BVMS - System design guide

Author: Verhaeg Mario (ST-ESS/MKP1)

Date: 09-Nov-2017 08:29

1 Document information

Project	BVMS 8.0
Reference	n/a
Version	24
Last modified	24 October 2017

1.1 Version history

Version	Date	Author	Comment
24	2017-10-24	Verhaeg Mario (ST-ESS/MKP1)	

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 8.0 and Bosch Video Stitcher 1.6 release notes can be found on the Bosch Security Systems website.

This document lists the valid design specifications for BVMS 8.0 You require an updated version of this document to commission sales for a more recent version of BVMS. This document has been last updated on 24 October 2017 .

Warning

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

3 Recommended hardware

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

The DSA E-series cannot be used as a storage device for the VMware platform.

3.1 Management Server and Mobile Video Service

With the BVMS Professional up to 500 cameras can be managed by a single server, combining the Management Server and the Video Recording Manager.

Item	Description
Operating System	Windows (Storage) Server 2008 R2 (DIP-3000 only) Windows (Storage) Server 2012 R2 (64-bit) Windows (Storage) Server 2016 (64-bit) Windows 8.1 Professional (64-bit) Windows 8.1 Enterprise (64-bit) Windows 10 Professional (64-bit), including Anniversary Update Windows 10 Enterprise (64-bit), including Anniversary Update
CPU	Intel Xeon E5-2620v3 (2.4 GHz, 6-core, 15MB, 85W)
RAM	8GB
Free disk space	15GB (+ 15% of the hard-drive after installation)
Network	1 Gigabit/s network interface card

3.2 Video Recording Manager

With the BVMS Professional up to 500 cameras can be managed by a single server, combining the Management Server and the Video Recording Manager.

Item	Description
Operating System	Windows (Storage) Server 2008 R2 (DIP-3000 only) Windows (Storage) Server 2012 R2 (64-bit) Windows (Storage) Server 2016 (64-bit) Windows 8.1 Professional (64-bit) Windows 8.1 Enterprise (64-bit) Windows 10 Professional (64-bit), including Anniversary Update Windows 10 Enterprise (64-bit), including Anniversary Update
CPU	Intel Xeon E5-2620v3 (2.4 GHz, 6-core, 15MB, 85W)
RAM	4GB
Free disk space	1GB (+ 15% of the hard-drive after installation)
Network	1 Gigabit/s network interface card

3.3 Bosch Video Stitcher

Item	Description
Operating System	Windows 10 Professional (64-bit), including Anniversary Update Windows 10 Enterprise (64-bit), including Anniversary Update
CPU	Intel Xeon E5-1620v3 (3.5GHz)
RAM	8GB
Free disk space	Minimum 5GB
Network	1 Gigabit/s network interface card
Display resolution	Minimum: 1280 x **1024** Recommended: 1920 x 1080
Graphic card	MHW-AWGC-M2000 (Nvidia Quadro M2000)

3.4 Operator Client

Item	Description
Operating System	Windows (Storage) Server 2008 R2 (DIP-3000 only) Windows 8.1 Professional (64-bit) Windows 8.1 Enterprise (64-bit) Windows 10 Professional (64-bit), including Anniversary Update Windows 10 Enterprise (64-bit), including Anniversary Update
CPU	Intel Core i7 4770 3.4 GHz (up to 3.9 GHz)
RAM	8GB
Free disk space	Minimum 3GB for Single Site Systems Minimum 5GB for Enterprise Systems
Network	1 Gigabit/s network interface card
Display resolution	Minimum: 1280 x 1024 Recommended: 1920 x 1080
Graphic card	MHW-AWGC-K620 (Nvidia Quadro K620) MHW-AWGC-M2000 (Nvidia Quadro M2000) MHW-AWGC-M4000 (Nvidia Quadro M4000)

3.5 Storage

3.5.1 iSCSI storage devices

The storage quick selection guide can be found on the http://ipp.boschsecurity.com/bvms website.

