BOSCH
Invented for life

# BVMS 11.1.1 - Upgrade and Migration

Author: Wrobel Maciej (BT-VS/XSW-SEC)
Date: 5 August, 2022

# 1 Document information

| | |
|---|---|
| Project | BVMS 11.1.1 |
| Reference | Upgrade guide |

## 1.1 Version history

| Date | Description |
|---|---|
| 2022-06-02 | Initial release for BVMS 11.1.1 |

# 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 10.1 (launched in December 2020) to BVMS 11.1.1 (launched in June 2022) no additional step is needed. However, when you want to upgrade from BVMS 10.0 to BVMS 11.1.1 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. You can find the exact release dates in the software service and support documentation.

# 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.<br>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.<br>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.<br>Otherwise the SQLDB migration for the logbook will fail. If the host name of the Management Server has changed, change the following registry key:<br>`[HKEY_LOCAL_MACHINE\SOFTWARE\BVMS\Installer\SelectedValues]"LOGBOOKDB_SERVER"="<hostname>\BVMS"`<br>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 11.1.1

### Colored Timeline

BVMS 11.1.1 supports timeline coloring for recording triggered by motion and alarms. How useful this coloring scheme is for you may vary with your use cases. Also the new coloring scheme may appear to be confusing. Therefore the timeline colors are switched off by default. To enable timeline coloring in the Operator Client, go to the User Settings dialog and enable the corresponding setting.

### SRTP for camera platforms CPP13/14

BVMS enables secure UDP streaming for camera platforms CPP 13 and CPP 14. If this setting is used with firmware 8.45.0017 or lower (**CPP13**), 8.30.0082 or lower (**CPP14.1**), 8.50.0138 or lower (**CPP14.2**) the devices will start streaming multicast even if multicast has not been configured on the device itself. If your network is not set up properly for multicast this may cause issues. In these cases it is recommended to switch to TCP live streaming for secured communication environments until new firmwares have been released for the affected device types.

## 3.2.2 BVMS 11.1

### Removed functionality

We have removed the following functionality from BVMS 11.1:

1. Routed access: It is no longer supported to directly map ports in your router in order to provide external access to your devices. Instead, use SSH support (see manual for a description)

## Tracking and Recognition Service (TRS)

Full Person Identification functionality for BVMS 11.1 is only offered with TRS 3.0. If Person Identification was used in BVMS 11.0 (or older), please make sure to update TRS to version 3.0 **before** upgrading BVMS to version 11.1.

## Licensing

| | BVMS <=11.0 | BVMS > 11.0 |
|---|---|---|
| Encoder < CPP7.3 (VRM, Live only, Local Storage, Failover, Secondary) | channel count | channel count |
| Encoder >= CPP7.3 (VRM, Live only, Local Storage, Failover, Secondary) | channel count | encoder count |
| Onvif cameras (Bosch & 3rd party) (Live only, VSG) | channel count | encoder count |
| VSG Bosch cameras < CPP7.3 | channel count | channel count |
| VSG Bosch cameras >= CPP7.3 | channel count | encoder count |
| VSG Jpeg cameras | channel count | channel count |
| VSG RTSP cameras | channel count | channel count |

For BVMS 11.1 the license counting for multichannel encoders was changed as depicted in the following table.

This means that for devices falling into a category with **encoder count** in the **BVMS > 11.0** section, only one channel license is counted for the whole encoder respectively VSG device.

## Video Recording Manager (VRM)

For BVMS 11.1 the VRM needs to be updated to version 4.02. Previous versions have not been tested in combination with BVMS 11.1 and may not work as expected.

## CPP13/CPP14 device support

- If you already have CPP13 or CPP14 cameras configured, you need to run the update device capabilities in the Configuration Client to bring the system up-to-date.
  Also make sure to check the camera and recording settings in the Configuration Client to see if the settings are matching.
- A configuration that relies on streams being switched for recording is not supported for CPP13 and CPP14 cameras.
- CPP13 and CPP14 cameras have a new feature that automatically lowers the frame rates of streams to avoid overload scenarios. BVMS has no influence on this. Please refer to the camera documentation

## Divar IP (DIP-52, DIP-71, DIP-72)

In contrast to previous releases the Divar IP models DIP-52, DIP-71 and DIP-72 can be updated by purely running the BVMS intallation. An additional DIP installer package is not needed. For DIP-73 the Device Management component is responsible of performing the update.

# 3.2.3 BVMS 11.0

## Removed functionality

We have removed the following functionality from BVMS 11.0:

1. Map migration: if you're upgrading BVMS 8.0 or older to BVMS 11.0, you should upgrade to at least one version (for example, BVMS 9.0) in between 8.0 and 11.0 to migrate you maps to a new dataformat.
2. SMS gateway: The SMS gateway is no longer supported. In concrete it is not possible any longer to cause an event to trigger the sending of an SMS. Also the corresponding functionality has been marked as obsolete in the SDKs and will not work anymore.
3. The Digital Monitor Wall control has been removed and can no longer be displayed in the Operator Client. Use Monitor Groups instead. Previously configured DMW will be lost after upgrading to BVMS 11.0, therefore please make sure to finish migration to MG before upgrading.

For a comparison between the feature sets of the Digital Monitor Wall and the Monitor Groups, please refer to System Design Guide.

4. Protection Inspection Service: The Protection Inspection Service has been removed.
5. ASF export: Video export in the ASF format is not longer possible. SDK methods are marked as obsolete. Calling these methods will create a MOV or MP4 exports instead of ASF, depending on the method.
6. DiBos/BRS: The DiBos and Bosch Recording Station integration into BVMS is no longer supported. You will not be able to connect to such devices, especially you cannot view video streams or archives.

## Video Recording Manager (VRM)

For BVMS 11.0 the VRM needs to be updated to version 4.00. The Operator Client can only connect to an older VRM in backwards compatibility mode if the VRM is configured as part of an older BVMS. Do not operate a VRM < version 4.00 that is configured at a system running BVMS 11.0.

With BVMS 11.0 installation no firewall rules are included to open RCP+ ports 1756 and 1757 for VRM connection, as secured connection is preferred by default. If needed to still use RCP+ ports, firewall has to be configured manually.

## SDKs

The Server and Client SDKs have been rectified in their error handling behaviour. Especially with respect to permission handling methods may now throw an SDK exception in case of missing permissions of the caller. Please check the SDK documentation for details on each method.

## XmlConfigurationEncryption tool (BIS integration)

If you are using the XmlConfigurationEncryption tool to edit configuration files like for the BVMS/BIS integration, you need to create an unencrypted copy of the corresponding configuration file before updating to BVMS 11.0. For better security the underlying encryption mechanism of the XmlConfigurationEncryption tool has been changed for BVMS 11.0 which prevents it from being able to decrypt configuration files created with previous versions of the tool.

In order to migrate your BIS configuration file (or other file managed through the XmlConfigurationEncryption tool), proceed as described in the following steps:

1. Before updating to BVMS 11.0, open the corresponding configuration file with the current version of XmlConfigurationEncryption.exe. Copy the readable configuration data to another file and save this file.
2. Remove the original, encrypted configuration file (.cxml).
3. Update to BVMS 11.0.
4. The automatically generated new configuration file can be opened with XmlConfigurationEncryption. Paste the configuration data from the unencrypted backup file into the XmlConfigurationEncryption tool and save the configuration file.

