BVMS 10.1.1 - Upgrade and Migration

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

Date: 26 March, 2021

1 Document information 3

1.1 Version history 3

2 Introduction 4

3 General preparations 6

3.1 Checklist 6

3.2 Version specific changes 8

4 Upgrading a BVMS system 10

4.1 Concepts and changes 10

4.2 Upgrade steps 11

4.3 Finalizing and confirming the upgrade 14

5 Software development kits 15

5.1 Upgrading BVMS CameoSDK 15

5.2 Upgrading BVMS Software Development Kit 15

6 Migration of a BVMS system 16

6.1 Migration of Management Server and VRM 16

6.2 Migration of iSCSI targets 17

6.3 Migration of logbook 17

6.4 Migration of user settings 17

6.5 Migration of VSG 18

7 Troubleshooting 19

7.1 Setup 19

7.2 System services 19

1 Document information

Project	BVMS 10.1.1
Reference	Upgrade guide

1.1 Version history

Date	Description
2020-03-27	Added BVMS 10.0.1 changes.
2020-04-02	Removed information on old BVMS version. Added comment on automated firewall configuration when upgrading to BVMS 10.0.1.
2020-07-15	Added BVMS 10.1 changes.
2020-10-20	Fixed grammar issues.
2020-02-22	Added BVMS 10.1.1 changes.

2 Introduction

This document should help you to make the upgrade process as smooth as possible. The upgrade itself is not restricted to BVMS software only. The supported software and firmware versions can be found in the release notes of the related BVMS version.

Notice!

Exit Configuration Client and Operator Client on all affected computers before you start the upgrade process. In some case, especially when the system load is high, we recommend stopping the Central Server service before starting setup.

We recommend to upgrade BVMS in steps. Each version should not be more than ~two years apart. This prevents potential issues in the upgrade process. For example, when you want to upgrade from BVMS 9.0 (launched in August 2018) to BVMS 10.1 (launched in August 2020) no additional step is needed. However, when you want to upgrade from BVMS 8.0 to BVMS 10.1 we recommend to upgrade to an arbitrary BVMS release in between those versions to reduce the risk of something going wrong in the upgrade process.

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.

Version	Release Date	Description
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))*

3 General preparations

3.1 Checklist

This chapter provides a check list to be considered before starting the upgrade. Check the system requirements for your desired BVMS feature with the BVMS datasheet available in the Online Product catalog. Before starting the upgrade process, consider and check the following points:

Check	Description
	Read the Release Notes, which also include a list of the available patches for the specific version.
	Make sure that the upgraded license activation codes for the new version are available. As a precaution have an Emergency Backup license at hand.
	Consider restrictions of the new version.
	Make sure that the hardware environment (servers, workstations, network, storage, keyboards) is up-to-date, is working stable and that there are no other issues which could negatively affect the upgrade process. Ensure that your network is configured correctly for huge amounts of cameras, for example use separate VLAN for up to 2000 cameras so that not more than 2000 cameras are located in one subnet. Have a network and/or IT systems specialist available.
	Get all information about network infrastructure and system design. The network design guide, published as an article on the Bosch Building Technologies Community, lists some best-practices regarding network infrastructure design.
	Make sure how to handle redundancy solutions. Have a specialist available if necessary.
	Collect all logon credentials for PCs and other devices belonging to the system.
	Be prepared for a possible failure of devices. Prepare a backup plan if possible.
	Discuss the required downtimes with the customer. The times for the different steps are mentioned below. The downtime for the individual recordings should not be longer than the time for the encoder's firmware upgrade.
	Check deviations from the standard software (for example, dome driver protocols) and have them at hand. Check if these are compatible with the new version.
	Make sure that all Operator Clients and Configuration Client were logged on to the Management Server at least once. This is required for an Auto Deployment of the SW for the clients. During Setup, Configuration Client must be closed.
	Be sure to have the latest supported firmware available for all IP devices.
	Backup all individual configurations and important logbooks (for example user settings, which is described in an article on the Bosch Building Technologies Community). Do not delete logbook files (BVMSLogbook.mdf, BVMSLogbook.ldf). **Note**: The encoder's Intelligent Video Analytics / Motion+ settings remain untouched.

Check	Description
	Check if there are other individual settings (e.g. Time Server) in the BVMS CentralServer.exe.config and note them (do not reuse the file after upgrade!)
	Check the multicast settings of all devices (the multicast settings will be lost after the firmware upgrade if you come from a firmware < 4.0 and have to be reconfigured).
	Check if an external SQL server is installed and connected (this situation is described in an article on the Bosch Building Technologies Community).
	Make sure that the host name of the Management Server was not changed since the first installation. Otherwise the SQLDB migration for the logbook will fail. If the host name of the Management Server has changed, change the following registry key: `[HKEY_LOCAL_MACHINE\SOFTWARE\BVMS\Installer\SelectedValues]"LOGBOOKDB_SERVER"="<hostname>\BVMS"` Replace the <*hostname*> with your current hostname of the SQL server or (local) if you run the default local SQL Server.
	Before the upgrade, download the required OMF files from the Bosch Building Technologies Community.

