

DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

DIP-74C0-00N | DIP-74C4-8HD | DIP-74C8-8HD | DIP-74CI-8HD |
DIP-74CI-12HD | DIP-74G0-00N | DIP-74GI-16HD

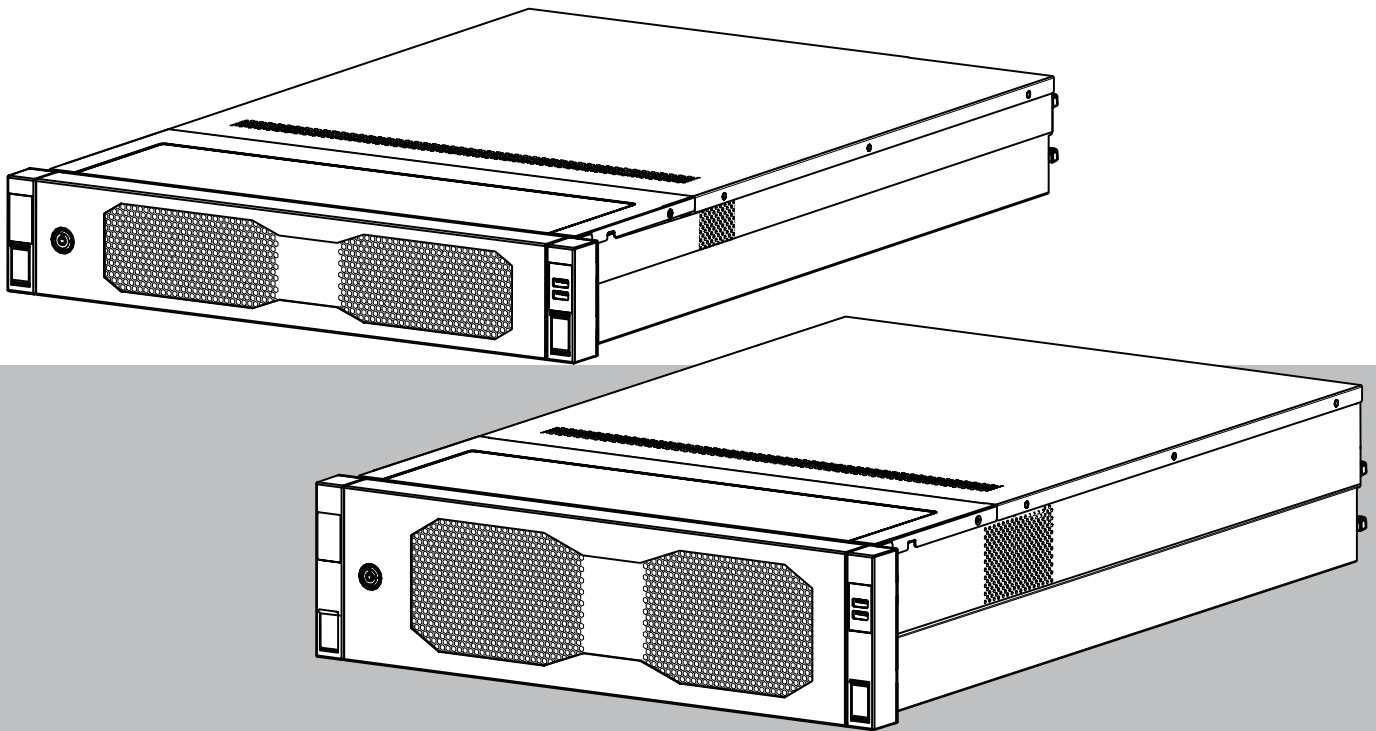


Table des matières

1	Sécurité	4
1.1	Précautions d'utilisation	4
1.2	Précautions en matière de cybersécurité	5
1.3	Précautions logicielles	6
1.3.1	Utiliser les derniers logiciels	6
1.3.2	Information OSS	7
2	Présentation	8
3	Présentation du système	9
4	Configuration du système	10
4.1	Paramètres par défaut	10
4.2	Exigences préalables	10
4.3	Première connexion et configuration initiale du système	10
4.3.1	Choix du mode de fonctionnement BVMS	12
4.3.2	Choix du mode de fonctionnement VRM	13
4.3.3	Choix du mode de fonctionnement du stockage iSCSI	13
5	Mise à niveau du logiciel	15
5.1	Mise à niveau du DIVAR IP System Manager	15
5.2	Mise à niveau du logiciel à l'aide du DIVAR IP System Manager	15
6	Connexion à distance au système	18
6.1	Protection du système contre tout accès non autorisé	18
6.2	Configuration du transfert de port	18
6.3	Choix d'un client approprié	18
6.3.1	Connexion à distance avec BVMS Operator Client	18
6.3.2	Connexion à distance avec l'application de sécurité vidéo	19
6.4	Connexion à Enterprise Management Server	19
6.5	Connexion à Remote Portal	19
6.5.1	Création d'un compte Remote Portal	20
6.5.2	Enregistrement des dispositifs DIVAR IP all-in-one sur Remote Portal	20
6.5.3	Annulation de l'enregistrement des dispositifs DIVAR IP all-in-one de Remote Portal	20
7	Maintenance	22
7.1	Connexion au compte administrateur	22
7.2	Surveillance du système	22
7.2.1	Surveillance du système à l'aide de l'application ASUS Inband Tool	22
7.2.2	Surveillance du système à l'aide de l'interface Web BMC	23
7.3	Remplacement d'un disque dur défectueux et configuration d'un nouveau disque dur	24
7.3.1	Remplacement d'un disque dur défectueux	24
7.3.2	Reconstruction du RAID5 avec le nouveau disque dur	24
7.4	Collecte des fichiers journaux du système DIVAR IP	25
7.5	Récupération de l'unité	25
8	Informations supplémentaires	27
8.1	Documentation supplémentaire et logiciel client	27
8.2	Services d'assistance et Bosch Academy	27

1 Sécurité

Veillez 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 éviter tout retrait non autorisé des disques durs. Retirez toujours la clé du verrou et rangez-la dans un endroit sûr.
- Utilisez la fonction Capteur d'intrusion du châssis pour détecter tout accès physique non autorisé à l'intérieur 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.
- Pour vous assurer que le navigateur Web est sécurisé et qu'il fonctionne correctement, maintenez-le toujours à jour.
