

# Bosch IP video products





# Table of contents

<b>1</b>	<b>Purpose of the document and target audience</b>	<b>5</b>
<b>2</b>	<b>Security concept and considerations</b>	<b>6</b>
<b>3</b>	<b>Secure installation</b>	<b>7</b>
<b>3.1</b>	Servers and storage devices	<b>7</b>
<b>3.2</b>	Cameras and edge devices	<b>7</b>
<b>4</b>	<b>Secure configuration</b>	<b>8</b>
<b>4.1</b>	Assigning IP addresses	<b>8</b>
<b>4.1.1</b>	Managing DHCP	<b>10</b>
<b>4.2</b>	User accounts and passwords	<b>10</b>
<b>4.2.1</b>	Assigning passwords	<b>11</b>
<b>4.2.2</b>	Assigning passwords using the device web page	<b>11</b>
<b>4.2.3</b>	Assigning passwords using Configuration Manager	<b>13</b>
<b>4.2.4</b>	Assigning passwords for VRM stand-alone installation	<b>13</b>
<b>4.2.5</b>	Assigning passwords using BVMS (on DIVAR IP or stand-alone)	<b>15</b>
<b>4.3</b>	Hardening device access	<b>16</b>
<b>4.3.1</b>	General network port usage and video transmission	<b>16</b>
<b>4.3.2</b>	Minimum TLS version	<b>17</b>
<b>4.3.3</b>	HTTP, HTTPS and video port usage	<b>17</b>
<b>4.3.4</b>	Video software and port selection	<b>18</b>
<b>4.3.5</b>	SSH tunneling	<b>18</b>
<b>4.3.6</b>	Telnet Access	<b>18</b>
<b>4.3.7</b>	RTSP: Real Time Streaming Protocol	<b>19</b>
<b>4.3.8</b>	UPnP: Universal Plug and Play	<b>20</b>
<b>4.3.9</b>	Multicasting	<b>20</b>
<b>4.3.10</b>	IPv4 filtering	<b>21</b>
<b>4.3.11</b>	SNMP	<b>22</b>
<b>4.3.12</b>	Secure time basis	<b>23</b>
<b>4.3.13</b>	Cloud-based services	<b>24</b>
<b>4.4</b>	Hardening IP cameras	<b>24</b>
<b>4.4.1</b>	Hardening levels	<b>24</b>
<b>4.4.2</b>	Hardening overview	<b>25</b>
<b>4.4.3</b>	Feature description and hardening recommendations	<b>26</b>
<b>4.4.4</b>	Defense in depth	<b>29</b>
<b>4.5</b>	Hardening storage	<b>30</b>
<b>4.5.1</b>	Setting a CHAP password on iSCSI devices	<b>30</b>
<b>4.6</b>	Hardening servers	<b>31</b>
<b>4.6.1</b>	Server Hardware recommended settings	<b>31</b>
<b>4.6.2</b>	Windows Operating System recommended security settings	<b>31</b>
<b>4.6.3</b>	Windows updates	<b>31</b>
<b>4.6.4</b>	Installation of anti-virus software	<b>31</b>
<b>4.6.5</b>	Windows Operating System recommended settings	<b>31</b>
<b>4.6.6</b>	Activate User Account Control on the server	<b>32</b>
<b>4.6.7</b>	Deactivate AutoPlay	<b>32</b>
<b>4.6.8</b>	External Devices	<b>32</b>
<b>4.6.9</b>	Configuration of user rights assignment	<b>33</b>
<b>4.6.10</b>	Screen saver	<b>34</b>
<b>4.6.11</b>	Activate password policy settings	<b>34</b>
<b>4.6.12</b>	Disable non-essential Windows Services	<b>34</b>

4.6.13	Windows Operating System user accounts	35
4.6.14	Enable firewall on the server	35
4.7	Hardening Windows clients	36
4.7.1	Windows Workstations	36
4.7.2	Windows Workstation hardware recommended settings	36
4.7.3	Windows Operating System recommended security settings	36
4.7.4	Windows Operating System recommended settings	36
4.7.5	Activate User Account Control on the server	36
4.7.6	Deactivate AutoPlay	37
4.7.7	External Devices	37
4.7.8	Configuration of user rights assignment	38
4.7.9	Screen saver	39
4.7.10	Activate password policy settings	39
4.7.11	Disable non-essential Windows Services	39
4.7.12	Windows Operating System user accounts	40
4.7.13	Enable firewall on the workstation	40
4.8	Protecting network access	41
4.8.1	VLAN: Virtual LAN	41
4.8.2	VPN: Virtual Private Network	41
4.8.3	Disable unused switch ports	42
4.8.4	802.1x protected networks	42
5	<b>Secure operation</b>	<b>43</b>
5.1	Network separation	43
5.2	Safe key storage in hardware vault	43
5.3	Unique device certificates	43
5.4	Checking log files	44
5.5	SIEM system	44
5.6	PKI	44
5.7	AD FS	45
5.8	Secure operation of IP cameras	45
5.8.1	Creating trust with certificates	45
5.8.2	Video Authentication	46
6	<b>Security update management</b>	<b>48</b>
7	<b>Security monitoring</b>	<b>49</b>
8	<b>Secure disposal and decommissioning</b>	<b>50</b>
9	<b>Additional information</b>	<b>51</b>
	<b>Glossary</b>	<b>52</b>

# 1 Purpose of the document and target audience

Technology is evolving at - sometimes breathtakingly - high speed. The rapid advancements in Artificial Intelligence (AI) and the Internet of Things (IoT), and their massive utilization (AIoT), changes the risk profile of products and services. Intentional malicious attacks become more feasible and more likely due to more connectivity. Providing secure and reliable products and services to customers is the objective of Bosch.

This guidebook should assist integrators to harden Bosch IP video products to better adhere to their customer's existing network security policies and procedures.

This guide will cover:

- Critical information on the features and fundamentals of Bosch IP video devices
- Specific features that can be modified or disabled
- Specific features that can be activated and utilized
- Best practices as they pertain to video systems and security

This guide will primarily focus on utilizing Configuration Manager to perform the discussed configurations. In most cases all configurations can be performed utilizing BVMS Configuration Client, Configuration Manager, and the built-in web interface of a video device.

## 2 Security concept and considerations

IP video products are becoming commonplace in today's network environment, and as with any IP device placed on a network, IT administrators and security managers have a right to know the full extent of a device's feature set and capabilities.

When dealing with Bosch IP video devices your first line of protection are the devices themselves. Bosch encoders and cameras are manufactured in a controlled and secure environment that is continually audited. Devices can only be written to via a valid firmware upload, which is specific to hardware series and chipset.

Most Bosch IP video devices come with an onboard security chip that provides functionality similar to crypto SmartCards and the so called Trusted Platform Module, or short TPM. This chip acts like a safe for critical data, protecting certificates, keys, licenses, etc. against unauthorized access even when the camera is physically opened to gain access.

Bosch IP video devices have been subjected to more than thirty thousand (30 000) vulnerability and penetration tests performed by independent security vendors. Thus far, there have been no successful cyberattacks on a properly secured device.

## 3 Secure installation

### 3.1 Servers and storage devices

All server components (for example BVMS Management Server and Video Recording Manager server) and storage devices should be installed 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 servers and storage devices are installed in a secure area, they have to be protected against unauthorized access.

#### Refer to

- *Hardening servers, page 31*
- *Hardening storage, page 30*

### 3.2 Cameras and edge devices

For the installation of cameras and edge devices a secure installation location and mounting orientation should be chosen. Ideally, this is a location where the device cannot be interfered with either intentionally or accidentally.

## 4 Secure configuration

### 4.1 Assigning IP addresses

All Bosch IP video devices currently come in a factory default state ready to accept a DHCP IP address.

If no DHCP server is available in the active network on which a device is deployed, the device will - if running firmware 6.32 or higher - automatically apply a link-local address out of the range of 169.254.1.0 to 169.254.254.255, or 169.254.0.0/16.

With earlier firmware, it will assign itself the default IP address 192.168.0.1.

There are several tools that can be used to perform IP Address assignment to Bosch IP video devices, including:

- Bosch Configuration Manager
- BVMS Configuration Client
- BVMS Configuration Wizard

All software tools provide the option of assigning a single static IPv4 address, as well as a range of IPv4 addresses to multiple devices simultaneously. This includes subnet mask and default gateway addressing.

All IPv4 addresses and subnet mask values need to be entered in the so-called “dot-decimal notation”.

#### Notice!



One of the first steps in limiting the possibilities of internal cyberattacks on a network, executed by unauthorized locally attached network devices, is to limit available unused IP addresses. This is done by using IPAM (**IP Address Management**), in conjunction with subnetting the IP address range that will be used.

Subnetting is the act of borrowing bits from the host portion of an IP address in order to break a large network into several smaller networks. The more bits you borrow, the more networks you can create, but each network will support fewer host addresses.

Suffix	Hosts	CIDR	Borrowed	Binary
.255	1	/32	0	.11111111
.254	2	/31	1	.1111111 <b>0</b>
.252	4	/30	2	.111111 <b>00</b>
.248	8	/29	3	.1111 <b>1000</b>
.240	16	/28	4	.1111 <b>0000</b>
.224	32	/27	5	.111 <b>00000</b>
.192	64	/26	6	.11 <b>000000</b>
.128	128	/25	7	. <b>10000000</b>

Since 1993, the Internet Engineering Task Force (IETF) introduced a new concept of allocating IPv4 address blocks in a more flexible way than used in the former “classful network” addressing architecture. The new method is called “Classless Inter-Domain Routing” (CIDR) and also used with IPv6 addresses.

IPv4 classful networks are designated as Classes A, B and C, with 8, 16 and 24 network number bits respectively, and Class D which is used for multicast addressing.

**Example:**

For an easy to understand example, we will use a C Class address scenario. The default subnet mask of a C Class address is 255.255.255.0. Technically, no subnetting has been done to this mask, so the entire last octet is available for valid host addressing. As we borrow bits from the host address, we have the following possible mask options in the last octet: .128, .192, .224, .240, .248, and .252.

If utilizing the 255.255.255.240 subnet mask (4 bits) we are creating 16 smaller networks that support 14 host addresses per subnet.

- Subnet ID 0:  
host address range 192.168.1.1 to 192.168.1.14. Broadcast address 192.168.1.15
- Subnet ID 16:  
host address range 192.168.1.17 to 192.168.1.30. Broadcast address 192.168.1.31
- Subnet IDs: 32, 64, 96, etc.

For larger networks the next bigger network Class B might be needed, or an appropriate CIDR block defined.

**Example:**

Prior to deploying your video security network, you perform a simple calculation of how many IP devices will be needed on the network, to include room for future growth:

- 20 Video Workstations
- 1 Central Server
- 1 VRM Server
- 15 iSCSI Storage Arrays
- 305 IP cameras

Total = 342 IP addresses needed

Taking into account the calculated number of 342 IP addresses, we at minimum need a B Class IP address scheme to accommodate that many IP addresses. Using the default B Class subnet mask of 255.255.0.0 allows for 65534 available IP addresses to be used within the network.

Alternatively, the network can be planned using a CIDR block with 23 bits used as prefix, providing an address space of 512 addresses respectively 510 hosts.

By breaking a large network into smaller pieces, by simply subnetting, or specifying a CIDR block, you can reduce this risk.

