Dallmeier

REV. 1.0.0 | 2021-10-25

CONFIGURATION

DALLMEIER DEVICE MANAGER

TLS SETUP

ENCRYPT AND SECURE CONNECTIONS FROM CAMERAS,
RECORDERS, AND CLIENTS ON THE NETWORK

MADE IN GERMANY

See more.

TABLE OF CONTENTS

INTRODUCTION

1.1 VALIDITY

This document is valid for the software Dallmeier Device Manager (DDM) in software version 1.0.10.

Illustrations (screenshots) in this document may differ from the actual product.

1.2 DOCUMENTS

The product documentation for the respective software includes various documents that are printed and/or provided in digital form, for example via the website www.dallmeier.com.

Read all product documentation for your software carefully and completely before using it. Always observe the instructions, notes, and warnings contained, as well as the technical data in the currently valid product specification. Keep all printed documents relating to your software in a legible condition and in a suitable location for future reference. Archive digital documents relating to your software (e.g., the technical product specification) on a suitable storage medium. Regularly check the website www.dallmeier.com for possible updates of the product documentation as well as the respective software versions.

1.2.1 This Document

The „Configuration“ document (this document) contains detailed descriptions of the configuration and operation of the software listed above.
The target audience of this document are trained system integrators (installers of video security systems).

1.2.2 Applicable Documents

Product Specification
The product specification contains detailed technical data, performance characteristics and features of the respective software.
The target group of the document are trained system integrators (installers of video security systems).

Technical Information
The „Technical Note“ document contains information on innovations and changes introduced with the respective update of the software version.

1.3 REPRESENTATION CONVENTIONS

Various text formatting and highlighting are used to improve the clarity and readability of this document:

NOTICE

NOTICE indicates measures to prevent damage to the device and/or property due to improper configuration of the device or incorrect operation.

Instructions for action are indicated by arrows (►).

► Carry out instructions for action always in the sequence described.

Expressions highlighted in bold and dark gray usually refer to the name of an application, product, or function, or indicate a control element of the web-based graphical user interface (button, checkbox, drop-down list, menu item, etc.).

Paragraphs in italics provide information on basics, specifics, and efficient procedures, as well as general recommendations.

1.4 LEGAL NOTICES

Observe the legal notices listed below concerning the product described in this document and/or its underlying software:

- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
- This product includes software written by Tim Hudson (tjh@cryptsoft.com).
- This software is based in part on the work of the Independent JPEG Group.

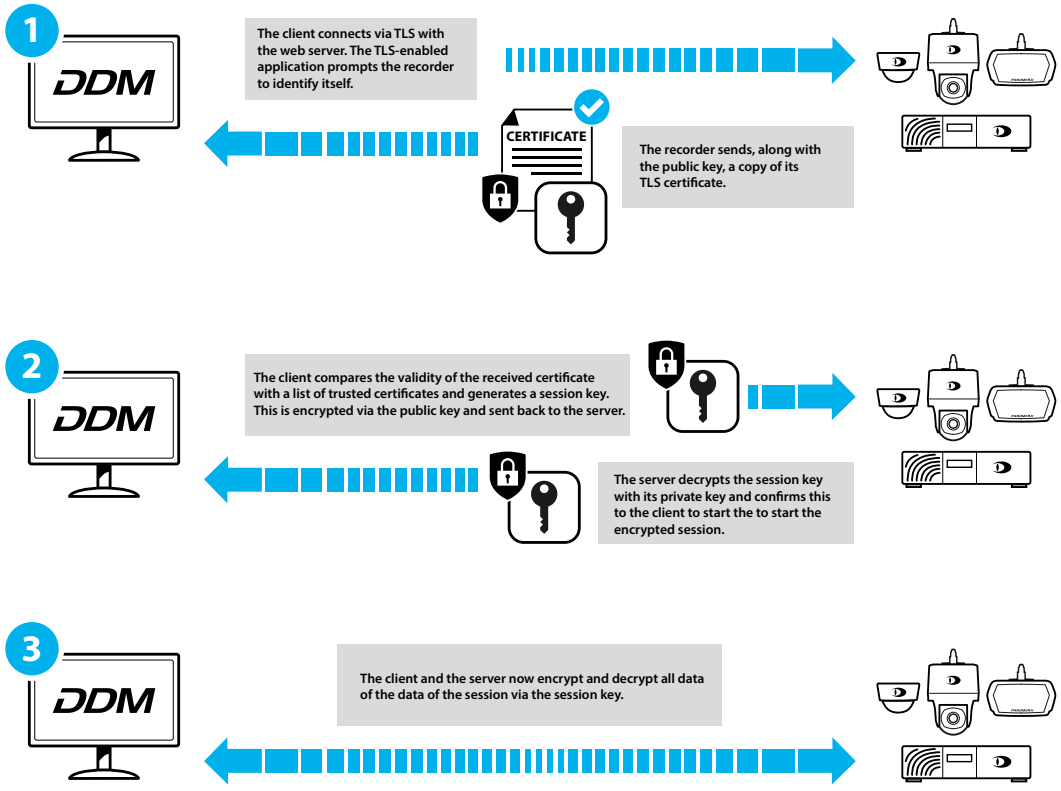
In this context, also read and observe the license texts provided in the information dialog of your device about any other third-party software components used on your device.

GENERAL NOTES

2.1 APPROPRIATE USE

Dallmeier Device Manager (DDM) is a powerful application for the convenient configuration and administration of extensive Dallmeier VideoIP systems. DDM scans the video network for Dallmeier devices, detects them automatically and provides them in an overview. Thus, cameras as well as recording systems can be conveniently managed. The extensive functions range from changing IP addresses to updates of the integrated software to directly opening the configuration dialogs.

Furthermore, the current version of DDM provides all tools to encrypt the network communication between Dallmeier recording systems, cameras and workstation clients using Transport Layer Security (TLS). TLS is a mechanism for encrypting data that is sent or received over the network. The encryption is intended to protect the transmitted data from unauthorized access by third parties and from manipulation or forgery.



The process of establishing a TLS connection consists of the following individual steps in simplified form. In the first step of the connection setup, the server identifies itself to the client with its certificate. The client validates the trustworthiness of the certificate and checks, among other things, whether the server name matches the server name of the certificate. Optionally, the client can identify itself to the server with a certificate. In the final step, the two communication partners derive a session key using the server's public key.

2.2 ADDITIONAL FEATURES AND FUNCTIONS

- Compatible with all Dallmeier recording systems
- Compatible with all Panomera® Multifocal sensor systems
- Compatible with all Dallmeier network cameras
- Independent definition of virtual systems
- Definition of camera groups in a system
- Setting IP addresses
- Implementation of updates

2.3 WARRANTY

The General Terms and Conditions (GTC) valid at the time of conclusion of the contract shall apply.

TLS CONFIGURATION

The Dallmeier Device Manager (DDM) provides all necessary tools to encrypt network connections of Dallmeier devices (cameras, recorders, workstation clients) via the standard Transport Layer Security (TLS) protocol and to manage the required certificates.

3.1 RECOMMENDED PROCEDURE

The following sequence of installation steps and procedures is recommended when setting up TLS connections in a network:

1. Create a self-signed root certificate with the Dallmeier Device Manager and set up a certificate authority (CA) in DDM with it.
2. Now create signing requests for cameras, have them signed by the DDM CA, and upload the resulting certificates to the cameras.
3. Import the root certificate created in point 1 to your recording systems.
4. Enable ports for encrypted network services in cameras (HTTPS 443, DaVid-TLS 29999) and recording systems (DaVid-TLS 29999).
5. Switch the connection to the devices to TLS.
6. Finally, after successfully establishing the TLS connections, you can disable the ports (HTTP 80, DaVid 30000) for unencrypted connection communication in cameras and recording systems.

NOTICE

Note that after disabling ports 80 (HTTP) and 30000 (DaVid), devices may become unreachable over the network if the connection over TLS ports was not set up properly before.

- Disable ports 80 and 30000 on devices only after you have successfully established connections over ports 443 (HTTPS) and 29999 (DaVid-TLS) to those devices.

3.2 OVERVIEW

DDM provides various tools to import root certificates, create self-signed certificates or manage certificates on network devices.

3.2.1 TLS Tools

The **TLS Tools** menu offers the possibility to display the certificate store on the own workstation and to view the existing certificates. The certificate store is available via the menu in the normal Windows view or in the style of the DDM user interface.

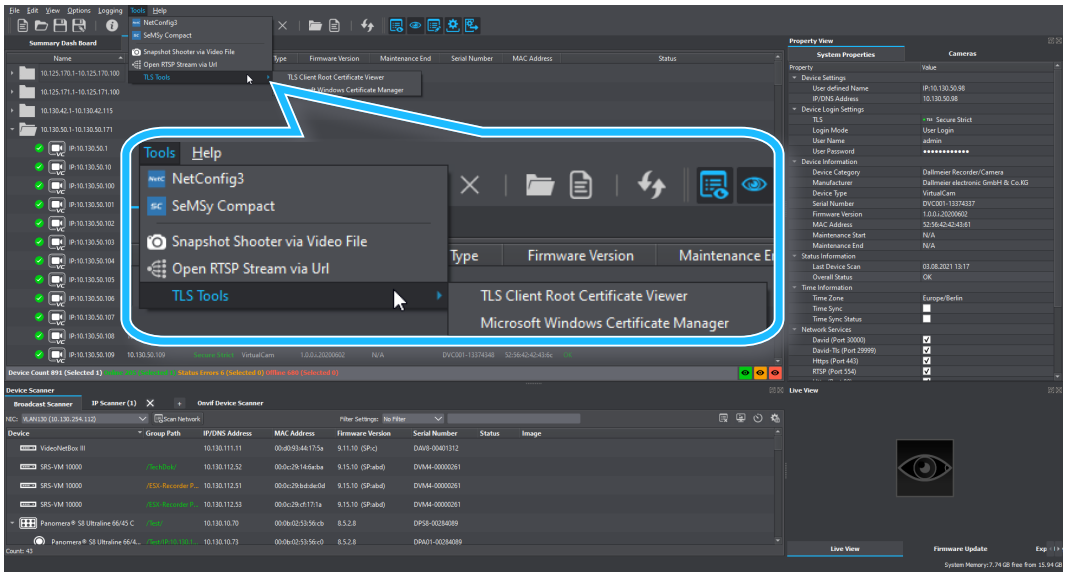


Fig. 3-1

- Open the **TLS Tools** menu via **Tools**.
- Select the option that suits your purposes:

- **TLS Client Root Certificate Viewer**
  Clear display of all certificates in the certificate store with search and sort function

- **Microsoft Windows Certificate Manager**
  Windows certificate manager for displaying the certificates in the certificate store with search, sort and edit functions (e.g. delete, copy)

3.2.2 TLS Configuration and Management

In the network settings for a device, you will find the options for a TLS configuration and for certificate management.