- Ne désactivez pas Windows Defender ni le pare-feu Windows et gardez-les toujours à jour. N'installez pas de logiciel antivirus supplémentaire, car cela peut perturber les configurations de sécurité.
- 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.
- Ne modifiez pas les paramètres BIOS UEFI. Une modification des paramètres BIOS UEFI peut compromettre ou même entraîner un dysfonctionnement du système.
- Le système BMC ne doit pas être connecté au réseau public.

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>
- Informations de sécurité, qui couvrent les effets potentiels provoqués par des vulnérabilités de partie tierce : <https://www.boschsecurity.com/us/en/support/product-security/security-information.html>

Pour recevoir des mises à jour de nos nouveaux conseils en matière de sécurité, vous pouvez vous abonner aux flux RSS sur la page Bosch Security and Safety Systems Security Advisories à l'adresse : <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 Présentation

DIVAR IP all-in-one 7000 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 256 voies (avec 8 voies sous pré-licence).

Le DIVAR IP all-in-one 7000 2U/3U est une unité de montage en rack 2U/3U associant des fonctionnalités Bosch Video Management System avancées et une gestion des enregistrements de pointe dans un dispositif d'enregistrement unique, abordable et facile à installer pour les clients du secteur informatique.

DIVAR IP all-in-one 7000 bénéficie d'une conception intégrée et de composants principaux. Cette solution est basée sur le système d'exploitation Microsoft Windows Server IoT 2022 for Storage Standard et dispose de disques durs SATA remplaçables à chaud « conçus pour l'entreprise » et offrant jusqu'à 216/288 To de capacité de stockage brute.

3 Présentation du système

Système d'exploitation

Le système d'exploitation Microsoft Windows Server IoT 2022 for Storage Standard 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 Standard 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 7000 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.
- Solution d'enregistrement vidéo avancée pour un système BVMS, qui utilise les principaux composants et services Video Recording Manager, et bénéficiant des fonctionnalités uniques des solutions d'enregistrement et des caméras Bosch. Il est possible d'ajouter jusqu'à deux serveurs Video Recording Manager à un système BVMS s'exécutant sur un dispositif DIVAR IP all-in-one.
- Extension de stockage iSCSI pour un système BVMS, qui s'exécute sur un autre matériel. Jusqu'à quatre de ces extensions de stockage iSCSI peuvent être ajoutées à un système BVMS s'exécutant sur un dispositif DIVAR IP all-in-one 7000.

