saisie de caractère supplémentaire dans le champ du mot de passe pendant quelques secondes ou lorsque vous cliquez à l'extérieur de ce champ.
Si les mots de passe de tous les dispositifs sont identiques, vous pouvez le saisir dans le premier champ **Mot de passe**. Cliquez ensuite avec le bouton droit de la souris sur

ce champ, puis cliquez sur **Copier la cellule dans la colonne**.



Dans la colonne **État**, les connexions réussies sont indiquées par



Les connexions qui ont échoué sont indiquées par

5. Cliquez sur **Terminer**.

L'élément est ajouté dans l'arborescence des dispositifs.

29.6

Configuration d'un événement d'incendie



Fenêtre principale > **Événements**

Pour procéder à une configuration :

1. Dans l'arborescence, sélectionnez **Encodeurs/décodeurs > Caméra > État d'incendie ou de fumée > Détection d'incendie ou de fumée**.

Le Tableau de configuration des événements correspondant s'affiche.

2. Dans la colonne **Déclencher l'alarme- Planification**, cliquez sur une cellule, puis sélectionnez la planification appropriée.

La planification détermine le moment où l'alarme est déclenchée.

Sélectionnez l'une des Planifications d'enregistrement ou Planifications des tâches que vous avez configurées dans la page **Planifications**.

3. Sélectionnez les paramètres appropriés.

Remarque : vous pouvez utiliser la même procédure pour les autres événements d'incendie disponibles.

29.7

Configuration d'une alarme incendie

Fenêtre principale > **Alarmes**

Pour procéder à une configuration :

1. Dans l'arborescence, sélectionnez **Encodeurs/décodeurs > Caméra > État d'incendie ou de fumée > Détection d'incendie ou de fumée**.

Le Tableau de configuration des alarmes correspondant s'affiche.

2. Sélectionnez les paramètres appropriés.

30

Configuration de MIC IP 7000 connecté à VIDEOJET connect 7000

Pour utiliser une caméra MIC IP 7000 connectée à un VIDEOJET connect 7000, vous devez effectuer la configuration suivante.

Avant d'ajouter la caméra MIC IP à BVMS, effectuez les tâches suivantes :

1. Réinitialisez les paramètres par défaut de la caméra MIC IP 7000 et du dispositif VIDEOJET connect 7000 sur la page Web de chaque dispositif.
2. Réglez la caméra MIC IP 7000 sur la variante **MIC IP Starlight 7000 HD-VJC-7000**.
3. Configurez la caméra MIC IP 7000 et dispositif VIDEOJET connect 7000 selon la documentation fournie avec les dispositifs.
4. Si vous souhaitez utiliser ANR, exécutez l'utilitaire de configuration de l'ANR pour le dispositif VIDEOJET connect 7000.

Effectuez cette tâche sur un ordinateur appartenant au même réseau que le dispositif VIDEOJET connect 7000.

L'utilitaire de configuration de l'ANR se trouve sur la page du catalogue de produits du dispositif VIDEOJET connect 7000.

Effectuez cette procédure pour ajouter et configurer la caméra MIC IP 7000 dans BVMS :

1. Dans l'arborescence des dispositifs, ajoutez uniquement la caméra MIC IP 7000. Vous ne pouvez pas ajouter le dispositif VIDEOJET connect 7000 à BVMS.
2. Cliquez avec le bouton droit de la souris sur la caméra qui vient d'être ajoutée, puis cliquez sur **Modifier l'encodeur**.

La boîte de dialogue **Modifier l'encodeur** s'affiche.

Les fonctions du dispositif sont récupérées automatiquement selon la variante configurée ci-dessus.

3. Si nécessaire, configurez l'ANR sur la page **Caméras et enregistrement**.

31

Dépannage

Ce chapitre explique comment résoudre les problèmes connus dans le cadre de l'utilisation de BVMS Configuration Client.

Problèmes rencontrés lors de l'installation

Problème	Cause	Solution
Dans le programme d'installation, certains caractères ne s'affichent pas correctement.	Le choix de langue dans Windows n'est pas correct.	<i>Configuration de la langue dans Windows, page 385</i>
Le programme d'installation s'interrompt, puis indique que le serveur OPC ne peut être installé.	Les fichiers du serveur OPC ne peuvent pas être écrasés.	Désinstallez OPC Core Components Redistributable et recommencez l'installation de BVMS.
Le logiciel ne peut être désinstallé via le programme d'installation.		Démarrez Control Panel > Add/Remove Programs et désinstallez BVMS.

Problèmes rencontrés immédiatement après le lancement de l'application

Problème	Cause	Solution
BVMS ne s'affiche pas dans la bonne langue.	Windows n'utilise pas la langue de votre choix.	<i>Configuration de la langue de Configuration Client, page 73</i> ou <i>Configuration de la langue de Operator Client, page 73</i>
La boîte de dialogue de connexion de Operator Client ne s'affiche pas dans la bonne langue.	Même si vous avez changé la langue pour Operator Client dans Configuration Client, la langue de la boîte de dialogue de connexion de Operator Client dépend de la langue choisie pour Windows.	<i>Configuration de la langue dans Windows, page 385</i>

Problèmes relatifs à la langue d'affichage

Problème	Cause	Solution
Certains textes d'affichage de Configuration Client ou Operator Client sont rédigés dans une langue étrangère, généralement l'anglais.	La langue du système d'exploitation de l'ordinateur sur lequel le Management Server est installé est souvent l'anglais. Par conséquent, lorsque la base de données du BVMS est générée sur cet ordinateur, bon nombre d'affichages texte sont créés en anglais. Ils restent	N'y changez rien.

Problème	Cause	Solution
	inchangés quelle que soit la langue de Windows sur l'ordinateur Operator Client. Pour éviter ces interférences de langue, installez le logiciel Management Server sur un ordinateur doté de la langue d'interface Windows voulue.	

Problèmes avec le clavier numérique IntuiKey de Bosch

Problème	Cause	Solution
Le clavier numérique IntuiKey de Bosch déclenche une alarme et l'affichage des touches programmables indique Off Line.	La connexion au poste de commande est perdue. Le câble est endommagé/débranché ou le poste de commande a été réinitialisé.	<i>Rétablissement de la connexion à un clavier numérique IntuiKey de Bosch, page 385</i>

Problèmes dans les paramètres de commande d'enregistrement de votre carte son

Problème	Cause	Solution
L'effet Larsen apparaît lors de l'utilisation d'un microphone pour la fonction Intercom.	Seul le microphone doit être sélectionné dans les propriétés d'enregistrement de votre carte son, et non le mélange stéréo (ou quoi que ce soit d'autre). Operator Client contrôle son fichier de configuration au démarrage et modifie les propriétés d'enregistrement en conséquence. Ce fichier de configuration contient une entrée par défaut qui peut ne pas correspondre à la configuration de votre système. Ce paramètre est rétabli à chaque démarrage de Operator Client.	Modifiez le paramètre dans le fichier de configuration de Operator Client et réglez-le sur Microphone.

Blocage de Configuration Client

Problème	Cause	Solution
Configuration Client se bloque.	S'il existe de nombreuses caméras configurées dans un fichier Allegiant qui ne sont pas connectées à Bosch Video Management System,	<i>Voir Réduction du nombre de caméras Allegiant, page 385.</i>

Problème	Cause	Solution
	vous pouvez réduire leur nombre. Cela évite les charges inutiles du système.	

31.1 Configuration de la langue dans Windows

Si vous souhaitez changer de langue d'affichage pour la configuration de BVMS, vous devez modifier la langue pour Windows. Lorsque vous changez de langue en suivant la procédure ci-dessous, l'ordinateur redémarre pour appliquer le paramètre de langue choisi.

Pour configurer la langue de votre choix :

1. Cliquez sur **Démarrer**, cliquez sur **Panneau de configuration**, puis double-cliquez sur **Options régionales et linguistiques**.
2. Cliquez sur l'onglet **Avancé**. Sous **Langue pour les programmes non-Unicode**, sélectionnez la langue de votre choix.
3. Cliquez sur **OK**.
4. Dans chaque boîte de message qui s'affiche, cliquez sur **Oui**. Votre ordinateur redémarre.

31.2 Rétablissement de la connexion à un clavier numérique IntuiKey de Bosch

1. Rebranchez le câble ou attendez que le poste de commande soit en ligne. Le message Off Line disparaît.
2. Appuyez sur la touche programmable Terminal pour accéder à BVMS.