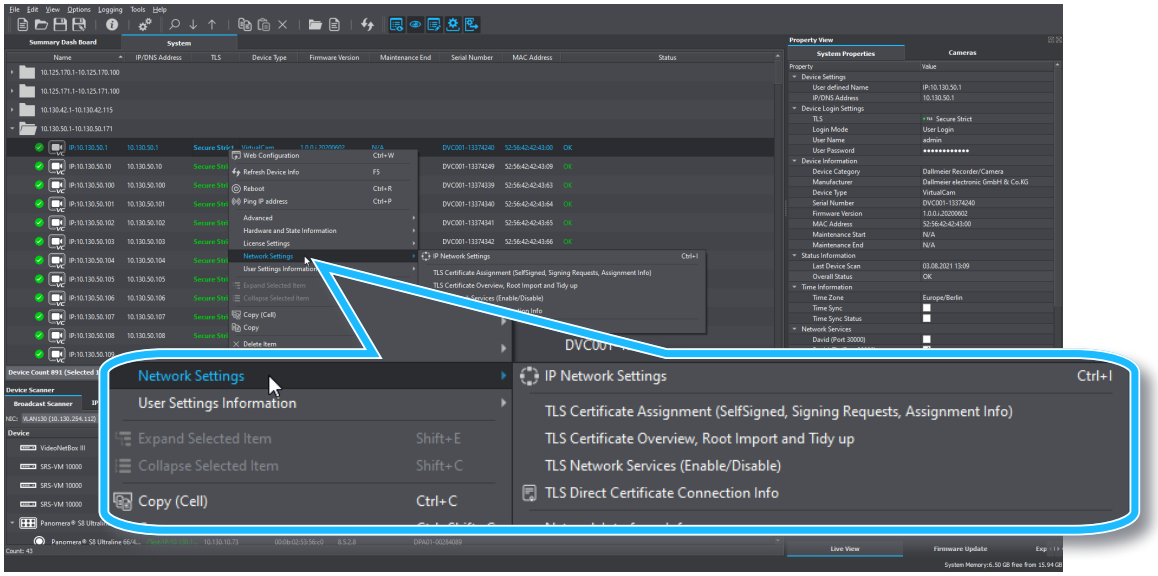


Fig. 3-2

- Select a device from the **System** list.
- Right-click to display the context menu.
- Select **Network Settings** to display the submenu.
- Open the TLS option you want to operate with:

- **TLS Certificate Assignment**
  Create self-signed root certificate; create signing requests for devices with subsequent signing and installation of device certificates; remove certificate assignments to services

- **TLS Certificate Overview**
  Overview of which certificates are installed on a device; certificate status information (valid from/to etc.)

- **TLS Network Services**
  Overview of activated/deactivated network services; configuration of the services (switch on/off)

- **TLS Direct Certificate Connection Info**
  Status information about the current TLS connection of the selected device

3.3 CERTIFICATION AUTHORITY

In order to be able to issue and sign your own certificates, you must first set up a certificate authority (CA). This is a special root certificate that can be used to sign other certificates.

Dallmeier Device Manager (DDM) can handle client and server certificates via its own certificate authority (root CA). An own root CA allows DDM to create and sign certificates and to install them on devices (cameras, recorders) in the network. On this basis, you can then encrypt device connections via HTTP and DaVid (Dallmeier Video Protocol) using the Transport Layer Security (TLS) protocol.

To set up a certification authority, you can use your own certificates issued by recognized certification authorities, for example. However, DDM also generates a self-signed root certificate.

NOTICE

Setting up a certification authority with a self-signed root certificate is only recommended for the transition until a certificate from a recognized certification authority is available. And also only within a local network.
If there is access to your own system from public, potentially dangerous networks (e.g., from the Internet), only certificates from recognized certification authorities should be used from the start to encrypt network connections and authenticate devices.

Set up a Certification Authority (CA)
Dallmeier Device Manager can be used as a certification authority with "an" externally issued root certificate ("Option A – Use Own Root Certificate" on page 13). For this purpose, you have to save the certificate and the corresponding private key on your local client PC. The certificate here can be a root certificate or a subordinate CA certificate.

However, you can also operate your DDM certification authority with a self-signed root certificate ("Option B – Generate Root CA" on page 14). In this case, you create your own self-signed root CA in DDM.

► Follow the procedure below to set up a DDM certification authority on your client PC.

To create TLS certificates in DDM, the free software toolkit "OpenSSL" must be installed in its current version. "OpenSSL" implements the corresponding network protocols as well as the cryptography standards used.
Further information, installation instructions and download of the current version at www.openssl.org.

- Open the **Settings** menu item .
- Switch to the **Certification Authority** setting option.

OpenSSL

OpenSSL implements the SSL and TLS encryption protocols and provides the functions to request, generate and manage certificates.

- Select the **OpenSSL** tab.

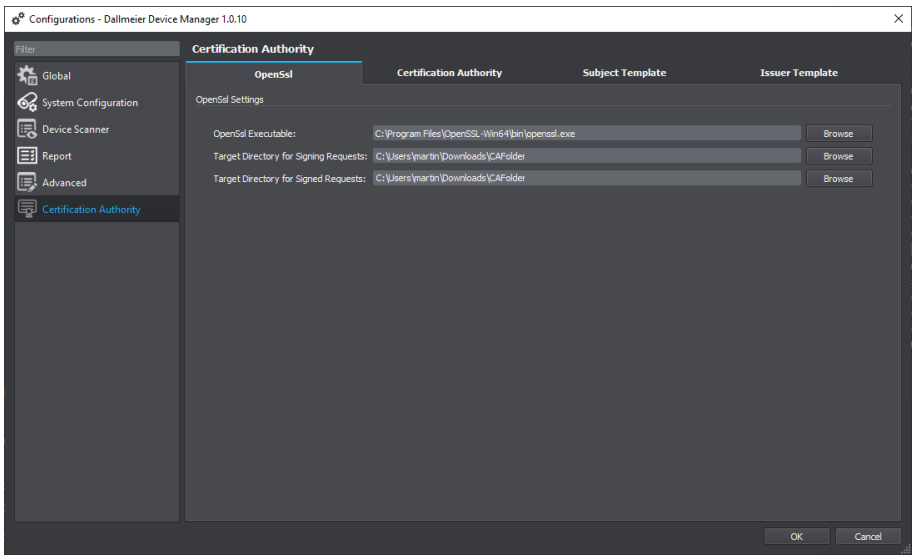


Fig. 3-3

- Enter the path to the OpenSSL executable directly in the first field or use the **Browse** button to navigate to the required directory using the file manager.
- In the next two fields, enter the path to the **Signing Requests** and **Signed Requests** directories respectively.

The directories are for your own overview and can be chosen arbitrarily.

- Click **OK** to save the entries and then open the **Certification Authority** settings option again.

Certification Authority

This tab contains all information about your DDM certification authority. Here you can specify the path to your own root certificate and the associated private key or generate a self-signed root certificate.

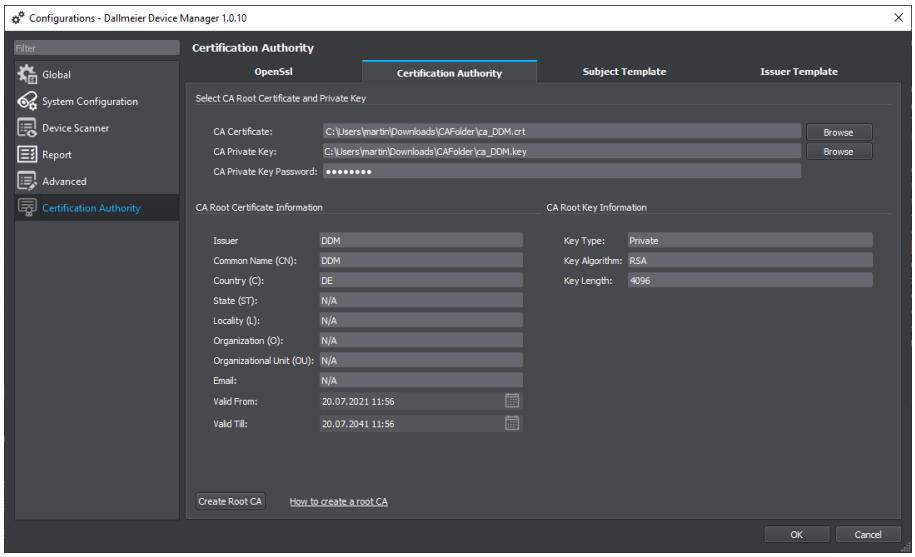


Fig. 3-4

Option A – Use Own Root Certificate

- Open the **Settings** menu item  and switch to the **Certification Authority** tab.
- In the **CA Certificate** field, enter the directory path to your own root certificate to be used for the certificate authority.
- In the **CA Private Key** field, enter the directory path to the private key file.
- In the **CA Private Key Password** field, enter the associated passphrase.