**Example:**

	Default	Subnetted
IP address range	172.16.0.0 - 172.16.255.255	172.16.8.0 - 172.16.9.255
Subnet mask	255.255.0.0	255.255.254.0
CIDR notation	172.16.0.0/16	172.16.8.0/23
Number of subnets	1	128

Number of hosts	65.534	510
Excess addresses	65.192	168

### 4.1.1

## Managing DHCP

IPAM can utilize DHCP as a powerful tool in the control and usage of IP addresses in your environment. DHCP can be configured to utilize a specific scope of IP addresses. It can also be configured to exclude a range of addresses.

If utilizing DHCP, it would be best, when deploying video devices, to configure non-expiring address reservations based on the MAC address of each device.



### Notice!

Even before using IP Address Management to track the usage of IP addresses, a network management best practice is to limit access to the network through port security on edge switches, for example only a specific MAC address can access through a specific port.

## 4.2

## User accounts and passwords

All Bosch IP video cameras and encoders come with three built-in user accounts:

- **live**  
This standard user account only allows access to live video streaming.
- **user**  
This more advanced user account allows access to live and recorded video, and camera controls like PTZ control.  
This account does not allow access to configuration settings.
- **service**  
This administrator account provides access to all device menus and configuration settings.

A password has to be assigned for each of the user accounts.

Password assignment is a critical step in protecting any network device. It is strongly advised that passwords are assigned to all installed network video devices.

**Notice!**

With firmware version 6.30, user management has been enhanced for more flexibility to allow other users and usernames with own passwords. The former account levels now represent the user group levels.

With firmware version 6.32, a stricter password policy has been introduced (for more details see *Assigning passwords using the device web page, page 11*).

**4.2.1****Assigning passwords**

Passwords can be assigned in several ways, depending on the size of the video security system and on the software being used. In smaller installations consisting of only a few cameras, passwords can be set utilizing either the device's web page or – as it conveniently supports multiple device configuration simultaneously and a configuration wizard – Bosch Configuration Manager.

**Notice!**

As stated previously, password protection is critical when securing data from possible cyber-attacks. This applies to all network devices in your complete security infrastructure. Most organizations already have strong password policies in place, but if you are working with a new installation with no policies in place, the following are some best practices when implementing password protection:

- Passwords should be between 8 and 12 characters in length.
- Passwords should contain both upper and lower case letters.
- Passwords should contain at least one special character.
- Passwords should contain at least one digit.

**Example:**

Using the passphrase "to be or not to be" and our basic rules for good password generation.

- 2be0rnOt!t0Be

**Notice!**

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.

**4.2.2****Assigning passwords using the device web page**

1. On the device web page, navigate to the **Configuration** page.
2. Select the **General** menu and the **User Management** submenu (Note: Before firmware version 6.30, the **User Management** submenu was called **Password**).

On first entering the web page of a camera, the user is asked to assign passwords to ensure minimum protection.

This will persistently be repeated on every reload of camera web pages as long as no password is set. Clicking **OK** leads to the **User Management** menu automatically.

Firmware 6.30 had the option to activate a **Do not show...** checkbox. This option has been removed with firmware 6.32 to avoid security escapes.

1. Select the **User Management** menu and enter and confirm the desired password for each of the three accounts.  
Please note:
  - Passwords need to be assigned at the highest access level (**Password 'service'**) first.

- From firmware release 6.20 onwards, a new indicator called the "password strength meter" shall give hints about the potential strength of passwords. This is a supportive tool and does not guarantee that a password really matches the security demand of an installation.
2. Click **Set** to push and save changes.

### Password

Password 'service'	<input type="password" value="....."/>	<span style="background-color: green; color: white; padding: 2px 5px;">Strong</span>
Confirm password	<input type="password"/>	
Password 'user'	<input type="password" value="....."/>	<span style="background-color: yellow; color: black; padding: 2px 5px;">Medium</span>
Confirm password	<input type="password"/>	
Password 'live'	<input type="password" value="....."/>	<span style="background-color: red; color: white; padding: 2px 5px;">Weak</span>
Confirm password	<input type="password"/>	

Set

The **User Management** introduced with firmware version 6.30 provides more flexibility to create freely named users with own passwords. The former account levels now represent the user group levels.

### User Management

⚠ Please make sure that all users are password protected.

User name	Group	Type	
service	service	Password	<span style="color: yellow;">⚠</span>
user	user	Password	<span style="color: yellow;">⚠</span>
live	live	Password	<span style="color: yellow;">⚠</span>

Add

The former users still exist, still using the passwords that were assigned running earlier firmware, which cannot be deleted nor their user group level changed.

Passwords can be assigned or changed by clicking or .  
A warning message is displayed as long as not all users have password protection.

1. To add a new user, click **Add**.  
A pop-up window appears.

2. Enter the new credentials and assign the user group.
3. Click **Set** to save changes.



**Notice!**

With firmware version 6.32, also a stricter password policy has been introduced. Passwords now require a minimum length of 8 characters.

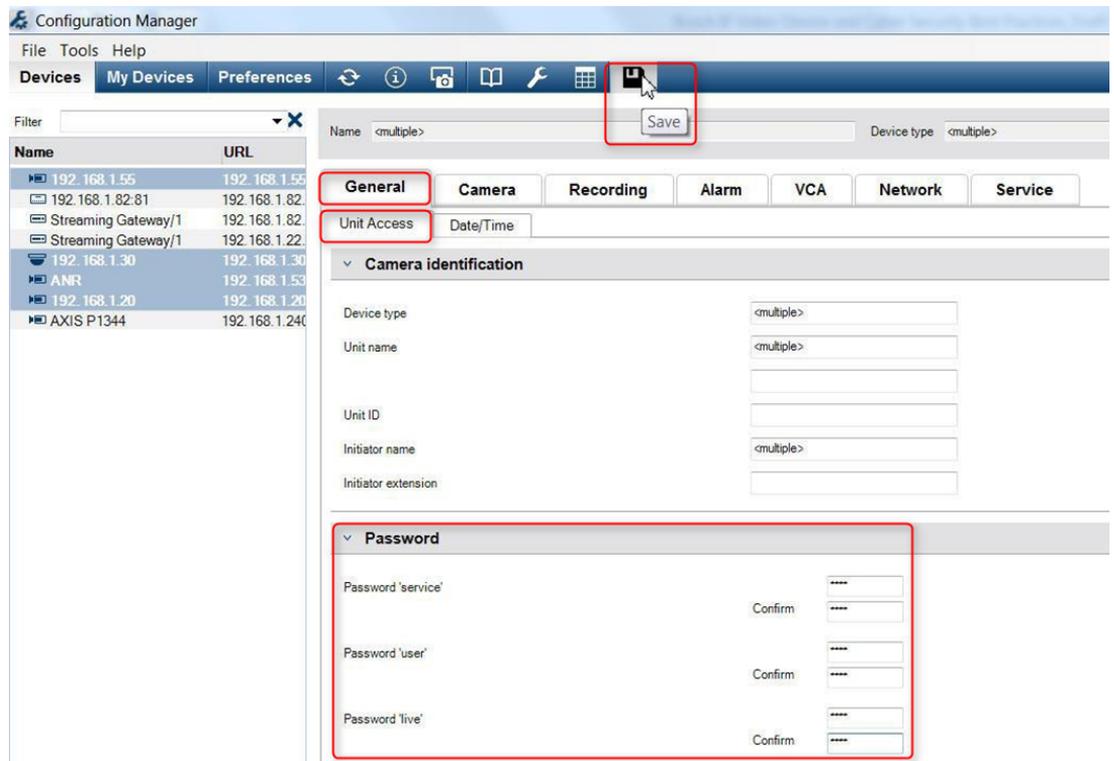
### 4.2.3

#### Assigning passwords using Configuration Manager

Utilizing Bosch Configuration Manager, passwords can be easily applied to individual or multiple devices simultaneously.

1. In the Configuration Manager, select one or more devices.
2. Select the **General** tab, then select **Unit Access**.
3. In the **Password** menu, enter and confirm the desired password for each of the three accounts (**Password 'service'**, **Password 'user'** and **Password 'live'**).

4. Click  to push and save changes.



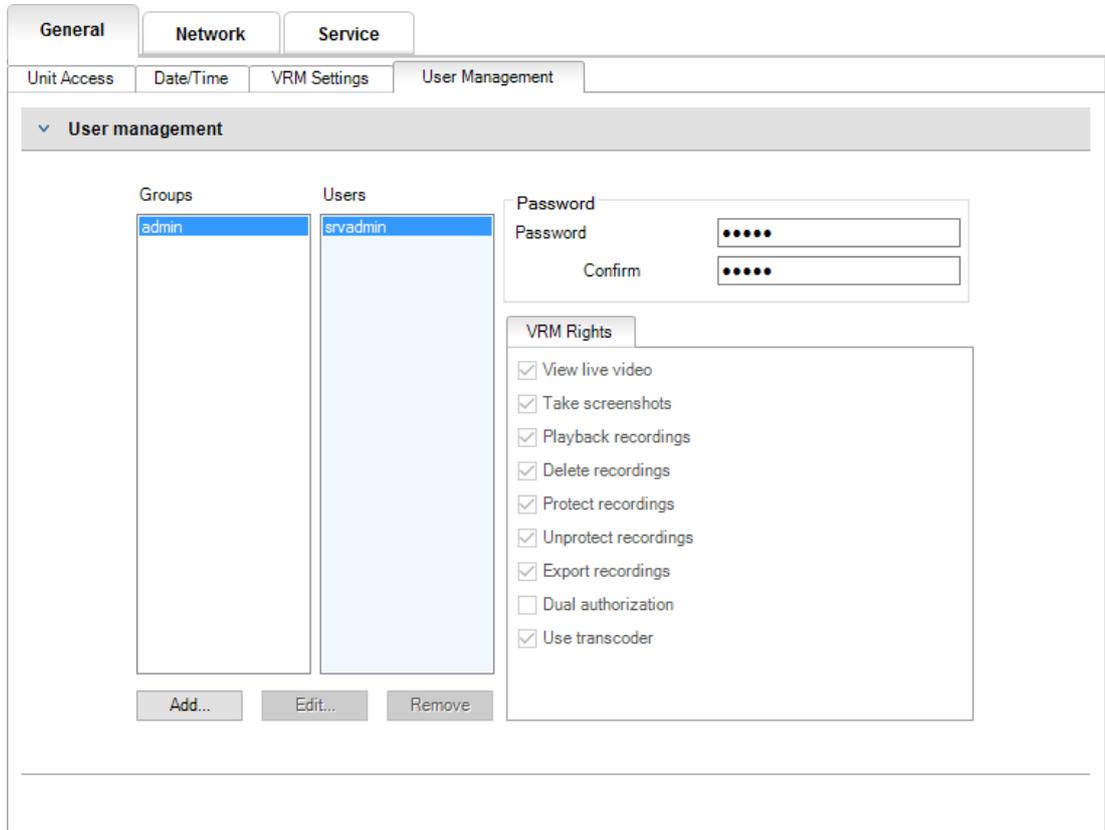
In larger installations that are managed by either BVMS, or Video Recording Manager installed on a recording appliance, global passwords can be applied to all IP video devices that are added to the system. This allows easy management and ensures a standard level of security across the entire network video system.

