

Alarm Management



Bosch offers a complete solution for video surveillance services. This solution builds on the infrastructure and features of the following Bosch platforms: Bosch Security Cloud, Remote Portal for device management and Bosch Alarm Management, a cloud-hosted platform for alarm verification, management, transmission and cloud storage. It provides users with all features required to configure and use video surveillance functions such as alarm message list, video verification view including event timeline, video investigation live-view with audio intercom, PTZ control, metadata visualization, geolocation maps, VCA metadata overlay, event and video storage, trouble and tamper notification.

- Alarm Verification verifies incoming camera events using a deep-learning neural network to reduce unwanted alarms.
- Alarm Management includes several ready-to-use functions, such as Live Intervention, Video Verification, Virtual Guard, Virtual Assistant and Smart Notification. Alarm Management is optimized to the needs of alarm operators in multi-location medium enterprises, retailers, quick service restaurants, remote utilities, control rooms and Smart City surveillance.
- Alarm Transmission allows forwarding of alarm scenarios to external recipients. With the licensed feature Cloud Alarm Transmitter,

- ▶ Operated, secured, maintained by Bosch as multi-tenant or dedicated Alarm Management instance with 24/7 support
- ▶ Scalable from single cameras to unlimited number of sites and cameras from Bosch or 3rd parties for multi-location use-cases
- ▶ Forwarding of alarms from individual cameras or on-site Alarm Management to central monitoring centers. Integration with more than 20 leading certified alarm automation solutions available
- ▶ Encrypted communication between cameras, cloud and clients according to IEC/EN 62676-2-33 cloud uplink standard

existing alarm automation software of many major brands can be integrated. This allows outsourcing of alarm processing to partners such as professional control rooms or certified central monitoring stations (CMS).

- Cloud Storage allows continuous or event-based recording of video from Bosch and 3rd party cameras with different retention times independent of Alarm Management.

To use Alarm Management, 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 connected using a plug-in provided by Bosch or by a cloud-hosted ONVIF gateway. 3rd party cameras are added to Alarm Management first, and then licensed in Remote Portal.

In Remote Portal, individual functional components of Alarm Management can then be activated per camera. Additional hardware such as a cloud gateway is not required to connect a camera to Remote Portal.

Remote Portal offers further services for connected devices such as device management, value-added services or application management.

For more details on 3rd party camera compatibility, refer to the Alarm Management compatibility list.

System overview

Bosch Alarm Management is available as a dedicated (private) cloud or via ready-to-go multi-tenant clouds hosted in the following regions:

eu.cbs.boschsecurity.com (EU)

na.cbs.boschsecurity.com (US)

ap.cbs.boschsecurity.com (SGP)

An account for a multi-tenant system is available after registering to the system on the respective domain. A private cloud is set-up on-demand after purchasing the dedicated cloud package.

Private data-center (“on-premise”) hosting of the platform is only offered use-case dependent as a managed service.

The usage of functional components like Alarm Transmission, Cloud Storage, etc. requires license activation per camera on Remote Portal.

Remote Portal is a separate cloud platform in Bosch Security Cloud for video surveillance as a service.

The following functions for cameras are available via Remote Portal:

- Configuration Manager access for remote camera configuration.
- Video view in combination with Video Security Client for Windows, Android and iOS.
 - Live viewing and local recording playback of multiple cameras, timeline, calendar search, PTZ control, export, forensic search for specific events: motion, line crossing, face-detection etc. on timeline and calendar with activity graph for results.
 - Geolocation maps for camera and moving object positions.
 - Intuitive PTZ control with touch and mobile position detection.
- Remote Alert: email notifications of technical camera issues.
- Counter Reports: browser-based application for users to access business reports such as Counter Reports.

Note the individual availability and service level provisions of Remote Portal for these functions.

