Bosch IP video and data security guidebook

en

Table of contents

1	**Introduction**	**5**
2	**Bosch IP video devices**	**6**
3	**Assigning IP addresses**	**7**
3.1	Managing DHCP	**9**
4	**User accounts and passwords**	**10**
4.1	Applying passwords	**10**
4.2	Device web page	**11**
4.3	Configuration Manager	**13**
4.4	DIVAR IP 2000 / DIVAR IP 5000	**13**
4.5	VRM stand-alone installation	**14**
4.6	Bosch Video Management System	**15**
4.6.1	Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: device password protection	**15**
4.6.2	Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: default password protection	**15**
4.6.3	Bosch VMS configuration and VRM settings	**16**
4.6.4	Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: encrypted communication to cameras	**17**
5	**Hardening device access**	**19**
5.1	General network port usage and video transmission	**19**
5.1.1	HTTP, HTTPS and video port usage	**20**
5.1.2	Video software and port selection	**20**
5.1.3	Telnet Access	**21**
5.1.4	RTSP: Real Time Streaming Protocol	**21**
5.1.5	UPnP: Universal Plug and Play	**22**
5.1.6	Multicasting	**22**
5.1.7	IPv4 filtering	**23**
5.1.8	SNMP	**24**
5.2	Secure time basis	**25**
5.3	Cloud-based Services	**26**
6	**Hardening Storage**	**28**
7	**Hardening Servers**	**29**
7.1	Windows Servers	**29**
7.1.1	Server Hardware recommended settings	**29**
7.1.2	Windows Operating System recommended security settings	**29**
7.1.3	Windows updates	**29**
7.1.4	Installation of anti-virus software	**29**
7.1.5	Windows Operating System recommended settings	**29**
7.1.6	Activate User Account Control on the server	**30**
7.1.7	Deactivate AutoPlay	**30**
7.1.8	External Devices	**30**
7.1.9	Configuration of user rights assignment	**31**
7.1.10	Screen saver	**32**
7.1.11	Activate password policy settings	**32**
7.1.12	Disable non-essential Windows Services	**32**
7.1.13	Windows Operating System user accounts	**33**
7.1.14	Enable firewall on the server	**34**
8	**Hardening Clients**	**35**
8.1	Windows Workstations	**35**
8.1.1	Windows Workstation hardware recommended settings	**35**
8.1.2	Windows Operating System recommended security settings	**35**

8.1.3	Windows Operating System recommended settings	**35**
8.1.4	Activate User Account Control on the server	**35**
8.1.5	Deactivate AutoPlay	**36**
8.1.6	External Devices	**36**
8.1.7	Configuration of user rights assignment	**37**
8.1.8	Screen saver	**38**
8.1.9	Activate password policy settings	**38**
8.1.10	Disable non-essential Windows Services	**38**
8.1.11	Windows Operating System user accounts	**39**
8.1.12	Enable firewall on the workstation	**39**
9	**Protecting network access**	**41**
9.1	VLAN: Virtual LAN	**41**
9.2	VPN: Virtual Private Network	**41**
9.3	Disable unused switch ports	**42**
9.4	802.1x protected networks	**42**
9.4.1	Extensible Authentication Protocol - Transport Layer Security	**42**
10	**Creating trust with certificates**	**43**
10.1	Secured in a safe (Trusted Platform Module)	**43**
10.2	TLS certificates	**44**
10.2.1	Device web page	**44**
10.2.2	Configuration Manager	**44**
11	**Video Authentication**	**46**
12	**Decomissioning and disposal**	**48**

1 Introduction

While every organization in today's environment may have cyber security procedures and policies in place, standards may vary from organization to organization based on many factors such as size, region, and industry.
In February 2014, The National Institute of Standards and Technology (NIST) introduced the Cyber Security Framework. This framework is based on Executive Order 13636 and was created utilizing existing standards, guidelines, and best practices. It is specifically designed to reduce cyber risks to critical infrastructures and their network attached devices and data. This framework is designed to help organizations understand both external and internal cyber security risks and is applicable to any size organization categorized from Tier 1 (Partial) to Tier 4 (Adaptive).

This educational paper is written to 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 Bosch Configuration Manager to perform the configurations discussed. In most cases all configurations can be performed utilizing Bosch Video Management System Configuration Client, Bosch Configuration Manager, and the built in web interface of a video device.

2 Bosch IP video devices

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 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:

- IP Helper
- Bosch Configuration Manager
- Bosch Video Management System Configuration Client
- Bosch Video Management System 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!
Data security hint no. 1
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, or **IP A**ddress **M**anagement, 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**0**
.252	4	/30	2	.111111**00**
.248	8	/29	3	.11111**000**
.240	16	/28	4	.1111**0000**
.224	32	/27	5	.111**00000**
.192	64	/26	6	.11**000000**
.128	128	/25	7	.1**0000000**

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:

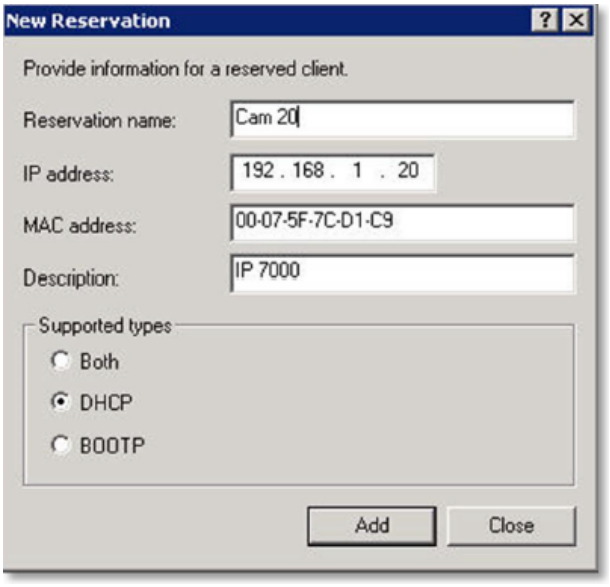
	Default	**Subnetted**
IP address range	172.16.0.0 – 172.16.255.255	172.16.8.0 – 172.16.9.255
Subnet mask	255.255.0.0	255.255.254.0
CIDR notation	172.16.0.0/16	172.16.8.0/23

Number of subnets	1	128
Number of hosts	65.534	510
Excess addresses	65.192	168

3.1 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!

