Remote System Management

CBS-RM-DIPx

en Service description

Table of contents

1	**Main functions**	**4**
2	**System requirements**	**5**
3	**Web application**	**6**
4	**Documentation**	**7**
5	**Open Source Software components**	**8**
6	**Service hosting**	**9**
7	**Maintenance and service level**	**10**
8	**Customer and user obligations**	**11**
9	**GDPR-related information**	**12**

1 Main functions

Bosch's Remote System Management service allows you to leverage the power of the Internet of Things (IoT) to provide secure, transparent, and cost-effective asset management throughout the lifecycle of a video system. This service enables end users, system integrators and installers to perform inventory and update management, as well as health monitoring tasks for an entire Bosch video system (DIVAR IP + BVMS + cameras) from one centralized Remote Portal platform.

The service brings peace-of-mind to end customers by enabling 24/7 system monitoring in a secure way. This allows the user to act proactively when issues arise and to address them, for instance, before video recordings are lost due to a hard drive failure. The secure MQTTS connection also preserves data privacy, as video footage cannot be accessed by anyone via this connection, due to the fact that video and image data transfer is not supported by this protocol. Moreover, the service allows for remote software and firmware rollouts, keeping the system up-to-date and secure. Cloud connectivity is based on a single outbound connection from the DIVAR IP to Remote Portal, where the DIVAR IP consolidates all inbound and outbound communication for the entire video system.

The service is designed to be used by larger end customer organizations performing their own system maintenance across multiple dispersed sites, or by installers offering such services to a multitude of different end customers. The benefits of using Remote System Management focus on increased efficiency when performing system maintenance tasks, avoiding unnecessary trips on-site through remote maintenance capabilities, such as update rollouts in case of a security advisory, or through latest system information insights allowing for better preparation of on-site trips. Positive side effect: Full service with minimum CO_2 emissions. Additionally, the users can improve the service experience they provide by acting proactively and gaining the opportunity to address field issues before (internal) customers even realize they have a problem.
For functional details, please refer to the respective datasheets of the service.

Notice!

You can find the datasheets in the respective product catalog for your region or country.

2 System requirements

Software requirements

The Remote Portal web interface can be used with modern web browsers that support HTML5. For the best experience, Bosch recommends the use of Google Chrome.

Device requirements

To use Remote System Management to its full extent, Bosch IP cameras need to run firmware version 6.50 or later.

As stated in the datasheet, only specific DIVAR IP models are supported. For these models, the minimum software requirement is to support DIVAR IP System Manager 2.0 or later. Please refer to the respective datasheet for details.

The required bandwidth depends on the video system's specifications and the site's structure, i.e., the number of cameras and DIVAR IP devices on site. Bosch recommends a minimum bandwidth of 11 Mbps or 1.31 MBps per DIVAR IP, as the DIVAR IP consolidates the inbound and outbound communication for itself and connected cameras. This recommendation is derived from the most demanding use case in terms of bandwidth, namely the download of larger update files that create a peak bandwidth demand whenever such updates are triggered from Remote Portal. The majority of non-peak operation time will demand bandwidths of about 10 Kbps, e.g., for monitoring health parameters and other telemetry data exchanges.

Notice!

This bandwidth requirement can vary and the user should verify that the available bandwidth fulfills the requirement of the application. Bosch provides several tools for the calculation of the required bandwidth, but takes no responsibility for actual bandwidth availability and proper configuration.

3 Web application

Remote System Management is integrated with Remote Portal, which serves as the central web-based platform for the service activation and additional general capabilities, independent of the service offering, as described below.

System and device management with a dashboard view
Systems and single devices can be grouped in hierarchical order to match customer or installation location, limit access for a set of devices or aggregate status of multiple devices.

Service overview
The "Services" section in Remote Portal provides an overview of all available services across device types. Each service will list a consolidated overview of all devices and systems where it is actively in use.

Service license management
Services can be activated by visiting Remote Portal after the initial commissioning of the DIVAR IP to Remote Portal.
The Remote System Management service requires licenses for activation. Depending on the DIVAR IP model and its operation mode, different licenses apply. Please check the datasheets for details. Licenses are managed and activated in Remote Portal in the "Service licensing" section.

User management
Remote Portal allows for fine-grained control of access to devices and services. Through role management *administrators*, *technicians* and *end users* can be individually associated with systems, groups and services.

