Configuration Manager 6.0

en Operation Manual

Table of contents

1 Using the Help

The online Help provides you with information about this program directly on your screen. You can also find this information in the manual.
To find out more about how to do something in this program, access the Help.

1.1 Finding information

To find information in the Help:

1. Press F1.
   or
   On the **Help** menu, click the help entry.
   The dialog box for the Help is displayed.
2. If the pane to the left is not visible, click the **Show** button.
3. In the Help window, do the following:
   Contents
   Display the table of contents for the Online Help. Click each book to display pages that link to topics, and click each page to display the corresponding topic in the right-hand pane.
   Index
   Search for specific words or phrases or select from a list of index keywords. Double-click the keyword to display the corresponding topic in the right-hand pane.
   Search
   Locate words or phrases within the content of your topics. Type the word or phrase in the text field, press ENTER, and select the topic you want from the list of topics.

Notice!
Texts of the user interface are marked **bold**.

- The arrow invites you to click on the underlined text or to click an item in the application.

Related Topics

- Click to display a topic with information on the application window you currently use. This topic provides information on the application window controls.

1.2 Printing the Help

While using the Online Help, you can print topics and information right from the browser window.
To print a Help topic:

1. Right-click in the right pane and select **Print**.
   The **Print** dialog box opens.
2. Click **Print**. The topic is printed to the specified printer.

2 Introduction

2.1 About this manual

This manual is intended for persons responsible for configuring and managing a CCTV system. This manual describes how to configure the program.
This document assumes that the reader is familiar with both the CCTV system and the other programs that are integrated into the system.

2.2 About this Help

This application help is intended for persons responsible for configuring and managing a CCTV system. The Help describes how to configure the program.
This Help assumes that the reader is familiar with both the CCTV system and the other programs that are integrated into the system.

2.3 Conventions in this document

The following symbols and notations are used to draw attention to special situations:

Notice!
This symbol indicates special features and provides tips and information for easier, more convenient use of the software.

Terms that you can find in the program, such as menu options, commands or text in the user interface, are written in **bold**.

2.4 Additional documentation

After the program has been installed, this document is also available as online Help within the program.

More information
For more information, software downloads, and documentation, visit www.boschsecurity.com and go to the respective product page.

3 System overview

Configuration Manager program is used to configure all IP devices and components in your CCTV network. With Configuration Manager you have access to all devices and software components.
The program offers also a configuration wizard for quick basic configuration of devices. However, you can also carry out the further configuration with the normal user interface.

3.1 Functions

Configuration Manager provides the following functions (the availability of these depends on the environment in which the program is used):

- **Network Scan**
  The network scan is performed automatically every time Configuration Manager starts, and is repeated at regular intervals.
  This function automatically detects all compatible devices present in a network, such as cameras or video senders, video receivers or VRM. The status of a device is also queried in each scan and then indicated by the icons in front of the devices.
- **Device information and configuration**
  Comparable with the Web browser view, Configuration Manager shows the current configuration for each device and allows you to change the settings.
- **Device system integration**
  You use the Device allocator in Configuration Manager to make devices accessible for use with Video Client.
- **MicroCA**
  The MicroCA functionality in the Configuration Manager program is an easy-to-use tiny certificate authority (CA) that facilitates the management of small to medium systems.
- **Multiple configuration**
  You can use Configuration Manager to make individual settings for multiple devices simultaneously (for example, time settings), allowing you to configure large systems more quickly.
- **Simpler access to devices**
  The **Screenshot Scan** function gives an overview of all the cameras that provide video data. The screenshots can be used to identify the camera and device, and give you direct access to said camera or device.
- **Table View**
  This allows you to compile specific parameter settings for selected devices. This provides you with a quick overview of the settings that are of interest to you and allows you to export this information for archiving at the push of a button.
- **Device Health Monitor**
  This provides you with a quick overview of the status of selected devices, such as the encoder load and type of network connection.
- **System emulation**
  The complete system configuration can be saved as a system image and emulated using a different Configuration Manager application. This function helps you to isolate problems without having to access the actual system.
- **Access to license management**
  Firmware modules requiring a license, such as IVA (Intelligent Video Analysis), are set up using Configuration Manager.

4 Installation and starting

Configuration Manager is automatically part of the installation for all video IP devices that require Configuration Manager for configuration purposes. Furthermore, you can also use Configuration Manager to simplify the configuration in a CCTV system with many similar video senders.

4.1 System requirements

Notice!
All Microsoft updates and hotfixes must be installed on target PCs. Graphic card drivers must also have the latest officially released version described in the VideoSDK help.

4.2 Installation

You can install Configuration Manager on as many computers running Microsoft Windows as you wish.

Notice!
Using multiple Configuration Manager programs in the network, maintaining the same or an overlapping set of devices simultaneously can result in unpredictable effects when writing to the devices.

To install Configuration Manager:

1. Close all other applications before beginning the installation.
2. Download the software package.
3. Select the extraction directory and double-click `Setup_ConfigManager.exe`.
   The Configuration Manager wizard dialog box is displayed.
4. On the **Welcome** dialog box, click **Next**.
5. In the **Select components to install:** list, select the respective tools, then click **Next**.
6. In the **Choose Install Location** dialog box, select the destination folder, then click **Install**.
   The installation process starts.
   Note: We recommend using the default destination folder.
7. Click **Finish**.

4.3 Starting the program

After successful installation, you will find the Configuration Manager icon on your desktop:
To start the program:

- Double click the Configuration Manager icon.

or

- On the **Start** menu, click **Configuration Manager**.

Note:
Several video IP devices enable you to start Configuration Manager directly within the relevant program.
Operation of Configuration Manager varies according to the context in which it is being used. In some cases, it is merely a tool that enables you to configure video IP devices more conveniently and more comprehensively. For certain programs and firmware modules, however, Configuration Manager is indispensable, as it is the only way to set these up.

4.4 Removing the program

If you no longer wish to use the program on your computer, you can remove the program at any time.

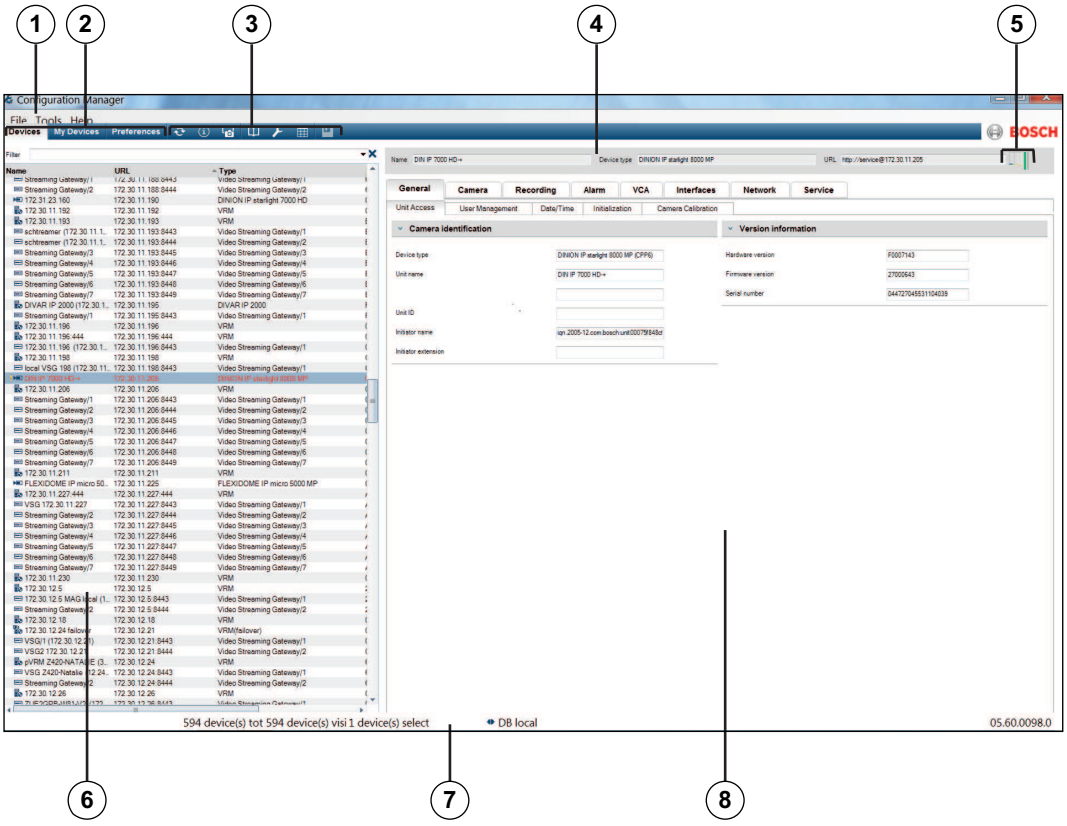
To remove the program:

1. Click **Start**, click **Settings**, then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Select the Configuration Manager entry.
4. Click **Remove**.

5 User interface

In this section, you will find detailed information about the user interface.

5.1 Overview



1 Menu bar

2 Toolbar tabs
For quick access (**Devices**, **My Devices**, **Preferences**)

3 Toolbar icons
For quick access (configurable).

4 Info bar
With name, type and IP address of the selected device.

5 Quick indication icons
Displays CPU load, network and recording status.

6 Device tree structure with filter option.

7 Status bar

8 View pane
Depending on the toolbar tab selected, this window displays different device tabs with configuration options and information.

5.2 The Menu bar

This section contains special operational functions, tools and help functions.

5.2.1 The File menu

To obtain the menu commands:

- Click the **File** menu. The following commands are displayed.

Connect to Bosch Remote Portal
Connects Configuration Manager prograam to the Bosch Remote Portal page to perform remote administration and maintenance tasks.

Emulate Alien System... / Abandon Emulation
Imports the system image of an alien Configuration Manager system.

Close
The Configuration Manager program is closed. This also breaks the connection between Configuration Manager and the server.

5.2.2 The Tools menu

To obtain the menu commands:

- Click the **Tools** menu. The following commands are displayed.

Logging...
Displays the **Device Communication Log** dialog box.
Here, you can view the RCP+ commands that are transmitted by Configuration Manager when connecting to devices, if you have enabled logging.

Device Allocator...
Displays the **Device Allocator** dialog box. An overview of all available devices in the network and all devices that are allocated to the system.

Table View...
Displays the devices in table view.

Screenshot Scan...
Displays a window in which a screenshot for each of the connected cameras is displayed. If you right-click a screenshot, the commands are displayed relevant for the device.

Device Health Monitor...
Displays the **Device Health Monitor** dialog box, which provides a quick overview of the status of selected devices.

Save System Image
Saves the image of the currentConfiguration Manager system for emulation on a different PC.

Import CSV File...
Displays a dialog box that allows you to import .csv files.

Video Client...
Opens the Video Client program.

5.2.3 The Help menu

To obtain the menu commands:

- Click the **Help** menu. The following commands are displayed.

Online Help...
Displays the Configuration Manager Help.

Online Help VRM...
Displays the Video Recording Manager Help.

Online Help IVA...
Displays the Intelligent Video Analytics Help.

About...
Displays the **About Configuration Manager** dialog box, containing information on, for example, the software components installed on this PC and the software version numbers of the installed components.

5.3 Toolbar tabs

The toolbar enables quick access to the most important functions.

5.3.1 The Devices tab

This tab shows all video IP devices supported by Configuration Manager that are detected in the network scan.