3.2 Version specific changes

3.2.1 BVMS 10.1 and 10.1.1

Access Management System

If you use BVMS 10.0 combined with the Access Management System 2.0, both systems need to be upgraded. BVMS 10.1 only works with Access Management System 3.0.

Tracking and Recognition Service

If you use BVMS 10.0 combined with the Tracking and Recognition Service 1.0 (Person Identification), both systems need to be upgraded. BVMS 10.1 only works with the Tracking and Recognition Service 2.0.

3.2.2 BVMS 10.0.1 and 10.0.2

Exports using the SDK

To prevent SDK applications to overwrite existing files a whitelist needs to be defined. Without the whitelist existing SDK application might not be able to export video footage. The details are described in the SDK documentation.

Machine dependent configuration encryption on operator clients

From BVMS 10.0.1 onwards the configuration file stored on the operator client can only be decrypted by the workstation that downloaded the file from the BVMS management server. Another machine cannot decrypt this file.

SDK changes

Some inner exceptions that are triggered by the SDK might have changed. The outer exceptions are consistent to previous versions of the SDK. The SDK might also trigger exceptions in cases that are not handled gracefully. The core functionality of the SDK and its limitations are still consistent with previous versions.

Automated firewall configuration

After you have upgraded to BVMS 10.0.1 we recommend you to remove the manually created firewall rules in the Windows firewall. The BVMS set-up will, in the future, take care that the rules are updated according to changes in the system behaviour.

3.2.3 BVMS 10.0

When upgrading to BVMS 10.0 the following changes should be considered.

Video Streaming Gateway 7

For BVMS 10.0 the ONVIF event handling mechanism has been moved from the BVMS management server to the VSG. When a system is upgraded to BVMS 10.0 the ONVIF event management of existing cameras is not changed. ONVIF cameras which are added to the system after the upgrade will automatically use the event handling mechanism embedded in the VSG. It is strongly recommended to move the event handling of the existing ONVIF cameras (described in the BVMS configuration manual) to the VSG as well.

The event handling mechanism in the BVMS management server will be removed in BVMS 11.0.

BIS configuration file password encryption

The configuration of the password which the BIS client to start the BVMS Operator Client is encrypted. This configuration is described in the BVMS 10.0 - BIS connectivity guide.

Digital Monitor Wall (DMW) and Analogue Monitor Groups

In BVMS 10.0 the functionality offered by the Digital Monitor Wall and the Analogue Monitor Groups has been consolidated into the Monitor Groups. Analogue Monitor Groups are automatically migrated to the new Monitor Groups. It is strongly recommended for customers to move their Digital Monitor Wall configuration to the new Monitor Groups. The Digital Monitor Wall functionality will be removed from BVMS 11.0.

DIVAR IP AiO Upgrade

When upgrading a DIVAR IP AiO to BVMS 10.0, the following information should be taken into account:

TSG: Upgrading VRM from 32bit to 64bit on DIVAR IP causes Transcoder to stop functioning

3.2.4 BVMS 8.0

Server and Client scripts

BVMS 8.0 is the first 64-bit BVMS version. When external, 32-bit, DLLs are used these need to be replaced with their corresponding 64-bit versions. Please contact the DLL supplier for an updated 64-bit version.

4 Upgrading a BVMS system

4.1 Concepts and changes

4.1.1 Password Security

If in your previous BVMS version the password length for a user was configured to be >0, the **Strong password policy** option is automatically enabled for this user after the upgrade.

4.1.2 Compatibility mode

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.
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.

4.1.3 No touch deployment

As of BVMS 6.0 you can upgrade using 2 different ways when your system consists of multiple servers and workstations:

- Upgrade your BVMS Management Server computer first to allow Offline Client Operation (available since BVMS 3.0) and make use of No-Touch-Deployment for the workstations.
- Upgrade your workstations first to allow continued monitoring in compatibility mode with BVMS 5.5 servers or later.

When you plan to update all workstations and servers, but are not able to do this at once, following sequence is recommended:

1. Workstations: these will connect to the BVMS management server in compatibility mode.
2. Server: workstations that are not updated will be updated using no-touch deployment.

Note

The SNMP feature support is optional and required if you like to monitor network devices via SNMP. The feature can also be independently installed later in the Windows Components Settings if required.

