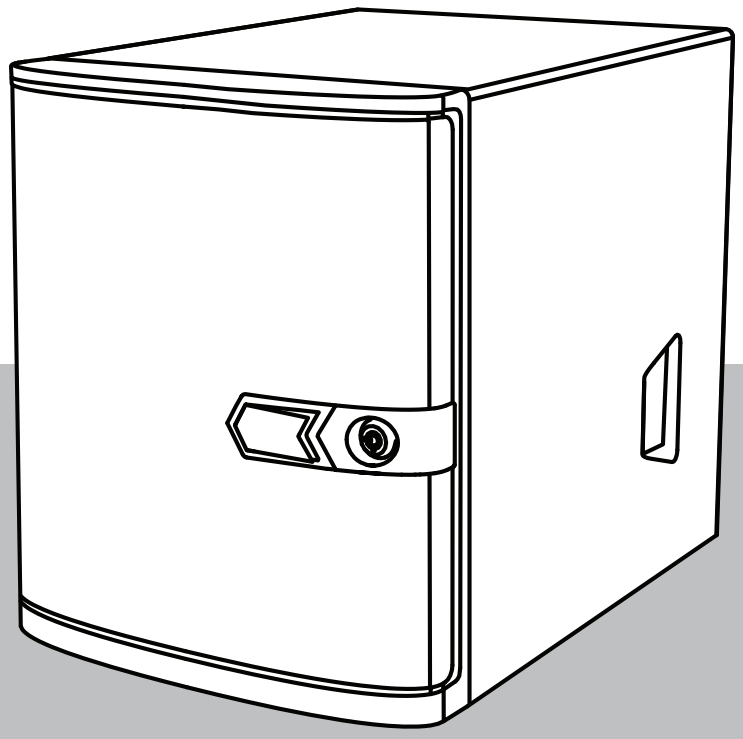
DIVAR IP all-in-one 4000

DIP-4420IG-00N | DIP-4424IG-2HD | DIP-4428IG-2HD | DIP-442IIG-2HD



fr Manuel d'utilisation

Table des matières

1 Sécurité

Veuillez respecter les consignes de sécurité figurant dans ce chapitre.

1.1 Précautions d'utilisation

Remarque!
Utilisation prévue
Ce produit est uniquement destiné à un usage professionnel. Il n'est pas destiné à être installé dans un espace public accessible à tous.

Remarque!
N'utilisez pas ce produit dans un endroit humide.

Remarque!
Prenez les précautions d'usage pour protéger le dispositif contre les surtensions du réseau électrique et contre la foudre.

Remarque!
Gardez la zone autour du dispositif propre et dégagée.

Remarque!
Orifices du caisson
N'obstruez en aucun cas ces orifices. Ils sont prévus pour la ventilation du caisson. Ils empêchent toute surchauffe et assurent la fiabilité du fonctionnement.

Remarque!
N'ouvrez pas ou ne retirez pas le capot du dispositif. L'ouverture ou le retrait du capot peut endommager le système et entraîner l'annulation de la garantie.

Remarque!
Ne renversez pas de liquides sur le dispositif.

Avertissement!
Observez la plus grande prudence en cas d'opération de maintenance ou d'utilisation à proximité du fond de panier. Lorsque le système est en fonctionnement, le fond de panier peut présenter une tension ou une énergie dangereuse. Ne touchez jamais le fond de panier avec un objet métallique et assurez-vous qu'aucun câble ruban n'est en contact avec le fond de panier.

Remarque!
Débranchez la source d'alimentation avant de déplacer le produit. Déplacez-le avec précaution. Des contraintes excessives ou des chocs sont susceptibles d'endommager le produit et les disques durs.

Avertissement!
La manipulation des matériaux de soudure au plomb utilisés dans ce produit peut vous exposer au plomb, un produit chimique reconnu par l'état de la Californie comme pouvant causer des malformations congénitales et d'autres troubles de l'appareil reproducteur.

Remarque!
La perte vidéo est inhérente à l'enregistrement vidéo numérique. C'est pourquoi Bosch Security Systems ne saurait être tenu responsable de tout dommage résultant d'un manque d'informations vidéo.
Afin de réduire les risques de perte d'informations, il est recommandé d'utiliser plusieurs systèmes d'enregistrement redondants et de mettre en œuvre une procédure de sauvegarde pour l'ensemble des informations analogiques et numériques.

1.2 Précautions en matière de cybersécurité

Pour des raisons de cybersécurité, respectez les points suivants :
- Veillez à ce que l'accès physique au système soit limité au personnel autorisé. Placez le système dans une zone protégée par contrôle d'accès afin d'éviter toute manipulation physique.
- Verrouillez le cache avant pour prévenir tout retrait non autorisé des disques durs. Retirez toujours la clé du verrou et rangez-la dans un endroit sûr.
- Utilisez le châssis arrière ou l'emplacement Kensington pour renforcer la sécurisation du dispositif.
- Le système d'exploitation inclut les tout derniers correctifs de sécurité Windows disponibles au moment où l'image logicielle a été créée. Utilisez la fonctionnalité de mise à jour en ligne de Windows ou les cumuls de correctifs mensuels correspondants pour une installation hors ligne afin d'installer régulièrement les mises à jour de sécurité du système d'exploitation.
- Ne désactivez pas Windows Defender ni le pare-feu Windows et gardez-les toujours à jour.
- N'installez pas de logiciel antivirus supplémentaire.
- Ne fournissez pas d'informations système ni de données sensibles aux personnes que vous ne connaissez pas à moins que vous ne soyez certain des droits de la personne.
- N'envoyez pas d'informations sensibles sur Internet avant d'avoir vérifié la sécurité d'un site Web.
- Restreignez l'accès au réseau local aux dispositifs de confiance uniquement. Les documents suivants, disponibles dans le catalogue en ligne des produits, contiennent des détails supplémentaires :
  - *Authentification réseau 802.1X*
  - *Guide sur la cybersécurité pour les produits vidéo IP Bosch*
- Pour un accès via les réseaux publics, utilisez uniquement les canaux de communication sécurisés (cryptés).
- Le compte administrateur offre des droits d'administration complets et un accès illimité au système. Les droits d'administration permettent aux utilisateurs d'installer, de mettre à jour ou de supprimer des logiciels et de modifier les paramètres de configuration. De plus, les droits d'administration permettent aux utilisateurs d'accéder directement aux clés du registre et de les modifier, et ainsi de contourner les paramètres de sécurité et de gestion centralisée. Les utilisateurs connectés au compte administrateur peuvent franchir les pare-feu et supprimer les logiciels antivirus, ce qui expose le système aux virus et aux