The information about the root CA certificate and key is read from the stored certificate and automatically entered in the corresponding fields.

- Click **OK** to save your entries.

Option B – Generate Root CA

- Open the **Settings** menu item and switch to the **Certification Authority** tab.

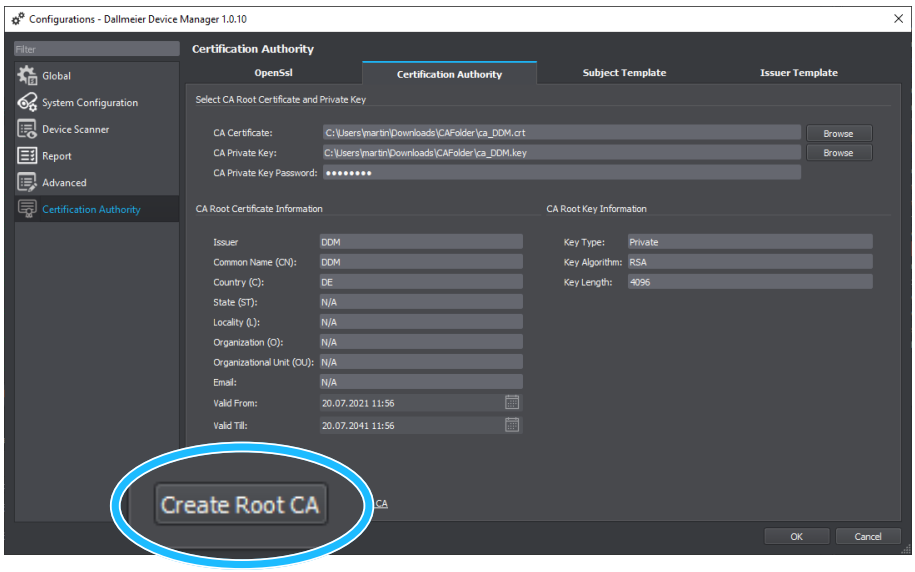


Fig. 3-5

- Click **Create Root CA**.

The **Create Root CA** dialog is displayed.

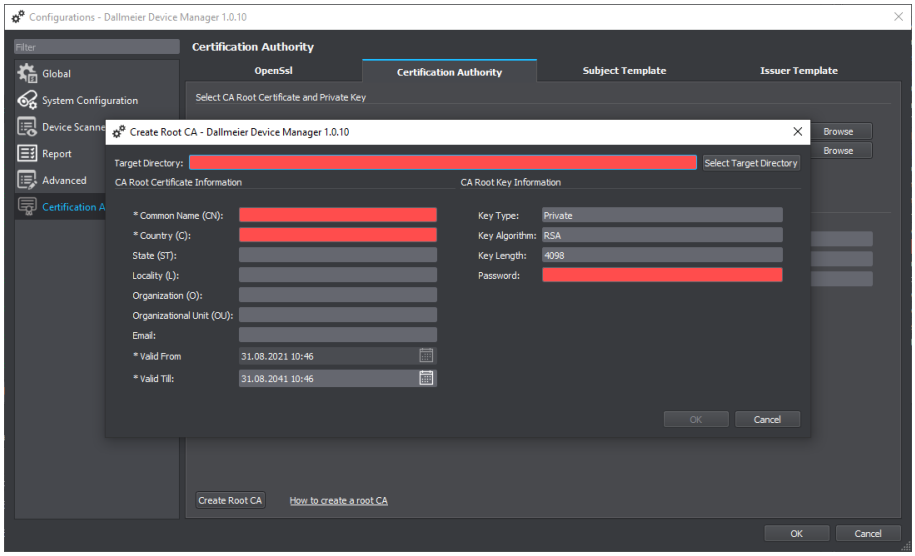


Fig. 3-6

The fields marked in red are mandatory, the others can be completed optionally.

- Click **Target Directory** and navigate to the required directory using the file manager.
- In the **Common Name** field, enter the name of the root CA. The name is freely selectable.
- In the Country field, enter the required country identifier (e.g. “DE” for Germany).
- Under **Valid From/Till**, specify the validity period of the root CA (default setting: 20 years).
- In the **Password** field, set a passphrase for the private key.
- Optionally complete other fields if required.
- Confirm your entries with **OK**.

The root CA is generated and the following files are created in the specified target directory:

- **ca_*common-name*.crt** – the root certificate
- **ca_*common-name*.key** – the private key

The private key is used to sign the device requests and must not leave the client PC in order not to break the TLS security chain.

Add Root Certificate in Windows

It is recommended to always add the CA certificate to your Windows certificate store as well, so that the web browser (for example when opening a camera web configuration) does not display a security warning about an invalid security certificate and the connection to the device is not blocked. A certificate import in Windows allows you to establish a secure HTTPS connection in the browser with your devices.

► Open the Windows certificate store via **Tools** > **TLS Tools** > **Microsoft Windows Certificate Manager**.

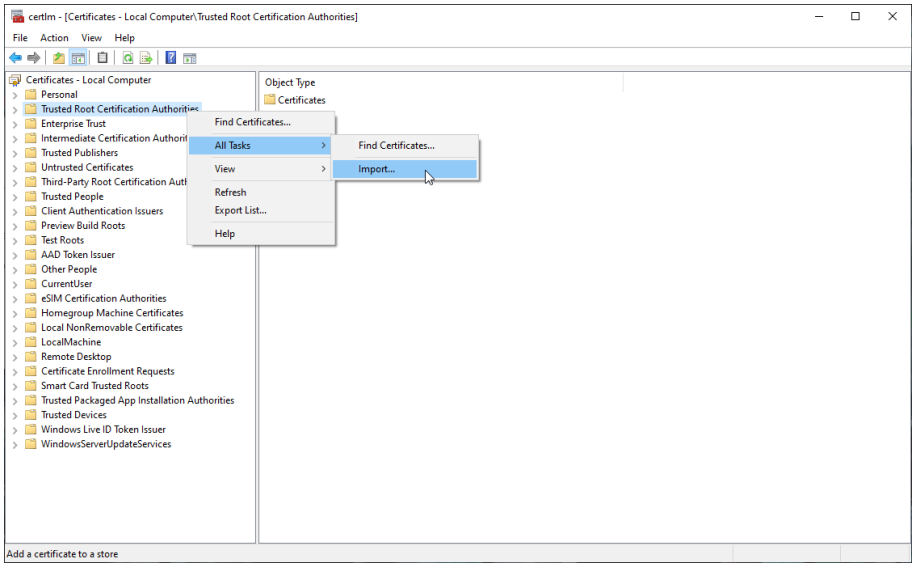


Fig. 3-7

► Right-click the **Trusted Root Certification Authorities** entry to display the context menu.
► Select **All Tasks** > **Import...**.

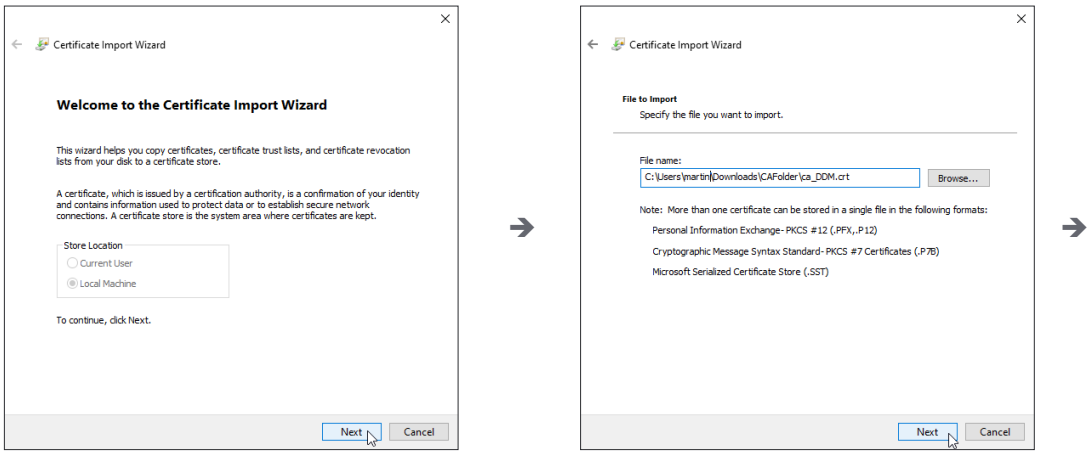


Fig. 3-8

► Click **Next**.
► Click **Browse...**, select the certificate you want to import and click **Next**.

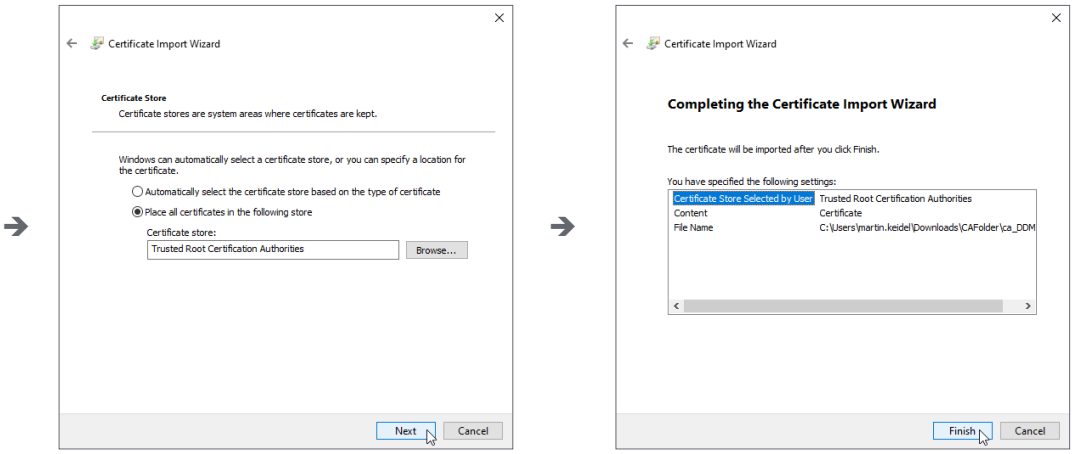


Fig. 3-9

- Select **Trusted Root Certification Authorities** as the certificate store and click **Next**.
- Click **Finish** to start the import process.