Data security hint no. 2

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 User accounts and passwords

All Bosch IP video devices 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.

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 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 *Device web page, page 11*).

4.1 Applying 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!
Data security hint no. 3
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 polices in place, the following are some best practices when implementing password protection:
- Passwords should be between 8 and 12 charters 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.

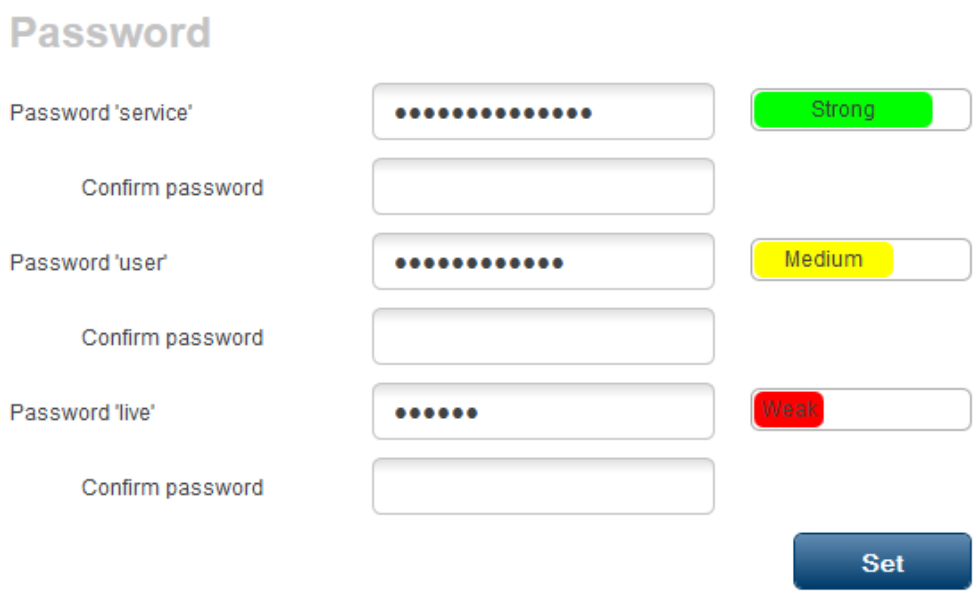
4.2 Device web page

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.



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.

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.

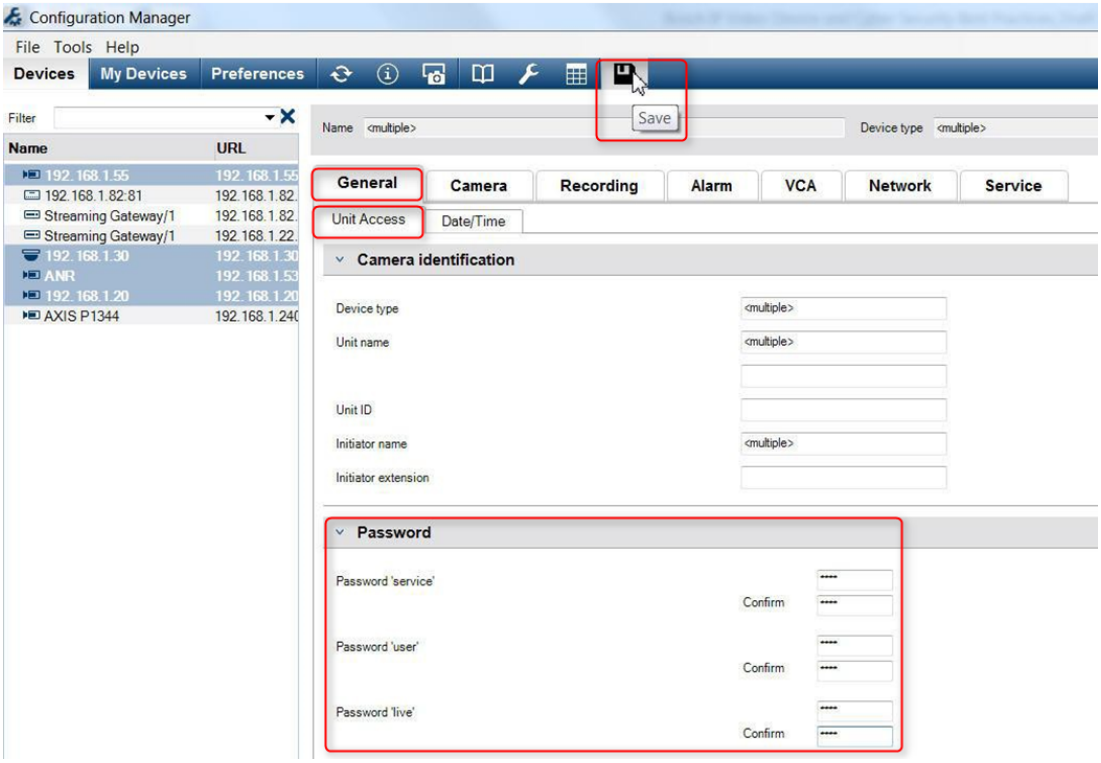
1. To add a new user, click **Add**.
   A pop-up window appears.
2. Enter the new credentials and assign the user group.
3. Click **Set** to save changes.

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

4.3 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.