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
 - Le mot de passe doit contenir des caractères appartenant à trois des quatre catégories suivantes :
 - Au moins une lettre majuscule.
 - Au moins une lettre minuscule.
 - Au moins un chiffre.
 - Au moins un caractères spécial.

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.





Remarque!

Pour des raisons de sécurité, des boîtes de dialogue Contrôle de compte utilisateur s'affichent et vous invitent à confirmer les modifications à apporter au système. Vous ne pouvez poursuivre l'installation qu'après avoir confirmé que vous souhaitez apporter les modifications appropriées.

Pour configurer le système :

1. Connectez l'unité DIVAR IP all-in-one et les caméras au réseau.
2. Allumez l'unité.
Attendez que l'écran du BIOS s'affiche et que les sous-programme de configuration de Microsoft Windows Server IoT 2022 for Storage Standard s'exécutent. 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
 - Le mot de passe doit contenir des caractères appartenant à trois des quatre catégories suivantes :
 - Au moins une lettre majuscule.
 - Au moins une lettre minuscule.
 - Au moins un chiffre.
 - Au moins un caractères spécial.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 qui affiche le fichier d'installation pour démarrer l'installation.
Remarque : assurez-vous que la dernière version du DIVAR IP System Manager est installée. 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. 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 mes conditions de la licence, puis cliquez sur **Accept** pour continuer.
 10. Dans les boîtes de dialogue Contrôle de compte utilisateur suivantes, cliquez sur **Yes** pour continuer. L'installation démarre.
 11. Une fois l'installation terminée, le système redémarre et vous redirige vers la page de connexion Windows. Connectez-vous au compte administrateur.
 12. 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 **Installer mode d'opération**.
Le contrat de licence BVMS s'affiche.
2. Lisez et acceptez le contrat de licence, puis cliquez sur **Oui, 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 **Installer mode d'opération**.
Le VRM contrat de licence s'affiche.
2. Lisez et acceptez le contrat de licence, puis cliquez sur **Oui, 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 **Installer mode d'opération**.
La boîte de dialogue d'installation s'affiche.
2. Dans la boîte de dialogue d'installation, cliquez sur **Oui, 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

Assurez-vous d'effectuer une mise à niveau du DIVAR IP System Manager vers la version la plus récente.

5.1 Mise à niveau du DIVAR IP System Manager

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 le fichier ZIP **SystemManager_[version 2.3.0 ou supérieure du logiciel].zip** et enregistrez-le sur un support de stockage tel qu'une clé USB.
4. Décompressez le fichier sur le support de stockage.
5. Connectez le support de stockage à votre dispositif DIVAR IP all-in-one.
6. Démarrez DIVAR IP System Manager :
 - Si vous êtes connecté à Windows avec le compte administrateur **BVRAdmin**, double-cliquez sur l'icône DIVAR IP System Manager du bureau Windows. 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. 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).
7. La page **Paquets logiciels** s'affiche. Sélectionnez le logiciel DIVAR IP System Manager, puis cliquez sur **Installer le pack** pour continuer.
La boîte de dialogue d'installation s'affiche.
8. Dans la boîte de dialogue d'installation, cliquez sur **Oui, installer** pour continuer.
L'installation démarre.
L'installation peut prendre quelques minutes. Ne retirez pas le système et ne retirez pas le support de stockage pendant le processus d'installation.
Respectez les notifications qui s'affichent en haut de la page.

5.2 Mise à niveau du logiciel à l'aide du DIVAR IP System Manager

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. Démarrez DIVAR IP System Manager :
 - Si vous êtes connecté à Windows avec le compte administrateur **BVRAdmin**, double-cliquez sur l'icône DIVAR IP System Manager du bureau Windows. 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. 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 **Paquets logiciels** affiche le type de périphérique et son numéro de série en haut de la page.
 - Dans la colonne **Nom du pack logiciel**, 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 **Versión 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 **Versión 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 du pack logiciel**, cliquez sur le bouton d'option correspondant pour sélectionner l'application logicielle à mettre à niveau ou à installer.
8. Dans la colonne **Versión disponible**, sélectionnez la version vers laquelle vous souhaitez mettre à niveau votre logiciel, ou que vous souhaitez installer, puis cliquez sur **Installer le pack**.
Le cas échéant, la boîte de dialogue du contrat de licence s'affiche.