Additional Information:

- The information about a device is shown in bold if the device is newly detected since the last network scan.
- The information about a device is shown in red if the device has an IP address or a MAC address that is already used by another device in the system. This might be the case, for example, if several devices that have not yet been configured are connected directly after one another.
- Additional information about the devices can be seen if you scroll to the right.

5.3.2 The My Devices tab

This tab shows all devices that have previously been manually allocated to the system.

Additional Information:

- The information about a device is shown in bold if the device is newly detected since the last network scan.
- The information about a device is shown in red if the device has an IP address or a MAC address that is already used by another device in the system. This might be the case, for example, if several devices that have not yet been configured are connected directly after one another.
- Additional information about the devices can be seen if you scroll to the right.

5.3.3 The Preferences tab

This tab enables you to access general and application-specific settings. Here, you can carry out a basic configuration for Configuration Manager itself as well as for other video IP devices. This tab has a tree structure with the following main folders:

- **General**
- **Applications**

If necessary, expand the folders to obtain subordinate items.

General folder

In this tab you make the settings that affect several programs. Changes only become active if you click the **Save** icon on the toolbar.

General > **Directories**

Specifies where screenshots, recording sequences and vdb.xml databases should be saved. These settings are relevant for Video Client.

- **Directories** tab > **Directories** group

  Screenshot folder

  Select the folder for the screenshots.

  Recording folder

  Select the folder for the recordings.

  Database folder

  Select the database folder.

General > **Logging**

- **Logging** tab > **Logging** group

  Enable RCP+ logging

Enable or disable the logging of RCP+ commands. A log file is created for every device in the system.

Maximum number of days to keep log files

Specify the maximum period for which you want the log data to be saved.

Applications folder

In this tab you make the settings that affect an individual program. When leaving this page Configuration Manager asks you whether you want to save the changes. Changes only become active if you click the **Save** icon on the toolbar.

Only programs that are installed on your computer are listed under this tab. If a program is not listed under this tab, check if it is installed on your computer and install it if necessary.

Applications > **Configuration Manager**

This is where you can change the default settings for Configuration Manager.

– **Access** tab > **Access** group

Password

Assign a password here that protects access to Configuration Manager. If you do not enter anything in this field, the program will start without asking for a password.

This password is only valid for the computer on which it was defined.

Password policy

We recommend that you use strong passwords to enhance the protection of your computer against unauthorized access.

– **Access** tab > **Security** group

Encrypted communication (defines the TLS connection preferences)

To define the TLS connection preferences, select the required levels.

– **Optional**

Encrypted connections (HTTPS) and non-encrypted connections (HTTP, RCP+) are allowed.

No certificate validation is performed. The certificate requirement level is not relevant.

The default protocol HTTP is used when adding devices to the system.

The VSDK security properties are set as follows: **Allow unencrypted connections**, **Allow unencrypted media exports**, and **Allow no forward secrecy**.

– **Preferred**

Encrypted connections (HTTPS) and non-encrypted connections (HTTP, RCP+) are allowed.

The certificate validation is performed. The certificate requirement level is relevant. If validation failed a warning is displayed but a connection still possible.

The default protocol HTTPS is used when adding devices to the system.

The VSDK security properties are set as follows: **Allow unencrypted connections**, **Allow unencrypted media exports**, and **Allow no forward secrecy**.

– **Required**

A communication with devices is only possible using HTTPS.

The certificate validation is performed. The certificate requirement level is relevant. If validation failed an error message is displayed and no connection is established.

The default protocol HTTPS is used when adding devices to the system.

There are no changes in the VSDK program.

Certificate requirement level (settings are used when validating certificates)

To validate certificates, select the required levels.

- **None**: All certificates are accepted. No validation is performed.
- **Valid**: Only an end certificate validation is performed. The certificate must be valid (standard validation procedure, time signature).
- **Trusted:** The entire chain validation is performed, The root CA certificate is used to sign the certificate and must be trusted on machines where the validation is performed.
- **Issued by the CA**: The entire chain validation is performed, The root CA certificate is used to sign the certificate and the MicroCA program must be configured in Configuration Manager program.

Database encryption level

Select the required levels.

- **Default**: Legacy mode. Encrypted with internal key:
- **Strong**: The AES encryption is used. If no password is configured in the **Access** group, the default AES key is used. After entering the access password the database is encrypted with this password.

– **Network** tab **>** **Network Scan** group

Run continuous network scan

Enable this option if the network is to be scanned at regular intervals.

Scan interval [s]

Enter the time interval in seconds for automatic scanning here, choosing a value between 10 and 3600 seconds (1 hour).

– **Network** tab **>** **Network Scan RCP+** group

Use Multicast

If you are using devices in various subnets, activate this option. This allows all devices that belong to a different subnet than the PC on which Configuration Manager is installed to also be included in the network scan. Otherwise you will have to manually add these devices to the system.

Multicast operation requires a multicast-enabled network that uses the UDP and the Internet Group Management IGMP protocols.

– **Network** tab > **IP address range** group

Mode

Specify the IP address ranges and select the protocols.

– **Network** tab > **DIVAR AN FW upload**

Select the port number for the DIVAR AN firmware upload.

– **Video** tab **>** **Monitor** group

Refresh interval

Select how often the screenshots that are shown in the various tabs (e.g. **VCA**) are refreshed:

Continuous: Image is refreshed as often as possible.

0 seconds: Image is displayed once but not refreshed.

1 ... 10 seconds: Image is refreshed accordingly.

Encoder

Select whether the images should be displayed in video format (**H.26x**) or as constantly updated screenshots (**JPEG**).

– **Repository** tab > **Repository** group
Database folder
If necessary, change the location in which configuration data is to be backed up.

– **Security** tab > **MicroCA** group
Here you can create a CA certificate.
Create: Click **Create**. The **Create CA** dialog box is displayed.
To create a CA certificate, refer to:
– *Configuring MicroCA using Smart Token, page 42*
– *Configuring MicroCA using USB file, page 44*
Load: Click **Load**. The **Load CA** dialog box is displayed. You can load existing CA certificates.
Signature Validity [days]: Select the validity of the certificate.

– **Security** tab > **User token** group
Certificate store type: Click the **Certificate store type** list to display a list of existing tokens known to your system.
To manage and create user tokens, refer to:
– *Managing user token, page 47*
– *Creating user token, page 48*

– **Logging** tab > **Device I/O** group
Select whether the device communication log should be wrtten in a file and which data it should include.

– **Logging** tab > **ONVIF logging** group
Enable logging; Enable or disable the logging of ONVIF commands. A log file is created for every device in the system containing the time stamp, the URL, the ONVIF service and the command. The output is displayed in the **Device Communication Log** dialog box.

– **Logging** tab > **Sony CGI logging** group
Enable logging; Enable or disable the logging of Sony cameras.

– **Appearance** tab > **General** group
Language: Select the display language.
Toolbar: Click **Edit** to adapt the toolbar to your needs.

– **Appearance** tab > **Startup** group
Restore last view
If enabled, the view last used is displayed when Configuration Manager is next started.
After confirmation only
If enabled, the next time you start Configuration Manager you will be asked whether you want to restore the last view used.

– **Appearance** tab > **Database camera name** group
Prefix device name to camera name

Displays the encoder device name before the camera name in the camera list if cameras are integrated into the system over video encoders.

Applications > Video Client
This is where you can change the settings of Video Client.

– **User Management** tab > **Management** tab
Users group
Implement user administration to control access to the Video Client program.

– **Cameras** tab > **Camera Order** tab
Camera order group
Define which cameras are listed in Video Client and define corresponding access rights.

– **Cameras** tab > **Camera Access** tab
Camera access group
Specify the access rights for the cameras listed in Video Client. Each user is assigned the highest authorization level by default.

– **Digital Inputs** tab > **Digital Input Order** tab
Digital input order group
Define which digital inputs are listed in Video Client and define corresponding access rights.

– **Digital Inputs** tab > **Digital Input Access**
Digital input access group
Specify the access rights for the digital inputs listed in Video Client. Each user is assigned the highest authorization level by default.

– **Alarm Outputs** tab > **Output Order** tab
Output order group
Define which alarm outputs are listed in Video Client and define corresponding access rights.

– **Alarm Outputs** tab > **Output Access**
Output access group
Specify the access rights for the alarm outputs listed in Video Client. Each user is assigned the highest authorization level by default.

– **Application** tab > **Application** tab
> **Workstation recording** group
Path for workstation recording
Select the path to the folder to which Video Client will export manual recordings. If you do not enter anything here, the following default setting is used:
%current user%\My Documents\ Bosch\VideoClient\Recording
Maximum disk usage [GB]
Define the maximum hard disk memory to be used for manual recordings. If you do not enter anything here, the default setting 10 is used.
Delete recordings when maximum disk usage exceeded

Activate this option if existing recordings are to be overwritten when the specified maximum memory capacity has been reached.

– **Application** tab > **Application** tab
> **IntuiKey** group
Use keyboard
Select the checkbox if a Intui Keyboard is used.
COM port
If the program is operated via an IntuiKey control panel, enter the number of the COM port here.

– **Application** tab > **License** tab
On this page you can find information on the licensing of camera channels in Video Client. A Video Client installation has 16 camera channels as standard. You can enable additional channels by purchasing a license.
For more information, please see the Video Client operator’s manual.
Host-ID
The host ID, which is needed to install a license for additional camera channels for Video Client, is displayed here.
Number of cameras
The number of enabled camera channels is displayed here.
Add License...
Click to add a license file for additional camera channels. The **Add License File**.

5.4 Toolbar icons

The toolbar icons allow quick access to several Configuration Manager functions.

 **Reload page**

Reloads device and page information and starts a device scan on the **Devices** tab.

 **Info**

Displays detailed information about the selected device.

 **Live video**

Displays the live video data from the selected device.

 **Logging**

Displays the **Device Communication Log** dialog box.
Here, you can view the RCP+ commands that are transmitted by Configuration Manager when connecting to devices, if you have enabled logging.

 **Device allocator**

Displays the **Device Allocator** dialog box. This dialog box allows you to allocate devices to the system and build the device tree structure.

 **Table view**

Displays the **Table View** dialog box. Click again to close the **Table View** window.

 **Export**

In the **Table View** window, click to export the content of the different **Table View** tabs as .csv file.

 **Import**

In the **Table View** window, click to import .csv files to the different **Table View** tabs.

 **Save**

Saves any settings that have been configured for the selected device.

5.5 The Info bar

When one of the **Devices** or **My Devices** tabs is selected, an info bar is displayed above the View pane. This info bar provides you with brief information about each selected device as follows:

- Device name
- Device type
- Device IP address

Note: If several devices are selected, all fields contain the entry **<Multiple>**
For hardware devices, you can use the icons on the right-hand edge of the bar to display additional information.

5.6 The Quick indication icons

To display the quick indication icons:

- Drag the pointer on the icons to view details on the processor load, network connection and recording status:

Quick indication icon description

- The left icon indicates the proportions of the individual functions on the encoder load, shown as percentages. For devices with two processors, a separate icon is shown for each processor.
- The icon in the middle indicates the network connection type and the speed of the outgoing (UL = Uplink) and incoming (DL = Downlink) data traffic.
- The right icon indicates information on the recording status.
  - Green: active recording
  - Red: error
  - Orange: recording scheduler active, no current recordings
  - Gray: recording scheduler not active, no current recordings

5.7 The Status bar

The status bar at the bottom edge of the window shows the following:

- In the left section: whether or not a network scan is currently in progress.
- In the central section: the number of detected, visible and selected devices.
- In the right section: whether you are currently working **Online**, and whether or not Configuration Manager is currently connected to a server. If it is connected to a server, the server IP address is displayed. Otherwise the entry **DB local** appears here.
  If you are emulating an alien system, the entry **System emulation** appears here.
- On the far right: the version number of Configuration Manager is displayed.

