Remote System Management

CBS-RM-DIPx

fr Description du service

Table des matières

1 Fonctions principales

Le service de Remote System Management de Bosch vous permet de tirer parti de la puissance de l'Internet des objets (IoT) pour gérer des actifs de manière sécurisée, transparente et économique tout au long du cycle de vie d'un système vidéo. Ce service permet aux utilisateurs finaux, aux intégrateurs et aux installateurs système de gérer l'inventaire et les mises à jour, ainsi que de surveiller l'état de l'ensemble du système vidéo Bosch (DIVAR IP + BVMS + caméras) depuis une plate-forme Remote Portal centralisée.

Ce service garantit la tranquillité d'esprit pour les clients en permettant une surveillance sécurisée du système 24h/24 et 7 j/7. L'utilisateur peut ainsi d'agir de manière proactive et résoudre les problèmes lorsqu'ils surviennent, par exemple avant de perdre les enregistrements vidéo en raison d'une défaillance du disque dur. La connexion MQTTS sécurisée permet également de préserver la confidentialité des données, car les séquences vidéo ne sont pas accessibles à tout le monde via cette connexion, dans la mesure où le transfert des données vidéo et image n'est pas pris en charge par ce protocole. En outre, ce service permet d'effectuer les mises à jour à distance des logiciels et du firmware, garantissant ainsi la mise à jour et la sécurité du système. La connectivité Cloud est basée sur une connexion sortante unique depuis DIVAR IP vers Remote Portal, où DIVAR IP regroupe toutes les communications entrantes et sortantes de l'intégralité du système vidéo

Le service est conçu pour être utilisé par des organisations clientes de grande taille qui effectuent leur propre maintenance système sur plusieurs sites dispersés, ou par des installateurs offrant ces services à un grand nombre de clients finaux différents. La Remote System Management présente des avantages car elle se concentre sur une efficacité accrue dans l'exécution des tâches de maintenance du système. Cela permet notamment d'éviter toute déplacement inutile sur site grâce aux opérations de maintenance à distance, telles que les mises à jour suite aux conseils de sécurité, ou les informations système les plus récentes qui permettent de mieux préparer les visites sur site. Effet secondaire positif : service complet avec émissions minimales de CO_2. De plus, les utilisateurs peuvent améliorer l'expérience de service qu'ils offrent, par une action proactive et la possibilité de régler les problèmes sur le terrain (en interne), avant même que les clients ne se rendent compte qu'ils ont un problème. Pour plus d'informations sur les fonctions, consultez la fiche technique du service.

Remarque!

Les fiches technique figurent dans le catalogue de produits respectif pour votre région ou votre pays.

2 Configuration minimale requise

Configuration logicielle

L'interface Web du Remote Portal peut être utilisée avec les navigateurs Web modernes qui prennent en charge HTML5. Pour un résultat optimal, Bosch recommande d'utiliser Google Chrome.

Dispositifs requis

Pour une utilisation optimale de la Remote System Management, il est nécessaire que les caméras IP Bosch exécutent la version 6.50 ou ultérieure du firmware.
Comme indiqué dans la fiche technique, seuls certains modèles DIVAR IP sont pris en charge. Sur ces modèles, les logiciels minimum requis doivent prendre en charge DIVAR IP System Manager version 2.0 ou ultérieur. Reportez-vous aux fiches techniques respectives pour plus de détails.
La bande passante requise dépend des caractéristiques techniques du système vidéo et de la structure du site, c'est-à-dire du nombre de caméras et de périphériques DIVAR IP sur site. Bosch recommande une bande passante minimale de 11 Mbit/s ou 1,31 Mo/s par dispositif DIVAR IP, car DIVAR IP regroupe les communications entrantes et sortantes pour lui-même et pour les caméras connectées. Cette recommandation se base sur les cas d'utilisation les plus exigeants en termes de bande passante, à savoir le téléchargement de fichiers de mise à jour plus importants qui créent une hausse de la demande de bande passante chaque fois que de telles mises à jour sont déclenchées à partir du Remote Portal. La majorité des opérations en dehors de ces périodes de forte demande exige des bandes passantes d'environ 10 Kbit/s, p. ex. pour la surveillance des paramètres d'état et d'autres données de télémétrie.

Remarque!

Les exigences en termes de bande passante peuvent varier et l'utilisateur doit s'assurer que la bande passante disponible répond aux exigences de l'application. Bosch fournit plusieurs outils qui permettent de calculer la bande passante requise, mais décline toute responsabilité concernant la disponibilité réelle de la bande passante et d'une configuration correcte.