3.5.2 Bosch DVRs

Device	Series
Bosch DIVAR AN	3000
Bosch DIVAR AN	5000
Bosch DIVAR Network	2000
Bosch DIVAR Network	3000
Bosch DIVAR Network	5000

Bosch DIVAR Hybrid	3000
Bosch DIVAR Hybrid	5000
Bosch DVR	700
Bosch DVR	4xx
Bosch DVR	6xx

3.6 Cameras

3.6.1 Bosch Cameras

All Bosch cameras can be used under the device compatibility concept, which is described in a whitepaper.

3.6.2 ONVIF Cameras

The list of supported ONVIF cameras can be found on the http://ipp.boschsecurity.com/bvms website. If a camera is not listed, testing can be ordered by filling in the custom camera integration form.

3.7 Network

The *BVMS blueprints* show the different network environments in which the system can perform reliably. 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 is experiencing a decrease in network performance the event response time and alarm visibility time may increase.

3.7.1 Required network ports

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

3.8 Other hardware

Type	Device	Remarks
Decoder	Bosch VIDEOJET decoder 3000	n/a
Decoder	Bosch VIDEOJET decoder 7000	n/a

Decoder	Bosch VIDEOJET decoder 8000	Supports displaying of 4K cameras
Foyer card reader	MINITER 485	n/a
Serial input	Werner Electronic DTP3N	n/a
Intrusion panel	Bosch G-series B9512G 3.03.14	Automation Device in the intrusion panels must be configured as Mode 2
Intrusion panel	Bosch B5812G 3.03.14	Automation Device in the intrusion panels must be configured as Mode 2
Intrusion panel	Bosch B5512 3.03.14	Automation Device in the intrusion panels must be configured as Mode 2
Intrusion panel	Bosch B4512 3.03.14	Automation Device in the intrusion panels must be configured as Mode 2
Intrusion panel	Bosch B3512 3.03.14	Automation Device in the intrusion panels must be configured as Mode 2
Intrusion panel	Bosch D9412GV4 2.03.018	Microsoft Windows Patch 3155464 should not be installed
Intrusion panel	Bosch D7412GV4 2.03.018	Microsoft Windows Patch 3155464 should not be installed
Monitor wall	Barco Transform N series	RCPPlus agent 0.9.4.0
Analog matrix switch	Bosch Allegiant Series	Firmware 8.75 or later, Master control software 2.94
ATM/POS Bridge	Bosch ATM/POS Bridge	Version 1.10.00.12
Keyboard	Bosch KBD-Universal XF	USB
Keyboard	Bosch Intuikey	Serial, firmware 1.96
Digital I/O	Advantech ADAM-6050	n/a
Digital I/O	Advantech ADAM-6052	n/a
Digital I/O	Advantech ADAM-6060	n/a
Digital I/O	Advantech ADAM-6066	n/a
USB to serial	Belkin serial adapter F5U103VEA	n/a
Ethernet to serial	Comtrol DeviceMaster RTS 4-port	n/a

4 Management Server

Subject	Management Server (MS)	Enterprise Management System (EMS)
Management Servers	1	Per Enterprise User group: 10 MS with 1000 channels per MS; 50 MS with 200 channels per MS. Configurations in between to be checked with a Bosch pre-sales engineer.
Total number of IP devices (Encoder inputs, (ONVIF) cameras, decoders, Intrusion areas and devices)	2.000 in device tree	10.000 per user group
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). Condition: VRMs operating in LAN (1Gb).	In theory: 10x125 is possible, but total number of devices in logical tree shall not exceed 10.000
DiBos / BRS	100	10 MS with 100 each = 1.000
DVR (400, 600, 700, AN, Hybrid, Network)	50	10 MS with 50 each = 500
POS/ATM	15	10 MS with 15 each = 150
Virtual Inputs	4.000 (limited in configuration)	Number of devices in logical tree shall not exceed 10.000
Adam modules	50	10 MS with 50 each = 500
Task Schedules	200 (limited in configuration)	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	• 500 events/s with Logbook • 1000 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	Limits apply to each MS
Special Days	24	Limits apply to each MS
Allegiant CCL commands	Max 10/sec	Limits apply to each MS
Allegiant systems	1 per management server. When using the Allegiant master/slave concept there is no limit defined.	10 MS with 1 each = 10
BIS-BVMS Connection	1 OPC Server per MS	No Enterprise functionality. Only 1 OPC Server per MS.