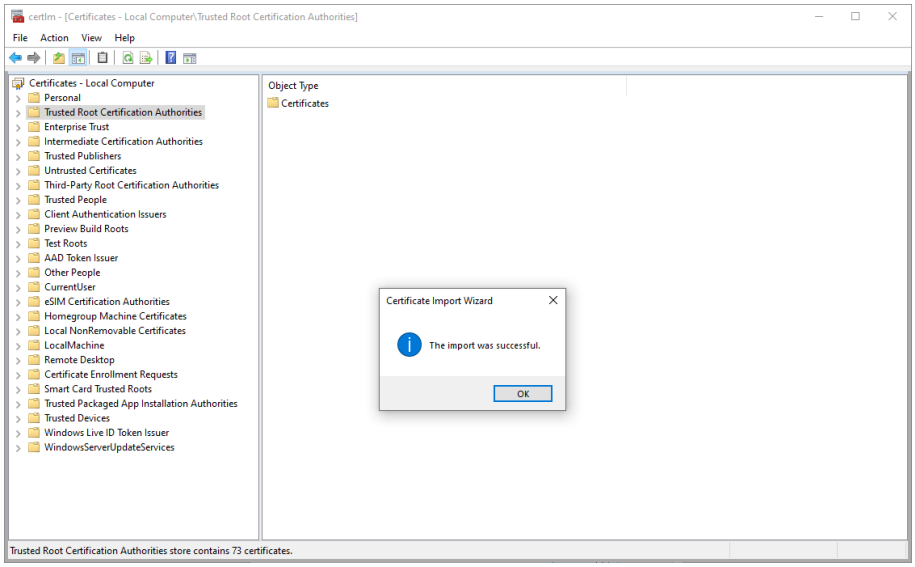


Fig. 3-10

- Confirm the **Certificate Import Wizard** with **OK** and exit the Certificate Manager after the import process is successful.

Subject Template

Your DDM certification authority uses the information from this dialog to create device certificates for signing requests.

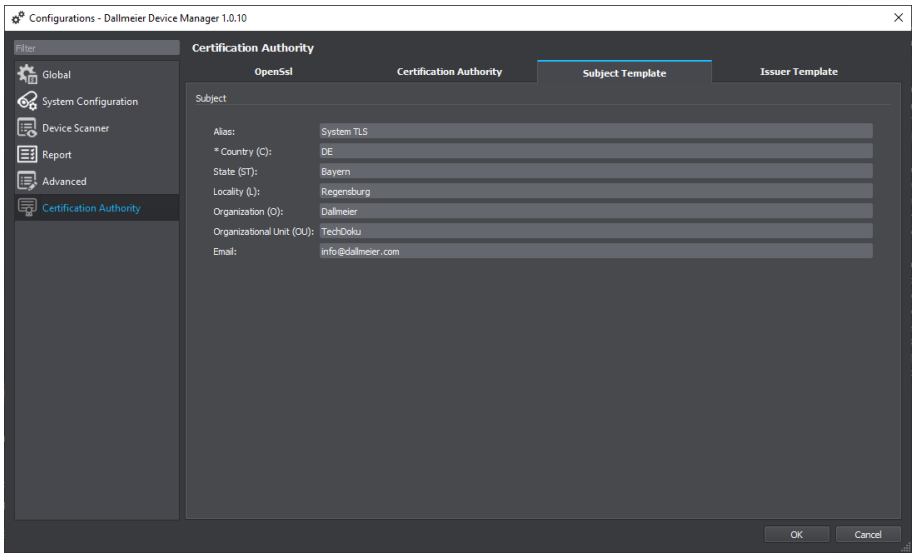


Fig. 3-11

- Enter the required information for the certificate owner in the appropriate fields.
- Confirm with **OK** to save your entries.

Issuer Template

In this dialog you define the validity period for the device certificates that your DDM certification authority issues for signing requests.

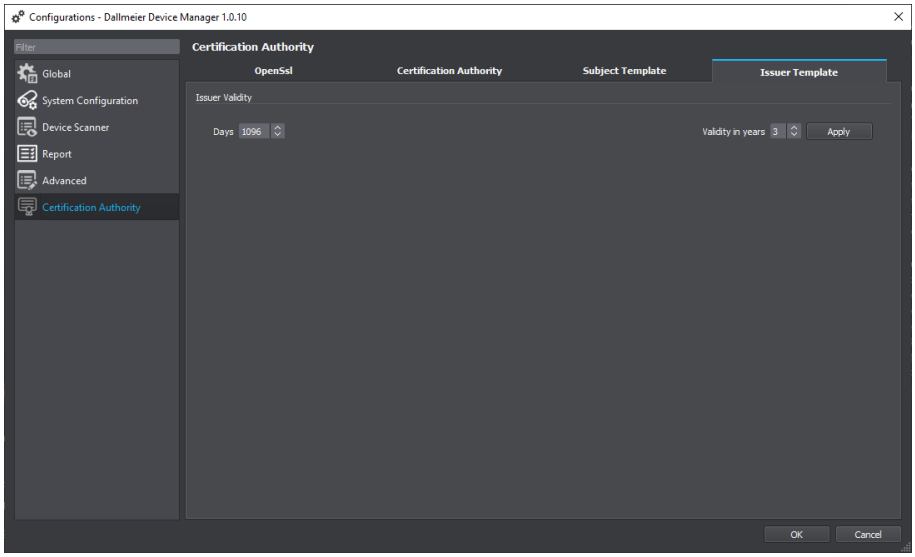


Fig. 3-12

- In the **Validity in years** field, enter the desired period.
- Click **Apply**.

3.4 ENCRYPT CONNECTIONS

After setting up a certificate authority (CA) on your client PC in the Dallmeier Device Manager (DDM) you can now start encrypting connections from your DDM client PC to cameras and recorders in your network with Transport Layer Security (TLS).
To enable the required protocols DaVid-TLS (cameras, recorders) and HTTPS (cameras), a certificate must be installed on a device. As a CA, DDM enables the corresponding certificates to be created, signed and installed on the devices. The procedure is the same for cameras and recorders.

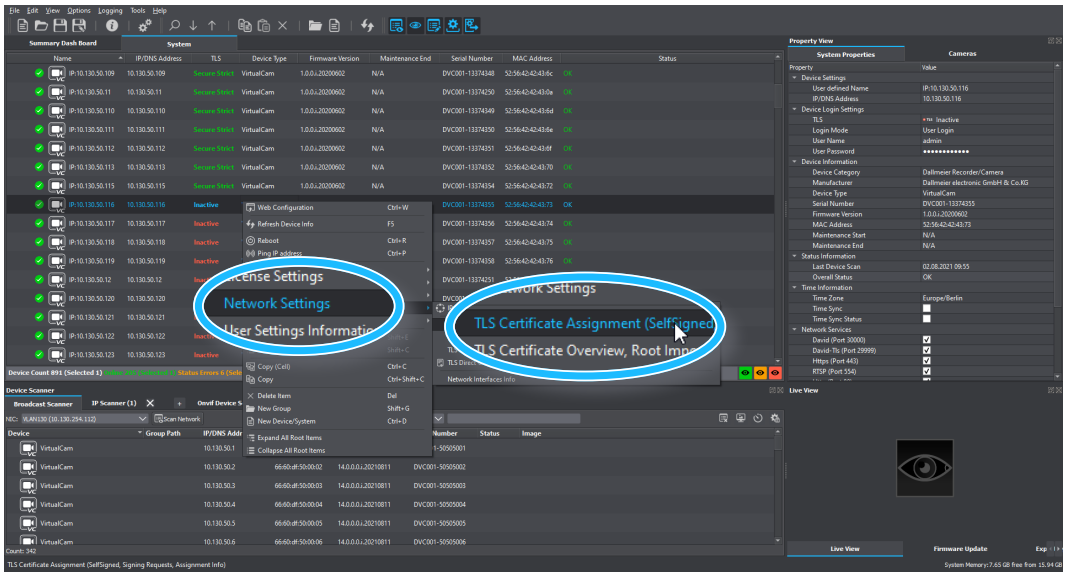


Fig. 3-13

- Select the required device in your **System**.
- Right-click the device to display the context menu.
- Open the required dialog via **Network Settings** > **TLS Certificate Assignment**.

The dialog is displayed in a new tab. You can see from the services marked in red that HTTPS and DaVid TLS are not yet enabled.