4.1.4 Documentation

Documentation and software for Bosch Building Technologies products can be found in the on-line product catalogue as follows:

Go to the Bosch Building Technologies product catalogue > select your region and your country > start a search for your product > select the product in the search results to show the existing files.

Additional documentation (like this upgrade guide) can be found in the Bosch Building Technologies Community > Search for "BVMS".

4.1.5 Automated software deployment

The BVMS Deployment guide, published in an article on the Bosch Building Technologies Community, describes how the BVMS software can be automatically deployed using command-line arguments in combination with the setup package. Bosch recommends testing these mechanisms in your specific environment first.

4.2 Upgrade steps

The following components require upgrading, depending on the existing deployment of your system. It is recommended to follow the order presented in the list below.

1. Management Server
2. Video Recording Manager
3. Operator Client
4. Configuration Client
5. Video Streaming Gateway
6. Cameo SDK
7. Mobile Video Service
8. Person Identification Device (covered in separate documentation)

Updating takes up to 30 minutes depending on the installed features. The BVMS installation package can be downloaded from https://downloadstore.boschsecurity.com.

Patches

An overview of the latest patches can be found in the latest release notes, which are published in the Bosch Building Technologies Product Catalogue. Go to the Bosch Building Technologies product catalogue > select your region and your country > start a search for your product > select the product in the search results to show the existing files.

4.2.1 Upgrading the Management Server

Copy the BVMS installation package to the management server and start Setup.exe. Follow the steps presented in the installation wizard to upgrade the Management Server.

4.2.2 Upgrading the Video Recording Manager (VRM)

Copy the BVMS installation package to the management server and start Setup.exe. Follow the steps presented in the installation wizard to upgrade the Video Recording Manager.

> In some cases the VRM installation package is separated from the BVMS installation package. The first VRM needs to be installed from the BVMS installation package, upgrades can also be installed with the smaller VRM package which can also be found in the *ISSetupPrerequisites\VRM* folder in the BVMS installation zip file.

4.2.3 Upgrading Operator Client and Configuration Client

The upgrade task takes approximately 10 minutes per client.

The Operator Clients can be upgraded by the No Touch Deployment or manually upgrading by using the BVMS installation zip file. Additionally the Client installation package can be extracted from the Management Server once this has been upgraded. This is described in an article on the Bosch Building Technologies Community. This package can also be used for software deployment systems.

As soon as the program starts, the program compares the installed version with the version of its last server connection. The upgrade starts automatically. If .NET framework is installed during Setup, the upgrade task takes approximately 60 minutes per client, depending on the performance of the used computer. A computer restart is required during installation of .NET framework. After the restart the Setup continues as usual. No Touch Deployment only works on computers where Configuration Client and Operator Client are installed but no other BVMS components.

To run the No Touch Deployment, log on as an administrator. The No Touch Deployment updates both Operator Client and Configuration Client simultaneously if both are installed. The following registry key of an Operator Client computer shows the IP address of the last connected Management Server computer:

```
\HKEY_CURRENT_USER\Software\Bosch Sicherheitssysteme GmbH\LastConnection
```

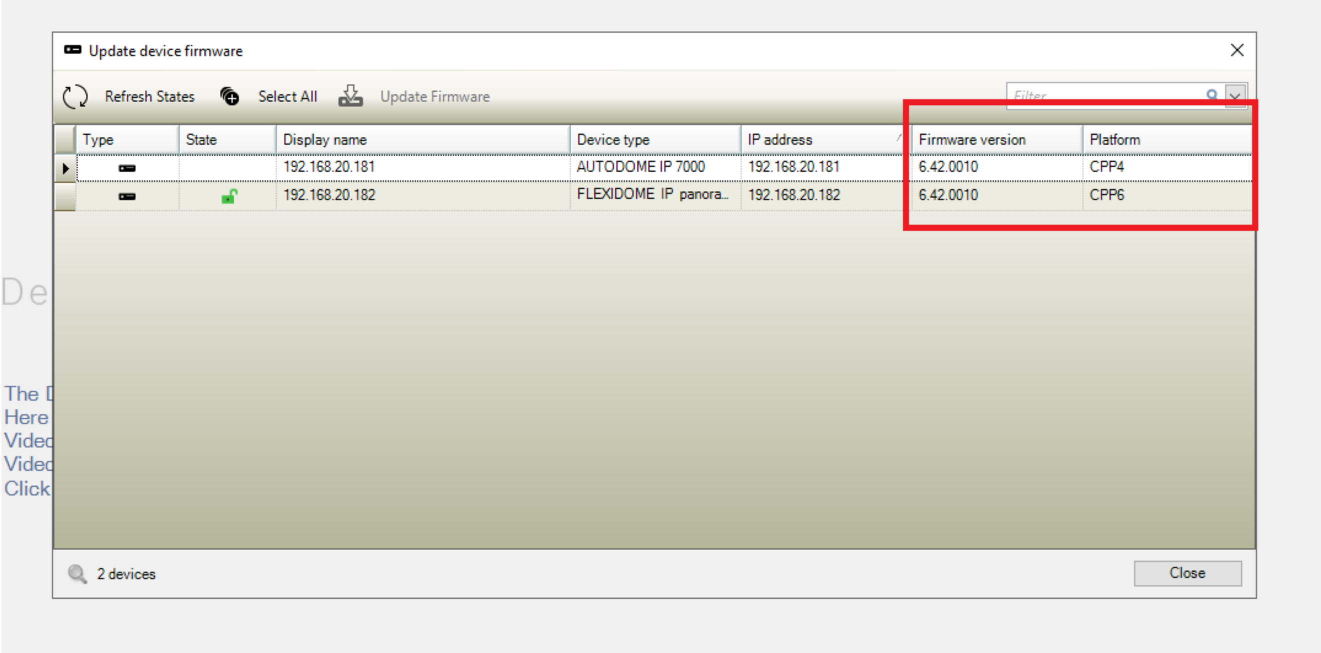
4.2.4 Upgrading encoder / decoder firmware