In Alarm Management the following interfaces are available after deployment and respective license activation:

• Configuration

Browser-based interface for user management and configuration of alarm scenarios. Configuration settings include:

- Account management and mobile access.
- Remote configuration of camera settings (for example IVA, PTZ) and configuration of alarm events.
- Event-based recordings, schedules and action plans.

• Event Monitor

Browser-based application for operators that handle alarms at front desks, in security operation centers (SOC) or central monitoring stations (CMS). The Event Monitor can be used at mobile clients and is suitable for:

- Viewing, managing and processing triggered device or system alarms, events and trouble notifications.
- Access to live views or video cloud storage.
- Interaction with the scene and control of action plans for interventions.

• Site Monitor app

End-user application available for iOS and Android smartphones and tablets. Supports live viewing of video from authorized devices, push notifications (service **Smart Notification**) for subscribed events and arming/disarming for authorized sites.

• Workflow integration

The integration with alarm automation platforms via Cloud Alarm Transmitter is optional.

Integration with certified alarm handling is available for more than 15 vendors.

• Advanced Diagnosis (only available for dedicated cloud and users with Config Agent role)

- Audit Event Log database for cloud recordings: Gives access to alarm video clips and event-based recordings of the configured retention time to investigate incidents for the purpose of loss-prevention etc.
- Audit user actions: Provides audit trails of user actions, for example for quality assurance on alarm operator actions.
- Diagnosis: Provides statistical and summary information of various system parameters, for example alarm, device, site, account status and trouble reports.
- Alarm diagnosis: Provides a statistical overview on all sites during initial field-tests and maintenance to optimize the VCA camera settings. Reduces false-alarms together with the triggering Alarm Object Image and checks camera sensitivity at night time.
- Site status diagnosis for installers: Provides an installer dashboard about the status of the local video system in terms of recording, video and network quality etc.
- Device Inventory: Provides an overview of installed devices with firmware version.
- Cyber Hygiene Status: Provides an overview of device Firmware Management status including update history.

Functions

Alarm Management comes with a number of pre-defined functions. The included functions are:

- **Live Intervention**
Camera-generated events (detected motion, IVA, virtual and digital inputs and outputs) are pre-processed by the cloud application according to set filtering rules and optionally forwarded to remote monitoring centers/control monitoring stations for certified verification and intervention. A 10-second alarm clip for quick investigation, review and export is stored.
- **Virtual Guard**
Prompts the operator to perform visual checks of selected cameras at scheduled intervals.
- **Virtual Assistant**
Remotely prompts the operator for assistance by means of push-button or other devices connected to a camera.
- **Live View**
Select from your list of sites any location and cameras from the map for permanent video live monitoring either low-bandwidth high-priority streaming with full control (PTZ, Audio, Intercom, etc.) or secondary video display and for possibly needed Intervention actions (open doors, switch light, email notification of site owners etc.). The operator can manually adjust for image quality or frame rate. Integrated 3rd party systems may offer this site access under a static reusable URL.
- **Video Verification**
Video verification of intrusion events, for example from Bosch B-Series and G-Series panels with live and recorded video from associated camera.
- **Smart Notification/Alarm Notification**
Push Notification service in combination with the Site Monitor app from Bosch, notifying customers or security guards about relevant events from their sites. These events could be the same events received by the central station but could also be events where no professional intervention is required but the user wants to be informed about, for example warehouse access during business hours. The user can access the related event clips.

Available but not a function of Alarm Management:

- **Alarm Verification**
This function is similar to the Live Intervention function. It adds additional verification using a cloud-based Artificial Intelligence that is based on deep neural networks. These networks verify camera events for moving human or vehicle presence to reduce unwanted alarms. Refer to the respective Application note for more information.
- **Cloud Storage**
On top of real-time alarm handling, Alarm Management offers cloud storage functionality for continuous or event-based recording of Bosch

cameras and 3rd party cameras. Cloud storage is offered in different packages of retention and storage. For more details, refer to the respective Application note.