3 Application Web

La Remote System Management est intégrée au Remote Portal, qui fait office de plate-forme Web centrale pour l'activation des services et des fonctions générales supplémentaires, indépendamment de l'offre de service, comme indiqué ci-dessous.

Gestion du système et des dispositifs partir d'une vue de tableau de bord

Les systèmes et les dispositifs uniques peuvent être regroupés dans un ordre hiérarchique qui correspond à un client ou à un emplacement d'installation, pour limiter l'accès à un ensemble de dispositifs ou regrouper l'état de plusieurs dispositifs.

Présentation du service

La section « Services » du Remote Portal fournit une vue d'ensemble de tous les services disponibles sur les différents types de dispositifs. Chaque service présente une vue d'ensemble consolidée de tous les dispositifs et systèmes sur lesquels il est activement utilisé.

Gestion de licence de service

Les services peuvent être activés en visitant le Remote Portal après la mise en service initiale de DIVAR IP dans le Remote Portal

Le service de Remote System Management requiert des licences d'activation. Selon le modèle de DIVAR IP et son mode de fonctionnement, différentes licences sont applicables. Pour plus de détails, consultez les fiche techniques. Les licences sont gérées et activées dans le Remote Portal dans la section « Licences de service »

Gestion des utilisateurs

Le Remote Portal permet un contrôle très précis de l'accès aux dispositifs et services. Grâce à la gestion des rôles, les *administrateurs*, les *techniciens* et les *utilisateurs finaux* peuvent être individuellement associés aux systèmes, groupes et services.

Remarque!

Pour de plus amples informations sur le Remote Portal, consultez la page produit respective à l'adresse : https://commerce.boschsecurity.com/gb/en/Remote-Portal/p/86180387339/

4 Documentation

La documentation utilisateur et les fiches technique de chaque DIVAR IP est accessible ici :

Formations techniques :	https://academy.boschsecurity.com/

REMARQUE : Une formation d'introduction au Remote System Management sera bientôt disponible. Cette formation sera ultérieurement intégrée dans la formation de certification DIVAR IP all-in-one.

Notes de procédure/ configuration :	https://community.boschsecurity.com/t5/Security-Video/tkb-p/bt_community-tkb-video/label-name/remote_system_mgmt?labels=remote_system_mgmt
Fiches technique/notes d’application :	https://commerce.boschsecurity.com/gb/en/bt/search/?text=cbs-rm-dip

5 Composants logiciels open source

Les composants logiciels en open Source inclus dans le Remote Portal sont disponibles ici : https://remote.boschsecurity.com/open_source/open_source_licenses.txt

6 Hébergement des services

Les services répertoriés ici sont hébergés au sein de l’infrastructure en tant que service AWS. L’application Remote Portal est une plate-forme multi-client globale. Cette plate-forme, sa base de données, ses systèmes backend et frontend, sont hébergés chez AWS dans la région de Francfort en Allemagne.

7 Maintenance et niveau de service

Bosch propose un Contrat de service (SLA) dédié pour les revendeurs inscrits au Remote System Management de Bosch. Ce contrat SLA décrit en détail les processus de disponibilité, de maintenance et d'assistance garantis pour le Remote System Management de Bosch et il comporte les coordonnées des services d’assistance téléphoniques d’urgence, les clauses de non-responsabilité, etc.
Pour plus de détails, veuillez contacter votre représentant commercial local.

8 Obligations du client et de l’utilisateur final

Pour les clients directs de Bosch, l’acceptation des Conditions générales pour revendeurs SaaS (Software as a Service) est requise pour pouvoir obtenir des licences ou des abonnements de Gestion du système à distance. Pour l’activation des licences ou abonnements de service, les utilisateurs doivent accepter les conditions du Remote Portal. Les autres obligations sont les suivantes :