cyberattaques. Cela peut constituer un risque important pour le système et la sécurité des données.
Pour minimiser les risques de cybersécurité, respectez les conseils suivants :
- Assurez-vous que le compte administrateur est protégé par un mot de passe complexe conforme à la stratégie de mot de passe.
- Assurez-vous que seul un nombre limité d'utilisateurs de confiance ont accès au compte administrateur.

– En raison des conditions d'utilisation requises, le lecteur système ne doit pas être chiffré. Sans chiffrement, il est facile d'accéder aux données stockées sur ce disque et de les supprimer. Pour éviter le vol de données ou une perte accidentelle de données, assurez-vous que seules les personnes autorisées ont accès au système et au compte administrateur.
– Pour installer et mettre à jour des logiciels ainsi que pour restaurer le système, il peut être nécessaire d'utiliser des dispositifs USB. Les ports USB de votre système ne doivent donc pas être désactivés. Toutefois, la connexion de dispositifs USB au système présente un risque d'infection par logiciel malveillant. Pour éviter les attaques par logiciels malveillants, assurez-vous qu'aucun dispositif USB infecté n'est connecté au système.

1.3 Précautions logicielles

1.3.1 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.
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.

Vous trouverez les derniers logiciels et les progiciels de mise à niveau disponibles dans le magasin de téléchargement de Bosch Security and Safety Systems, sous : https://downloadstore.boschsecurity.com/

1.3.2 Information OSS

Bosch utilise un logiciel open source dans les produits DIVAR IP all-in-one.
Vous trouverez les licences des composants logiciels open source utilisés sur le lecteur système à l'adresse :

C:\license txt

Les licences des composants logiciels open source utilisés dans tout autre logiciel installé sur votre système sont stockées dans le dossier d'installation de chaque logiciel, par exemple sous :

C:\Program Files\Bosch\SysMgmService\apps\sysmgm-commander\[version]\License

ou sous :

C:\Program Files\Bosch\SysMgmService\apps\sysmgm-executor\[version]\License

2 Introduction

DIVAR IP all-in-one 4000 est une solution de gestion, d'enregistrement et de visualisation tout-en-un simple et économique destinée aux réseaux de vidéosurveillance prenant en charge jusqu'à 32 voies (avec 8 voies sous pré-licence).
DIVAR IP all-in-one 4000 est une mini-tour à 2 baies associant des capacités Bosch Video Management System avancées et une gestion des enregistrements de pointe dans un dispositif d'enregistrement IP abordable et facile à installer et à utiliser, pour les clients du secteur informatique.
DIVAR IP all-in-one 4000 bénéficie d'une conception intégrée et de composants de base. Cette solution est basée sur le système d’exploitation Microsoft Windows Server IoT 2022 for Storage Workgroup.
Le DIVAR IP all-in-one 4000 dispose de disques durs SATA amovibles par la face avant « conçus pour l'entreprise » et offrant jusqu'à 36 To de capacité de stockage brute.

3 Présentation du système

Système d'exploitation

Le système d'exploitation Microsoft Windows Server IoT 2022 for Storage Workgroup offre une interface utilisateur unique pour la configuration initiale du serveur, la gestion unifiée des dispositifs de stockage, la configuration et la gestion simplifiées du stockage, ainsi que la prise en charge de Microsoft iSCSI Software Target.
Celui-ci est spécialement configuré pour permettre aux systèmes de stockage en réseau d'atteindre des performances optimales. Le système d'exploitation Microsoft Windows Server IoT 2022 for Storage Workgroup apporte des améliorations considérables en termes de gestion du stockage, mais aussi d'intégration des composants et des fonctionnalités de gestion des dispositifs de stockage.

DIVAR IP System Manager

L'application DIVAR IP System Manager est une interface utilisateur centrale qui simplifie l'installation du système, sa configuration et les mises à niveau logicielles.

Modes de fonctionnement

Les systèmes DIVAR IP all-in-one 4000 peuvent fonctionner dans trois modes différents :

- Système de gestion et d'enregistrement vidéo complet, utilisant les composants et services principaux BVMS et Video Recording Manager.
  Ce mode fournit une solution de sécurité vidéo IP unique qui permet une gestion transparente des flux vidéo et audio, ainsi que des métadonnées sur un réseau IP. Il associe de manière transparente caméras IP et encodeurs, permet la gestion des événements et des alarmes à l'échelle du système, surveille l'état du système et assure la gestion des priorités et des utilisateurs. Ce mode constitue le système de gestion vidéo le plus adapté aux dispositifs de vidéosurveillance Bosch, bénéficiant des fonctionnalités uniques des solutions d'enregistrement et des caméras Bosch. Il inclut des composants Video Streaming Gateway pour intégrer des caméras tierces.
- Système d'enregistrement vidéo, qui utilise les principaux composants et services Video Recording Manager et bénéficiant des fonctionnalités uniques des solutions d'enregistrement et des caméras Bosch.
- Extension de stockage iSCSI pour un système BVMS ou Video Recording Manager, qui s'exécute sur un autre matériel. Jusqu'à deux de ces extensions de stockage iSCSI peuvent être ajoutées à un système BVMS ou Video Recording Manager en cours d'exécution un DIVAR IP all-in-one 4000.

