CBS-RM-DIP4 Remote System Management DIP 4000 1an

Remote Portal

- Gestion centralisée des stocks à distance offrant un accès rapide à l'ensemble du système connecté à Remote Portal
- Administration et maintenance du système simplifiées pour les mises à jour et les correctifs ; l'ensemble du système est donc toujours à jour et sécurisé
- Surveillance détaillée de l'état et des alertes avec des informations en temps réel sur l'état d'un système et d'un dispositif particulier
- Connexion au Cloud axée sur la confidentialité

Les services de Remote System Management de Bosch vous permettent de tirer parti de la puissance de l'Internet des objets (IoT) pour fournir un ensemble d'outils et de fonctionnalités faciles à utiliser permettant de gérer des actifs de manière sécurisée, transparente et économique tout au long de la durée de vie d'un dispositif ou d'un système. Ce service permet aux utilisateurs de gérer les stocks et les mises à jour, et de surveiller l'état de l'ensemble d'un système à partir d'une plateforme Remote Portal centralisée.

Fonctions

Gestion des stocks
Connectez facilement votre système à Remote Portal, qui garantit une connectivité sécurisée au dispositif ainsi que l'enregistrement vérifiable du dispositif. Cette plateforme de gestion centralisée fournit une vue d'ensemble en temps réel de l'inventaire d'un système, notamment des informations concernant les versions actuelles des logiciels et du firmware.

Gestion des mises à jour
La fonctionnalité de gestion des mises à jour est conçue pour gérer et déployer des mises à jour à distance sur l'ensemble d'un dispositif ou d'un système sur un ou plusieurs sites.

- Déployez rapidement des correctifs de sécurité et des mises à jour de firmware/logiciels.
- Générez automatiquement des rapports de mise à jour pour fournir un résumé détaillé des modifications implémentées par une campagne de mises à jour.

Surveillance de l'état
Les fonctionnalités de surveillance de l'état du service de Remote System Management favorisent les prises de décision éclairées et les dépannage proactifs pour accroître la disponibilité du système et réduire le temps passé sur site.

- Permet de surveiller la connectivité, la disponibilité des mises à jour et le statut des autorisations du dispositif.
- Fournit des informations détaillées sur l'état du matériel et des enregistrements.
- Permet de définir des alertes concernant l'état par e-mail.

Prise en charge des modes de fonctionnement
La connectivité de DIVAR IP à Remote Portal et le service de Remote System Management sont compatibles avec tous les modes de fonctionnement - BVMS, Video Recording Manager (VRM) et cible iSCSI. Les modes VRM et iSCSI permettent uniquement de gérer le dispositif DIVAR IP. Pour gérer l'ensemble d'un système, y compris les caméras, le système DIVAR IP doit être utilisé en mode BVMS. Dans le cadre du service de Remote System Management, les

modes VRM et iSCSI sont efficaces s'ils sont utilisés comme sous-systèmes intégrant un système vidéo principal, comprenant lui-même un système DIVAR IP fonctionnant en mode BVMS.
Remarque : chaque DIVAR IP se connecte individuellement à Remote Portal pour tous les modes de fonctionnement. Les dispositifs DIVAR IP faisant partie d'un système vidéo principal doivent être regroupés en fonction du compte d'entreprise dont ils dépendent.

Sécurité des données
Le plus haut niveau de sécurité pour l'accès à distance aux dispositifs et le transport des données est garanti. L'intégration d'une infrastructure de clés publiques (PKI) assure une attestation d'identité et une protection anti-sabotage optimales. Cela permet d'appliquer une authentification forte basée sur un certificat entre le dispositif et le Cloud et de bénéficier de communications sécurisées pour les accès à distance au dispositif.
La sécurité locale des dispositifs est assurée par des configurations de renforcement de la sécurité multi-couches et par l'utilisation de fonctionnalités de sécurité Windows Server, notamment :

- Windows Security Baseline, groupe de paramètres de configuration standard de sécurité recommandés par Microsoft.
- Windows Defender Device Guard pour s'assurer que seuls les logiciels de confiance sont exécutés sur le serveur.
- Control Flow Guard pour offrir une protection intégrée contre les attaques par corruption de mémoire.
- L'antivirus Windows Defender, qui est une solution anti-programme malveillant intégrée permettant de gérer la sécurité.
- Windows Defender Credential Guard, qui utilise la sécurité par virtualisation pour isoler les informations d'identification et empêcher ainsi l'interception des tickets Kerberos ou des informations de hachage des mots de passe.
- L'autorité de sécurité locale (LSA), qui réside dans le processus LSASS (Local Security Authority Security Service), valide les utilisateurs pour les accès locaux et distants et applique les règles de sécurité locales.