- **Alarm Transmission**

Integrates alarm scenarios with supported 3rd party alarm automation platforms.

User management

Alarm Management users are defined by roles and are assigned appropriate permissions according to their service task. This user management is independent from the Remote Portal user management. The available roles are:

- **Config Agent** (only available on dedicated cloud):
Access to all system components for system administration, configuration and diagnostics.
- **Alarm Agent** (operator):
Access limited to the Events list, for operation of applicable service, for example live image, time of alarm, reference image for alarm verification. This access can be limited to certain accounts, for example to support multiple enterprise customers with their own in-house control rooms with a single Alarm Management cloud application.
- **Integrator** (technician with configuration permissions):
Access to the system components of all accounts assigned to his installer company for the turn-key configuration and administration of all related services, sites, and cameras.
This access is limited to the accounts of the installer company.
- **User** (customer, site owner, security guard):
Access to live stream of customer site's cameras and change of arming state (on configured sites) via mobile device. Receives smart notifications via push messages, views Events list and accesses related event clips.

Configuration interface

Browser-based application providing following functions:

- Location: `<cloud application URL>/config`
- Access via dedicated Config Agent user ID and password.
- Management of customer and installer company accounts with name and logo. Customer accounts provide logical grouping of sites and access to control these sites.
- Remote commissioning of cloud enabled cameras (connected via Remote Portal).
- Management and configuration of sites with name, identifier and optional geodata. Geodata is used for map display of a site in a mobile application. Sites can be configured to be always armed, armed by camera input or manually from the Site Monitor app.

- Management and configuration of schedules in 15-minute increments in addition to the default *Day*, *Night*, and *Weekend* schedules. Date-based schedules for special days, for example holidays can be added. Schedules are defined per account and can be used across sites and services of an account.
- Management of actions: email (recipients and customized message content), camera ("relay on"/"relay off", move to pre-defined PTZ position, AUX command), play pre-recorded audio, push notifications (to compatible devices) and forward actions to the control center. Actions can be executed automatically or manually during alarm processing.
- Management of user credentials with first name, last name, email address and user role. New users receive an email with sign-in information upon creation or when requested manually by Config Agent to reset password.
- Customizing content of system generated email messages (for example for new users or password reset).
- Remote access to installed camera's configuration page, initial configuration for optimum operation with Alarm Management, save/load configuration per camera. Remote update of firmware (limits site access to camera with update in progress). Assignment of video channels to sites.
- Adding virtual inputs to a site. Update of virtual input token.
- Activating trouble forwarding to the control center (tamper and malfunction events, trouble message if the device cannot be accessed, trouble message for monitored functions such as recording).
- Setting current image as a reference image for camera.
- Retrieving device parameters, including MAC address, device type, firmware version, local IP address and device passwords.
- Enabling audio verification, audio intervention and configuring audio devices.
- Configuring Live Intervention and Virtual Guard services:
Live Intervention can be configured with triggering device, trigger event, schedule, action and video channel to be displayed and action to be performed manually in the event of an alarm. For Virtual Guard tours, a schedule and a camera selection can be configured.
- Configuring Smart Notification service:
The Smart Notification service can be configured with site, triggering device, trigger event, schedule, action and video channel and the user recipients list that will receive push notifications when triggered.

Event Monitor interface

Browser-based application that supports viewing and processing events during evaluation or troubleshooting. The application offers Alarm Management for selected customer accounts independent of workflow integration with 3rd party alarm automation systems:

- Location: `<cloud application URL>/eventmonitor`
- Access via user ID (with assigned role) and password or via browser certificates.
- Live Intervention:
Split-display of alarm, time and live images from selected cameras. Incident evidence image is displayed and replaced by a ten second video clip (centered on time of alarm) when upload from camera is completed. Offers event batching that logically groups an event that spans across cameras in the same site. This provides the operator with complete scene overview and holistic chain of evidence.
When activated, allows audio intervention to selected camera. View of reference images from all cameras of the site is available. Further site alarms can be manually snoozed for a variable time. Configured alarm intervention actions can be executed manually (trigger relay, move to pre-defined PTZ position).
- Virtual Guard:
Split-display shows live images from all cameras to be verified (highlighted in yellow) and reference images set for each camera. When available allows audio intervention to selected camera. View of reference images from all cameras of the site is available. Configured alarm intervention actions can be executed manually (trigger relay, move to pre-defined PTZ position).
- Live View via Site-list or integrated 3rd party systems may offer this site access under a static reusable URL.
- Virtual Assistant interface
- Trouble:
Split-display shows live images from the affected camera. Trouble event, time off, and whether trouble continues to persist are displayed; any other cameras with trouble status are highlighted as well. When available, allows audio intervention to the selected camera.
Summary trouble report is displayed. View of incident intervention image and reference images from all cameras of the site is available.
- Allows to view cameras or to perform site actions (snooze site, enable maintenance mode).
- Review of event-based recordings with site, time/date and event filter.

Diagnosis interface (only available for dedicated cloud)

Browser-based application, provides summary information of various system parameters, for example alarm, device status or site trouble reports.

- Location: `<cloud application URL>/diagnosis`
- Access via Config Agent user ID and password.
- Hardware Status menu: Helps ensure that all devices are up to date and stable for Alarm Management operations.
- Site Status menu: Supports analysis of site connectivity and activity.
- Operator Performance menu: Supports evaluation of operator performance in Alarm Management video events.
- Operator Capacity menu: Supports operator capacity planning to handle contracted services and alarm load.
- Alarm Rates menu: Supports smart adaptation of camera analytics to generated alarms and changing conditions over time.
- Service Operation documentation: Provides audit trail of every alarm operation.
- Customer Base menu: Supports analysis of customer and service sale evolution over time.
- Export menu: All table information can be exported to a XLS/CSV format.

Site Monitor app

The Site Monitor app provides the following functions:

- Site list map view.
- Thumbnail view of cameras per site.
- Live video stream.
- Selected device alarms received by push notification, directly connect to device.
- Access to all event clips through event list.
- Remote arming/disarming of site.
- Password-protected, SSL/TLS encrypted connection.
- Support of iOS and Android smart phone and tablet platforms.

Technical specifications

Device compatibility and settings

Bosch IP cameras with firmware version 6.40 or later connected to Remote Portal or supported 3rd party cameras. For more details on 3rd party camera compatibility, refer to the Alarm Management compatibility list.

It is recommended to adapt the initial camera configuration for the Alarm Management use-cases to ensure best performance.

Digital video recorders

In an Alarm Management system setup, the cameras will always directly connect to the application (as opposed to connecting through the digital video recorder) and record locally to SD-cards or any iSCSI medium such as direct iSCSI, Video Recording Manager or DIVAR IP:

- DIVAR IP 2000/DIVAR IP 6000
 - DIVAR IP 3000/DIVAR IP 7000
- However, cameras may record in parallel to the following local digital video recorders:
- Bosch Recording Station
 - 3rd party video management systems and network video recorders (non-Bosch iSCSI recording based)
 - DIVAR network and DIVAR hybrid (IP cameras only)

Network

Internet connection from connected devices to Remote Portal is required. No further network configuration (for example port forwarding) is required after connection to Remote Portal.

Bandwidth

- Minimum recommended upstream: 512 kbit/s
- Minimum recommended downstream: 512 kbit/s
- Mobile wireless network connections have less availability, influenced by parameters, such as the weather, number of network users etc. Therefore, Bosch recommends to use a mobile wireless network connection only if the application allows for a lower level of availability. The available bandwidth must be repeatedly determined and averaged using appropriate testing tools.

The unique Bosch Intelligent Digital Noise Reduction (IDNR) streaming technologies and long GOP rates make the Bosch Security Cloud platform the best choice for limited bandwidth connections such as 3G.