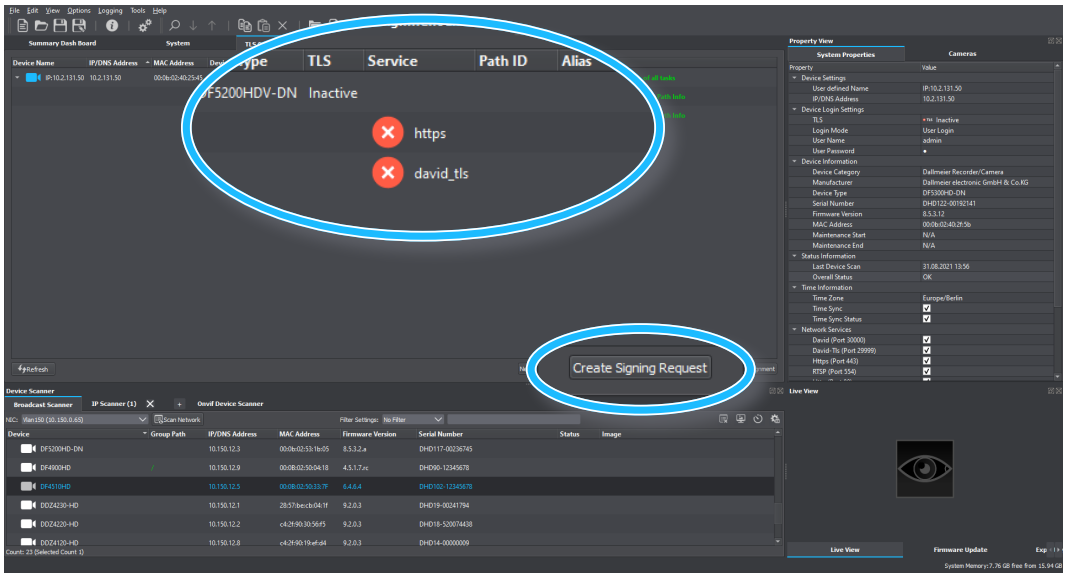
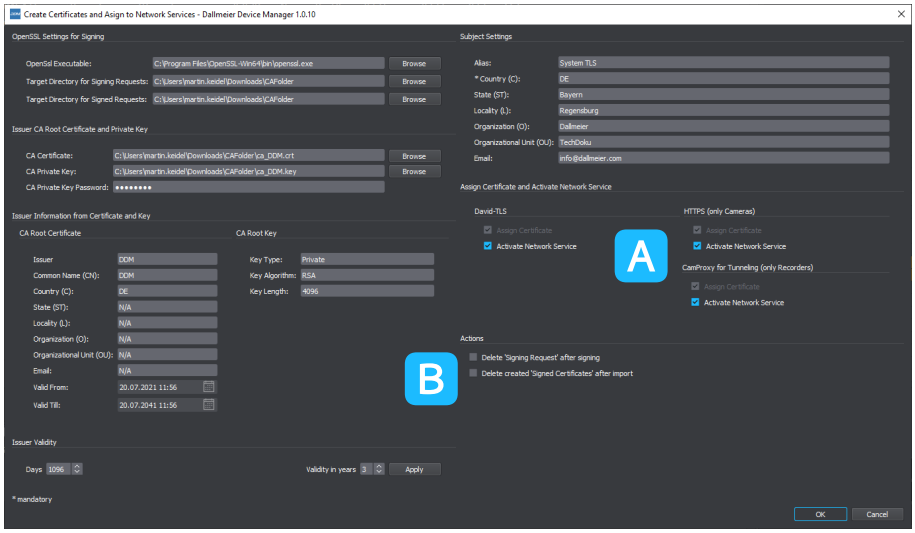


Fig. 3-14

- Click **Create Signing Request**.

The **Create Certificates and Assign to Network Services** dialog is displayed.



Left side: Information of the root CA; right side: Details for the device certificate to be issued as made in the DDM settings (see sections “Certification Authority” on page 13, “Subject Template” on page 17, “Issuer Template” on page 17).

Fig. 3-15

A By default, the certificate assignment also activates the corresponding network services. Deactivate them if necessary.

B You can prevent the signing request and the device certificate from being saved on your local client PC and delete the files after the process if you activate the checkboxes here.

► Click **OK** and confirm the following security prompt to start the certificate creation process.

Your DDM root CA signs the certificate request and automatically installs the appropriate certificate on the device.

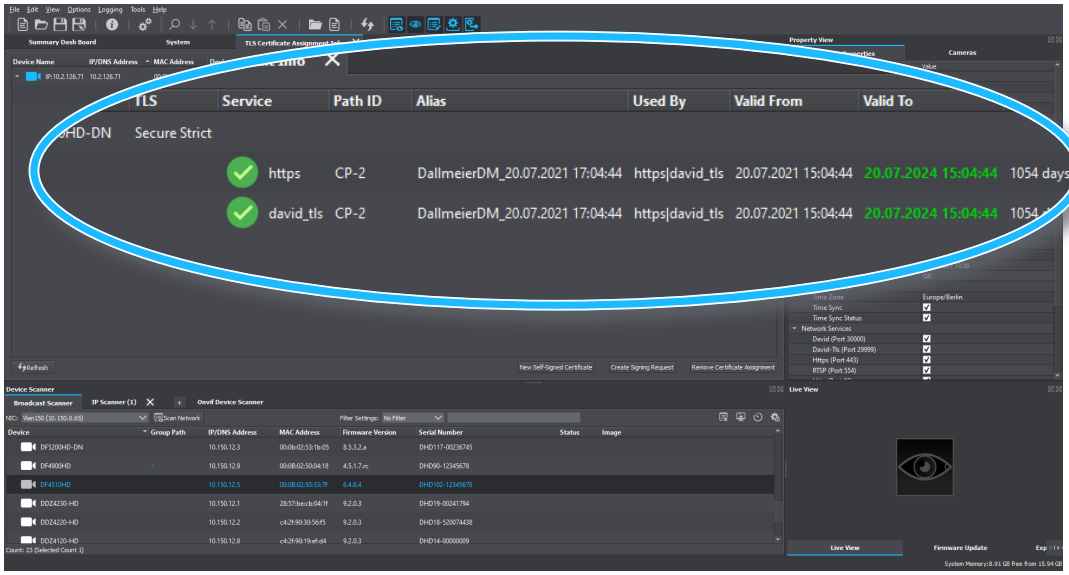


Fig. 3-16

The HTTPS and DaVid TLS services are now enabled on the device and you can establish an encrypted connection to it.

- To do so, switch to the **System** tab.

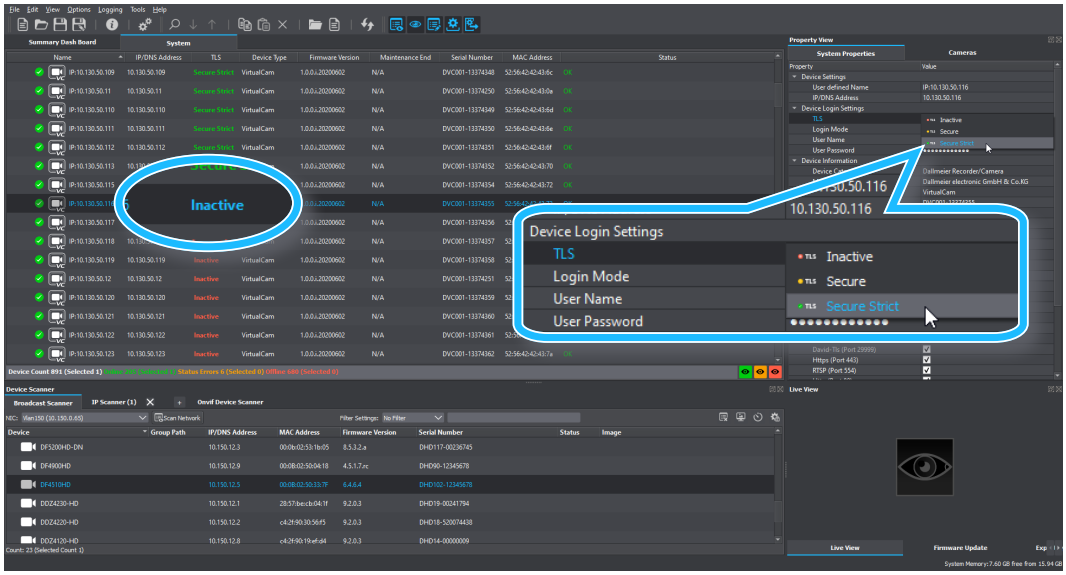


Fig. 3-17

The **TLS** settings show the **Inactive** mark for an unencrypted connection.

- Open the **TLS** drop-down menu under the **Device Login Settings** in the **System Properties**.
- Select the **Secure Strict** option.
- Refresh the connection to the device with the **F5** key.

When the connection is re-established, your DDM Root CA validates the device certificate and both communicate over a TLS encrypted connection from now on.

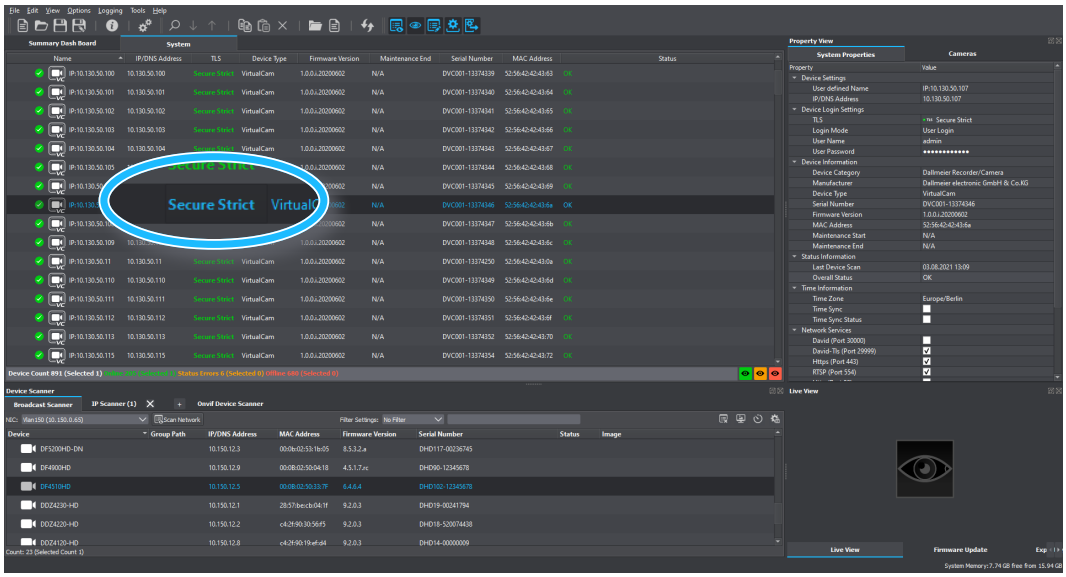


Fig. 3-18

The **TLS** settings of the device now show **Secure Strict**.

