



**BOSCH**


Invented for life

## **BVMS - Device Compatibility**

Author: Verhaeg Mario (BT-SC/PAS4-MKP)  
Date: 9 October, 2019

<b>1 Document information</b>	<b>3</b>
1.1 Version history	3
<b>2 Introduction</b>	<b>4</b>
<b>3 Executive Summary</b>	<b>5</b>
<b>4 Device compatibility concept</b>	<b>6</b>
4.1 Device type	6
4.2 Device properties and interfaces	6
4.3 Stream properties	7
4.4 Camera configuration	8
4.5 Upgrade BVMS	8
<b>5 Implemented functionality</b>	<b>9</b>
5.1 Technical support	10
<b>6 Specific technology introduction</b>	<b>17</b>
6.1 Q3-2017 H.265	17
6.2 Q3-2017 Camera firmware 6.4x	17
6.3 Q3-2017 DSA E2800 series	17
6.4 Q3-2019: Video Streaming Gateway 7.0 onwards	17
6.5 Q3-2019: Encrypted recording	17
6.6 Q3-2019 Secure connectivity	17
6.7 Q3-2019 Camera firmware 7.1x and 7.5x	18

# 1 Document information

Project	BVMS 10.0
Reference	TFS#71995
Version	<a href="#">44</a>
Last modified	 09 October 2019

## 1.1 Version history

Version	Date	Author	Comment
<a href="#">44</a>	2019-10-09	<a href="#">Verhaeg Mario (BT-SC/PAS4-MKP)</a>	

## 2 Introduction

Up until some years ago, new released cameras, encoders, domes and decoders that are introduced into market after a BVMS release could not be connected to an existing BVMS version because these cameras were not known to the BVMS. In the BVMS 4.5.1, a new concept was introduced. This concept treats Bosch video encoders and decoders as generic devices, and automatically recognizes specific device functionality (for example the number of streams, relays and inputs). Based on this information the, at that time, unknown device is added to the system and can be used by the operator.

This document provides a detailed description of this functionality.

## 3 Executive Summary

Before the BVMS 4.5.1 was introduced, compatibility control between hardware device and installed management software was limited due to a tight release control (only tested exact combination are officially supported). This tight version compatibility control is be relaxed (BVMS 4.5.1 in May 2013), solving 90% of the incompatibilities. As a consequence new Bosch IP devices or firmware will be supported by up to two years old software clients. Customers can upgrade to the latest BVMS version using the SMA, which is included in the initial license free of charge for the first year. All BVMS components (including the Video Recording Manager) are included in this concept.

### **Architectural changes**

The support does not include major architectural changes. A current example is the introduction of H.265 (this new decoding standard needs to be explicitly implemented). Previous examples include the introduction of the panoramic cameras and the 4K cameras. Please note that the examples mentioned above are just examples, and do not represent a complete list of architectural changes.

An example: The DINION IP Thermal 8000 is released with CPP7 firmware 6.32.0099, introduced in September 2016. As a result the camera will provide basic functionality (limitations defined in this document) in BVMS 5.0 (the active version in September 2014) and newer.

## 4 Device compatibility concept

Bosch Security Systems has many devices and software packages which are all connected. Before the generic device functionality was introduced, inter-compatibility between devices and software was strict and published in complex matrices.

During the development of a BVMS version all existing devices, with the latest firmware, are tested. Using the generic device concept, new models, providing a similar functionality set compared to existing models, will work in preceding BVMS releases. Minor functionality enhancements (for example, more inputs) are detected automatically when the device is added to the configuration. Major technology changes, for example the introduction of the H.265 codec or major changes to the authentication behavior, requires an upgrade to the BVMS which includes this functionality.

