BOSCH
Invented for life

BVMS - Securing the Security System

Author: Verhaeg Mario (BT-VS/PAS4-MKP)
Date: 4 August, 2020

1 Document information

Project	BVMS 10.1
Reference	n/a
Version	44
Last modified	31 July 2020

1.1 Version history

Date	Version	Description
2020-07-31	10.1	Added communication with (Tattile) LPR camera.
2020-02-18	10.0.1	Added multicast encryption between VSG and OC. The Windows firewall is automatically configured. IP or IQN filtering on the iSCSI target is recommended.

2 Introduction

This guide assumes the BVMS Management Server, VRM, VSG, iSCSI targets, DVRs and MVS are located in a secure area (physically as well as logically).

2.1 Security levels

The following security levels are defined. Please note that the definition of the levels will change: the default security level will be increased gradually.

2.1.1 Definition

Level	Name	Description
Legacy	Compatibility	The compatibility mode is the least secure mode the system can operate in, but this ensures that functionality based on the integration of other systems (mainly older systems which do not offer secure connections) is not affected.
Default	Default system configuration, standard protection	The default configuration included the security enforcements that are applied to the system. Protection mechanisms from level 1 will slowly be migrated to the default level.
1	Hardening stage 1	The first hardening level assumes little additional effort can be spend in further hardening the system: spending 20% more time on the configuration of the system will increase the system security with 80%. Protection mechanisms from level 2 will slowly be migrated to this level.
2	Hardening stage 2	The last hardening level describes the maximum security the system can offer.

2.1.2 Summary

	Compatibility	Default	Level 1	Level 2
End-of-Life devices	YES	NO	NO	NO
Password based Authorization	OPTIONAL	NO	YES	YES
Secure data in transit (default)	OPTIONAL	YES	YES	YES
Secure data at rest (default)	OPTIONAL	YES	YES	YES
Secure data in transit (configurable)	OPTIONAL	OPTIONAL	YES	YES
Secure data at rest (configurable)	OPTIONAL	OPTIONAL	OPTIONAL	YES

	Compatibility	Default	Level 1	Level 2
Authenticate data in transit (configurable)	OPTIONAL	N/A	N/A	N/A
Authenticate data at rest (configurable)	OPTIONAL	OPTIONAL	OPTIONAL	YES

BVMS currently does not include functionality to verify the source of data in transit.

2.2 Configuration

This guide describes which options are available to secure a security system. The BVMS Configuration Manual describes how these options can be configured.

3 Best practices

3.1 Software installation

BVMS (or other software) should be installed into the default %ProgramFiles% location. This locations required administrative privileges to modify. This privilege-level can prevent attackers to execute malicious code by replacing components of BVMS or other software.

Make sure that SYSTEM PATH environment variable only contains directories that cannot be modified by a normal user. Modifying the content in these directories should require administrative privileges. This privilege-level can prevent attackers to execute malicious code by replacing components of BVMS or other software.

The safe software delivery article on the Bosch Building Technologies knowledge base explains how you can validate the integrity of the software you have downloaded from the Bosch Building Technologies downloadstore. Don't hesitate to inform us when you find a mismatch between the published checksums and the output of the described validation process.

You should unzip the installation files into a clean directory with limited access rights to prevent attackers from manipulating the installation files.

3.2 Network security

Network security is crucial: it's main goal is to prevent unauthorized persons to access the network infrastructure. Only when unauthorized persons have breached through the network security layers, the security of the video surveillance system itself (including hardening of the operating system, system authentication, and encryption of live and recorded video) becomes important, and acts as another security layer serving the system's overall security level. The BVMS network design guide (which can be found in the Bosch Building Technologies Community) describes several methods to harden the network, and provide logical intrusion detection.