The migration is now complete and the configuration file can now be edited with the XmlConfigurationEncryption tool as before.
Hint: For security reasons you should keep the unencrypted copy of the configuration data at a safe place.

## Licensing

After updating the BVMS system to BVMS 11, the software licenses have to be migrated from the Bosch Software License Manager System to Bosch Remote Portal

# 4 Upgrade with Software Assurance PRO to BVMS 11.0

## 4.1 Introduction

This document describes how you can migrate existing activated BVMS licenses from the Bosch Software License Manager System (SLMS) licensing system to the new Bosch Remote Portal licensing.

In general only systems with a valid Software Assurance (SMA) PRO can upgrade to the next BVMS version. You can check the software assurance status in the SLMS system. In case the software assurance is expired, order an SMA expansion for your system.

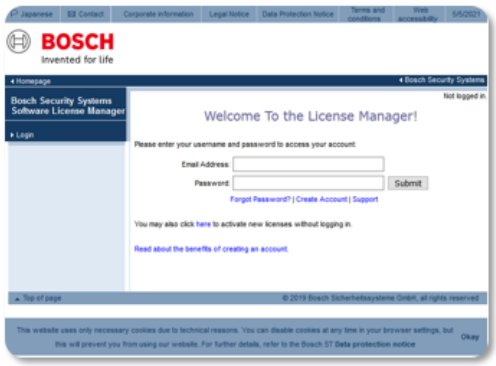
**Note:**

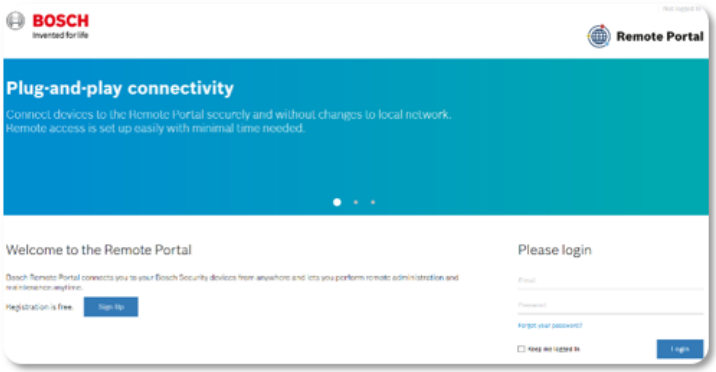
With the new licensing technology in BVMS 11.0, BVMS uses a new algorithm to create the unique identifier of the system. This identifier is called "fingerprint". Because of the new algorithm to generate the unique identifier, you can not upgrade the licenses directly with the upgrade process. The upgrade process generates a new software order ID that you have to activate manually in the Remote Portal together with the new unique identifier.

## 4.2 Glossary

Changes in the terms for licensing:

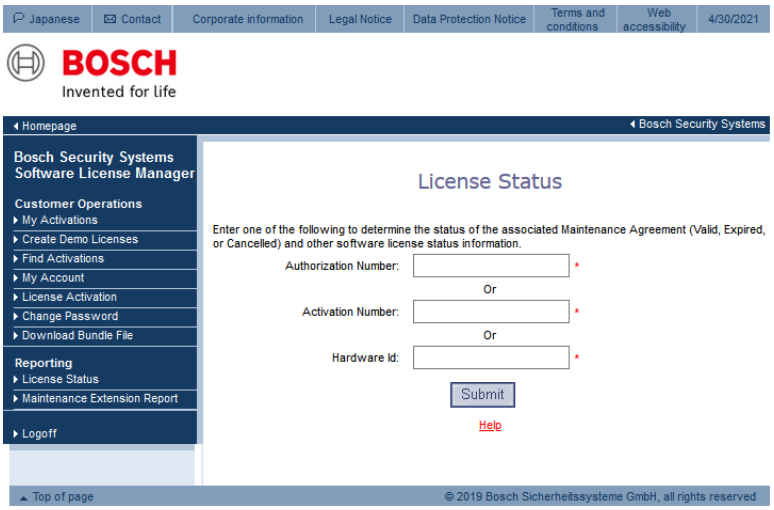
| Bosch Software License Manager | | Bosch Remote Portal |
|---|---|---|
| Authorization number | → | **Software Order ID** |
| Computer Signature / Hardware ID | → | **System Fingerprint** |
| Computer Signature / Hardware ID | → | **System Info File** |
| Activation Key | → | **Activation File** |

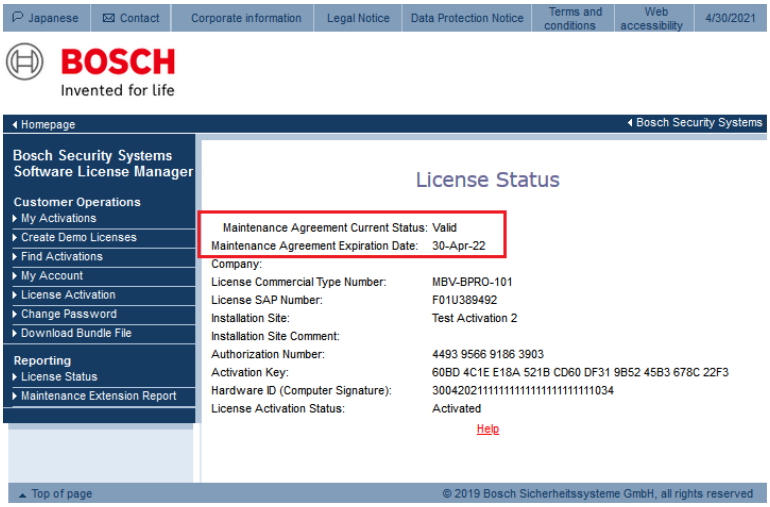


# 4.3 Check software assurance status in the Bosch Software License Manager System (SLMS)

To check the software assurance status of the system in SLMS, open the **License Status** page in SLMS and enter either the **Authorization Number**, **Activation Number** or **Hardware Id**.

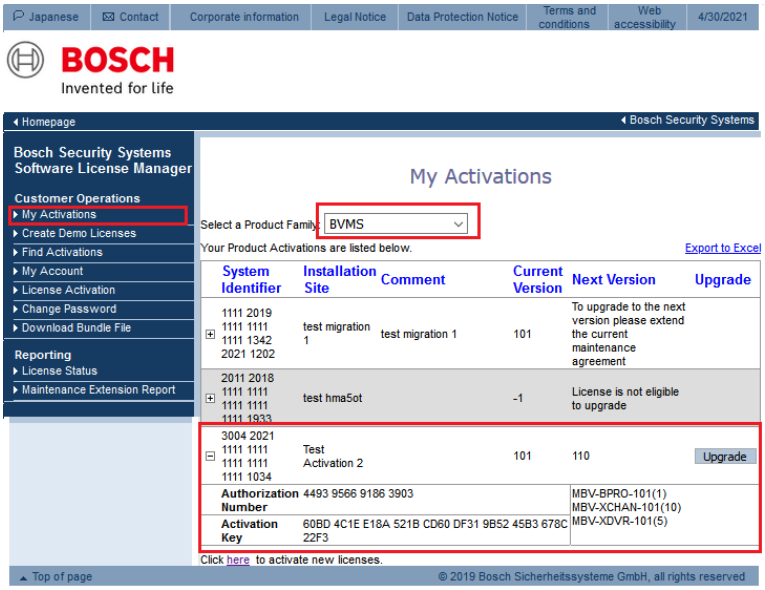



If the system has a valid software assurance status until the official release date of BVMS 11.0, you can upgrade the system to BVMS 11.0!