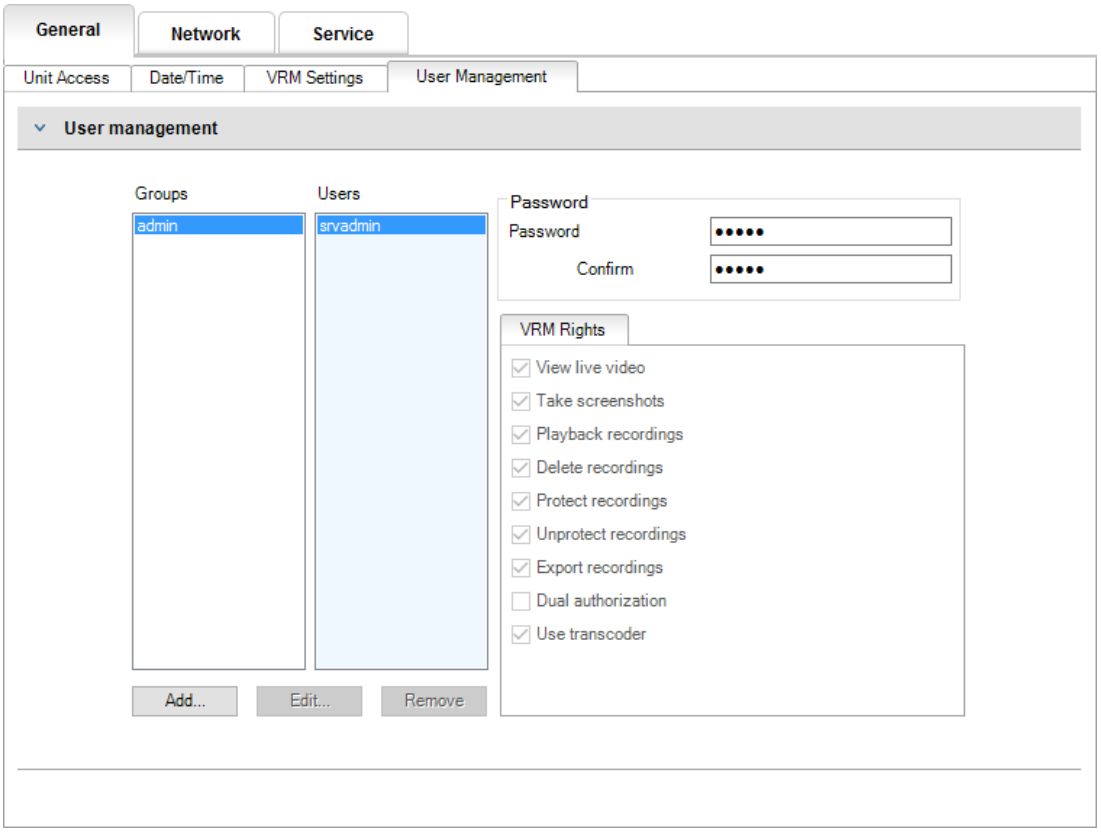
In larger installations that are managed by either Bosch Video Management System, or Video Recording Manager installed on a recording appliance, global passwords can be applied to all IP video devices that are added to the system. This allows easy management and ensures a standard level of security across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

4.4 DIVAR IP 2000 / DIVAR IP 5000

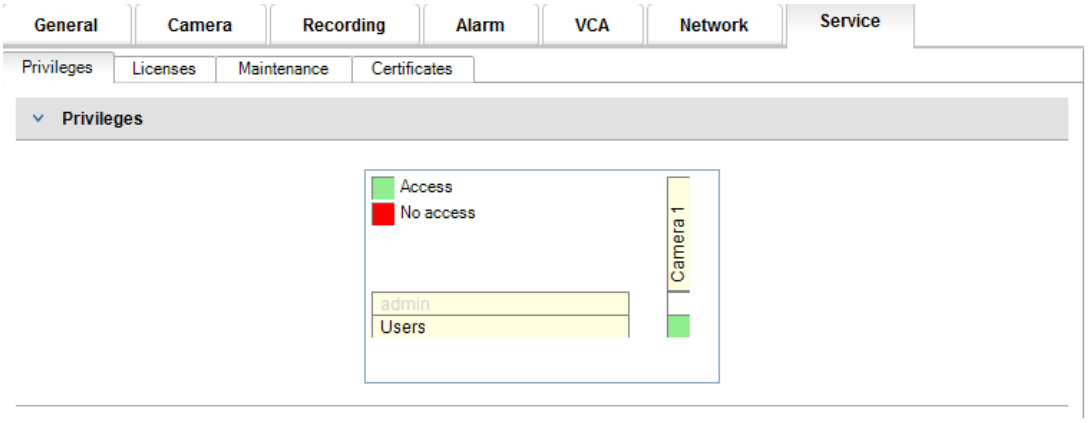
The DIVAR IP recording appliances are equipped with an easy to use Configuration Wizard. The assignment of a system-wide administrator password is mandatory when configuring the system. This password is assigned to the service account of all IP video cameras added to the system. The ability to add an user account password is also provided by the Configuration Wizard, but implementation is not mandatory. The password strength indicator is using a similar algorithm as when using the camera web pages.

4.5 VRM stand-alone installation

The Bosch 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.



4.6 Bosch Video Management System

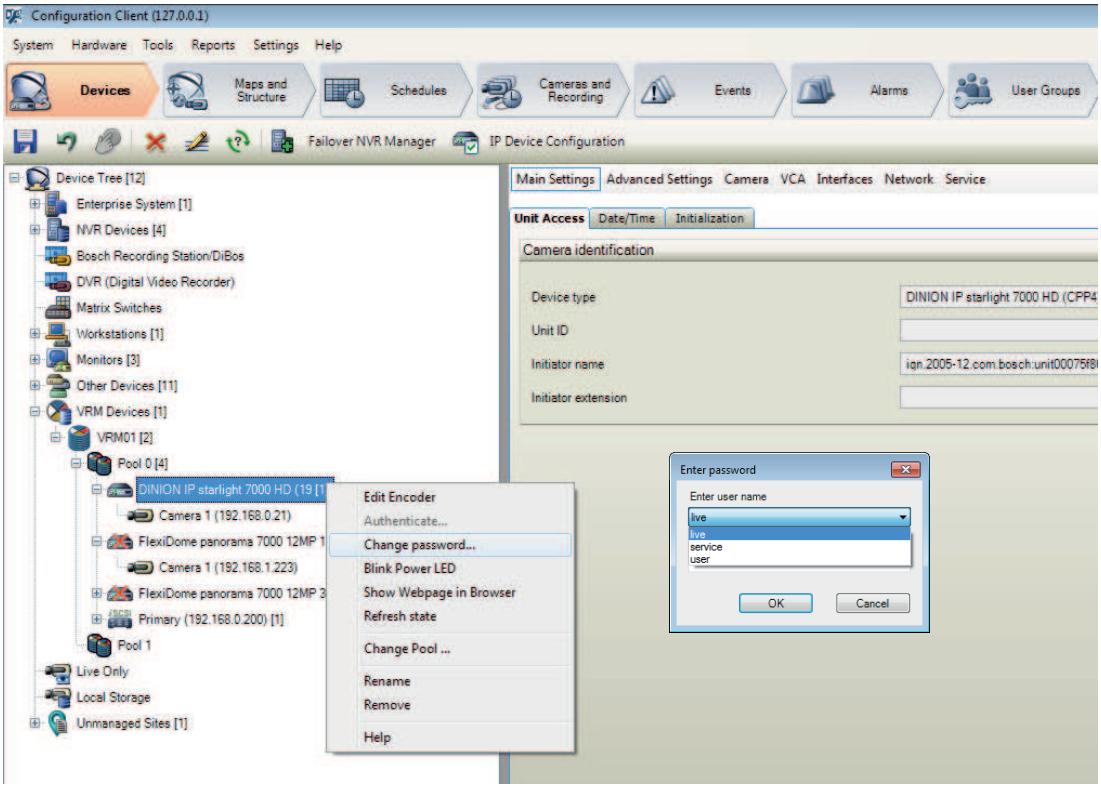
4.6.1 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: device password protection