### 4.2.4

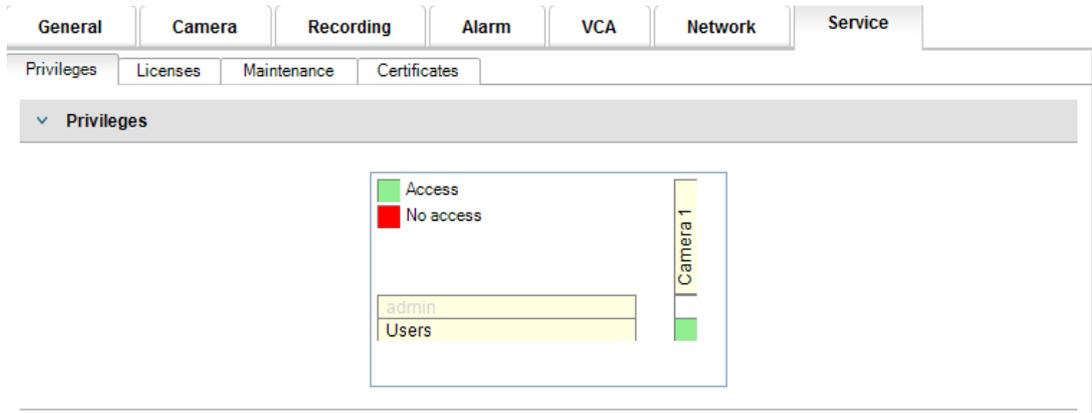
#### Assigning passwords for VRM stand-alone installation

The Video Recording Manager provides user management to enhance flexibility and security. By default, there are no passwords assigned to any of the user accounts. Password assignment is a critical step in protecting any network device. It is strongly advised to assign passwords to all installed network video devices.

The same is valid for the users of Video Recording Manager.



Additionally, members of a user group can be assigned to have access to certain cameras and privileges. Thus, a detailed user-based right-management can be achieved.



## 4.2.5 Assigning passwords using BVMS (on DIVAR IP or stand-alone)

### Device password protection

Cameras and encoders, managed by BVMS can be protected against unauthorized access with a password protection.

Passwords for the built-in user accounts of encoders / cameras can be configured with the BVMS Configuration Client.

To set a password for the built-in user accounts in the BVMS Configuration Client:

1. In the Device tree, select the desired encoder.
2. Right-click the encoder and click **Change password....**
3. Enter a password for the three built in user accounts live, user and service.

### Default password protection

BVMS versions 5.0 and higher provide the ability to implement global passwords on all devices in a video system of up to 2000 IP cameras. This feature can be accessed either via the BVMS Configuration Wizard when working with DIVAR IP 3000 or DIVAR IP 7000 recording appliances, or through BVMS Configuration Client on any system.

To access the global passwords menu in BVMS Configuration Client:

1. On the **Hardware** menu, click **Protect Devices with Default Password....**
2. In the **Global default password** field, enter a password and select **Enforce password protection on activation.**

After saving and activating system changes, the entered password will be applied to the live, user, and service accounts of all devices, including the administrator account of Video Recording Manager.



### Notice!

If the devices already have existing passwords set in any of the accounts, they will not be overwritten.

For example, if password is set for service but not for live and user, global password will only be configured for live and user accounts.

### BVMS configuration and VRM settings

By default, the BVMS uses the built-in administration account **srvadmin** to connect to Video Recording Manager with a password protection. To avoid unauthorized access to Video Recording Manager, the admin account **srvadmin** shall be protected with a complex password.

To change the password of the **srvadmin** account in BVMS Configuration Client:

1. In the Device tree, select the VRM device.
2. Right-click the VRM device and click **Change VRM Password.**  
The **Change password...** dialog box is displayed.
3. Enter a new password for the **srvadmin** account and click **OK.**

### Encrypted communication to cameras

Since BVMS version 7.0, live video data and control communication between the camera and the BVMS Operator Client, Configuration Client, Management Server and Video Recording Manager can be encrypted.

After enabling the secure connection in the **Edit Encoder** dialog box, the BVMS Server, Operator Client and Video Recording Manager will use a secure HTTPS connection in order to connect to a camera or encoder.

The BVMS internally used connection string will change from rcpp://a.b.c.d (plain RCP+ connection on port 1756) to https://a.b.c.d (HTTPS connection on port 443) instead. For legacy devices that do not support HTTPS the connection string remains unchanged (RCP+).

If selecting the HTTPS communication, the communication will utilize HTTPS (TLS) to encrypt all control communication and video payload via the encryption engine in the device. When utilizing TLS, all HTTPS control communication and video payload is encrypted with an AES encryption key up to 256 bits in length.

To enable the encrypted communication in BVMS Configuration Client:

1. In the Device tree, select the desired encoder/camera.
2. Right-click the encoder/camera and click **Edit Encoder**.
3. In the **Edit Encoder** dialog box, enable **Secure connection**.
4. Save and activate the configuration.

After enabling the secure connection to the encoder, other protocols can be disabled (see *General network port usage and video transmission, page 16*).

**Notice!**

BVMS only supports the default HTTPS port 443. Usage of different ports is not supported.

## 4.3

### Hardening device access

All Bosch IP video devices come with built-in multi-purpose web pages. The device-specific web pages support both live and playback video functions, as well as some specific configuration settings that may not be accessible via a video management system. The built-in user accounts act as the access to the different sections of the dedicated web pages. While the web page access cannot be completely disabled via the web page itself - the Configuration Manager could be used for -, there are several methods to cloak the presence of the device, restrict access, and manage video port usage.

#### 4.3.1

##### General network port usage and video transmission

All Bosch IP video devices utilize Remote Control Protocol Plus (RCP+) for detection, control, and communications. RCP+ is a proprietary Bosch protocol which uses specific static ports to detect and communicate with Bosch IP video devices - 1756, 1757, and 1758. When working with BVMS, or another 3rd-party vendor video management system that has integrated Bosch IP video devices via the Bosch VideoSDK, the listed ports must be accessible on the network for the IP video devices to function correctly.

Video can be streamed from the devices in several ways: UDP (Dynamic), HTTP (80), or HTTPS (443).

The HTTP and HTTPS port usage can be modified (see *HTTP, HTTPS and video port usage, page 17*). Prior to making any port modifications, the desired form of communication to a device must be configured. The Communication menu can be accessed using Configuration Manager.

1. In the Configuration Manager, select the desired device.
2. Select the **General** tab, then select **Unit Access**.
3. Locate the **Device access** portion of the page.



4. In the **Protocol** list, select the desired protocol:
  - RCP+
  - HTTP (default)
  - HTTPS

If selecting HTTPS communications, communication between Configuration Manager and video devices will utilize HTTPS (TLS) to encrypt the payload with an AES encryption key up to 256 bits in length. This is a free basic feature. When utilizing TLS, all HTTPS control communications and video payload is encrypted via the encryption engine in the device.



**Notice!**

The encryption is specifically for the "transmission path". After video is received by either a software or hardware decoder, the stream is permanently decrypted.

### 4.3.2 Minimum TLS version

Some older clients might need to use older and less secure TLS versions. However, if possible define a minimum version for TLS to avoid clients forcing the device into a less secure access mode.

Select the highest possible TLS version as a minimum version.



**Notice!**

When defining the minimum level of security to access devices from a client software, make sure that all ports and protocols that allow a lower access level are switched off or disabled in the devices.

### 4.3.3 HTTP, HTTPS and video port usage

HTTP and HTTPS port usage on all devices can be altered or turned off. Encrypted communication can be enforced by disabling RCP+ port as well as the HTTP port, forcing all communication to use encryption. If HTTP port usage is turned off, HTTPS will remain on and any attempts to turn it off will fail.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **Network Access**.
3. Locate the **Details** portion of the page.



4. In the **Details** portion, modify the HTTP and HTTPS browser ports and RCP+ port using the drop down menu:
  - HTTP browser port modification: 80 or ports 10000 to 10100
  - HTTPS browser port modification: 443 or ports 10443 to 10543
  - RCP+ port 1756: **On** or **Off**

**Notice!**

In firmware release 6.1x, if the HTTP port is disabled and an attempt to access the device's web page is made, the request will be directed to the HTTPS port that is currently defined. The redirect feature is omitted in firmware release 6.20 and higher. If the HTTP port is disabled and the HTTPS port has been modified to utilize a port other than 443, accessing the web pages can only be accomplished by navigating to the device's IP address plus the assigned port.

**Example:**

https://192.168.1.21:10443. Any attempts to connect to the default address will fail.

**4.3.4****Video software and port selection**

Adjusting these settings will also affect what port is utilized for video transmission when using video management software in your LAN.

If all IP video devices are set to HTTP port 10000, as an example, and the BVMS Operator Client is configured for "TCP tunneling", then all video transmissions on the network will be made across HTTP port 10000.

**Notice!**

Changes to port settings in devices must match the settings in the management system and its components as well as in the clients.

**Notice!**

Depending on the deployment scenario and security goals of the installation, best practices can vary. Disabling and redirecting port usage of either HTTP or HTTPS has its benefits. Changing the port in either protocol can help avoid supplying information to network tools such as NMAP (Network Mapper, free security scanner). Applications like NMAP are typically used as reconnaissance tools to identify weaknesses in any device on a network. This technique combined with strong password implementation adds to the overall security of the system.

**4.3.5****SSH tunneling**

For a remote device access with BVMS Operator Client via public networks, BVMS provides Secure Shell (SSH) tunneling to ensure secure (encrypted) communication. SSH tunneling constructs an encrypted tunnel established by an SSH protocol/socket connection. This encrypted tunnel can provide transport to both, encrypted and un-encrypted traffic. The Bosch SSH implementation also utilizes Omni-Path protocol, which is a high performance low latency communications protocol developed by Intel.

For more information on how to configure the SSH service in BVMS, refer to the BVMS documentation.

For more information on how to configure DIVAR IP systems for a secure remote access with BVMS Operator Client, refer to the DIVAR IP documentation.

**4.3.6****Telnet Access**

Telnet is an application layer protocol that provides communication to devices via a virtual terminal session for maintenance and troubleshooting purposes. All Bosch IP video devices are Telnet capable, and by default Telnet support is turned on in firmware releases up to 6.1x. From firmware release 6.20 onwards, the Telnet port is disabled by default.



**Notice!**

There has been an increase in cyber-attacks utilizing the Telnet protocol since 2011. In today’s environment, best practices state you should disable Telnet support on all devices until it is needed for either maintenance or troubleshooting.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **Network Access**.
3. Locate the **Details** portion of the page.



4. In the **Details** portion, turn **Telnet support On** or **Off** using the dropdown menu.



**Notice!**

Since firmware release 6.20 Telnet is also supported via so-called "web sockets", which use secure HTTPS connections. Web sockets are not using the standard Telnet port, and provide a secure way of accessing the IP device’s command line interface if required.

**4.3.7**

**RTSP: Real Time Streaming Protocol**

Real Time Streaming Protocol (RTSP) is the primary video component utilized by the ONVIF protocol to provide streaming video and device control to ONVIF conformant video management systems. RTSP is also utilized by various third party video applications for basic streaming functions, and in some cases, can be used for device and network troubleshooting. All Bosch IP video devices are capable of providing streams using the RTSP protocol. RTSP services can be easily modified using Configuration Manager.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **Advanced**.