3.3 Physical security

All server components like the BVMS Management Server and the Video Recording Manager server shall be placed in a secure area. The access to the secure area should be ensured with an access control system and should be monitored. The user group, which has access to the central server room, should be limited to a small group of persons. Although the server hardware is installed in a secure area, the hardware has to be protected against unauthorized access.

3.4 System maintenance

The video surveillance system is consisting out of multiple components, which all run their own software or firmware.

3.4.1 BVMS maintenance

BVMS patches are released on a regular basis (which also triggers an update of the release notes) and security issues are announced on the Bosch PSIRT page (including an RSS subscription). It is recommended to subscribe to the RSS feed of the PSIRT page to receive the latest security vulnerabilities (Subscribe Outlook to RSS feed). It is recommended to apply security updates immediately after they are published or to apply the suggested mitigation/work-around steps. Other (non-security) patches only need to be applied when the system is suffering from the specific issue the patch fixes and do not increase the security level of the system. A major BVMS system **upgrade** is recommended at least every two years.

3.4.2 Operating system maintenance

Bosch recommends to keep the operating systems used by the video surveillance system updated on a contineuous basis, with a maximum **update** cycle of 6 months. Windows updates often include patches to newly discovered security vulnerabilities, such as the Heartbleed SSL vulnerability, which affected millions of computers worldwide. Patches for these significant issues should be installed. A major operating system **upgrade** is recommended every two years.

The Windows lifecycle fact sheet (support.microsoft.com) is published by Microsoft and describes the current status of their operating systems.

4 Operating system configuration

We recommend to use the least privilege approach for the access rights of operating system users and disable or limit permissions of normal users to the application directories.

4.1 Compatibility level

In the compatibility level the embedded Windows security mechanisms (Windows Firewall and Windows Defender Antivirus) are disabled.

4.2 Default level

The default level includes the settings which are enabled in the operating system by default.

The Windows 10 security functionality is described on the Microsoft website (The most secure Windows ever - and built to stay that way), which includes the Windows Firewall, Automatic update mechanisms, Windows Defender Antivirus, and Windows Defender Security Center.

> *Windows Defender Firewall with Advanced Security is an important part of a layered security model. By providing host-based, two-way network traffic filtering for a device, Windows Defender Firewall blocks unauthorized network traffic flowing into or out of the local device. Windows Defender Firewall also works with Network Awareness so that it can apply security settings appropriate to the types of networks to which the device is connected. Windows Defender Firewall and Internet Protocol Security (IPsec) configuration settings are integrated into a single Microsoft Management Console (MMC) named Windows Defender Firewall, so Windows Defender Firewall is also an important part of your network's isolation strategy.*

Source: Windows Defender Firewall with Advanced Security

4.2.1 Anti-virus software

The usage of anti-virus software (either the Windows Defender or another product) is recommended and should be kept up to date. BVMS has been tested with Symantec Endpoint Detection and Microsoft Windows Defender, however, other virus scanners should not influence the behaviour of BVMS.

> Exclude the iSCSI storage location folders (if running on a Windows Server or DIVAR IP) from the anti-virus scanning repository to limit the impact of the performance of the anti-virus software.

4.2.2 Firewall

The usage of firewall software (either the Windows firewall of another product) is recommended and should be kept up to date. The BVMS setup automatically configures the Windows firewall based on the components that are selected for installation.

4.3 Level 1

4.3.1 Bosch Operating System Hardening tool

All BVMS server components, such as the BVMS Management Server and the Video Recording Manager server as well as the workstations used for BVMS Client applications, have to be hardened to protect the video data, the documents and other applications against unauthorized access. The BVMS Operating System Hardening Tool hardens the Windows servers and workstations by automatically configuring the recommended Local Group Policy Settings in the Windows Operating System. The BVMS Operating System Hardening Tool can run either as an executable file or as a PowerShell script. It is recommended to run the BVMS Operating System Hardening Tool as an executable file. The PowerShell script is only recommended for experienced users and system administrators. To run the BVMS Operating System Hardening Tool as a PowerShell script, copy the text from the delivered text file, modify the settings accordingly and execute the script. You can find the BVMS hardening tool in the *bonus* directory of the installation zip.