5 Scalability

5.1 BVMS Enterprise

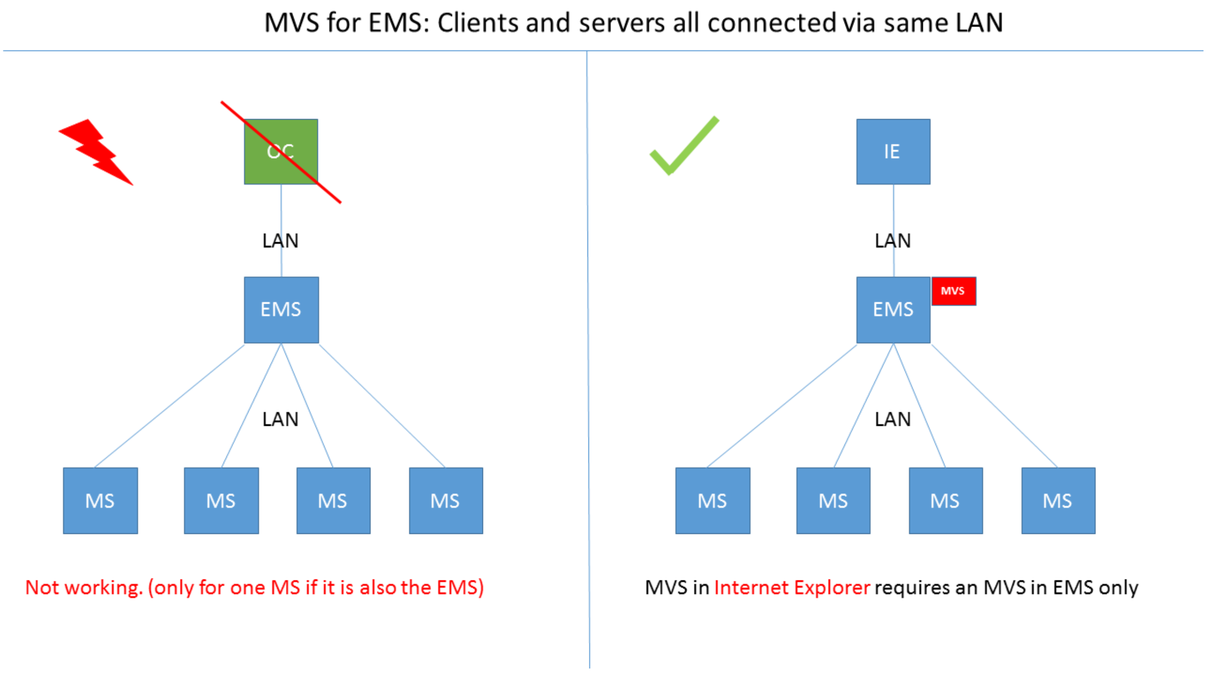
5.1.1 Licensing

The MBV-BENT license contains 2 subsystem, where of one subsystem can be used to connect the Enterprise Management Server itself.

Each workstation which is connected to the Enterprise Management Server should be licensed as MBV-XWST-xx, where xx is the BVMS version. The workstation licenses included in the Professional license of the subsystems cannot be used for the Enterprise Operator Clients. When a migration is done from a Professional to an Enterprise system, the workstation licenses used in the sub-systems cannot be used for the Enterprise Operator Clients.

5.1.2 Mobile Video Service

There are a couple of scenarios in which MVS can be used in an Enterprise environment. These are shown below.

