AI Alarm Verification

en Service description

Table of contents

1	Main functions	4
2	System requirements	5
3	Web application	6
4	Mobile/Desktop applications	7
5	Documentation	8
6	Open Source Software components	9
7	Service hosting	10
8	Maintenance	11
9	Customer and user obligations	12
10	GDPR-related information	13

1 Main functions

AI Alarm Verification by Bosch is a cloud-based Video Content Analysis alarm verifier for intelligent Bosch cameras. It uses specialized AI models in the cloud to verify alarms triggered by cameras, in order to improve detection accuracy and to reduce unwanted alarms.

It is especially valuable for operators managing a high volume of centralized Video Content Analysis alarms, allowing them to focus on critical moments. This reduces fatigue from repetitive tasks, improves decision-making, and enables faster response times.

The AI Alarm Verification family by Bosch includes two separate services that support different object classes. The supported services include camera-triggered gun detection (IVA Pro Visual Gun Detection) and camera-triggered perimeter detection, such as people and vehicles (IVA Pro Perimeter).

AI Alarm Verification is currently available for two platforms: Milestone XProtect® (external product from external company) and Cloud-Based Alarm Management (Bosch service).

AI Alarm Verification can verify different types of alarms ranging from IVA Pro Visual Gun Detection to IVA Pro Perimeter (human and vehicle) alarms. Refer to the respective datasheets, available for download in the Bosch online catalog.

Integration with Milestone XProtect®

AI Alarm Verification seamlessly integrates with Milestone XProtect® using version 2023 R3 or higher. The integration is done through two main components:

- **Management Client Plugin**: This plugin enables basic configuration within Milestone XProtect®. Once a Bosch camera is enabled for the service, the plugin automatically adjusts settings to activate AI Alarm Verification and to optimize performance, including stream settings.
- **AI Gateway**: This Windows service runs in the background, connects to Milestone XProtect®, and manages alarms triggered by selected cameras. The service subscribes to gun detection alarms and sends representative images or videos to the Bosch-managed cloud, which is hosted on AWS or Azure, for verification using a powerful Bosch-developed AI module. To select the hosting provider and hosting location, contact your local sales representative.

  Based on the AI analysis, the alarm is either verified and displayed to the operator, or rejected and potentially removed from the operator's view.

Licensing and management

A system integrator setting up the service requires a Remote Portal account and must assign a license to the AI Gateway.

The registration process for the gateway follows a defined process in the Remote Portal.

The Bosch AI Alarm Verification Management Client Plugin for Milestone XProtect® assists with configuration and setup.

Licenses for AI Alarm Verification services are managed and activated in the Remote Portal.

Notice!

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

2 System requirements

Milestone XProtect® video management software

- Requires Milestone XProtect®, version 2023 R3 or higher
- To ensure reliable verifications, Milestone machines must not be overloaded in terms of CPU, disk space, RAM, or network connection
- The AI Gateway must run either on the same machine as Milestone XProtect®, or on a different machine with a stable network connection to the Milestone XProtect® video management software
- The plugin requires the system to have Webview2 runtime available

Notice!
If WebView2 is not available by default, such as with a few Milestone Husky systems, you must install it in the host machine.
Refer to Microsoft documentation for downloading and installing the latest version of WebView2 runtime.

Device requirements

- Compatible Bosch cameras with activated IVA Pro Visual Gun Detection. The camera must be correctly configured, and must comply with the application requirements or restrictions
- Cameras must continuously record in the Milestone XProtect® system and must be locally connected
- For lossless video and for metadata transmission, the device requires a fast and reliable connection between cameras and the VMS

Network requirements

- Bosch recommends a minimum upload bandwidth of 10 Mbit/s. This recommendation can be different depending on camera type, settings, and alarm scenarios. A lower bandwidth can cause longer processing times for verification results. A lower bandwidth can also cause more timeouts, leading to an increased number of fallback alarms

3 Web application

Service License Management

Some services require licenses for activation. Licenses are managed and activated in Remote Portal.

License Terms and Conditions are accepted during the activation on Remote Portal. Refer to remote.boschsecurity.com for more information.

4 Mobile/Desktop applications

For mobile applications for Milestone XProtect®, refer to the respective documentation from Milestone. The XProtect® Smart Client is available as a desktop application. Bosch recommends using the XProtect® Mobile Client for portable use.
The AI Alarm Verification service integrates with both options to enable different use cases. For example, the integration with the XProtect® Mobile Client enables the display of verified alarms. This is especially useful for on-site security personnel when deciding on response scenarios. The integration with the XProtect® Smart Client provides workflow and scalability when managing multiple sites and numerous alarms.
In general, Bosch takes no responsibility for the configuration of these clients and offers no support for the local Milestone XProtect® system. Refer to the knowledge base for best practices.