4.3.2 Firewall

In level 1 it is recommended to apply IP filtering to the Windows firewall. This moves the Windows firewall configuration from an "accept communication from all sources" to an "deny communication from all undefined sources" configuration. This can be achieved by allowing the BVMS workstations and servers to communicate with pre-defined network end-points, while denying all undefined communication. Information on how to design and deploy the Windows Defender Firewall with Advanced security can be found on the Microsoft documentation pages.

4.3.3 iSCSI

In level 1 it is recommended to apply IP or IQN restrictions to limit the access to the iSCSI target. You can find the configuration details in the BVMS - Configuring a Microsoft iSCSI target article on the Bosch Building Technologies community.

4.4 Level 2

4.4.1 BIOS

The server's BIOS offers the ability to set lower-level passwords. These passwords allow to restrict people from booting the computer, booting from removable devices, and changing BIOS or UEFI (Unified Extensible Firmware Interface) settings without permission. It is recommended to prevent changes to the BIOS configuration by protecting it with a password.

4.4.2 Microsoft operating systems

Microsoft provides documentation on Windows Enterprise Security and publishes Security Baselines on the Microsoft Security Guidance blog for each released Windows version. Additionally Microsoft describes Windows 10 Enterprise Security on a specific portal: Windows 10 Enterprise Security, which includes Identity and access management, threat protection and information protection.

Security Baseline
Security baseline for Windows 10 v1903 and Windows Server v1903
Security baseline for Windows 10 v1809 and Windows Server 2019
Security baseline for Windows 10 "April 2018 Update" (v1803)
Security baseline for Windows 10 "Fall Creators Update" (v1709)
Security baseline for Windows 10 v1607 ("Anniversary Update") and Windows Server 2016

5 BVMS configuration

5.1 Compatibility level

In the compatibility level the password enforcement options are removed by using the opt-out settings for the administrative accounts, other system accounts and devices.

5.2 Default level

5.2.1 New installation

Authentication

BVMS provides authentication methods for operators and system administrators. At the same time authentication mechanisms are also used to authenticate towards sub-devices (for example cameras) and sub-systems. Op top of the username and password based authentication scheme a certificate can be added (and is already enforced in some cases) to increase the level of the security.

> There are some restrictions for the use of special characters such as: ‘@’, '&', '<', '>', ‘:’ in passwords due to their dedicated meaning in XML and other markup languages. While the web interface will accept those, other management and configuration software might refuse acceptance.

> BVMS is able to lock-out an account after an configurable amount of failed password entries. This functionality is not enabled by default for the default "Admin" account. Bosch strongly recommends enabling this option for the user-group "Admin Group", changing the name of the "Admin" user-account, and adding a second user-account to the user-group "Admin Group". This minimizes the chance that the system administrator is fully locked-out of the system.

Password context	Usage	Opt-out	Certificate-based authentication
Operator and administrative access			
BVMS Administrative accounts	ENFORCED	YES	NO
BVMS Other accounts	ENFORCED	YES	NO
Subsystem management			
Bosch Cameras	OPTIONAL	N/A	NO
Bosch Decoders	OPTIONAL	N/A	NO
Bosch DVRs	OPTIONAL	N/A	NO
Bosch Video Recording Manager	OPTIONAL	N/A	NO

ONVIF Cameras	OPTIONAL	N/A	NO
Person Identification Device	N/A	NO	YES
Access Management System	ENFORCED	NO	NO
iSCSI (based on chap)	OPTIONAL	N/A	N/A