9. Lisez et acceptez le contrat de licence, puis cliquez sur **Oui, 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. Si l'installation des logiciels aboutit, un message vous confirme que l'installation est réussie.
11. Si l'installation échoue, un message vous informe de la manière de procéder.

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 18.*
2. *Configuration du transfert de port, page 18.*
3. *Choix d'un client approprié, page 18.*

Vous pouvez également vous connecter à votre DIVAR IP all-in-one via Bosch Remote Portal et utiliser les fonctionnalités actuelles et futures disponibles via Remote Portal. Pour plus d'informations, reportez-vous à *Connexion à Remote Portal, page 19.*

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 18.*
- *Connexion à distance avec l'application de sécurité vidéo, page 19.*

**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.

6.5

Connexion à Remote Portal

Vous pouvez vous connecter à votre dispositif DIVAR IP all-in-one via Bosch Remote Portal et utiliser les fonctionnalités actuelles et futures telles que le service Bosch Remote System Management disponible via Remote Portal.

Pour plus d'informations sur le service Remote System Management, consultez la documentation logicielle et les ressources de formation Remote System Management.

Exigences préalables

Connexion Remote Portal

Pour connecter les dispositifs DIVAR IP all-in-one à Remote Portal, assurez-vous que les exigences préalables suivantes s'appliquent :

- DIVAR IP System Manager 2.3.0 (ou version supérieure) doit être installé sur le dispositif.
- Un compte Remote Portal doit être créé.

Communication avec Remote Portal

Conditions de connectivité requises pour la communication avec Remote Portal.

Remarque : Toutes les connexions sont sortantes.

HTTPS (Port 443)

- <https://api.remote.boschsecurity.com/rest/iot/devices>
- <https://sw-repo-remote.s3.eu-central-1.amazonaws.com>

MQTTS (Port 8883)

- [tls://a1j83emmuys8gs-ats.iot.eu-central-1.amazonaws.com:8883](https://a1j83emmuys8gs-ats.iot.eu-central-1.amazonaws.com:8883)

6.5.1

Création d'un compte Remote Portal

Pour créer un compte Remote Portal :

1. Accédez à <https://remote.boschsecurity.com/login>.
2. Cliquez sur **Sign up**.
3. Saisissez le nom de votre entreprise et votre adresse e-mail.
4. Sélectionnez la région de votre entreprise.
5. Lisez les conditions générales et la notification de protection des données, puis cochez les cases à cocher pour les accepter.
6. Cliquez sur **Sign up** pour créer un compte.

6.5.2

Enregistrement des dispositifs DIVAR IP all-in-one sur Remote Portal

Pour enregistrer un dispositif DIVAR IP all-in-one sur Remote Portal :

1. Démarrez DIVAR IP System Manager.
2. Cliquez sur l'onglet **Connexion Remote Portal**.
3. Si vous possédez un compte Remote Portal existant, saisissez votre adresse e-mail et votre mot de passe, puis cliquez sur **S'inscrire** pour enregistrer votre dispositif DIVAR IP all-in-one sur Remote Portal.
4. Si votre e-mail est affecté à plusieurs comptes d'entreprise avec des privilèges d'administrateur, une boîte de dialogue contenant les comptes d'entreprise respectifs s'affiche.

Dans la boîte de dialogue, sélectionnez le compte d'entreprise sur lequel vous souhaitez enregistrer votre dispositif DIVAR IP all-in-one.

Remarque!

SingleKey ID

Bosch a introduit SingleKey ID comme fournisseur d'identité pour autoriser une connexion centrale à l'ensemble des applications, services et plates-formes Bosch.

Pour connecter le dispositif à Remote Portal à l'aide de SingleKey ID, suivez les instructions à l'écran.



5. Si vous ne possédez pas encore de compte Remote Portal, cliquez sur **Créer un compte** pour commencer par créer un compte Remote Portal. Reportez-vous à .