> **Notice!**
>
> Ensure that the firmware of your 3rd party cameras that are connected to your BVMS, is on the latest compatible version.

This task takes approximately 5 minutes per device. When updating devices in parallel, the time might increase depending on the network speed. The firmware upgrades are performed with the BVMS Configuration Client in the IP Device Configuration dialogue. The following steps describe the upgrade using BVMS Configuration Client.

1. On the **Hardware** menu, click **Update device Firmware**
2. Select one or more devices with left clicking on the grid. For a multi-select operation please hold the left mouse button and move the arrow down on the grid. You can also hold down the CTRL key while you click other devices that you want to select. The selected rows are highlighted in blue. We do not recommend selecting more than 20 devices per batch upgrade.
3. Click **Update Firmware**.

In BVMS 10.0 the update device firmware dialogue was enhanced with the firmware version and camera platform.



Type	State	Display name	Device type	IP address	Firmware version	Platform
		192.168.20.181	AUTODOME IP 7000	192.168.20.181	6.42.0010	CPP4
		192.168.20.182	FLEXIDOME IP panora...	192.168.20.182	6.42.0010	CPP6

If the combined firmware package is used, multiple devices can be selected for a parallel upgrade. The upgrade speed depends on the network infrastructure. The Open dialog box is displayed.

1. Select the appropriate firmware, for example vip_x_app1.fw. Then click **Open**. The **Firmware upload status** dialog box is displayed.
2. Click **Start**. Wait until the firmware upload of all devices is finished and the automatic reset of the updated devices is done. After that the status **Available** is displayed in the **Status** column. Then click **Close**

4.2.5 Upgrading the Video Streaming Gateway (VSG)

Copy the BVMS installation package to the management server and start Setup.exe. Follow the steps presented in the installation wizard to upgrade the Video Streaming Gateway.

In some cases the VSG installation package is separated from the BVMS installation package. The first VSG needs to be installed from the BVMS installation package, upgrades can also be installed with the smaller VSG package which can also be found in the *ISSetupPrerequisites\VSG* folder in the BVMS installation zip file.

4.2.6 Upgrading BIS-BVMS connectivity

When using a BIS-BVMS connection, the installation routine will reset the credentials for the authentication. Make sure that user and password is restored in the file Bosch.Vms.BISProxy.dll.config in the Management Server's %appdata% directory. Run:

```
…\<Program directory>\Bosch\VMS\bin\BoschVMSProxyFileInstaller.exe
```

The following files are copied into the Global Assembly Cache (GAC):

- Bosch.Vms.Core.FeatureSupportInterface.dll
- Bosch.Vms.Core.IUserAuthenticationService.dll

You can check the GAC in C:\Windows\Microsoft.NET\assembly\GAC_32

4.3 Finalizing and confirming the upgrade

We recommend performing the following tasks after the upgrade:

Check	Description
	Ensure that all workstations (Operator Client) with alarm handling are updated.
	Adjust time server settings (protocol, IP address), if required. BVMS supports SNTP.
	Check that all workstations with alarm handling are upgraded because newer software versions connected in Compatibility Mode to the Management Server offer only video monitoring.
	Check correct time synchronization on all devices. Check time zone settings if required.
	Check reference images on encoders.
	Reinstall special protocols if required.
	Check recording status.
	Check playback.
	Check live images.
	Check IntuiKey keyboards and AMGs. Can you log on and control?
	Check IVA settings and alarms.
	Check multicast settings and confirm the correct function.
	Check Logbook.
	Check alarms.
	Check Favorites, Bookmarks and user preferences.
	Check operation of inputs (Compatibility Mode).
	Check recording preferences settings of encoders.
	Check SNMP traps.
	Check custom scripts.
	Check and adjust the load balancing settings of the iSCSI disk arrays.
	Optionally check the BIS-BVMS connection.

