BOSCH

Invented for life

BVMS - System design guide

Author: Wrobel Maciej (BT-VS/MKR-SEP)

Date: 26 March, 2021

1 Document information

Project	BVMS 10.1.1
Reference	n/a

1.1 Version history

Date	Version	Changes
2020-01-02	BVMS 10.0	Extended and improved VSG performance description.
2020-02-18	BVMS 10.0.1	Updated according to BVMS 10.0.1 specification.
2020-08-19	BVMS 10.1	Updated according to BVMS 10.1 specification.
2020-09-17	BVMS 10.1	Added "script" comment to monitor group sequences on alarm, described impact on VSG performance when running in virtual machine and encrypted recording is turned on.
2020-10-14	BVMS 10.1	DIVAR IP All-in-one can be expanded with MBV-XSITE-xx and MBV-XSUB-xx. Adjusted description.
2021-02-24	BVMS 10.1.1	Information valid for BVMS 10.1 also relevant to BVMS 10.1.1.

2 Introduction

This document summarizes the BVMS design details, and serves as a guide to planning a BVMS system with Bosch cameras and storage. It focuses on BVMS combined with the VRM. The BVMS 10.1 release notes can be found on the Bosch Security Systems website. This document lists the valid design specifications for **BVMS 10.1.1**.

Warning

This document is subject to change. Once a new version is published, earlier versions are void.

3 System Components

Component	Description
(Enterprise) Management Server	The Management Server software provides management, monitoring, and control of the entire system. One single Management Server manages up to 2000 Cameras/encoders. Enterprise Management Server serves as an address book, and allows one Operator Client to access to multiple Management Servers.
Video Recording Manager	Video Recording Manager (VRM) provides recording and playback management of video, audio, and data. One single VRM manages up to 2000 cameras/ encoders (including up to 2000 ONVIF cameras). Bosch Video Recording Manager (VRM) provides a Distributed Network Video Recorder solution, eliminating the need for dedicated NVRs. VRM provides load balancing and failover for the iSCSI Storage System and makes it easy to add additional iSCSI Storage Systems later on. VRM introduces the concept of a storage virtualization layer. This abstraction layer enables VRM to manage all of the individual disk arrays in the entire system as various "virtual" pools of storage, which are intelligently allocated as needed. A storage pool is a container for one or more iSCSI storage systems that share the same load balancing properties. Dual / failover recording: • A Primary VRM manages the normal recording of the cameras of your system. You use a Secondary VRM to achieve dual recording of your cameras. Dual recording allows you to record video data from the same camera to different locations. A Secondary VRM can manage the secondary recording for multiple Primary VRMs. • A Failover VRM is used for continuing the recording of a failed Primary VRM or a failed Secondary VRM computer.
Configuration client	Configuration Client software provides the straight forward user interface for system configuration and management.
Operator client	Operator Client software provides the ergonomic and intuitive user interface for system monitoring and operation.
Configuration wizard	Configuration Wizard software provides easy and fast setup of a small recording system when using the BVMS Appliance.
Appliances	DIVAR IP devices are simple and reliable all-in-one recording, viewing, and management solution for network surveillance systems.
Mobile Video Service	Mobile Video Service provides a transcoding service. It transcodes the live and recorded video stream from a configured camera according to the available network bandwidth. This service enables video clients to view high-quality images via low bandwidth. The Web Client: Access live and playback video from remote in single or quad-view. Search for text data and trigger export of videos on Management Server.
Mobile applications	Mobile App (iPhone or iPad): Access live and playback video from remote in single or quad-view. Alert and share live video from mobile camera with other security staff with a single click. The app is available in the Apple appstore and can be found by searching for "Mobile Video Security".

Component	Description
Video Streaming Gateway	Bosch Video Streaming Gateway (VSG) is a separate that runs independently VSG acts as an iSCSI NVR for non iSCSI capable devices, for example ONVIF devices, JPEG, RTSP, and legacy H.263 Bosch devices.

4 Recommended hardware

The recommended hardware for the Operator Client, VRM and server components (Management Server, VSG and MVS) can be found on the different (BVMS Professional, Plus and Lite) datasheets. The recommended hardware is fine-tuned to the maximum system size.

The server components of the BVMS can be virtualized. More information on virtualization can be found in the Virtualization - A concept explained document.

DSA E-series as storage for VMware

It is not recommended to use the DSA E-series as a storage device within a VMware environment. The DSA E-series can be used to store video data when BVMS is virtualized.

4.1 Cameras

All Bosch cameras can be used under the device compatibility concept, which is described in the article "How-to: BVMS - Device compatibility" on the Bosch Security & Safety community. The list of tested ONVIF cameras can be found on the Bosch Security Systems website.

4.2 Network

The BVMS Network Design Guide (which can be found on the Bosch Security System Community) describes general recommendations related to the network.

To achieve the performance listed in the table below, an 1 Gigabit/s network is a minimum requirement between the Operator Client and Management Server.

(**Unicast**) Maximum number of workstations simultaneously viewing the same camera	5
(**Multicast**) Maximum number of workstations simultaneously viewing the same camera	100
Event response time (assuming sufficient network performance considering bandwidth and delay)	< 1 second
Alarm visibility time (assuming sufficient network performance considering bandwidth and delay), including 1 live image pane, 1 instant playback image page, and 1 map image pane.	< 2 seconds

When the system does not have enough network resources, or is experiencing a temporary decrease in network performance, the event response time and alarm visibility time may increase.

The list of communication channels and required network ports can be found in the configuration manual of the BVMS.

5 Operating Systems

BVMS is designed to run on the Microsoft Windows operating system. This section lists the tested BVMS operating system versions and the expected end-of-service dates from Microsoft.

5.1 Supported operating systems

The overview below relates Windows version to specific BVMS releases. We distinguish two levels of compatibility:

1. The tested operating systems (also listed on the datasheets. These versions are tested extensively).
2. The compatible operating systems are tested for selected use-cases and we are confident they are usable in production environments.

If you run into an issue on a compatible operating system, our after sales support teams will investigate this issue to determine the root-cause. It might be recommended to upgrade your Windows version if we determine the root-cause is related to this. For Windows Server based operating systems, we always recommend to use the tested versions.

Windows Version	Tested BVMS versions	Compatible BVMS versions
Windows Client editions		
Windows 10 Professional (64-bit) April 2020 update (2004)	10.1.1, 10.1	10.0.2, 10.0.1, 10.0
Windows 10 Professional (64-bit) November 2019 update (1909)	10.1.1, 10.1, 10.0.2, 10.0.1	10.0
Windows 10 Professional (64-bit) May 2019 update (1903)	10.0.2, 10.0.1, 10.0	10.1.1, 10.1
Windows 10 Professional (64-bit) October 2018 update (1809)	10.0.2, 10.0.1, 10.0	10.1.1, 10.1
Windows 10 Enterprise (64-bit) LTSC build 1809	10.1.1, 10.1, 10.0.2, 10.0.1, 10.0	9.0
Windows 10 Professional (64-bit) Spring Creators update (1803)	9.0	10.0
Windows 10 Professional (64-bit) Fall Creators update (1709)	9.0	
Windows 10 64-bit creators update (1703)	n/a	9.0, 8.0
Windows 10 64-bit anniversary update (1607)	8.0, 7.5, 7.0	
Windows 10 Enterprise (64-bit) LTSB 2016 (1607)	8.0, 7.5, 7.0	
Windows 8.1 64-bit	8.0, 7.5, 7.0	
Windows 7 SP1 64-bit		7.0, 7.5, 8.0
Windows Server editions		
Windows (Storage) Server 2019 (64-bit)	10.1.1, 10.1, 10.0.2, 10.0.1, 10.0	
Windows (Storage) Server 2016 (64-bit)	10.1.1, 10.1, 10.0.2, 10.0.1, 10.0, 9.0, 8.0	

Windows (Storage) Server 2012 R2 (64-bit)	10.1.1, 10.1, 10.0.2, 10.0.1, 10.0, 9.0, 8.0, 7.5, 7.0	
Windows Server 2008 R2 SP1 64-bit	8.0, 7.5, 7.0	

5.2 Microsoft support policies

5.2.1 Microsoft life-cycle policy

Mainstream support: security updates/patches as well as non-security updates/patches.