5.8 The View pane

The View pane for the **Devices** and **My Devices** tabs shows a series of subdivided tabs, the number and content of which depend on the device selected in the list.
The tabs in the View pane can be used to make the configuration settings that the device also provides in the Web browser view, some of them with a slightly different composition.
Access from Configuration Manager to the devices can be configured when selecting the **General** and **Unit Access** tab (not necessary for web browser).
Detailed information about the configuration options for a device can be found in the relevant device documentation and the online Help in the relevant Web browser view.

Notice!
Changes only become active if you click the **Save** icon on the toolbar.

5.9 Used icons

The devices in the **Devices** / **My Devices** tabs are represented by the following icons:

Device icons

 Camera

 Device (for example, Encoder/Decoder/Streaming Gateway)

 Hardware recorder (for example, DIVAR)

 Storage system (for example, DIVAR)

 DomeCamera

 iSCSI target

 Video Recording Manager server

 Video Recording Manager failover server

 Video Recording Manager server for second recording stream

 Video Recording Manager failover server for second recording stream

 Unknown

Device status icons

The status of the icons is shown exemplarily by using a camera. Other devices are displayed in the same manner

Icon	Color	Status	Online	Authentication	Secure connection	Trusted certficates
	Camera grey	OK	No	Unknown	Unknown	Unknown
	Camera grey, exclamation mark yellow	Warning *	No	Unknown	Unknown	Unknown
	Camera grey, exclamation mark red	Error *	No	Unknown	Unknown	Unknown
	Camera grey, lock red	No access	No	No *	Unknown	Unknown
	Camera blue	OK	Yes	Yes	No	Not relevant
	Camera blue, exclamation mark yellow	Warning	Yes	Any	No	Not relevant

Icon	Color	Status	Online	Authentication	Secure connection	Trusted certficates
	Camera blue, exclamation mark red	Error	Yes	Any	No	Not relevant
	Camera blue, lock red	No access	Yes	No	No	Not relevant
	Camera yellow	OK	Yes	Yes	Yes	No
	Camera yellow, exclamation mark yellow	Warning	Yes	Any	Yes	No
	Camera yellow, exclamation mark red	Error	Yes	Any	Yes	No
	Camera yellow, lock red	No access	Yes	No	Yes	No
	Camera green	OK	Yes	Yes	Yes	Yes
	Camera green, exclamation mark yellow	Warning	Yes	Any	Yes	Yes
	Camera Green, exclamation mark red	Error	Yes	Any	Yes	Yes
	Camera green, lock red	No access	Yes	No	Yes	Yes

* Device was online

Icons on the View pane

The following icons are used on the View pane:

 Help. Click the icon to open context-related help.

 Warning. This element contains important information.

 Danger. This element contains very important information.

 Info. Click the icon to display a camera's properties.

 Connection established.

 Connection lost.

 Recording state: Device is recording.

 Recording state: Device is not recording.

 Relay state: Relay is in default state.

 Relay state: Relay switched to alert state.

 Locked: This element does not allow input or changes.

MicroCA icons
The following icons are related to the MicroCA functions:

 Device has a valid certificate.

 Signing button: Click this icon to sign and upload a certificate.

 User token button: Click this icon to add a user token.

5.10 Shortcut menu

Right-click a device to open the shortcut menu. If you have selected multiple devices, not all options in the shortcut menu are enabled.
The following provides an overview of the commands:

Add to System...
(**Devices** tab)
Allocates the selected device to the system. Before making an allocation, you can select a group or create a new one.
This command corresponds to the **Device Allocator** dialog box.

Select Group
(**My Devices** tab)
If several devices have been grouped, use this command to select all devices or cameras of that group for editing.

Node > Expand Child Nodes
(**My Devices**)
Click to expand a group or site to see the devices and cameras assigned to it.
Node > **Collapse Child Nodes**
(**My Devices** tab)
Click to collapse a group or site to hide the devices and cameras assigned to it.

New Device...
(**My Devices** tab)
Allocates a non-listed device to the system. This command is only active if you click the area in the left pane in which no devices are listed.

Delete
(**My Devices**)
Deletes the selected device from the system.

Site
(**My Devices**)
Click to change a group to a site. Select the group first.

Set Session Authentication...
(**Devices** tab)
If a selected device is protected by a password, you must authenticate yourself for that device.

Configure...
Displays the respective configuration tool if installed.

Add iSCSI System... (VRM)
Displays the **Add iSCSI System** dialog box.
Here, you can add an iSCSI system to the VRM using the host IP address and the SNMP IP address.

LUN Assignment... (iSCSI system)
Displays the **LUN Assignment** dialog box. Here, you can add individual LUNs to the system.

File Upload
- **Firmware...**
  You can select the desired upload file and start the upload. Refer to the information about firmware uploads in the documentation for the relevant device.
  You can use this command to carry out a firmware upload for several devices at the same time. You must ensure that all selected devices are of the same device type when you carry out a firmware upload for several devices at the same time.
- **SSL Certificate...**
  Upload an SSL certificate to the device to enable encrypted communication with the device.
- **Decoder Logo...**
  The decoder logo is the image displayed by the decoder if there is no connection to a device. You can upload your own logo for this purpose. This must be in H.263 format.

Settings
(**Add to System...** and **My Devices** tab)
- **Download...**
  Configuration data of the selected devices is saved on your computer for offline editing.
- **Upload...**
  The configuration data that was edited offline is sent to the selected device. Once the upload has been successfully completed, the device operates according to the new configuration data.
- **Replacement...** (only in **My Devices** tab)
  Configuration data of replaced devices is automatically replaced with locally stored data of a device of the same type.

Device Network Settings...
(**Add to System...** and **My Devices** tab)
You will see the **Network settings** dialog box.
This dialog box is used to change the IP address, subnet mask and gateway of the selected device or activate automatic IP assignment via DHCP.
This is only possible for devices that are not password-protected.

Show Live Video...
(**Add to System...** and **My Devices** tab)
A window opens, displaying the live video data from the selected device. You are offered different display options depending on which device you selected.

Show in Web Browser...
(**Add to System...** and **My Devices** tab)
The live page of the Web browser view for the device is opened in the default browser.

Show Settings in Web Browser...
The configuration page of the Web browser view for the device is opened in the default browser.

Device Info...
The dialog box containing device information is displayed.

Blink LED
(**Add to System...** and **My Devices** tab)
A LED on the device flashes. This allows you to check whether there is any communication between Configuration Manager and the device. This command also helps you to identify a device if several devices of the same type are installed at the same location.

Restart
(**Add to System...** and **My Devices** tab)
Initiates a reboot of the device. This is only possible for devices that are not password-protected.

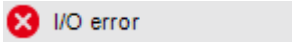
Ping
(**Add to System...** and **My Devices** tab)
Pings the selected device to confirm network communication with the device.

5.11 Blocked input fields

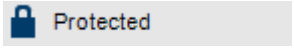
It is possible that some fields are blocked for editing. The causes for the block are indicated by different entries in the fields.

If several devices are selected, some settings cannot be made. The input fields are marked with a padlock.

If a device is currently recording, some settings cannot be modified. The input fields are marked with a padlock. If necessary, stop the recording.



If there is a configuration error, individual fields are marked accordingly.
This icon is also displayed if the device is offline and you attempt to load or save settings.



Input fields you are not authorized to change are marked by a padlock and are blocked for editing.

Some input fields cannot be edited when you are working offline (date and time settings).

6 Working with Configuration Manager

The following section offers a list of user actions for configuring hardware and software components that can be performed using Configuration Manager.

6.1 Adding devices to the system

You can add devices and components to the system that are detected in the network.
To add devices to the system:

1. On the toolbar, click the **Devices** tab, right-click a device in the tree structure, then click **Add to System...**.
   The **Add Device to System** dialog box is displayed.
2. Select an existing group to assign the device or leave the field empty if you do not want to assign the device to a group.
3. Click **OK**. The device is added to the system.

See also:

– *Allocating devices, page 26*

6.2 Allocating devices

Before working with Video Client, you must complete the allocation, as the program can only access devices that have been allocated to the system.

6.2.1 Allocating listed devices

You can allocate all devices using the **Devices** tab. It is also possible to allocate devices to the system by adding them to the **My Devices** tab. This simplifies configuration as you can limit yourself to a relevant selection of available devices and clearly arrange the allocated devices in groups.
To allocate listed devices using the **Device Allocator** icon:

1. On the toolbar, click the **Device Allocator**  icon.
   The **Device Allocator** dialog box is displayed.
   All devices detected in the network are displayed on the left-hand side of the dialog box, while those allocated to the system appear on the right.
2. Drag the unallocated devices from the left to the right-hand side of the window.
3. If necessary, sort the list of entries. To do this, click the appropriate table header.
4. Click **OK**.
   The devices are integrated into the system.

Notice!
If it is not possible to integrate a device, a warning message appears.

See also:

– *Creating groups, page 27*
– *Defining a group as site, page 28*

6.2.2 Allocating unlisted devices

The **Device Allocator** dialog box also enables you to allocate devices to the system that were not detected during the network scan.
Allocating an unlisted device:

1. In the **Device Allocator** dialog box, right-click into the **Allocated devices** area (but not on a device).
2. Click **New Device...**.
   The **Device Editor** dialog box is displayed.
3. Enter the URL (for example, the IP address with the port number) of the device. The IP address must previously have been set on the device.
4. In the **Type** list, select **<Auto detect>** or select the device type from the list of supported devices.
   If you select an ISDN-compatible device, the field for the telephone number is also activated.
5. Enter the telephone number for the ISDN connection if you want a device to be connected using an ISDN line.
6. Click **OK**.
   The device is listed as allocated device.

Notice!
You can only allocate supported devices. In the tree structure of the **Devices** and **My Devices** tabs, not supported devices are displayed dimmed or red.

See also:
- *Creating groups, page 27*
- *Defining a group as site, page 28*
- *Used icons, page 21*

6.3 Clearing device allocations

You can remove devices from the system at any time by clearing the allocation. The devices are then no longer listed in the **My Devices** tab and can no longer be accessed in Video Client. To clear device allocations:

1. On the toolbar, click the **Device Allocator** icon.
   The **Device Allocator** dialog box is displayed.
2. Drag a device from the right to the left-hand side of the dialog box
   or
   right-click the device and click **Delete**.
3. Click **OK**.

Notice!
Delete groups in the same way. If you delete a group, you also clear the allocation of all devices that you have allocated to that group.

6.4 Creating groups

The **Device Allocator** dialog box enables you to clearly combine the devices into groups, for example sorted by locations.
To create groups:

1. In the **Device Allocator** dialog box, right-click into the **Allocated devices** area (but not on a device).
2. Click **New Group...**.
   The **Add New Group** dialog box is displayed.
3. Enter a name for the new group.

4. Click **OK**.
   The group is added to the list.
5. Drag a device from the list to the group name.
   The device is added to the group and listed under the corresponding name.
   Note: To remove a device from a group, drag the device from the group to the list.
6. Click **OK**.
   The grouping is displayed in the device tree structure.

You can also create sub-groups by dragging a group to the name of another group in the **Device Allocator** dialog box.