5 Software development kits

BVMS offers two software development kits (SDKs):

- CameoSDK: this SDK can be used to build an "Operator Client" and handles events and video.
- BVMS SDK: this SDK can be used for events, alarms and commands.

5.1 Upgrading BVMS CameoSDK

CameoSDK

If a BVMS upgrade is done, the application using the CameoSDK should be re-compiled together with the correct CameoSDK version.

Example: you have created a CameoSDK application in the past based on CameoSDK of BVMS 5.5. The customer now wants to upgrade to BVMS 7.5.

1. Recompile your CameoSDK application against the CameoSDK of BVMS 7.5.
2. Deploy the newly compiled CameoSDK application on the customer PC(s).

5.2 Upgrading BVMS Software Development Kit

This chapter provides information on upgrading BVMS SDK. Although the BVMS SDK is a pure command SDK (which offers no streaming video functionality), and is downwards compatible, it is strongly recommended to use the BVMS SDK version found in the BVMS installation directory to match the version between the SDK and other BVMS components.

External DLLs

BVMS 8.0 is the first 64-bit BVMS version. When external, 32-bit, DLLs are used these need to be replaced with their corresponding 64-bit versions. Please contact the DLL supplier for an updated 64-bit version.

6 Migration of a BVMS system

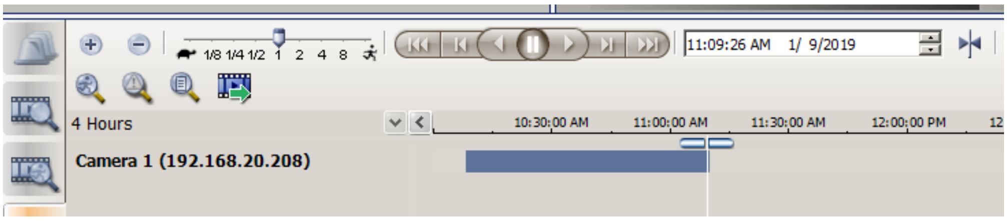
Next to an upgrade, it is sometimes required to migrate an entire system to new hardware and/or a new operating system. An example could be when an upgrade from BVMS 6.5 to BVMS 9.0 is planned, which would require the operating systems to be upgraded as well. Depending on the size and complexity of the system, it is recommended to plan the migration extensively and (optionally) set-up a test environment to test the migration on a small test-system.

6.1 Migration of Management Server and VRM

The process below was tested using a BVMS 7.0 system as existing system and a BVMS 9.0 system as new system. The BVMS 7.0 system was running on Windows Server 2008 R2 and the BVMS 9.0 was running on Windows Server 2016. A single camera was connected to this system, configured to record continuously. The steps below assume the iSCSI targets are not migrated. If this is required as well, it is highly recommended to split these tasks conceptually.

> If something goes wrong during this process, the new system can be disconnected from the network and the old system can be re-connected, which will restore the previous state of the system.

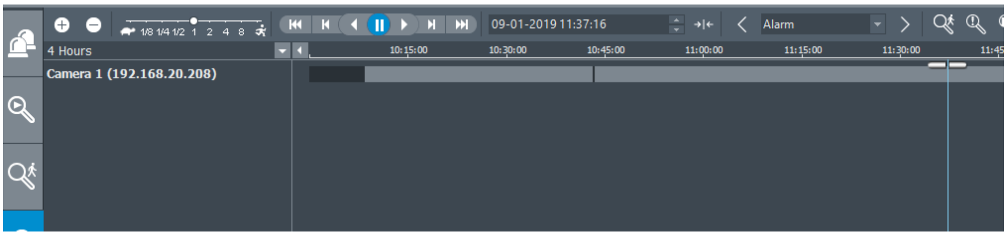
The image below shows the timeline of the existing system (BVMS 7.0) before the migration steps where initiated.



In general, the following generic procedure is recommended.