3. Locate the **RTSP** portion of the page.
4. In the **RTSP port** dropdown menu switch off or modify the RSTP service:
  - RTSP default port: 554
  - RTSP port modification: 10554 to 10664



**Notice!**

There have been recent reports of cyberattacks utilizing an RTSP stack overflow buffer assault. These attacks were written to target specific vendors’ devices. Best practices would be to disable the service if it is not being utilized by an ONVIF conformant video management system or for basic real-time streaming.

Alternatively, and when the receiving client allows, the RTSP communication can be tunneled using a HTTPS connection, which is so far the only way to transmit RTSP data encrypted.



**Notice!**

For more details on RTSP, refer to the Application note *RTSP usage with Bosch VIP Devices* in the Bosch Security Systems online product catalog under the following link:

[https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP\\_VIP\\_Application\\_note\\_enUS\\_9007200806939915.pdf](https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP_VIP_Application_note_enUS_9007200806939915.pdf)

**4.3.8**

**UPnP: Universal Plug and Play**

Bosch IP video devices are capable of communicating with network devices via **UPnP**. This feature is primarily utilized in smaller systems with only a few cameras where the cameras automatically appear in the PC’s network directory and thus can easily be found. But so they do for any device in the network.

**UPnP** can be turned off using Configuration Manager.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **Network Management**.



3. Locate the **UPnP** portion of the page.
4. In the **UPnP** dropdown menu, select **Off** to disable **UPnP**.



**Notice!**

**UPnP** should not be used in large installations due to the large number of registration notifications and the potential risk of unwanted access or attack.

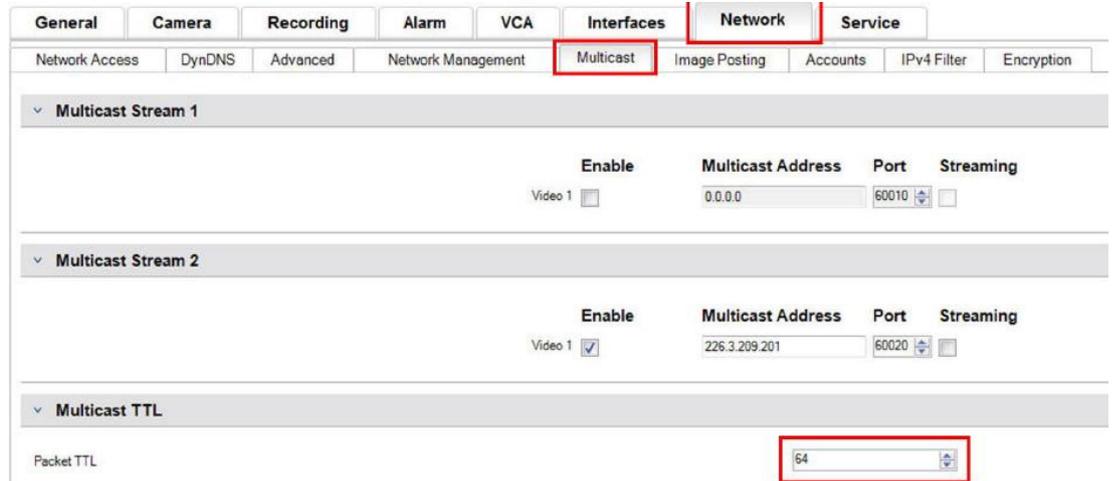
**4.3.9**

**Multicasting**

All Bosch IP video devices are capable of providing both “Multicast on Demand” or “Multicast Streaming” video. Where unicast video transmissions are destination based, multicast is source based and this can introduce security issues at the network level, including: group access control, group center trust, and router trust. While router configuration is beyond the scope of this guide, there is a security solution that can be implemented from the IP video device itself.

TTL (time-to-live) scoping defines where and how far multicast traffic is allowed to flow within a network, each hop decreasing TTL by one. When configuring IP video devices for multicast usage, the packet TTL of the device can be modified.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **Multicast**.
3. Locate the **Multicast TTL** portion of the page.
4. Adjust the **Packet TTL** settings using the following TTL values and Scoping Limits:
  - TTL Value 0 = Restricted to local host
  - TTL Value 1 = Restricted to same subnet
  - TTL Value 15 = Restricted to same site
  - TTL Value 64 (Default) = Restricted to same region
  - TTL Value 127 = Worldwide
  - TTL Value 191 = Worldwide with limited bandwidth
  - TTL Value 255 = Unrestricted Data



**Notice!**

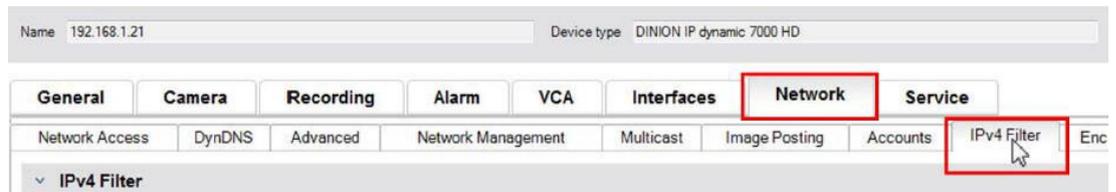
When dealing with video surveillance data, a best practice would be to set your TTL settings to 15, restricted to same site. Or better, if you know the exact maximum number of hops, use this a TTL value.

**4.3.10**

**IPv4 filtering**

You can restrict access to any Bosch IP video device via a feature called IPv4 filtering. IPv4 filtering utilizes the basic fundamentals of "subnetting" to define up to two allowable IP address ranges. Once defined, it denies access from any IP address outside these ranges.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **IPv4 Filter**.



**Notice!**

To successfully configure this feature, you must have basic understanding of subnetting or have access to a subnet calculator. Entering incorrect values into this setting can restrict access to the device itself and a factory default reset may need to be performed to regain access.

3. To add a filter rule, make two entries:
  - Enter a base IP address that falls within the subnet rule you create. The base IP address specifies which subnet you are allowing and it must fall within the desired range.
  - Enter a subnet mask that defines the IP addresses with which the IP video device will accept communication.

In the following example the **IP address 1** of 192.168.1.20 and the **Mask 1** of 255.255.255.240 have been entered. This setting will restrict access from devices that fall within the defined IP range of 192.168.1.16 to 192.168.1.31.

General	Camera	Recording	Alarm	VCA	Interfaces	Network	Service	
Network Access	DynDNS	Advanced	Network Management	Multicast	Image Posting	Accounts	IPv4 Filter	Encryption
<b>IPv4 Filter</b>								
IP address 1	192.168.1.20							
Mask 1	255.255.255.240							
IP address 2	0.0.0.0							
Mask 2	0.0.0.0							

While utilizing the **IPv4 Filter** feature devices will be able to be scanned via RCP+, but access to configuration settings and video is not possible via clients that fall outside the allowed IP address range. This includes web browser access.

The IP video device itself does not need to be located in the allowed address range.

### Notice!



Based on the set-up of your system, utilizing the **IPv4 Filter** option can reduce unwanted visibility of devices on a network. If enabling this function, make sure to document settings for future reference.

Note that the device will still be accessible via IPv6, so IPv4 filtering only makes sense in pure IPv4 networks.

## 4.3.11

### SNMP

Simple Network Management Protocol (SNMP) is a common protocol to monitor the health status of a system. Such a monitoring system typically has a central management server that collect all the data from the system's compatible components and devices.

SNMP provides two methods to gain the system health status:

- The network management server can poll the health status of a device via SNMP requests.
- Devices can actively notify the network management server about their system health status in case of error or alarm conditions through sending SNMP traps to the SNMP server. Such traps must be configured inside the device.

SNMP also allows configuration of some variables inside devices and components.

The information, which messages a device supports and which traps it can send, is derived from the Management Information Base, the so-called MIB file, a file that is delivered with a product for easy integration into a network monitoring system.

There are three different version of the SNMP protocol:

- SNMP version 1
  - SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. It is widely used and has become the de facto standard protocol for network management and monitoring.
  - But SNMPv1 has become under threat due to its lack of security features. It only uses '*community strings*' as a kind of passwords, which are transmitted in clear text.
  - Thus, SNMPv1 shall only be used when it can be assured that the network is physically protected against unauthorized access.
- SNMP version 2
  - SNMP version 2 (SNMPv2) included improvements in security and confidentiality, amongst others, and introduced a bulk request to retrieve large amounts of data in a single request. However, its security approach was considered way too complex, hindering its acceptance.

Thus, it was soon pushed out by version SNMPv2c, which equals SNMPv2 but without its controversial security model, reverting to the community-based method from SNMPv1 instead, similarly lacking security.

- SNMP version 3  
SNMP version 3 (SNMPv3) mainly adds security and remote configuration enhancements. These include improvements on confidentiality by encryption of packets, message integrity and authentication.  
It also addresses large-scale deployment of SNMP.



**Notice!**

Both SNMPv1 and SNMPv2c have become under threat due to their lack of security features. They only use 'community strings' as a kind of passwords, which are transmitted in clear text. Thus, SNMPv1 or SNMPv2c should only be used when it can be assured that the network is physically protected against unauthorized access.

Bosch cameras currently only support SNMPv1. Make sure to have SNMP switched off if you do not use it.

**4.3.12**

**Secure time basis**

In addition to Time protocol and SNTP, which are both non-secured protocols, a 3rd mode for the Timeserver client has been introduced with FW 6.20, using TLS protocol. This method is also commonly known as *TLS-Date*.

In this mode any arbitrary HTTPS server can be used as time server. The time value is derived as a side-effect from the HTTPS hand-shake process. The transmission is TLS secured. An optional root certificate for the HTTPS server can be loaded to the camera's certificate store to authenticate the server.

The screenshot shows the 'Configuration' menu with 'Date/Time' selected. The 'Date/Time' settings are as follows:

- Date format: DD.MM.YYYY
- Device date: Sunday, 22, 01, 2017
- Device time: 13 : 00 : 13
- Device time zone: (UTC +1:00) Western & Central Europe
- Daylight saving time: Details
- Time server IP address: 192.168.0.2
- Overwrite by DHCP:
- Time server type: TLS protocol (selected from a dropdown menu that also includes Time protocol, SNTP protocol, and Off)

**Notice!**

Make sure that the entered time server IP address has a stable and uncompromised time base itself.

**4.3.13****Cloud-based services**

All Bosch IP video devices can communicate with Bosch cloud-based services such as Remote Portal. Depending on the region of deployment, this allows IP video devices to use services such as Remote Device Management or Cloud VMS to forward alarms and other data to a central station.

For further information, refer to the Bosch Building Technologies Knowledge Base: <https://community.boschsecurity.com>.

There are three modes of operation for cloud-based services:

- **On:**  
The video device will constantly poll the cloud server.
- **Auto (default):**  
The video devices will attempt to poll the cloud server a few times, and if unsuccessful, it will cease attempting to reach the cloud server.
- **Off:**  
No polling is performed.

Cloud-based services can be easily turned off using Configuration Manager.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select the tab **Advanced**.
3. Locate the **Cloud-based services** section of the page and select **Off** from the list.

**Notice!**

If you are utilizing Bosch cloud-based services, keep the default configuration. In all other cases switch the cloud-based services mode to **Off**.