Additional Options

– On the toolbar, click the **My Devices** tab, right-click the tree structure area (but not on device), then click **New Device...**.
– On the toolbar, click the **Devices** tab, right-click a device in the tree structure, then click **Add to System...**.
  A dialog box is displayed, in which you can assign the device to a group. Select an existing group to assign the device or leave the field empty if you do not want to assign the device to a group.

See also:

– *Defining a group as site, page 28*

6.5 Defining a group as site

You can define a group as site to use it in Video Client.

Notice!
Cameras that are assigned to a group are only available if the site is connected. That means, for chargeable connections costs only arise in this case.

To define a group as site:

1. On the toolbar, click the **My Devices** tab.
2. Right-click the group in the tree structure or in the **Device Allocator** dialog box, then click **Site**.
   The icon to the left changes from  to  .

To define a site as group:

1. On the toolbar, click the **My Devices** tab.
2. Right-click the site in the tree structure or in the **Device Allocator** dialog box, then click **Site**.
   The icon to the left changes from  to  .

6.6 Accessing the device

If a device is not currently communicating with the system, for example, because it is only temporarily contactable or because a firewall is blocking communication, a message is displayed in the view window.
In this case, Configuration Manager offers various setting options to enable communication again.

IP address failure

Communication can fail because the device IP address has been changed (for example, using the device's Web browser view) and Configuration Manager is still using the old IP address to establish the connection.

To refresh the system:

1. On the toolbar, click the **Devices** tab.
2. Click the icon.
   Configuration Manager scans the network for devices and displays them with their current settings.

Device Access

If a firewall is blocking communication between the device and Configuration Manager, you can change the transmission protocol:

To change the transmission protocol:

1. On the toolbar, click the **My Devices** tab, click the **General** tab, then click the **Unit Access** tab.
2. In the **Device access** group, select the transmission protocol from the **Protocol** list.
   - **RCP+**
     TCP transmission using port 1756
   - **HTTP**
     TCP transmission using preset port
   - **HTTPS**
     TCP transmission using preset port
3. If you have selected HTTP or HTTPS as the protocol, you must set the port to correspond to the settings stored in the device.
4. Under **Authentication**, you can set up a password for a user name of the relevant device. This means that Configuration Manager automatically has access to the device when establishing a connection without the password protection having to be disabled each time.

Notice!
Do not use any special characters, for example **&**, in the password.
Special characters are not supported for the password and can prevent you from being able to access the program.

6.7 Replacing devices

If devices must be replaced, most of the configuration for the new devices can be done automatically using the **Replacement** function.

The **Replacement** function can only be used on devices that are allocated to the system - such devices are listed in the **My Devices** tab.

To replace devices:

1. On the toolbar, click the **Preferences** tab, expand **Applications** in the tree structure, click Configuration Manager, then click the **Repository** tab.
2. In the **Database folder** box, enter the location in which configuration data is to be backed up.
3. On the toolbar, click the **My Devices** tab, right-click the device, click **Settings**, then click **Download...**.
   The device configuration settings are saved locally on your PC.
4. Replace the device.
5. In Configuration Manager, click the **My Devices** tab.
   The replaced device is shown as not being configured.
6. Right-click the device, click **Settings**, then click **Replacement...**.
   The **Device Replacement Wizard** dialog box lists all devices that are the same type as the replaced device and for which configuration data is saved.

7. Select the replacement device that was installed instead of the selected device.
8. Click **Next >**.
   Automatic configuration is started.
9. You will be informed if the firmware version of the device and the configuration file differ. You are able to download a new firmware version onto the device.
10. Click **Next >** again.
    The **Device Replacement** dialog box is displayed, listing the selected device and additional information.
11. Click **Start**.
    The configuration files are transferred. If it is not possible to transfer all the data, the number of data packets not transferred is listed in the **Failed** column.
    Once the transfer is complete the device is rebooted so that the new settings take effect.
    When the **Cancel** button is replaced by the **Close** button, the procedure is complete.
12. Click **Close**.
    The **Device Replacement Wizard** dialog box is displayed again.
13. Click **Finished** to complete the procedure.

6.8 Saving screenshots, recordings and vbd.xml databases

Specify where screenshots, recording sequences and vdb.xml databases should be saved. These settings are relevant for Video Client.

To save screenshots, recordings and vbd.xml databases:

1. On the toolbar, click the **Preferences** tab, expand **General** in the tree structure, click **Directories**, then click the **Directories** tab.
2. In the relevant input field, enter the path for the storage location or click **...** to select a folder.

You can select any directory that is available in the network as the target location.

If you do not enter a screenshot folder and a recording folder, the following default setting is used:

– C:\New Folder

Warning!
Check the selected directories regularly for available storage capacity. Delete recordings that are no longer required.

6.9 System emulation

The complete system configuration can be saved as a system image and emulated using a different Configuration Manager application. This function helps you to isolate problems without having to access the actual system.

To save a system image:

1. On the **Tools** menu, click **Save System Image...**.
   The **Save System Image** dialog box is displayed.
2. Select the storage location and enter a name for the zip file.
3. Click **Save**.

To emulate an alien system:

1. Save the zip file containing the image of the alien system to your PC.
2. On the **File** menu, click **Emulate Alien System...**.
   The **Choose Alien System** dialog box is displayed in which you can select the storage location and the image file.

3. Click **Open**.
   The emulation is performed automatically. The message **System emulation** appears in the status bar.
4. On the **File** menu, click **Abandon Emulation** to return to your own system.
   The message **System emulation** disappears in the status bar.

6.10 Notes on multiple configuration

It is possible to select multiple devices and then simultaneously make settings for all selected devices. In this way, CCTV systems can be set up quickly and efficiently.
To configure multiple devices:

1. Click the **Devices** or **My Devices** tab, then select the devices in the tree structure.
   Note: For selecting multiple devices, use **CTRL** and/or **SHIFT**.
2. In the View pane, select the tab in which you want to make changes.
   The following special features are available for multiple selections:
   - Input fields that can only be changed for individual devices (for example, **Device IP address**) are blocked.
   - Input fields where the settings for the selected devices differ because of their type (for example, recording planning for different video senders) are blocked.
   - Input fields that already have identical settings for all selected devices show these settings.
   - Input fields containing different entries for the selected devices show **<multiple>** or M.
   - Options that are only activated (checked) for some of the selected devices are indicated by a green square.
3. Change the settings as desired.
4. Click **Save**.
   Changed input fields that previously contained **<multiple>** or M now display the uniform value.
5. Continue for all other tabs in which you want to make changes.

6.11 Configuring the toolbar

You can adapt the toolbar individually to your needs.

Notice!
Do not use any special characters, for example **&**, in the password.
Special characters are not supported for the password and can prevent you from being able to access the program.

To adapt the toolbar to your requirements:

1. On the toolbar, click the **Preferences** tab, expand **Applications** in the tree structure, click Configuration Manager, then click the **Appearance** tab
2. In the **Toolbar** group, click **Edit...**. The **Toolbar Settings** dialog box is displayed.
3. Select an entry and click one of the arrow buttons to move the entry.
   You can move an entry from the **Available actions** list to the **Showed actions** list or vice versa.
   You can move an entry in the **Showed actions** list up and down.
4. Click **Apply** to adopt the changes and make further changes.
5. If necessary, click **Default** to restore the original settings.
6. Click **OK**.

6.12 Obtaining device information

Configuration Manager gives you easy access to all devices in the network and you can quickly obtain all the information you need for each individual device in a clear format.

To obtain device information:

1. On the toolbar, click the **Devices** or **My Devices** tab.
2. Right-click a device, then click **Device Info...** . The hardware, configuration and connection information are displayed.

Additional options:

– The info bar above the view pane shows the name, device type and IP address. For hardware devices, it also gives information on the processor load, network connection and recording status.
– The tabs in the view pane show all the available configuration settings (comparable with the Web browser view for the relevant device).

6.13 Disabling network scan

If you do not want to use the automatic network scan, you can disable it. Note that in this case the status of the devices will not be checked regularly.
Regardless of the default setting, you can trigger a network scan manually at any time.
To disable the automatic network scan:

1. On the toolbar, click the **Preferences** tab, expand **Applications** in the tree structure, click Configuration Manager, then click the **Network Scan** tab.
2. In the **Network Scan** group, click to clear the **Run continuous network scan**.

To trigger a network scan manually:

1. On the toolbar, click the **Devices** tab.
2. Click the **Reload page** icon.

6.14 Working with Video Client

Configuration Manager is indispensable when working with Video Client, as it allocates those devices to the system to which Video Client is to have access.
This is where you can change the default settings for Video Client.

Notice!
Do not use any special characters, for example **&**, in the password.
Special characters are not supported for the password and can prevent you from being able to access the program.

Note: If you define a password for the user `administrator`, this must be entered every time the database is opened.

6.14.1 Creating users and user rights

To create users and define user rights:

1. On the toolbar, click the **Preferences** tab, expand **Applications** in the tree structure, click Video Client, then click the **User Management** tab.
2. To create an additional user, in the **Users** group, click **Add...**. The **User** dialog box is displayed.
3. Enter the user name and password.
4. To define individual user rights, under **Rights**, select the relevant check boxes.
   Playback recordings
   The user can replay recordings in Video Client
   Export recordings
   The user can export recordings in Video Client
   Delete recordings
   The user can delete recordings in Video Client
   Allow text display
   The user can view data from ATM/POS devices
   Close application
   The user can close the Video Clientapplication
   Exit full-screen mode
   The user can exit full-screen mode in Video Client
   Allow workstation recording
   The user can record on the local workstation.
5. To remove a user, select an entry in the list of created users and click **Remove**.

6.14.2 Selecting components

To select components:

1. On the toolbar, click the **Preferences** tab, expand **Applications** in the tree structure, click Video Client, click the **Cameras**/**Alarm Outputs** tab, then click the relevant **Order** tab.
2. Select the components to be listed in Video Client.
   The sort order of these lists matches that in Video Client.
3. Click the **Top**, **Up**, **Down** and **Bottom** buttons to change the position of a selected component within the list.

6.14.3 Specifying access rights

You can specify different access rights for each user.

To specify access rights:

1. On the toolbar, click the **Preferences** tab, expand **Applications** in the tree structure, then click Video Client.
2. Click the **Cameras**, **Digital Inputs** or **Alarm Outputs** tab, then click the relevant **Access** tab (**Camera Access**, **Digital Input Access**, or **Output Access**).
   - To change the access rights for a single device:
     Left-click the relevant colored table cell until the desired authorization level is selected.
   - To assign the access rights for all components (or vice versa):
     Right-click the header of the colored column or row header and select the desired access right.

Camera Access rights

PTZ configuration

The user can configure the PTZ settings.

PTZ control

The user can control the camera.

View only

The user can display video.

Access denied

The user has no access to the camera.

Digital Input Access / Output Access rights

Control allowed

The user can control the component.

View only

The user can display the component.

Access denied

The user has no access to the component.

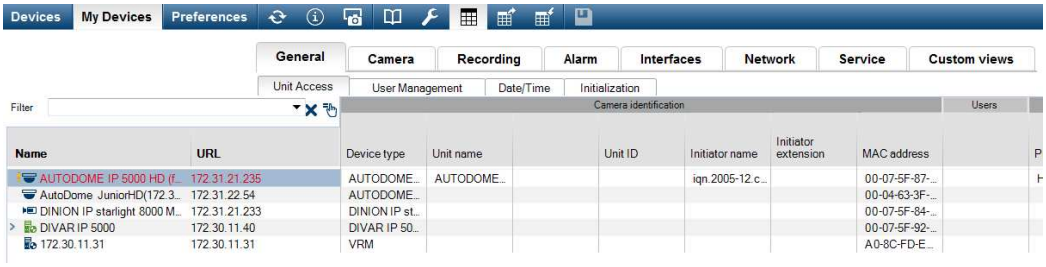
6.15 Using the Table view

The table view provides the option of presenting a summary of specific settings for individually selected devices in the form of a clearly arranged table.