31.3 Réduction du nombre de caméras Allegiant

Vous avez besoin du logiciel Master Control Software d'Allegiant pour pouvoir modifier le fichier Allegiant.

Pour réduire le nombre de caméras Allegiant :

1. Démarrez le logiciel MCS.
2. Ouvrez le fichier Allegiant.
3. Cliquez sur l'onglet Camera.
4. Marquez les caméras inutiles.
5. Dans le menu Edit, cliquez sur Delete.
6. Enregistrez le fichier. La taille du fichier ne change pas.
7. Répéter la dernière étape pour les moniteurs dont vous n'avez pas besoin. Cliquez sur l'onglet Monitors.
8. Importez ce fichier dans Bosch Video Management System (voir *Ajout d'un dispositif*, page 127).

31.4 Ports utilisés

Cette section répertorie, pour tous les composants de BVMS, les ports qui doivent être ouverts sur un réseau local. N'ouvrez pas ces ports sur Internet ! Pour un fonctionnement via Internet, utilisez des connexions sécurisées telles qu'un VPN.

Chaque tableau répertorie les ports locaux qui doivent être ouverts sur l'ordinateur sur lequel le serveur est installé ou sur le routeur/commutateur de niveau 3 qui est connecté au matériel.

Sur un pare-feu Windows, configurez une règle de trafic entrant pour chaque port ouvert. Autorisez toutes les connexions sortantes pour toutes les applications logicielles BVMS.

Ports de Management Server/Enterprise Management Server

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Management Server	UDP	123	Encodeur	TimeServer NTP
Management Server	TCP	5322	Operator Client	Connexion SSH
Management Server	TCP	5323	Operator Client	Service de fournisseur d'autorisation
Management Server	TCP	5389	Dispositif ONVIF	Proxy ONVIF, notification d'événement
Management Server	TCP	5390	Operator Client, Configuration Client	Communication à distance .NET
Management Server	TCP	5391	Operator Client, Configuration Client, clients NVR	Port distant pour l'ensemble des services NVR
Management Server	TCP	5392	Operator Client, Configuration Client, Mobile Video Service, Application BVMS SDK	WCF, gateway.push.apple.com
Management Server	TCP	5393	Operator Client, VRM, MVS	Data-Access-Service
Management Server	TCP	5394	Operator Client	Port distant pour Operator Client
Management Server	TCP	5395	Configuration Client, Operator Client	Préférences utilisateur, Transfert de fichier
Management Server	TCP	5396	Configuration Client, clients WCF	Point d'entrée Mex (généralement désactivé)
Management Server	TCP	5397	Operator Client pour NoTouchDeployment	Port NoTouchDeployment
Management Server	TCP	5398	Client de l'API de configuration	Communication interne entre le composant AKKA.Net et CS
Management Server	UDP	12544	Client SNMP	BVMS SNMP get port
Management Server	TCP	162	SNMP	
Management Server	TCP	5389 - 5396	Ports BVMS	

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Management Server	TCP, UDP	135	BRS DCOM	BRS
Management Server	TCP	808	BRS WebService (DIBOS)	Serveur central connecté au Dibos sur ce port avec WCF
Management Server	TCP	1756 / 1757	RCP	1757 pour le VRM secondaire

Composants centraux supplémentaires

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Configuration Client	UDP	1024 - 65535	Encodeur, VRM	Flux vidéo
API de configuration	TCP	5399	Client de l'API REST	API de configuration
Management Server	TCP	5443	PID	Connexion PID, accès via HTTPS
Surveillance de la station de travail	TCP	5410	Operator Client, Management Server	
Surveillance de la station de travail	TCP	5411	Service GRPC	

Ports Video Recording Manager

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
VRM	TCP	554 / 555	Client RTSP	Récupérer le flux RTSP principal/secondaire
VRM	TCP	40023	Client Telnet	Telnet (hôte local uniquement à partir de VRM 4.x)
VRM	TCP	40080 / 40081	Client VRM	Port HTTP vj_generic.dll
VRM	TCP	41080 / 41081	Client VRM	HTTP vj_generic.dll (hôte local uniquement)
VRM	TCP	1756 / 1757	Management Server, Configuration Client	Via RCP+, (1757 pour le client VRM RCP+ secondaire)

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
VRM	UDP	1757	Management Server, Operator Client	Balayage de la diffusion cible
VRM	UDP	1758	Management Server, Configuration Client	Réponse de l'analyse
VRM	UDP	1759	Management Server, Configuration Client	Exploration réseau, Analyse du multicast cible
VRM	UDP	1760		
VRM	UDP	1800 / 1900	Management Server, Operator Client	Analyse du multicast cible
VRM	TCP	80	Operator Client	Lecture VRM principale via http
VRM	TCP	443	Operator Client	Lecture VRM principale via https
VRM	TCP	81	Operator Client	Lecture VRM secondaire via http
VRM	TCP	444	Operator Client	Lecture VRM secondaire via https

Ports Bosch Video Streaming Gateway

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Bosch Video Streaming Gateway	TCP	8080 - 8086	VRM, Management Server, Configuration Client, Operator Client	HTTP
Bosch Video Streaming Gateway	TCP	8443 - 8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	TCP	8756 - 8762	VRM, Management Server, Configuration Client	RCP +
Bosch Video Streaming Gateway	TCP	8443-8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	UDP	1757	VRM Client	Balayage de la diffusion cible
Bosch Video Streaming Gateway	UDP	1758	VRM Client	Réponse de l'analyse

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Bosch Video Streaming Gateway	UDP	1759	VRM Client	Exploration réseau, Analyse du multicast cible
Bosch Video Streaming Gateway	UDP	1800, 1900	VRM Configuration Client	Exploration réseau, Analyse du multicast cible
Bosch Video Streaming Gateway	UDP	1064-65535	Encodeur, VRM	Flux vidéo

Ports de Mobile Video Service

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Mobile Video Service	TCP	80	Management Server, Operator Client, Configuration Client, Client HTML, Applications mobiles	Lecture VRM principale via HTTP
Mobile Video Service	TCP	443	Management Server, Operator Client, Configuration Client, Client HTML, Applications mobiles	Lecture VRM principale via HTTPS
Mobile Video Service	TCP	2195	Notification Push Apple	Mac iOS
Mobile Video Service	UDP	1064-65535	Encodeur, VRM	Flux vidéo
Transcodeur de Mobile Video Service	TCP	5382	Opérateur de téléphonie mobile de Mobile Video Service	Flux multimédia
Fournisseur BVMS de Mobile Video Service	TCP	5383	Operator Client	Flux multimédia
Fournisseur BVMS de Mobile Video Service	TCP	5384	Client HTML, Applications mobiles	Flux multimédia
Transcodeur de Mobile Video Service	TCP	5385	Opérateur de téléphonie mobile de Mobile Video Service	Flux multimédia

Ports de système de stockage iSCSI

Configurez le transfert de port sur le routeur connecté pour ce périphérique.

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Système de stockage iSCSI	TCP	3260	Encodeur, VRM, Configuration Client, Operator Client	Système de stockage iSCSI

Ports DVR

Configurez le transfert de port sur le routeur connecté pour ce périphérique.

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
DVR	TCP	80	Management Server, Configuration Client, Operator Client	Accès via HTTP
DVR	TCP	443	Management Server, Configuration Client, Operator Client	Accès via HTTPS

Caméra ONVIF/caméra/ports d'encodeur

Configurez le transfert de port sur le routeur connecté pour ce périphérique.

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Encodeur	TCP	80	Management Server, VSG, Configuration Client, Operator Client	Accès via HTTP
Encodeur	TCP	443	Management Server, VSG, Configuration Client, Operator Client	Accès via HTTPS
Encodeur	UDP	123	Management Server, VRM	SNTP
Encodeur	UDP	161	Management Server, VRM	SNMP
Encodeur	TCP	554	Operator Client, Application BVMS SDK, VSG	Diffusion RTSP
Encodeur	TCP	3260	Encodeur (sortant)	Enregistrement iSCSI
Encodeur	TCP	1756	Décodeur, Management Server, Operator Client	Connexion sortante pour les caméras Bosch
Encodeur	UDP	1757	Décodeur, Management Server, Operator Client	Balayage de la diffusion cible
Encodeur	UDP	1758	Décodeur, Management Server, Operator Client	Réponse de l'analyse
Encodeur	UDP	1800	Décodeur, Management Server, Operator Client	Exploration réseau, Analyse du multicast cible

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Encodeur	UDP	1900		SSDP (port d'encodeur en option)
Encodeur	UDP	21		FTP (port d'encodeur en option)
Encodeur	UDP	3702		UPNP (port d'encodeur en option)
Encodeur	UDP	9554		SRTSP (port d'encodeur en option)
Encodeur	UDP	15344 / 15345		RTSP send (port d'encodeur en option)

Ports du décodeur BVMS

Configurez le transfert de port sur le routeur connecté pour ce périphérique.