3.5 RECORDER-TO-CAMERA CONNECTIONS

TLS connections of a recording system (recorder) to its cameras can be set up with the root certificate of your DDM certification authority. To do this, you import the certificate on the recorder and it uses it to validate the camera certificates that you previously installed on the cameras via DDM using this root certificate.

- Right-click the required recorder in the **System** view to display the context menu.

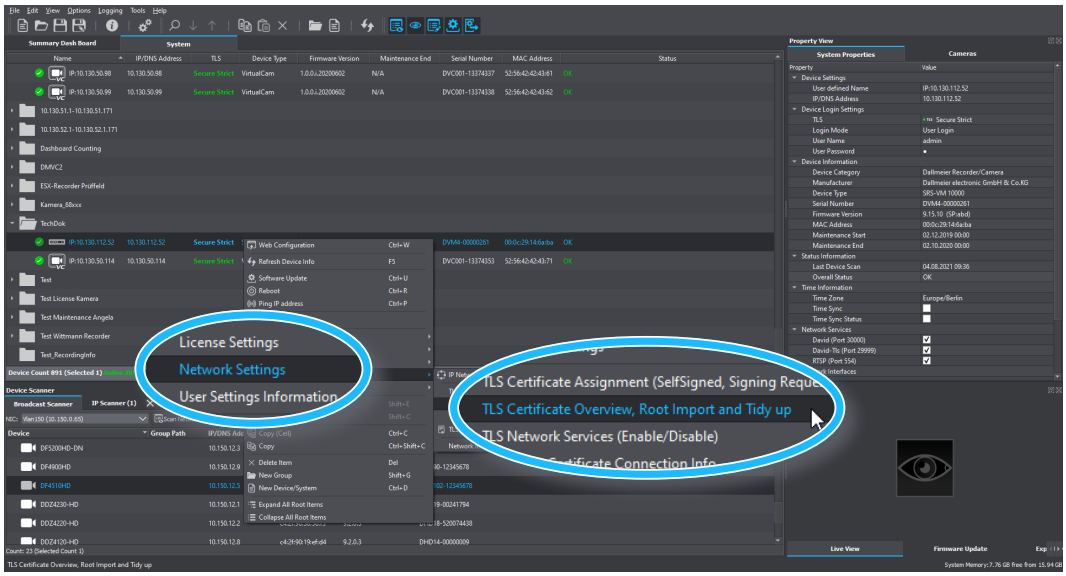


Fig. 3-19

- Select **Network Settings** > **TLS Certificate Overview**.

The **TLS Certificate Overview** dialog is displayed in a new tab.

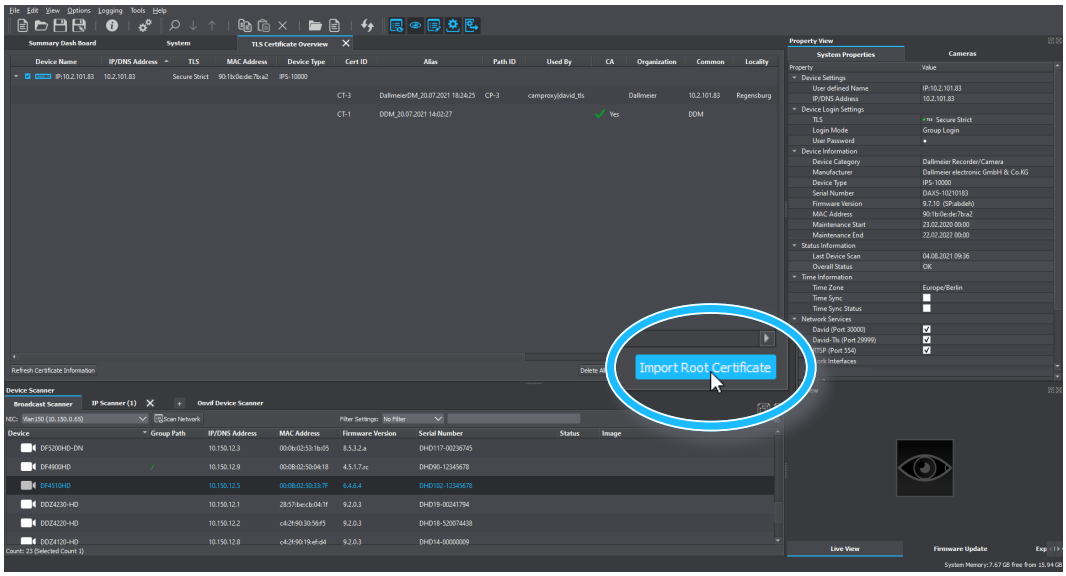


Fig. 3-20

- Click **Import Root Certificate**.

The **Root Certificate Import** dialog is displayed.

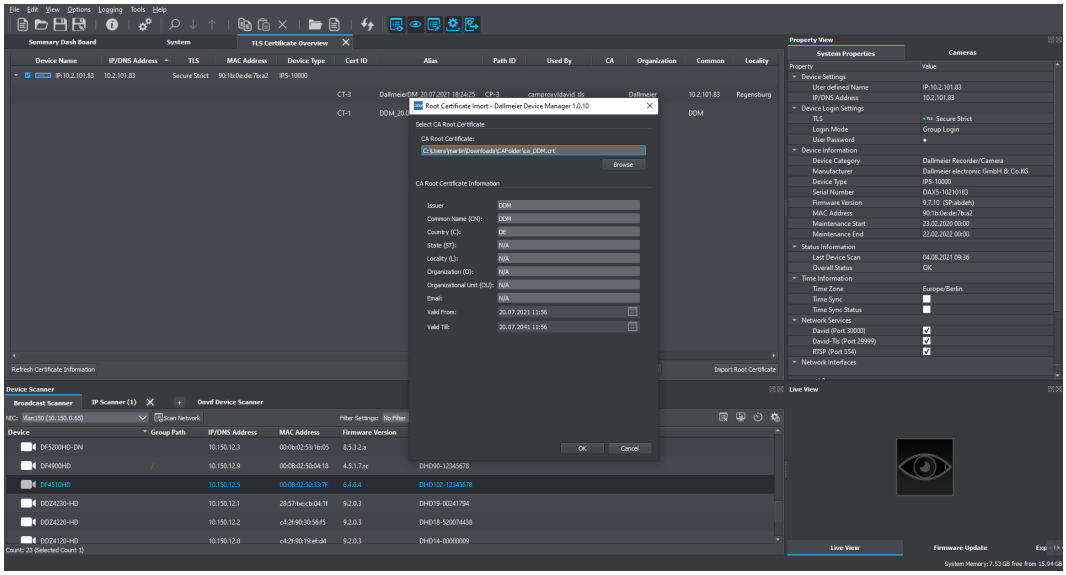


Fig. 3-21

The dialog automatically adopts the root certificate previously set up in the DDM settings.

- ▶ Click **OK**.
- ▶ Confirm the following security dialog to start the import process.

The root certificate is loaded onto the recording system.

Enable DaVid TLS for Camera Connections

After importing the root certificate, you can now enable DaVid TLS over port 29999 for the recorder's camera connections and disable DaVid port 30000 to no longer allow unencrypted camera connections over it.

- ▶ Right-click the required recorder in the **System** view to display the context menu.

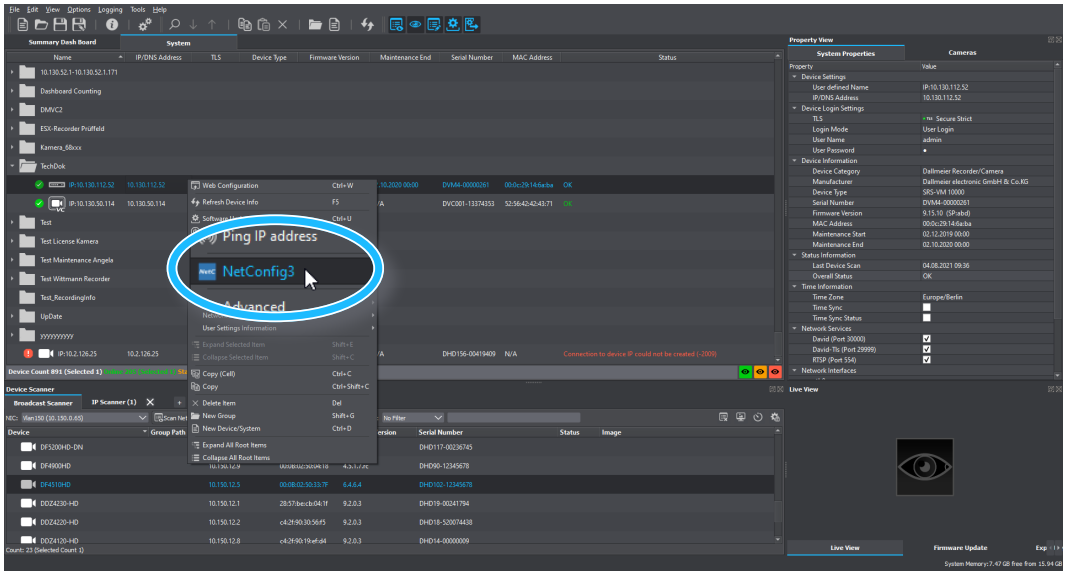


Fig. 3-22

- ▶ Select **NetConfig3** to open the recorder configuration.