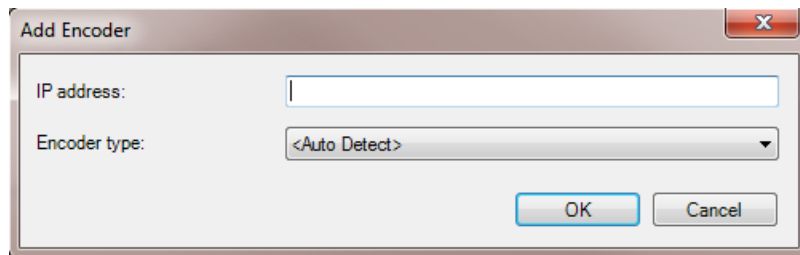
This chapter lists the device parameters that are supported in this scenario.

### 4.1 Device type

When adding a device-type which is unknown to the system, the device-type (either an encoder or decoder) needs to be recognized.

### 4.2 Device properties and interfaces

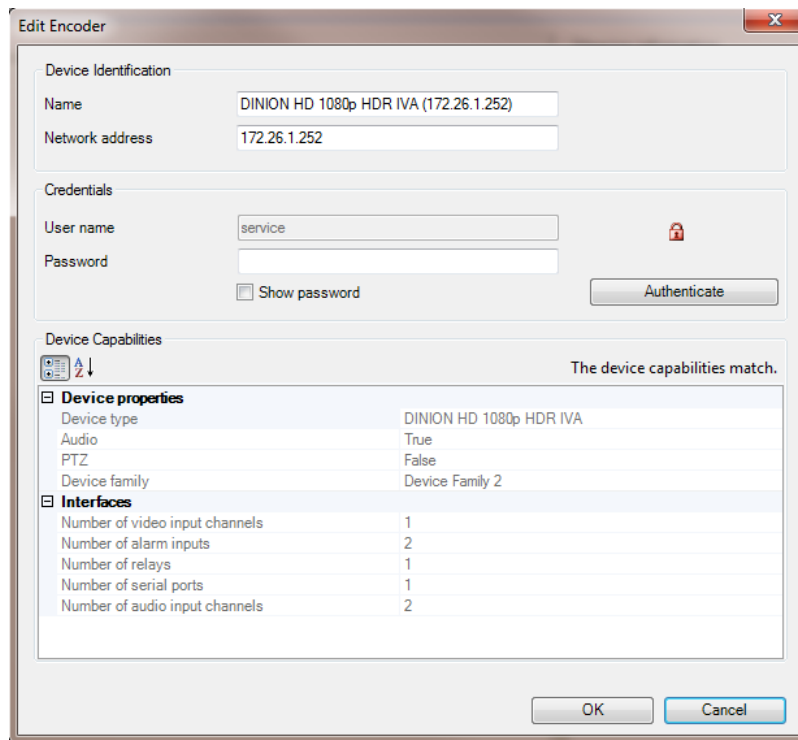
Device-types which are unknown to the current BVMS version will be recognized by the device scan and can also be manually added to the system configuration. If a device-type is not in the list of known devices, the "auto detect" option can be used. The device must be available in the network.



The image shows a dialog box titled "Add Encoder". It has a close button (X) in the top right corner. Inside the dialog, there are two main fields: "IP address:" followed by a text input field, and "Encoder type:" followed by a dropdown menu. The dropdown menu currently shows "<Auto Detect>". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

When the device is not available, the device capabilities cannot be read and the device cannot be added to the system.

When the device is available, the BVMS configuration client will automatically read the: device-type, audio capabilities, pan-tilt-zoom functionality, and device family from the encoder. Additionally the number of video input channels, alarm inputs, relays, serial ports and audio input channels are retrieved.



## 4.2.1 Encoder capabilities

After an encoder is added, this information can be reviewed in the "Edit Encoder" dialogue, which can be opened by right clicking on the encoder. When an encoder is replaced (the same IP address is re-used) by a different model, this dialogue must be used to re-scan the device capabilities.