Secure data in transit

Endpoint 1	Endpoint 2	Protocol	Method	Set	Comment
Person Identification Device	Camera	TLS 1.2	negotiated	Default	Implemented in BVMS 10.0.
Management server	Operator client	TLS 1.2	negotiated	Default	Implemented in BVMS 10.0.
Management server	Person Identification Device	TLS 1.2	negotiated	Default	Implemented in BVMS 10.0.
Management server	Access Management System	TLS 1.2	negotiated	Default	Implemented in BVMS 9.0.
Management Server	Intrusion Panel (B/G Series)	TLS 1.0 / SSL 3.0	negotiated	Default	Implemented in BVMS 7.0.
Management server	Decoder	TLS 1.2	negotiated	Default	Implemented in BVMS 10.0.
Configuration client	VRM	TLS 1.2	negotiated	Default	Implemented in BVMS 10.0.
Operator client	Decoder	TLS 1.2	negotiated	Default	Implemented in BVMS 10.0.
Camera	Decoder	TLS 1.2	negotiated	Configurable	Video only (unicast). Implemented in BVMS 10.0. Only for Videojet Decoder 8000, 75xx or newer.
VSG	Operator client	TLS 1.2	negotiated	Configurable	Implemented in BVMS 10.0.
VSG	Management server	TLS 1.2	negotiated	Configurable	Implemented in BVMS 10.0.
Configuration client	VSG	TLS 1.2	negotiated	Configurable	Implemented in BVMS 10.0.

Endpoint 1	Endpoint 2	Protocol	Method	Set	Comment
Management Server	DVR	HTTPS (TLS)	negotiated	Configurable	Command and control. Implemented in BVMS 9.0. Not available on DVR400/600/700/XF.
Operator Client	DVR	HTTPS (TLS), n/a	negotiated	Configurable	Command and control only. Video data is not encrypted. Not available on DVR400/600/700/XF.
Operator client	Decoder	TLS 1.2	negotiated	Configurable	Implemented in BVMS 10.0.
VRM	Operator client	TLS 1.2	negotiated	Configurable	Implemented in BVMS 10.0. No Direct iSCSI playback.
VRM	Management server	TLS 1.2	negotiated	Configurable	Implemented in BVMS 10.0.
Management server	Tracking & Recognition Service	TLS 1.2	negotiated	Default	Implemented in BVMS 10.0 for Person Identification.
Tracking & Recognition Service	Camera	TLS 1.2	negotiated	Default	Implemented in BVMS 10.0 for Person Identification.
Management Server	(Tattile) LPR Camera	TLS 1.2	negotiated	Default	Implemented in BVMS 10.1

When the TLS protocol is used a cipher is automatically selected based on the capability of the client and service. Typically this results in an AES-256 cipher.

Secure data at rest

Element	Cipher	Set	Location	Comment
Configuration (including device passwords)	AES-256	Default	Management Server, Operator Clients	Implemented in BVMS 9.0. Device passwords are not hashed.
Configuration (BVMS user accounts)	AES-256	Default	Management Server, Operator Clients	MD5 hashing used for passwords.
Feature vectors suspect database (biometric profiles)	AES-256	Default	Person Identification Device	Implemented in BVMS 10.0.

Element	Cipher	Set	Location	Comment
Durable Event Queue	AES-256	Default	Operator Client	Serves as a buffer for user action events while Operator Client is in offline mode. Stored on Operator Client PC.
Feature vectors detected persons (biometric profiles)	AES-256	Default	Person Identification Device	Implemented in BVMS 10.0. Feature vectors are only stored as long as needed for matching with the subject database.

5.2.2 Existing installation

If an existing BVMS system is upgraded to a newer version, the system configuration is not changed as part of the upgrade process. This is done to ensure existing functionality is not lost when upgrading a BVMS system. In this case some security enhancements need to be manually configured.