Cameras and encoders, managed by a Bosch Video Management System 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 Bosch Video Management System Configuration Client.

To set a password for the built-in user accounts in the Bosch Video Management System 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.

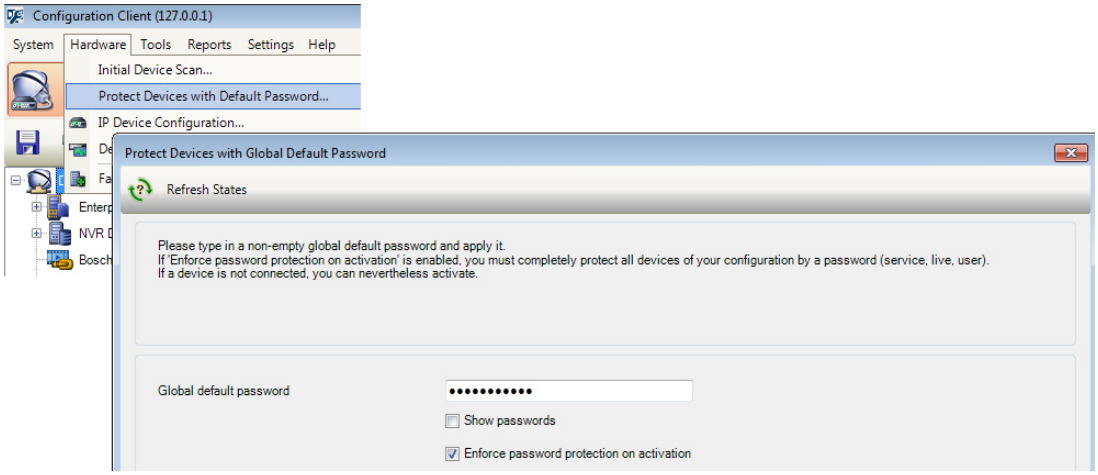


4.6.2 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: default password protection

Bosch Video Management System 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 Bosch Video Management System Configuration Wizard when working with DIVAR IP 3000 or DIVAR IP 7000 recording appliances, or through Bosch Video Management System Configuration Client on any system.

To access the global passwords menu in Bosch Video Management System 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.

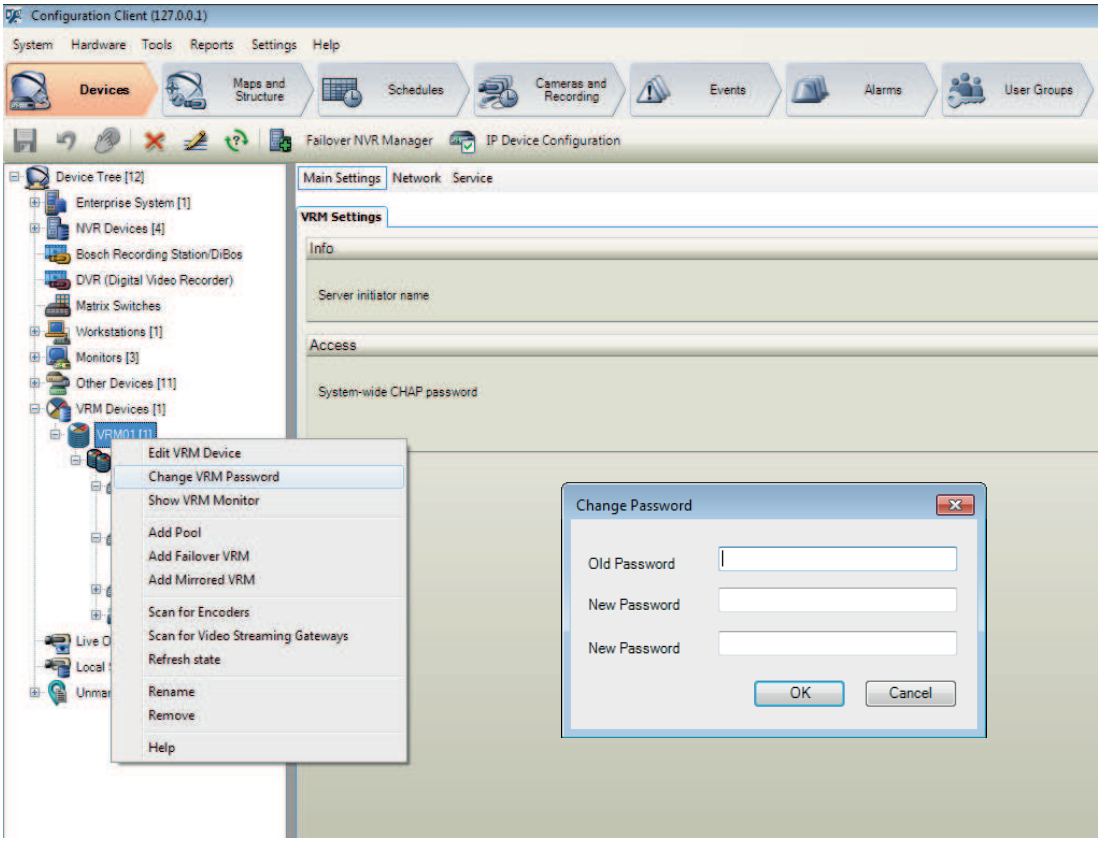
For example, if password is set for service but not for live and user, global password will only be configured for live and user accounts.

4.6.3 Bosch VMS configuration and VRM settings

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

To change the password of the **srvadmin** account in Bosch Video Management System 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**.