1. Install the new system next to the old system. The BVMS system components (mainly the management server and video recording manager) could be deployed with brand-new IP addresses to make it possible for both the old system and new system to run in the same network. It is recommended to activate the licenses of the new system before continuing to the next step.
2. Check the VRM downtime configuration for all configured pools. The minimum configuration is set to 1 day, this means that the cameras will continue to record even when the VRM is down for an entire day. This functionality is used to ensure the recording continues while the system is migrated.
3. Export the configuration from the existing system. After the export the configuration on the existing system should not be changed!
4. Shutdown the existing VRM server (either by stopping the VRM services or shutting down the system itself).
5. Import the configuration in the new system. The configuration client will restart and will ask you to log-in again. Login to the configuration client by using the username and password of the **new** system, configured when the license was activated.
6. Change the IP address of the configured VRM(s): right click the **VRM**, **Edit device**. Ensure that the connectivity between the new VRM and new Management Server is working properly. Check if the devices (cameras as well as iSCSI targets) configured in the VRM pools match the configuration of the old system.
7. Shutdown the existing BVMS Management Server (either by stopping the BVMS services or shutting down the system itself).
8. Save and activate the configuration on the new system. The configuration client is restarted again. Login to the configuration client by using the username and password of the **old** system. If necessary, adjust the username and password of the administrative users to increase the level of security.
9. Check an arbitrary number of devices on their recording state in the Configuration Client. These devices should now be managed by the new VRM.
10. Open the Operator Client and check the recording state and timeline of an arbitrary number of devices.

The image below show the timeline of the new system (BVMS 9.0) after the migration steps where finalized. As you can see, the existing recordings are available in the new system.



Small recording gap

When the default BVMS time-server is used, the change of management server might cause a small recording gap due to the potential difference in time between the existing management server and the new management server. In order to reduce the gap (and possible prevent it) it is highly recommended to ensure a proper time synchronisation between the existing management server and the new management server.

6.2 Migration of iSCSI targets

When an iSCSI device is out of service, it is recommended to replace this device. Before changing any settings, the new device(s) should be added to the configuration and functioning as expected. The configuration manager (this is unfortunately not possible in the BVMS Configuration Client) allows to set a read-only property on the LUN. Once this is set, the available blocks on the LUN will not be distributed to the devices, which will prevent new video from being recorded on the specific LUN, while the recorded video is still available. Once the configured retention time has passed, the video recorded on the specific LUN will not be available and the device can be shutdown.

6.3 Migration of logbook

The BVMS logbook contains important information as well. This can be migrated from one server to another, even when the servers contain different BVMS versions. The following steps should be executed:

1. Stop BVMS Services on **old** server.
2. Stop SQL service on **old** server.
3. Copy the database files file from the **old** server (MDF and LDF, located in C:\Programdata\Bosch\VMS\DB).
4. *Optional (start BVMS and SQL services on old services to be up and running again)*
5. Stop BVMS Services on **new** server.
6. Stop SQL service on **new** server.
7. Replace mdf and ldf on **new** server with old files (in the same directory on the new server: C:\Programdata\Bosch\VMS\DB).
8. Start SQL service on **new** server.
9. Run “DBLogbookMigrator.exe” located in the bin directory of the **new** server installation (If necessary the database schema will be migrated to the required one).
10. Start BVMS Services on **new** server.

6.4 Migration of user settings

The user-settings can be exported and migrated to a new system using the following steps.

Please note that, currently, the export mechanisms provided in the BVMS Configuration Client do not export the user-data. This is a known problem and being worked on. Until then this work-around should be applied

1. Stop the BVMS Central Server service on the existing server from the Windows task manager or Services overview.
2. Stop the BVMS Central Server service on the new server from the Windows task manager or Services overview.
3. Copy the contents of the directory C:\programdata\Bosch\VMS\UserData on the existing server to the same directory on the new server (via the network or other media).
4. Copy the "elements.bvms" file located in the directory C:\programdata\Bosch\VMS\ on the existing server to the same location on the new server (via the network or other media).

5. Start the BVMS Central Server service on the new server from the Windows task manager or Services overview.

6.5 Migration of VSG

The Video Streaming Gateway (VSG) can be migrated from one server to another without losing access to the recorded video. This can be achieved using one of two scenarios: 1) the IP address of the server will **not be changed** or 2) the IP address of the server **will be changed**.

> When the VSG IP address needs to be changed, the old recordings will not be available.

New server IP address is same as the existing server

1. Stop the VSG services (for all instances) on the existing server.
2. Copy the whole VSG folder located in *C:\ProgramData\Bosch\* from the existing server to the new server.
3. Remove the IP address from the existing server and configure the IP address the new server.
4. Start the VSG services (for all instances) on the new server.

Previous recordings should be available and VSG will continue recording.

New server IP address has changed

1. Stop the VSG services (for all instances) on the existing server.
2. *Copy the whole VSG folder located in C:\ProgramData\Bosch\ from the existing server to the new server.*
3. Launch BVMS Configuration Client, go to edit dialogue of VSG and change the IP address to the IP address of the new server.
4. Activate the BVMS changes.
5. Start VSG and VRM services on the new server.