Lorsque vous configurez le système, dans l'application DIVAR IP System Manager, vous devez choisir le mode de fonctionnement souhaité pour la configuration de votre système.
Avec l'application DIVAR IP System Manager, vous pouvez également mettre à jour et à niveau le logiciel installé.
Vous trouverez les derniers logiciels et les progiciels de mise à niveau disponibles dans le magasin de téléchargement de Bosch Security and Safety Systems, sous :
https://downloadstore.boschsecurity.com/

Remarque!
Les flux vidéo enregistrés doivent être configurés de manière à ce que la bande passante maximale du système (système de base BVMS/VRM et extensions de stockage iSCSI) ne soit pas dépassée.

4 Configuration du système

4.1 Paramètres par défaut

Tous les systèmes DIVAR IP sont préconfigurés à l'aide de l'adresse IP et des paramètres iSCSI par défaut :

- Adresse IP : automatiquement affectées par DHCP (adresse IP de secours : 192.168.0.200).
- Masque de sous-réseau : automatiquement affecté par DHCP (masque de sous-réseau de secours : 255.255.255.0).

Paramètres utilisateur par défaut pour le compte administrateur

- Nom d'utilisateur : **BVRAdmin**
- Mot de passe : à définir lors de la première connexion
  Exigences de mot de passe :
  - 14 caractères minimum.
  - Au moins une lettre majuscule.
  - Au moins une lettre minuscule.
  - Au moins un chiffre.

4.2 Exigences préalables

Tenez compte des points suivants :

- Le modèle DIVAR IP nécessite une liaison réseau active lors de l'installation. Assurez-vous que le commutateur réseau auquel vous vous connectez est sous tension.
- L'adresse IP par défaut ne doit pas être occupée par un autre périphérique du réseau. Veillez à ce que les adresses IP par défaut des systèmes DIVAR IP existants sur le réseau soient modifiées avant d'en ajouter un autre DIVAR IP.

4.3 Première connexion et configuration initiale du système

Remarque!
Ne modifiez aucun paramètre du système d'exploitation. Une modification des paramètres du système d'exploitation peut entraîner un dysfonctionnement du système.

Remarque!
Pour effectuer des tâches d'administration, vous devez vous connecter au compte administrateur.

Remarque!
En cas de perte du mot de passe, une restauration du système doit être exécutée comme décrit dans le manuel d'installation. La configuration doit être à nouveau effectuée depuis le début ou être importée.

Pour configurer le système :

1. Connectez l'unité DIVAR IP all-in-one et les caméras au réseau.
2. Mettez l'unité sous tension.
   Les routines d'installation de Microsoft Windows Server IoT 2022 for Storage Workgroup sont exécutées. Cette opération peut prendre quelques minutes. N'éteignez pas le système.
   Une fois le processus terminé, l'écran de sélection de langue Windows s'affiche.

3. Sélectionnez votre pays/région, la langue du système d'exploitation et la disposition du clavier souhaitées dans la liste, puis cliquez sur **Suivant**.
   Le contrat de licence logicielle Microsoft s'affiche.
4. Cliquez sur **Accepter** pour accepter les conditions de la licence et attendez que Windows redémarre. Cette opération peut prendre quelques minutes. Ne mettez pas le système hors tension.
   Après le redémarrage, la page de connexion Windows s'affiche.
5. Définissez un nouveau mot de passe pour le compte administrateur **BVRAdmin** et confirmez-le.
   Exigences de mot de passe :
   - 14 caractères minimum.
   - Au moins une lettre majuscule.
   - Au moins une lettre minuscule.
   - Au moins un chiffre.

   Appuyez ensuite sur Entrée**.**
   La page **Software Selection** s'affiche.
6. Le système scanne automatiquement le lecteur local et tout support de stockage externe connecté pour rechercher le fichier d'installation de DIVAR IP System Manager **SystemManager_x64_[software version].exe**, lequel se trouve dans un dossier dont la structure est la suivante : *Drive root\BoschAppliance*.
   L'analyse peut prendre un certain temps. Attendez que la recherche se termine.
7. Dès que le système a détecté le fichier d'installation, celui-ci s'affiche sur la page **Software Selection**. Cliquez sur la barre affichant le fichier d'installation pour démarrer l'installation.
8. Si la recherche ne permet pas de trouver le fichier d'installation, procédez comme suit :
   - Accédez à https://downloadstore.boschsecurity.com/.
   - Sous **Software** l'onglet, sélectionnez **BVMS Appliances** dans la liste, puis cliquez sur **Select**.
     La liste de tous les logiciels disponibles s'affiche.
   - Localisez le fichier ZIP **SystemManager_[software version].zip** et enregistrez-le sur un support de stockage tel qu'une clé USB.
   - Décompressez le fichier sur le support de stockage en vous assurant que le dossier **BoschAppliance** se trouve à la racine du support de stockage.
   - Connectez le support de stockage au système DIVAR IP all-in-one.
     Le système recherche automatiquement le support de stockage du fichier d'installation.
     L'analyse peut prendre un certain temps. Attendez que la recherche se termine.
   - Une fois le fichier d'installation détecté, il s'affiche sur la page **Software Selection**. Cliquez sur la barre affichant le fichier d'installation pour démarrer l'installation.
     Remarque : Pour être détecté automatiquement, le fichier d'installation doit être placé dans un dossier dont la structure est la suivante : *Drive root\BoschAppliance* (par exemple *F:\BoschAppliance*).
     Si le fichier d'installation se trouve à un autre emplacement qui ne correspond pas à la structure de dossier prédéfinie, cliquez sur  pour accéder à l'emplacement correspondant. Cliquez ensuite sur le fichier d'installation pour commencer l'installation.