Confidentialité des données
Le service de Remote System Management assure la protection de la confidentialité des données client et utilisateur grâce aux mesures suivantes :

- Connexion Cloud dédiée pour la maintenance et la surveillance uniquement (conformément au protocole MQTTS).
- Pas d'accès vidéo à distance mais une transparence 24h/24 et 7 j/7 concernant l'état du système.
- Les données vidéo et les données de maintenance des dispositifs DIVAR IP sont distinctes : connexion à distance pour les services de maintenance du système sans risque d'accès vidéo non autorisé.

Gestion simplifiée des pare-feu
Les dispositifs DIVAR IP consolident toutes les communications des caméras de l'ensemble du système vidéo en une seule connexion sortante vers Remote Portal. Le fait de ne conserver qu'une seule connexion sortante réduit considérablement les efforts requis pour les tâches de gestion des pare-feu informatiques.

Intégration de Remote Portal
Le service de Remote System Management est intégré en toute transparence à Remote Portal.
La connectivité initiale à Remote Portal est gratuite. Avec la licence appropriée, les fonctionnalités du service de Remote System Management peuvent être activées en ligne dans Remote Portal.

ⓘ **Remarque**
Les fonctionnalités et les services peuvent varier en fonction du dispositif.
Pour plus d'informations sur la configuration requise pour chaque système, reportez-vous à la documentation de chaque dispositif.

Inscrivez-vous gratuitement sur :
https://remote.boschsecurity.com

REMARQUE : le service de Remote System Management propose une période d'essai gratuite, au terme de laquelle les utilisateurs pourront continuer à utiliser les fonctionnalités suivantes :

- Connectivité à Remote Portal.
- Gestion de base des stocks permettant de visualiser et d'organiser les ressources installées.
- Surveillance de la connectivité, de la disponibilité des mises à jour et de l'état des autorisations/licences.

ⓘ **Remarque**
Détails du service
Des informations supplémentaires sont disponibles dans le document décrivant le service de Remote System Management, qui peut être téléchargé à partir de la page du catalogue de produits.

Composants

Quantité	Composant
1	Remote System Management - licence de 1 an

Caractéristiques techniques

Connectivité

Réseau	Pour de meilleures performances, une connexion Internet fixe doit être utilisée pour connecter les dispositifs au Bosch Security Cloud. Les connexions Internet cellulaires peuvent être utilisées, mais elles peuvent avoir un impact sur les performances ou la disponibilité.
Navigateur	Les interfaces avec navigateur de Remote Portal offrent une meilleure qualité d'affichage avec les navigateurs suivants : • Google Chrome • Firefox • Microsoft Edge **REMARQUE** : JavaScript doit être activé.

Sécurité des données

Processeur de chiffrement sécurisé (TPM)	TPM v2.0
PKI	Certificats X.509
Sécurité réseau	TLS v1.2 ou supérieur, DTLS 1.2 ou supérieur
Chiffrement local	Chiffrement des dispositifs, n°AES-256

Compatibilité

Dispositif	Version minimale du firmware/du logiciel
DIVAR IP all-in-one 4000	DIVAR IP System Manager 2.0
Caméras IP Bosch (connectées au dispositif DIVAR IP all-in-one sous licence)	Version 6.5 du firmware

Informations de commande

CBS-RM-DIP4 Remote System Management DIP 4000 1an
Licence d'utilisation des services de Remote System Management pour un dispositif DIVAR IP all-in-one 4000 pendant 1 an
Numéro de commande **CBS-RM-DIP4 | F.01U.410.890**

Représenté par :

Europe, Middle East, Africa:
Bosch Security Systems B.V.
P.O. Box 80002
5600 JB Eindhoven, The Netherlands
Phone: + 31 40 2577 284
www.boschsecurity.com/xc/en/contact/
www.boschsecurity.com

Germany:
Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Tel.: +49 (0)89 6290 0
Fax:+49 (0)89 6290 1020
de.securitysystems@bosch.com
www.boschsecurity.com