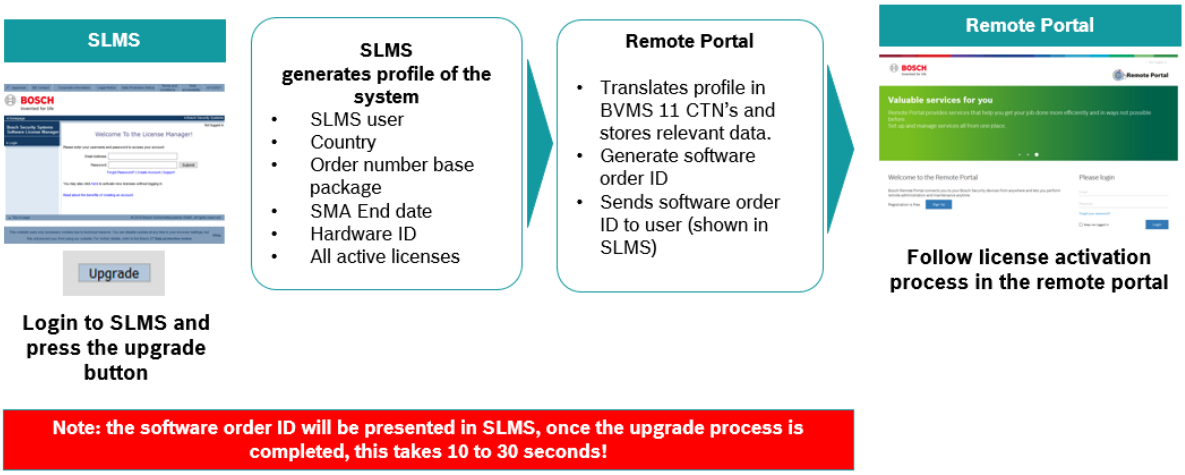
# 4.4 Upgrade license to BVMS 11.0

To start the upgrade process to BVMS 11.0, search for the system under **My Activations**:




If a system is entitled to upgrade to the next BVMS version, the **Upgrade** button is available. In this example the red marked system has a valid maintenance agreement to upgrade to BVMS 11.0. The other systems are not allowed to upgrade to BVMS 11.0.

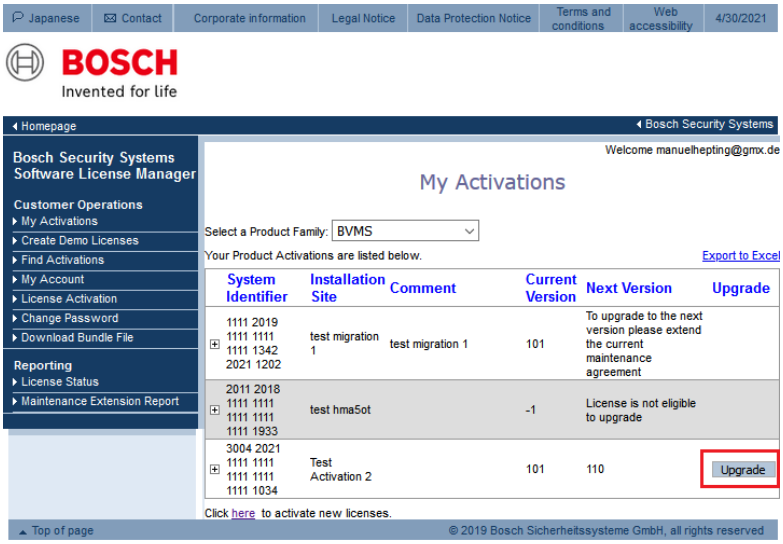
When you click the **Upgrade** button, the migration process of the license from SLMS to Remote Portal starts.



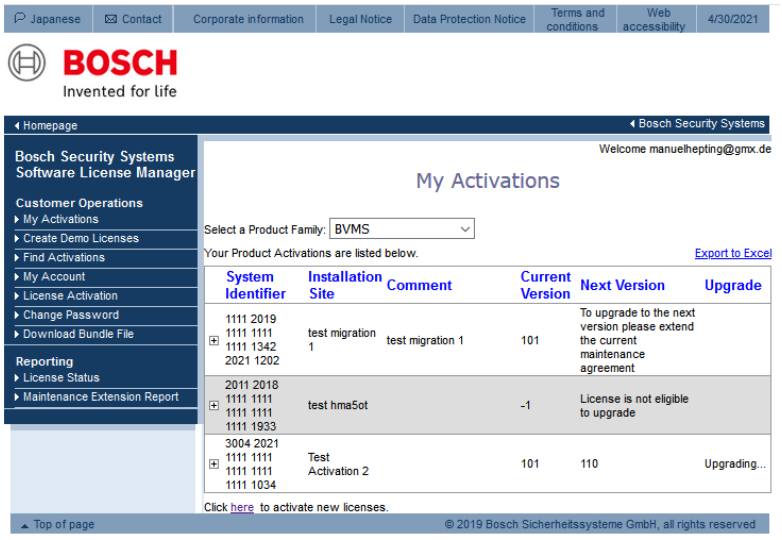

**Note: the software order ID will be presented in SLMS, once the upgrade process is completed, this takes 10 to 30 seconds!**

# 4.5 Start the upgrade process

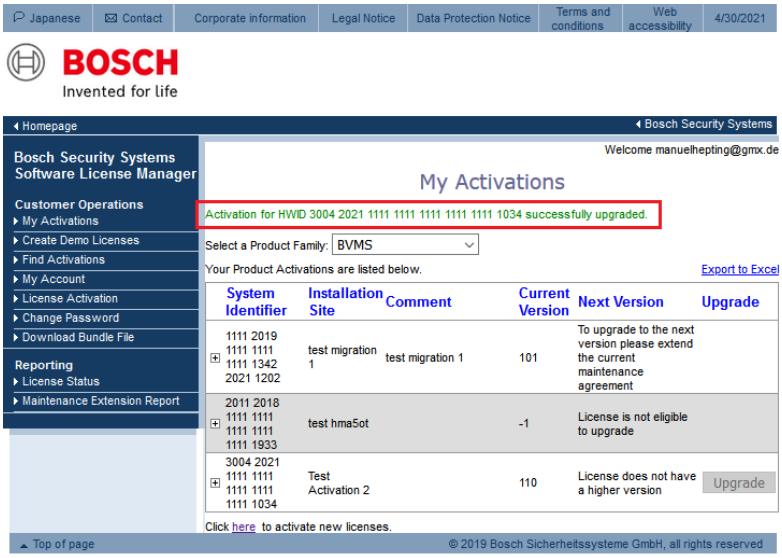
In order to start the upgrade process, click the **Upgrade** button of the system:



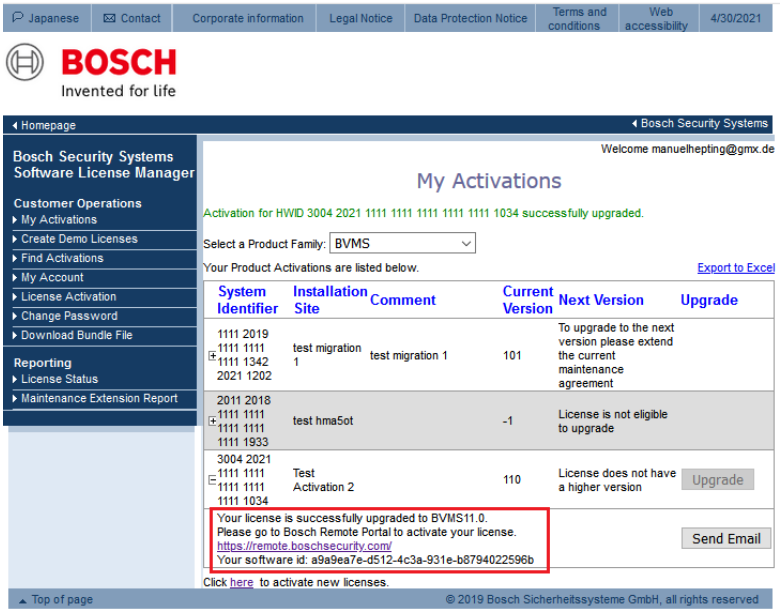

The SLMS system starts the upgrade process. During collecting data and creating the software order ID, the system displays **Upgrading...**.



Once the upgrade is finished, the system displays the following information:




When you click **+** next to the hardware ID, you see the software order ID:




In order to activate the BVMS 11.0 license, copy the software order ID and start the activation process in Bosch Remote Portal.

## 4.6 Data transfer from the Bosch Software License Manager System to the Bosch Remote Portal

During the license upgrade from BVMS 10.1 to BVMS 11.0, the license migrates from the SLMS system to the Remote Portal system. The following data transfers from the SLMS System to the Remote Portal system:

- All active licenses on the computer signature
- Software assurance end date
- Assigned country to the SLMS user ID

Not visible for users, only transferred for documentation reason:

- The old unique identifier of the BVMS system, called computer signature
- User ID of the SLMS user that requests the migration
- Order number of the base package

# 5 BVMS initial license activation

**Introduction**

This section describes the initial license activation process of BVMS licenses.

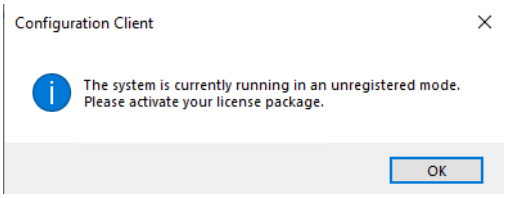
Follow these steps:

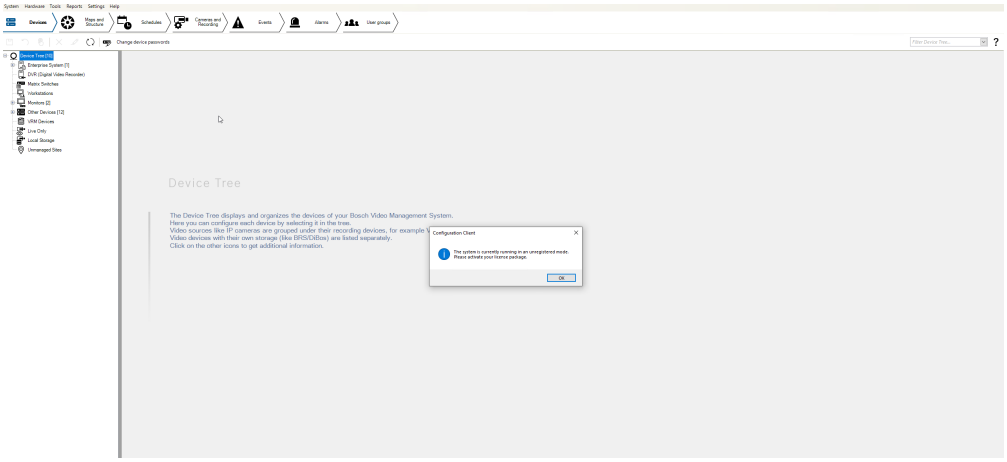
- Collect system info file from the BVMS system
- Claim ownership of the software order ID in the Remote Portal
- Activate the software order ID with the system info file in Remote Portal and download the activation file
- Add the activation file to the BVMS system to enable the software

**How to get started**

Open your BVMS Configuration Client application and sign in with the BVMS administrator user account.

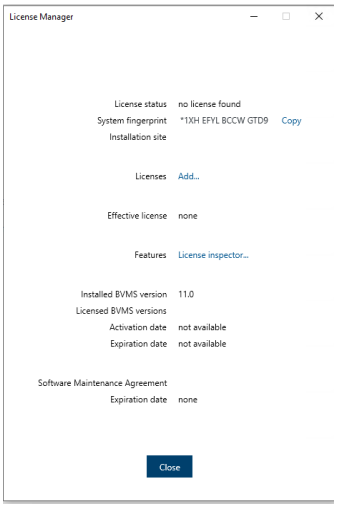
After you successfully logged in, you see the following BVMS message. It tells you that the system is currently running in an unregistered mode and that you have to activate your license package.




Directly click on **OK**. Since you want to initially activate a license, the license status is “not activated”.

## Activate a license




To obtain an active license you need to execute the following steps:

### Step 1: Click Add... to enter the Add license dialog

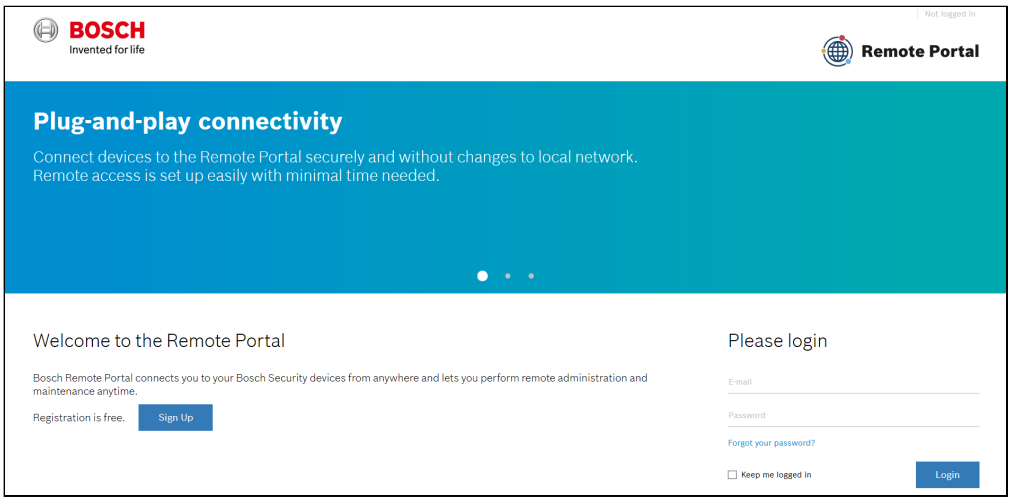
### Step 2: Save your system info to a file

Click the **Save** button and a file with the system info is created. Safe the system info file on your computer.