9. Avant de démarrer l'installation, la boîte de dialogue **End User License Agreement (EULA)** s'affiche. Lisez les termes du contrat de licence, puis cliquez sur **Accept** pour continuer. L'installation démarre.
10. Une fois l'installation terminée, le système redémarre et vous redirige vers la page de connexion Windows. Connectez-vous au compte administrateur.
11. Le navigateur Microsoft Edge s'ouvre et la page **DIVAR IP - Paramétrage du système** s'affiche. La page affiche le type de périphérique et le numéro de série du périphérique, ainsi que les trois modes de fonctionnement et les versions logicielles disponibles pour chaque mode de fonctionnement.
    Vous devez choisir le mode de fonctionnement souhaité et la version du logiciel de votre choix pour configurer votre système DIVAR IP all-in-one.
    Remarque : Si la version logicielle souhaitée pour le mode de fonctionnement correspondant n'est pas disponible sur un disque local, procédez comme suit :
    - Accédez à https://downloadstore.boschsecurity.com/.
    - Sous **Software** l'onglet, sélectionnez **BVMS Appliances** dans la liste, puis cliquez sur **Select**.
      La liste de tous les logiciels disponibles s'affiche.
    - Localisez les fichiers ZIP des packages logiciels souhaités, par exemple **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, et enregistrez-les sur un support de stockage tel qu'une clé USB.
    - Décompressez les fichiers sur le support de stockage. Ne modifiez pas la structure des dossiers des fichiers décompressés.
    - Connectez le support de stockage à votre système DIVAR IP all-in-one.

Remarque!
La modification du mode de fonctionnement après l'installation nécessite une réinitialisation complète.

4.3.1 Choix du mode de fonctionnement BVMS

Pour utiliser le système DIVAR IP all-in-one en tant que système de gestion et d'enregistrement vidéo :

1. Sur la page **DIVAR IP - Paramétrage du système**, sélectionnez le mode de fonctionnement **BVMS** et la version BVMS que vous souhaitez installer, puis cliquez sur **Suivant**.
   Le BVMS contrat de licence s'affiche.
2. Lisez et acceptez le contrat de licence, puis cliquez sur **Installer** pour continuer.
   L'installation démarre et la boîte de dialogue d'installation indique la progression de l'installation. N'éteignez pas le système et ne retirez pas le support de stockage durant le processus d'installation.
3. Une fois tous les packages logiciels correctement installés, le système redémarre. Après le redémarrage, vous êtes dirigé vers le bureau de BVMS.
4. Sur le bureau de BVMS, cliquez sur l'application souhaitée pour configurer votre système.

Remarque!
Pour de plus amples informations, reportez-vous à la formation Web DIVAR IP all-in-one correspondante et à la documentation BVMS.
La formation est disponible à l'adresse suivante : www.boschsecurity.com/xc/en/support/training/

4.3.2 Choix du mode de fonctionnement VRM

Pour utiliser le système DIVAR IP all-in-one en tant que système d'enregistrement vidéo pur :

1. Sur la page **DIVAR IP - Paramétrage du système**, sélectionnez le mode de fonctionnement **VRM** et la version VRM que vous souhaitez installer**,** puis cliquez sur **Suivant**.
   Le VRM contrat de licence s'affiche.
2. Lisez et acceptez le contrat de licence, puis cliquez sur **Installer** pour continuer.
   L'installation démarre et la boîte de dialogue d'installation indique la progression de l'installation. N'éteignez pas le système et ne retirez pas le support de stockage durant le processus d'installation.
3. Une fois tous les packages logiciels correctement installés, le système redémarre. Après le redémarrage, vous êtes dirigé vers l'écran de connexion Windows.

Remarque!
Pour plus d'informations, consultez la documentation de VRM.

4.3.3 Choix du mode de fonctionnement du stockage iSCSI

Pour utiliser le système DIVAR IP all-in-one en tant qu'extension de stockage iSCSI :

1. Sur la page **DIVAR IP - Paramétrage du système**, sélectionnez le mode de fonctionnement **Stockage iSCSI** et la version de stockage iSCSI que vous souhaitez installer**,** puis cliquez sur
   Suivant. La boîte de dialogue d'installation s'affiche.
2. Dans la boîte de dialogue d'installation, cliquez sur **Installer** pour continuer.
   L'installation démarre et la boîte de dialogue d'installation indique la progression de l'installation. N'éteignez pas le système et ne retirez pas le support de stockage durant le processus d'installation.
3. Une fois tous les packages logiciels correctement installés, le système redémarre. Après le redémarrage, vous êtes dirigé vers l'écran de connexion Windows.
4. Ajoutez le système en tant qu'extension de stockage iSCSI à un serveur BVMS ou VRM externe en utilisant BVMS Configuration Client ou Configuration Manager.

Remarque!
Pour plus d'informations, consultez la documentation de BVMS ou Configuration Manager.

5 Mise à niveau du logiciel

L'application DIVAR IP System Manager permet de mettre à niveau les logiciels installés sur votre système.
Vous trouverez les derniers logiciels et les progiciels de mise à niveau disponibles dans le magasin de téléchargement de Bosch Security and Safety Systems, sous :
https://downloadstore.boschsecurity.com/

Remarque!
Le rétrogradation du logiciel installé à une version antérieure n'est pas prise en charge.