5 Documentation

The user documentation and datasheets for all individual components contained in the AI Alarm Verification portfolio can be found and accessed here:

Technical trainings:	https://academy.boschsecurity.com/
How-tos/Configuration notes:	https://community.boschsecurity.com/
Datasheets/Application notes:	https://www.boschsecurity.com/xc/en/product-catalog/
Camera compatibility sheet:	https://www.boschsecurity.com/xc/en/product-catalog/
Service Level Agreement	Available from your reseller
Alarm Management Service description	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
- Milestone Configuration Plugin from Bosch: <Program Files>\VideoOS\MIPPlugins\BoschAVConfigPlugin\ClientPlugin\open_source_licenses.txt
- Milestone Gateway from Bosch: <Program Files>\VideoOS\MIPPlugins\BoschAVConfigPlugin\ClientPlugin\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 and AZURE infrastructure-as-a-service.
The application Remote Portal is a global multi-tenant platform. This platform, its database, backend and frontend are hosted in the AWS region Frankfurt, Germany. Remote Portal provides three global endpoints for device connectivity and streaming of video data. These video relays are hosted regionally in the 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.
For the application of AI Alarm Verification for Milestone, the service for the verification is hosted in a multi-tenant environment on AWS and Microsoft Azure, region USA. This means that video data is only transferred and evaluated in the United States. For further information, contact your local sales representative.

8 Maintenance

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

9 Customer and user obligations

- **Accept agreements**: Agree to the relevant Service Level Agreement (SLA) and, if applicable, the Terms and Conditions for Software as a Service Resellers. Users must also agree to the Remote Portal's terms and conditions.
- **Understand functionality and limitations**: The user needs to understand whether the service is applicable to the on-site security target and understand its functionality, e.g. how alarms are verified and how these alarms are returned to the operator display. The user must further understand the terminology between rejected, verified, unverified and the impact settings in the Configuration Client can have.
- **Maintain infrastructure**: Be solely responsible for the internet connection between their monitoring center/control room, VMS, and the installation site of compatible devices, as well as the relationship with their contractual partners.
- **Install and maintain devices**: Properly install, operate, maintain, and repair all devices used with the service.
- **Adhere to usage restrictions**: Refrain from using the application in high-risk activities where failure could lead to death, injury, or severe damage.
- **Obtain consent for data processing**: Obtain necessary consent for processing personal data according to data protection regulations.
- **Protect against malware**: Scan data and information for viruses or other malware before sending them to Bosch.
- **Report defects promptly**: Immediately report any defects in the contractual services to Bosch.
- **Manage roles and devices**: Assign roles and permissions within the application, allocate devices to contractual partners, and manage their sites.
- **Procure and configure devices**: Procure, install, and connect suitable devices according to the system requirements outlined in the documentation.
- **Test the system thoroughly**: The user is responsible for rigorously testing the AI Alarm Verification system after installation. This includes subjecting the system to various scenarios to ensure its reliability and functionality under all expected conditions. Proper testing is essential to identify and address any potential issues before the system goes live.
- **Ensure high-quality video recordings**: It is crucial for the AI Gateway to have access to high-quality video recordings without encoding errors or frame losses. Any degradation in video quality can negatively and severely affect the functionality of the AI Alarm Verification service. Possible causes of encoding errors include overloading either the camera encoder, the network traffic, or the recording server. By proceeding, the user acknowledges and accepts the following responsibilities:
  - To ensure that all recordings are of high-quality
  - To regularly monitor and maintain the streaming and recording settings
  - To understand that any issue due to low-quality recordings can result in failure

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. to meet Bosch's obligations under the agreement/terms of use of AI Alarm Verification 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 the customer to Bosch),

Data categories

- Video data: data generated by the AI Alarm Verification service of the customer/user to comply with the Bosch verification service as laid out in the functional description of the application.
- User configuration data: data entered by Data Controller while using the solution such as user access information including first name, last name and e-mail address necessary to provide user application access (especially for Remote Portal).
- 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 10.1**.

	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 (Remote Portal)	AWS infrastructure regions (see section 7)	Single images/ video clips, video metadata
2.	Microsoft Azure	Infrastructure/ Hosting provider	Microsoft Azure infrastructure	Single images/ video clips, video metadata

3.	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-560095 Karnataka, India	All categories and data subjects listed in data 10.2 OPs-team has only OS level access to application and storage, not account or site-level

Table 10.1: List of subcontractors

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)
- II. Physical access control: No unauthorized access to data processing systems, e.g.: magnetic or smart cards, keys, electronic door openers, plant protection or security guard, alarm systems, video systems.
- III. Logical access control: No unauthorized system use, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, data encryption.
- IV. Data access control: No unauthorized reading, copying, changing or removing within the system, e.g.: authorization concepts and user-specific access rights, logging of access.
- V. Separation control: Separate processing of data collected for various purposes, e.g.: multi-client capability, sandboxing.
- VII. Procedures for periodical review, assessment and evaluation (Art. 32 para. 1 lit. d of the GDPR; Art. 25 para. 1 of the GDPR), e.g.
  - 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

202410111753