**Note:** If you do not have internet access on the computer where your BVMS application is installed, transfer the system info file to a computer with internet connection.

### Step 3: Go to remote.boschsecurity.com to generate your activation file

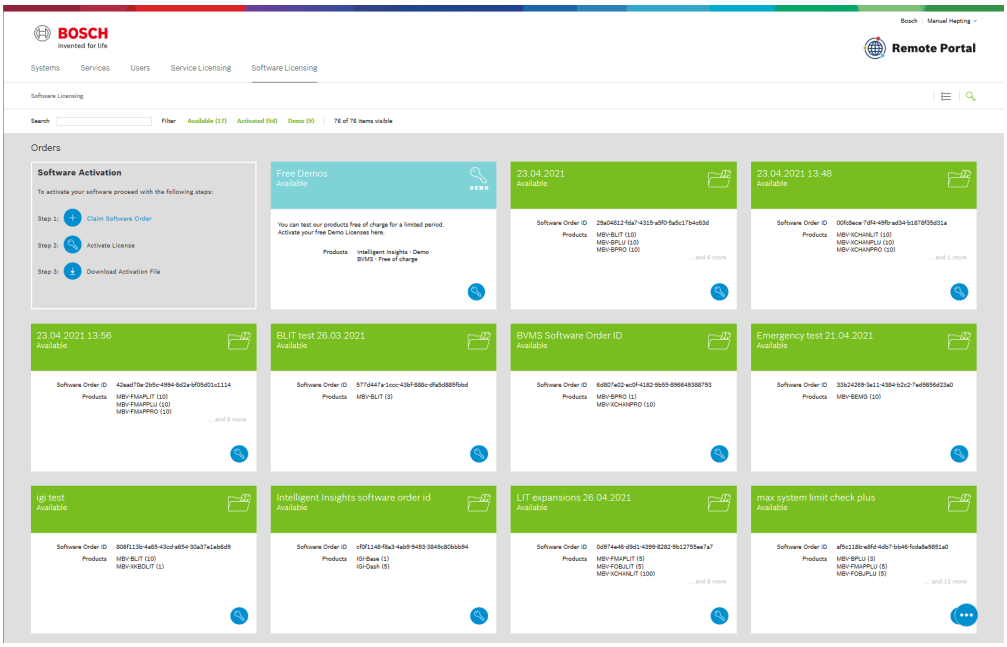
Click the link and the Bosch Remote Portal website displays. You can either sign up or login in case you already have a user account.




In case of an initial user account creation, please click **Sign Up**, fill in the required information and select the terms of agreement check boxes. After your account is successfully created, you can login to the Bosch Remote Portal.

**Step 4: Follow the instructions on** remote.boschsecurity.com/softwarelicensing **to generate your activation file by uploading your system info.**

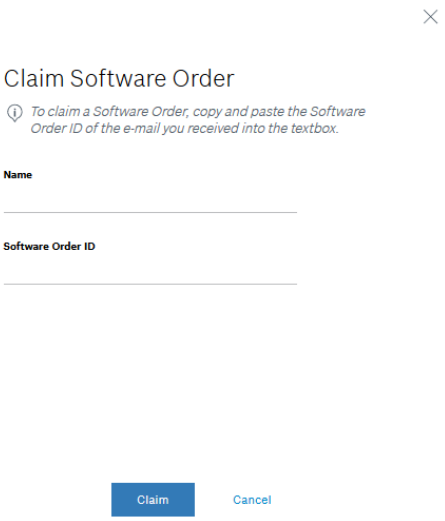
Click the link in **Step 3** or directly go to the **Software Licensing** tab in the Remote Portal toolbar. The following screen displays:




**Step 5: Claim the ownership of the software order ID in Remote Portal**

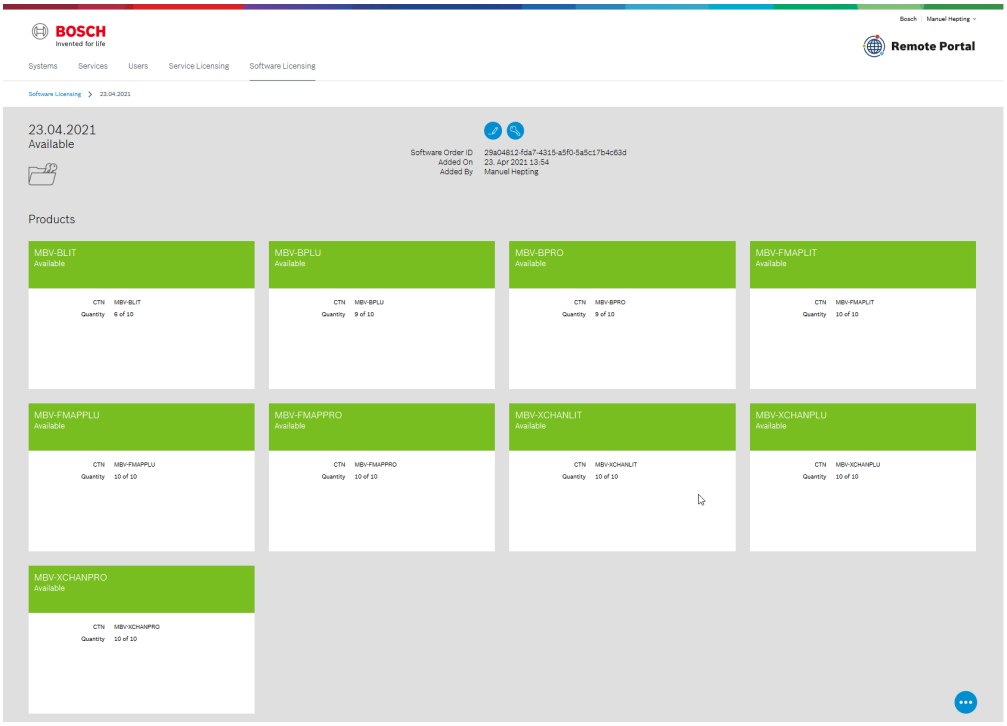
The software order ID can be obtained by placing a software order or by a upgrading a license from the Bosch Software License Manager System.

