# VideoView+

CBS-MOBILE

en Service description

# Table of contents

# 1 Main functions

VideoView+ is a service for an easy-to-use, light-weight and cloud-based video security system. VideoView+ is the ideal fit for customers, who want to manage minimum hardware and need affordable, basic remote management capabilities with a preference for Bosch IP cameras. The service builds upon the components Video Security Client/Video Security App, Remote Portal, and Alarm Management.

Bosch delivers Remote Portal - a portal for management of devices and licenses to technical teams, installers, and integrators, which allows the service configuration of VideoView+ and the remote connectivity from Video Security Client/Video Security App to Bosch cameras.
Bosch delivers Video Security App/Video Security Client - a desktop app for Windows or a mobile app for iOS and Android smartphones and tablets to security operators, security staff in general and smartphone users.
Video Security App/Video Security Client allows to connect to Bosch IP cameras and encoders at any time from all over the world via Remote Portal and supports immediate video live view and playback of recordings, forensic search on cameras with Bosch video analytics support and smooth control of PTZ cameras.
Together with Alarm Management - a cloud-based monitoring platform provided by Bosch, push event notifications with 10 seconds event clips recorded in the Alarm Management cloud can be received and replayed in Video Security App/Video Security Client.
These functions and processes support remote video surveillance for multi-site customers for Bosch cameras without requiring expensive on-site hardware or maintenance.

For a detailed description of functions, refer to the following datasheets or application notes:

- Cloud applications:
  - Datasheet Remote Portal
  - Datasheet Alarm Management

- Client applications:
  - Datasheet Video Security Client (MFT-VSC)
  - Datasheet Project Assistant (MFT-PA)
  - Datasheet Configuration Manager (MFT-CM)
- Cloud service
  - Datasheet VideoView+ Service

# 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.
Video Security Client requires Windows 11, Windows 10.1607 "Anniversary Update" (64 bit) or higher. Video Security app requires Android 8.0 or higher with OpenGL ES 3.0 or higher, iOS 13 or higher. Refer to the respective app store for the latest compatibility information.
To receive push notifications in the Video Security app, specific settings may be required on the mobile device to allow these notifications. The mobile device needs to be registered with the push notification service in Alarm Management.

**Device requirements**

To use VideoView+, any Bosch IP camera with firmware version 6.40 and later must be connected to Remote Portal first.
It is required that the camera is either equipped with a local SD card or a managed recording target (iSCSI NAS, Video Recording Manager, DIVAR IP).
3rd party cameras are currently not supported by VideoView+.
On Remote Portal, the VideoView+ service can then be activated per camera. Additional hardware such as a cloud gateway is not required to connect a camera to Remote Portal.
The required bandwidth on site depends on the camera type, camera settings, stream settings, alarm scenarios and site structure (for example number of cameras on site). Bosch recommends a minimum of 512 kbit/s per Bosch IP camera. 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 applications

The provided web applications consist of Remote Portal and Alarm Management. The VideoView+ license management and the VideoView+ service activation is integrated in Remote Portal. While the push event notification service configuration of VideoView+ is contained in the web interface of Alarm Management, all other VideoView+ service configurations are performed in Remote Portal. In detail, the Remote Portal web application provides functions to achieve the following:

**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**
VideoView+ service requires a license per camera per year for activation. Licenses are managed and activated in Remote Portal.

**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.

**Push event notification**
Configuration of a push event notification service in combination with the Video Security app / Video Security Client notifying customers or security guards about relevant events from their sites. The user can access the related event clips.
This function is available when the license VideoView+ is activated in Remote Portal and the push notification service including 10 seconds event video clip cloud recording in the Alarm Management cloud is configured.

**Live View via "Camera Viewers"**
As a customer user of Remote Portal select from your cameras and devices from the map for permanent video live monitoring as either low-bandwidth or high-priority streaming with full control (PTZ, Audio, Intercom, etc.).
Camera Viewers are a light-weight viewing tool that gives end-customers browser-based access to live images and video streams of cameras. Up to four cameras can be displayed with live streaming or JPEG polling.

# 4 Mobile/Desktop applications

The VideoView+ service license unlocks features within Video Security Client/ Video Security App and must be used together with this application.

Video Security Client and Video Security App focus on on-demand live streaming and access to the cameras for staff that is not on-site. Both applications provide following features:

- List of groups of cameras created in Remote Portal
- Thumbnail view of cameras per site
- Live video stream
- Flexible cameo and grid view
- Access to the local recordings of the individual cameras
- Use of camera functions (PTZ, Relay, Audio)
- Interactive timeline for local recordings
- Base forensic search
- Export of video clips
- Selected device alarms, also called events, received by push notification, directly connect to device
- Access to event clips through event list
- Remotely arm/disarm site (available after May/June 2024)
- iOS, Android (for Video Security App) and Windows compatible (for Video Security Client)

# 5 Documentation

You can find the user documentation and datasheets for all individual components of the VideoView+ service under the following links:

| | |
|---|---|
| Technical trainings: | https://academy.boschsecurity.com/ |
| How-to/Configuration notes: | https://community.boschsecurity.com/ |
| Datasheets/Application notes: | https://www.boschsecurity.com/xc/en/product-catalog/ |

# 6 Open Source Software components

The Open Source Software components included in the components can be found here:

- Remote Portal:
  https://remote.boschsecurity.com/open_source/open_source_licenses.txt
- Alarm Management:
  https://<cloud application URL>/static/open_source_licenses.txt
  Example: https://demo.cbs.boschsecurity.com/static/open_source_licenses.txt

Each client application provides the Open Source Software component information within the application.