The **NetConfig3** connection dialog is displayed and the logon to the recorder is automatic.

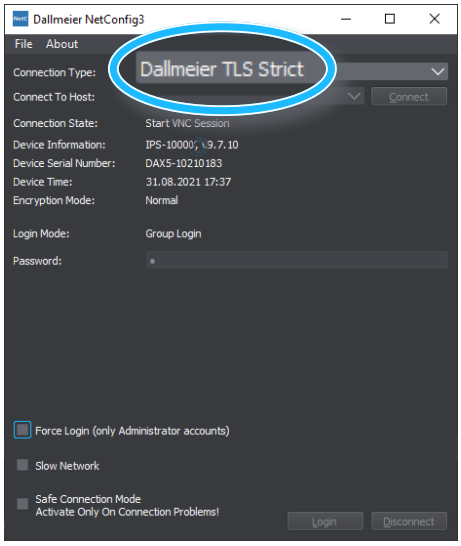


Fig. 3-23

Note the **Connection Type Dallmeier TLS Strict***: DDM client PC and recorder communicate via an encrypted connection. Login and configuration data cannot be "read".*

The configuration interface of the recorder is displayed:

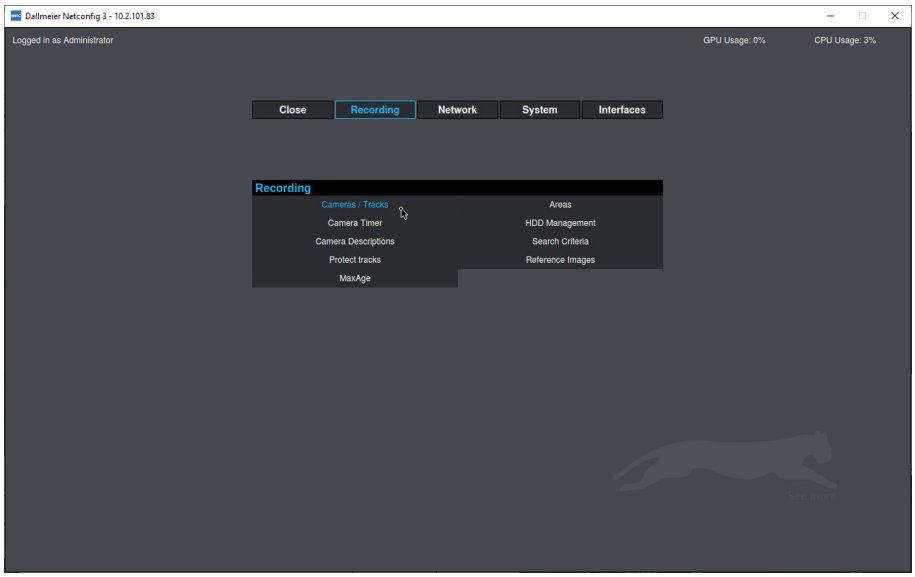


Fig. 3-24

► Select **Recording** > **Cameras / Tracks**.

The camera configuration of the recorder is displayed:

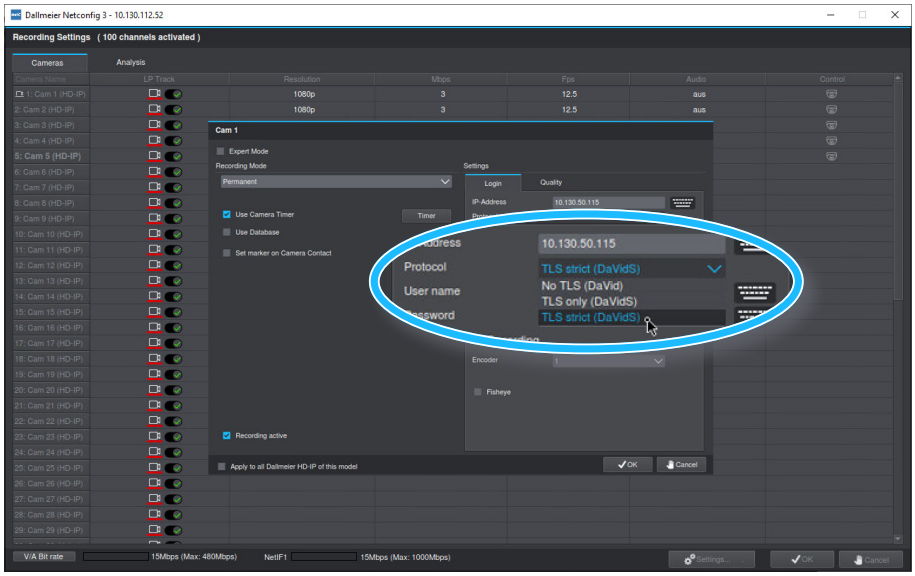


Fig. 3-25

- Click on a camera in the **LP Track** column to display the camera's recording dialog.
- Select **TLS Strict (DaVidS)** from the **Protocol** drop-down menu.
- Click **Test** to check the camera connection, if required.

If the connection test to the camera is successful, close the camera's recording dialog by clicking OK.
If no connection can be established to the camera using the TLS protocol, reset the protocol to the **No TLS (DaVid)** option and first check the certificates on the devices involved.

- Proceed as described above to enable the TLS option for all required cameras.

If all recorder-camera connections have been successfully changed over in this way, you can also check this in the Dallmeier Device Manager (DDM):

- Select the required recorder in the **System** view.
- Use the **F5** key to refresh the connection if not already done after TLS configuration.
- In the **Property View**, select the **Cameras** tab.

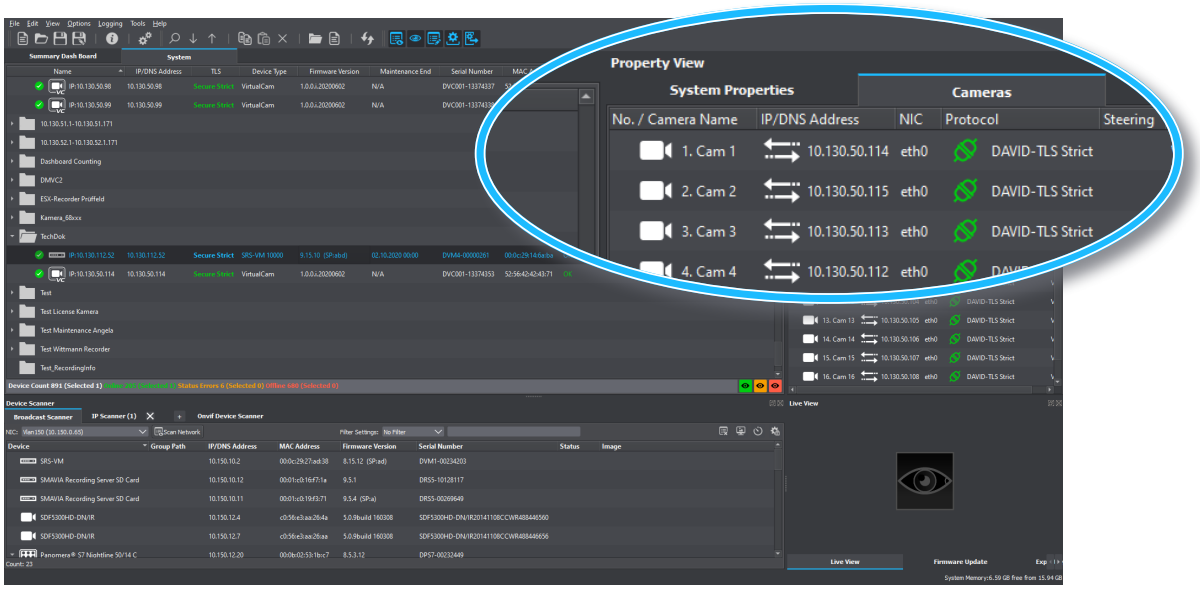


Fig. 3-26

The **Cameras** tab displays all the information about the recorder's camera connections, including the protocol used to connect the cameras to the recorder.

3.6 DISABLE INSECURE PORTS

After the installation of the device certificates and the establishment of the encrypted TLS connections you can now finally deactivate the ports (HTTP port 80, DaVid port 30000) on the devices, which unencrypted communication would still be possible, in order to prevent insecure connections from being no longer permitted. You can see the currently active **Network Services** A of the device in its **System Properties**.

► Right-click the device to display its context menu B.