The content of all main tabs and sub-tabs can be exported in **.csv* format.

To open the table view:

1. On the toolbar, click the **Devices** or **My Devices** tab, then click the **Table view** icon.
   The **Table View** window is displayed. The table contains a column to the left with all devices and cameras.
   In the view pane to the right, all well-known main tabs (for example, **General**, **Camera:**, etc.) and sub-tabs (for example, **Unit Access**, **Date/Time**, etc.) are displayed.

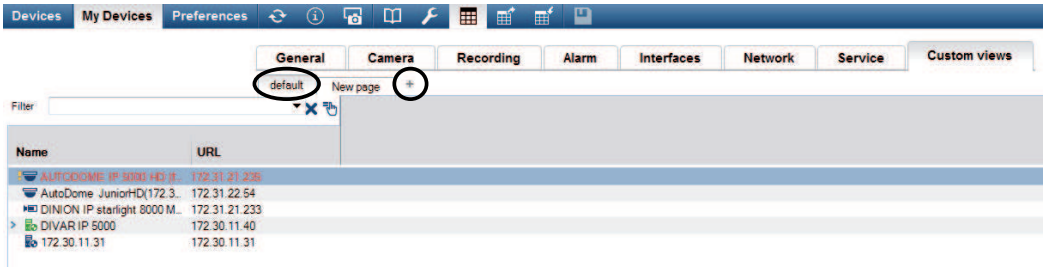


2. If necessary, minimize the amount of displayed devices and cameras as follows:
   – Select the desired cameras, then click the **Show the selected only/all** icon.
   or
   – In the **Filter** dialog box, enter an appropriate filter. To delete the filter, click the icon.

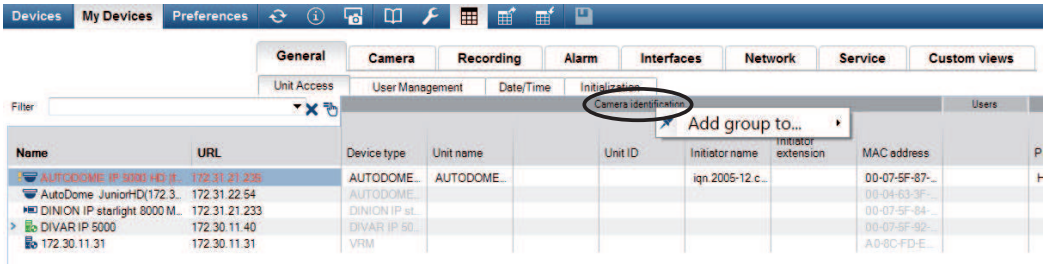
In table view you can also define your own custom views.
To define a custom view:

1. On the toolbar, click the **Devices** or **My Devices** tab, then select one or more devices or cameras in the tree structure.

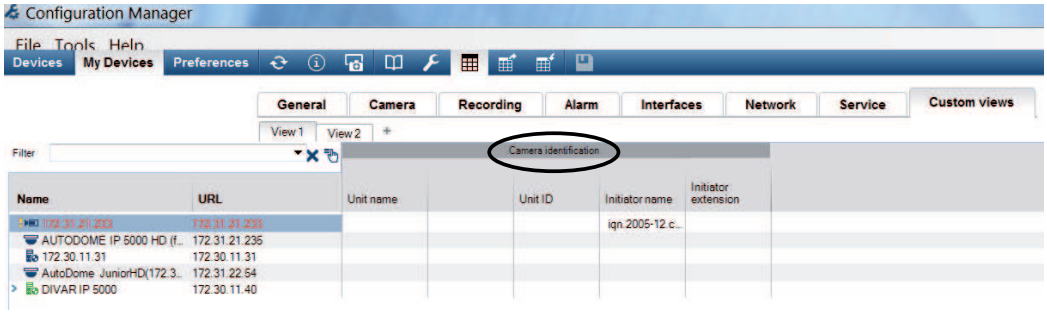
2. On the toolbar, click the **Table view** icon.
   The **Table View** window with all devices is displayed. And also the **default** sub-tab where you can add your first view with specific parameters.
   To rename the **default** tab, double-click the tab, then enter an appropriate name.
   To add further views, click the **+** sign. A **New page** tab for the next view is displayed.



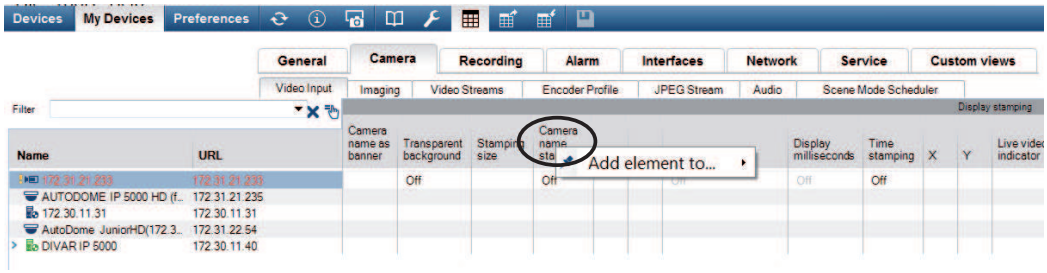
3. Add groups to your custom view as follows:
   Select a device, then click one of the main tabs and a sub-tab (for example, **General** > **Unit Access**).
   Right-click a group (for example, **Camera identification**), then click **Add group to...**, and select the view the group should appear.



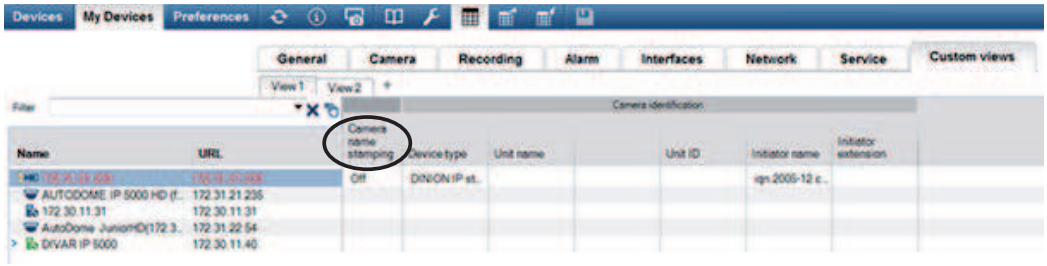
Note: A new column **Camera identification** group is added to your custom view.



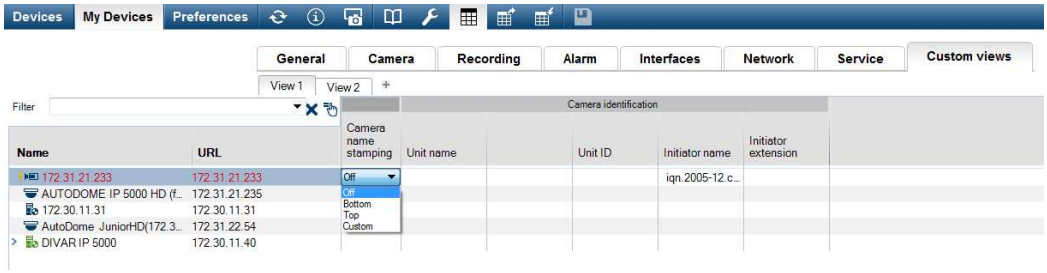
4. Add elements to your custom view as follows:
   Select a device, then click one of the main tabs and a sub-tab (for example, **Camera:** > **Video Input**).
   Right-click an element (for example, **Camera name stamping**), then click **Add element to**... and select the view the element should appear.



Note: A new column **Camera name stamping** element is added to your custom view.



5. Add more columns to the custom view in this way
   Note: Not all groups or elements can be added to the custom view.
6. If necessary, add more devices or cameras to the table.
7. In custom view, click a field in the table. You can set parameters for individual devices or cameras directly from here.



Toolbar icons in the Table View

See *Toolbar icons, page 19*

Additional options in the Table View

– Sorting the table:
  Click a column header to sort the table.

- Device commands:
  Right-click one of the devices.
- Removing a column:
  Right-click a column header, then click **Remove...**.

6.16 Importing .csv files

The Configuration Manager program allows you to import .csv files with additional attributes. The .csv file must at least contain:

- A headline with column definitions
- 1°line with a device

The headline of the .csv file defines the mapping of the columns to the artefacts in the Configuration Manager program. Information above the headline will be ignored during import. Possible values are:

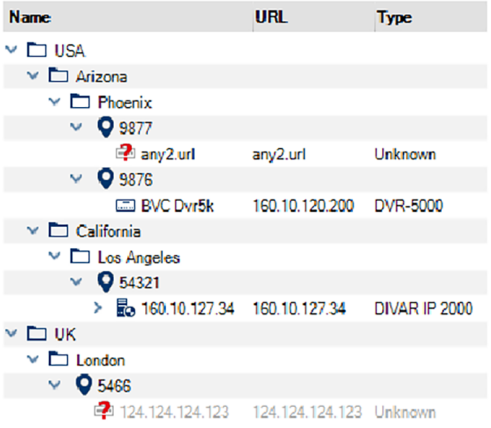
- Level: Creates a folder. If folder is already present, no folder will be created. Level may appear several times to create folder-structures.
- Site: Creates a folder, that is flagged as site. This is only allowed to appear once per line.
- Attribute (name): Defines an attribute column with the attribute name in brackets.
- ConnectionString: Creates a device by connecting to the URI specified.
- DeviceName: Name of the device.
- User: Username for authentication.
- Password: User password for authentication.

To import a .csv file:

1. On the toolbar, click the **Devices** or **My Devices** tab. The **Import Data** dialog box is displayed.
2. Click **Browse**, then select the .csv file you want to import.
   Example: .csv import file

```
1 This is a sample-file for CSV-Import;;;;;;;;
2 Version;1.0;;;;;;;;
3 Date;23.05.2014;;;;;;;;
4 Level;Level;Level;Attribute(ZIP);Site;Attribute(Manager);DeviceName;ConnectionString;User;Password
5 USA;California;Los Angeles;12345;54321;John Doe;Store LA;http://160.10.127.34;srvadmin;123456
6 USA;Arizona;Phoenix;54321;9876;Mike Paso;Store Phoenix;http://160.10.120.200;ADMINISTRATOR;000000
7 USA;Arizona;Phoenix;54322;9877;Mike Paso;Store Outer-Phoenix;http://any2.url;admin;admin
8 UK;;London;1111;5466;Charlotte Jose;Store London;bvms://124.124.124.123;admin;Admin
```

3. Click **OK**. The content of the .csv file is displayed in a device list.
   Example: Imported .csv file



Notice!
The attributes can be used to search for such data in the device tree. Use the **Filter** functionality.