Extended support: only security updates.

Existing Windows Life Cycle	Life-cycle start	Mainstream support	Extended support
Windows 10 Enterprise 2019 LTSC build 1809	2018-10-02	2023-10-10	2028-10-10
Windows 10 Enterprise 2016 LTSB build 1607	2016-08-02	2021-10-12	2026-10-13
Windows 10 Enterprise 2015 LTSB build 1507	2015-07-29	2020-10-14	2025-10-14
Windows 8.1 Enterprise	2013-11-13	2018-01-09	2023-01-10
Windows Server 2008 R2 Standard (SP1)	2011-02-22	2015-01-13	2020-01-14
Windows Server 2012 R2 Standard	2013-11-25	2018-10-09	2023-10-10
Windows Server 2016 Standard	2016-10-15	2022-11-01	2027-11-01

Source: Search product lifecycle and Microsoft Business, Developer and Desktop Operating systems policy

5.2.2 Windows as a Service (WaaS)

Using Windows as a Service (Windows 10) requires an organization to **update their systems on a regular basis**. Bosch might require the organization to update the system to the latest available version in order to use support.

Windows as a service	Life-cycle start	Home, Pro EOS	Enterprise, Education EOS
Windows 10 version 2004	2020-05-27	2021-12-14	2021-12-14
Windows 10 version 1909 "November 2019 update"	2019-10-12	2021-05-11	2022-05-10
Windows 10 version 1903 "May 2019 update"	2019-05-21	2020-12-08	2020-12-08
Windows 10 version 1809 "October 2018 update"	2018-10-02	2020-11-10	2021-04-13

Windows as a service	Life-cycle start	Home, Pro EOS	Enterprise, Education EOS
Windows 10 version 1803 "Spring creators update"	2018-04-30	2019-10-12*	2020-11-10
Windows 10 version 1709 “Fall creators update”	2017-10-17	2019-03-01*	2020-10-13
Windows 10 version 1703 “Creators update”	2017-04-05	2018-09-01*	2019-10-08
Windows 10 version 1607 “Anniversary update”	2016-08-02	2018-03-01	2019-04-09
Windows 10 version 1511 “Threshold 2”	2015-11-01	2017-10-10	2017-05-09
Windows 10 version 1507	2015-07-29	2017-05-09	n/a

Sources: Quick guide to Windows as a Service, Overview of Windows as a Service, Windows lifecycle fact sheet and Windows 10 update history

6 Management Server

Subject	Management Server (MS)	Enterprise Management System (EMS)
Management Servers	1	100 management servers * 100 cameras (maximum amount of servers) 50 management servers * 200 cameras (example) 10 management servers * 1000 cameras (maximum number of cameras per server in Enterprise scenario)
Total number of IP devices	2.000 per management server;	n/a
Total number of items in the logical tree per (enterprise) user group	10.000	10.000
Enterprise User Groups	n.a.	20 with overall max. 1000 users
User Groups	20 with overall max 1000 users	20 with overall max. 1000 users
Workstations connected in parallel	100	100 (per management server)
Logbook	4GB (6 Million Entries)	4GB (6 Million Entries) per server
VRM	125 VRMs (primary VRMs + Secondary VRMs).	In theory: 50x125 is possible, but total number of devices in logical tree shall not exceed 10.000
DiBos / BRS	100	100 MS with 100 each = 10.000 (10.000 devices in the logical tree of an operator user group)
Tattile (LPR) camera	50	100 MS with 50 each = 5.000 (10.000 devices in the logical tree of an operator user group)

Subject	Management Server (MS)	Enterprise Management System (EMS)
DVR (400, 600, 700, AN, Hybrid, Network)	50	100 MS with 50 each = 5.000 (10.000 devices in the logical tree of an operator user group)
POS/ATM	15	100 MS with 15 each = 1.500(10.000 devices in the logical tree of an operator user group)
Tattile LPR cameras	50	Limits apply to each MS
Virtual Inputs	4.000 (limited in configuration)	(10.000 items in the logical tree of an operator user group)
Adam modules	50	100 MS with 50 each = 5.000 (10.000 items in the logical tree of an operator user group)
Task schedules	200 (limited in configuration)	Limits apply to each MS
Recording schedules	10	Limits apply to each MS
Compound Events	1000, up to 10 devices per compound event	Limits apply to each MS
Max. number of sustained events	• 1000 events/s with Logbook • 2500 events/s without Logbook • 5000 events/s at peaks (within 60 minutes) with Logbook	Limits apply to each MS
Max. number of alarms	100 alarms/s on MS and on 10 alarms/s in alarm list of Client. Up to 1000 unprocessed alarms per MS.	Limits apply to each MS
Alarm priorities	100	Limits apply to each MS
Special Days	24	Limits apply to each MS
Allegiant CCL commands	Max 10/sec	Limits apply to each MS

Subject	Management Server (MS)	Enterprise Management System (EMS)
Allegiant systems	1 per management server. When using the Allegiant master/slave concept there is no limit defined.	100 MS with 1 each = 100
BIS-BVMS Connection	1 OPC Server per MS	No Enterprise functionality. Only 1 OPC Server per MS.

7 Scalability

7.1 BVMS Subsystems (previously known as Enterprise)

7.1.1 Licensing

BVMS Plus, BVMS Professional, and DIVAR IP All-in-one 7000 can act as a BVMS Enterprise server and be expanded with subsystems. This expands the previously known Enterprise functionality to BVMS Plus, Professional, and DIVAR IP All-in-one 7000 as well. Each workstation which is connected to the Enterprise management server should be licensed as MBV-XWST-xx, where xx is the BVMS version. Workstation licenses are not relevant for subsystems that are connected to an Enterprise management server. The workstation licenses are relevant when workstations are directly connected to the subsystem.

7.1.2 Special considerations

Topic	Remark
Monitor wall	Operator Clients with the permissions to access subsystems in an Enterprise Management System are able to display cameras from various Management Servers on a monitor group.
Building Integration System	The BIS can only monitor multiple BVMS management servers when it's directly connected to that specific management server. The Enterprise management server is not exposed with an OPC server. One BIS server can connect to multiple BVMS Management Servers to monitor states. Enterprise Operator Client can be controlled by BIS by mapping the BVMS virtual inputs on the specific management server(s) to BIS events.

7.2 BVMS Unmanaged sites

7.2.1 Licensing

For each site, the MBV-XSITE-xx license is required. The DIVAR IP 3000/7000 cannot be expanded with MBV-XSITE-xx. DIVAR IP All-in-one 7000 can be expanded with MBV-XSITE-xx and therefore act as an unmanaged site server. Devices inside the subsite do not need to be licenses in the main site, but (depending on the device) need to be licensed within the sub-site.

Device	Per license in one site
Cameras	16
DIVAR	5
DIVAR IP	1
BVMS	1

7.2.2 Specification

Specification	Limit
Number of sites	10.000
Devices per site (DVR, DIVAR Network, DIVAR Hybrid, DIVAR AN)	5
Devices per site (DIVAR IP, BVMS Professional)	1
Minimum BVMS version subsystem (without SSH)	5.5
Minimum BVMS version subsystem (with SSH)	7.5
Maximum simultaneous connections to sub-sites	20
Total number of simultaneous connected devices in the sub-sites	9999
Functionality	Live, playback, PTZ
Bookmarks	Yes
Favourites	Yes, taking the 20 simultaneous connections into consideration.
State monitoring	States of the devices in the sub-site are not monitored.