Minimum upstream for event-based recording: Upstream rate of each site needs to be higher than the average event and motion activity of all cameras respecting the selected video recording profile. Check whether the network parameters on-site support the system set-up. Contact your local Bosch representative to use the comprehensive trial options.

Browser

Compatibility of web applications has been tested with the latest version of Google Chrome. Bosch recommends the use of Chrome or Chromium-based browsers.

Integrations with alarm automation platforms (optional via Cloud Alarm Transmitter)

The Bosch integration team will set-up a dedicated mediator between your Alarm Management and your alarm automation platform. Alarm Management can be integrated with the below listed alarm automation platforms. This ensures seamless operation of Alarm Management functions within a legacy in-house Monitoring Control Center or certified Central Monitoring Station environments. For all integrations, the appropriate number of Cloud Alarm Transmitter licenses needs to be activated.

Events that are configured to be forwarded to the central monitoring station, will be displayed in the respective alarm automation platform's alarm stack similar to other signals. When an operator selects an alarm to be processed, or a site, Event Monitor is launched for quick and effective verification and intervention.

The following software is supported for Alarm Transmitter:

- Safecon - Alcensoft
- BOLD Technologies - Manitou
- AzurSoft - Horus alarm management system (AMS)
- Digital Monitoring Products (DMP) - Entré alarm software
- MasterMind - MasterMind
- Micro Key Solutions (MKS) - Millennium Monitoring
- Security Information & Management Systems, Inc. - SIMS
- DICE - Matrix monitoring software
- Secure Global Solutions (SGS) - stagesTM
- ESI – European Systems Integration - V1
- Monitor Computer Systems Ltd. - Sentinel
- Monitor Soft - Sentinel
- Sureview - Immix
- Suretek
- Netcom
- Any SIA DC09 compatible Alarm Receiver software
- and others (refer to the compatibility document)

Camera feature support

The operator can remotely control/use the following features and key technologies of Bosch cameras during alarm operation via the operator interface:

- Live video streaming with metadata overlay
- Alarm clip/snapshots with Alarm Synopsis/event-based clips
- Audio in/out
- Digital and virtual in- and output(s)

The following features of Bosch cameras are also supported:

- Motion detection (IVA/EVA/MOTION+)

- Camera event buffering for network disconnections and replenishment of alarms and clips
- PTZ control, prepositions and commands
- Tamper detection

For more information on 3rd party camera support, refer to the Alarm Management compatibility list.

Site Monitor app

- iOS version for iPhone/iPad: iOS 10 or later
- OS version for Android phones and tablets: OS 5.0 or later.

Note: The app is not intended to permanently access cameras and is not a self-monitoring tool. For these cases, use the Video Security Client (Windows, iOS, Android).

- Camera performance and bandwidth is shared between all accessing apps. With too many parallel connections image transmission may fail or get cancelled.

Cloud Storage

Alarm Management functions with video alarm recordings include a 30-day retention of 10-second alarm clips by default. On top of this, further Cloud Storage packages can be added to offer continuous or event-based recording independent from Alarm Management scenarios.

To avoid bandwidth issues with included alarm clip storage, it is recommended to actively lower false alarms by proper VCA configurations. For example with the help of the Alarm diagnosis tool in Alarm Management or masking disturbances such as moving lights, foliage, objects, etc. in the camera configuration.

Availability

The multi-tenant Alarm Management platform and its functions are offered as a managed, cloud-based service licensed via Remote Portal.

Such services provided via Remote Portal that are subject to charges are provided with an availability in Bosch' area of responsibility according to the availability indicated in the Terms and Conditions of Remote Portal services.

For more information, refer to the Terms and Conditions on <https://remote.boschsecurity.com>.