**4.4****Hardening IP cameras**

Bosch IP cameras are delivered with a default configuration that allows easy integration into different environments.

Depending on the target environment and its intended security level, it might be required to change some camera settings to increase cyber and data security.

However, there can be limitations of the operational environment that mandates the use of a certain protocol or a feature, which is less secure (for example SNMPv1).

**4.4.1****Hardening levels**

There are two levels of hardening defined: *elevated* and *strict*.

Hardening level *strict* features the most secure means of setting up a device but might be limiting the usage of the device as features like auto discovery of a device are disabled. For each feature, it should be evaluated if the setting *elevated* or *strict* can be applied.

#### 4.4.2 Hardening overview

Network - Network Services	Default	Elevated	Strict
HTTP	Enabled	Disabled	Disabled
HTTPS	Enabled	Enabled	Enabled
RTSP	Enabled	Optional	Disabled
RCP	Enabled	Disabled	Disabled
SNMPv1	Disabled	Disabled	Disabled
SNMPv3	Disabled	Enabled	Enabled
iSCSI	Enabled	Optional	Disabled
UPnP	Disabled	Disabled	Disabled
NTP server	Disabled	Disabled	Disabled
Discovery	Enabled	Enabled	Disabled
ONVIF Discovery	Enabled	Enabled	Disabled
GBT/28181	Disabled	Disabled	Disabled
Password reset mechanism	Enabled	Disabled	Disabled
Ping response	Enabled	Enabled	Disabled
RTSPS	Enabled	Enabled	Enabled
HTTP	Enabled	Disabled	Disabled

Network - Network Access	Default	Elevated	Strict
Minimum TLS version	1.0	1.2	1.2
HSTS	Disabled	Enabled	Enabled

Network - Advanced	Default	Elevated	Strict
802.1x	Disabled	Optional	Enabled
Syslog	Disabled	TCP	TLS

Network - Network Management	Default	Elevated	Strict
SNMPv3 mode	Disabled	SHA1 / AES	SHA1 / AES

Network - IPv4 Filter	Default	Elevated	Strict
IPv4 filter	Disabled	Enabled	Enabled

General - Date/Time	Default	Elevated	Strict
Date/Time (NTP Client)	Disabled	SNTP / TLS Date	TLS Date

Connectivity - Cloud services	Default	Elevated	Strict
Remote Portal	Disabled	Enabled	Enabled

Service - Logging	Default	Elevated	Strict
Software sealing	Disabled	Enabled	Enabled

### 4.4.3

## Feature description and hardening recommendations

### HTTP

HTTP is enabled by default, but unencrypted, so credentials or settings are transferred unencrypted if used.

**Recommendation:** Plain HTTP should be disabled in favor of the encrypted HTTPS, especially if the network is untrusted.

### HTTPS

HTTPS is encrypted and should be the default choice for accessing the web interface or access the web-based RCP API. Using own PKI and certificates is recommended.

**Recommendation:** HTTPS is the default secure protocol used for configuration and should remain enabled.

### RTSP

RTSP is used for video streaming, but normally unencrypted. If the software receiving the video stream is capable of using RTSPS, it is recommended to disable plain RTSP. When using other Bosch components (for example decoders/BVMS/VRM/DIVAR IP) a Bosch proprietary encryption for RTSP can be enabled, making transmission secure.

**Recommendation:** Risk based approach if video can be transmitted unencrypted or via Bosch encryption. If possible, use encrypted RTSPS.

### RCP

The Bosch proprietary Remote Control Protocol plus is the configuration protocol for Bosch IP cameras. Plain RCP is unencrypted, so settings are transferred unencrypted. All Bosch tools now use RCP over HTTPS communication for some time, but it might be needed for 3rd party integration tools or scripting tools still relying on this protocol.

**Recommendation:** Disable RCP if not used by 3rd party tools or legacy systems.

**SNMPv1**

SNMP is the common network monitoring protocol used to query health information of a device or send out trap to a remote receiver, but unencrypted.

**Recommendation:** Keep disabled if not required for health monitoring or other compatibility reasons. Use SNMPv3 if possible.

**SNMPv3**

SNMPv3 is successor of SNMPv1 and can also be used encrypted.

**Recommendation:** Recommended if SNMP monitoring must be implemented.

**iSCSI**

Disables the internal iSCSI server which is used to make internal recordings on the camera accessible via iSCSI. iSCSI is an unencrypted protocol.

**Recommendation:** Disable iSCSI server if not used on the camera.

**UPnP**

Making the camera discoverable via UPnP protocol.

**Recommendation:** Disable UPnP if not needed.

**NTP server**

Enable an NTP server on the camera to allow other devices or cameras to synchronize the time. If possible, a dedicated device should serve time to the camera network allowing separation of services. If no other device is available, time can be served by a camera.

**Recommendation:** NTP server should be disabled if not needed.

**Discovery**

Using a Bosch propriety mechanism to make cameras discoverable by a Bosch software, such as Configuration Manager.

**Recommendation:** When working with dynamic IP addresses this feature should remain enabled. When working in an environment with fixed IP addresses, this feature can be turned off.

**ONVIF Discovery**

Support the discovery of camera devices via the ONVIF Discovery protocol

**Recommendation:** When working with dynamic IP addresses and ONVIF compliant tools, this feature should remain enabled. When working in a fixed environment with fixed IP addresses, this feature can be turned off.

**GBT/28181**

GBT/28181 is a Chinese standard for interoperability between different devices.

**Recommendation:** Keep disabled if not required.

**Password reset mechanism**

IP cameras can be mounted in very remote locations which makes it hard to do maintenance work or a factory reset in case that the access to the camera has been locked. Bosch offers the possibility to reset the password of a camera via challenge-response mechanism based on a secure public/private key mechanism.

**Recommendation:** If this feature is not needed, it is recommended to disable it.

### Ping response

Configures if the camera answers to ping requests in the network. Can help with debugging. In a high secure network this can be disabled to avoid device enumeration via ping sweep, although there are several other means of device discovery that can be used by an attacker.

**Recommendation:** Risk based approach, can be disabled for high security networks.

### RTSPS

RTSPS is the encrypted version of RTSP and used for video streaming. If the receiving software supports it, RTSPS should always be preferred over plain RTSP. As many RTSP clients do not support the secure variant, RTSP is still enabled for Level 1 security.

**Recommendation:** Use RTSPS if possible.

### Minimum TLS version

IP cameras do not allow unsecure SSLv3 or older connections. TLS 1.0 and 1.1 are deprecated by the IETF and there are potential security issues known (BEAST, FREAK).

CPP4, CPP6, CPP7 and CPP7.3 cameras support the secure TLS 1.2, which should be set as minimum required version.

CPP13 and CPP14 cameras do not allow TLS versions earlier than 1.2. They also support the newer TLS 1.3 specification.

**Recommendation:** Set minimum TLS version to 1.2.

### HSTS

HTTP Strict Transport Security (HSTS) is a policy set by a website to protect against man-in-the-middle attacks and protocol downgrade attacks. It allows the website to tell the browser to only allow HTTPS connections within this connection and not allow any unencrypted HTTP connections.

**Recommendation:** Enable HSTS on the camera.

### 802.1x

802.1x is a standard for Network Access Control (NAC). It allows devices to authenticate in the network, granting only authenticated devices access to the network. Bosch IP cameras support 802.1x either with password or certificate-based authentication, with certificate-based authentication being the preferred method. To use 802.1x the network switch must support this standard, and an authentication server is needed.

**Recommendation:** If the network infrastructure allows it, use network authentication with 802.1x.

### Syslog

As the camera does only provide a limited space for log messages, log messages should be sent to a central location and analyzed there to detect any attacks or misconfigurations.

**Recommendation:** Use TCP Syslog to avoid losing messages due to packet loss. Use Syslog with TLS to encrypt and authenticate messages.

### SNMPv3 mode

SNMPv3 is the successor of SNMPv1 and allows for secure authentication and transfer of information.

**Recommendation:** When using SNMPv3, use SHA1 as authentication protocol and AES as privacy protocol (if supported).

#### **IP filter**

In IP Filter several IP addresses (single hosts or network subnets) can be defined, that are allowed to access the camera. It is recommended to define the computers or networks accessing the camera here.

**Recommendation:** It is recommended to use the IP filter to define allowed hosts or networks.

#### **Date/Time**

To have the correct timestamp on logs and video data, it is recommended to synchronize the time to a central timeserver. Both, SNTP and TLS date can be used to achieve this. The advantage of SNTP is a more precise time synchronization. The advantage of TLS date is the possibility to check for a correct certificate, making it the more secure solution.

**Recommendation:** Use a secure means of synchronizing time, either with SNTP or TLS date.

#### **Cloud-based services**

Bosch offers its own cloud-based services to manage cameras over the Bosch cloud (Remote Portal). The cloud services do not automatically connect to Remote Portal and are disabled by default. Each camera needs to be connected to Remote Portal first if it should be used. Every precaution has been taken to secure the connection between Remote Portal and camera, so if needed Remote Portal can be used in any environment.

**Recommendation:** Remote Portal can be used depending on if cloud solution is in use.

#### **Software sealing**

After a completed configuration of an IP camera, the settings of the device should not change. A software seal can be enabled to notify of device configuration changes.

**Recommendation:** Enable software sealing if there are no pending configuration changes.

### **4.4.4**

#### **Defense in depth**

Defense in depth refers to a layered security approach, where no single measure alone is responsible for the security of a product, but there are multiple layers that an attacker needs to breach to exploit a product. At each release of a product, it is evaluated if new features are needed to mitigate new attacks or to increase overall security of the product.

Here is an overview of the main security functions of the IP camera.

- **Firmware signing**

Each firmware update file is encrypted and signed by a Bosch certificate. Only updates published by Bosch can be installed on the cameras, avoiding installation of malicious firmware.

- **Secure Boot**

Cameras of platforms CPP13, CPP14 or newer, feature a Secure Boot mechanism. Secure Boot checks the integrity of the whole system, starting with the bootloader and continuing with the firmware itself on the cameras, each step of the boot process is verifying the next, starting with an unchangeable hardware root of trust. This prevents an attacker to modify bootloader or firmware on the device.

- **Login Firewall**  
To protect against password brute forcing but at the same time allowing administrators to login and to protect against Denial of Service (DoS) attacks, the login firewall checks login attempts based on behavioral analysis and dynamically blocks or allows access based on IP addresses.
- **Camera authentication**  
To uniquely identify and authenticate a camera, a Bosch device certificate is created on each camera during production. This certificate can be used to check whether communicating with a genuine Bosch device. In addition, custom certificates can be uploaded or created on the camera to provide integration with a PKI environment to protect against man-in-the-middle attacks.

## 4.5 Hardening storage

As Bosch IP-cameras or encoders are capable of establishing an iSCSI session directly to an iSCSI drive and write video data to an iSCSI drive, the iSCSI units have to be connected to the same LAN or WAN as the Bosch peripheral devices.

To avoid unauthorized access to the recorded video data, the iSCSI units have to be protected against unauthorized access:

- Use password authentication via CHAP to ensure only known devices are allowed to access the iSCSI target. Set 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 a CHAP password is used in a BVMS VRM environment, all storage systems have to be configured to use the same password.
- Remove all default usernames and passwords from the iSCSI target.
- Use strong password for administrative user accounts of the iSCSI target.
- Disable administrative access via Telnet to the iSCSI targets. Use SSH access instead.
- Protect console access to the iSCSI target via strong password.
- Disable unused network interface cards.
- Monitor system status of iSCSI storages via 3rd party tools to identify anomalies.