### Persistency of device capabilities

The device capabilities are read and compared to the device capabilities persisted in the configuration. Four cases can occur:

1. While retrieving the device capabilities the message "Retrieving device capabilities..." is shown.
  2. The device capabilities match the capabilities persisted within the configuration: no message is shown.
  3. The device capabilities differ from the capabilities persisted within the configuration: the message "The device capabilities changed. Apply changes?" is shown. Clicking on the confirmation button shows a message box with the text "If you apply the device capabilities, the event settings for this device may change. Check these settings for this device." With OK the device capabilities read from the device are overtaken to BVMS.
    1. If the device-type changed the device family is set to "Device family 1" if only 1 stream is supported by the device.
    2. If the device-type changed the device family is set to "Device family 2" if 2 streams are supported by the device.
    3. If the device-type does not change the device family is preserved.
- The device capabilities could not be read: the message "Retrieving device capabilities failed." is shown. The BVMS management server shall never automatically correct a mismatching configuration of "Compatible devices".

## 4.3 Stream properties

The parameters to configure the I-Frame Distance, I-Frame Quality and P-Frame Quality may change from encoder type to encoder type. Within the BVMS all not known device-types are linked to the default recording profiles. Customers can adjust these settings by creating a new profile.

## 4.4 Camera configuration

The camera configuration tabs in the BVMS configuration client are tightly connected to a specific camera firmware version. When trying to add an unknown camera to the BVMS, Bosch recommends taking the following steps:

- Download and install the latest version of the Bosch Configuration Manager from <http://downloadstore.boschsecurity.com>.
- Pre-configure the camera settings (IVA, network, imaging, etc...) using the Bosch Configuration Manager. It could be possible that the BVMS Configuration Client is not able to configure all settings.
- Add the camera to the BVMS using the BVMS Configuration Client.

## 4.5 Upgrade BVMS

A valid BVMS SMA allows the system to be upgraded to the latest version. There will be no impact on device configuration and devices do not have to be re-configured after a system upgrade.



## 5 Implemented functionality

Cameras, encoders, and decoders that are currently not known to the BVMS can be operated with:

1. Live video: the operator can display the live stream of the device.
2. Playback: the operator can access the recorded stream of the device.
3. Export: the recorded video can be exported to the supported file formats.
4. Protect: the recorded video can be protected.
5. Pan-tilt-zoom: the operator can control the camera using pan-tilt-zoom commands. This is also possible for fixed cameras with a serial port and an external pan-tilt-zoom component connected.
6. Events: currently known events (connection state, input state, relay state, motion detection, recording mode, reference image check, storage state, video analytics 01 - 16, video loss, video signal too bright, video signal too dark, video signal too noisy) can be used. Other events require an upgrade to the correct BVMS version in which the device-type is known.

## 5.1 Technical support

The BVMS release notes lists the firmware versions which are used in the system tests. These firmware versions are fully compatible with the released version. New Bosch IP devices or firmware will be supported by up to two years old software clients (taking the limitations mentioned earlier into account), based on the release date of the firmware and the BVMS version. When a support case is raised, and the difference between the BVMS release and firmware release is larger than 2 years, the technical support team will require the system to be upgraded to the recommended firmware and/or BVMS version before further troubleshooting is offered.

### 5.1.1 Cameras

BVMS	Release date	CPP3	CPP-ENC	CPP4	CPP5	CPP6	CPP7	CPP7.3
minimum	2014-10-28	5.73.0045	5.52.0015	5.93.0025	5.92.0015	6.00.1203	6.30.0136	6.40.0240
7.0	2016-10-28	5.73.0046	5.52.0015	6.21.0008	5.92.0029	6.21.0008	6.21.0008	n/a
maximum	<b>2018-10-28</b>	5.75.0010	5.53.0004	6.44.0027	6.30.0059	6.44.0027	6.44.0027	6.44.0027
minimum	2015-04-29	5.73.0052	5.52.0015	6.10.0126	5.92.0026	6.10.0127	6.30.0136	6.40.0240
7.5	2017-04-29	5.74.0004	5.53.0004	6.32.0111	6.30.0047	6.32.0111	6.32.0111	n/a
maximum	<b>2019-04-29</b>	5.74.0010	5.54.0004	6.61.0025	6.61.0025	6.61.0025	6.61.0025	6.61.0025
minimum	2015-10-27	5.73.0052	5.52.0015	6.20.0089	5.92.0029	6.20.0089	6.30.0136	6.40.0240
8.0	2017-10-27	5.74.0004	5.53.0004	6.41.0037	6.30.0047	6.41.0037	6.41.0037	6.41.0037
maximum	2019-10-27	latest	latest	latest	latest	latest	latest	latest