6.5.3

Annulation de l'enregistrement des dispositifs DIVAR IP all-in-one de Remote Portal

Pour annuler l'enregistrement d'un dispositif DIVAR IP all-in-one de Remote Portal :

1. Démarrez DIVAR IP System Manager.
2. Cliquez sur l'onglet **Remote Portal connection**.
3. Cliquez sur **Se désinscrire** pour annuler l'enregistrement de votre dispositif DIVAR IP all-in-one de Remote Portal.

Remarque : L'annulation de l'enregistrement du dispositif de Remote Portal ne

supprime pas la configuration du dispositif sur Remote Portal. Pour supprimer la configuration du dispositif, connectez-vous au compte d'entreprise Remote Portal correspondant.

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

7.2.1 Surveillance du système à l'aide de l'application ASUS Inband Tool

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

Le service d'application est activé par défaut.

Pour lancer l'application :

1. Connectez-vous au compte administrateur (voir *Connexion au compte administrateur*, page 22).
2. Sur le bureau, ouvrez le dossier **Outils** et double-cliquez sur le raccourci ASUS Inband Tool.
L'application démarre.
3. Connectez-vous à l'aide des identifiants par défaut suivants :
 - Compte : **admin**
 - Mot de passe : **admin**
4. Après la première connexion, il vous sera demandé de modifier ce mot de passe initial. Saisissez un nouveau mot de passe, puis confirmez-le.
Veillez à stocker le nouveau mot de passe dans un endroit sûr.
Respectez les conditions suivantes :
 - Les mots de passe doivent avoir une longueur minimale de 14 caractères.
 - Les mots de passe doivent contenir au moins une lettre majuscule.
 - Les mots de passe doivent contenir au moins une lettre minuscule.
 - Les mots de passe doivent contenir au moins un caractère spécial.
 - Les mots de passe doivent contenir au moins un chiffre.
5. Après confirmation du nouveau mot de passe, la page **Tableau de bord** indique l'état général du système.
6. Dans le volet **Menu** de gauche, vous pouvez sélectionner les pages respectives pour recevoir des informations détaillées sur l'état du système.
7. Dans l'élément de menu **SNMP**, vous pouvez définir les utilisateurs SNMP et la destination SMMP.

8. La page **Rapport** vous permet de générer un rapport contenant les informations appropriées que vous avez sélectionnées.

7.2.2

Surveillance du système à l'aide de l'interface Web BMC

DIVAR IP all-in-one 7000 dispose d'un port BMC dédié à l'arrière.

Chaque unité DIVAR IP all-in-one 7000 est fournie avec le nom **admin** de l'utilisateur BMC par défaut et avec un mot de passe BMC initial. Le mot de passe BMC initial est unique pour chaque unité. Vous pouvez le trouver sur l'étiquette à l'arrière de l'unité, sous le port BMC. Après la première connexion à l'interface Web BMC, il vous sera demandé de modifier ce mot de passe initial. Veillez à stocker le nouveau mot de passe dans un endroit sûr.

Respectez les conditions suivantes :

- Les mots de passe doivent avoir une longueur minimale de 14 caractères.
- Les mots de passe doivent contenir au moins une lettre majuscule.
- Les mots de passe doivent contenir au moins une lettre minuscule.
- Les mots de passe doivent contenir au moins un caractère spécial.
- Les mots de passe doivent contenir au moins un chiffre.



Remarque!

Pour des raisons de sécurité, ne connectez pas le dispositif à un réseau public via le port BMC.

Configuration des paramètres BMC

Pour configurer les paramètres BMC :

1. Allumez l'appareil et appuyez sur Suppr pour entrer dans la configuration du BIOS.



Remarque!

Mot de passe BIOS

Le mot de passe initial du BIOS est unique pour chaque unité. Vous pouvez le trouver sur l'étiquette à l'arrière de l'unité. Bosch vous recommande vivement de modifier ce mot de passe initial. Veillez à stocker le nouveau mot de passe dans un endroit sûr.

Respectez les conditions de mot de passe suivantes :

- Les mots de passe doivent avoir une longueur minimale de 14 caractères.
- Les mots de passe doivent contenir au moins une lettre majuscule.
- Les mots de passe doivent contenir au moins une lettre minuscule.
- Les mots de passe doivent contenir au moins un caractère spécial.
- Les mots de passe doivent contenir au moins un chiffre.