5.3 Level 1

5.3.1 Secure data in transit

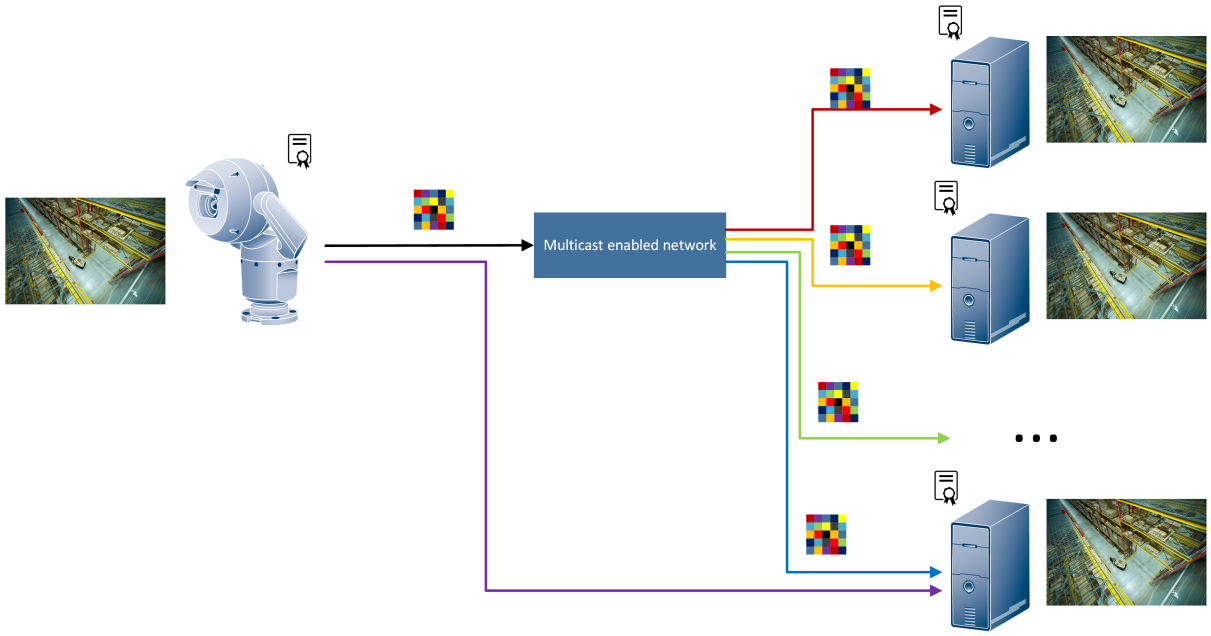
In the first level Bosch recommends to protect all data in transit by enabling encryption of the communication.

Endpoint 1	Endpoint 2	Protocol	Cipher	Set	Comment
Camera	Operator client	RTP	AES-128	Configurable	**Multicast**, Implemented in BVMS 10.0.
Camera	Operator client	TLS	negotiated	Configurable	Implemented in BVMS 7.0. TLS version depending on camera FW version.
Camera	VSG	TLS 1.2	negotiated	Configurable	Implemented in BVMS 10.0.
VSG	Operator client	RTP	AES-128	Configurable	**Multicast**, Implemented in BVMS 10.0.1.

> When the TLS protocol is used a cipher is automatically selected based on the capability of the client and service. Typically this results in an AES-256 cipher.