To display attributes imported with the .csv file:

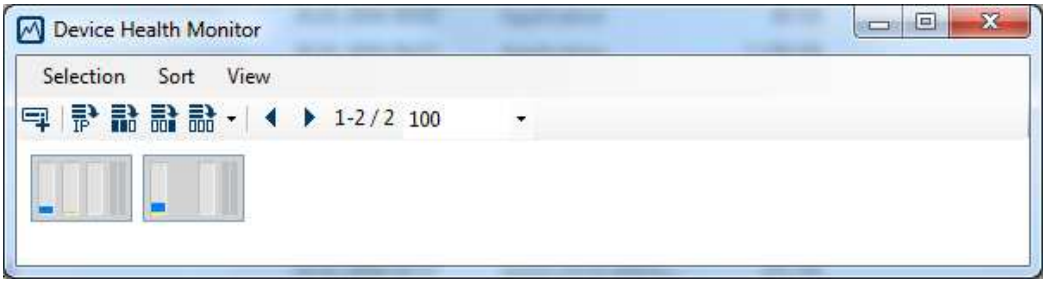
1. On the toolbar, click the **Devices** or **My Devices** tab.
2. Right-click a device, then click **Device Info...**.

6.17 Using Device Health Monitor

The device health monitor displays a dialog box containing status information for selected devices, which would otherwise be viewed via the icons on the right edge of the info bar.

To display status information:

1. On the toolbar, click the **Devices** or **My Devices** tab, then select one or more devices or cameras in the tree structure.
2. In the **Tools** menu, click **Device Health Monitor...**.
   The **Device Health Monitor** dialog box is displayed.
3. In the menu bar, click **Selection**
   or
   On the toolbar, click .
   For each device selected, the quick indication icons from the info bar are displayed.



4. Place the pointer on the icons to view details on the processor load, network connection and recording status:
5. To display information for other devices, change the selection in the main tab and click **Selection** in the dialog box.
6. To reorganize the display, click **Sort** and select the category by which to sort.
   A second click reverses the sort order.
7. In the **View** menu, click **Show Icon Bar** to display a toolbar providing quick access to the various menu options.

Quick indication icon description

- The left icon indicates the proportions of the individual functions on the encoder load, shown as percentages. For devices with two processors, a separate icon is shown for each processor.
- The icon in the middle indicates the network connection type and the speed of the outgoing (UL = Uplink) and incoming (DL = Downlink) data traffic.
- The right icon indicates information on the recording status.
  - Green: active recording
  - Red: error
  - Orange: recording scheduler active, no current recordings
  - Gray: recording scheduler not active, no current recordings

6.18 Device configuration using the View pane

The View pane for the **Devices** and **My Devices** tabs shows a series of tabs, the number and content of which depend on the device selected in the tree structure.
The tabs can be used to make the configuration settings that the device also provides in the Web browser view, some of them with a slightly different composition.
Due to the large number of possible settings, not all of the details are dealt with here. Below are just a few examples of the configuration options:

- Display stamping (camera name, time stamp) on or off

– Creation of encoder profiles
– Configuration of output to an analog monitor (decoder)
– Alarm configuration
– Planning local recordings
  etc.

Detailed information about the configuration options for a device can be found in the relevant device documentation and the online Help in the relevant Web browser view.

To make changes in the View pane:

1. On the toolbar, click the **Devices** or **My Devices** tab, then select the device in the tree structure.
2. In the View pane on the right, click the tab for the area you want to edit.
3. Make the desired changes.
4. On the toolbar, click the **Save** icon to save the new settings.
5. Continue with the settings in the other tabs.

Some settings (for example, **Device time**) can only be changed if the device is not currently recording. If necessary, stop any recordings before making changes.

6.19 Managing certificates using MicroCA

6.19.1 Background information

The Configuration Manager MicroCA functionality facilitates the management of small to medium systems deploying certificate device authentication and certificate-based user authentication.

Each certificate consists of the following parts:

– A publicly available certificate with the public key
– A corresponding private key

For highest level of security, the private key must be concealed in hardware, a physical key store, typically performed by a Trusted Platform Module (TPM) chip. For this purpose, Bosch cameras include a TPM chip. Use a USB or smart card crypto token for MicroCA use to guarantee exclusive ownership.

For test purposes, or in case of low expectations on measures against stolen keys, you may also store the private key and certificate on a standard USB flash stick as PKCS12 file.

Notice!

Weak protection by PKCS12 implementations

Malware on the PC may create an unnoticed copy and crack the PIN due to weak encryption of most PKCS12 implementations. Never use PKCS12 implementations in security-critical applications.

Very high protection through certificate-based authentication

Certificate based authentication allows you to create closed systems with very high protection against malicious access. This certification mechanism allows you to set up distributed camera systems that reach security level 3 of FIPS-140-2 standard.

However, note that before the initial creation of certificates on the devices no technical means can hinder so-called man in the middle attacks. Preferably use a secure environment to roll-out the initial certificates to your devices.

6.19.2 Initializing the MicroCA

The MicroCA functionality in the Configuration Manager program is an easy-to-use tiny certificate authority (CA).

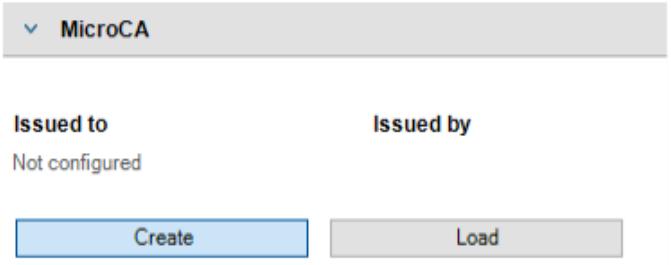
After the CA certificate is created, it can be immediately used for signing other certificates.

When using a file-based CA certificate make sure to store it on a USB flash stick kept in a safe place. We also recommend that you create a security copy to reduce the risk of losing your CA certificate.
Preferably, use a USB token or smart card. Check the release notes for a list of supported crypto hardware.

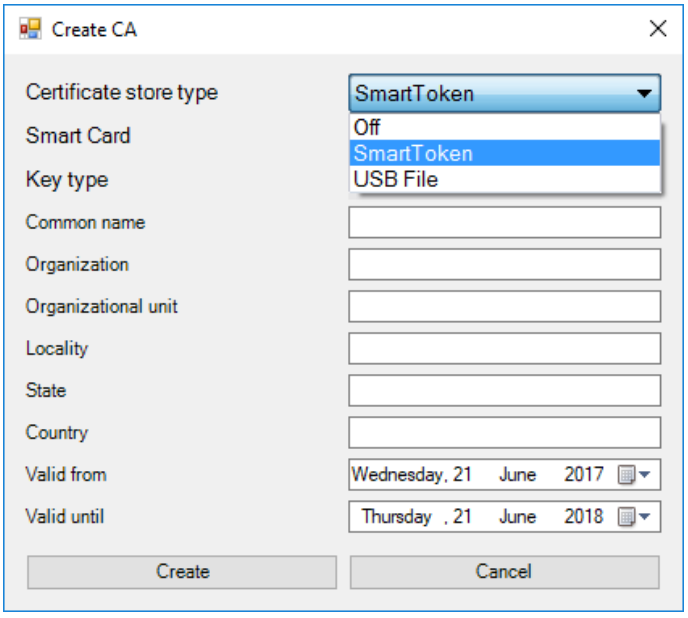
6.19.3 Configuring MicroCA using Smart Token

To create a Smart Token:

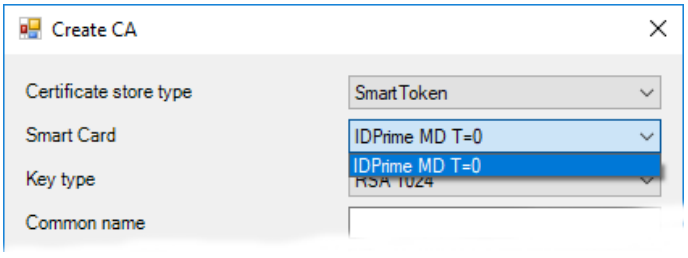
1. In Configuration Manager program, navigate to **Preferences** > **Applications** > Configuration Manager.
2. Click the **Security** tab.



3. Click **Create**. The **Create CA** dialog box is displayed.
4. In the **Certificate store type** list, click **Smart Token**.

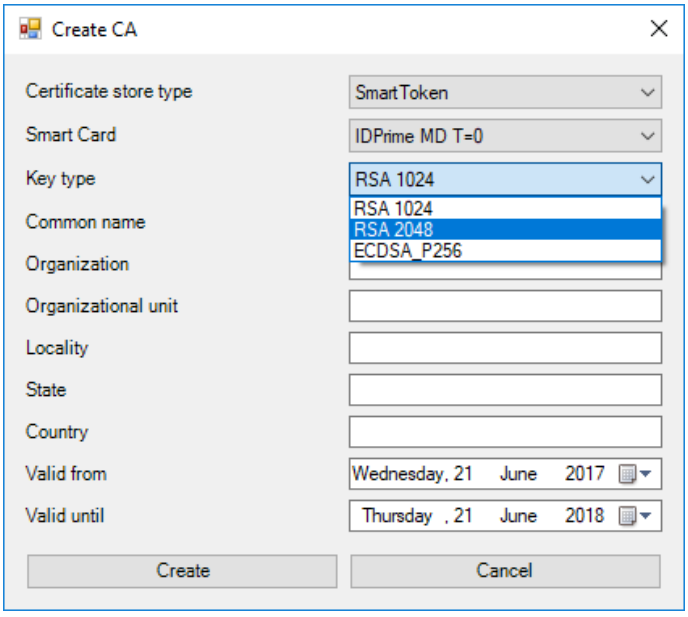


5. In the **Smart Card** list, select the smart card type.

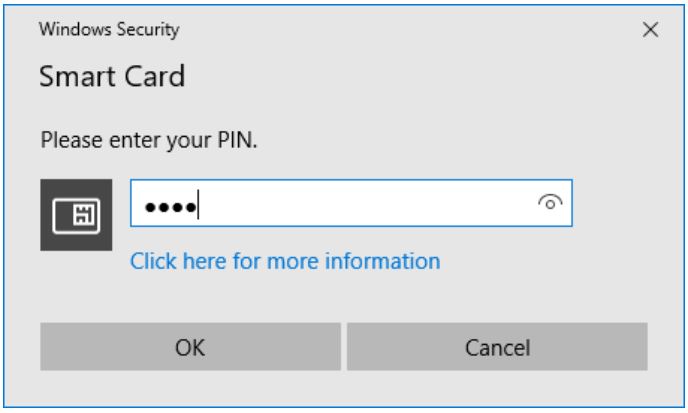


6. In the **Key type** list, select an entry.
   The list contains different key sizes and two different key types: the classical RSA type and the ECDSA type, a so-called Diffie-Hellman exchange type. While RSA is much more

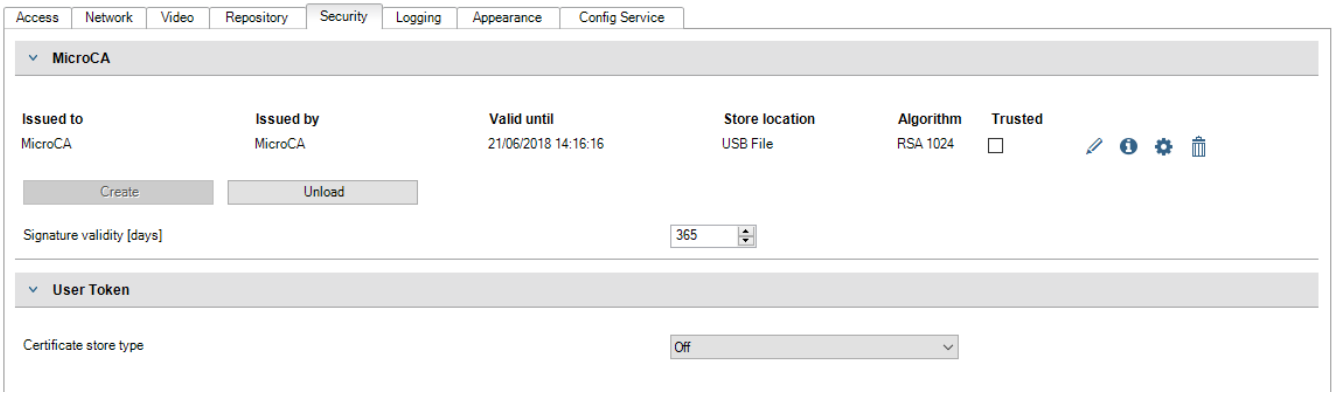
common, Diffie-Hellman has lower computational overhead. Although mixing both types on different tokens is possible, we recommend that you use the same type for all tokens.
Note: Higher numbers reflect higher levels of security. For example, RSA 2048 is more secure than RSA 1024, but requires more computation time.