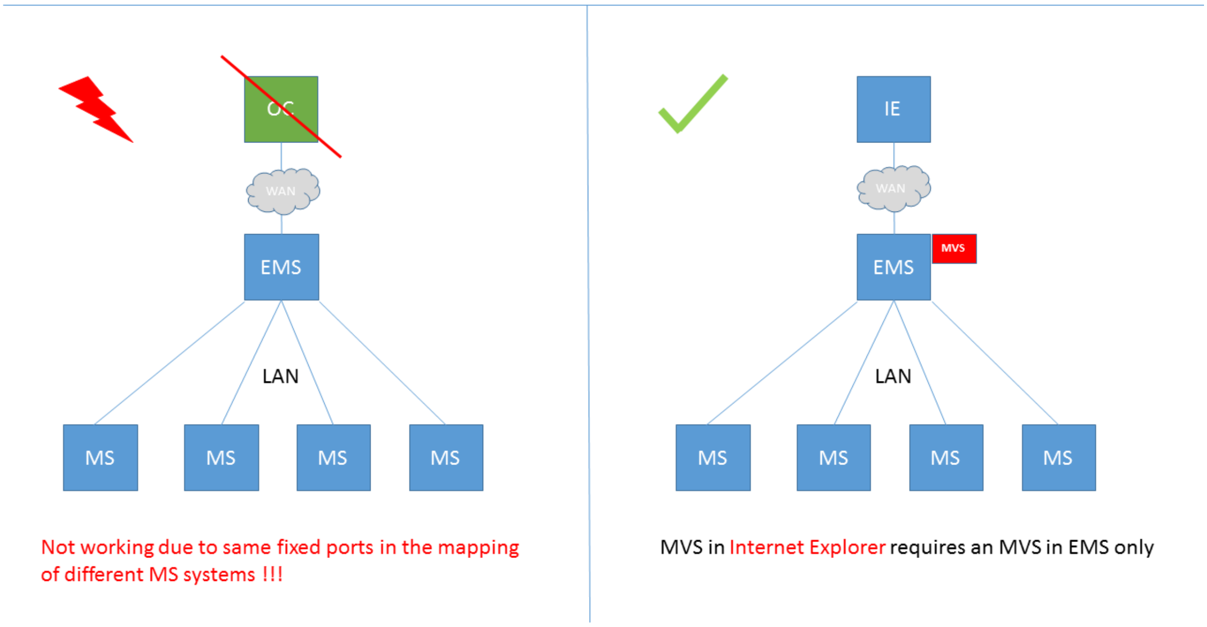


MVS for EMS: Clients and servers all connected via same LAN

Not working. (only for one MS if it is also the EMS)