4.6.4 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: encrypted communication to cameras

Since Bosch Video Management System version 7.0, live video data and control communication between the camera and the Bosch Video Management System 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 Bosch Video Management System Server, Operator Client and Video Recording Manager will use a secure HTTPS connection in order to connect to a camera or encoder.

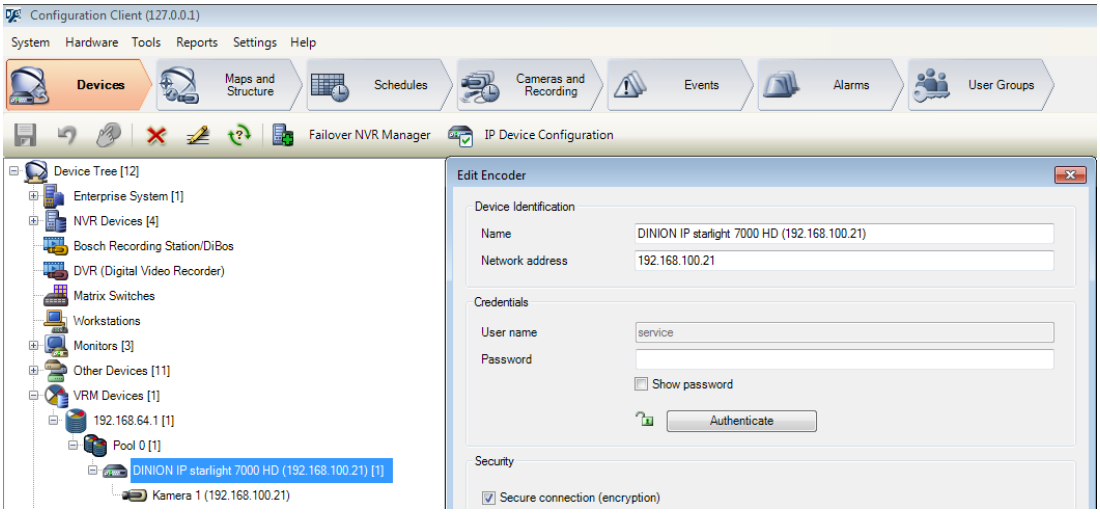
The Bosch Video Management System internally used connection string will change from rcpp://a.b.c.d (plain RCP+ connection on port 1756) to https://a.b.c.d (HTTPS connection on port 443) instead.

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 Bosch Video Management System 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 (encryption).**
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 19*).

Notice!
Bosch VMS only supports the default HTTPS port 443. Usage of different ports is not supported.

5 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.

5.1 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 Bosch Video Management System, 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 20*). 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.

Notice!

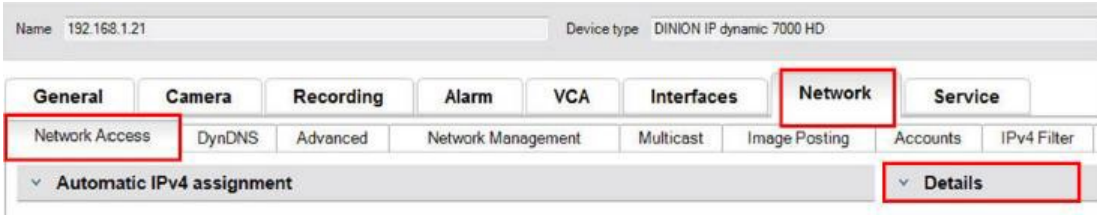
Data security hint no. 4

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.

5.1.1 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 devices IP address plus the assigned port.

Example:

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

5.1.2 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 Bosch Video Management System 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!

Data security hint no. 5

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.

5.1.3 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!

Data security hint no. 6

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!

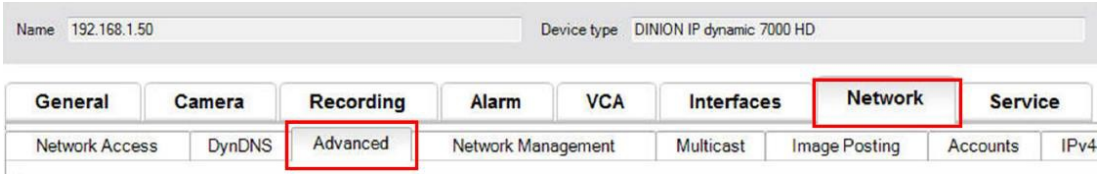
Data security hint no. 7

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.

5.1.4 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!
Data security hint no. 8
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.

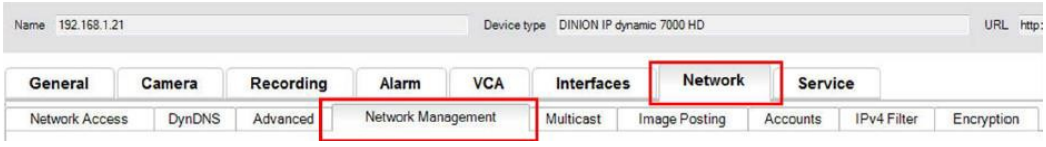
Notice!
For more details on RTSP see the Technical service note "RTSP usage with Bosch VIP Devices" in the Bosch Security Systems online product catalog under the following link:

http://resource.boschsecurity.com/documents/RTSP_VIP_Configuration_Note_enUS_9007200806939915.pdf

5.1.5 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!
Data security hint no. 9
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.