For Alarm Management, an empirical availability of above 99% throughout the year is measured. A dedicated operations team is monitoring all cloud applications 24/7 and is minimizing any service interruption based on automated uptime monitoring. For dedicated cloud systems, Bosch offers a Service Level Agreement (SLA) with availability, response and resolution guarantees as well as 24/7 emergency hotlines. To receive an Alarm Management Service Level Agreement (SLA), contact your local Bosch representative.

For non-critical support cases Bosch offers dedicated support access for the functions of Alarm Management. Requests for support may be submitted at any time via email to support.security-cloud@bosch.com. Here, Bosch will process and provide support during regular business hours. 24/7 access to support outside of business hours with guaranteed response, workaround and resolution times is offered within the Service Level Agreement for dedicated Cloud systems. Contact your local Bosch representative for more information.

Supported operator user interface languages

- English
- German
- Dutch
- Italian
- Portuguese
- Spanish
- Swedish
- Danish
- French

Ordering information

CBS-CLOUD-ENT VSaaS Enterprise Cloud Instance, 1yr

Set-up of a dedicated Alarm Management system. Alarm forwarding optional.

Order number **CBS-CLOUD-ENT**

CBS-ALMGT-CAM Alarm management for 1 camera, 1yr

License to use Alarm Management functions for 1 camera for 1 year. Account available upon request. Alarm forwarding optional.

Order number **CBS-ALMGT-CAM**

CBS-ALMGT-CAT Alarm transmitter for ALMGT 1 cam, 1yr

License to connect 1 camera with activated Alarm Management to external alarm automation platforms.

Order number **CBS-ALMGT-CAT**

CBS-ALMGT-NOTI1 Alarm notification for 1 camera, 1yr

License for 1 camera to receive camera VCA events on a mobile device with the Bosch Site Monitor app.

Order number **CBS-ALMGT-NOTI1**

CBS-REC-MINI Cloud Storage, 50GB/month/cam, 1yr

License to activate continuous or event-based cloud storage for 1 camera for 1 year, with 50 GB monthly storage.

Order number **CBS-REC-MINI**

CBS-REC-LITE Cloud Storage, 125GB/month/cam, 1y

License to activate continuous or event-based cloud storage for 1 camera for 1 year, with 125 GB monthly storage.

Order number **CBS-REC-LITE**

CBS-REC-PLUS Cloud Storage, 250GB/month/cam, 1y

License to activate continuous or event-based cloud storage for 1 camera for 1 year, with 250 GB monthly storage.

Order number **CBS-REC-PLUS**

CBS-REC-PRO Cloud Storage, 500GB/month/cam, 1y

License to activate continuous or event-based cloud storage for 1 camera for 1 year, with 500 GB monthly storage.

Order number **CBS-REC-PRO**

CBS-REC-ENT Cloud Storage, 1TB/month/cam, 1y

License to activate continuous or event-based cloud storage for 1 camera for 1 year, with 1 TB monthly storage.

Order number **CBS-REC-ENT**

Services

CBS-ALMGT-CUST Custom setup for alarm management

Bosch customer service for special deployments or adaptations of the dedicated Alarm Management system. Contact your local sales representative.

Order number **CBS-ALMGT-CUST**

CBS-ALMGT-CATX Custom setup for alarm transmitter

Bosch customer service for special integration of protocols or adaptations to Alarm Transmitter (CBS-ALMGT-CAT). Contact your local sales representative.

Order number **CBS-ALMGT-CATX**

CBS-PORTAL-TOFF On-site training day for ALMGT EBR

Bosch training on Remote Portal, Alarm Management and Alarm Transmission, at customer site. Contact your local sales representative.

Order number **CBS-PORTAL-TOFF**

CBS-PORTAL-TON Online training session ALMGT EBR

Bosch training on Remote Portal, Alarm Management and Alarm Transmission, online. Contact your local sales representative.

Order number **CBS-PORTAL-TON**

CBS-MOBILE Video Security Cloud Service 1yr

License to enable VideoView+ services for one camera for a 1-year period.

Order number **CBS-MOBILE**

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