MVS in Internet Explorer requires an MVS in EMS only

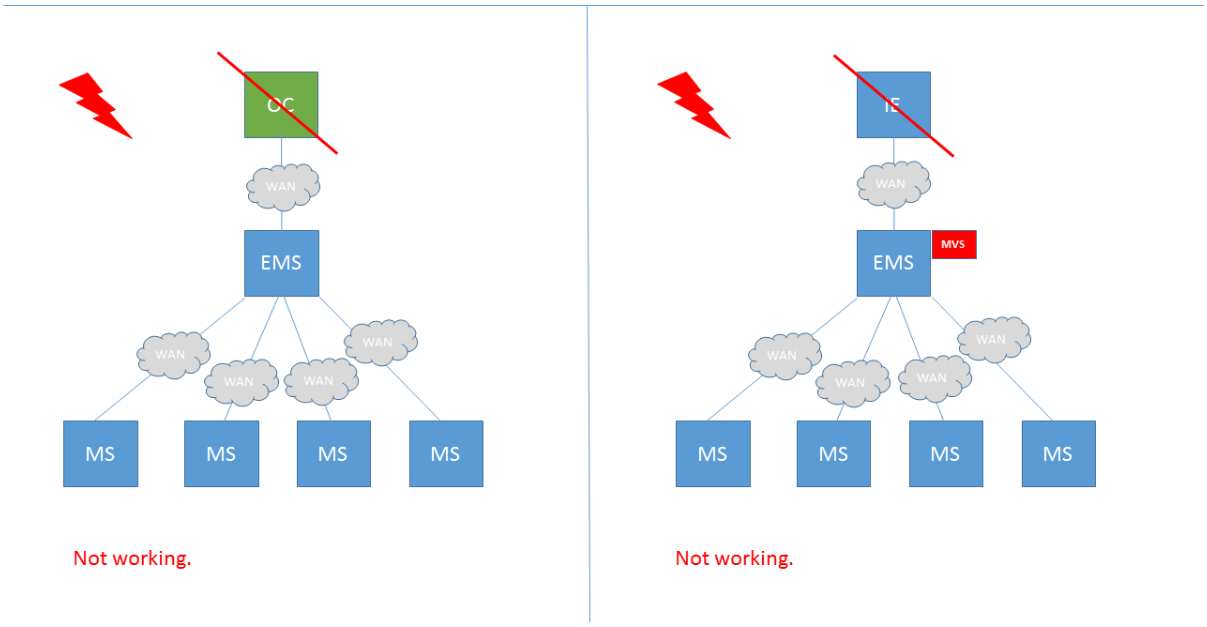
MVS for EMS: Clients connected via WAN and server all in same LAN



Not working due to same fixed ports in the mapping of different MS systems !!!

MVS in Internet Explorer requires an MVS in EMS only

MVS for EMS: Clients and servers connected via WAN



Not working.

Not working.

5.1.3 Special considerations

Topic	Remark
Monitor wall	As analog monitor groups are only exposed to the management server directly, these cannot be used in an Enterprise environment.
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 digital onitor wall.

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.

5.2 BVMS Unmanaged sites

5.2.1 Licensing

The MBV-BPRO-x contains one license for a sub-site. For each additional site, MBV-XSITE-xx is required. The DIVAR IP 3000/7000 cannot be expanded with MBV-XSITE-xx and a BVMS Professional system is required to act as the main site. Devices inside the sub-site do not need to be licenses in the main site, but (depending on the device) need to be licensed within the sub-site.

5.2.2 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	10.000
Functionality	Live, playback, PTZ
Bookmarks	Yes
Favorites	Yes, taking the 20 simultaneous connections into consideration.
State monitoring	States of the devices in the sub-site are not monitored.

5.2.3 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

5.2.4 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.
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 footrage 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.
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.

5.3 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 channels	2000	2000	200.000
Max# of channels 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 (50)
Max# of subsystems	n/a	9999	30
Max# of parallel connected subsystems in one Operator Client	n/a	20	10 (50)
Max# of connected system with unmanaged devices	0	9999	0

6 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 (10x faster than ASF), maximum 4 cameras in parallel.
Application architecture	64 bit
Decoding	GPU (Nvidia) first, CPU second. CPU decoding is used by default for streams smaller than 1080p.
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.

6.1 Languages

English, German, Dutch, Italian, Portuguese, French, Spanish, Simplified Chinese, Traditional Chinese, Russian, Hungarian, Japanese, Czech, Danish, Finnish, Greek, Norwegian, Polish, Swedish, Thai, Turkish, Korean, Arabic, and Vietnamese.

7 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

7.1 Web-client

The web client is based on HTML5, tested on:

- Firefox v30
- Chrome v36
- Safari v7.0.5, showing some limitations on the in Image pane PTZ functionality (control though can be used instead).
- Internet Explorer 11

Feature scope:

- Live
- Playback
- Trigger relays
- Trigger export on .MOV and native export on a Management Server

8 Maps

8.1 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.

8.2 File recommendations

The file size should not exceed 1MB as loading time will increase. 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.