Pour mettre à niveau le logiciel installé :

1. Accédez à https://downloadstore.boschsecurity.com/.
2. Sous **Software** l'onglet, sélectionnez **BVMS Appliances** dans la liste, puis cliquez sur **Select**.
   La liste de tous les logiciels disponibles s'affiche.
3. Localisez les fichiers ZIP des packages logiciels souhaités, par exemple **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, et enregistrez-les sur un support de stockage tel qu'une clé USB.
4. Décompressez les fichiers sur le support de stockage. Ne modifiez pas la structure des dossiers des fichiers décompressés.
5. Lancez l'application DIVAR IP System Manager :
   - Si vous êtes connecté à Windows **BVRAdmin** avec le compte administrateur, double-cliquez sur l'icône DIVAR IP System Manager du bureau Windows.
     L'application DIVAR IP System Manager démarre.
   - Si votre système fonctionne en mode BVMS, cliquez sur l'icône DIVAR IP System Manager du bureau BVMS et connectez-vous au compte administrateur BVRAdmin.
     L'application DIVAR IP System Manager s'ouvre dans une boîte de dialogue plein écran. (Vous pouvez quitter la boîte de dialogue en appuyant sur Alt+ F4).
6. La page **Packages logiciels** affiche le type de périphérique et son numéro de série en haut de la page.

- Dans la colonne **Nom**, vous voyez toutes les applications logicielles DIVAR IP System Manager déjà installées sur votre système, ainsi que toutes les autres applications logicielles DIVAR IP System Manager détectées par le système sur le disque **Images** ou sur un support de stockage.
- Dans la colonne **Version installée** figure la version de l'application logicielle actuellement installée sur votre système.
- La colonne **État** indique l'état de l'application logicielle correspondante :
  - L'icône  indique qu'aucune version ultérieure du logiciel installé n'a été détectée par le système sur le disque **Images** ou sur un support de stockage.
    Remarque : pour vous assurer d'utiliser la dernière version du logiciel, vérifiez les versions logicielles disponibles dans le magasin de téléchargement Bosch Security and Safety Systems sous :
    https://downloadstore.boschsecurity.com/

  - L'icône indique que le système a détecté des versions ultérieures du logiciel installé sur le disque **Images** ou sur un support de stockage.
    Cette icône s'affiche également si le système a détecté une application logicielle qui n'est pas encore installée sur votre système.
- La colonne vous permet **Version disponible** de voir les versions ultérieures des applications logicielles installées. Le système a détecté ces versions sur le disque dur **Images** ou sur un support de stockage.
  La colonne affiche également les versions disponibles des applications logicielles détectées qui ne sont pas encore installées sur votre système.
  Remarque : seules les versions ultérieures des applications logicielles installées sont affichées. Le rétrogradation d'un logiciel à une version antérieure n'est pas prise en charge.

7. Dans la colonne **Nom**, cliquez sur le bouton d'option correspondant pour sélectionner l'application logicielle à mettre à niveau ou à installer.
8. Dans la colonne **Version disponible**, sélectionnez la version vers laquelle vous souhaitez mettre à niveau votre logiciel, ou que vous souhaitez installer, puis cliquez sur **Suivant**.
   Le cas échéant, la boîte de dialogue du contrat de licence s'affiche.
9. Lisez et acceptez le contrat de licence, puis cliquez sur **Installer** pour continuer.
   L'installation démarre et la boîte de dialogue d'installation indique la progression de l'installation. N'éteignez pas le système et ne retirez pas le support de stockage durant le processus d'installation.
10. Une fois tous les logiciels installés correctement, le message **Installation réussie terminée.** s'affiche en haut de la page.
11. Si l'installation échoue, le message **Échec de l'installation.** s'affiche et l'icône  apparaît. Dans ce cas, appuyez sur F5 pour revenir à la page **Packages logiciels**.
    Téléchargez à nouveau les logiciels et réessayez.
    Si le problème persiste, contactez le service technique.

6 Connexion à distance au système

Vous pouvez établir une connexion à distance avec votre système DIVAR IP all-in-one et y accéder via Internet.
Pour créer une connexion à distance, procédez comme suit :

1. *Protection du système contre tout accès non autorisé, page 15*.
2. *Configuration du transfert de port, page 15*.
3. *Choix d'un client approprié, page 15*.

6.1 Protection du système contre tout accès non autorisé

Afin de protéger le système contre tout accès non autorisé, nous vous recommandons de suivre des règles de mot de passe fort avant de connecter le système à Internet. Plus votre mot de passe est puissant, plus votre système est protégé des personnes non autorisées et des logiciels malveillants.

6.2 Configuration du transfert de port

Pour accéder à un système DIVAR IP all-in-one à partir d'Internet via un routeur NAT/PAT, le transfert de port doit être configuré sur le système DIVAR IP all-in-one et sur le routeur.

Pour configurer le transfert de port :

- Saisissez les règles de port suivantes dans les paramètres de transfert de port de votre routeur Internet :
  - port 5322 pour l'accès au tunnel SSH avec BVMS Operator Client.
    Remarque : cette connexion n'est valable que pour le mode de fonctionnement BVMS.
  - port 443 pour un accès HTTPS à VRM avec Video Security Client ou Video Security App.
    Remarque : cette connexion n'est valable que pour le mode de fonctionnement BVMS ou VRM.

Votre système DIVAR IP all-in-one est à présent accessible depuis Internet.

6.3 Choix d'un client approprié

Vous avez deux options pour établir une connexion à distance avec votre système DIVAR IP all-in-one :

- *Connexion à distance avec BVMS Operator Client, page 15*.
- *Connexion à distance avec l'application de sécurité vidéo, page 16*.