minimum	2016-08-17	5.73.0052	5.53.0004	6.30.0140	6.30.0047	6.30.0140	6.30.0136	6.40.0240
9.0	2018-08-17	5.74.0010	5.53.0004	6.50.0128	6.30.0059	6.50.0128	6.50.0128	6.50.0128
maximum	2020-08-17	latest	latest	latest	latest	latest	latest	latest
minimum	2017-08-13	5.74.0004	5.53.0004	6.41.0037	6.30.0047	6.41.0037	6.41.0037	6.41.0037
10.0	2019-08-13	5.74.0010	5.54.0004	7.10.0074	6.30.0059	7.10.0074	7.10.0074	7.10.0074
maximum	2021-08-13	latest	latest	latest	latest	latest	latest	latest

### 5.1.2 Decoders

BVMS	Release date	C P - E N C	VIP XD HD	VJD 3000	VJD 7000	VJD 7513	VJD 8000
minimum	2014-10-28	5 . 5 9 . 0 0 2 3	1.8.00	5.93.0015	54.8.1	n/a	8.10

7.0	2016-10-28	5 . 5 9 . 0 0 2 3	1.8.00	5.93.0023	54.8.2	n/a	8.10
maximum	<b>2018-10-28</b>	5 . 9 7 . 0 0 0 5	1.8.00	5.97.0005	1.8.00	n/a	1.8.00
minimum	2015-04-29	5 . 5 9 . 0 0 2 3	1.8.00	5.93.0023	54.8.1	n/a	8.10

7.5	2017-04-29	5 . 9 7 . 0 0 0 5	1.8.00	5.97.0005	54.8.2	n/a	8.21.0028
maximum	<b>2019-04-29</b>	5 . 9 7 . 0 0 0 5	1.8.00	5.97.0005	54.8.2	n/a	9.10.0029
minimum	2015-10-27	5 . 9 7 . 0 0 0 5	1.8.00	5.93.0023	54.8.2	9.51.0 058	8.10

8.0	2017-10-27	5 . 9 7 . 0 0 0 5	1.8.00	5.97.0005	54.8.2	9.51.0 058	9.00.0134
maximum	2019-10-27	l a t e s t	latest	latest	latest	latest	latest
minimum	2016-08-17	5 . 9 7 . 0 0 0 5	1.8.00	5.93.0023	54.8.2	9.51.0 058	8.21.0028
9.0	2018-08-17	5 . 9 7 . 0 0 0 5	1.8.00	5.97.0005	54.8.2	9.51.0 058	9.10.0029

maximum	2020-08-17	l a t e s t	latest	latest	latest	latest	latest
minimum	2017-08-13	5 . 9 7 . 0 0 0 5	1.8.00	5.93.0023	54.8.2	9.51.0 058	8.10
10.0	2019-08-13	5 . 9 7 . 0 0 0 7	1.8.00	5.97.0005	54.8.2	9.51.0 058	9.51.0058
maximum	2021-08-13	l a t e s t	latest	latest	latest	latest	latest

## 5.1.3 Video Streaming Gateway

<b>BVMS</b>	<b>Release date</b>	<b>VSG 6.x</b>	<b>VSG 7.x</b>
9.0	2018-08-17	6.44.0022	n/a
maximum	2020-08-17	latest	n/a
minimum	2017-08-13	n/a	7.0.2
10.0	2019-08-13	n/a	7.0.2
maximum	2021-08-13	latest	latest



## 6 Specific technology introduction

### 6.1 Q3-2017 H.265

BVMS 8.0 (released in October 2017) will decode Bosch H.265 cameras. When Bosch H.265 cameras are connected to previous versions of the BVMS these need to put into H.264 mode and can then still be used.