### 4.5.1 Setting a CHAP password on iSCSI devices

When you set a global CHAP password in BVMS Configuration Client, this password is automatically transferred to all encoders, decoders and VSG devices.

For some iSCSI devices this function is not supported. You have to set the CHAP password on these devices manually.



#### Notice!

You have to set the global CHAP password on the iSCSI devices before adding them to BVMS. iSCSI devices cannot be added to a BVMS configuration where the global CHAP password is already activated.

**To manually set a CHAP password on an iSCSI device (for example DIVAR IP), which is based on a recent version of the Microsoft Windows Server operating system:**

1. Open the **Server Manager** and navigate to **File and Storage Services > iSCSI**.
2. In the **iSCSI TARGETS** list, right-click the desired iSCSI target and click **Properties**.  
The **Properties** dialog box is displayed.
3. In the **Properties** dialog box, click **Security**, then select the check box **Enable CHAP**.
4. Enter the following:
  - **User name:** user

- **Password:** enter the global CHAP password as given in the BVMS Configuration Client (under the menu **Hardware > Protect iSCSI storages with CHAP password...**).
5. Click **OK**.  
The CHAP password is assigned to the iSCSI target.

## 4.6 Hardening servers

### 4.6.1 Server Hardware recommended settings

- 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.
- In order to prevent data transfer to the server, the USB ports and the CD / DVD drive shall be disabled.  
In addition the unused NIC ports shall be disabled and management ports like the HP ILO (HP Integrated Lights-Out) interface or console ports shall be either disabled or password protected.

### 4.6.2 Windows Operating System recommended security settings

Servers shall be part of a Windows Domain.

With the integration of the servers to a Windows domain, user permissions are assigned to network users managed by a central server. Since these user accounts often implement password strength and expiration rules, this integration may improve security over local accounts which do not have these restrictions.

### 4.6.3 Windows updates

The Windows software patches and updates shall be installed and shall remain up to date. 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.

### 4.6.4 Installation of anti-virus software

Install anti-virus and anti-spyware software and keep it up to date.

### 4.6.5 Windows Operating System recommended settings

The following Local Group Policy Settings are recommended group settings in a Windows Server Operating System. To change the default Local Computer Policies (LCP), use the Local Group Policy Editor.

You can open the Local Group Policy Editor by using the command line or by using the Microsoft Management Console (MMC).

To open the Local Group Policy Editor from the command line:

- ▶ Click **Start**, in the **Start** search box type **gpedit.msc**, and then press Enter.

To open the Local Group Policy Editor as an MMC snap-in:

1. Click **Start**, in the **Start** Search box, type **mmc**, and then press Enter.
2. In the **Add or Remove Snap-ins** dialog box, click **Group Policy Object Editor**, and then click **Add**.
3. In the **Select Group Policy Object** dialog box, click **Browse**.
4. Click **This computer** to edit the Local Group Policy object, or click **Users** to edit Administrator, Non Administrator, or per-user Local Group Policy objects.

5. Click **Finish**.

#### 4.6.6

##### Activate User Account Control on the server

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options**

User Account Control: Admin Approval Mode for the built-in Administrator account	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

**Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> Credential User Interface**

Enumerate administrator accounts on elevation	Disabled
---	----------

#### 4.6.7

##### Deactivate AutoPlay

**Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies**

Turn off AutoPlay	Enabled all drives
Default behavior for AutoRun	Enabled, do not execute any AutoRun commands
Turn off AutoPlay for non-volume devices	Enabled

#### 4.6.8

##### External Devices

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options**

Devices: Allow undock without having to log on	Disabled
Devices: Allowed to format and eject removable media	Administrators

Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled

#### 4.6.9

### Configuration of user rights assignment

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment**

Access Credential Manager as a trusted caller	No one
Access this computer from the network	Authenticated users
Act as part of the operating system	No one
Add workstations to domain	No one
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Change the system time	Administrators
Change the time zone	Administrators, Local Service
Create a page file	Administrators
Create a token object	No one
Create permanent shared objects	No one
Deny access to this computer from the network	Anonymous Logon, Guest group
Deny log on as a batch job	Anonymous Logon, Guest group
Deny log on as a service	No one
Deny log on locally	Anonymous Logon, Guest group
Deny log on through Remote Desktop Services	Anonymous Logon, Guest
Enable computer and user accounts to be trusted for delegation	No one
Force shutdown from a remote system	Administrators
Generate security audits	Local Service, Network Service
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Modify an object label	No one
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators

Profile single process	Administrators
Remove computer from docking station	Administrators
Restore files and directories	Administrators
Shut down the system	Administrators
Synchronize directory service data	No one
Take ownership of files or other objects	Administrators

#### 4.6.10

##### Screen saver

- Activate password protected screen saver and define timeout time:

**Local Computer Policies -> User Configuration -> Administrative Templates -> Control Panel -> Personalization**

Enable Screen saver	Enabled
Password protect the screen saver	Enabled
Screen saver timeout	1800 second

#### 4.6.11

##### Activate password policy settings

- Enabling password policy settings ensures users passwords meet minimum password requirements

**Local Computer Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy**

Enforce password history	10 passwords remembered
Maximum Password Age	90 days
Minimum Password Age	1 day
Minimum Password Length	10 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

#### 4.6.12

##### Disable non-essential Windows Services

- Disabling non-essential Windows Services enables a higher security level and minimizes points of attacks.

Application Layer Gateway Service	Disabled
Application Management	Disabled
Computer Browser	Disabled
Distributed Link Tracking Client	Disabled
Function Discovery Provider Host	Disabled
Function Discovery Resource Publication	Disabled
Human Interface Device Access	Disabled

Internet Connection Sharing (ICS)	Disabled
Link-Layer Topology Discovery Mapper	Disabled
Multimedia Class Scheduler	Disabled
Offline Files	Disabled
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
Routing and Remote Access	Disabled
Shell Hardware Detection	Disabled
Special Administration Console Helper	Disabled
SSDP Discovery	Disabled

### 4.6.13 Windows Operating System user accounts

The Windows Operating System user accounts have to be protected with complex passwords. Servers are normally managed and maintained with Windows administrator accounts, ensure that strong passwords are used for the administrator accounts.

Passwords must contain characters from three of the following categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: ~!@#\$%^&\* \_+=` \(){}[];:"'<>.,?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

Use of Windows Account Lockout to make it harder for password-guessing attacks to succeed. Windows 8.1 Security Baselines recommendation is 10/15/15:

- 10 bad attempts
- 15 minute lockout duration
- Counter reset after 15 minutes

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy**

Account lockout duration	Account lockout duration
15 minutes Account lockout threshold 10 failed logon attempts	15 minutes Account lockout threshold 10 failed logon attempts
Reset account lockout counter after	Reset account lockout counter after

- Ensure that all default password of the server and the Windows Operating system are replaced with new strong passwords.

### 4.6.14 Enable firewall on the server

- ▶ Enable communication of BVMS standard port according to BVMS ports.

**Notice!**

Refer to the BVMS documentation for relevant port settings and usage. Be sure to re-check settings on upgrades of firmware or software.

## 4.7 Hardening Windows clients

### 4.7.1 Windows Workstations

The Windows desktop operating systems, used for BVMS Client applications like the BVMS Operator Client or Configuration Client, are installed outside of the secure area. The workstations have to be hardened to protect the video data, the documents and other applications against unauthorized access.

The following settings should be applied or checked.

### 4.7.2 Windows Workstation hardware recommended settings

- Set a BIOS / UEFI password to restrict people from booting alternative operating systems.
- In order to prevent data transfer to the client, the USB ports and the CD / DVD drive shall be disabled. In addition the unused NIC ports shall be disabled.

### 4.7.3 Windows Operating System recommended security settings

- Workstation shall be part of a Windows Domain.  
Integration of the workstation to a Windows domain, security relevant settings can be managed centrally.
- Windows updates  
Stay up to date with windows operating software patches and updates.
- Installation of Antivirus software  
Install Antivirus and antispysware software and keep it up to date.

### 4.7.4 Windows Operating System recommended settings

The following Local Group Policy Settings are recommended group settings in a Windows Server Operating System. To change the default Local Computer Policies (LCP), use the Local Group Policy Editor.

You can open the Local Group Policy Editor by using the command line or by using the Microsoft Management Console (MMC).

To open the Local Group Policy Editor from the command line:

- ▶ Click **Start**, in the **Start** search box type **gpedit.msc**, and then press Enter.

To open the Local Group Policy Editor as an MMC snap-in:

1. Click **Start**, in the **Start** Search box, type **mmc**, and then press Enter.
2. In the **Add or Remove Snap-ins** dialog box, click **Group Policy Object Editor**, and then click **Add**.
3. In the **Select Group Policy Object** dialog box, click **Browse**.
4. Click **This computer** to edit the Local Group Policy object, or click **Users** to edit Administrator, Non Administrator, or per-user Local Group Policy objects.
5. Click **Finish**.

### 4.7.5 Activate User Account Control on the server

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options**

User Account Control: Admin Approval Mode for the built-in Administrator account	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

**Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> Credential User Interface**

Enumerate administrator accounts on elevation	Disabled
---	----------

**4.7.6 Deactivate AutoPlay**

**Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies**

Turn off AutoPlay	Enabled all drives
Default behavior for AutoRun	Enabled, do not execute any AutoRun commands
Turn off AutoPlay for non-volume devices	Enabled

**4.7.7 External Devices**

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options**

Devices: Allow undock without having to log on	Disabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled

## 4.7.8

**Configuration of user rights assignment**

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment**

Access Credential Manager as a trusted caller	No one
Access this computer from the network	Authenticated users
Act as part of the operating system	No one
Add workstations to domain	No one
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Change the system time	Administrators
Change the time zone	Administrators, Local Service
Create a page file	Administrators
Create a token object	No one
Create permanent shared objects	No one
Deny access to this computer from the network	Anonymous Logon, Guest group
Deny log on as a batch job	Anonymous Logon, Guest group
Deny log on as a service	No one
Deny log on locally	Anonymous Logon, Guest group
Deny log on through Remote Desktop Services	Anonymous Logon, Guest
Enable computer and user accounts to be trusted for delegation	No one
Force shutdown from a remote system	Administrators
Generate security audits	Local Service, Network Service
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Modify an object label	No one
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Remove computer from docking station	Administrators
Restore files and directories	Administrators
Shut down the system	Administrators

Synchronize directory service data	No one
Take ownership of files or other objects	Administrators

### 4.7.9

#### Screen saver

- Activate password protected screen saver and define timeout time:

**Local Computer Policies -> User Configuration -> Administrative Templates -> Control Panel -> Personalization**

Enable Screen saver	Enabled
Password protect the screen saver	Enabled
Screen saver timeout	1800 second

### 4.7.10

#### Activate password policy settings

- Enabling password policy settings ensures users passwords meet minimum password requirements

**Local Computer Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy**

Enforce password history	10 passwords remembered
Maximum Password Age	90 days
Minimum Password Age	1 day
Minimum Password Length	10 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

### 4.7.11

#### Disable non-essential Windows Services

- Disabling non-essential Windows Services enables a higher security level and minimizes points of attacks.