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Décodeur	TCP	1756	Management Server, Operator Client, Configuration Client, Application BVMS SDK	Connexion sortante pour les caméras Bosch
Décodeur	UDP	1757	Management Server, Operator Client	Balayage de la diffusion cible
Décodeur	UDP	1758	Management Server, Operator Client	Réponse de l'analyse
Décodeur	UDP	1800	Management Server, Operator Client	Exploration réseau, Analyse du multicast cible
Décodeur	TCP	80	Operator Client	Accès via HTTP
Décodeur	TCP	443	Operator Client	Accès via HTTPS
Décodeur	UDP	1024-65535	Encodeur	Ports de diffusion
Décodeur	UDP	123	Management Server, VRM	SNTP
Décodeur	UDP	161	Management Server, VRM	SNMP

Ports Operator Client BVMS / Cameo SDK

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Operator Client	TCP	5394	Application BVMS SDK, BIS	WCF
Operator Client	UDP	1024-65535	Encodeur, VRM	Flux vidéo
Operator Client	TCP	40082		
Operator Client	TCP	41756		

Ports d'adaptateur de dispositif LPR, BVMS

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
Adaptateur de dispositif BVMS	TCP	31000	Client de caméra LPR	VRC

Ports de AMS, Access Management System

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
AMS	TCP	62904	Management Server	Accès via HTTPS

Transcodeur

Serveur (d'écoute)	Protocole	Ports d'entrée	Client (demandeur)	Remarque
	UDP	5080		
	UDP	5443		
	UDP	5756		

31.5 Activation de la journalisation des événements ONVIF**Remarque!****Sachez que cette fonctionnalité sera bientôt obsolète.**

Utilisez ONVIF Camera Event Driver Tool pour un mappage des événements ONVIF plus facile.

Voir *Démarrage de ONVIF Camera Event Driver Tool à partir de Configuration Client*, page 215.

Vous pouvez activer la journalisation des événements ONVIF, par exemple en cas de problèmes de réception d'événements BVMS. La journalisation vous aide alors à résoudre le problème.

Pour activer la journalisation :

- Ouvrez le fichier %programfiles%\Bosch\VMS\AppData\Server\CentralServer\BVMSLogCfg.xml dans un éditeur approprié, par exemple Notepad. Exécutez l'application Notepad en tant qu'administrateur.
- Accédez à la ligne contenant la chaîne suivante :
Add logging for onvif events of a device by network address
Les lignes commentées contiennent une brève explication.
- Saisissez le nom de journal (logger name) OnvifEvents.<Networkaddress>
Saisissez uniquement OnvifEvents pour consigner les événements de tous les dispositifs ONVIF.
- Saisissez la valeur de niveau (level value) DEBUG pour tous les événements entrants et sortants.
Saisissez INFO pour tous les événements sortants.
Saisissez WARN ou ERROR pour désactiver.

Remarque : L'activation peut nécessiter un redémarrage du serveur central.

Les lignes suivantes montrent un exemple de journalisation des événements du dispositif 172.11.122.22 avec tous les événements sortants et entrants.

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



Assistance

Accédez à nos **services d'assistance** à l'adresse www.boschsecurity.com/xc/en/support/. Bosch Security and Safety Systems propose une assistance dans les domaines suivants :

- [Applications & Outils](#)
- [Building Information Modeling](#)
- [Garantie](#)
- [Dépannage](#)
- [Réparation & Échange](#)
- [Sécurité des produits](#)



Bosch Building Technologies Academy

Visitez le site Web Bosch Building Technologies Academy et accédez à des **cours de formation, des didacticiels vidéo** et des **documents** : www.boschsecurity.com/xc/en/support/training/

Se reporter à

- *Démarrage de ONVIF Camera Event Driver Tool à partir de Configuration Client, page 215*
- *Configuration d'un tableau de mappage ONVIF, page 248*
- *Mappage des événements ONVIF, page 41*

Glossaire

Accès Enterprise

Enterprise Access est une fonction BVMS qui se compose d'un ou de plusieurs comptes Enterprise Account. Chaque compte Enterprise Account contient des autorisations d'un dispositif pour accéder à des dispositifs d'un serveur Management Server spécifique.

Alarme

Événement configuré pour la création d'une alarme. Il s'agit d'une situation particulière (détection de mouvements, retentissement d'une sonnette, perte de signal, etc.) nécessitant une intervention immédiate. Une alarme peut afficher une vidéo en Mode Temps réel, une vidéo en Mode Lecture, un plan d'action, une page Web ou une carte.

Allegiant

Systèmes analogiques de commutation Bosch

ANR

Automated Network Replenishment. Processus intégré qui copie les données vidéo manquantes d'un émetteur vidéo vers l'enregistreur vidéo sur réseau après une panne réseau. Les données vidéo copiées viennent exactement combler les lacunes survenues du fait de la panne réseau. L'émetteur doit donc posséder une capacité quelconque de stockage local. La capacité d'enregistrement de ce stockage local se calcule comme suit : (bande passante réseau x durée d'indisponibilité estimée du réseau + marge de sécurité) x (1 + 1/vitesse de sauvegarde). La capacité d'enregistrement obtenue est nécessaire, car l'enregistrement continu doit se poursuivre pendant le processus de copie.

Arborescence des Périphériques

Liste hiérarchique de tous les périphériques disponibles dans le système.

Arborescence logique

Arborescence regroupant tous les périphériques au sein d'une structure personnalisée. L'arborescence logique permet de sélectionner des caméras ainsi que d'autres périphériques sur Operator Client. Le Configuration Client, permet de configurer l'« arborescence logique

Complète » (dans la page Cartes et structure) et de l'adapter à chaque groupe d'utilisateurs (dans la page Groupes d'utilisateurs).

Barre du volet des Images

Barre d'outils d'un volet des Images.

Basculement VRM

Logiciel de l'environnement BVMS. Prend en charge la tâche du VRM principal ou du VRM secondaire affecté en cas de défaillance.

BIS

Building Integration System.

Caisse enregistreuse

Caisse enregistreuse

Calendrier d'Enregistrement

Permet de planifier des enregistrements et certains événements, comme par exemple le démarrage d'une sauvegarde ou la restriction du nombre d'ouvertures de session. Les Planifications d'Enregistrement ne doivent comporter ni temps morts, ni chevauchements. Elle régit également la qualité d'enregistrement vidéo.

Caméra mobile

Caméra dotée de fonctions de balayage horizontal/vertical et de zoom.

centrale d'alarme

Nom générique pour le dispositif principal dans un système de sécurité de détection d'intrusion Bosch. Les claviers, les modules, les détecteurs et d'autres dispositifs se connectent à la centrale d'alarme.

Clonage

Sabotage d'un lecteur de cartes Foyer. Un périphérique de clonage lit les données de carte inscrite sur la bande magnétique sans connaître le titulaire de la carte.

DAB

Distributeur automatique de billets.

décodeur

Transforme un flux numérique en flux analogique.

Déformation

Utilisation d'un logiciel pour convertir l'image circulaire d'un objectif macro avec distorsion radiale en image rectiligne pour un affichage normal (déformer consiste à corriger la distorsion).

Déformation d'angle

Déformation effectuée sur la caméra elle-même.

DNS

Domain Name System (Système de noms de domaine). Un serveur DNS convertit une URL (www.monpériphérique.fr, par exemple) en adresse IP sur les réseaux utilisant le protocole TCP/IP.

Document

Les fichiers document pris en charge par BVMS sont HTM, URL, MHT, HTML et TXT.