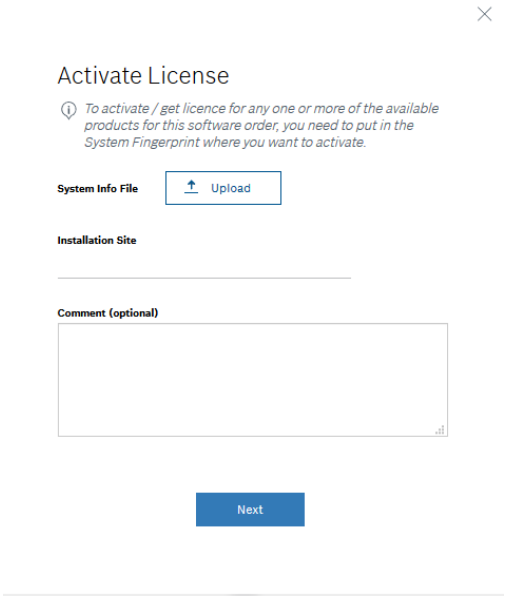
In order to claim the ownership of the software order ID, click **Claim Software Order** in the bottom right corner of the display. The **Claim Software Order** window displays. Click **Claim**.



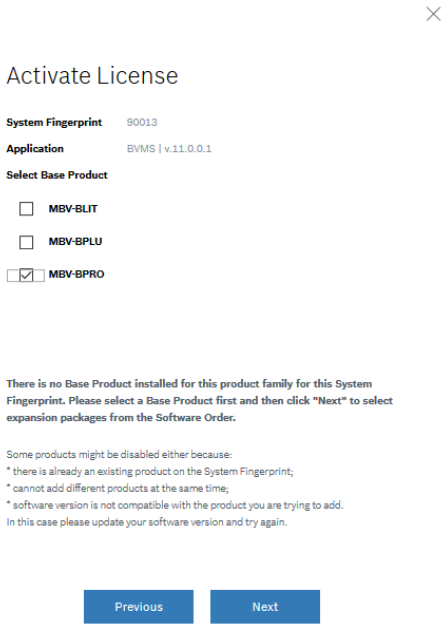
### Step 6: Activate a license

In order to activate a license, click **Activate License** in the bottom right corner of the display. The **Activate License** window opens. Upload the system info file that you saved earlier and fill in the required information.

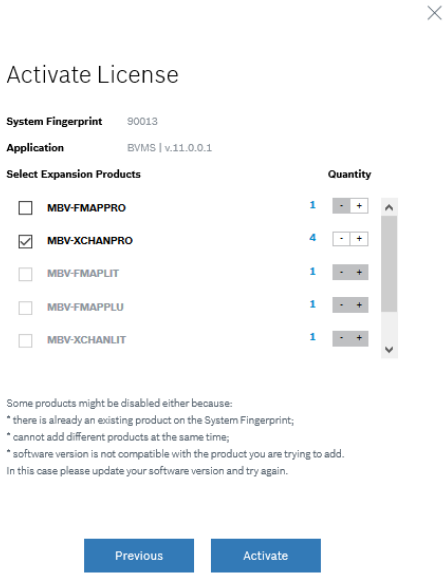


Select the base package to activate it:



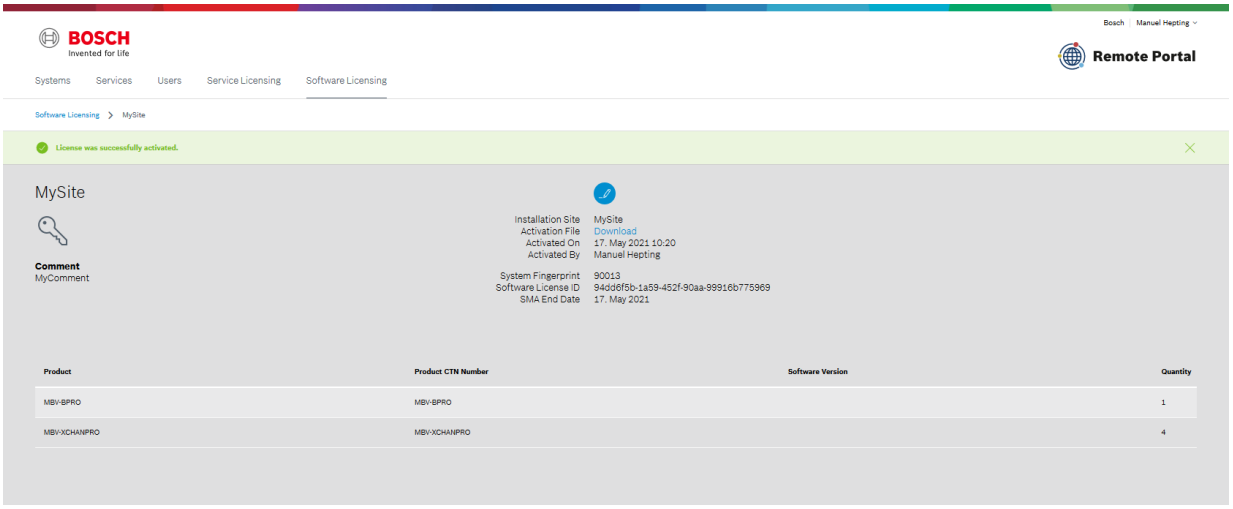

Select the expansion licenses and the quantity to activate them:

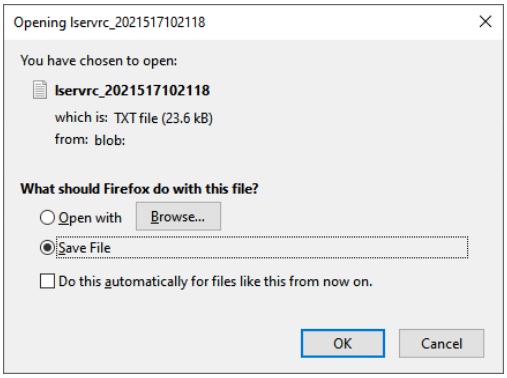


**Step 7: Download your activation file and make it accessible to the BVMS computer**

After you successfully added your license, you will see the following license dashboard in the Remote Portal. Click **Download** to download the activation file and save it on your computer.

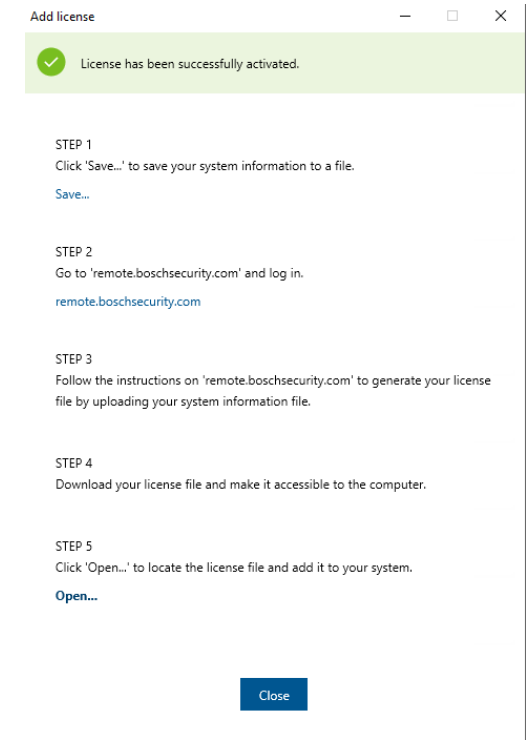
**Note:** If your BVMS application is not installed on the same computer where your activation file is saved, transfer the activation file to the computer with the BVMS application.