7.2.3 Devices

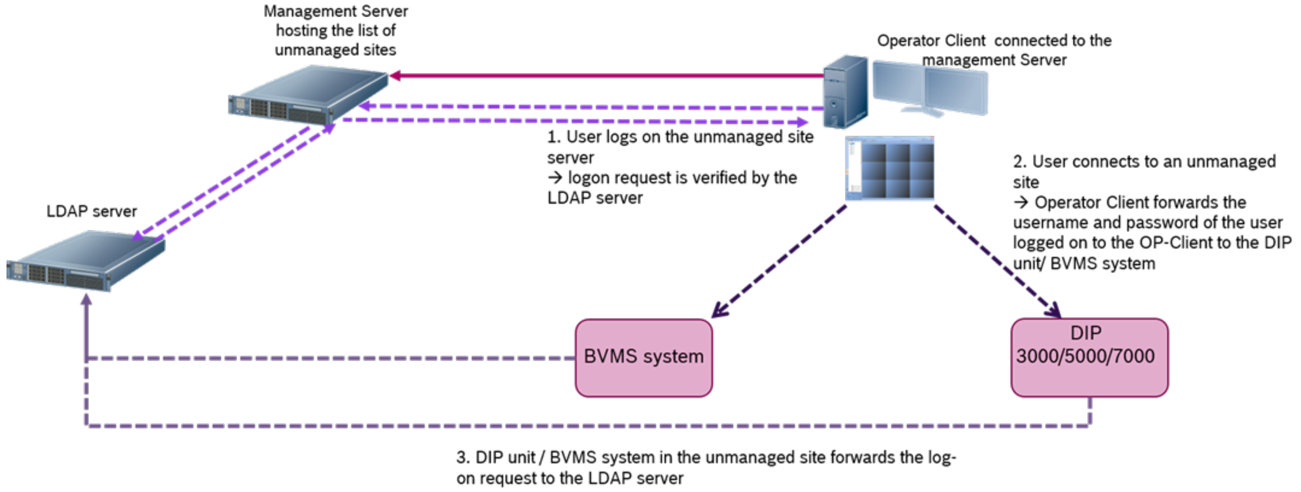
Device	Implemented
DVR 400 / 600/ 700 / 3000 / 5000	YES
DIVAR Hybrid / Network	YES
DIVAR IP 3000 / 7000 (BVMS 5.5 or higher)	YES
BVMS Management Server (BVMS 5.5 or higher)	YES
DiBOS	NO
Bosch Recording Station (BRS)	NO

7.2.4 Special considerations

Topic	Remark
Panoramic dewarping	When BVMS 6.0 or earlier is acting as a sub-site, only a fish-eye is shown when a panoramic camera is displayed.

Topic	Remark
Workstation licenses	When connecting to a BVMS 6.5 system, no workstation license is consumed, but wen connecting to former BVMS system (6.0, 5.5.5 or 5.5) via unmanaged site concept, one workstation license has to be available and not in use.
Resilience	Only recording from primary VRM can be replayed (no secondary VRM or Failover VRM footage can be replayed).
Logging	No user actions (like deleting or protecting video data on network devices of unmanaged sites) are logged in the unmanaged site system nor in the unmanaged site server.
PTZ pre-positions	Preposition names of PTZ cameras are not shown, but calling up a preposition via default number is possible.
PTZ aux commands	AUX commands of PTZ cameras are **not** supported. Work-around: make the AUX command part of a PTZ pre-position.
PTZ permissions	Dome permissions are ignored.
PTZ analogue	Only IP domes can be operated. Domes connected via serial port (via encoder) may appear as a dome camera but cannot use the PTZ functionality.
Region of Interest	Region of interest (ROI) is not implemented.
Audio	Audio will not be forwarded (live and replay) from the sub-site.
Operating permissions	The following device permissions from the Tab "Camera Permissions" will be applied to the remote client: device access, live video, playback video, text data, export, PTZ, PTZs presets, reference image.
Operating permissions	The following device permissions from the Tab "Camera Permissions" will **not** be applied to the remote client: live audio, manual recording, playback audio, aux.
Transcoding	Hardware transcoding can be used. Software transcoding cannot be used.
User management	When the feature “Allow multiple logon with the same user” is disabled in the unmanaged site system, then this particular user has to be available for Operator Clients to the system via unmanaged site concept. Local BVMS Operator Client shall use OTHER users to ensure the connection remains available for other Operator Clients connecting to the system via unmanaged site.
Logbook	The logbook in the sub-site cannot be accessed.

Topic	Remark
LDAP	It is not recommend to mix users in the local user configuration and in the LDAP server. This means a user should be either configured locally on the device or in the LDAP server. Setting up the user twice, locally in the BVMS configuration and in the LDAP server is not recommended. In this case we cannot make sure, that if the BVMS system in the site cannot connect to the LDAP server, that the user login request is denied.


Management Server hosting the list of unmanaged sites
Operator Client connected to the management Server
1. User logs on the unmanaged site server
→ logon request is verified by the LDAP server
2. User connects to an unmanaged site
→ Operator Client forwards the username and password of the user logged on to the OP-Client to the DIP unit/ BVMS system
LDAP server
BVMS system
DIP 3000/5000/7000
3. DIP unit / BVMS system in the unmanaged site forwards the log-on request to the LDAP server

7.2.5 BVMS Unmanaged sites on Microsoft Azure

If the BVMS Management Server does not have locally connected cameras it serves as an address book for the Operator Clients. In this case, the Management Server can run on Microsoft Azure. We recommend to tailor the performance of the Azure virtual machine to match your expected performance and use SSH to login to the Management Server.

7.3 Enterprise versus Unmanaged sites

Consider this table for the design decision to go for unmanaged site concept on a Professional License or for a “Managed Solution” => Enterprise license with subsystems.

A subsystem is equal to a site.

	Single Management Server	**Single Management Server with unmanaged sites**	**Enterprise Management System**
Max# of managed devices	2000	2000	200.000

Max# of devices in one Operator Client	2000	10.000	10.000
Optimized for large (>100 cameras) subsystems	n/a	no	yes
Optimized for small (<100 cameras) subsystems	n/a	yes	no
Max# of large(small) subsystems	n/a	0	10 (100)
Max# of subsystems	n/a	9999	100
Max# of parallel connected subsystems in one Operator Client	n/a	20	10 (100)
Max# of connected system with unmanaged devices	0	9999	0

8 Software security

The software security concept is explained in the BVMS - Securing a Security System document, which can be found on the Bosch Security Systems Community.

9 Operator Client

Subject	Operator Client Limit
Number of devices in the logical tree	10.000
Simultaneous connections to logbook	1
Maximum number of open maps	20
Total number of hotspots opened (using one or several maps)	10.000, up to 4.000 hotspots per map.
Alarms per second in alarm list	10
Simultaneous camera connections	Depends on workstation performance.
Export	Native; MOV, MP4, maximum 4 cameras in parallel.
Application architecture	64 bit
Decoding	GPU (Nvidia, Intel) first, CPU second. CPU decoding is used by default for streams smaller than 1080p. CPU decoding is used for playback.
Replay speed < 4x	True-to-image: every frame is shown.
Replay speed > 2x	i-frame only: only i-frames are shown. Some i-frames might be dropped at higher speeds. Display speed will depend on system (network, workstation, storage) performance.