Remarque!
La compatibilité des versions BVMS Operator Client ou Video Security App est déterminée par les versions des logiciels BVMS ou VRM installés dans DIVAR IP.
Pour plus d'informations, consultez la documentation logicielle et les ressources de formation correspondantes.

6.3.1 Connexion à distance avec BVMS Operator Client

Remarque!
Cette connexion n'est valable que pour le mode de fonctionnement BVMS.

Pour établir une connexion à distance avec BVMS Operator Client :

1. Installez BVMS Operator Client sur le poste de commande client.

2. Une fois l'installation effectuée, lancez Operator Client à l'aide du raccourci de bureau  .
3. Entrez ce qui suit, puis cliquez sur **OK**.
   Nom d'utilisateur : admin (ou un autre utilisateur s'il a été configuré)
   Mot de passe : mot de passe utilisateur
   Connexion : ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

6.3.2 Connexion à distance avec l'application de sécurité vidéo

Remarque!
Cette connexion n'est valable que pour le mode de fonctionnement BVMS ou VRM.

Pour établir une connexion à distance avec Video Security App :
1. Dans Apple App Store, recherchez Bosch Video Security.
2. Installez l'application Video Security sur votre dispositif iOS.
3. Démarrez l'application Video Security.
4. Sélectionnez **Add**.
5. Saisissez l'adresse IP publique ou le nom dynDNS.
6. Assurez-vous que la connexion sécurisée (SSL) est active.
7. Sélectionnez **Add**.
8. Entrez ce qui suit :
   Nom d'utilisateur : admin (ou autre utilisateur s'il est configuré)
   Mot de passe : entrer le mot de passe de l'utilisateur

6.4 Connexion à Enterprise Management Server

Pour une gestion centralisée de plusieurs systèmes DIVAR IP all-in-one en mode de fonctionnement BVMS, vous pouvez utiliser un serveur BVMS Enterprise Management Server installé sur un serveur distinct.
Pour des informations plus détaillées sur la configuration et l'utilisation de BVMS Enterprise System, consultez la documentation et les ressources de formation de BVMS.

7 Maintenance

7.1 Connexion au compte administrateur

Connexion au compte administrateur en mode de fonctionnement BVMS

Pour vous connecter au compte administrateur en mode de fonctionnement BVMS :

1. Sur le bureau BVMS, appuyez sur Ctrl+Alt+Suppr.
2. Maintenez enfoncée la touche Maj de gauche immédiatement après avoir cliqué sur **Switch User (Changer d'utilisateur)**.
3. Appuyez de nouveau sur Ctrl+Alt+Suppr.
4. Sélectionnez l'utilisateur **BVRAdmin** et saisissez le mot de passe qui a été défini lors de la configuration du système. Appuyez ensuite sur Entrée.

Remarque : Pour revenir au bureau BVMS, appuyez sur Ctrl+Alt+Suppr et cliquez sur **Switch user (Changer d'utilisateur)** ou **Sign out (Se déconnecter)**. Le système revient automatiquement au bureau BVMS sans redémarrage du système.

Connexion au compte administrateur en mode de fonctionnement VRM ou iSCSI

Pour vous connecter au compte administrateur en mode de fonctionnement VRM ou iSCSI :

- Sur l'écran de connexion Windows, appuyez sur Ctrl+Alt+Suppr et saisissez le mot de passe **BVRAdmin**.

7.2 Surveillance du système

Les systèmes DIVAR IP all-in-one sont fournis avec l'application **SuperDoctor** préinstallée que vous pouvez utiliser pour surveiller votre système.

Activation de la fonctionnalité de surveillance

Pour activer la fonctionnalité de surveillance :

1. Connectez-vous au compte administrateur (voir *Connexion au compte administrateur, page 17*).
2. Sur le bureau, dans le dossier **Tools**, cliquez avec le bouton droit de la souris sur le script **startSD5Service**, puis cliquez sur **Run with PowerShell**.
3. Double-cliquez sur l'icône **SuperDoctor 5 Web** de votre bureau.
4. Connectez-vous à l'interface Web à l'aide des identifiants par défaut suivants :
   - Nom d'utilisateur : **admin**
   - Mot de passe : **DivaripSD5**
5. Cliquez sur l'onglet **Configuration**, puis cliquez sur **Account Setting** et modifiez le mot de passe par défaut.
   Remarque : Bosch recommande vivement de modifier le mot de passe par défaut immédiatement après la première connexion à l'application SuperDoctor**SuperDoctor**.
6. Sous l'onglet **Configuration**, cliquez sur **Alert Configuration**.
7. Activez la fonctionnalité **SNMP Trap** et spécifiez l'adresse IP du récepteur pour les alertes SNMP.

Désactivation de la fonctionnalité de surveillance

Pour désactiver la fonctionnalité de surveillance :

1. Connectez-vous au compte administrateur (voir *Connexion au compte administrateur, page 17*).
2. Sur le bureau, dans le dossier **Tools**, cliquez avec le bouton droit de la souris sur le script **stopSD5Service**, puis cliquez sur **Run with PowerShell**.

7.3 Remplacement d’un disque dur défectueux et configuration d’un nouveau disque dur

Si un disque dur installé sur votre système DIVAR IP all-in-one est défectueux et ne peut plus être utilisé, procédez comme suit :

1. *Remplacement d’un disque dur défectueux, page 18*.
2. *Configuration d’un nouveau disque dur, page 18*.

Remarque!