9 Monitor wall

Specification	BVMS Professional	BVMS Enterprise
Decoders	128	128
Keyboards per decoder	1	1
Analog Monitor Groups	20 per management server	n/a

9.1 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.

9.2 Monitor wall versus Analog Monitor Groups (AMG)

Digital Monitor (MW) supports max. of 14 cameras per step due to its layout (3x3 or 1 large cameo with 13 small cameos).

Feature	AMG	Digital MW
Usage in local Operator Client	YES	YES
Usage in Enterprise Operator Client	NO	YES
Assigned via drag&drop in Operator Client	YES	YES
Control by workstation keyboard including PTZ	YES	NO
Control by decoder/server keyboard including PTZ	YES	NO
Control by SDK	YES	NO
Display camera on alarms	YES	NO
Display pre-configured sequences	YES	YES
Display automatic sequences	YES	NO
Support special layouts	NO	YES
Unmanaged site cameras	NO	YES

9.3 Special considerations

Topic	Remark
ONVIF	ONVIF cameras can be displayed on the Digital Monitor Wall using VIDEOJET 7000, VIDEOJET 8000 or VIP-XDHD.
Sequence	Sequence supports a max. of 100 steps and max. 25 cameras per step
Sequence	Sequences are controlled from the Operator Client. If the Operator Client is stopped, the sequence will also stop.
Allegiant	Status from Satellite Allegiant cameras will not be displayed
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 BVIP decoder .

9.4 Non-Bosch Monitor walls

9.4.1 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
- 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-70) per RCP+ Agent
- The RCP+ Agent supports asymmetrical layouts

10 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, ASF 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).

10.1 List of tested ONVIF cameras

The latest list of tested ONVIF cameras can be found on http://ipp.boschsecurity.com/bvms

10.2 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.

10.3 Video Streaming Gateway

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

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).
Performance	One Video Streaming Gateway (8 instances) can process up to 350 Mbit/s on MHW-S380R8-SC.
Performance	The Video Streaming Gateway performance of DIVAR IP devices is mentioned in the datasheets of the specific device.

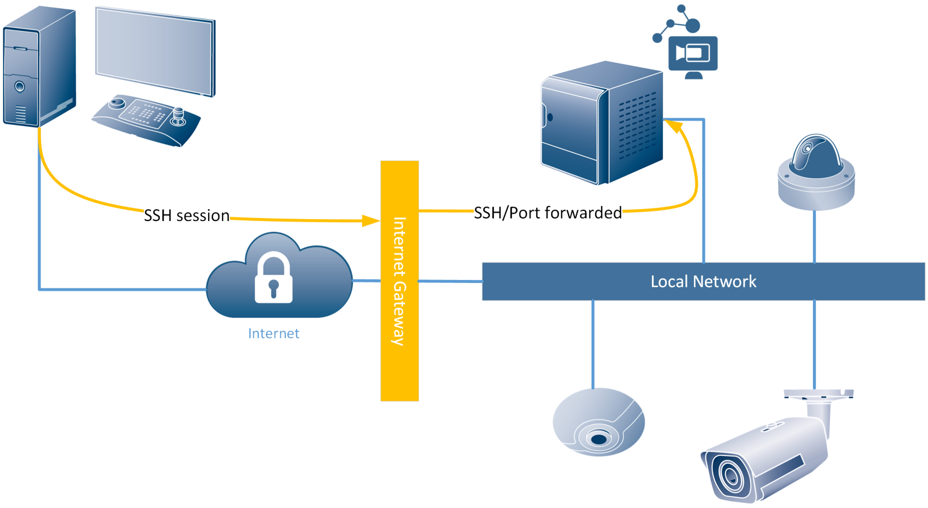
11 Remote access

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.

11.1 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.

11.1.1 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.

11.1.2 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.

12 Recording

12.1 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

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).