9.1 Compatibility

When an operator client is connected to an older version (then itself) of the (Enterprise) Management Server, it will run in **compatibility mode**.

1. An operator client cannot connect to a newer (Enterprise) Management Server: the Operator Client needs be of a higher version than the (Enterprise) Management Server.
2. The compatibility in an Enterprise system is determined by the version of the Management Server of the Subsystem and the Operator Client.

In production systems it is not recommended to use versions which are released more than two years apart.

Client	Server	Functionality
10.1.1, 10.1	10.0.2, 10.0.1, 10.0	Live and playback; favourites and bookmarks; permissions; pan-tilt-zoom; address book; relay control; device states; logbook (no event filtering); notification on configuration changes; changing an operator's password; alarms, assigning cameras to monitor groups.

Client	Server	Functionality
10.1.1, 10.1, 10.0.2, 10.0.1	10.0	Live and playback; favourites and bookmarks; permissions; pan-tilt-zoom; address book; relay control; device states; logbook (no event filtering); notification on configuration changes; changing an operator's password; alarms, **assigning cameras to monitor groups.**
10.1.1, 10.1, 10.0.2, 10.0.1, 10.0	9.0	Live and playback; favourites and bookmarks; permissions; pan-tilt-zoom; address book; relay control; device states; logbook (no event filtering); notification on configuration changes; **changing an operator's password**; **alarms**.
10.1.1 <= 5.5.5	8.0 <= 5.5.5	Live and playback; favourites and bookmarks; permissions; pan-tilt-zoom; address book; relay control; device states; logbook (no event filtering); notification on configuration changes.

The CameoSDK acts as a Client to the server, and benefits from the same compatibility as the Operator Client. It is important the CameoSDK is updated with every release, as this allows it to connect to older as well as the latest BVMS versions.

10 Mobile Video Service

The web client requires a Mobile Video Service (available with the BVMS setup).

Specification	Details
Mobile Video Service(s) per BVMS management server	5
Maximum number of connections per Mobile Video Service (**Each mobile device consumes 1 connection, each stream consumes another connection**)	20
Codec (H265 is not implemented)	H264
GOP (B-frames are not implemented)	IP

11 Maps

11.1 Performance

The speed at which a map is opened is depending on the amount of objects that is placed on a map and the size of the map file.

Hotspots on map	Time to open (seconds)
50	0.5s
500	1s
1000	2s
2000	3s
3000	5s
4000	6s

The amount of maps that can be opened simultaneously is also depending on the amount of objects that are placed on a map.

11.2 File recommendations

For DWF: Only use layers containing the building structure and remove all unnecessary layers (for example, electronic, water, and others) as they increase the file size of the file, and therefore the loading time. 3D and multimaps cannot be used. It is recommended to use DWF files with version 5 or higher.

Type	Size
DWF	1MB
PDF	1MB
PNG,JPG	4MB

12 SSH Service

For remote security connectivity the built-in SSH service can be used. Due to the increased overhead it is not recommended to use the SSH service's functionality in a local network:

- Multicast is not used, which means each client will set-up a dedicated unicast connection to the camera. This limits the number of simultaneous clients connecting to one camera considerably.
- Direct iSCSI replay is not possible, the system will fallback on VRM replay.
- Each camera connection through the SSH service is handled by using a separate (CPU) thread, which could (when hundreds of cameras are opened in several connected clients) overload the management server.

12.1 Performance

The number of cameras is depending on the bandwidth generated per cameras.

Subject	Performance
Clients	5
Bandwidth (per client)	10Mbit/s
Bandwidth (total)	50Mbit/s

13 Monitor Groups

Specification	BVMS Professional	BVMS Enterprise
Decoders	128	128
Keyboards per decoder	1	1
Monitor Groups	50 per management server, 20 per operator client	20 per operator client

13.1 Licensing

Each decoder requires a channel license per connected monitor: if a VIDEOJET 7000 and VIDEOJET 8000 have 2 connected monitors, 2 channel licenses are required.

13.2 Monitor wall versus (Analog) Monitor Groups

From BVMS 10.0.1 onwards panoramic pre-positions can be assigned to the monitor group in alarm scenarios. Panoramic pre-positions cannot be assigned manually to the monitor group.

Functionality	AMG	DMW	Monitor Groups (MG)
Usage in local Operator Client	YES	YES	YES
Usage in Enterprise Operator Client	NO	YES	YES
Assign via drag&drop (logical tree) in Operator Client	YES	YES	YES
Assigned via drag&drop (map) in Operator Client	YES	NO	YES
Control by workstation keyboard including PTZ (Intuikey)	YES	NO	YES
Control by decoder/server keyboard including PTZ (Intuikey)	YES	NO	YES
Control by SDK	YES	NO	YES
Display camera on alarms	YES	NO	YES
Display sequences (manually)	YES	YES	YES
Display sequences (on alarm)	YES	NO	SCRIPT

Functionality	AMG	DMW	Monitor Groups (MG)
Display sequences (manually, Enterprise)	NO	YES	NO
Display sequences (on alarm, Enterprise)	NO	NO	SCRIPT
Support special layouts	NO	YES	YES
ONVIF cameras (via VSG)	YES	YES	YES
Allegiant cameras	YES	NO	NO
IVA Overlay	NO	YES	YES
Snapshot in Operator Client	NO	YES	YES
Dewarping	NO	NO	PARTIAL
Replay	NO	NO	NO
Maps	NO	NO	NO

13.3 Special considerations

Topic	Remark
ONVIF	Live-only cameras cannot be assigned to a decoder, this is only possible for VSG configured cameras.
Sequence	Sequence supports a max. of 100 steps and max. 25 cameras per step
Sequence	When using the DMW: sequences are controlled from the Operator Client. If the Operator Client is stopped, the sequence will also stop.
Sequence	Prepositions of a pre-configured sequence will only be activated when an MG is used.
Allegiant	Cameras can only be assigned to a decoder when trunklines are configured.

Topic	Remark
DVRs	DiBos, BRS and DVRs are integrated into BVMS as transceivers. This means, both live and playback video is streamed through DiBos/BRS/DVR. Therefore it is not possible to show an DiBos/BRS/DVR image on a decoder.

13.4 Security configuration

While we are working on improving the security configuration, the following settings are tested related to the usage of decoders.

Decoder	VSG	VSG Stream Encryption	ONVIF Encoder
Unsecure	Unsecure	Off	Unsecure
Secure	Secure	On	Secure

13.5 Non-Bosch Monitor walls

13.5.1 Barco Transform N-series

Barco developed a RCP+ SDK Agent to integrate the BARCO Transform N series for BVMS 5.0 or higher.

TransForm N Universal Streaming Video Input Node

- Barco RCP+ SDK Agent requires activation of multicast in all used cameras
- The Barco RCP+ SDK Agent should be added to the BVMS configuration as "Automatic" detected device.
- The Barco RCP+ SDK Agent does not work in a system with secured connections.
- It does **not** support multiple drag and drop support (sequences).
- It does **not** support replay.
- The RCP+ Agent requires a license from BARCO.
    - In BVMS the RCP+ Agent is connected as a single decoder supporting up to 64 cameras.
    - In BVMS the monitor wall is licensed with a single channel license (MBV-XCHAN-xx) per RCP+ Agent.
- The RCP+ Agent supports asymmetrical layouts.