Bosch ne saurait être tenu responsable de toute perte de données, de dommages ou de défaillances système des appareils équipés de disques durs non fournis par Bosch. Bosch ne pourra offrir aucune assistance si le problème est dû à des disques durs non fournis par Bosch. Pour résoudre les problèmes matériels potentiels, les disques durs installés doivent avoir été fournis par Bosch.

7.3.1 Remplacement d’un disque dur défectueux

Pour remplacer un disque dur défectueux :

1. Mettez l’unité DIVAR IP all-in-one hors tension.
2. Retirez le disque dur défectueux de l’unité et installez le nouveau disque dur.
   Reportez-vous au chapitre *Installation d’un disque dur SATA* dans le manuel d’installation.

7.3.2 Configuration d’un nouveau disque dur

Pour configurer un nouveau disque dur, procédez comme suit :

1. *Création d’une nouvelle partition et d’un nouveau volume, page 18*
2. *Activation du service du serveur, page 19*.
3. *Création des LUN (disques virtuels iSCSI), page 19*.
4. *Désactivation du service du serveur, page 20*.
5. *Formatage des LUN, page 20*.

Création d’une nouvelle partition et d’un nouveau volume

Pour créer une nouvelle partition et un nouveau volume :

1. Dans le menu **Démarrer** de Windows, sélectionnez **Server Manager**, puis **File and Storage Services** > **Volumes** > **Disks**.
   Tous les disques durs installés sur votre système s’affichent.
2. Cliquez avec le bouton droit de la souris sur le nouveau disque dur que vous avez installé, puis cliquez sur **New Volume...**
   . La boîte de dialogue **New Volume Wizard** s’affiche.
3. Cliquez sur **Next** pour continuer.
   La boîte de dialogue **Server and Disk** s'affiche.
4. Sélectionnez le serveur et le disque correspondants, puis cliquez sur **Next** pour continuer.
   La boîte de dialogue **Size** s’affiche.
5. Dans le champ **Volume size:**, entrez la taille de volume que vous souhaitez utiliser. Si vous souhaitez utiliser la taille de volume maximale, gardez la valeur présélectionnée. Cliquez ensuite sur **Next** pour continuer.
   La boîte de dialogue **Drive Letter or Folder** s’affiche.
6. Dans la liste **Drive letter:**, sélectionnez la lettre du lecteur à attribuer au volume, puis cliquez sur **Next** pour continuer.
   La boîte de dialogue **File System Settings** s’affiche.
7. Appliquez les paramètres suivants :
   – **File system: NTFS**

- **Allocation unit size: Default**
- **Volume label:** entrez le même nom de volume que celui du disque défectueux remplacé (**Data** ou **Data2**).

8. Cliquez sur **Next** pour continuer.
   La boîte de dialogue **Confirmation** s'affiche.
9. Vérifiez que tous les paramètres sont corrects, puis cliquez sur **Create**.
   Le système commence la création de la nouvelle partition et du nouveau volume.
   Une fois la création terminée, la boîte de dialogue **Results** s'affiche.
10. Cliquez sur **Next** pour continuer.
    La nouvelle partition et le nouveau volume sont créés et l'espace de stockage est alloué.

Activation du service du serveur

1. Dans le menu **Démarrer** de Windows, sélectionnez **Services.**
   La boîte de dialogue **Services** s'affiche.
2. Localisez le service **Server** dans la liste, puis double-cliquez dessus.
   La boîte de dialogue **Server Properties** s'affiche.
3. Sous l'onglet **General**, dans la liste **Startup type:**, sélectionnez **Manual**, puis cliquez sur **Apply**.
4. Sous **Service status:**, cliquez sur **Start** pour démarrer le service, puis sur **OK** pour appliquer les modifications. Ensuite, fermez la boîte de dialogue **Services**.

Création des LUN (disques virtuels iSCSI)

1. Dans le menu **Démarrer** de Windows, sélectionnez **Server Manager**, puis **File and Storage Services** > **iSCSI**.
   Tous les disques virtuels iSCSI de votre système sont affichés.
2. Cliquez avec le bouton droit de la souris sur le LUN (le disque virtuel iSCSI) du disque dur remplacé, dont l'état est **Error,** puis cliquez sur **Remove iSCSI Virtual Disk**.
   La boîte de dialogue **Remove iSCSI Virtual Disk** s'affiche.
3. Cliquez sur **OK** pour confirmer la suppression du LUN.
4. Répétez cette procédure pour tous les LUN dont l'état est **Error**.
5. Dans la boîte de dialogue **iSCSI VIRTUAL DISKS**, cliquez avec le bouton droit de la souris sur un espace vide, puis cliquez sur **New iSCSI Virtual Disk...**
   . La boîte de dialogue **iSCSI Virtual Disk Location** s'affiche.
6. Sous **Server**, sélectionnez le serveur correspondant, sous **Storage location:**, sélectionnez **Type a custom path** et saisissez la lettre que vous avez attribuée au nouveau disque dur (voir *Création d'une nouvelle partition et d'un nouveau volume, page 18*). Cliquez ensuite sur **Next** pour continuer.
   La boîte de dialogue **iSCSI Virtual Disk Name** s'affiche.
7. Dans le champ **Name:**, saisissez le nom du LUN. Cliquez ensuite sur **Next** pour continuer.
   La boîte de dialogue **iSCSI Virtual Disk Size** s'affiche.
8. Dans le champ **Size**, saisissez 2 000 et modifiez l'unité de volume en **GB**
   Si la capacité du LUN est inférieure à 2 000 Go, configurez la taille du LUN sur la valeur de l'espace disponible en Go moins 50 Mo.
9. Sous **Fixed size:**, cochez la case **Clear the virtual disk on allocation**. Cliquez ensuite sur **Next** pour continuer.
   La boîte de dialogue **iSCSI Target** s'affiche.
10. Sous **Existing iSCSI target:**, sélectionnez **TG0**. Cliquez ensuite sur **Next** pour continuer.
    La boîte de dialogue **Confirmation** s'affiche.