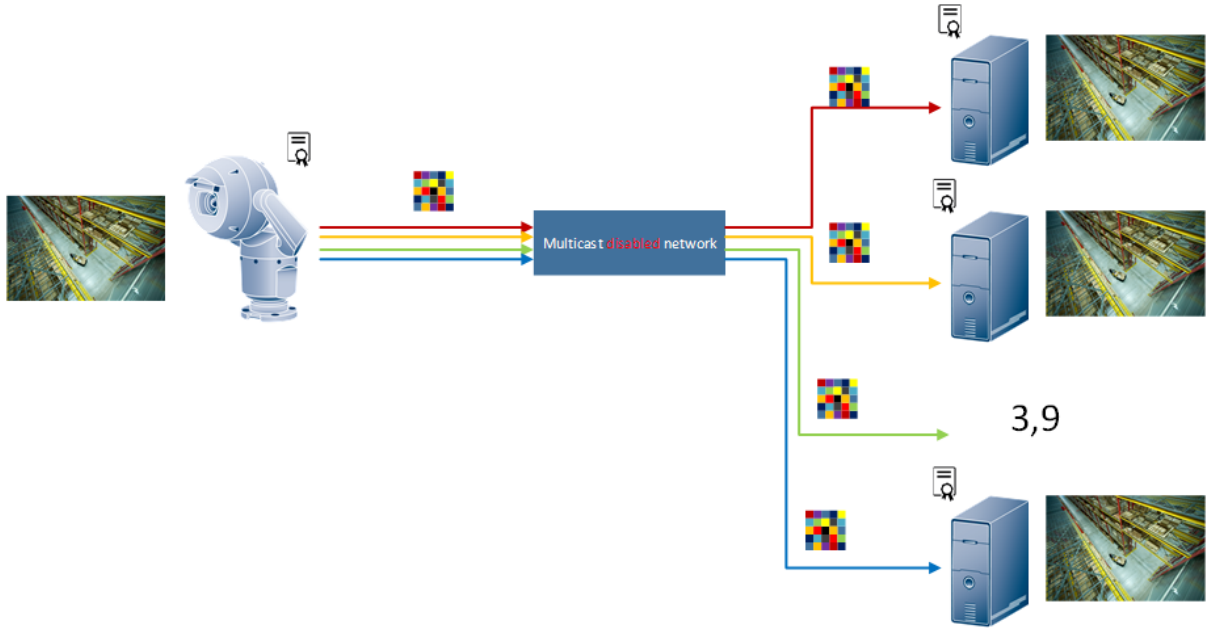
Mitigate man in the middle attacks: Multicast

The camera uses the workstation’s public key to encrypt HTTPS (control) connection to each workstation. multicast AES (128bit) key is distributed to workstation and can be used to decrypt multicast stream. The camera generates one stream and the network distributes an (encrypted) stream to up to 100 workstations. An unicast HTTPS control connection maintained for AES key distribution for multicast stream (per workstation). The workstation uses his private key to decrypt HTTPS traffic and extracts multicast AES key to decrypt multicast video traffic.



Mitigate man in the middle attacks: Unicast

The camera uses workstation's public key to encrypt HTTPS (control and video) traffic and generates up to 10 unicast streams and distributed them to the workstations. The workstation uses his private key to decrypt HTTPS (control and video) traffic.



5.3.2 Secure data at rest

Protect unauthorized access to data when the network is compromised

By default, iSCSI units grant all iSCSI initiators access to the iSCSI LUN's. To ensure, that only components of the Bosch Video Management solution (cameras, encoders, workstations and servers) are allowed to access the iSCSI LUN's, the default LUN mapping can be disabled. To allow devices the access to the iSCSI targets of BVMS, the iSCSI Qualified Names (IQN) or IP address of all components in the BVMS have to be configured on all iSCSI targets. This causes efforts during the installation, but minimizes the risk of video data being lost, leaked or manipulated.

Use password authentication via CHAP to ensure only known devices are allowed to access the iSCSI target. Setup a CHAP password on the iSCSI target and enter the configured password in the VRM configuration. The CHAP password is

valid for VRM and is sent to all devices automatically. If CHAP password is used in a Bosch Video Management System VRM environment, all storage systems have to be configured to use the same password.

5.3.3 Functionality

Some functionality in BVMS is build with compatibility in mind. In this security level Bosch does not recommend using Bosch Recording Station or Dibos devices, Matrix Switchers (Allegiant), ATM/POS communication, Foyer Card Readers, and Allegiant CCL emulation. For Bosch Recording Station devices and Matrix Switchers Bosch recommends replacing the hardware and software. For ATM/POS communication and Allegiant CCL emulation the BVMS SDK can be used as a secure alternative.