14 ONVIF

Topic	Remark
Configuration	ONVIF cameras can be added to a BVMS system by using a network scan.
Configuration	Basic configuration of the most important settings of an ONVIF camera is supported from within BVMS, when implemented the by camera manufacturer.
PTZ	ONVIF compliant PTZ cameras can be controlled and PTZ presets can be enabled.
Export	Footage recorded by the Video Streaming Gateway can be exported to the available export formates (MOV, MP4, and Bosch native)
Streaming	If an ONVIF camera provides a second stream, this can be selected for live view
Events	Events of the ONVIF cameras (including camera state, inputs, relays and IVA) can be received and processed by the BVMS. ONVIF events can be browsed and mapped to the current BVMS events used for Bosch IP cameras to e.g. trigger alarm recording. The event mapping can be applied for other cameras of the same type or be exported in order to be used with other BVMS systems
Audio	Audio can be recorded and replayed. Push-to-talk is not implemented.

Note

Please note, that ONVIF events (based on HTTP/SOAP) need a much higher processing power than events from Bosch cameras (RCP+ based).

14.1 List of tested ONVIF cameras

The latest list of tested ONVIF cameras can be found on https://community.boschsecurity.com

14.2 Performance

Some manufacturers do not provide a de-bounce time, leading to events occurring in high frequency. Therefore, please ensure that the total event load in the system does not exceed **500 events/second**. To ensure this:

- Check, whether the created event mapping is unintentionally deployed to all cameras of the same type
- Note that mapping one ONVIF event does subscribe to all events in the camera
- Therefore we recommend to connect the camera with busiest scene to the ONVIF Device Manager to get an estimate of the occurring number events/second as a basis to calculate the overall event load
- Remove unused ONVIF events from the event mapping table. For supported manufacturers this acts as a filtering mechanism.

14.3 Video Streaming Gateway

The Video Streaming Gateway acts as an iSCSI NVR for ONVIF cameras in the BVMS environment.

Bosch cameras should be added as ONVIF cameras to the VSG or added as direct Bosch cameras to the VRM.

Topic	Remark
Alarm recording	VSG supports alarm recording triggered by BVMS events.
Protocols	RCP+, RTSP, JPEG. PTZ operations cannot be used when using the RTSP or JPEG protocols.
Protocols	A camera can be added to a VSG multiple times with the same IP address (for purpose of connecting 360° 3rd party cameras using 4 cameras with same IP).
Performance	One Video Streaming Gateway can use up to 7 instances for 32 camera connections per instance (resulting in 224 camera channels per VSG).

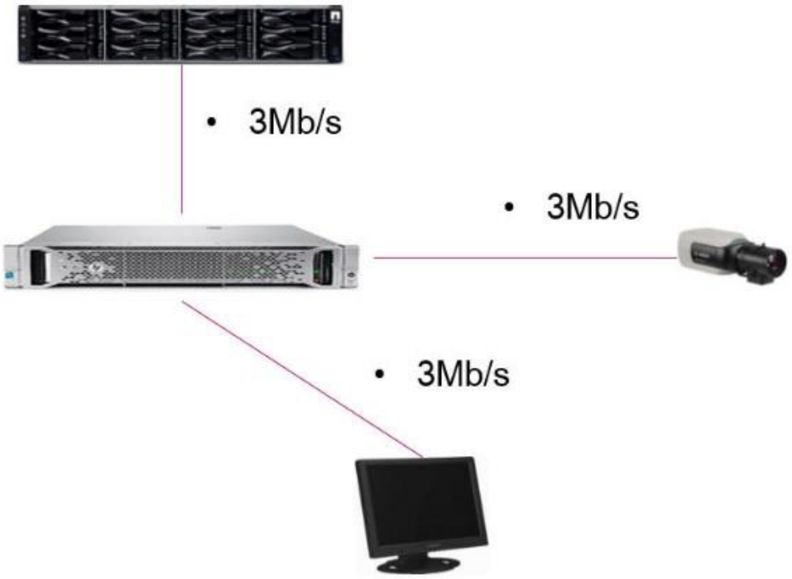
14.3.1 Throughput

VSG throughput and performance is determined by several factors:

- The server platform it is installed on
- The iSCSI target it is writing to
- The number of possible clients in the VMS
- The number of cameras assigned to the VSG

When designing a system, all of these factors must be considered in order to build a cleanly-functioning system. When using a standalone server, the VSG throughput will vary based on the hardware platform itself. Older generation servers could provide 350 to 400 Mb/s of throughput. This includes both the RTSP pull from cameras, as well as the iSCSI push to the storage target. The new Generation 10 Server can supply 3000 Mb/s of throughput.

The second part of the equation is the available throughput of the iSCSI target.



Overview

The table below shows the VSG performance when using DIVAR IP appliances.

Appliance	iSCSI sessions	Maximum recording performance	VSG throughput
DIVAR IP 7000	128	200 Mbit/s	140 Mbit/s
DIVAR IP 6000	128	200 Mbit/s	140 Mbit/s
DIVAR IP 7000 R2	256	550 Mbit/s	440 Mbit/s
DIVAR IP 6000 R2	256	550 Mbit/s	440 Mbit/s
DIVAR IP AiO 5000	42	170 Mbit/s	136 Mbit/s

The table below shows the VSG performance when using a dedicated VSG server combined with an external iSCSI target (for example, the DSA E2800).

Server	iSCSI target	VSG throughput	Cameras
HPE DL380 G8 (MHW-S380R8-SC) (1Gbit/s)	DSA E2700 (1Gbit)	700 Mbit/s	224
HPE DL380 G10 (MHW-S380RA-SC) (10Gbit/s)	DSA E2800 (10Gbit)	3000 Mbit/s	224
HPE DL380 G10 (MHW-S380RA-SC) (4x1Gbit/s teamed)	DSA E2800 (4x1Gbit/s teamed)	3000 Mbit/s	224
HPE DL380 G10 (MHW-S380RA-SC) (1Gbit)	DSA E2800 (1Gbit)	700 Mbit/s	224

There is a ~5% performance impact when enabling encrypted recording and encrypted communication on the VSG server. There is a ~20% performance impact when running the VSG in a virtual machine. The throughput should be reduced with the performance impact depending on the scenario.

Example calculation

In a VSG standalone sever scenario with a camera that is streaming at 3Mb/s:

- 3 Mbit/s VSG incoming from the camera
- 3 Mbit/s VSG outgoing into the iSCSI target
- [Optional] 3 Mbit/s Viewing (1 operator client)
  - Operator clients can stream directly from the camera or from the VSG. When the stream comes directly from the camera the optional bandwidth should not be included in the VSG performance calculation.

Bandwidth calculation for a single camera would be 9 Mb/s. A 100 camera system would be calculated at a theoretical worst case scenario 900 Mbit/s.

14.4 Streaming protocols

			VSG Secure & Camera secure		VSG secure & Camera insecure		VSG insecure & Camera secure		VSG insecure & Camera insecure	
Endpoint 1	**Endpoint 2**	**Camera**	**Security**	**Protocol options**	**Security**	**Protocol options**	**Security**	**Protocol options**	**Security**	**Protocol options**
OC	VSG	ONVIF	Encrypted	TCP	Encrypted	TCP	Unencrypt.	UDP / TCP	Unencrypt.	UDP / TCP
OC	VSG	Bosch (RCP+)	Encrypted	TCP	Encrypted	TCP	Unencrypt.	UDP / TCP	Unencrypt.	UDP / TCP
OC	Camera	ONVIF	Encrypted	TCP	Unencrypt.	UDP	Encrypted	TCP	Unencrypt.	UDP
OC	Camera	Bosch (RCP+)	Encrypted	UDP / TCP	Unencrypt.	UDP / TCP	Encrypted	UDP / TCP	Unencrypt.	UDP / TCP
VSG	Camera	ONVIF	Encrypted	TCP	Unencrypt.	UDP	Encrypted	TCP	Unencrypt.	UDP
VSG	Camera	Bosch (RCP+)	Encrypted	TCP	Unencrypt.	UDP	Encrypted	TCP	Unencrypt.	UDP

