CBS-RM-DIP4 Remote System Management DIP 4000 1yr
Remote Portal

- Centralized remote inventory management providing quick access to the entire system connected to the Remote Portal
- Streamlined system administration and maintenance to rollout updates and patches, ensuring your entire system is up-to-date and secure
- Detailed health and alert monitoring providing real-time information on single device and system health
- Privacy focused cloud connection

Bosch's Remote System Management service allows you to leverage the power of the Internet of Things (IoT) to provide an easy-to-use set of tools and capabilities for secure, transparent and cost-effective asset management throughout the life cycle of a device or system.
This service enables users to perform inventory and update management, as well as health monitoring tasks for an entire system from one centralized Remote Portal platform.

Functions

Inventory management
Easily connect your system to Remote Portal ensuring secure device connectivity and verifiable device enrollment. This centralized management platform provides a continuous real-time overview of a system's inventory, including information on current software and firmware versions.

Update management
The update management feature is designed to remotely manage and deploy updates to a device or system as a whole across one or multiple sites.

- Quickly deploy security patches and firmware/ software updates.
- Automatically generate update reports to provide a detailed summary of changes implemented by an update campaign.

Health monitoring
The health monitoring capabilities of the Remote System Management service promote informed decision making and proactive troubleshooting for increased system uptime and reduced time spent on site.

- Monitor connectivity, update availability and device authorization status.
- Detailed insights on hardware and recording health.
- Define health alerts via email.

Operation mode support
The DIVAR IP connectivity to Remote Portal and the Remote System Management service support all operation modes - BVMS, Video Recording Manager (VRM), and iSCSI target. The VRM and iSCSI modes offer management of the DIVAR IP device only. To manage an entire system, including cameras, the DIVAR IP needs to be operated in BVMS mode. In the context of Remote System Management, the VRM and iSCSI modes are effective when used as sub-systems that integrate an overarching video system, which includes a DIVAR IP head system operating in BVMS mode.

Note: Each DIVAR IP connects individually to Remote Portal for all operation modes. DIVAR IP devices belonging to an overarching video system need to be grouped accordingly within the respective company account.

Data security
The highest level of security for remote device access and data transport is ensured.
The inclusion of a Public Key Infrastructure (PKI) delivers superior identity attestation and protection against tampering. This allows for strong certificate-based authentication between device and cloud, and secure communications for remote device access.
Local device security is ensured by multi-layer security hardening configurations and by leveraging Windows Server security capabilities, including:

- Windows Security Baseline, which is a group of industry-standard security configuration settings recommended by Microsoft.
- Windows Defender Device Guard to ensure that only trusted software is run on the server.
- Control Flow Guard to provide built-in protection against memory corruption attacks.
- Windows Defender Antivirus, which is a built-in antimalware solution that provides security and antimalware management.
- Windows Defender Credential Guard, which uses virtualization-based security to isolate credential information, preventing password hashes or Kerberos tickets from being intercepted.
- Local Security Authority (LSA), which resides within the Local Security Authority Security Service (LSASS) process, validates users for local and remote sign-ins and enforces local security policies.

Data privacy
Maintaining the privacy of customer and user data is assured by the Remote System Management with the following measures:

- Dedicated cloud connection for maintenance and monitoring purposes only (based on MQTTS protocol).
- No remote video access, while having 24/7 transparency on system health.
- Video and maintenance data are separated for DIVAR IP devices: remote connection for system maintenance services without risking unauthorized video access.

Simplified firewall administration
DIVAR IP devices consolidate all camera communication for an entire video system into a single outbound connection to Remote Portal. Maintaining a single outbound connection greatly reduces the effort required for IT firewall administration tasks.

Remote Portal integration
The Remote System Management service is seamlessly integrated with the Remote Portal.
The initial connectivity to the Remote Portal is free-of-charge.
With the appropriate license, the Remote System Management service capabilities can be activated online in Remote Portal.

Notice
Functionality and services may vary by device.
For more details about the respective system requirements, refer to the respective documentation for each device.

Register for free on:
https://remote.boschsecurity.com

NOTE: The Remote System Management provides a free trial period, after which users will still be able to use the features listed below:

- Remote Portal connectivity.
- Basic inventory management to view and organize installed assets.
- Monitoring of connectivity, update availability and authorization/license status.

Notice
Service details
Additional service details are described in the Remote System Management Service description document which can be downloaded from the product catalog page.

Parts included

Quantity	Component
1	Remote System Management 1 year license

Technical specifications

Connectivity

Network	For best performance, a fixed internet connection should be used to connect devices to the Bosch Security Cloud. Cellular internet connections may be used but they can impact performance or availability.
Browser	The browser-based interfaces of the Remote Portal are best displayed with contemporary browsers: • Google Chrome • Firefox • Microsoft Edge **NOTE**: JavaScript must be enabled.

Data security

Secure crypto-processor (TPM)	TPM v2.0
PKI	X.509 certificates
Network security	TLS v1.2 or higher, DTLS 1.2 or higher
Local encryption	Device encryption, AES-256

Compatibility

Device	Minimum firmware/software version
DIVAR IP all-in-one 4000	DIVAR IP System Manager 2.0
Bosch IP cameras (connected to the licensed DIVAR IP all-in-one device)	Firmware version 6.5

Ordering information

CBS-RM-DIP4 Remote System Management DIP 4000 1yr
License to enable Remote System Management services for one DIVAR IP all-in-one 4000 device for a 1 year period
Order number **CBS-RM-DIP4 | F.01U.410.890**

Represented by:

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

North America:
Bosch Security Systems, LLC
130 Perinton Parkway
Fairport, New York, 14450, USA
Phone: +1 800 289 0096
Fax: +1 585 223 9180
onlinehelp@us.bosch.com
www.boschsecurity.com

Asia-Pacific:
Robert Bosch (SEA) Pte Ltd, Security Systems
11 Bishan Street 21
Singapore 573943
Phone: +65 6571 2808
Fax: +65 6571 2699
www.boschsecurity.com/xc/en/contact/
www.boschsecurity.com