7. In the **Common name** box, enter a meaningful name for the new Certificate Authority.
8. Fill out the **Organization**, **Organization unit**, **Locality**, **State** and **Country** boxes. In larger installations, this information will help you to identify the authority.
9. In the **Valid from** and **Valid until** lists, click the desired start and end date.
   Note: Since the MicroCA functionality has no provisions to prolong validity, make sure that you select an appropriate period of time.
10. Click **Create**. The **Windows Security** dialog box is displayed.
11. Type the smart card PIN to be authorized using the private key including self-signing.
    A new Certificate Authority is displayed in the **MicroCA** list.



12. In the **MicroCA** list entry, click the **Trusted** check box. A **Security Warning** message is displayed that you are about to install a certificate from a certificate authority claiming to represent MicroCA.
    Note: The **Trusted** check box facilitates to add MicroCA to the Windows **Trusted Certificates** list.
    Applications, for example the Chrome browser, identifies the certificate as valid.

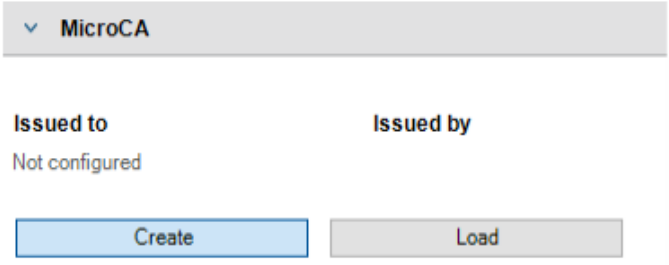


13. To confirm, click **Yes**.

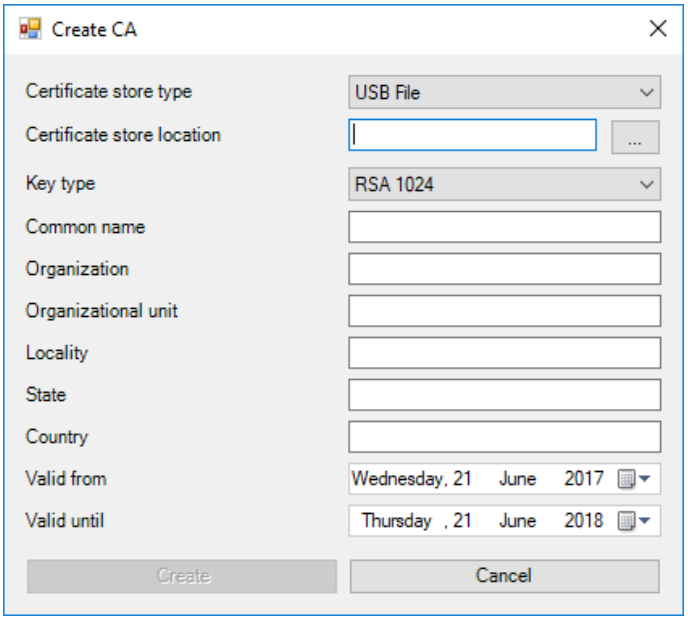
6.19.4 Configuring MicroCA using USB file

To create a USB file:

1. In Configuration Manager program, navigate to **Preferences** > **Applications** > Configuration Manager.
2. Click the **Security** tab.

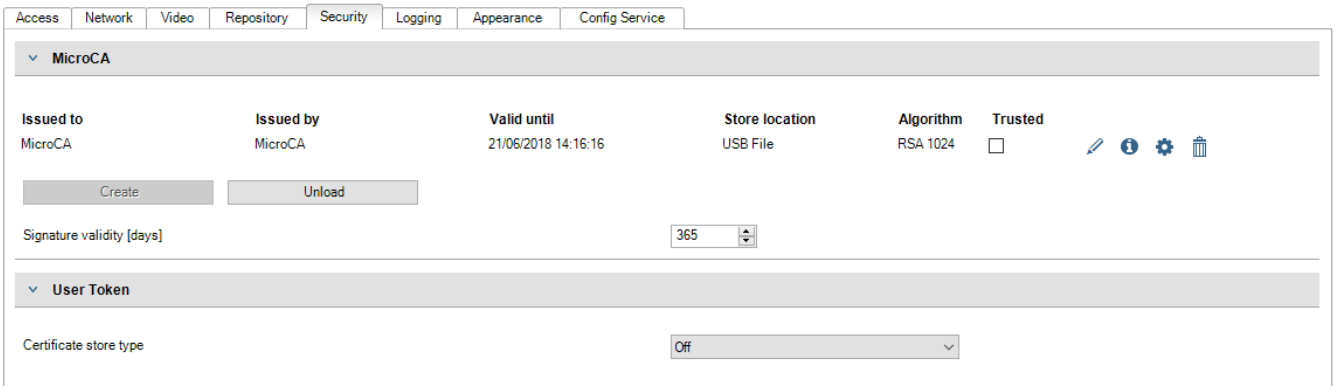


3. Click **Create**. The **Create CA** dialog box is displayed.
4. In the **Certificate store type** list, click **USB File**.



1. Insert a USB stick into your system, click the icon ... to the right of the **Certificate store location** box, then select a storage location.

2. In the **Key type** list, select an entry.
   The list contains different key sizes and two different key types: the classical RSA type and the ECDSA type, a so-called Diffie-Hellman exchange type. While RSA is much more common, Diffie-Hellman has lower computational overhead. Although mixing both types on different tokens is possible, we recommend that you use the same type for all tokens.
   Note: Higher numbers reflect higher levels of security. For example, RSA 2048 is more secure than RSA 1024, but requires more computation time.
3. In the **Common name** box, enter a meaningful name for the new Certificate Authority.
4. Fill out the **Organization**, **Organization unit**, **Locality**, **State** and **Country** boxes. In larger installations, this information will help you to identify the authority.
5. In the **Valid from** and **Valid until** lists, click the desired start and end date.
   Note: Since the MicroCA functionality has no provisions to prolong validity, make sure that you select an appropriate period of time.
6. Click **Create** to open the **Generate Certificate** dialog box.
7. To confirm creating a new certificate, click **OK**. A **Password** dialog box is displayed.
8. Type a new password. While you type, the **Password** dialog box will change its color from red (very weak password) to yellow (weak password) and to green (very strong password). Use a combination of characters, digits, and special characters to achieve a very strong password.
9. In the **Confirm** box, type the same password.
10. To create the certificate, click **OK**. A new Certificate Authority is displayed in the **MicroCA** list.

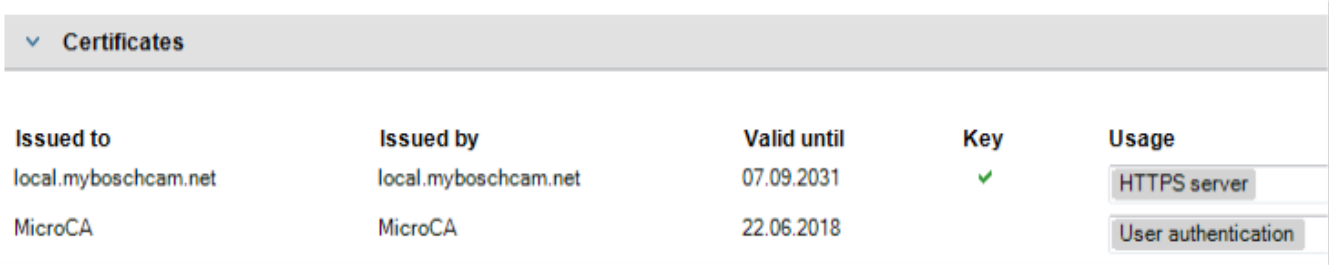


6.19.5 Signing device certificates

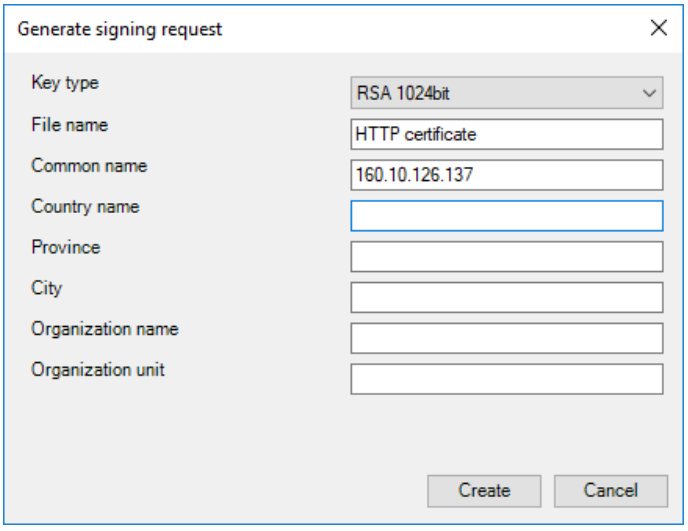
One of the main purposes of the MicroCA functionality is to deploy certificates to devices. To achieve this, you will replace a self-signed certificate by a MicroCA signed certificate. For signing, you will need your MicroCA crypto token or USB drive, and you need to enter the MicroCA PIN to authorize its use.
In order to secure device access by using certificates you need to change the devices authentication mode.
To sign device certificates:

1. In the Configuration Manager program, click the **Devices** or **My Devices** tab, then click the desired device.
2. Click the **General** tab, then click the **Unit Access** tab.
3. In the **Allowed authentication modes** group, click the upload icon .
   A message box will inform you that MicroCA certificate is active on your system and that you can upload the MicroCA certificate.

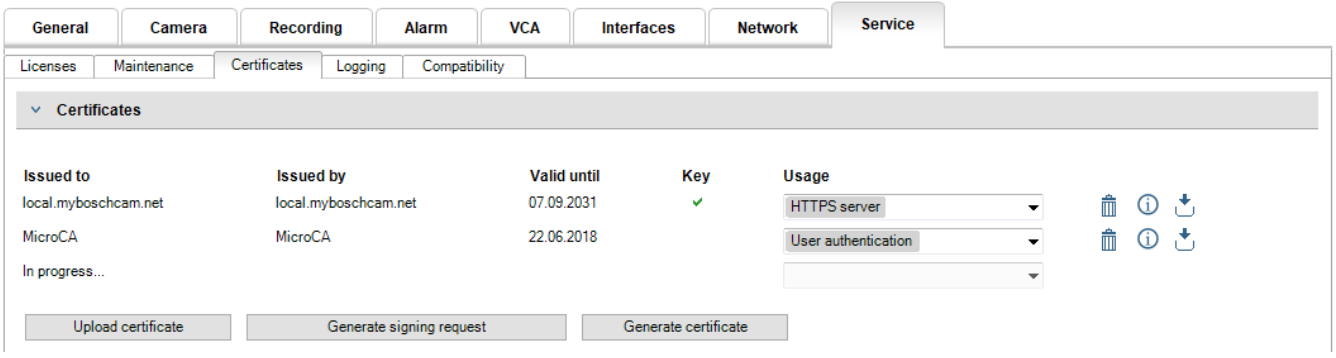
4. Click **Yes** to start certificate-based authentication on the device.
   After successfully uploading the MicroCA certificate, the device needs a restart in order to engage certificate handling.
5. Confirm the restart by clicking **Yes** when the message box appears.
6. Wait for the device to be online again. In order to verify the successful switching to certificate based authentication, click the **Service** tab, then click the **Certificates** tab of the device. You will find a MicroCA certificate similar to the one shown here:



7. To create a signing request, click **Generate signing request**. The **Generate signing request** dialog box is displayed.