Application Layer Gateway Service	Disabled
Application Management	Disabled
Computer Browser	Disabled
Distributed Link Tracking Client	Disabled
Function Discovery Provider Host	Disabled
Function Discovery Resource Publication	Disabled
Human Interface Device Access	Disabled
Internet Connection Sharing (ICS)	Disabled
Link-Layer Topology Discovery Mapper	Disabled
Multimedia Class Scheduler	Disabled
Offline Files	Disabled

Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
Routing and Remote Access	Disabled
Shell Hardware Detection	Disabled
Special Administration Console Helper	Disabled
SSDP Discovery	Disabled

### 4.7.12 Windows Operating System user accounts

The Windows Operating System user accounts have to be protected with complex passwords. Servers are normally managed and maintained with Windows administrator accounts, ensure that strong passwords are used for the administrator accounts.

Passwords must contain characters from three of the following categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: ~!@#\$%^&\* \_+=` \()\{\}[]:;'"<>.,?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

Use of Windows Account Lockout to make it harder for password-guessing attacks to succeed. Windows 8.1 Security Baselines recommendation is 10/15/15:

- 10 bad attempts
- 15 minute lockout duration
- Counter reset after 15 minutes

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy**

Account lockout duration	Account lockout duration
15 minutes Account lockout threshold 10 failed logon attempts	15 minutes Account lockout threshold 10 failed logon attempts
Reset account lockout counter after	Reset account lockout counter after

- Ensure that all default password of the server and the Windows Operating system are replaced with new strong passwords.
- Disable unused Windows Operating system accounts.
- Disable Remote Desktop Access to the client workstation.
- Run workstation with non-administrative rights to avoid that standard user are changing system settings.

### 4.7.13 Enable firewall on the workstation

- ▶ Enable communication of BVMS standard port according to BVMS ports.

**Notice!**

Refer to the BVMS documentation for relevant port settings and usage. Be sure to re-check settings on upgrades of firmware or software.

## 4.8 Protecting network access

Currently many small to medium sized IP video surveillance systems are deployed on the customer's existing network infrastructure as just "another IT application". While this has its benefits in terms of cost and maintenance, this type of deployment also exposes the security system to unwanted threats, including internal ones. Appropriate measures need to be applied and to avoid situations like event video being leaked onto the Internet or social media. Events such as these may not just violate privacy, but possibly harm the company.

There are two major technologies to create a network-in-a-network. Which one will be chosen by the IT infrastructure architects is highly dependent on the existing network infrastructure, the network equipment deployed, and the demanded capabilities and the topology of the network.

### 4.8.1 VLAN: Virtual LAN

A Virtual LAN is created by subdividing a LAN into multiple segments. The network segmentation is done through network switch or router configuration. A VLAN has the advantage that resource needs can be addressed without rewiring of device network connections.

Quality of service schemes, applied to specific segments like for video surveillance, might help to not only improve security but performance as well.

VLANs are implemented on data link layer (OSI layer 2) and provide analogy to IP subnetting (see *Assigning IP addresses, page 8*) which is similar on network layer (OSI layer 3).

### 4.8.2 VPN: Virtual Private Network

A Virtual Private Network is a separated (private) network that often extends across public networks or the Internet. Various protocols are available to create a VPN, typically a tunnel that carries the protected traffic. Virtual private networks might be designed as point-to-point tunnels, any-to-any connections, or multi-point connections. VPNs can be deployed with encrypted communications, or merely rely on secure communication within the VPN itself.

VPNs can be used to connect remote sites via wide area network (WAN) connections, while also protecting privacy and increasing security within a local area network (LAN). Because a VPN acts as a separate network, all devices added to the VPN will work seamlessly as if they were on a typical network. A VPN not only adds an additional layer of protection for a surveillance system, but it also provides the additional benefit of segmenting the production networks business traffic and video traffic.

**Notice!**

If applicable, VLAN or VPN increase the security level of the surveillance system combined into existing IT infrastructure.

Besides protecting the surveillance system from unauthorized access on shared IT infrastructure, a look needs to be given to who is allowed to connect to the network at all.

### 4.8.3 Disable unused switch ports

Disabling unused network ports ensures that unauthorized devices do not get access to the network. This mitigates the risk of someone trying to access a security subnet by plugging his device into a switch or unused network socket. The option to disable specific ports is a common option in managed switches, both low cost and enterprise.

### 4.8.4 802.1x protected networks

All Bosch IP video devices can be configured as 802.1x clients. This allows them to authenticate to a RADIUS Server and participate on a secured network. Prior to placing the video devices on to the secured network, you will need to connect directly to the video device from a technician's laptop to enter valid credentials as detailed in the steps below.

802.1x services can be easily configured via Configuration Manager.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **Advanced**.



3. Locate the **802.1x** portion of the page.
4. In the **802.1x** dropdown menu select **On**.
5. Enter a valid **Identity** and **Password**.
6. Save changes.
7. Disconnect and place the devices onto the secured network.



#### Notice!

802.1x itself does not provide a secure communication between the supplicant and authentication server.

As a result the user-name and password could be "sniffed" from the network. 802.1x can use EAP-TLS to ensure secure communication.

#### Extensible Authentication Protocol - Transport Layer Security

The Extensible Authentication Protocol (EAP), provides support for multiple authentication methods. Transport Layer Security (TLS) provides for mutual authentication, integrity-protected cipher suite negotiation, and key exchange between two endpoints. EAP-TLS includes support for certificate-based mutual authentication and key derivation. In other words, EAP-TLS encapsulates the process in which both the server and client send each other a certificate.



#### Notice!

Refer to the specific Technical White Paper *Network Authentication - 802.1x - Secure the Edge of the Network*, available on the Bosch Security Systems online product catalog under: [http://resource.boschsecurity.com/documents/WP\\_802.1x\\_Special\\_enUS\\_22335867275.pdf](http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf).

## 5 Secure operation

### 5.1 Network separation

If possible, the device should be operated in a separate network (for example using VLANs) with access restrictions to limit broadcast traffic and protect the device from network attacks.

### 5.2 Safe key storage in hardware vault

Private keys from certificates are best protected when safely stored in a hardware component, or hardware vault. Such chips provide protection against unauthorized access to private keys even when the device is physically open to gain access.

In Bosch cameras, such keys are stored in a separate crypto-coprocessor or secure element (SE). Both provide secure storage as well as cryptographic functions that never expose private keys to locations or memory where it could potentially be retrieved.

On workstations and servers, typically a Trusted Platform Module (TPM) chip is available. Cryptographic libraries and functions should be configured to use the TPM storage where possible.

### 5.3 Unique device certificates

Though a self-signed default certificate is typically available with every device that is capable of TLS or HTTPS, this certificate should not be considered sufficient solely for authentication, as it does not protect from a man-in-the-middle (MITM) attack.

If devices are deployed in an environment where extra steps are required to validate the identity of each individual IP video device, new certificates and private keys can be created and loaded to the video devices themselves. New certificates can be obtained from a certificate authority (CA), or they can be created with an OpenSSL Toolkit.

If devices are used in public networks, it is recommended to obtain certificates from a public certificate authority, or have own certificates signed by such an authority, which is also capable of verifying the origin and validity - in other words the trustfulness - of the device certificate.

Since years, all Bosch cameras come with a preinstalled unique device certificate and a private key, derived from the Bosch Root Certificate and installed in a secure production environment, proving the camera being an "originally manufactured" Bosch device. This certificate is used for HTTPS connections automatically and can be used to identify and authenticate a device by verifying the certificate chain up to the Bosch Root Certificate.



#### **Notice!**

Certificates should be used to authenticate a single device. It is recommended to create a specific certificate per device, derived from a root certificate.

The most secure variant of a certificate deployment is to generate a certificate signing request (CSR) on the device and to request a certificate from an internal or external certification authority.

With a certificate signing request, the device holds the private key internal and only exposes the rest of the certificate to be signed by the certificate authority. The private key is securely stored in the Secure Element (SE) of the camera, or for example on the Trusted Platform Module (TPM) of the device.

Therefore, whenever a device provides a CSR possibility, this should be the preferred way to create a certificate.

Certificates can be uploaded to a device by either using the device web page of a video device or by using Configuration Manager.

#### **Uploading certificates by using the device web page**

Certificates can be uploaded using the device web page of a video device.

On the device web page, on the **Certificates** page, new certificates can be added and deleted, and their usage can be defined.

#### **Uploading certificates by using Configuration Manager**

In Configuration Manager, certificates can be easily uploaded to individual or multiple devices simultaneously.

To upload certificates:

1. In Configuration Manager, select one or more devices.
2. Right-click and click **File Upload**, then click **SSL Certificate....**

A Windows Explorer window opens to locate the certificate for upload.

For smaller systems, Configuration Manager provides a supportive function called **MicroCA**, which allows to create or use a Root CA and derive device certificates from this, or use it for signing the devices' certificate signing requests, also for multiple devices simultaneously. For more details, refer to the Configuration Manager User manual.

#### **Refer to**

- *Creating trust with certificates, page 45*

## **5.4 Checking log files**

Monitoring the log files is an important part of security analysis or maintenance activity. Regular review of the log files can reveal configuration problems or security violations like false logins.

To analyze log files and store them for long term it is advised to send the log files of the device to a syslog server or a SIEM system as for example a camera will reserve a fixed space for logging internally but will overwrite older logs if that space is filled.

## **5.5 SIEM system**

Security Information and Event Management (SIEM) system is used to collect and analyze information from different devices and systems. The devices can be integrated with a SIEM system by sending the logs via syslog protocol. Analyzing these logs can help to do the maintenance and to detect configuration errors or attacks on the device (for example false logins).

## **5.6 PKI**

Public Key Infrastructure (PKI) refers to the systems needed to generate and manage digital certificates. For HTTPS, network authentication with 802.1x, user authentication with certificates and other encryption functions, custom certificates can be installed on the device.

## 5.7 AD FS

Active Directory Federation Services (AD FS) is a service offered by Microsoft, allowing authentication to a local Active Directory (using an AD FS server) or to the Azure Cloud. Besides local user authentication with either passwords or certificate-based authentication, integration of devices into an Active Directory Domain is possible with AD FS to authenticate and manage user access centrally.

## 5.8 Secure operation of IP cameras

### 5.8.1 Creating trust with certificates

All Bosch IP cameras running FW 6.10 or newer use a certificate store, which can be found under the **Service** menu of the camera configuration.

Specific server certificates, client certificates and trusted certificates can be added to the store.

To add a certificate to the store:

1. On the device web page, navigate to the **Configuration** page.
2. Select the **Service** menu and the **Certificates** submenu.
3. In the **File list** section, click **Add**.
4. Upload the desired certificates.

After the upload is completed, the certificates appear in the **Usage list** section.

5. In the **Usage list** section, select the desired certificate.
6. To activate the usage of the certificates the camera must be rebooted. To reboot the camera, click **Set**.