Notice!

For more information on the Remote Portal visit the respective product page available at:
https://commerce.boschsecurity.com/gb/en/Remote-Portal/p/86180387339/

4 Documentation

The user documentation and datasheets for all individual DIVAR IP-based systems can be found and accessed here:

Technical trainings: https://academy.boschsecurity.com/

NOTE: A standalone Remote System Management Introduction Training will be made available. This training will later be integrated into the DIVAR IP all-in-one Certification Training.

How-to/Configuration notes: https://community.boschsecurity.com/t5/Security-Video/tkb-p/bt_community-tkb-video/label-name/remote_system_mgmt?labels=remote_system_mgmt

Datasheets/Application notes: https://commerce.boschsecurity.com/gb/en/bt/search/?text=cbs-rm-dip

5 Open Source Software components

The Open Source Software components included in the Remote Portal platform can be found here: https://remote.boschsecurity.com/open_source/open_source_licenses.txt

6 Service hosting

The services listed here are hosted on AWS infrastructure-as-a-service.
The application Remote Portal is a global multi-tenant platform. This platform, its database, backend and frontend is hosted in the AWS region Frankfurt, Germany.

7 Maintenance and service level

Bosch offers a dedicated Service Level Agreement (SLA) for signed resellers of Remote System Management by Bosch. This SLA outlines the guaranteed availability, maintenance and support process in detail for Remote System Management by Bosch and contains contact details for emergency hotlines, penalty clauses etc.
Contact your local sales representative for more information.

8 Customer and user obligations

For direct customers of Bosch acceptance of the Terms and Conditions for Software as a Service Resellers is required to be able to obtain Remote System Management licenses or subscriptions. For the activation of service licenses or subscriptions users need to agree to the terms and conditions of Remote Portal. Further obligations include:

- 8.1. The Internet connection between customers, their monitoring center/control room, and the installation site of compatible devices (including video cameras, hereinafter referred to as "Devices") up to the data center's Internet interface used by Bosch, as well as the end customer relationship between customer and its contractual partners are the sole responsibility of customers.
- 8.2. Installing, operating, maintaining, and - where necessary - repairing devices are the sole responsibility of customers.
- 8.3. The application is not designed or warranted for use in high-risk applications requiring special fail-safe performance, such as in the operation of nuclear facilities, air traffic control, life support, or other applications, devices or systems in which the failure of a device or application could lead directly to death, personal injury, or severe physical or environmental damage (“high risk activities”). Notwithstanding any other provision customers shall not use or permit any third party to use the Application with any high-risk activity.
- 8.4. To obtain the necessary consent of the persons affected in accordance with data security and data protection regulations as personal data is collected, processed, or used in the course of said persons’ use of the application and no legislation permitting such collection, processing, or use without the need to obtain consent applies to the case in question.
- 8.5. Check data and information for viruses or other malware before sending the data and information to Bosch, and to ensure that antivirus programs meet the latest requirements.
- 8.6. Report defects in the contractual services to Bosch immediately after being made aware of the defect. If there is a delay in sending the notification or if notification is not provided despite customer being aware of the defect, a unilateral reduction in the fee or suspension by customer, as well as extraordinary termination, is excluded.
- 8.7. The following roles and tasks are the sole responsibility of customer:
  - 8.7.1. Assigning roles and authorizations to the corresponding persons or units for the user roles available in the Remote Portal, and managing these roles and authorizations.
  - 8.7.2. Allocating devices to contractual partners of customer and to the contractual partners' sites.
  - 8.7.3. Procuring, installing, and connecting suitable devices for operation in accordance with the system requirements. The Application supports the operation of devices by customer by means of the functions outlined.

9 GDPR-related information

Purpose of the data processing

Bosch processes personal data only to the extent, and in such a manner, as is necessary:
1. in order to meet Bosch's obligations under the agreement/terms of use of the Remote System Management service offering; and
2. to comply with customers instructions from time to time (which may be specific instructions or instructions of a general nature as set out in this agreement or as otherwise notified by customer to Bosch),
3. and shall not process the personal data for any other purpose.