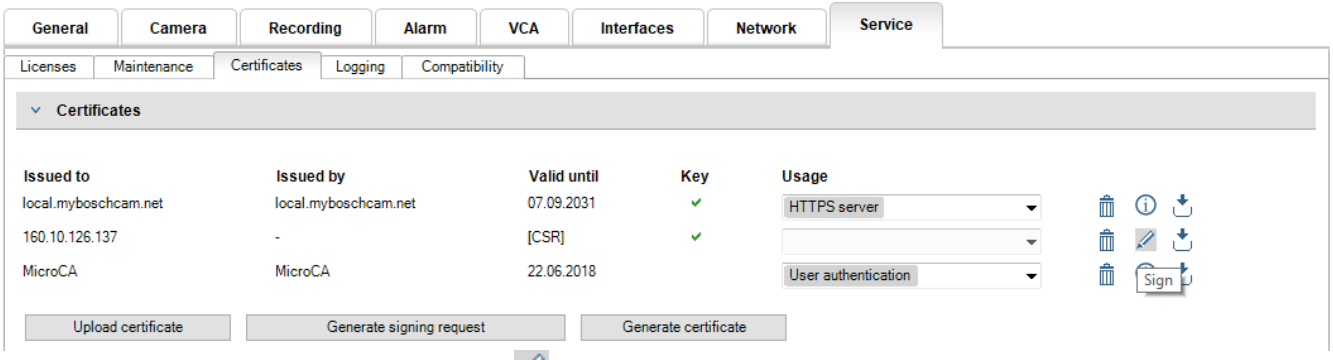


8. In the **Common name** box, the IP address of the device is displayed. Do not change this!
9. The remaining boxes are filled from the MicroCA certificate and can be adapted according to your needs.
10. Click **Create**.
    Note: Creating the certificate request may take some time due to the key creation process.

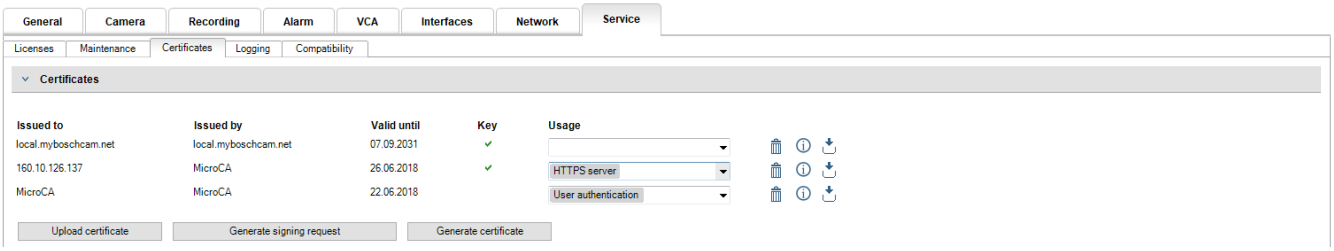


11. To sign and upload the certificate, click the reload icon or press **F5** to update until the line shows a valid signing request.

    Note: The sign icon is available after the MicroCA has been configured. The sign icon allows you to sign and upload the signed certificate in a single step.



12. Click the sign icon to the right of the certificate's list entry. You may be asked to insert your smart card and/or to type your PIN to authorize the action.
13. After the certificate is signed, in the **Usage** column switch to **HTTPS server**:



14. Restart the device. After the restart, the newly created signed certificate will apply as a TLS communication encryption certificate.

6.19.6 Managing user token

A user token - also known as security token - is a physical device which can be used to gain access to an electronically secured computer. A user token can be used as a replacement for, or in addition to a password. MicroCA certificate uses smart cards or (crypto-) USB sticks as the token hardware.

The user token contains a private key which will be tested against the public key of the MicroCA certificate. Only if this test is successful, access to the device or to the video software will be granted.

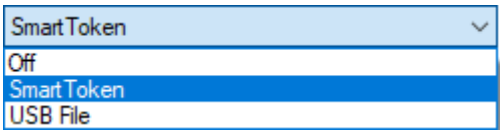
Smart cards are well-known devices for user authentication, although in principle you may deploy any other certificate technology for this purpose.

To manage tokens:

1. In Configuration Manager program, navigate to **Preferences** > **Applications** > Configuration Manager. Then, click the **Security** tab.

   The **User Token** group allows you to inspect existing tokens. Smart tokens and PKCS12 files on USB sticks are supported.

   Note: To display a list of existing tokens known to your system, click the **Certificate store type** list.



2. In the **Certificate store type** list, click the corresponding entry.

3. Select a certificate. For the following reasons, more than one certificate can be displayed in the list:
   – You have inserted multiple different tokens into your system.
   – A single token contains multiple certificates.

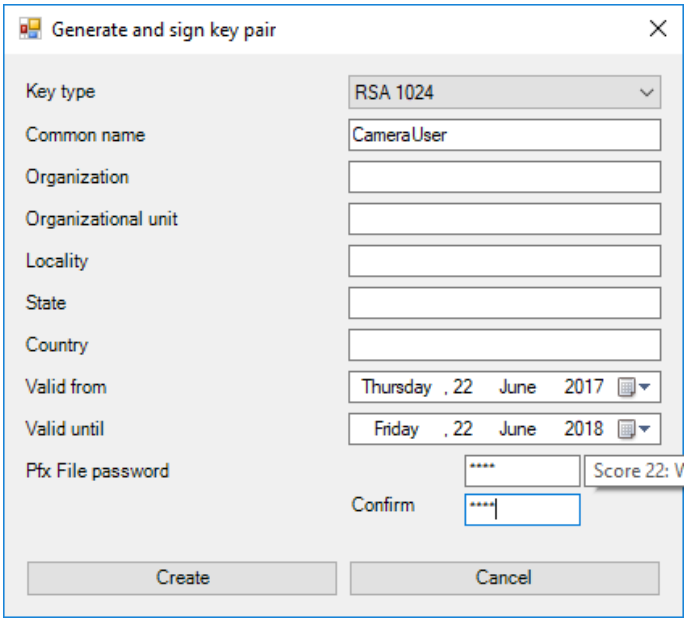
For each certificate two functions are available:
– Showing detailed certificate information
– Deleting the certificate from the token

Notice!
Use caution when deleting token information. You cannot recover the token information.

6.19.7 Creating user token

User token creation is similar to certificate creation.
To create user token:

1. In Configuration Manager program, navigate to **Preferences** > **Applications** > Configuration Manager. Then, click the **Security** tab.
2. Insert a smart card, and in the **Certificate store type** list, click **Smart Token** and select the smart card.
   or
   Click **USB File** and enter a path and a new file name.
3. Click **Create**. The **Generate and sign key pair** dialog box is displayed.
4. In the **Common name** box, enter a meaningful name for the new Certificate Authority.
5. Fill out the **Organization**, **Organization unit**, **Locality**, **State** and **Country** boxes. In larger installations, this information will help you to identify the authority.
6. In the **Valid from** and **Valid until** lists, click the desired start and end date.
   Note: Since the MicroCA functionality has no provisions to prolong validity, make sure that you select an appropriate period of time.



7. To submit, click **Create**.
   Note: To allow the creation of a valid user token, the system needs access to the CA certificate. Insert a smart card with a valid CA certificate and authorize its use by entering the CA PIN and the user token pin.

6.19.8 Configuring token-based device authentication

To configure token-based device authentication you must add the user to the device's list of users.

To add the user to the device's list of users:

1. In the Configuration Manager program, click the **Devices** or **My Devices** tab, then click the desired device.
2. Click the **General** tab, then click the **Unit Access** tab.
3. In the **Users** group, click **Add user**. The **Add User** dialog box is displayed.
4. In the **Type** list, click **Certificate**.
5. In the **Group** list, click the appropriate entry to specify the user's role.
6. In the **User name** box, enter the name of the user.
   Note: The name must be the identical to the name you entered in the **Common name** box when creating the user token.
7. Click **Create**.
8. Activate the new authentication mode. To do this, in the **Allowed authentication modes** group, click the **Certificate** check box.
   Note: A green check mark indicates that the new authentication mode is active.

6.20 Finding/editing DSA E-Series devices

Configuration Manager allows you to find DSA E-Series devices and to edit certain settings of these devices.

6.20.1 Finding DSA E-Series devices

To find DSA E-Series devices:

1. On the **Tools** menu, click **DSA E-Series Discovery...**.
   The **DSA E-Series Discovery...** dialog box with all DSA E-Series devices is displayed.

6.20.2 Editing the port settings

To edit the port settings of DSA E-Series devices:

1. On the **Tools** menu, click **DSA E-Series Discovery...**.
   The **DSA E-Series Discovery...** dialog box with all DSA E-Series devices is displayed.
2. Select the device, then click **Management Ports...** or **iSCSI Host Ports...**. A dialog box with the port settings is displayed.
3. Change the port settings if necessary.

6.20.3 Changing the password

To change the password of a DSA E-Series device:

1. On the **Tools** menu, click **DSA E-Series Discovery...**.
   The **DSA E-Series Discovery...** dialog box with all DSA E-Series devices is displayed.
2. Select the device, then click **Configuration Password...**.
3. Enter the new password.

6.20.4 Renaming the device

To rename a DSA E-Series device:

1. On the **Tools** menu, click **DSA E-Series Discovery...**.
   The **DSA E-Series Discovery...** dialog box with all DSA E-Series devices is displayed.
2. Select the device, then click **Rename...**.
3. Enter the new name.

6.21 Working with other components

6.21.1 IVA / IVMD

IVA (Intelligent Video Analytics) and IVMD (Intelligent Video Motion Detection) are modules in the device's firmware that may require a license. They are enabled in the **License** tab of the relevant device. IVA and IVMD are set up exclusively using Configuration Manager.

6.21.2 Video Client

Configuration Manager is indispensable when working with Video Client, as it allocates those devices to the system to which Video Client is to have access. In addition, you can use the **Preferences** tab to make basic settings for using Video Client.
Also refer to the separate Video Client documentation.

6.21.3 VRM

If you want to play back recordings managed by Video Recording Manager using Video Client, the devices for which the recordings are available, must be allocated to the system with Configuration Manager. In addition, a connection must be established to the Video Recording Manager server.
Further details can be found in the separate Video Recording Manager documentation.

6.21.4 Monitor Wall

Monitor Wall is treated as a hardware decoder by Configuration Manager. As soon as Monitor Wall is running on a PC with an IP network connection, it is added to the list after the network scan.
You can use Configuration Manager to make various settings, which are explained in more detail in the separate Monitor Wall documentation.

Index

W

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