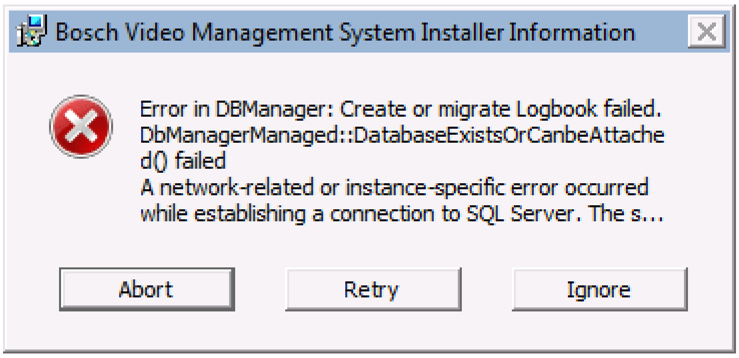
Previous recordings are **not** available and VSG will continue recording.

7 Troubleshooting

If you import a configuration file with an earlier version in BVMS with the current version, you must activate the new configuration and restart the BVMS Central Server service. Otherwise new BVMS events that were added since that earlier version are not available.

7.1 Setup

During Setup an error message can be displayed with the message text cut:



Bosch Video Management System Installer Information

Error in DBManager: Create or migrate Logbook failed.
DbManagerManaged::DatabaseExistsOrCanbeAttache
d() failed
A network-related or instance-specific error occurred
while establishing a connection to SQL Server. The s...

This error message may be displayed when your SQL server is busy or not available. Perform one of the following steps to solve the issue:

- Click Retry to **retry** the migration of your Logbook database after addressing possible causes.

A possible reason is that the SQL Instance **BVMS** is not started. Please check in **Control Panel** > **Administrative Tools** > **Services** if the **SQL Instance BVMS** is started, and start if necessary. Then click **Retry**.

or

- Press **Ignore** to continue the Setup without migrating your logbook. You possibly do not have access to your logbook.

or

- If your logbook fails because it was not migrated, you can restart Setup later in Repair mode to repeat the migration.

or

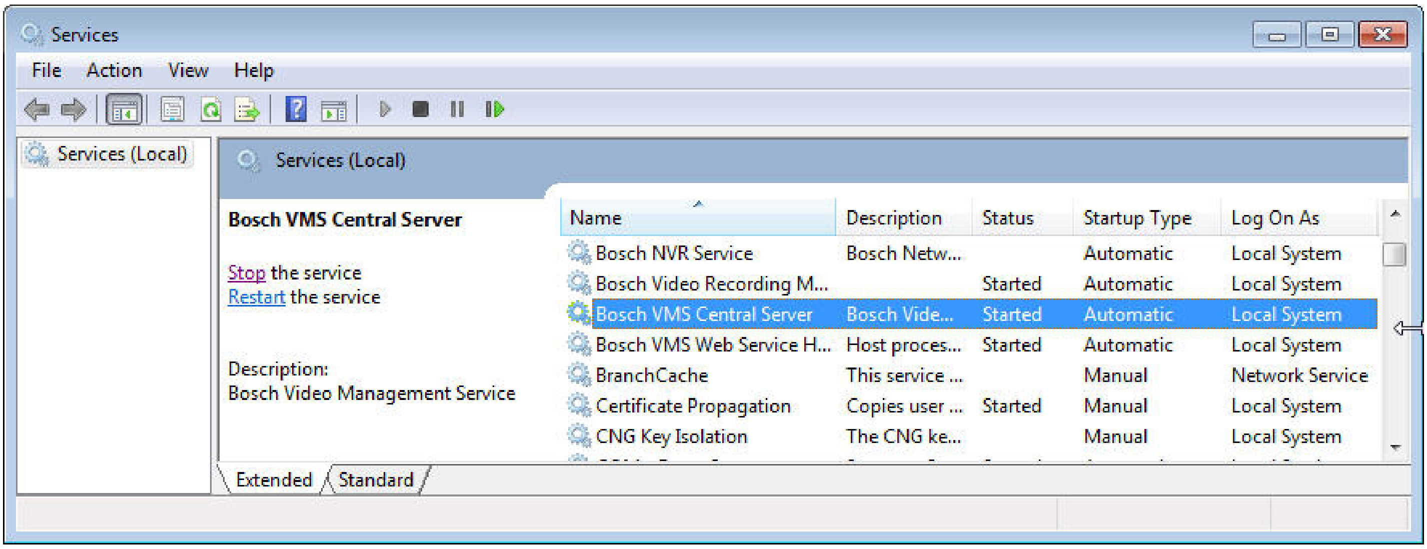
- Press **Cancel** to abort the BVMS installation.