Données de texte

Données d'une caisse enregistreuse ou d'un DAB, telles que la date et l'heure ou le numéro de compte bancaire, stockées avec les données vidéo correspondantes. Ces données fournissent des compléments d'informations à des fins d'analyse.

double autorisation

Politique de sécurité nécessitant deux utilisateurs différents pour pouvoir établir la connexion à l'Operator Client. Ces deux utilisateurs doivent être membres d'un groupe d'utilisateurs Bosch Video Management System normal. Ce groupe d'utilisateurs (ou ces groupes d'utilisateurs, si les utilisateurs en question sont membres de groupes différents) doit faire partie d'un groupe de double autorisation. Un groupe de double autorisation possède ses propres droits d'accès dans Bosch Video Management System. Ce groupe de double autorisation doit posséder davantage de droits d'accès que le groupe d'utilisateurs normal auquel l'utilisateur appartient. Exemple : l'utilisateur A est membre d'un groupe d'utilisateurs appelé Groupe A. L'utilisateur B est membre du Groupe B. Par ailleurs, un groupe de double autorisation est configuré, avec pour membres le Groupe A et le Groupe B. Pour les utilisateurs du groupe A, la double autorisation est facultative ; pour les utilisateurs du groupe B, elle est obligatoire.

Lorsque l'utilisateur A se connecte, une deuxième boîte de dialogue de confirmation de connexion s'affiche. Dans cette boîte de dialogue, un deuxième utilisateur peut se connecter, le cas échéant. Si ce n'est pas le cas, l'utilisateur A peut continuer et démarrer l'Operator Client. Il ne possède alors que les droits d'accès du Groupe A. Lorsque l'utilisateur B se connecte, une deuxième boîte de dialogue de connexion s'affiche de nouveau. Dans cette boîte de dialogue, un deuxième utilisateur doit se connecter. Si ce n'est pas le cas, l'utilisateur B ne peut pas démarrer l'Operator Client.

Double streaming

La double diffusion permet d'encoder simultanément le flux de données entrant en fonction de deux profils différents configurés individuellement. Deux flux de données sont créés : l'un pour l'enregistrement en temps réel et de pré-événement, et l'autre pour l'enregistrement continu, de mouvement et d'alarme.

DTP

Un dispositif DTP (Data Transform Processor, processeur de transformation de données) transforme des données série de dispositifs ATM en format de données défini et envoie ces données via Ethernet à BVMS. Vous devez vous assurer qu'un filtre de transformation est défini sur le dispositif DTP. Cette tâche est effectuée à l'aide d'un logiciel distinct du fabricant du dispositif DTP.

duplex

Terme utilisé pour définir le sens de la transmission des données entre deux parties. Le semi-duplex permet une transmission des données bidirectionnelle, mais pas simultanée. Le duplex intégral permet une transmission des données bidirectionnelle et simultanée.

Durée de rembobinage

Valeur (en secondes) dans un volet des Images avant de passer en Mode Lecture instantanée.

Durée de temporisation

Pour une séquence de caméras, durée prédéfinie pendant laquelle une fenêtre Image affiche une caméra avant de passer à la caméra suivante.

DVR

Enregistreur numérique

DWF

Design Web Format. Format servant à afficher des dessins techniques sur un moniteur informatique.

DynDNS

Dynamic Domain Name System (Système de noms de domaine dynamique). Un service d'hébergement DNS qui enregistre les adresses IP dans une base de données prête à l'emploi. Le DNS dynamique permet d'établir une connexion au périphérique via Internet à l'aide du nom d'hôte du périphérique. Voir DNS.

émulation CCL

Émulation du Langage de commande (CCL) utilisé pour le contrôle d'une matrice Allegiant. Vous pouvez utiliser cet ensemble de commandes pour commuter une caméra/un encodeur IP BVMS en décodeur IP BVMS. Vous ne pouvez pas contrôler directement d'anciennes caméras analogiques ou la matrice Allegiant elle-même.

Encodeur

Convertit un flux analogique en flux numérique, par exemple pour intégrer des caméras analogiques dans un système numérique tel que Bosch Video Management System. Certains encodeurs peuvent disposer d'une mémoire locale (une carte Flash ou un disque dur USB, par exemple) ou peuvent stocker leurs données vidéo sur des périphériques iSCSI. Les caméras IP possèdent un encodeur incorporé.

Enterprise Account

Enterprise Account désigne une autorisation permettant à un utilisateur Operator Client de se connecter aux dispositifs d'un serveur Management Server appartenant à un système Enterprise System. Dans un compte de type Enterprise Account, toutes les autorisations des dispositifs de ce serveur Management Server sont configurées. Operator Client peut se connecter simultanément à tous les serveurs Management Server qui font partie de ce système Enterprise System. Cet accès est contrôlé par l'adhésion auprès d'un groupe

Enterprise User Group et par les autorisations de dispositif configurées dans le compte Enterprise Account pour ce serveur Management Server.

Enterprise Management Server

Enterprise Management Server désigne un serveur BVMS Management Server hébergeant la configuration des groupes Enterprise User Group. Vous avez besoin d'un ou de plusieurs groupes Enterprise User Group se référant à un ou plusieurs serveurs. Les rôles du serveur Enterprise Management Server et du serveur Management Server peuvent être réunis dans une configuration unique.

Enterprise System

Enterprise System est une fonction de Bosch Video Management System permettant à un utilisateur Operator Client d'accéder simultanément à plusieurs serveurs Management Server.

Enterprise User Group

Enterprise User Group désigne un groupe d'utilisateurs configuré sur un serveur Enterprise Management Server. Enterprise User Group définit les utilisateurs autorisés à accéder simultanément à plusieurs serveurs Management Server. Définit le fonctionnement des autorisations disponibles pour ces utilisateurs.

Entrée virtuelle

Sert à transférer des événements de systèmes tiers vers Bosch Video Management System.

Événement

Circonstance ou état lié(e) à une alarme et/ou une action. Les événements peuvent provenir de plusieurs sources, telles que des caméras, des archiveurs, des répertoires, des entrées numériques, etc. Il peut s'agir d'états de démarrage des enregistrements, de perte d'états de signal, de messages de type « disque saturé », d'ouvertures de session utilisateur ou de déclencheurs par entrée numérique.

Événement Combiné

Association de différents événements au moyen des expressions booléennes ET et OU. Vous pouvez uniquement combiner des changements d'état, par exemple le passage d'une connexion à l'état déconnecté ou l'activation d'une planification.

exclure/rétablir

Exclure un dispositif signifie ignorer les alarmes qu'il peut générer, généralement pendant la durée de certaines circonstances atténuantes telles que des opérations de maintenance. Rétablir signifie ne plus les ignorer.

Famille de périphériques

Les encodeurs/caméras IP Bosch peuvent appartenir à l'une des familles de périphériques suivantes : Famille de périphériques 1, Famille de périphériques 2, Famille de périphériques 3. Les périphériques de la famille de périphériques 1 peuvent uniquement enregistrer le flux 1. Les périphériques de la famille de périphériques 2 peuvent enregistrer le flux 1 ou le flux 2. Les périphériques de la famille de périphériques 3 peuvent enregistrer le flux 1, le flux 2 ou le flux composé uniquement d'images I.

Fenêtre Image

Conteneur renfermant des volets d'Images dont la disposition suit un diagramme particulier.

Fenêtre Image d'alarme

Fenêtre Image affichant un ou plusieurs volets des images d'Alarme.

Fichiers carte de site

BVMS prend en charge les fichiers de carte de site suivants : PNG, JPG, PDF et DWF.

Fichiers de carte

BVMS prend en charge les fichiers de carte suivants : PNG et JPG.

Fonction intercom

Permet de parler dans les haut-parleurs d'un encodeur. Cet encodeur doit être équipé d'une entrée audio et d'une sortie audio. La fonction intercom peut être accordée par groupe d'utilisateurs.

groupe de moniteurs

Ensemble de moniteurs connectés à des décodeurs. Le groupe de moniteurs peut être affecté au traitement des alarmes dans une zone physique donnée. Ainsi, une installation comportant trois salles de contrôle séparées physiquement peuvent comporter trois groupes de moniteurs. Les moniteurs d'un groupe de moniteurs sont configurés logiquement en lignes

et colonnes et peuvent être définis sur des dispositions différentes, par exemple en plein écran ou en vue quadravision.

Groupe d'utilisateurs

Groupe servant à définir des attributs communs à plusieurs utilisateurs, tels que des autorisations, des droits d'accès et un niveau de priorité en matière de balayage horizontal/vertical et de zoom. Lorsqu'un utilisateur devient membre d'un groupe, il hérite automatiquement de tous les attributs du groupe.

GSM

Abréviation de Global System for Mobile Communication. Standard de téléphonie numérique mobile.