- 8.1. La connexion Internet entre les clients, leur centre de surveillance/la salle de contrôle et le site d’installation de dispositifs compatibles (notamment les caméras vidéo, désignées ci-après « Dispositifs »), ainsi que l’interface Internet du centre de données utilisée par Bosch, de même que la relation de client final avec le client et ses partenaires contractuels, relèvent de la seule responsabilité des clients.
- 8.2. L’installation, l’utilisation, l’entretien et, si nécessaire, la réparation des dispositifs, relèvent exclusivement de la responsabilité des clients.
- 8.3. L’application n’est pas conçue ou garantie pour une utilisation dans les applications à risque élevé qui nécessitent des performances de sécurité particulières, telles que l’utilisation d’installations nucléaires, la gestion du trafic aérien, les systèmes de survie, ou d’autres applications, dispositifs ou systèmes dans lesquels la défaillance d’un dispositif ou d’une application pourrait entraîner directement la mort, des blessures corporelles ou des dégâts matériels ou environnementaux graves (activités à risque élevé). Nonobstant toute autre disposition, les clients ne peuvent pas utiliser ou autoriser un tiers à utiliser l’Application présentant une activité à risque élevé.
- 8.4. L'obtention du consentement nécessaire des personnes affectées s'applique dans ce cas, conformément aux réglementations relatives à la sécurité et à la protection des données, lors de la collecte, du traitement ou de l’utilisation de données personnelles au cours de l’utilisation par ces personnes de l’application, notamment lorsqu'aucune règlementation relative à la collecte, au traitement ou à l'utilisation sans la nécessité d'obtenir une autorisation ne s’applique dans le cas en question.
- 8.5. Consultez les données et les informations relatives aux virus ou autres logiciels malveillants avant d’envoyer les données et les informations à Bosch et assurez-vous que les programmes antivirus répondent aux exigences les plus récentes.
- 8.6. Signalez les défauts des services contractuels à Bosch immédiatement après avoir été informés de tels défauts. En cas de retard d’envoi de la notification ou si aucune notification n'est transmise alors que le client est au courant du défaut, toute réduction unilatérale des frais ou toute suspension par le client, ainsi que toute résiliation exceptionnelle, est exclue.
- 8.7. Les rôles et tâches suivants relèvent exclusivement de la responsabilité du client :
  - 8.7.1. Affectation de rôles et d’autorisations aux personnes ou unités correspondants pour les rôles d’utilisateur disponibles dans le Remote Portal, et gestion de ces rôles et autorisations.
  - 8.7.2. Affectation de dispositifs à des partenaires contractuels du client et aux sites des ces partenaires contractuels.
  - 8.7.3. Fourniture, installation et connexion de dispositifs adaptés au fonctionnement conformément aux exigences du système. L’Application prend en charge l'utilisation des dispositifs par le client à l’aide des fonctions décrites.

9 Informations relatives au RGPD

Objet du traitement des données

Bosch traite uniquement les données personnelles, dans la mesure nécessaire, et selon les modalités suivantes :

1. dans le but de respecter les obligations de Bosch en vertu de l'accord/des conditions d'utilisation du service de Gestion du système à distance ; et
2. afin de se conformer ponctuellement aux instructions du client (qui peuvent être des instructions spécifiques ou des instructions de nature générale telles que définies dans cet accord ou notifiées d'une autre manière à Bosch par le client),
3. et les données personnelles ne doivent pas être traitées à toute autre fin.

Catégories de données

- Données de dispositif : données saisies par le Contrôleur de données ou transférées par le dispositif du Contrôleur de données - données maître du dispositif, données de télémétrie de l'état du dispositif et métadonnées des versions logicielles. Emplacement et contact d'un dispositif. Pour à activer le service Remote System Management fourni vers le Contrôleur de données.
- Journaux liés au dispositif : les activités du dispositif sont consignées pour permettre le dépannage du système.
- Données de configuration utilisateur : données saisies par le Contrôleur de données lors de l'utilisation de la solution, notamment les informations d'accès utilisateur (comme l'adresse IP, la société, le prénom, le nom et l'adresse e-mail requis pour fournir l'accès de l'application à l'utilisateur).
- Journaux d'action utilisateur : la documentation d'utilisation du système utilisateur, notamment les actions effectuées et les horodatages associés. Permet de résoudre les problèmes de maintenance et d'améliorer l'expérience utilisateur.
- Données non personnelles telles que les données de site, de compte client et de configuration de service, y compris les types et flux.

Sujets de données

- Employés du client
- Utilisateurs finaux ou partenaires contractuels du client (« client du client »)

Sous-traitants

Toutes les sous-traitants sont répertoriées dans le **Tableau 1**.