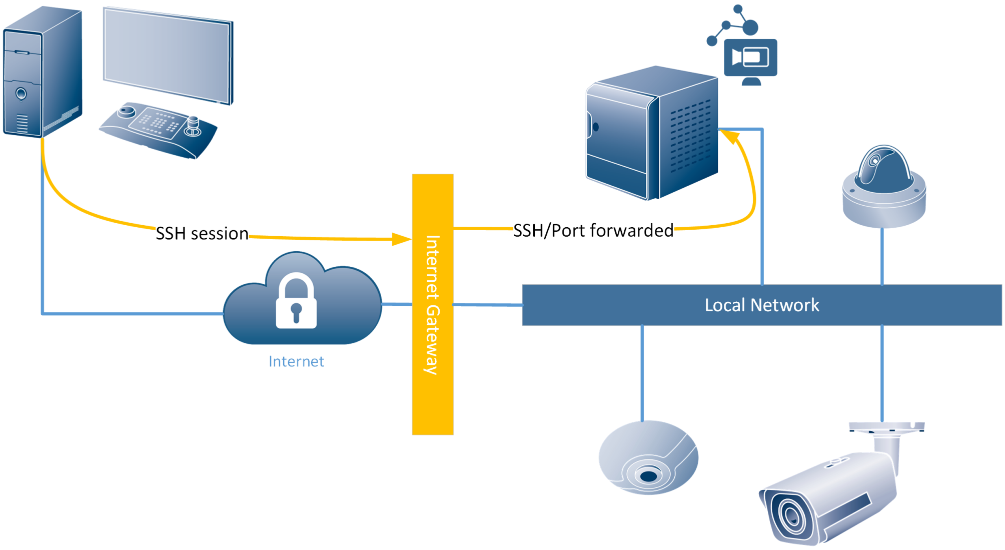
15 Remote access

BVMS offers two ways to access the system from a remote connection:

- SSH tunnelling: as of BVMS 7.5 SSH tunnelling was introduced. SSH tunnelling allows all BVMS related traffic to be send through an SSH tunnel.
- Port forwarding: the BVMS components can be made aware of a port-forwarded connection to the system. As of BVMS 7.5 it is not recommended to use this functionality any more.

15.1 SSH tunnelling

SSH Tunnelling constructs an encrypted tunnel established by an SSH protocol/socket connection. This encrypted tunnel can provide transport to both encrypted and un-encrypted traffic. The Bosch SSH implementation also utilizes Omni-Path protocol, which is a high performance low latency communications protocol developed by Intel.



The SSH client is embedded into the BVMS Operator Client. The SSH service can be, optionally, installed on the BVMS management server. When using SSH tunneling, all BVMS related traffic is routed through the SSH service and this will therefore also create a single-point-of-failure in the system.

15.1.1 Forensic Search

Due to the huge amount of data that needs to be transferred to the BVMS operator client a limited version of Forensic Search is available when connected to a BVMS system via SSH.

15.1.2 Transcoding

Transcoding enables to BVMS Operator Client to operate within low bandwidth (>=300 kbit/s) networks.

If no transcoder sessions or hardware transcoder is available in the VRM no image will be displayed in the BVMS operator client. Transcoded videos are selected by operator per device and it will be indicated in the cameo that a transcoded stream is being used. The following operations cannot be executed when a transcoded session to a device is used:

- Delete Video
- Protect/Unprotect Video
- Authenticate Video
- Forensic Search
- Export Video

Software transcoding

Software transcoding is offered in Operator Client as a fall-back level when no hardware transcoder is available, but only for live.

Hardware transcoding

The hardware transcoder is available for LIve and playback for VRM connected Bosch cameras. BVMS is able to utilize the transcoder service within the internal transcoder of the VRM installed on DIVAR IP 3000/7000 as well as DIVAR IP 2000/6000. The hardware transcoding device or service cannot be configured from the BVMS config client, but needs to be configured in the Bosch Configuration Manager.

16 Recording

16.1 Video Recording Manager

When planning for larger environments we strongly recommend using large sized disk arrays instead of a large number of small disk arrays (vertical scaling instead of horizontal scaling). For systems with more than 40 disk arrays, please contact a Bosch Pre-sales engineer. iSCSI based storage systems not qualified by Bosch are not supported.

One VRM is required to manage:

- up to 2048 channels
- up to 2 PB storage (net capacity)
- up to 40 disk arrays (recommended)
- up to 120 iSCSI targets
- up to 64 playback sessions simultaneously (using VRM replay)

The VRM tolerates a downtime of 7 days of the BVMS management server, as the central server executes a license push. This means the recording will continue for 7 days if the BVMS management server is down. After 7 days the VRM will stop recording. With older VRM versions (prior to 3.55) the recording will stop after 24 hours.

BVMS supports multiple Pools (Pooling implemented in VRM 3.0), a migration from former VRM versions is possible.

Direct iSCSI and Local Storage is supported for devices which support Firmware 4.x and above. I.e. no Local Storage support for VIPX1/X2 and VJ800x.

Pre-Alarm, Alarm and Post-Alarm, while pre- and post- must be at least 15 seconds. This means, pre-alarm is always streaming over the network (except when using ANR).

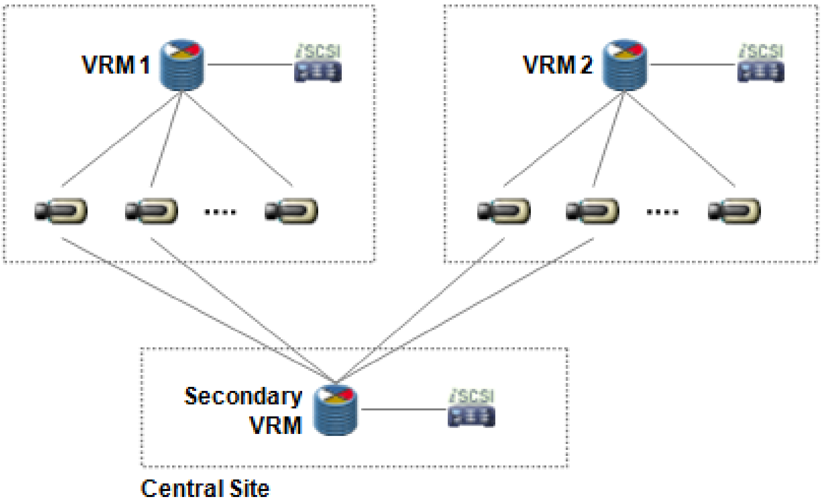
Continuous, Alarm and Post-Alarm, while post must be at least 15 seconds.

VRM/iSCSI and local recording do not support the configuration of Holidays for recording. Special Days must be used.

Support of E-series with dual controller system with 2x2 ports to increase number of cameras

Dual recording:

- Licensed per channel using the following license: MBV-XDUR-[version]
- Dual recording refers to simultaneous recording from one camera on two different storage targets.
- A Secondary VRM can record the second stream of the camera from various primary VRMs



16.1.1 Dual recording

Dual recording has a special mode called “Mirrored recording”:

- The Secondary VRM uses the exact same configuration with the same devices and quality settings as the Primary VRM. Only the retention time can deviate.
- Advantage: Devices added to the Primary VRM are automatically added to the Secondary VRM.
- It is not possible to combine dual recording and ANR (s. chapter on Automatic Network Replenishment)

- Video Streaming Gateway does not yet support dual recording.
- VJM-4016 does not support dual recording.