Data categories

- Device data: Data entered by Data Controller or transferred by the device of the Data Controller - device master data, device health telemetry data, and software versions metadata. Location and contact person of a device. Used to enable the provided Remote System Management service to the Data Controller.
- Device related logs: Device activities are logged to enable troubleshooting of the system.
- User configuration data: Data entered by Data Controller while using the solution such as user access information including IP address, company, first name, last name and email address necessary to provide user application access.
- User action logs: Documentation of users' system use including performed actions and associated timestamps. Used to help resolve maintenance cases and to improve user experience.
- Non-personal data such as site, customer account and service configuration data incl. types and flows.

Data subjects

- Employees of customer
- End-users or contractual partners of customer ("customer-of-customer")

Subcontractors

All subcontractors are listed in **Table 1**.

	Name and address of subcontractor and name of data privacy officer / contact person for privacy related questions	**Scope of service (scope of the order placed by the contractor)**	**Place of data processing**	**Transfer/access to personal data of the client (type of data and group of data subjects)**
1	Amazon Web Services (AWS)	Infrastructure/Hosting Provider (as outlined in security concept) as well as managed service provider for storage, manipulation and retrieval of data, and cloud connectivity	AWS Infrastructure Regions (see section 6)	All categories and data subjects listed in data 9

	Name and address of subcontractor and name of data privacy officer / contact person for privacy related questions	Scope of service (scope of the order placed by the contractor)	Place of data processing	Transfer/access to personal data of the client (type of data and group of data subjects)
2	Robert Bosch India Data Protection Officer Bosch India (RBEI/DSO) DPO.India@in.bosch.com	Restricted group of Technical Operations Support	No.123, Industrial Layout, Hosur Road, Koraman-galaBengaluru-560 095 Karnataka, India	All categories and data subjects listed in data 9 OPs-team has only OS level access to application and storage, not account or site-level
3	Bosch.IO GmbH https://www.bosch-digital.com/imprint/	Operation and Maintenance of Digital Device Twin database (https://eclipse.dev/ditto/) for storage, manipulation and retrieval of device data	AWS Infrastructure Regions (see section 6)	Data category device data

Table 1

Technical and organizational measures

The following TOMs are agreed between the Data Controller and the Data Processor and specified in the present individual case. See specimen list.

- I. Measures to ensure confidentiality (Art. 32 para. 1 lit. b of the GDPR)
  - I. Physical access control: No unauthorized access to data processing systems.
  - II. Logical access control: No unauthorized system use via (secure) passwords, automatic locking mechanisms, two-factor authentication, and data encryption.
  - III. Data access control: No unauthorized reading, copying, changing or removing within the system via authorization concepts and user-specific access rights, and logging of access.
  - IV. Separation control: Separate processing of data collected for various purposes.

- II. Measures to ensure integrity (Art. 32 para. 1 lit. b of the GDPR)
  - I. Transfer control: No unauthorized reading, copying, changing or removing during electronic transmission or transport via encryption, Virtual Private Networks (VPN), and electronic signature.
  - II. Input control: Determination of whether and by whom personal data was entered, changed or removed in data processing systems via logging and document management.

- III. Measures to ensure availability and resilience (Art. 32 para. 1 lit. b of the GDPR), e.g.:

  - I. Availability control: Protection against accidental damage or destruction or loss via backup strategy.
  - II. Order control: No data processing under commission according to Art. 28 of the GDPR without corresponding instructions from the Data controller via explicit contract design, formalized order management, stringent selection of the service provider, obligation to convince in advance, and follow-up inspections.
  - III. Resilience: Systems and services (e.g. storage, access, line capacities, etc.) are designed in a way that even intermittent high stresses or high constant loads of processings can be ensured.

- IV. Measures for the pseudonymization of personal data via:
  - I. Separation of customer data controller master data and customer data
  - II. Use of personnel, customer, and supplier ID instead of names

- V. Measures for the encryption of personal data via:
  - I. Symmetrical encryption
  - II. Asymmetrical encryption
  - III. Hashing

- VI. Measures to quickly restore the availability of personal data to them after a physical or technical incident via back-up concept.

- VII. Procedures for periodical review, assessment and evaluation (Art. 32 para. 1 lit. d of the GDPR; Art. 25 para. 1 of the GDPR) via:
  - I. Privacy management
  - II. Incident response management
  - III. Data protection by default (Art. 25 para. 2 of the GDPR)
  - IV. Assessment by DSO, IT audits
  - V. External assessment, audits, certifications

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

Building solutions for a better life.

202309141013