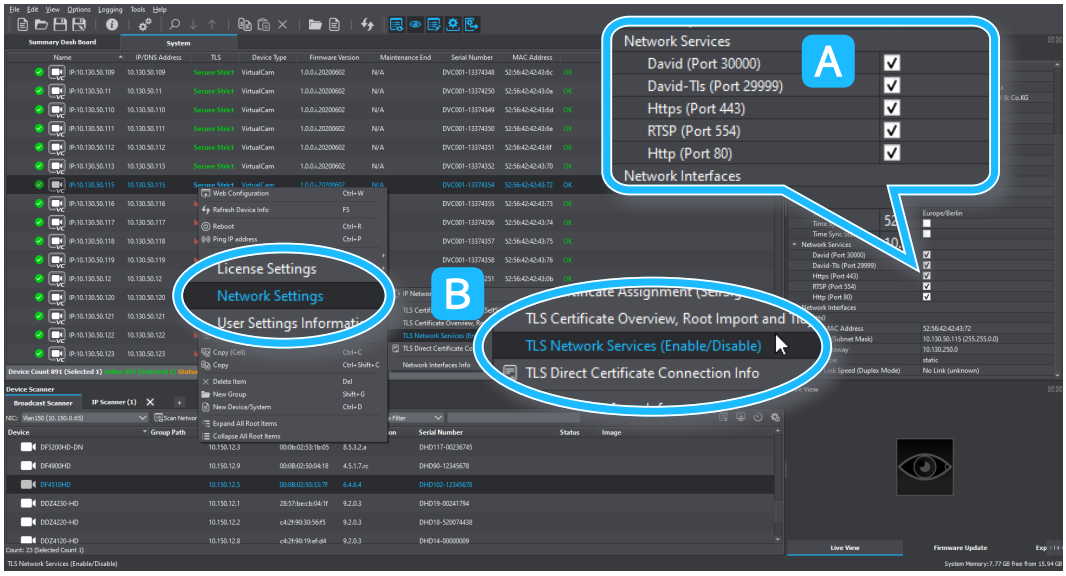


Fig. 3-27

► Select **Network Settings** > **TLS Network Services (Enable/Disable)**.

The **Network Services** dialog is displayed in a new tab. Here you can once again clearly see the available communication ports of the active network services.

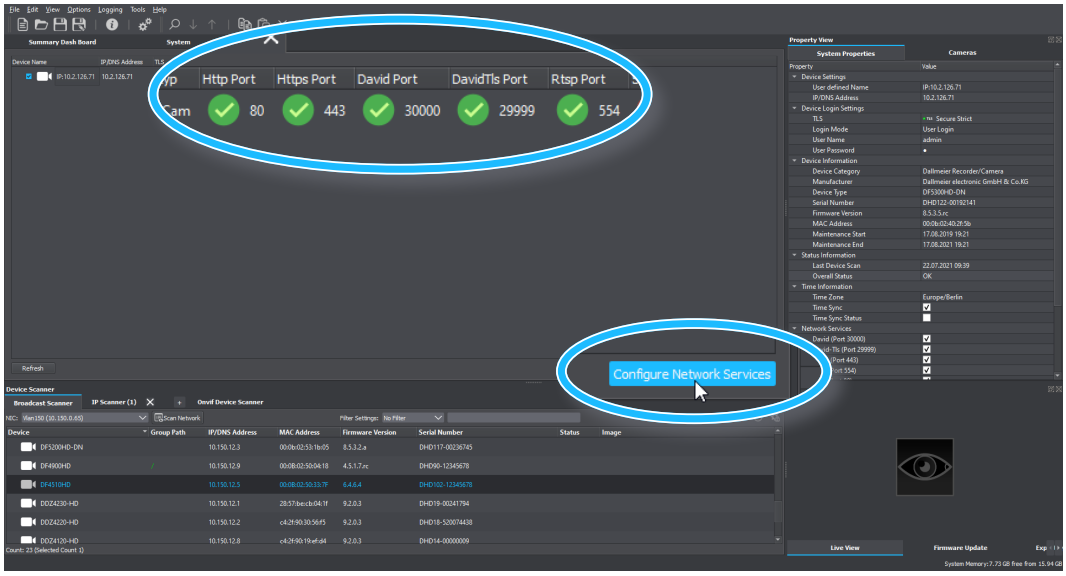


Fig. 3-28

► Click **Configure Network Services**.

The **Network Services Settings** dialog is displayed.

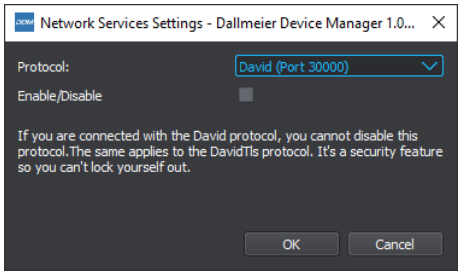


Fig. 3-29

- From the **Protocol** dropdown menu, select **DaVid (Port 30000)**.
- Do not select the **Enable/Disable** checkbox if you want to disable the selected protocol.
- Click **OK** and confirm the following security prompt.

The DaVid port 30000 is disabled. Now switch off port 80.

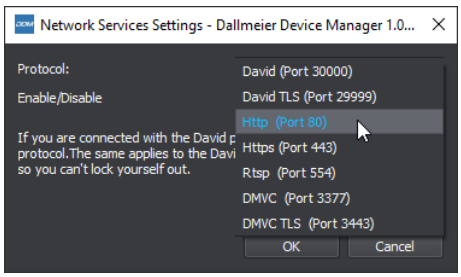


Fig. 3-30

- From the **Protocol** dropdown menu, select **HTTP (Port 80)**.
- Do not select the **Enable/Disable** checkbox if you want to disable the selected protocol.
- Click **OK** and confirm the following security prompt.

The device can now no longer be reached via ports 80 and 30000 and therefore unencrypted communication via them is no longer possible.

In the **Network Services** dialog, you will see that the corresponding ports are now disabled.

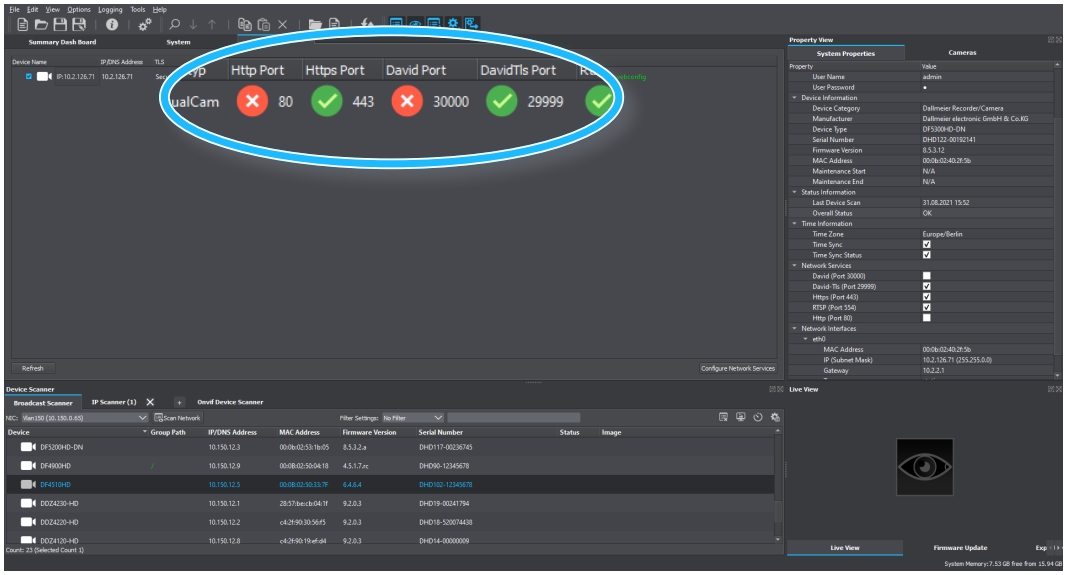


Fig. 3-31

- Switch to the **System** tab and refresh the device connection with the **F5** key to update the **Network Services** display in the **System Properties**.

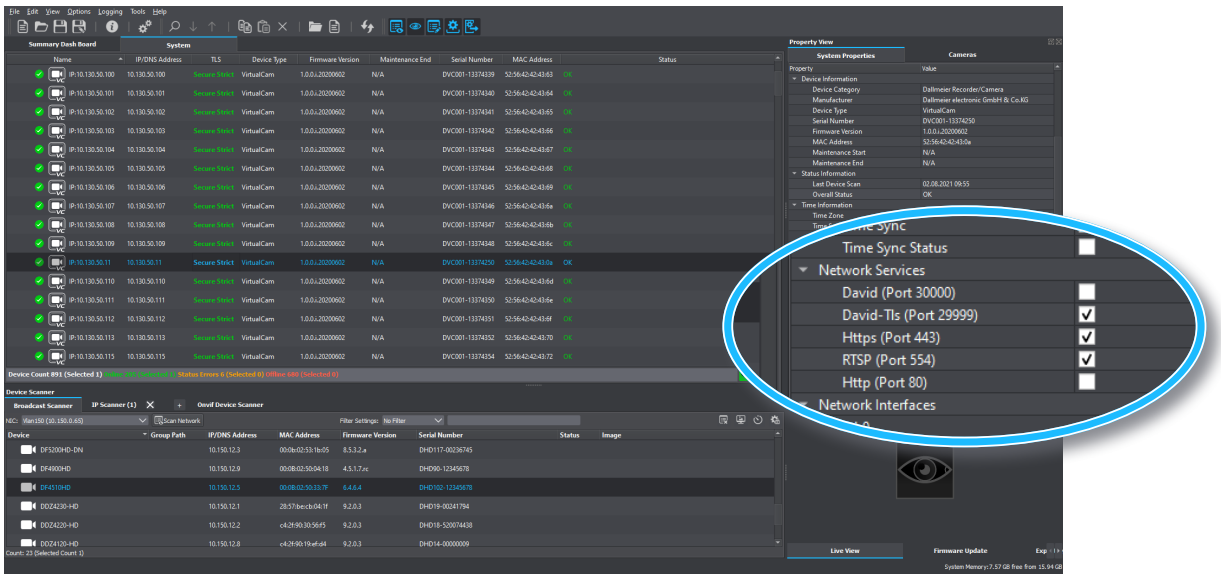


Fig. 3-32

Here you can see which **Network Services** are used for communication.

HEAD & ACCOUNTS OFFICE

Dallmeier electronic GmbH & Co.KG
Bahnhofstr. 16
93047 Regensburg
Germany

tel +49 941 8700 0
fax +49 941 8700 180
mail info@dallmeier.com

www.dallmeier.com