H.264

Norme pour le codage (la compression) de données numériques audio et vidéo pour les applications multimédias. Cette norme inclut différents profils pouvant dépendre du fabricant. Les profils suivants sont disponibles : Baseline, Baseline+ et Main Profile. Le profil Baseline (n'est pas utilisé dans Bosch Video Management System) prend en charge 2 CIF. Le profil Baseline+ prend en charge 4 CIF et offre une meilleure qualité d'image que le profil Baseline. Le profil Main Profile prend en charge 4 CIF et fournit un algorithme de compression hautement efficace, appelé CABAC (Context-adaptive binary arithmetic coding). Celui-ci offre un encodage haute qualité pour le stockage.

H.265

H.265 est une norme de compression vidéo définie par ISO 2 et ITU3 et ratifiée le 29 octobre. 2014. Elle est considérée comme successeur de la norme MPEG-4 AVC (Advanced Video Codec), également appelée H.264, pour adresser la compression des résolutions de 4K et ultra HD jusqu'à 36 mégapixels.

Image de référence

Une image de référence est comparée en permanence avec l'image vidéo actuelle. Une alarme se déclenche si l'image vidéo en cours diffère de l'image de référence dans les zones marquées. Vous pouvez ainsi détecter une

tentative de vandalisme qui ne le serait pas autrement, par exemple, si la caméra était tournée.

Image B

Image bidirectionnelle. Partie d'une méthode de compression vidéo.

Image I

Image intra. Partie d'une méthode de compression vidéo. Contient les informations d'une image complète, contrairement aux images P ou B qui ne contiennent que les informations des modifications subies par rapport à l'image précédente ou suivante.

Image P

Image prédite. Partie d'une méthode de compression vidéo.

IPS

Images par seconde. Nombre d'images vidéo transmises ou enregistrées par seconde.

IQN

iSCSI Qualified Name (nom qualifié). Le nom d'initiateur au format IQN est utilisé pour fournir les adresses à la fois aux initiateurs et aux cibles iSCSI. Avec le mappage des IQN, vous créez un groupe initiateur qui contrôle l'accès aux LUN d'une cible iSCSI et vous inscrivez les noms d'initiateur de chaque encodeur et du VRM dans ce groupe initiateur. Seuls les périphériques dont les noms d'initiateur sont ajoutés au groupe initiateur sont autorisés à accéder à un LUN. Voir LUN ; voir iSCSI.

iSCSI

Internet Small Computer System Interface (SCSI sur IP). Protocole qui gère le stockage des données via un réseau TCP/IP. iSCSI permet d'accéder aux données stockées à partir de n'importe quel endroit du réseau. Grâce à l'avènement du Gigabit Ethernet, tout particulièrement, la configuration des serveurs de stockage iSCSI en tant que disques durs distants pour les ajouter à un réseau informatique est devenue une opération abordable. Dans la terminologie iSCSI, le serveur qui fournit les ressources de stockage est appelé « cible iSCSI », tandis que le client qui se connecte au serveur et accède à ses ressources est appelé « initiateur iSCSI ».

Jonction

Sorties analogiques d'une matrice analogique connectées à un encodeur. Ainsi, les sources vidéo de matrice peuvent être utilisées dans Bosch Video Management System.

Journal des Connexions

Conteneur pour la consignation de tous les événements qui se produisent dans Bosch Video Management System.

JPEG

Joint Photographic Expert Group

JPEG

Joint Photographic Experts Group. Processus de codage d'images.

LDAP

Lightweight Directory Access Protocol. Protocole réseau exécuté sur TCP/IP autorisant l'accès à des annuaires. Par exemple, un annuaire peut dresser la liste de groupes d'utilisateurs et de leurs droits d'accès. Le système Bosch Video Management System s'en sert pour accéder aux mêmes groupes d'utilisateurs que MS Windows, ou à un système de gestion des utilisateurs d'une autre entreprise.

Lecture instantanée

Lit l'image enregistrée de la caméra sélectionnée dans un volet des images sur l'écran en Mode Temps Réel. Il est possible de configurer l'heure de début (nombre de secondes dans le passé ou durée de rembobinage).

Liste des Alarmes

Fenêtre de Bosch Video Management System servant à afficher une liste d'alarmes actives.

Logiciel MCS

Logiciel utilisé en tant qu'interface entre Bosch Video Management System et un périphérique Allegiant. Version 2.8 ou ultérieure.

LUN

Logical Unit Number (Numéro logique de lecteur). Utilisé dans l'environnement iSCSI pour adresser une unité de disque individuelle ou une partition virtuelle (volume). La partition fait partie d'une matrice de disques RAID (la cible iSCSI).

MHT

Également appelé « archive Web ». Format de fichier capable d'enregistrer tous les fichiers HTML et image d'un site Internet au sein d'un seul fichier. Pour éviter les problèmes, il est conseillé de créer les fichiers MHT à l'aide d'Internet Explorer 7.0 ou d'une version supérieure.

Mode Temps Réel

Fonction de l'Operator Client . Utilisé pour la visualisation en temps réel de la vidéo.

No Touch Deployment

Méthode permettant de télécharger, installer et exécuter automatiquement des applications .NET sans modifier le registre ou les composants système partagés. Avec Bosch Video Management System, le mécanisme No Touch Deployment est utilisé pour mettre à jour les Operator Clients à partir du serveur. La mise à jour a lieu si une version plus récente est présente sur le Management Server, et au moment où chaque utilisateur se connecte à Operator Client. Si vous travaillez avec un seul Operator Client et plusieurs ordinateurs Management Server, le mécanisme No Touch Deployment utilise uniquement la version du logiciel présente sur le dernier Management Server auquel l'Operator Client s'est connecté avec succès. Si vous essayez d'ouvrir une session sur un autre Management Server avec une version différente de l'application, celle-ci affiche le serveur comme « hors-ligne » étant donné que les versions du logiciel ne correspondent pas.

Numéro logique

Les numéros logiques sont des identifiants uniques affectés à chaque périphérique dans le système pour en faciliter le référencement. Ils ne sont uniques que pour un type de périphérique particulier. Les scripts de commande sont un exemple type d'utilisation des numéros logiques.

NVR

Network Video Recorder (Enregistreur vidéo numérique) Bosch. Ordinateur dans l'environnement Bosch Video Management System, stockant des données audio et vidéo, et pouvant opérer comme Basculement NVR ou

NVR Redondant. Ce NVR est différent des systèmes VIDOS NVR qui peuvent être intégrés à Bosch Video Management System.

OID

Identifiant d'objet. Terme employé dans l'environnement SNMP. Détermine une variable MIB.

ONVIF

Open Network Video Interface Forum. Norme internationale pour les produits vidéo en réseau. Les dispositifs conformes à la norme ONVIF sont capables d'échanger en temps réel des informations vidéo, audio, des métadonnées et des informations de commande, et permettent de les détecter et de les raccorder automatiquement à des applications réseau, telles que des systèmes de gestion vidéo.

Operator Client

Composant de Bosch Video Management System qui offre une interface utilisateur destinée à la surveillance et à l'utilisation du système.

PID

Dispositif d'identification de la personne. Il extrait les caractéristiques d'une personne à partir d'une image, par exemple le visage. Il exécute des algorithmes spéciaux qui peuvent identifier une personne dans un flux vidéo.

Planification des Tâches

Sert à planifier des événements qui peuvent se produire dans Bosch Video Management System, par exemple pour l'exécution d'un Script de Commande. La page Événements permet d'affecter des Planifications de Tâches à des événements. Pour planifier des événements, vous pouvez également utiliser des Planifications d'Enregistrement. Dans une Planification des Tâches standard, vous êtes amené à configurer des périodes pour chaque jour de la semaine, pour les jours fériés et pour les Jours d'Exception. Dans une Planification des Tâches récurrente, vous pouvez configurer des périodes récurrentes. Elles peuvent se répéter tous les jours, toutes les semaines, tous les mois ou tous les ans.

point

Dispositif de détection connecté au système de sécurité. Les points figurent individuellement sur le clavier et avec un texte personnalisé. Le texte peut décrire une porte, un capteur de mouvement, un détecteur de fumée ou un espace protégé comme UPSTAIRS ou GARAGE.