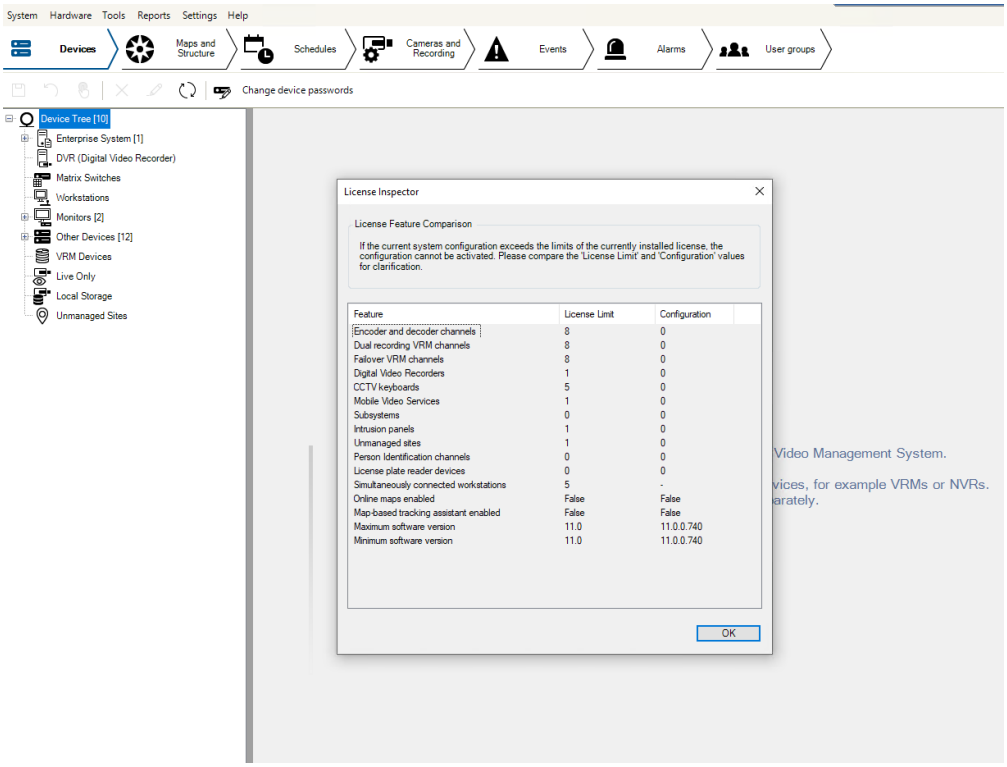


### Step 8: Upload the generated activation file

Go back to your BVMS application and click the **Open** button under **STEP 5** to upload your activation file. After successfully uploading your activation file, the license status changes to “activated” and your license information displays.




Now you can start using the full potential of your BVMS application and configure your system by adding cameras, for example.

# 5.1 BVMS 10.1

## 5.1.1 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.

## 5.1.2 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.

# 5.2 BVMS 10.0.1

## 5.2.1 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.

## 5.2.2 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.

## 5.2.3 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.

## 5.2.4 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.

# 5.3 BVMS 10.0

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

## 5.3.1 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.

## 5.3.2 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.

### 5.3.3 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.

### 5.3.4 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

## 5.4 BVMS 8.0

### 5.4.1 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.

# 6 Upgrading a BVMS system

## 6.1 Concepts and changes

### 6.1.1 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.

### 6.1.2 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 |
|---|---|---|
| 11.1.1 | 11.0, 10.1.1, 10.1 | 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. |
| 11.1.1, 11.0, 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. |
| 11.1, 11.0, 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.** |
| 11.1, 11.0, 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**. |
| 11.1 <= 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.