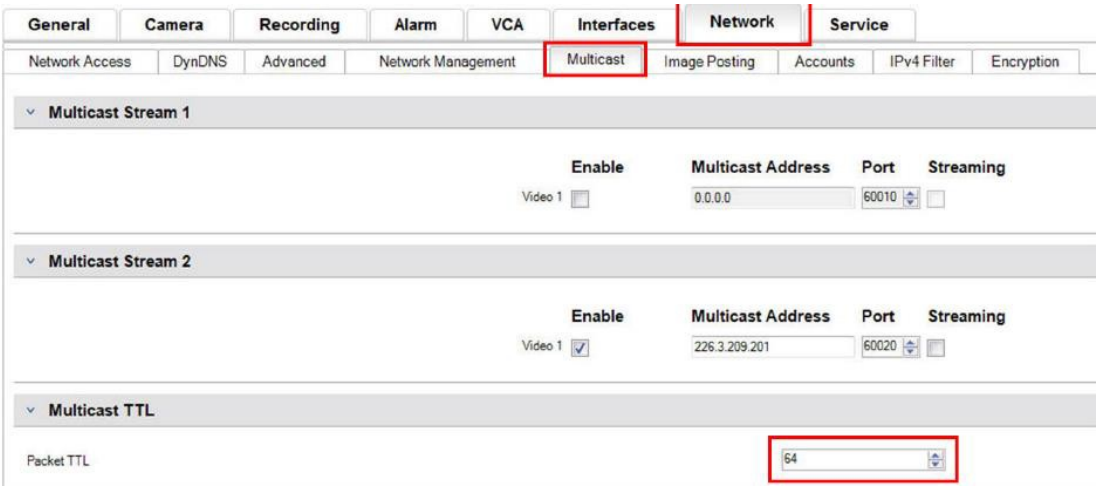
5.1.6 Multicasting

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!

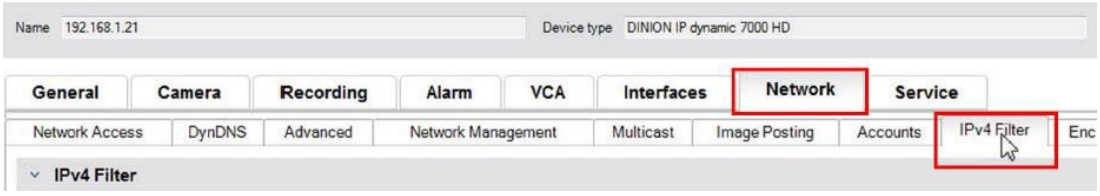
Data security hint no. 10

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.

5.1.7 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.

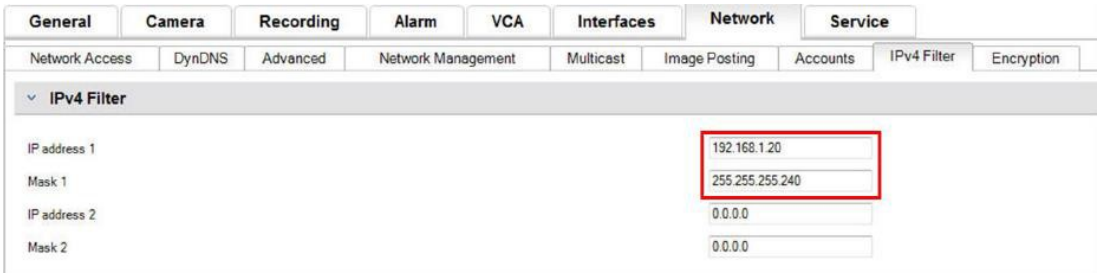
1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **IPv4 Filter**.



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.



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!
Data security hint no. 11
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 ensure 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.

5.1.8 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.

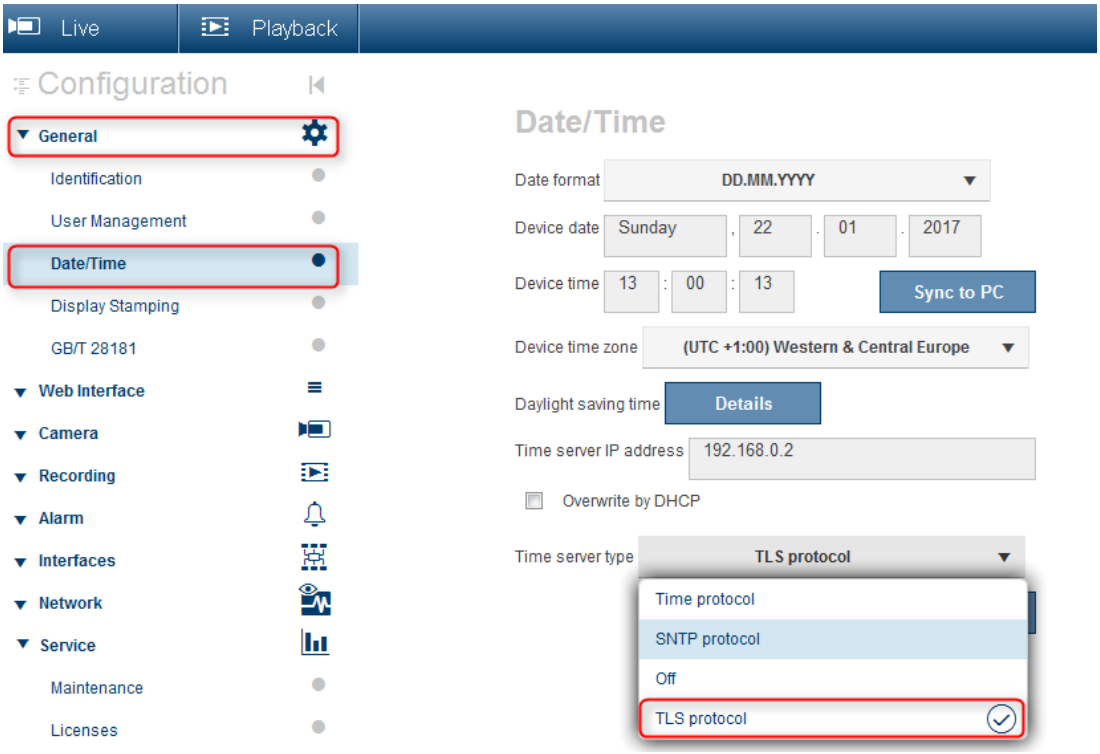
There are three different version of the SNMP protocol:

– 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!
Data security hint no. 12
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 shall only be used when it can be assured that the network is physically protected against unauthorized access.
Bosch cameras to date only support SNMPv1. Make sure to have SNMP switched off if you don’t use it.

5.2 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.



Notice!
Data security hint no. 13
Make sure that the entered time server IP address has a stable and uncompromised time base itself.