Port

1) Sur les ordinateurs et les périphériques de télécommunication, un port (nom) désigne un endroit physique particulier où connecter d'autres périphériques, généralement au moyen d'une prise et d'une fiche. Un PC est généralement doté d'un ou de plusieurs ports série et d'un port parallèle. 2) En programmation, un port (nom) désigne un lieu de raccordement logique et, plus particulièrement, le moyen par lequel un programme client sur un ordinateur en réseau fait référence à un programme de serveur donné via le protocole Internet TCP/IP. Les applications de haut niveau utilisant TCP/IP, telles que le protocole Web Hypertext Transfer Protocol, sont dotées de ports portant des numéros prédéfinis. Il s'agit des « ports connus » attribués par l'IANA (Internet Assigned Numbers Authority). Des numéros de port sont attribués aux autres processus d'application de manière dynamique lors de chaque connexion. Lors du démarrage initial d'un service (programme de serveur), ce service se lie au numéro de port qui lui a été attribué. Les autres programmes client souhaitant utiliser ce serveur doivent également demander à se lier au numéro de port désigné. Les numéros de port sont compris entre 0 et 65 535. Les ports allant de 1 à 1023 sont réservés à des services particuliers. Par exemple, le port 80 est réservé par défaut au service HTTP. Il est donc inutile de le spécifier dans l'URL (Uniform Resource Locator).

portées

La portée est un terme utilisé dans le domaine des caméras ONVIF. Il s'agit d'un paramètre utilisé pour le sondage d'un dispositif ONVIF. Le paramètre contient généralement un URI, par exemple : `onvif://www.onvif.org/<path>`. Le paramètre `<path>` peut être par exemple

`video_encoder` ou `audio_encoder`. Un dispositif ONVIF peut avoir plusieurs portées. Cette URI dénomine la zone de tâche du dispositif.

Poste de commande

Dans l'environnement BVMS Bosch : un ordinateur dédié sur lequel Operator Client est installé. Cet ordinateur est configuré comme un poste de commande dans Configuration Client pour activer des fonctions spécifiques.

Poste de commande Operator Client

Ordinateur dans l'environnement de Bosch Video Management System permettant de visualiser une vidéo en mode temps réel et lecture, et d'effectuer des tâches de configuration. Operator Client est installé sur cet ordinateur.

RAID

Redundant Array of Independent Disks. Sert à structurer plusieurs disques durs comme s'il ne s'agissait que d'un seul disque dur. Sur les lecteurs de ce type, les données sont partagées ou répliquées. Cela permet d'obtenir de meilleures performances en matière de capacité, de fiabilité et de vitesse.

RCP

Remote Control Protocol

Recherche de serveur

Méthode d'accès pour un utilisateur de Configuration Client ou d'Operator Client pour se connecter de manière séquentielle à plusieurs points d'accès au système. Un point d'accès au système peut être un serveur ou un serveur d'entreprise.

Résolution vidéo

Nombre de pixels horizontaux et verticaux transférés via des signaux vidéo. 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 = encodage 1280 x 720 1080p = encodage 1920 x 1080

RMon et Sntp

Simple Network Management Protocol. Protocole IP permettant de recueillir des informations auprès des périphériques réseau

(GET), de définir des paramètres sur les périphériques réseau (SET) et d'être averti de certains événements (EVENT).

RTP

Real-Time Transport Protocol : protocole de transmission audio et vidéo en temps réel

RTSP

Real Time Streaming Protocol. Protocole réseau permettant de gérer la transmission continue de données ou de logiciels audiovisuels sur les réseaux IP.

Script de Commande

Macro que l'administrateur peut programmer pour lancer une action automatique, telle que le placement d'une caméra mobile ou l'envoi d'e-mails. Bosch Video Management System propose un ensemble limité de commandes pour cette fonctionnalité. Les scripts de commande sont divisés en scripts de clients et de serveur. Les scripts de clients sont utilisés sur les postes de commande client pour exécuter certaines tâches exécutables sur ce type de poste. Les scripts de serveur sont exécutés automatiquement par un événement déclenché dans le système. Ils reçoivent des arguments de l'événement, tels que la date et l'heure. Un Script de Commande peut se composer de plusieurs scripts. Vous pouvez créer un Script de Commande en utilisant les langages de script suivants : C#, VB.Net. Les scripts de commande sont exécutés en réponse à des événements ou des alarmes (scripts de serveur uniquement) de manière automatique en fonction d'une planification, ou de manière manuelle à partir de l'arborescence logique, d'icônes ou de cartes.

Serveur

Dispositifs de gestion du serveur BVMS.

site non géré

Élément de l'arborescence des dispositifs dans BVMS pouvant contenir des dispositifs réseau vidéo tels que des enregistreurs vidéo numériques. Ces dispositifs ne sont pas gérés par le serveur Management Server de votre système. L'utilisateur Operator Client peut se connecter aux dispositifs d'un élément unmanaged site à la demande.

Surveillance réseau

Mesure de valeurs relatives au réseau et évaluation de ces valeurs par comparaison avec des seuils configurables.

TCP

Transmission Control Protocol (protocole de contrôle de transmission)

TCP/IP

Transmission Control Protocol / Internet Protocol. Également appelé « Suite des protocoles Internet ». Ensemble de protocoles de communication servant à transmettre des données via un réseau IP.

temps de réponse

Période commençant par un événement. Normalement, au cours de cette période aucun autre événement de même type n'est accepté. Utilisez ce paramètre pour éviter que les commutations d'un capteur ne génèrent des événements incessants, par exemple. Pour les événements avec plusieurs états, vous pouvez configurer un paramètre de priorité différent pour chaque état. Les exemples suivants vous aideront à mieux comprendre le concept de temps de réponse. L'exemple 1 traite d'événements provoquant le même état : l'événement Informations sur le système se produit et le temps de réponse configuré démarre. Au cours de cette période, un autre événement Informations sur le système se produit. Cet événement Informations sur le système n'est pas considéré comme un nouvel événement. L'exemple 2 traite d'événements provoquant des états différents mais de même priorité : un événement Mouvement détecté se produit et le temps de réponse configuré démarre. Au cours de cette période, l'événement Mouvement arrêté de même niveau de priorité se produit. Cet événement Mouvement arrêté n'est pas considéré comme un nouvel événement. L'exemple 3 traite également d'événements provoquant des états différents mais de même priorité : l'état Entrée virtuelle est activé. Les deux changements d'état comportent un niveau de priorité identique. À un moment précis, l'entrée virtuelle est coupée et le temps de réponse démarre. Pendant ce temps de réponse, l'entrée virtuelle est sous tension. Ce

changement d'état n'est pas accepté en tant que nouvel événement car il présente la même priorité. Une fois le temps de réponse écoulé, l'état de l'entrée virtuelle est modifiée. L'horodatage de la mise sous tension correspond à la fin du temps de réponse et aucun nouveau temps de réponse ne démarre. L'exemple 4 traite d'événements avec des priorités différentes provoquant des états différents : l'événement Mouvement détecté se produit et le temps de réponse configuré démarre. Au cours de cette période, l'événement Mouvement arrêté d'un niveau de priorité plus élevé se produit. L'événement Mouvement arrêté est accepté en tant que nouvel événement, mais le temps de réponse ne redémarre pas. L'exemple 5 traite également d'événements avec des priorités différentes provoquant des états différentes : l'état Entrée virtuelle est désactivé. La priorité de l'état est « 5 » pour sous tension et « 2 » pour hors tension. À un point précis, l'entrée virtuelle est mise sous tension (prio « 5 ») et le temps de réponse démarre. Pendant ce temps de réponse, l'entrée virtuelle est désactivée (prio « 2 »). Ce changement d'état est accepté en tant que nouvel événement car il comporte un niveau de priorité plus élevé. Le temps de réponse de la première mise sous tension se poursuit. Des modifications supplémentaires ne sont pas possibles pendant ce temps de réponse.

trajets multiples

Utilisation de la technique basée sur plusieurs chemins de stockage de l'ordinateur.

trajets multiples

Technique de stockage de l'ordinateur avec plusieurs chemins physiques définis qui connectent le serveur de données à une cible de stockage (à l'aide de différents contrôleurs, commutateurs de bus ou équivalents) comme solution de basculement ou d'équilibrage de charge (redondance, efficacité).

Trap

Terme employé dans l'environnement SNMP pour un message non demandé envoyé par un périphérique surveillé (agent) au système de surveillance réseau (gestionnaire) à propos d'un événement survenu au niveau de ce périphérique.

UDP

User Datagram Protocol. Protocole en mode non connecté servant à échanger des données sur un réseau IP. Le protocole UDP est plus efficace que le protocole TCP pour la transmission vidéo, car il nécessite moins de ressources.