16.1.2 Fail-over recording

- Licensed per channel using the following license: MBV-FOV-[version].
- Fail-over recording is set up for another VRM. When the Primary VRM fails, the Fail-over VRM will take over the management of the recording, using the exact same configuration. Hence, one Fail-over VRM is needed for redundancy of another VRM (1:1 relation).
- Fail-over VRM can be configured for a Primary VRM as well as for a Secondary VRM.

16.2 Automated Network Replenishment

ANR is meant to buffer network outages and then push it to storage, once network is back.

- ANR works with CPP-ENC and CPP4 with Firmware version 5.90 or later.
- Firmware 5.92 improves the initial functionality of ANR to become more robust against local storage media failures.
- BVMS issues an alarm, when the buffer storage on the local SD card reaches a critical state (default setting is 90%) and another alarm, when recordings are overwritten. An alarm is also issued, when SD card is missing or broken.
- ANR and dual recording is mutually exclusive. User can configure either ANR or dual recording for a camera.
- Please refer to the Release Notes and the Whitepaper of ANR to find out about the known limits and recommendations. These documents are available in the documents’ section of the IP cameras in the Bosch Product Catalogue in the Internet.
- Local playback sessions, especially those of extended continuity, should be avoided, or at least treated with care, to have ANR 2.0 perform as configured.

Passwords

The service, user and live password of an encoder should be equal in order for ANR to work. ANR does not work when the connection to an encoder is set to "secure".

17 Person Identification

Person identification is currently only possible with Bosch cameras.

Specification	Limit
Suspect lists	5
Suspects	1000 suspects on 1 list, or up to 5000 suspects on 5 lists
Person Identification Devices per BVMS management server	25
Minimum face size	45px * 45px
Maximum viewing angle	An increased viewing angle decreases the detection performance.
Maximum quantity of faces in the scene	An increased amount of faces in the scene might increase the delay in the identification process.
Identification time	An increased amount of faces in the scene might increase the delay in the identification process.
Maximum person identification cameras per system	200, based on 25*DL380 Gen10 AI Server
Anti-spoof (live detection)	No.
Video codec	h.264 (no h.265)
GOP structure / length	IP (no b-frames, IBP, IBBP), 30 (maximum 60)
Recommended BVMS Profile	Image Optimized (busy, quiet, standard). The Balanced (busy, quiet, standard) profile uses an IBP GOP structure and Bit rate optimized (busy, quiet, standard) uses an IBBP GOP structure, which cannot be used combined with the person identification functionality.
Accuracy (LFW)	99,65%
Suppress duplicate alarms (same person, same camera)	Yes, configurable
(Bosch) camera firmware version	7.10 or higher
Stream usage	Stream 1

The CORE Person Identification Device hosts the suspect database and consolidates events from the EDGE Person Identification Devices. If the CORE Person Identification Device is unavailable, the Person Identification functionality is not operational.

18 Intrusion

BVMS 5.5 or higher supports UL intrusion panels supporting Mode 2 protocol:

- GV4 (requires vs.2.x FW update to support Mode 2): tested and approved with D9412GV4
- B-series: tested and approved with B5512

Specification	BVMS Professional	BVMS Enterprise
Intrusion panels	20 intrusion panels with maximum 20 x 512 detection points. It has to be ensured, that the alarms from all Intrusion panels does not exceed 100 per minute	Limits apply to each MS
Intrusion panels	40 intrusion panels with maximum 40 x 256 detection points. It has to be ensured, that the alarms from all Intrusion panels does not exceed 100 per minute	Limits apply to each MS

Supported feature set:

- Areas and devices are scanned from panel
- Intrusion events can be mapped to BVMS events and thus be used in the BVMS Event and Alarm management
- Intrusion Events are logged in BVMS logbook
- Status of Outputs, Doors, Points and Areas are shown on map (BVMS 6.0 or higher)
- Operator is capable to execute the following actions from the Operator Client (BVMS 6.0 or higher):
- Control outputs (on/off)
- Lock/unlock, secure and cycle doors
- Bypass and Un-bypass points
- Arm and disarm areas from the Client
- Silencing areas from the Client

An B/G series intrusion panel can maintain up to two client connections at the same time. If both BVMS and AMS are connected to an intrusion panel, RPS cannot connect. When RPS, BVMS, and AMS are used in the same environment, BVMS might not receive state updates from the panel.

18.1 Events

Event name in BVMS	Event ID included	Name in Intrusion panel
Access denied	139	Access Denied – No rights in area by passcode
	140	Access Denied – No rights in area by card
	141	Access Denied – Interlocked
	142	Access Denied – Unknown ID
	143	Access Denied – Door Secured
Access granted	2	Access Granted

Event name in BVMS	Event ID included	Name in Intrusion panel
	3	Access Granted to Sub-User
Alarm	19	Alarm
	20	Alarm with Recent Closing
	21	Alarm Exit Error
	22	Alarm Cross Point
	27	Missing Alarm
	238	Keypad Silent (Hold-Up) Alarm
Area armed	120	Force armed perimeter instant
	121	Force armed perimeter delay
	122	Armed perimeter instant
	123	Armed perimeter delay
	64	Forced Closing by Area
	65	Forced Close Early by Area
	66	Forced Close Late by Area
	67	Closing by Area
	68	Closing Early by Area
	69	Closing Late by Area
Area Disarmed	61	Opening by Area
	62	Opening Early by Area
	63	Opening Late by Area
Door left open	144	Door Left Open Alarm
	145	Door Left Open Trouble
Duress	4	Duress
	240	Keypad Panic Alarm
	242	Keyfob Silent (Hold-Up) Alarm
	243	Keyfob Panic Alarm
Fire Alarm	14	Fire Alarm

Event name in BVMS	Event ID included	Name in Intrusion panel
Fire Supervision	154	Fire Supervision
	159	Missing Fire Supervision
Gas Alarm	215	Gas Alarm
	219	Gas Supervisory
Medical Alarm	236	Keypad Medical Alarm
User passcode tamper	77	User passcode tamper – too many attempts

19 DIVAR recording devices

19.1 DIVAR IP

From BVMS 10.0 onwards the BVMS installation package can be directly installed on the supported DIVAR IP devices.

Licenses

BVMS non-commercial and sales-demo licenses can be applied on the DIVAR IP 3000, AIO 5000, and (AIO) 7000 and will override the built-in license.

DIVAR IP	Generation	CTN	Operating System	Minimum BVMS version	Maximum BVMS version
7000	2	DIP-71x	Windows Server 2012 R2	BVMS 6.0	See remarks below
AiO 5000	1	DIP-52x	Windows Server 2016 R2	BVMS 9.0	See remarks below
AiO 7000	1	DIP-72x	Windows Server 2016 R2	BVMS 9.0	See remarks below

19.2 DIVAR AN, Network, Hybrid

BVMS can operate in a system with:

- DIVAR AN 3000/5000
- DIVAR Network 2000/3000/5000
- DIVAR Hybrid 3000/5000
- DVR 400/600 and 700
- DVR 431, 440, 451, 480
- DVR 630, 650, 670
- Divar 700

One MBV-XDVR-xx license is required per DVR. The connected cameras are included.

Implemented functionality:

Feature	Supported DVR
Playback	
Record Video	ALL
Audio	ALL
Export ASF, MOV, Native	ALL
Forward, Reverse playback	ALL

Speed adjustment	ALL
Single stepping	ALL
Protect / Unprotect	DIVAR AN
Delete video	DIVAR 700 DIVAR AN
Go to next	ALL
Add bookmark	ALL
Print image	ALL
Restrict video	DIVAR AN
Instant playback	NONE
Playback in alarm cameo	NONE
Live	
PTZ	ALL
Aux	NONE
Pre-position	ALL
Focus / Iris	ALL
Sequencing	ALL
Motion search	ALL
Inputs	ALL
Relays	ALL

Each DIVAR can handle up to five simultaneous connections. One connection is consumed by:

- Playback, per camera
- Live, per camera
- Events, per BVMS system.