5.3 Cloud-based Services

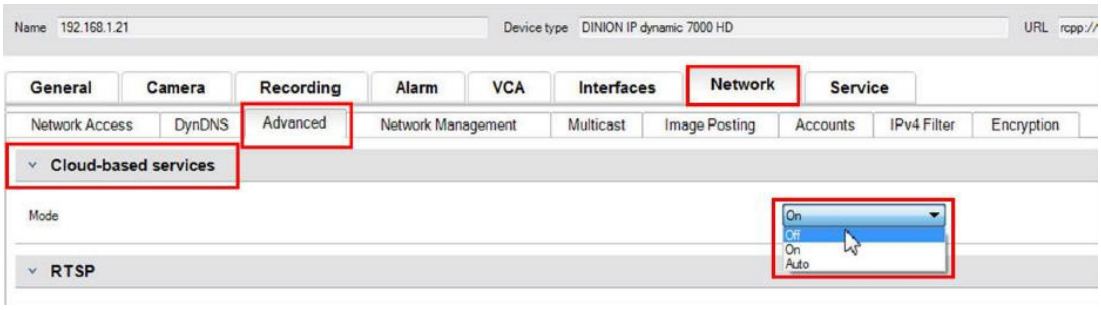
All Bosch IP video devices can communicate with Bosch **Cloud-based services**. Depending on the region of deployment, this allows IP video devices to forward alarms and other data to a central station.

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 **Advanced**.
3. Locate the **Cloud-based services** portion of the page.
4. In the drop down menu, select **Off.**



Notice!

Data security hint no. 14

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

6 Hardening Storage

The iSCSI storage units shall be installed in the secure area. The access to the secure area shall be ensured with an access control system and shall be monitored. The user group, which has access to the central server room, shall be limited to a small group of persons.
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:

- By default, iSCSI units grant all iSCSI initiators access to the iSCSI LUN's. To ensure, that only components of the Bosch Video Management solution (cameras, encoders, workstations and servers) are allowed to access the iSCSI LUN's, the default LUN mapping can be disabled.
  To allow devices the access to the iSCSI targets of a Bosch Video Management System, the iSCSI Qualified Names (IQN) of all components in the Bosch Video Management System have to be configured on all iSCSI targets. This causes efforts during the installation, but minimizes the risk of video data being lost, leaked or manipulated.
- Use password authentication via CHAP to ensure only known devices are allowed to access the iSCSI target. Setup a CHAP password on the iSCSI target and enter the configured password in the VRM configuration. The CHAP password is valid for VRM and is sent to all devices automatically. If CHAP password is used in a Bosch Video Management System VRM environment, all storage systems have to be configured to use the same password.
- 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.

7 Hardening Servers

7.1 Windows Servers

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

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.1.4 Installation of anti-virus software

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

7.1.5 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.**

7.1.6 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

7.1.7 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

7.1.8 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

7.1.9 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

7.1.10 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

7.1.11 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

7.1.12 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

7.1.13 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.

7.1.14 Enable firewall on the server

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

Notice!

Data security hint no. 15

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

8 Hardening Clients

8.1 Windows Workstations

The Windows desktop operating systems, used for Bosch VMS Client applications like the Bosch VMS 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.

8.1.1 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.

8.1.2 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 antispyware software and keep it up to date.

8.1.3 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.**

8.1.4 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

8.1.5 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

8.1.6 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

8.1.7 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

8.1.8 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

8.1.9 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

8.1.10 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

8.1.11 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

LCP -> 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.

8.1.12 Enable firewall on the workstation

- Enable communication of Bosch VMS standard port according to Bosch VMS ports.

Notice!

Data security hint no. 16

Please refer to the Bosch VMS installation and user documentation for relevant port settings and usage. Be sure to re-check settings on upgrades of firmware or software.

9 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.

9.1 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 7*) which is similar on network layer (OSI layer 3).

9.2 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!
Data security hint no. 17
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.

9.3 Disable unused switch ports

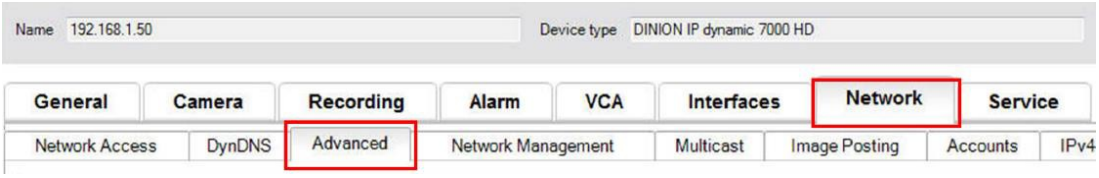
Disabling unused network ports ensures that unauthorized devices do not get access to the network. This mitigates the risk of someone trying to access a security subnet by plugging his device into a switch or unused network socket. The option to disable specific ports is a common option in managed switches,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

9.4 802.1x 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.

9.4.1 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!
Data security hint no. 18
Please 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.

10 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**.