URI

Uniform Resource Identifier (Identifiant de ressource uniforme). Chaîne de caractères pour identifier une ressource de réseau. Chaque URI est constitué des chaînes de schéma, d'autorité, de chemin, de requête, de fragment. Seules les chaînes de schéma et de fragment sont obligatoires pour le service vidéo mobile. Exemple : `http:<scheme>//example.com<authority>/over/therepath?name=ferret<query>#nose<fragment>`

URL

Uniform Resource Locator : format de nommage universel

VCA

Analyse de contenu vidéo : analyse informatique des flux vidéo afin de déterminer ce qu'il se passe sur la scène surveillée. Voir aussi Intelligent Video Analytics

Video Analytics

Video Analytics désigne un processus logiciel qui compare l'image d'une caméra avec les images enregistrées de personnes ou d'objets spécifiques. En cas de correspondance, le logiciel déclenche une alarme.

Video Streaming Gateway (VSG)

Périphérique virtuel permettant d'intégrer des caméras Bosch, ONVIF, JPEG, et des encodeurs RTSP.

Volet des images

Permet d'afficher une vidéo en direct ou enregistrée à partir d'une seule caméra, d'une carte de site, d'un document, d'une séquence, d'un groupe de moniteurs, d'une application externe ou d'une zone de visualisation de carte.

VRM

Video Recording Manager. Pack logiciel Bosch Video Management System, qui gère le stockage des données vidéo (MPEG-4 SH++, H.264 et H.265) avec les données et métadonnées audio

sur les périphériques iSCSI présents sur le réseau. VRM alimente une base de données contenant les informations relatives à la source des enregistrements et tient à jour la liste des disques iSCSI associés. VRM est un service qui s'exécute sur un ordinateur relié au réseau Bosch Video Management System. VRM ne stocke pas les données vidéo elles-même, mais répartit les capacités de stockage des périphériques iSCSI sur les encodeurs, tout en gérant l'équilibrage de charge entre les différents périphériques iSCSI. VRM transfère la lecture des périphériques iSCSI aux Operator Clients.

VRM principal

Synonyme de VRM.

VRM redondant

Logiciel de l'environnement BVMS. Cas particulier d'un VRM secondaire. Garantit que l'enregistrement effectué par un VRM principal est effectué en plus et simultanément sur une autre cible iSCSI avec les mêmes paramètres d'enregistrement.

VRM secondaire

Logiciel de l'environnement BVMS. Garantit que l'enregistrement effectué par un ou plusieurs VRM principaux est effectué en plus et simultanément sur une autre cible iSCSI. Les paramètres d'enregistrement peuvent être différents des paramètres du VRM principal.

Zone

Un groupe de dispositifs de détection connectés au système de sécurité.

Zone de visualisation de carte

Une zone de visualisation de carte est une région de l'écran utilisée pour afficher une partie définie de la carte de géolocalisation globale.

Zone d'intérêt (ROI)

Zone d'intérêt. Les zones d'intérêt (ROI) sont prévues pour économiser de la bande passante lorsqu'un zoom est effectué sur une section de l'image de la caméra à l'aide d'une caméra HD fixe. Cette section fonctionne comme une caméra mobile.

Zone réactive

Icône changeant en fonction du passage de la souris dans une carte. Les zones réactives sont configurées dans le client de configuration. Les zones réactives peuvent être, par exemple, des caméras, des relais, des entrées. L'opérateur s'en sert pour rechercher un dispositif dans un bâtiment, puis le sélectionner. Lorsqu'elles sont configurées, les zones réactives peuvent afficher une couleur d'arrière-plan clignotante si un événement d'état spécifique ou une alarme se produit.

Index

A		
accès à l'aide	14	
accès refusé		
émulation CCL Allegiant	163	
acquisition de commandes de balayage horizontal/ vertical et de zoom	373	
activation	96	
configuration	93	
retard	93	
retardé	105	
activation parole	352	
activation retardée	93, 105	
activer	93	
Bosch Video Management System	75	
configuration précédente	94	
actualisation des états	107, 109, 110	
actualiser les états	102	
adresse IP		
doublons	106	
modification	238	
modifier	107, 127, 143	
adresse IP par défaut	106	
adresse réseau		
modification	238	
modifier	143	
adresses IP déjà utilisées	106	
affichage automatique des alarmes	40	
aide	14, 15	
aide du script de l'interface API de Bosch	90	
aide en ligne	14	
ajout d'encodeur BVIP	145, 230	
ajouter des données texte à l'enregistrement continu	321	
ajouter un décodeur BVIP	144, 187, 216, 224	
ajouter un dispositif Video Analytics	168	
ajouter un élément unmanaged site	219	
ajouter un encodeur	183, 193, 223, 379	
ajouter un encodeur BVIP	144, 187, 216, 224	
ajouter un site non géré	218, 221	
ajouter une alarme d'entrée Bosch Allegiant	99	
ajouter une interface POS/ATM Bosch	98	
ajouter une zone de stockage		
VRM	181	
ajouter VRM		175
alarmes		
ordre de tri		323
Allegiant		
caméra mobile		300
canal de contrôle		60, 61
émulation CCL		128, 164
programme Network Host		60
système satellite		61
trop de caméras		385
version du firmware		52, 53
ANR		84, 237, 299
Arborescence des périphériques		126, 177, 266
Arborescence logique		268, 328
Assistant de configuration		
Mobile Video Service		65
aucun mot de passe		93
autorisations		266, 268
B		
balayage		
à travers les sous-réseaux		122
encodeurs		129
encodeurs à stockage local		129
encodeurs temps réel uniquement		129
sous-réseaux		122
VRM		130
base de données du journal des connexions		123
chaîne de connexion		123
blocage		373
Client de Configuration		384
Blocage du balayage horizontal/vertical et de zoom		347
Blocage PTZ		354, 373
Bosch Video Management System		17
activer		75
aide en ligne		14
gestion des licences		75
langue de l'interface utilisateur graphique		383
vue d'ensemble		17
bouton d'événement utilisateur		333
C		
CABAC		307
caméra de détection incendie		378
caméra initiale		150
caméra mobile		311
Allegiant		300

caméra mobile	313	D	
caméra panoramique		Débit de données cible	306
modes d'affichage	43	déclencher l'enregistrement de données texte	338
Caméra PTZ	313	décodeur	
Caméras UHD	141	Clavier numérique IntuiKey de Bosch	148
caméras HD	354	décodeur BVIP	
carte		ajouter	144, 187, 216, 224
zones réactives clignotantes	317, 339	Décodeur BVIP	82, 229
carte d'alarme	324	décodeur:mot de passe de destination	217, 234
cartes	266	déconnecté	360
centrale d'intrusion	165, 166	déconnexion automatique	122
chaîne de connexion	123	découplé	360
changement de mot de passe	180	déplacer un dispositif	202, 213, 236
changements rapides dans les capteurs	336	désactiver la protection forcée par mot de passe	106
changer de mot de passe	180	désactiver les sirènes	352
Clavier DCZ	160	dispositif ATM POS	127
clavier de vidéosurveillance	160	dispositif BVIP	
problèmes de connexion	384	mot de passe	146, 223, 235
clavier IntuiKey	160	page Web	223
Clavier IntuiKey de Bosch	52, 53, 54, 128, 139	dispositif DiBos	127
Clavier KBD universal XF	52	dispositifs sans protection par mot de passe	93
Clavier KBD universel XF	139	données de configuration	
Clavier KBD-Universal XF	53, 128	exporter	95
clavier numérique	160	données de configuration vers OPC	
Clavier numérique IntuiKey de Bosch	56, 148, 160	exporter	96
client Web	165	double autorisation	345
codecs	307	double diffusion	141
Commande d'orientation/d'inclinaison et de zoom		DSA E-Series	191, 192, 197, 198
blocage	347	DTP3N	154
commande d'une caméra	100, 307	duplication d'un événement	333
commandes CCL Allegiant	62	durée post-alarme	308
commandes CLL	163	durée post-événement	301, 308
commandes de menu	102	durée pré-événement	301, 308
comportement contextuel automatique des alarmes	40	E	
configuration de l'enregistrement VRM	99	effacer l'utilisateur	344
configuration par défaut	199	Émulation CCL	164
configuration précédente	94	émulation CCL Allegiant	163
configuration standard	199	accès refusé	163
configuration système	21	encodage sur les NVR	126, 177
connexion		encodeur	
clavier IntuiKey de Bosch et BVMS	54	ajouter	183, 193, 223, 379
matrice Allegiant et BVMS	57	page Web	223
consignation	333	encodeur BVIP	82, 229
contrôle PTZ		ajouter	144, 187, 216, 224
blocage	354	Encodeur BVIP :ajout	145, 230
copier et coller	302	encodeur:mot de passe de destination	217, 234
créer		240	
script de commande	90	enregistrement d'alarme	323, 337, 338
		enregistrement de pré-alarme	308