### 6.1.3 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.

### 6.1.4 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".

### 6.1.5 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.

## 6.2 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.

## 6.2.1 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.

## 6.2.2 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.

## 6.2.3 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
```

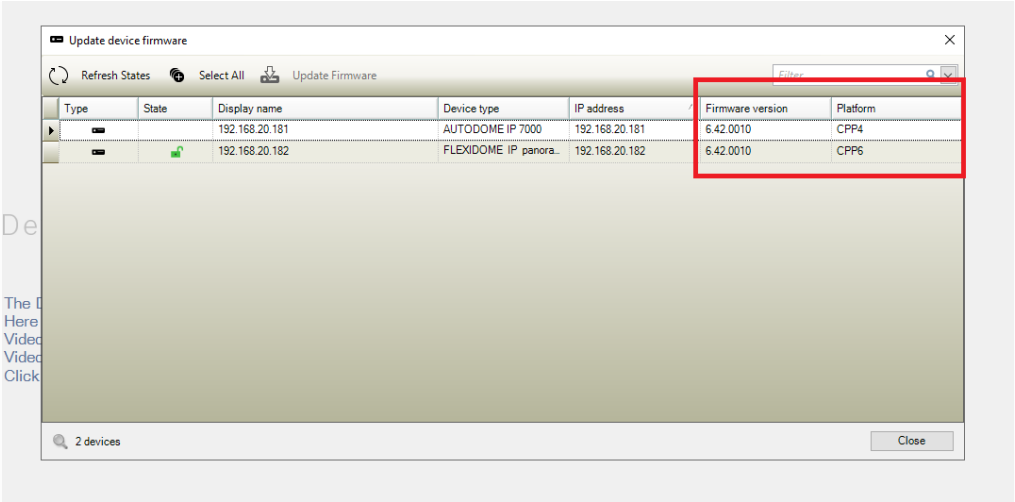
## 6.2.4 Upgrading encoder / decoder firmware

> **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.




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**

## 6.2.5 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.

## 6.2.6 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

# 6.3 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. |

| Check | Description |
|---|---|
| | 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. |

# 7 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.

## 7.1 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).

## 7.2 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.

# 8 Migration of a BVMS system

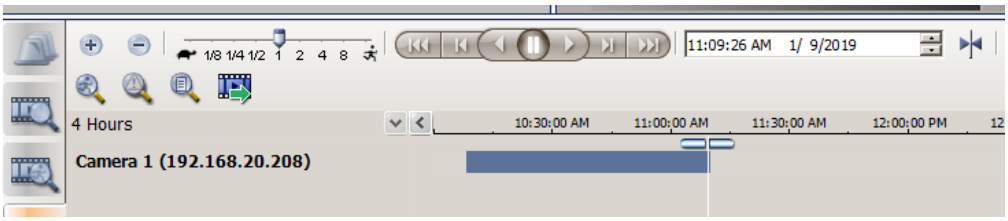
Next to an upgrade, it is sometimes required to migrate an entire system to new hardware and/or a new operating system. An example could be when an upgrade from BVMS 6.5 to BVMS 9.0 is planned, which would require the operating systems to be upgraded as well. Depending on the size and complexity of the 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.

## 8.1 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.

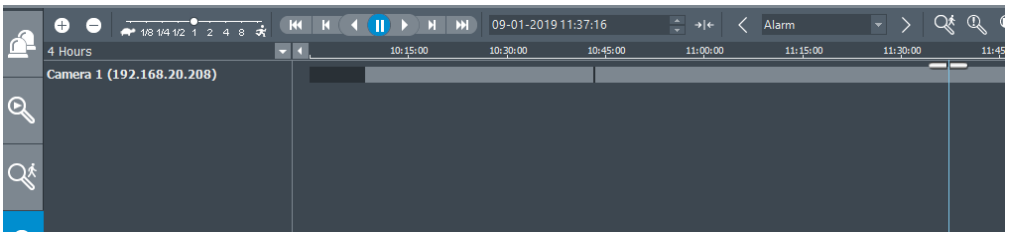
The image below shows the timeline of the existing system (BVMS 7.0) before the migration steps where initiated.




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.

# 8.2 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.

# 8.3 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.

# 8.4 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.

# 8.5 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.

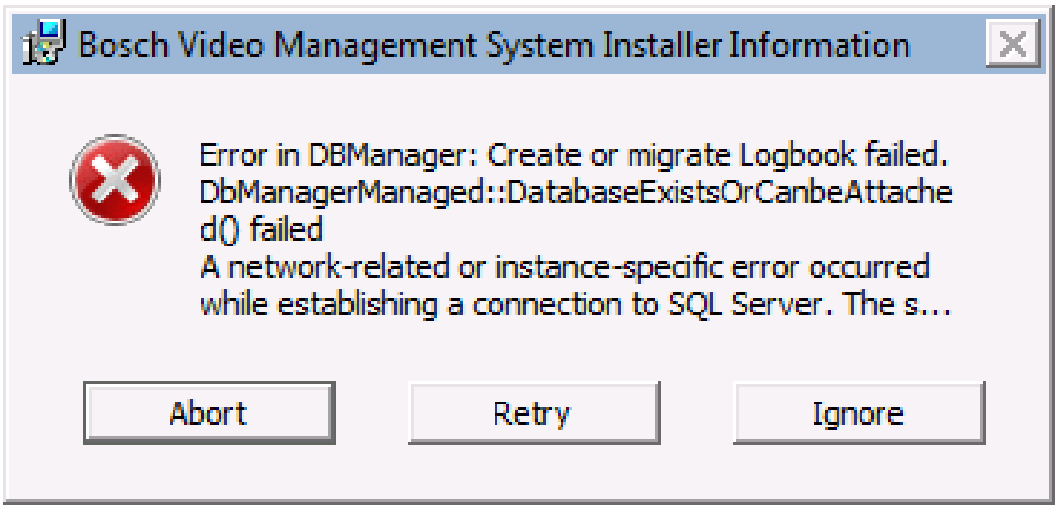
Previous recordings are **not** available and VSG will continue recording.

# 9 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.

## 9.1 Setup

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




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

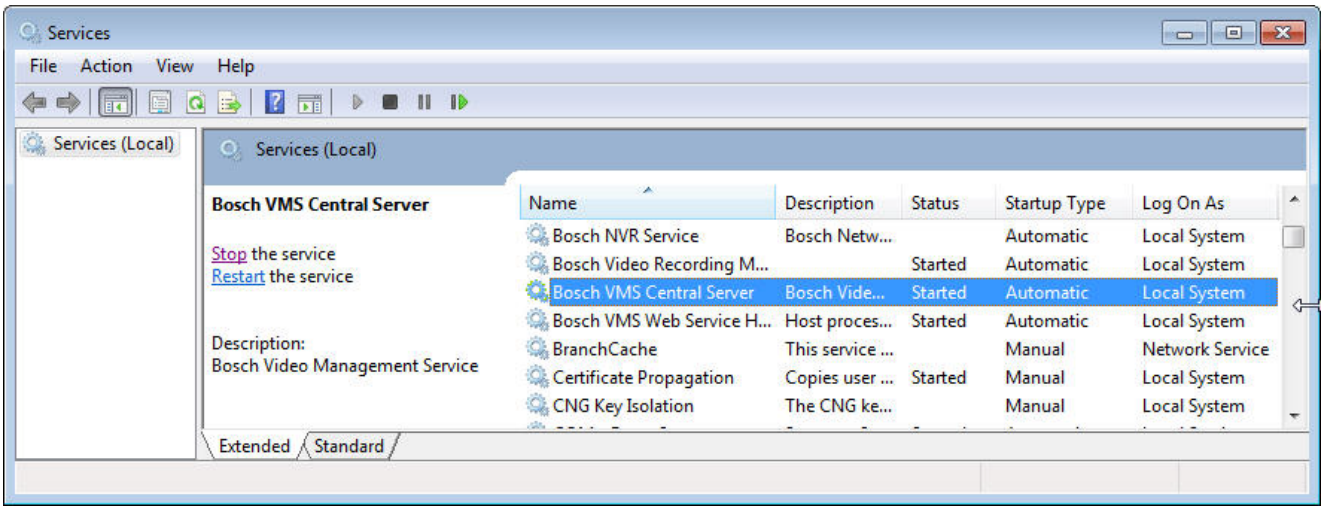
- Press **Cancel** to abort the BVMS installation.

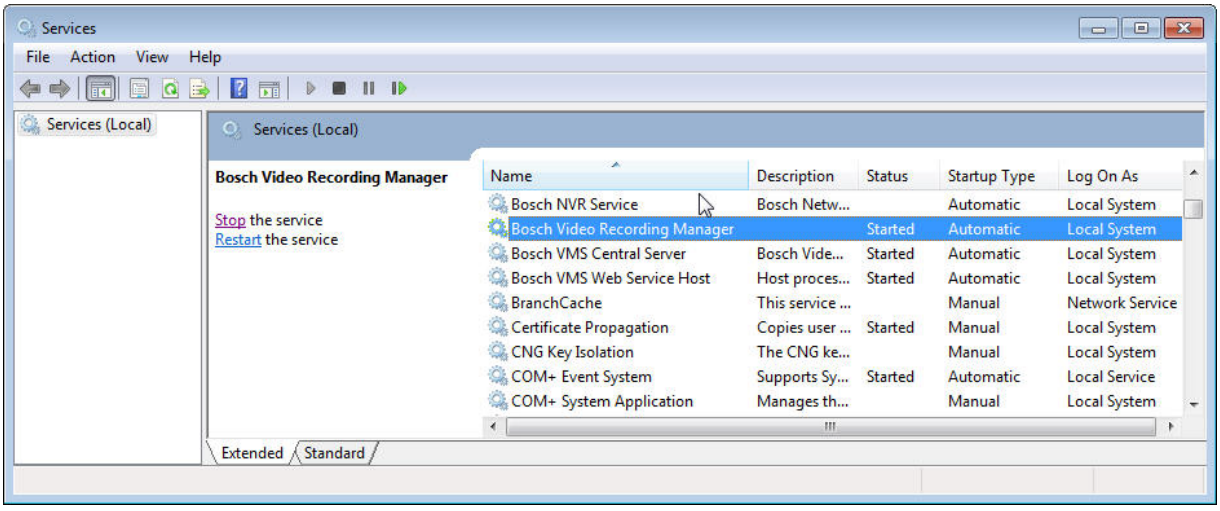
You can restart Setup later. Your current Logbook and custom data is retained.

## 9.2 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**.




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.