	Nom et adresse du sous-traitant et nom de l'agent chargé de la confidentialité des données/personne contact pour toute question liée à la confidentialité des données	Portée du service (portée de la commande passée par le sous-traitant)	Lieu de traitement des données	Transfert/accès aux données personnelles du client (type de données et groupe de sujets de données)
1	Amazon Web Services (AWS)	Fournisseur d'infrastructure/ d'hébergement (décrit dans le concept de sécurité) et prestataire de services gérés pour le stockage, le traitement et l'extraction des données, ainsi que la connectivité du Cloud	Régions d'infrastructures AWS (voir la section 6)	Ensemble des catégories et des sujets de données répertoriés dans les données 9
2	Robert Bosch India Agent chargé de la protection des données Bosch India (RBEI/DSO) DPO.India@in.bosch.com	Groupe restreint de support des opérations techniques	No.123, Industrial Layout, Hosur Road, Koraman-galaBengaluru-560 095 Karnataka, India	Ensemble des catégories et des sujets de données répertoriés dans les données 9 L'équipe OPs dispose uniquement d'un accès de niveau SE à l'application et au stockage, et non d'un accès au niveau compte ou site
3	Bosch.IO GmbH https://www.bosch-digital.com/imprint/	Fonctionnement et maintenance de bases de données jumelles numériques de dispositifs (https://eclipse.dev/ditto/) pour le stockage, le traitement et l'extraction des données de périphériques	Régions d'infrastructures AWS (voir la section 6)	Données de dispositif de catégorie de données

Tableau 1

Mesures techniques et organisationnelles

Les mesures suivantes sont convenues entre le Contrôleur de données et le Processeur de données et sont spécifiées dans le présent cas. Voir liste des pièces.

- I. Mesures permettant de garantir la confidentialité (Art. 32 para. 1 sect. b du RGPD)
  - I. Contrôle des accès physiques : aucun accès non autorisé aux systèmes de traitement des données.
  - II. Contrôle d'accès logique : aucune utilisation système non autorisée via des mots de passe (sécurisés), des mécanisme de verrouillage automatique, une authentification à deux facteurs et un chiffrement des données.
  - III. Contrôle de l'accès aux données : aucune lecture, copie, modification ou suppression non autorisée au sein du système via des concepts d'autorisation, des droits d'accès spécifiques à un utilisateur et une journalisation des accès.
  - IV. Contrôle de séparation : traitement séparé des données collectées à diverses fins.

- II. Mesures permettant de garantir l'intégrité (Art. 32 para. 1 sect. b du RGPD)
  - I. Contrôle de transfert : lecture, copie, modification ou suppression non autorisée pendant la transmission électronique ou le transport via un chiffrement, des réseaux privés virtuels (VPN) et une signature électronique.
  - II. Contrôle des entrées : détermination du moment et de la personne par laquelle des données personnelles ont été saisies, modifiées ou supprimées dans les systèmes de traitement des données via la gestion des journalisation et des documents.

- III. Mesures permettant de garantir la disponibilité et la résilience (Art. 32 para. 1 sect. b du RGPD), par ex. :
  - I. Contrôle de disponibilité : protection contre les dégâts accidentels, la destruction ou la perte dans le cadre d'une stratégie de sauvegarde.
  - II. Contrôle de commande : aucun traitement des données sur commande conformément à l'Art. 28 du RGPD sans les instructions correspondantes du Contrôleur de données via une conception explicite du contrat, une gestion des commandes formalisée, une sélection rigoureuse du fournisseur de services, l'obligation d'information à l'avance et le suivi des inspections.
  - III. Résilience : les systèmes et les services (p. ex. stockage, accès, capacités de ligne, etc.) sont conçus de manière à garantir même des contraintes intermittentes ou des charges de traitement élevées.

- IV. Mesure relatives à l'anonymisation des données personnelles via :
  - I. La séparation des données maître du contrôleur de données du client et des données client
  - II. L'utilisation d'ID de personnel, de client et de fournisseur au lieu de noms

- V. Mesure relatives au chiffrement des données personnelles via :
  - I. Le chiffrement symétrique
  - II. Le chiffrement asymétrique
  - III. Hachage

- VI. Mesures visant à restaurer rapidement la disponibilité des données personnelles après un incident physique ou technique, au moyen de mesures de sauvegarde.

- VII. Procédures de revue et d’évaluation périodiques (Art. 32 para. 1 sect. d du RGPD ; Art. 25 para. 1 du RGPD via :
  - I. Gestion de confidentialité
  - II. Gestion la réponse aux incidents
  - III. Protection des données par défaut (Art. 25 para. 2 du RGPD)
  - IV. Évaluation par DSO, audits IT
  - V. Évaluation, audits, certifications externes

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202309141013