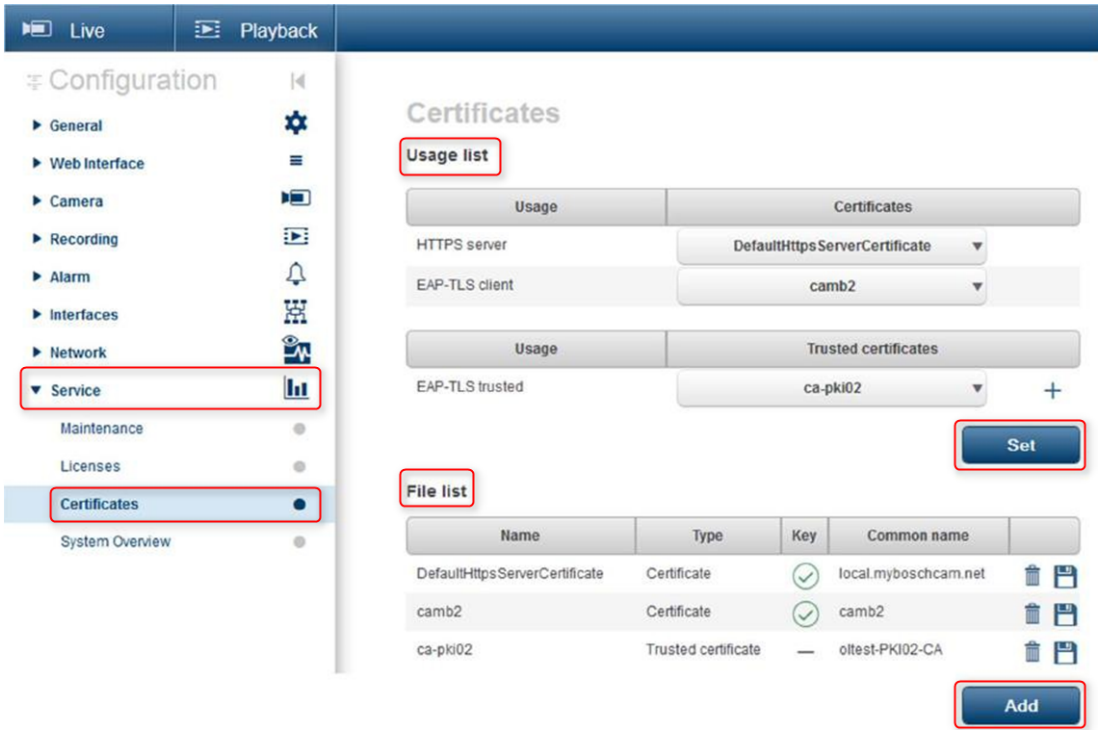


Figure 10.1: Example: EAP/TLS certificates stored in a Bosch camera (FW6.11)

10.1 Secured in a safe (Trusted Platform Module)

The keys are stored in a chip like being used on crypto SmartCards, also called a “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.

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.

10.2 TLS certificates

All Bosch video devices running firmware up to FW 6.1x come with a preinstalled TLS certificate and private key which is being used for HTTPS connections automatically. The default certificate and key is meant for testing purposes only, as all devices come with the same default certificate.

Since FW 6.20, a device-specific self-signed TLS certificate is automatically created when needed for HTTPS connections, allowing unique authentication. This self-signed certificate can be renewed manually by simply deleting it. The device will itself create a new one as soon as needed.

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 e.g. an OpenSSL Toolkit.

10.2.1 Device web page

Certificates can be uploaded using the device web page of a video device.
On the **Certificates** page new certificates can be added and deleted, and their usage can be defined.

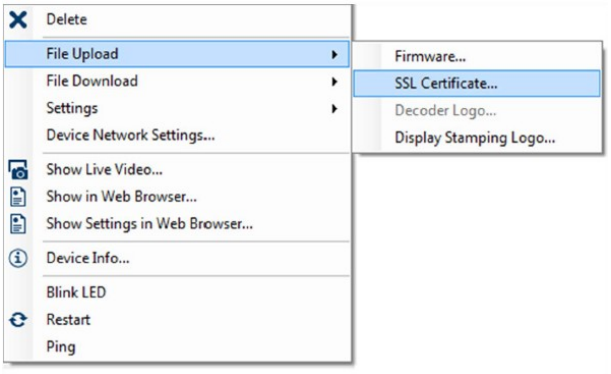
Refer to

– *Creating trust with certificates, page 43*

10.2.2 Configuration Manager

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

1. In the 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.



Notice!
Certificates can be uploaded using Configuration Manager, but usage definition must be done via the **Certificates** web page.

Notice!

Data security hint no. 19

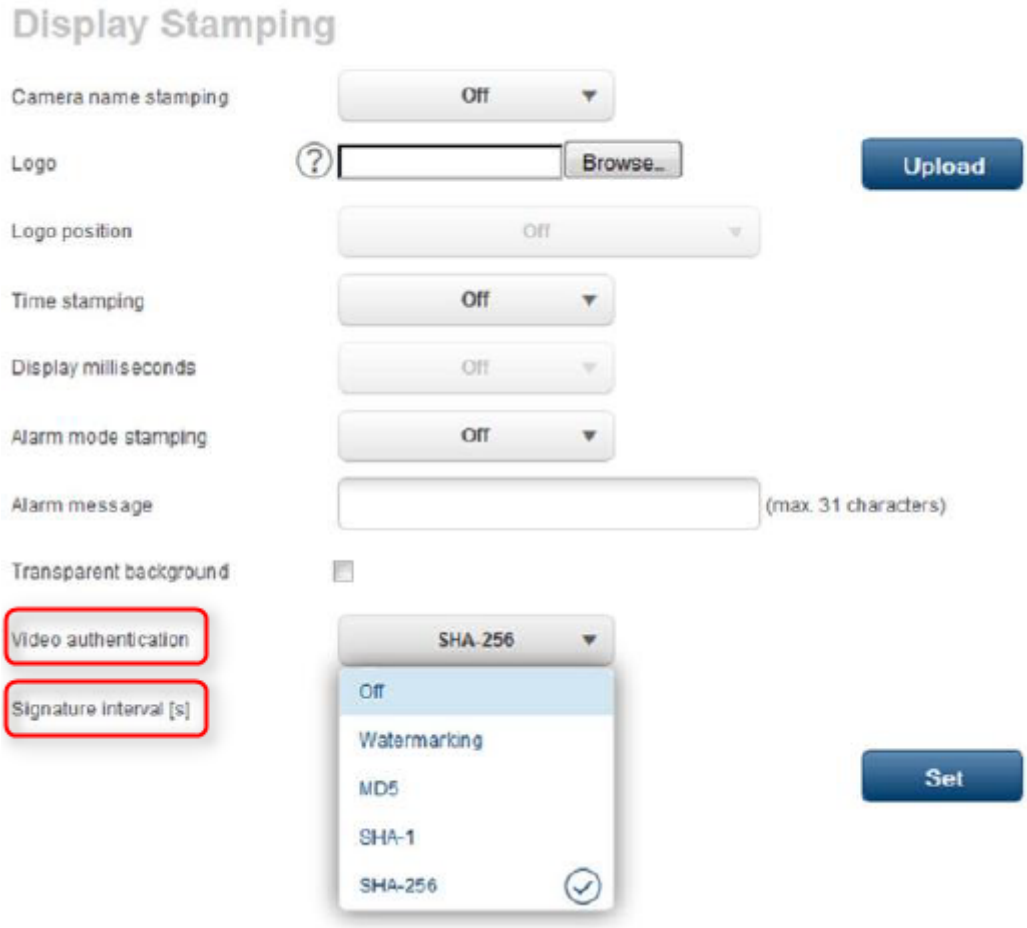
Certificates shall be used to authenticate a single device. It is recommended to create a specific certificate per device, derived from a root certificate.

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, which is also capable of verifying the origin and validity – in other words the trustfulness – of the device's certificate.

11 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.



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.

12 Decomissioning and disposal

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. 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.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com

202104261717