### 6.2 Q3-2017 Camera firmware 6.4x

This specific firmware release introduces a password enforcement policy on the Bosch cameras. BVMS 8.0 (released in October 2017) will handle FW 6.4x or newer cameras. When Bosch FW6.4x cameras, or newer, are connected to previous versions of the BVMS the passwords of those cameras needs to be pre-configured using external tools (for example, the camera web-interface or Bosch Configuration Manager). Once the cameras are added, the pre-configured password can be used to authenticate the system to the camera.

### 6.3 Q3-2017 DSA E2800 series

The DSA E2800 series requires a minimum firmware level on the devices. CPP3 devices cannot be used in a system enabled for multi-pathing. DSA E2800 units are only supported by Bosch camera firmware version 6.32 and later, VRM Video Recording Manager version 3.70 and later, and Configuration Manager version 5.51 and later. Dual controller systems require Bosch camera firmware version 6.43 and later, VRM Video Recording Manager version 3.71 and later, and Configuration Manager version 5.53 and later.

### 6.4 Q3-2019: Video Streaming Gateway 7.0 onwards

Video Streaming Gateway 7.0 requires BVMS 10.0 or newer.

### 6.5 Q3-2019: Encrypted recording

Encrypted recording requires BVMS 10.0 or newer combined with device firmware 7.10 or newer. Devices produced before January 2014 (with Crypto-Coprocessor version older than 3) might not be able to encrypt their recordings. Devices which are not able to run firmware 7.10 can be connected to the Video Streaming Gateway to enable them to encrypt recordings.

### 6.6 Q3-2019 Secure connectivity

When the secure communications flag is set, the firmware published in the BVMS release notes is the minimum firmware that is supported. Older firmware might not support all functionality when the secure communication option is used.

#### 6.6.1 Decoders

Secure connectivity to decoders is only working for Videojet Decoder 8000 and other Videojet Decoder released after June 2019.

#### 6.6.2 Encoders

Secure connectivity to encoders is only working for CCP4, CPP6, CPP7 and CPP7.3 devices and newer. CPP3, CPP-ENC and CPP5 devices might work, but communication issues will not be investigated when the secure communication flag is set in the configuration.

## 6.7 Q3-2019 Camera firmware 7.1x and 7.5x

### 6.7.1 UDP encryption: "Error: Frame cannot be parsed"

BVMS 10.0 or newer can decrypt UDP communication. Earlier BVMS versions are not capable of decrypting UDP traffic. When a camera is added to BVMS 10.0 UDP encryption is turned on for all clients. In this situation older BVMS clients cannot decrypt the video, which results in a black cameo in Operator client and an "Error: Frame cannot be parsed!" on Configuration Client tabs. When using BVMS Enterprise combining different BVMS versions it is recommended to update all systems to the latest BVMS version or disable UDP encryption. When adding a camera to a BVMS 9.0 (or older) system which has previously been added to a BVMS 10.0 system, UDP encryption needs to be disabled in the camera configuration itself. Disabling UDP encryption needs to be done in the BVMS Configuration Client (disable "Secure Connection" in the Edit Encoder dialogue) and in the camera configuration itself. Alternatively the camera can be operated in TCP mode.

### 6.7.2 Password characters

The "+" character cannot be used in device passwords from camera firmware 7.1 onwards. BVMS 10.0 and earlier BVMS versions do not display a proper warning message that the device declines the new password.

### 6.7.3 IVA Configuration

Due to a breaking change the IVA configuration needs to be done from the Configuration Manager and cannot be done from BVMS 10.0 or earlier BVMS versions.