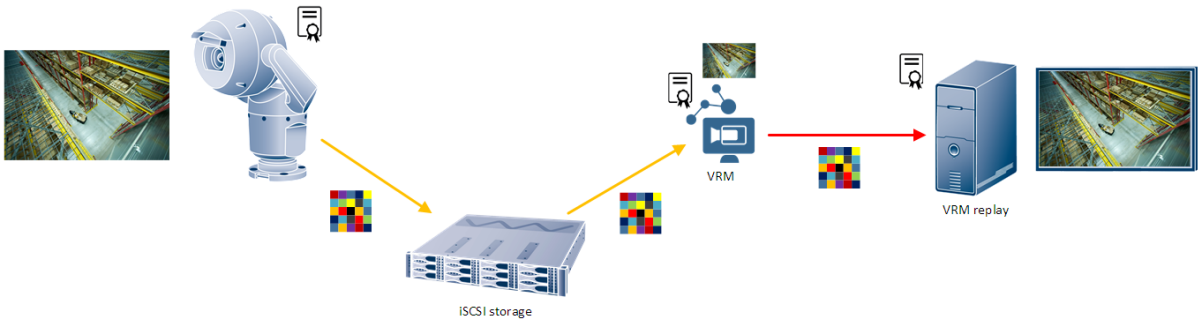
5.4 Level 2

5.4.1 Secure data at rest

Element	Method	Key length	Set	Comment
Video storage	XTS-AES	256	Configurable	Implemented in BVMS 10. Bosch cameras with co-processor version 6 (produced from January 2017 onwards) or other (Bosch/ONVIF) cameras using Video Streaming Gateway.
Logbook (SQL)	n/a	n/a	Configurable	Stored in Microsoft SQL Server database. Can be encrypted by using Windows bitlocker. SQL content encryption limits SQL query flexibility and performance.
Log files	n/a	n/a	Configurable	Can be encrypted by deploying using Windows bitlocker. Not encrypted on an application level to ensure troubleshooting capabilities.
Video exports	TripleDES	n/a	Configurable	The security operator can decide if exports are encrypted.

Protect unauthorized access to data when the operating system or storage location is compromised

The camera or Video Streaming Gateway generates an XTS-AES key. For each client (workstation / VRM) an entry is added to the header of the block. This header contains the encrypted (using the workstation's public key) XTS-AES key. The VRM's private key used to decrypt block header an get access to XTS-AES key for decryption of video in block. Network level encryption is used to send video to workstation (unencrypted video through encrypted tunnel). Encryption done with workstation's public key.



Only replay clients that are known by the camera (by means of a certificate containing the client's public key) at the time of recording can decrypt the video footage. If a workstation is added to the system, only the video recorded after the workstation is added will be available for decryption by the new workstation. Existing workstations have access to the historical recording as well.

In BVMS 10, the Video Recording Manager decrypts the recorded video from the iSCSI target and forwards it to the workstation.

5.4.2 Authenticate data at rest

Detect manipulation of video data

Once the devices in a system are protected and authenticated it is important to keep an eye on the integrity of the video data. This functionality is called video authentication. Video authentication deals solely with methods of validating the authenticity of video. Video authentication does not deal with the transmission of video, or data, in any way.

Element	Method	Set	Comment
Video storage	MD5/SHA1/SHA256	Configurable	Implemented in BVMS 7.5

Due to several weaknesses the use of MD5 is not recommended.

5.4.3 Functionality

No additional functionality needs to be disabled as part of the second security level.

6 Glossary

Term	Definition
Data at rest	Data stored on hard-drives.
Data in transit	Data transmitted across a network.
Encryption	Preventing access to data by deploying a mathematical model to transform usable data into unusable data.
Authentication	Validating if the data is not manipulated.
Authorization	Validating if access to data is permitted.