enregistrement double	29, 194, 314		
enregistrement manuel	43, 323, 337		
enregistrement RAM	308		
enregistrement redondant	29		
enregistrement secondaire	194, 314		
enregistreur numérique	127		
Enterprise Management Server	355		
Enterprise System	24		
Enterprise user groups	341		
entrée virtuelle	127		
état	96		
états	102, 107, 109, 110		
événement utilisateur	333		
événements combinés	316, 334		
événements personnalisés	316, 334		
exclure			
point	353		
exemples	98		
ajouter l'alarme d'entrée Bosch Allegiant	99		
configuration d'un enregistrement VRM	99		
exportation			
MOV	351		
script de commande	92		
exportation à distance	43		
exporter			
données de configuration	95		
données de configuration vers OPC	96		
Tableau des caméras	303		
F			
fiche technique	21		
fichier Allegiant	385		
fichiers de ressource	270		
importer	270		
fichiers HTML	266		
filtrage	108, 109, 110, 126, 267, 296, 316, 319, 322, 343		
Filtre de déblocage H.264	307		
flux	299, 310		
flux par défaut	139, 299		
Fonction intercom	352		
Fonction intercom audio	352		
fonctions du périphérique			
mise à jour	82, 229		
format 16/9	354		
fuseau horaire	219, 220		
G			
gestion des licences			
Bosch Video Management System	75		
Gestionnaire de licences			
serveur Stratus	75		
gestionnaire de périphériques	96		
groupe de moniteurs	149, 150, 323, 328		
ajouter	149		
caméra de démarrage	150		
caméra initiale	150		
OSD	150, 241, 328		
vue quadravision	150		
vue simple	150		
groupe de moniteurs analogiques	124, 128		
groupe LDAP	119, 371		
groupes d'utilisateurs	343		
groupes d'utilisateurs LDAP	119, 343, 371		
groupes d'utilisateurs	341		
H			
H.264	307		
hors ligne	344, 360		
I			
icônes de dispositif clignotantes	317, 339		
Identification de la personne			
Ajout de caméras à un dispositif d'identification de la personne	171		
Identification de personne			
Ajout d'un dispositif d'identification de personne	169		
Dispositif d'identification de personne	169		
importation			
script de commande	91		
importer			
fichiers de ressource	270		
impression de l'aide	15		
inactivité	122		
iPad	164, 165		
iPhone	164, 165		
J			
journalisation	179, 336		
journalisation des événements ONVIF	392		
journalisation ONVIF	392		
jours d'exception	293		
jours fériés	293		
L			
langue	383		
Configuration Client	122		
Operator Client	344		

langue de l'interface utilisateur graphique	383	mot de passe manquant	93
licences		mot de passe par défaut	93, 106
Assistant de configuration	72	mot de passe par défaut global	93
lien de carte link	278	mot de passe vide	93
lien vers une carte	278	MOV	351
Liste des serveurs		multicast	209
ajouter des colonnes	87, 132	N	
supprimer des colonnes	87, 132	nom de l'initiateur du serveur	178
LUN		notes de mise à jour	21
supérieure à 2 To	186	nouveaux périphériques DiBos	135, 136
LUN de grande taille	186, 190, 197, 203	NVR	21
M		O	
Management Server	21, 24, 360	Operator Client	17, 268
Map-based tracking assistant	285	Operator Client indépendant	360
Mappage des IQN	199	ordre de tri	
matrice Allegiant	127, 136, 137	alarmes	323
matrice analogique	136	P	
MIC IP 7000	382	Page Émulation CCL Allegiant	162
mise à jour		paramètres d'alarme généraux	336
fonctions du périphérique	82, 229	paramètres de l'interface	
mise à niveau du firmware		VIP XD	148
Clavier numérique IntuiKey de Bosch	56	Paramètres SNMP	117
mise en commun	174	pare-feu	209
Mobile Video Service	65	périphérique	127
mode à plusieurs moniteurs	354	périphérique de messagerie	127
mode compatibilité	43	périphérique de surveillance réseau	127
mode d'enregistrement		Périphérique DVR	133
automatique	185	périphérique iSCSI	199
basculement	185	Personne non autorisée	
mode d'enregistrement automatique	185	Personne non autorisée détectée	340
mode d'enregistrement de basculement	185	point	
encodeur	240	exclure	353
mode enregistrement d'alarme	308	pool de stockage VRM	195
mode hors ligne	360	poste de commande	124
modes d'affichage d'une caméra panoramique	43	préférences d'enregistrement (Recording preferences)	241
modification de l'adresse IP	238	priorité d'alarme	373
modification de l'adresse réseau	238	profil de qualité d'enregistrement	304
modification du mot de passe	146, 223, 235	Profil de support ONVIF	299
modification du mot de passe	344	protection forcée par mot de passe	106
modifier l'adresse IP	107, 127	protéger les enregistrements d'alarme	338
modifier l'adresse réseau	143	R	
modifier l'adresse IP	143	recherche	
modifier le mot de passe	344	informations dans l'aide	14
modifier mot de passe	223	périphériques	108, 109, 110, 126, 267, 296, 316, 319, 322, 343
modifier une zone de stockage	236	Recherche contextuelle	139
modules d'E/S	128	recherche de conflits d'adresses IP	106
mot de passe	146, 223, 235		
mot de passe de destination	217, 234		
mot de passe global par défaut	72, 106		

Recherche de serveur	132	tour de caméra	275, 277
reconnexion automatique	93	Traps SNMP	
redémarrage automatique	93	envoyer	117
regroupement	195	get	117
relais		trop de caméras Allegiant	385
dysfonctionnement	285	U	
relais de dysfonctionnement	285	urée post-événement	308
remplacement de dispositif	78	utilisateur	
remplacement des dispositifs	77	supprimer	344
remplacer le contenu	270	utilisateur LDAP	343
réseau de serveurs	218, 219, 220, 221	V	
réseau non fiable	164	vérifier l'authenticité	233
ROI	299, 314, 347	Video Analytics	168
S		Video Streaming Gateway	127
script de commande	266, 274	VIDEOJET connect 7000	382
aide du script de l'interface API de Bosch	90	VIP X1600 XFM4	307
exportation	92	VIP XD	52
importation	91	vue quadravision	150
Script de Commande client		VIP XD	
alarme acceptée	328	mode semi-duplex	148
exécuté au démarrage	92, 141	paramètres de l'interface	148
exécuté lors du démarrage	91	volet des périphériques	266
sélection multiple	268, 269	VRM	
séquence	277	ajouter	175
séquence d'alarme	323, 337	ajouter une zone de stockage	181
séquence de caméras	266, 275, 277	Basculement	29, 130, 181
Server ID	79	Basculement principal	181
serveur de synchronisation	84	Basculement secondaire	181
serveur OPC	383	Principal	29, 130, 176
serveur Stratus		redondant	29, 130, 182
gestion des licences	75	Secondaire	29, 130, 176
Serveur VRM de basculement principal	181	zone de stockage	181, 236
Service de transcodage	164, 165	VRM 3.50	184
Service vidéo mobile	164	VRM de basculement	29, 130, 181
silence sonneries	352	VRM de basculement secondaire	181
supprimer des positions prédéfinies	311	VRM principal	29, 130, 176
supprimer l'utilisateur	344	VRM redondant	29, 130, 182
synchronisation	84	VRM secondaire	29, 130, 176
synchronisation du temps	84	vue quadravision	150
synchroniser		W	
Configuration VRM	184	WLAN	164, 165
système de stockage iSCSI	195	Z	
Système d'entreprise	86	zone de stockage	
système tout-en-un	65	déplacer un dispositif	202, 213, 236
systèmes de contrôle d'accès	166	modifier	236
T		VRM	181, 236
Tableau d'enregistrement	296	zone de stockage iSCSI	174, 195
		Zone de stockage VRM	174

zone de visualisation de carte	280
Zone d'intérêt	299, 314, 347
zones réactives	266

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2024

Des solutions pour les bâtiments au service d'une vie meilleure

202404251917