11. Vérifiez que tous les paramètres sont corrects, puis cliquez sur **Create**.
    Le système commence la création du nouveau disque virtuel iSCSI.
    Une fois la création terminée, la boîte de dialogue **Results** s'affiche.
12. Cliquez sur **Close** pour fermer la boîte de dialogue.
13. Répétez ces étapes pour créer d'autres LUN en utilisant tout l'espace disponible.
14. Une fois créés, les LUN figurent dans la liste **iSCSI VIRTUAL DISKS**.

Désactivation du service du serveur

1. Dans le menu **Démarrer** de Windows, sélectionnez **Services.**
   La boîte de dialogue **Services** s'affiche.
2. Localisez le service **Server** dans la liste, puis double-cliquez dessus.
   La boîte de dialogue **Server Properties** s'affiche.
3. Sous l'onglet **General**, sous **Service status:**, cliquez sur **Stop** pour arrêter le service.
4. Dans la liste **Startup type:**, sélectionnez **Disabled**, puis cliquez sur **Apply**.
5. Cliquez sur **OK** pour appliquer les modifications, puis fermez la boîte de dialogue **Services**.

Formatage des LUN

1. Démarrez BVMS Configuration Client.
2. Dans l'**Arborescence des Périphériques**, accédez au groupe incluant le disque dur défectueux, cliquez avec le bouton droit de la souris sur la cible iSCSI **TG0**, puis cliquez sur **Rechercher cible** pour mettre à jour la liste des LUN disponibles sur cette cible iSCSI. Cela supprimera les LUN associés au disque dur défectueux et ajoutera les LUN créés sur le nouveau disque dur.
3. La boîte de dialogue **LUN** répertorie tous les LUN disponibles et indique leur état (formaté ou non formaté).
4. Sélectionnez les LUN non formatés et cliquez sur **Formater LUN**Format LUN. Cliquez ensuite sur **OK** pour continuer.
5. Une fois le formatage terminé, une boîte de dialogue de confirmation s'affiche. Cliquez sur **OK** pour finaliser le processus.

7.4 Collecte des fichiers journaux du système DIVAR IP

L'application DIVAR IP System Manager inclut un script dédié pour simplifier la collecte de fichiers journaux.

Pour récupérer des fichiers journaux DIVAR IP System Manager :

1. Connectez-vous au compte administrateur (voir *Connexion au compte administrateur, page 17*).
2. Dans le menu **Démarrer** de Windows, cliquez sur **Export System Manager Logs**.
   Le script exporte les fichiers journaux dans le dossier `Documents\Bosch` et crée un fichier ZIP avec la structure de noms suivante `SysMgrLogs-[date]_[time].`
   Vous pouvez utiliser ce fichier ZIP pour le joindre à la description détaillée de l'erreur.

7.5 Récupération de l'unité

Pour récupérer l'unité :

1. Mettez l'appareil sous tension et appuyez sur F7 pendant le test d'autodiagnostic (POST) du système BIOS pour accéder à Windows PE.
   La boîte de dialogue **System Management Utility** s'affiche.
2. Sélectionnez l'une des options suivantes :

- **System factory default** : cette option formate les partitions de données vidéo et restaure la partition du système d'exploitation sur les images par défaut.
  Cette opération peut prendre jusqu'à 5 minutes.
- **Full data overwrite and system factory default** : cette option formate les partitions de données vidéo en écrasant complètement les données existantes et restaure la partition du système d'exploitation avec les images par défaut.
  Cette opération peut prendre jusqu'à 48 heures.
- **OS system recovery only** : cette option permet de restaurer la partition du système d'exploitation avec l'image par défaut et d'importer les disques durs virtuels existants à partir de partitions de données vidéo existantes.
  Cette opération peut prendre jusqu'à 5 minutes.

Remarque :
L'option **OS system recovery only** n'efface pas les séquences vidéo qui sont stockées sur les disques durs de données. Cependant, il remplace la partition complète du système d'exploitation (y compris les paramètres du système de gestion vidéo) par une configuration par défaut. Pour accéder aux séquences vidéo existantes après la récupération, la configuration du système de gestion vidéo doit être exportée avant la récupération du système puis ensuite réimportée.

Remarque!
Veuillez ne pas éteindre l'unité lors du processus. Ceci risquerait d'endommager le support de récupération.

3. Confirmez l'option sélectionnée.
   Le système démarre le processus de formatage et de récupération d'image.
4. Une fois le processus de récupération terminé, confirmez le redémarrage du système.
   Le système redémarre et les routines de configuration sont exécutées.
5. Une fois le processus terminé, l'écran de sélection de la langue de Windows s'affiche.
6. Procédez à la configuration initiale du système.

Se reporter à
– *Première connexion et configuration initiale du système, page 9*

8 Informations supplémentaires

8.1 Documentation supplémentaire et logiciel client

Pour plus d'informations et de détails sur les logiciels, le téléchargement et la documentation, visitez le site http://www.boschsecurity.com et affichez la page produit respective dans le catalogue produit.
Vous trouverez les derniers logiciels et les progiciels de mise à niveau disponibles dans le magasin de téléchargement de Bosch Security and Safety Systems, sous : https://downloadstore.boschsecurity.com/

8.2 Services d’assistance et Bosch Academy

Assistance

Accédez à nos **services d'assistance** à l'adresse www.boschsecurity.com/xc/en/support/.

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/

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Pays-Bas
www.boschsecurity.fr

Building solutions for a better life.

202211241440