# 7 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. Remote Portal provides three global endpoints for device connectivity and streaming of video data. These endpoints are called "Video Relay". These video relays are hosted regionally in the AWS regions USA-EAST (USA), ASIA-PACIFIC (Singapore) and EUROPE (Germany). The user can select during the device commissioning process of a device to Remote Portal which of these video relays is to be used for device connectivity.

The Alarm Management cloud is either hosted as a regional multi-tenant service or a dedicated single- tenant service. This depends on the required system set-up and order of the customer. For the dedicated single-tenant option, customers can choose the hosting location from the main AWS availability/infrastructure regions. The available regions are listed here: https://aws.amazon.com/de/about-aws/global-infrastructure/regions_az/

During the set-up of a dedicated instance of Alarm Management the customer then needs to specify to which "video relay" this instance should connect (EUROPE, ASIA-PACIFIC, USA-EAST). The hosting specifications for a dedicated single-tenant instance are gathered in a structured onboarding process once legitimate business interest is established.

# 8 Maintenance and service level

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

# 9 Customer and user obligations

Direct Bosch customers have to accept the **Terms and Conditions for Software as a Service Resellers** (SaaS) as well as the respective **Service Level Agreement** (SLA) to be able to obtain VideoView+ licenses or subscriptions.
For the activation of service licenses or subscriptions, users need to agree to the terms and conditions of Remote Portal. Users of VideoView+ applications and clients need to agree to the respective SaaS terms and conditions of use in Remote Portal:

- 9.1. 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.
- 9.2. Installing, operating, maintaining, and - where necessary - repairing devices are the sole responsibility of customers.
- 9.3. 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.
- 9.4. 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.
- 9.5. 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.
- 9.6. 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.
- 9.7. The following roles and tasks are the sole responsibility of customer:
  - 9.7.1. Assigning roles and authorizations to the corresponding persons or units for the user roles available in the Application, and managing these roles and authorizations.
  - 9.7.2. Allocating devices to contractual partners of customer and to the contractual partners' sites.
  - 9.7.3. Activating contractual partners to use the Video Security Client or Video Security App.
  - 9.7.4. 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.

# 10 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 and applications of VideoView+ functions; 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**

- 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. In action logs, user names are encoded with a key and cannot directly be read from action logs.
- Non-personal data such as site, customer account and service configuration data incl. types and flows.
- In case of complying with customers' instructions to Bosch as laid out in 10.1: video data such as livestream and recordings - used for remote setup, configuration, optimization specifically for camera intelligent video analytics.

**Data subjects**

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

**Subcontractors**

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

| | **Company name, direction of the subprocessor and contact partner for data protection questions** | **Content of assignment (Scope of the commission by the Data processor)** | **Place of data processing and/or storage** | **Transmission of/ access to personal data of the Data controller (category of data and data subjects)** |
|---|---|---|---|---|
| 1 | Amazon Web Services (AWS) | Infrastructure/ Hosting Provider (as outlined in security concept) | AWS Infrastructure Regions: USA-EAST (USA), ASIA-PACIFIC (Singapore) and EUROPE (Germany) | All categories and data subjects listed in the specific service description |

| | Company name, direction of the subprocessor and contact partner for data protection questions | Content of assignment (Scope of the commission by the Data processor) | Place of data processing and/or storage | Transmission of/ access to personal data of the Data controller (category of data and 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, Koramangala, Bengaluru, 560095 Karnataka, India | All categories and data subjects listed in the specific service description OPs-team has only OS level access to application and storage, not account or site-level |
| 3 | Thales EMS | License management system | Tour Carpe Diem 31, Place des Corolles - Quartier La Defense, COURBEVOIE EUROPE (France) | Minimal information to identify a customer or Remote Portal company |
| 4 | Bosch.IO GmbH https://www.bosch-digital.com/imprint/ | BT user hub | EUROPE (Germany) | Identity of the Remote Portal user account and associated attributes |
| 5 | Google Analytics | web analytics tools | EUROPE | Usage data of Remote Portal |
| 6 | Google Maps | Maps api | EUROPE | Device location & site information |
| 7 | VXG https://www.videoexpertsgroup.com/ | Cloud video storage | USA-EAST (USA) and EUROPE (Germany) | Video footage |
| 8 | L1 tec support (Timisoara) CentralSupport.BT@bosch.com | Restricted group of Technical Support | EUROPE (Romania) | Contact name and description of system setup |
| 9 | L1 tec support (Heredia) Technical.Support@us.bosch.com | Restricted group of Technical Support | NORTH AMERICA (Costa Rica) | Contact name and description of system setup |

| | Company name, direction of the subprocessor and contact partner for data protection questions | Content of assignment (Scope of the commission by the Data processor) | Place of data processing and/or storage | Transmission of/ access to personal data of the Data controller (category of data and data subjects) |
|---|---|---|---|---|
| | soporte.seguridad@bosch.com | | | |

**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**

202404161711