You can restart Setup later. Your current Logbook and custom data is retained.

7.2 System services

If after installation and restart, in the logon dialog the Management Server is not displayed as online:

- Check whether the installed services (BVMS Central Server and Bosch Video Recording Manager) are started: On the **Start** menu, click **Control Panel**, double-click **AdministrativeTools**, and then double-click **Services**.

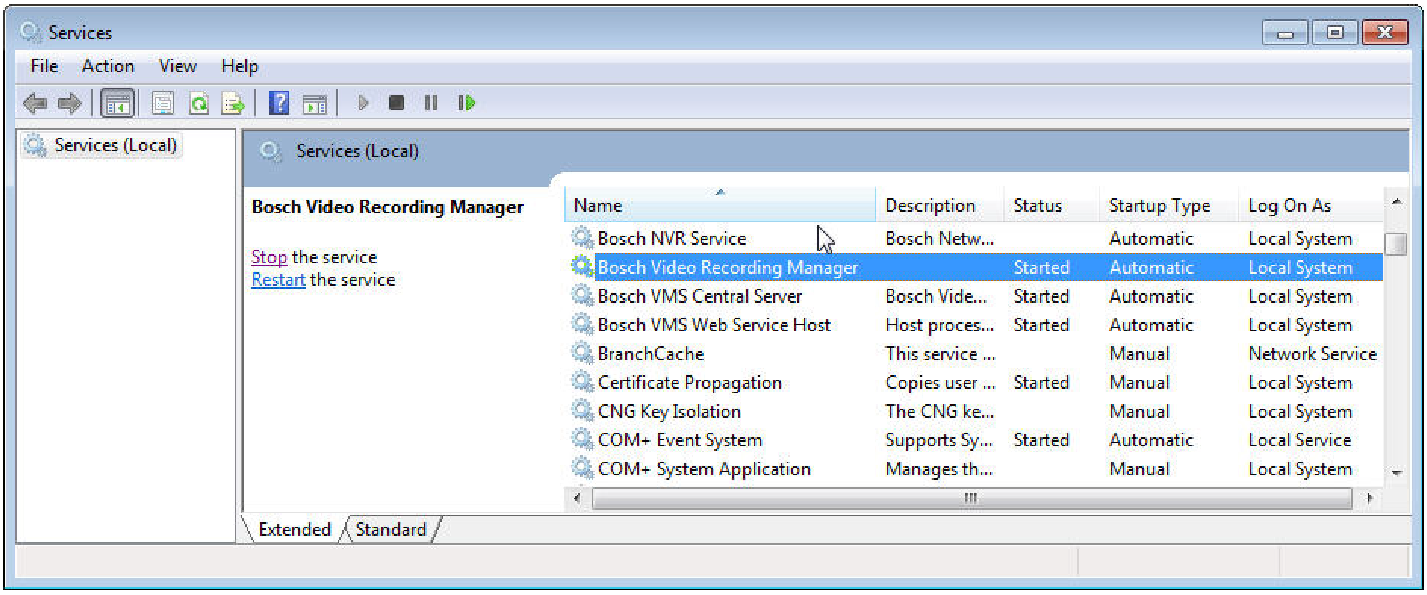


Bosch VMS Central Server

Stop the service
Restart the service

Description:
Bosch Video Management Service

Name	Description	Status	Startup Type	Log On As
Bosch NVR Service	Bosch Netw...		Automatic	Local System
Bosch Video Recording M...		Started	Automatic	Local System
Bosch VMS Central Server	Bosch Vide...	Started	Automatic	Local System
Bosch VMS Web Service H...	Host proces...	Started	Automatic	Local System
BranchCache	This service ...		Manual	Network Service
Certificate Propagation	Copies user ...	Started	Manual	Local System
CNG Key Isolation	The CNG ke...		Manual	Local System



Bosch Video Recording Manager

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Bosch NVR Service	Bosch Netw...		Automatic	Local System
Bosch Video Recording Manager		Started	Automatic	Local System
Bosch VMS Central Server	Bosch Vide...	Started	Automatic	Local System
Bosch VMS Web Service Host	Host proces...	Started	Automatic	Local System
BranchCache	This service ...		Manual	Network Service
Certificate Propagation	Copies user ...	Started	Manual	Local System
CNG Key Isolation	The CNG ke...		Manual	Local System
COM+ Event System	Supports Sy...	Started	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local System

Note that the BVMS Web Service Host must also be started. Only for Management Server and NVR Server: If the service is not listed, start the command prompt, run <Install Directory>\bin\serviceinstaller.exe. If installation fails, see the logfile: bvms.log.

Client-Server certificates are installed that are also used by Mobile Video Service.