2. Dans l'installation BIOS, accédez à l'onglet **Server Mgmt.**
3. Sélectionnez l'option **BMC Network Configuration**, ensuite appuyez sur Entrée.
4. Dans la boîte de dialogue suivante, sélectionnez l'option **Configuration Address source**, puis appuyez sur Entrée.
La boîte de dialogue **Configuration Address source** s'affiche.
5. Dans la boîte de dialogue **Configuration Address source**, sélectionnez l'option de votre choix pour configurer l'adresse BMC, puis appuyez sur Entrée.
6. Définissez les paramètres de configuration réseau souhaités.
7. Appuyez sur F4 et Entrée pour enregistrer et quitter.
L'unité DIVAR IP all-in-one 7000 redémarre.

Fonctionnement à distance via l'interface iKVM BMC

Par défaut, les dispositifs DIVAR IP all-in-one 7000 sont destinés à fonctionner avec un ou deux moniteurs locaux, connectés aux interfaces HDMI à l'arrière de l'unité.

Si aucun moniteur local n'est connecté aux interfaces HDMI, il est possible de contrôler l'unité à distance à l'aide de l'interface iKVM BMC.

Pour permettre la commande à distance du système :

1. Assurez-vous qu'aucun moniteur HDMI local n'est connecté au système.
2. Connectez-vous à l'interface Web BMC.
3. Dans le volet Menu de gauche, sélectionnez la page **Commande à distance**.
4. Cliquez sur le bouton **Lancer H5Viewer**.

Une fenêtre s'ouvre, affichant la sortie moniteur DIVAR IP all-in-one 7000 et permettant de commander la souris et le clavier de l'ordinateur distant.

7.3

Remplacement d'un disque dur défectueux et configuration d'un nouveau disque dur



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 :

- ▶ 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


Reconstruction du RAID5 avec le nouveau disque dur

Reconstruction automatique du RAID5

1. Sur le bureau DIVAR IP all-in-one, double-cliquez sur le raccourci **Launch LSA**. L'application **LSI Storage Authority** démarre et la page **Remote Server Discovery** s'affiche.
2. Connectez-vous avec les identifiants du compte administrateur **BVRAdmin**. Une boîte de dialogue s'affiche et indique qu'un contrôleur présente un problème critique.
3. En haut de la page, cliquez sur **Sélectionner le contrôleur**, puis cliquez sur la barre **Controller ID** pour ouvrir les paramètres du contrôleur.
 - Si vous n'avez pas encore supprimé le disque dur défectueux, il s'affiche sous **Drives > Foreign Drives > Unconfigured Drives**.
 - Une fois le disque dur défectueux retiré et le nouveau disque dur installé, le système lance automatiquement la reconstruction du RAID5 avec le nouveau disque dur et la progression de la reconstruction s'affiche.
4. Une fois la reconstruction terminée, l'icône  s'affiche.

Reconstruction manuelle du RAID5

Si la reconstruction du RAID5 du nouveau disque dur ne démarre pas automatiquement, procédez comme suit :

1. Dans la boîte de dialogue des paramètres du contrôleur, sous **Drives > Foreign Drives > Unconfigured Drives**, sélectionnez le disque dur avec l'état **Unconfigured Bad**, puis, dans le volet droit, sélectionnez **Make Unconfigured Good**.
Une boîte de dialogue s'affiche.
2. Cochez la case **Confirm**, puis cliquez sur **Yes, Make Unconfigured Good** pour continuer.
Le système lance la reconstruction du RAID5 avec le nouveau disque dur.
3. Une fois la reconstruction terminée, l'icône  s'affiche.

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).
2. Dans le menu **Démarrer** de Windows, cliquez avec le bouton droit de la souris sur **Export System Manager Logs** et exécutez le script en tant qu'administrateur.
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. Allumez l'appareil et appuyez sur F7 pendant l'autotest de mise sous tension du 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 prend quelques 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.
Remarque : Ce processus peut prendre plusieurs jours.
 - **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.
Ce processus prend plusieurs 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!**

Veillez 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.

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>

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

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2024

Des solutions pour les bâtiments au service d'une vie meilleure

202404171736