For example, if 2 operators are looking at 2 cameras each, LIVE:

1 Server + 2 LIVE + 2 LIVE = 5 connections.

It is not possible to send cameras connected to a DIVAR to a decoder.

20 External data

BVMS 5.0 and higher can record additional data. Additional data is searchable in the BVMS via the Logbook. Additional data can be received by BVMS by the following means:

- Virtual inputs
- Foyer Card Reader (maximum 2 to one management server)
- DTP3N with serial interface (datasheet)
  - Supports up to 4 ATMs or Foyer Card readers
  - Translates protocols of the ATMs into a defined format, which is needed for BVMS
  - Currently no list of supported manufacturers available
  - Serial RS232 connection in and out – connected to Bosch Management Server
- ATM/POS bridge
  - This is a HW device to connect IP devices to the Management Server, but is **not produced** any more.
  - To translate Text data into a format BVMS could read
  - ATM/POS bridge SW still exists and is used to transfer text data from an IP device to BVMS
    - ATM/POS 1.00.00.09 installation package download on IPP website
    - ATM/POS service user guide

Known restrictions:

- Additional data can be recorded in either logbook only, or in logbook and recording.
- Additional data can only be displayed when the operator client is in playback mode.
- The search for additional data is always performed in the logbook and has the following limitations:
  - 10 * Virtual input with length 300 = 3000 characters: 109 items*/sec (average)
  - 10 * Virtual input data field with length 800 = 8000 characters: 22 items*/sec (average)
  - 10 * Virtual input data field with length 30 = 300 characters: 500 items*/sec

Average

Item = data Input Event. If data is stored in the recording then there is an additional restriction:

- A maximum of 3200 Bytes (corresponds to about 3200 English characters in Unicode) can be processed per event.

21 Infrastructure

The BVMS management server, the VRM and the workstations can function perfectly in an enterprise (domain) environment. Bosch recommends the following:

- The BVMS related services (to be found in the Microsoft Management Console - Services) should run under an account with local administrative privileges.
- The SQL server, which BVMS is using to store its logbook, should be configured for access based on Windows Authentication. The account under which the BVMS management service is running should have access to the SQL server. This can be tested by using the Microsoft SQL Server Management Studio (SSMS).
- The BVMS components need to have access to write the necessary (logging, configuration) files to the disk. Locations:
    - C:\ProgramData\Bosch
    - C:\Program Files (x86)\Bosch (BVMS 7.5 or earlier)
    - C:\Program Files\Bosch (BVMS 8.0 or newer)
    - C:\Users\%username%\AppData

When problems arise when running BVMS in a domain environment, Bosch recommends looking at the Windows event log for service start-up problems. Alternatively the BVMS Config Collector can be used to gather the required log files and these can be send to the technical support team for further analysis.

22 Access Management System

22.1 Scalability

AMS - BVMS integration

BVMS 10.0.1 or 10.0.2 is not able to connect to AMS 2.0 or AMS 3.0. Integration with AMS 3.0 is possible for BVMS 10.1 or BVMS 10.1.1.

Specification	**BVMS Lite, Plus, Professional, DIVAR IP**	**BVMS Enterprise**
Access Management Systems	5 access management systems	Limits apply to each MS (500 in one Enterprise environment)

22.2 SDK

The BVMS SDK capabilities are documented in the BVMS SDK documentation. The BVMS SDK documentation is available on the Bosch Knowledge Base.

22.3 Events

Device	**Event**	**Type**	**Description**	**Stored information**
Relay	Relay State (**control**)	State	Open, Closed	n/a
Digital Input	Input State	State	Open, Closed	n/a
Door	Unauthorized door opening	Peak		n/a
Door	Door open too long	Peak		n/a
Door	Door contact state	State	Open, Closed.	n/a
Door	Door state	State	Secured, Locked, Unlocked	n/a
Door	Door operation mode (**control**)	State	Normal, Manual, Disabled	n/a
Reader	Access granted	Peak		Firstname, Surname, CredentialID
Reader	Access denied	Peak		Firstname, Surname, CredentialID
Reader	Access requested (**control**)	Peak	Video verification event	Firstname, Surname, CredentialID
Reader	Person did not enter	Peak		Firstname, Surname, CredentialID

Device	Event	Type	Description	Stored information
Reader	Authorized but selected by random screening	Peak		Firstname, Surname, CredentialID
Reader	Duress event	Peak		Firstname, Surname, CredentialID

23 Software security

The software security concept is explained in the BVMS - Securing a Security System document, which can be found on the Bosch Security Systems Community.

24 Services

When installed on a single device, BVMS installs the services mentioned in the table below.

Name	Log On As
Bosch Video Recording Manager	Local System
Bosch Video Streaming Gateway	Local System
Bosch VSG Worker Instance x	Local System
BVMS Central Server	Local System
BVMS DVR Adapter	Local System
BVMS Snmp Server	Local System
BVMS SSH Server	Local System
BVMS Web Service Host	Local System
SQL Server (BVMS)	Local System

25 Software Assurance

Technical support services and upgrading to a newer BVMS version requires Software Assurance PRO. The table below can be used to check the exact release dates of the different BVMS versions.

Version	Release Date	Description
3.0	2011-09-12	Moving from 500 to 2.000 cameras supported by a single Management Server and VRM
4.0	2012-08-10	Important steps towards scalability, mobility and openness. The ability to run in multi-site environments with up to 200 servers and 200.000 cameras to enable central monitoring and operation of multiple sites. Mobile Device access w/ live and playback Basic ONVIF integration for live, PTZ, playback
4.5.5	2013-07-01	Distributed systems across WAN (TCP tunneling and DynDNS); Transcoded streams on demand; Support of different time zones; Support of a Web-Client for simple life and playback; Support of Bosch DIVAR series 400/600/700.
5.0	2014-07-28	Support of dual recording and failover; Automatic Network Replenishment 2.0; IOS App to capture and share video; Support of 4k camera; Support of additional data in video stream; Combination of HW with Software transcoding for Operator Client; Support of Onvif Status supervision.
5.5	2015-01-31	Added resilience; intrusion integration; backwards compatibility; first step on ONVIF based integration of non-Bosch cameras; Client dewarping for Panoramic cameras.
6.0	2015-12-10	Added ONVIF events; unmanaged sites; map improvements; configuration reports.
6.5	2016-04-29	Server based analytics; Video Fire Detection; Enhancements of unmanaged sites; Enhancements of Panoramic camera.
7.0	2016-10-28	Streamlining; encrypted communication to/from cameras; video verification; data security guidebook; corridor mode.
7.5	2017-04-29	Secure remote access, forensic search free of charge, storage openness.
8.0	2017-10-27	Operator client performance improvements (live), Enterprise scalability (64-bit architecture), Unmanaged site improvements (SSH, favourites).
9.0	2018-08-17	BVMS Plus, Dark user interface, modern pan-tilt-zoom control, easier alarm management, AAC audio, intelligent streaming, limit amount of image-panes.
10.0	2019-08-13	Person identification, ONVIF Profile S certification, Data security, Enterprise (100 sites), monitor wall consolidation.
10.0.1	2020-04-03	Forensic Search improvements, dewarping pre-sets in alarms, running in a FIPS environment.
10.0.2	2021-03-24	Data security improvements.
10.1	2020-08-25	Access Control improvements, Person Identification scalability, Native LPR camera integration (IPP).
10.1.1	2021-03-24	Data security improvements.
11.0	2021-Q1	*Object tracking and Here maps integration, enhanced software licensing (adding BVMS to the enterprise management system (EMS))*