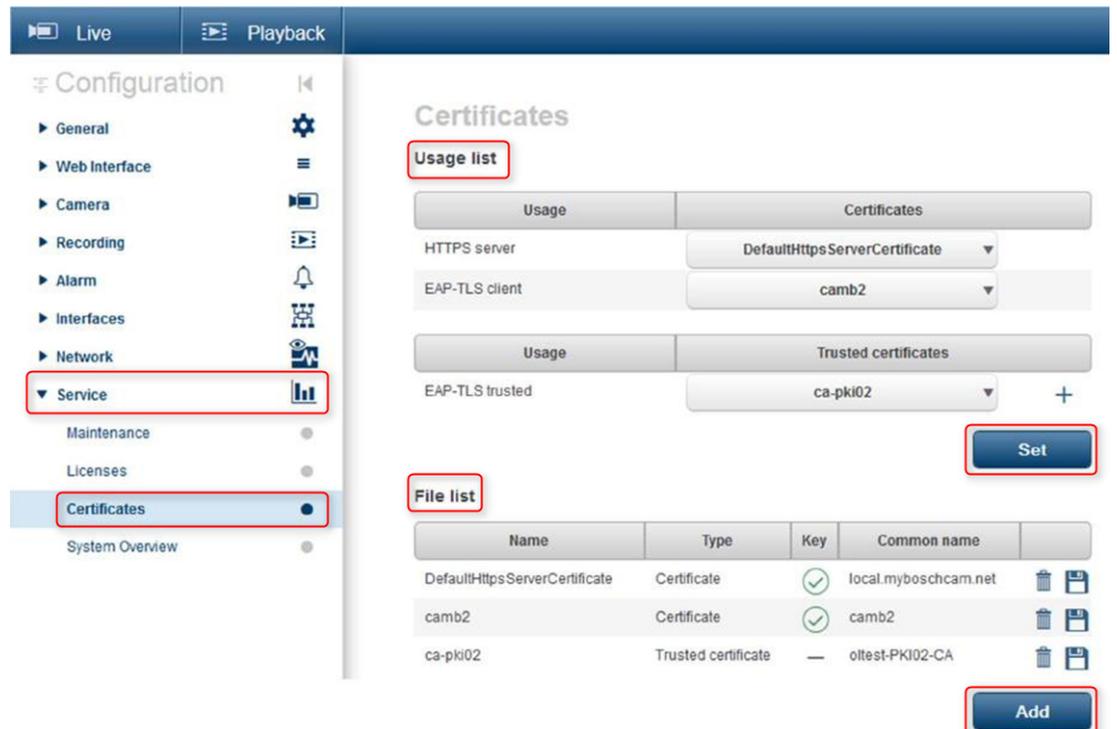


Figure 5.1: Example: EAP/TLS certificates stored in a Bosch camera (FW6.11)

Certificates are accepted in \*.pem, \*.cer or \*.crt format and must be base64-coded. They may be uploaded as one combined file, or split into certificate and key parts and uploaded in this order as separate files to be automatically re-combined.

Since firmware version 6.20, password-protected PKCS#8 private keys (AES-encrypted) are supported which must be uploaded in base64-coded \*.pem format.

### 5.8.2 Video Authentication

Once the devices in a system are protected and authenticated correctly it is worth keeping an eye also on the video data delivered from them. The method 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. Prior to the release of firmware 5.9 watermarking was performed via a simple checksum algorithm over the video stream. When dealing with basic watermarking there is no use of certificates or encryption. A checksum is a baseline measurement of a file's "Data Fixity" and validates a file's integrity.

To configure video authentication, for example in the web browser:

1. Navigate to the **General** menu and then select **Display stamping**.
2. In the **Video authentication** drop-down menu, select the desired option:  
Firmware versions 5.9 and later provide three options in video authentication besides classic watermarking:
  - MD5: Message-digest that produces a 128- bit hash value.
  - SHA-1: Designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit hash value.
  - SHA-256: SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash.

#### Display Stamping

Camera name stamping

Logo

Logo position

Time stamping

Display milliseconds

Alarm mode stamping

Alarm message  (max. 31 characters)

Transparent background

Video authentication

- Off
- Watermarking
- MD5
- SHA-1
- SHA-256

**Notice!**

Hash is a one way function - it cannot be decrypted back.

---

When utilizing video authentication, every packet of a video stream is hashed. These hashes are embedded in the video stream and hashed themselves together with the video data. This ensures integrity of the stream content.

The hashes are signed in regular periods, defined by the signature interval, using the private key of the stored certificate within the TPM of the device. Alarm recordings and block changes in iSCSI recordings are all closed with a signature to ensure continuous video authenticity.

**Notice!**

Calculating the digital signature requires computational power which might influence the overall performance of a camera if done too often. Therefore a reasonable interval should be chosen.

---

Since the hashes and digital signatures are embedded in the video stream they will be also stored in the recording, allowing video authentication also for playback and exports.

## 6 Security update management

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. For consistent functionality, compatibility, performance, and security, regularly update the software throughout the operational life of the device. Follow the instructions in the product documentation regarding software updates.

The following links provide more information:

- General information: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Security advisories, that is a list of identified vulnerabilities and proposed solutions: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch assumes no liability whatsoever for any damage caused by operating its products with outdated software components.

You can find the latest firmware and software versions in the Bosch Security and Safety Systems download store:

<https://downloadstore.boschsecurity.com/>

For devices connected to Remote Portal, users can receive an email notification about available firmware updates through the Remote Alert service.

More comprehensive download packages are distributed through the Bosch Security and Safety Systems product catalog:

<https://www.boschsecurity.com>

## 7 Security monitoring

Because requirements are constantly changing, 100% security is never guaranteed. Therefore, a structured vulnerability and incident management process is established at Bosch to professionally manage potential product security vulnerabilities and incidents.

The professional systematic handling of reported security vulnerabilities as well as transparency towards our customer is very important for us. That is why we investigate all vulnerability reports. We perform an evaluation of product security vulnerabilities according to the Common Vulnerability Scoring System (CVSS). CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe.

In case of confirmed vulnerability, we inform customers about an identified security vulnerability in product or solution and its remediation by publishing of security advisory. All security advisories contain:

- Description of the vulnerability with Common Vulnerabilities and Exposures (CVE) reference and CVSS score.
- Identity of known affected products and software/hardware versions.
- Information on mitigating factors and workarounds.
- Timeline and the location of available fixes or other remedial measures.

You can find the list of published Security Advisories on our website <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>.

Whenever you think you have identified a vulnerability or any other security issue related to a Bosch product or service, contact the Bosch Product Security Incident Response Team (PSIRT): <https://psirt.bosch.com>.

## 8 Secure disposal and decommissioning

At a certain point in the life cycle of a product or a system, it might be necessary to replace or to take out of order a device or a component. As the device or the component may hold sensitive data, like credentials or certificates, make sure to delete these data completely and securely.

You can set the most devices to factory default.

For the most IP cameras and encoders, you can use for this the reset button. For the ones that do not have a reset button, use the factory default function via the web interface before dismantling them from the network.

All users and their respective passwords will be deleted and the settings will be set back to the factory default settings. All certificates and the respective keys that were stored in the TPM or secure element will also be deleted.

Other devices may have different options to set them to factory default. Refer to the instructions in the respective user documentation for correct disposal procedures.

Servers and workstations may also have certificates and credentials stored. Use the proper tools and methods to make sure that your relevant data is securely deleted during decommissioning or before disposal.

It is recommended to set devices to factory default also in case that they must be moved into another installation that may use other credentials or certificates.

**Notice!**

Refer to the instructions in the respective user documentation for correct disposal procedures.

---

## 9 Additional information

For more information, software downloads, and documentation, go to the respective product page in the product catalog:

<http://www.boschsecurity.com>

# Glossary

## 802.1x

The IEEE 802.1x standard provides a general method for authentication and authorization in IEEE-802 networks. Authentication is carried out via the authenticator, which checks the transmitted authentication information using an authentication server (see RADIUS server) and approves or denies access to the offered services (LAN, VLAN or WLAN) accordingly.

## authentication

Process of verifying the authenticity of a video stream. The user can start an authentication process. If non-authentic data is encountered, a message is displayed.

## device

Hardware component such as camera, encoder/decoder, NVR, DiBos, analog matrix, ATM/POS bridge.

## DHCP

Dynamic Host Configuration Protocol: uses an appropriate server to enable dynamic assignment of an IP address and other configuration parameters to computers on a network (Internet or LAN)

## hardening

Process of increasing the security of a system by only using dedicated software that is necessary for systems operation, applying specific protective settings, and the removing of software that is not mandatory.

## HTTP

Hypertext Transfer Protocol: protocol for transmitting data over a network

## HTTPS

Hypertext Transfer Protocol Secure: encrypts and authenticates communication between Web server and browser

## IPv4 address

A 4-byte number uniquely defining each unit on the Internet. It is usually written in dotted decimal notation, for example "209.130.2.193"

## LAN

Local Area Network. This is a network that connects devices within a confined geographical area.

## Multicast

Communication between a single transceiver and multiple receivers on a network by distribution of a single data stream on the network to a number of receivers in a defined group. Requirement for multicast operation is a multicast compliant network with implementation of the UDP protocol and the IGMP protocol.

## Net mask

A mask that explains which part of an IP address is the network address and which part is the host address. It is usually written in dotted decimal notation, for example "255.255.255.192."

## ONVIF

Open Network Video Interface Forum. Global standard for network video products. ONVIF conformant devices are able to exchange live video, audio, metadata, and control information and ensure that they are automatically discovered and connected to network applications such as video management systems.

## RADIUS server

Remote Authentication Dial-In User Service: a client/server protocol for the authentication, authorization and accounting of users with dial-up connections on a computer network. RADIUS is the de-facto standard for central authentication of dial-up connections via Modem, ISDN, VPN, Wireless LAN (see 802.1x) and DSL.

## RCP+

Remote Control Protocol: a proprietary Bosch protocol which uses specific static ports to detect and communicate with Bosch IP video devices

## RTSP

Real Time Streaming Protocol. A network protocol which allows to control the continuous transmission of audio-visual data or software over IP-based networks.

---

**SNMP**

Simple Network Management Protocol; a protocol for network management, for managing and monitoring network components

---

**SSL**

Secure Sockets Layer; an outdated encryption protocol for data transmission in IP-based networks (see TLS).

---

**TCP**

Transmission Control Protocol. Connection-oriented communication protocol used to transmit data over an IP network. Offers a reliable and ordered data transmission.

---

**Telnet**

Login protocol with which users can access a remote computer (Host) on the Internet

---

**TLS**

Transport Layer Security. TLS 1.0 and 1.1 are the standard advanced developments of SSL 3.0 (see SSL). Modern devices use TLS 1.2 or 1.3

---

**TTL**

Time-To-Live; life cycle of a data packet in station transfers

---

**UDP**

User Datagram Protocol. A connectionless protocol used to exchange data over an IP network. UDP is more efficient than TCP for video transmission because of lower overhead.

---

**User group**

User groups are used to define common user attributes, such as permissions, privileges and PTZ priority. By becoming a member of a group, a user automatically inherits all the attributes of the group.

---

**VPN**

A virtual private network (VPN) implements a private network within a public network, such as the Internet. Network traffic within the VPN is encrypted and so protected from espionage.

---

**Wide Area Network**

A long distance link used to extend or connect remotely located local area networks





**Bosch Sicherheitssysteme GmbH**

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Sicherheitssysteme GmbH, 2022

**Building solutions for a better life.**

202212092154