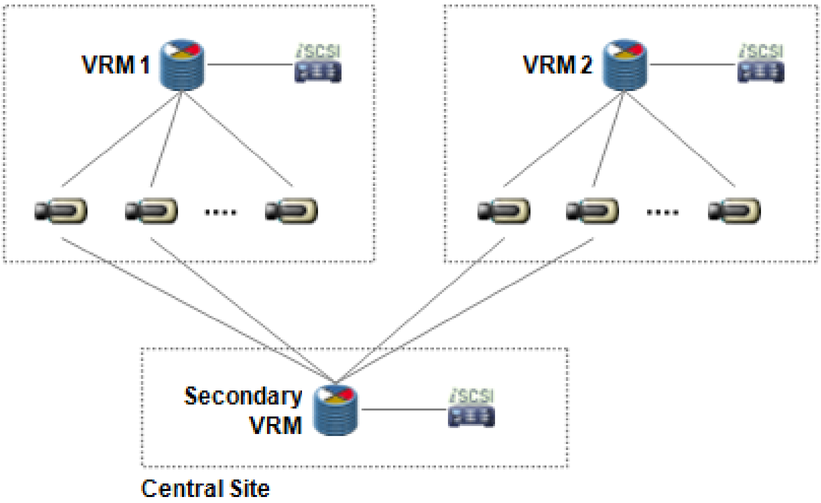
Continuous, Alarm and Post-Alarm, while post must be at least 15 seconds.

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-70
- 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



12.1.1 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

12.1.2 Fail-over recording

- Licensed per channel using the following license: MBV-FOV-60.
- 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.

12.2 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.

13 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	10x20 intrusion panels, but total number of devices in logical tree shall not exceed 10.000 AND the alarms from all Intrusion panels shall not exceed 100 per minute

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

13.1 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
	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
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

14 DIVAR recording devices

14.1 DIVAR IP

DIVAR IP 3000 and DIVAR IP 7000 are BVMS based appliances. The information listed in this document applies for those devices as well.

Licenses

BVMS commercial and sales licenses can be applied on the DIVAR IP 3000 and 7000 and will override the built-in license.

14.2 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	ALL
Pre-position	ALL
Focus / Iris	ALL
Sequencing	ALL
Motion search	ALL
Inputs	ALL
Relays	ALL

The following restriction apply:

DIVAR only support five connections:

- 1 connection for events etc. from server
- 1 connection per live cameo per camera
- 1 connection for playback per camera

There is no support for decoder connections.

Please consult the Data Security guidebook.

15 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.

16 Infrastructure

16.1 Domain and group policies

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.

17 Bosch Video Stitcher

17.1 Localization

The Bosch Video Stitcher Wizard is not translated and only available in English. The configuration manual is available in English, Spanish (EU), Simplified Chinese and French.

17.2 Terminology

Term	Description
Stitching instance	Also called: "Stitcher". The process, or software, that stitches multiple stitching channels into one stitched channel.
Stitching channel	The video channel that is feeding the Bosch Video Stitcher with a video stream.
Stitched channel	The output video channel that is generated by the Bosch Video Stitcher.

Examples are given in the commercial training.

17.3 Network

Component	Protocol	Port	Editable
ONVIF Server	HTTP	80	Yes
RTSP streaming	RSTP	554	Yes
License server	.net TCP	5388	No

17.4 Limitations

Description	Limit
Maximum number of cameras per stitching instance	16
Maximum number of tags per stitching instance	200
Number of stitching instances per workstation	1

18 Software Assurance

Upgrading to a newer BVMS version requires a valid SMA. The table below can be used to check the exact release dates of the different BVMS versions.

Version	Release Date	Description
3.0	2011-12-09	Moving from 500 to 2.000 cameras supported by a single Management Server and VRM
4.0	2012-10-08	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; date 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, favorites)

18.1 Details

- New purchases have one year of SMA included
- Without a valid SMA the system is covered by first line technical support via email or phone and has access to released hotfixes.
- Without a valid SMA the system owner cannot request for hotfixes and has no access to Software Service Releases, Software Version Releases and third party compatibility up-dates.