

REV. 1.0.0 | 2021-10-25

CONFIGURATION

DALLMEIER DEVICE MANAGER



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





Copyright © 2021 Dallmeier electronic GmbH & Co.KG

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization is prohibited. Offenders will be held liable for the payment of damages.

All rights reserved in the event of the grant of a patent, utility model or design.

The manufacturer accepts no liability for damage to property or pecuniary damages arising due to minor defects of the product or documentation, e.g. print or spelling errors, and for those not caused by intention or gross negligence of the manufacturer.

Figures (e.g. screenshots) in this document may differ from the actual product. Specifications subject to change without notice. Errors and misprints excepted.

All trademarks identified by [®] are registered trademarks of Dallmeier electronic.

All trademarks identified by *) are trademarks or registered trademarks of the following owners: Microsoft, Microsoft Edge and Windows of Microsoft Corporation headquartered in Redmond, Washington, USA;

Third-party trademarks are named for information purposes only. Dallmeier electronic respects the intellectual property of third parties and always attempts to ensure the complete identification of third-party trademarks and indication of the respective holder of rights. In case that protected rights are not indicated separately, this circumstance is no reason to assume that the respective trademark is unprotected.

In addition, the following legal notices concerning the product described in this document and/or its underlying software must be observed: 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.

TABLE OF CONTENTS

KAPITEL 1:	INTRODUCTION	4
1.1	Validity	4
1.2	Documents	4
1.2.1	This Document	4
1.2.2	Applicable Documents	4
1.3	Representation Conventions	5
1.4	Legal Notices	5
KAPITEL 2:	GENERAL NOTES	6
2.1	Appropriate Use	6
2.2	Additional Features and Functions	7
2.3	Warranty	7
KAPITEL 3:	TLS CONFIGURATION	8
3.1	Recommended Procedure	8
3.2	Overview	9
3.2.1	TLS Tools	9
3.2.2	TLS Configuration and Management	10
3.3	Certification Authority	11
3.4	Encrypt Connections	18
3.5	Recorder-to-Camera Connections	21
3.6	Disable Insecure Ports	26

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.

Elle Edit Yiew Options Logging 🔤	NetConfig3		× 🖿 (🖹 🎸 民	ی 🗐 👁	e .							
Summary Dash Board	seway compact										Property View		
Nama	Snapshot Shooter v		Int Emu	a Vertino Mainten		Number	MAC Address				System Properties	Cameras	
- · · · · · · · · · · · · · · · · · · ·	Open RTSP Stream		1795 TITLING										
10.125.170.1-10.125.170.100		N									 Device Settings 		
x 10 105 171 1 10 105 171 100			0 Wins	lows Certificate Manager									
+ 10.130.42.1-10.130.42.115											 Device Login Settings 		
						-							
 10.130.50.1-10.130.50.171 											Login Mode		
Operation 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	Tools -	lelp									User Password	•••••	
Image: 10 10 10 10 10 10 10 10 10 10 10 10 10											 Device Information 		
	Not(Config2							(. 🛛 🧲		Device Category	Dallmeier Recorder/Camera	
IP:10.130.50.100	THEIR	conings				X I		=	Z		Manufacturer	Dallmeier electronic GmbH &	Co.KG
<u> </u>										0 -		VirtualCarn	
🕗 🛄 IP:10.130.50.101	🛛 🖛 🛛 SeM	Sv Compa	et								Serial Number	DVC001+13374337	
· · · · · · · · · · · · · · · · · · ·											Firmware Version	1.0.0.1.20200602	
											MAC Address	52:5642:42:43:61	
Image: 10 (10) 100 (10) 100 (10)	Snar	schot Shoo	ter via Vide	o File							Maintenance Start	N/A	
		31101 31100		o me	π.,		F:	- W	Malas	F .	Maintenance End		
IP:10.130.50.104	12.0				- IV	pe	Firmwar	e version	iviaint	enance El	Status Information		
	i 🗄 Ope	n RISP Stre	am via Url								Last Device Scan	03.08.20211817	
IP:10.130.50.105											Overall Status		
	TIS	Tools		N 1	•	TISC	lient Root	Certificate '	Viewer		Time Promadon	Courses (Perfor	
						125 0	Sherre Root	Certificate			Time Supr	cuoperterm	
Image: 10,130,50,107							6 M C 1				Time Supe Status		
<						Micro	osoft Wind	ows Certific	cate Manag	jer 🇾	* Network Services		
🕗 🛄 IP:10.130.50.108 🔪						_					David (Port 30000)	V	
											David-TIs (Port 29999)	V	
V Line 101 100 101											Https (Port 443)	V	
Device Count 891 (Selected 1) 00000000										000	RTSP (Port 554)	V	
Devke Scanner											Live View		
Broadcast Scanner IP Scanner (1)		Onvif Device Scanner											
MC+ W 4N130 (10 130 254 117)	V Rom Natural			Fiber Settioner No. Filter	~					■ ■ ● ♣			
Denter	Course Both	10/DMC Address	MAC Address	Compare Mandan	Control Management	Cardon .	lerrer.						
Device	 Group Path 	IP/UNS Address	MAC Address	Firmware version	Senal Number	Status	Image						
VideoNetBox III				9.11.10 (SPic)	DAV8-00401312								
SRS-VM 10000													
SRS-VM 10000													
SRS-VM 10000				9.15.10 (SP:abd)	DVM4-00000261								
-													
Panomera Sis Ultraline 66/45 C			00000021591507cb		0758-00284089								
Panomera® S8 Ultraline 66/4.													
Count: 43											UVe Yiew	remware Opdate	Exp (1)
												System Memory: 7,74 GB	Tree from 15.94 GE

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.

م ⁰ Configurations - Dallmeier Device Manager 1.0.10 ×										
Filter	Certification Authority									
🚓 Global	OpenSsl	Certification Authority	Subject Template	Issuer Template						
System Configuration	OpenSsl Settings									
Revice Scanner	OpenSsl Executable:	C:\Program Files\OpenSSL-Win64\bin\openssl.exe		Browse						
E Report	Target Directory for Signing Requests:	C:\Users\martin\Downloads\CAFolder		Browse						
📑 Advanced	Target Directory for Signed Requests:	C:\Users\martin\Downloads\CAFolder		Browse						
Certification Authority										
				OK Cano	rel					

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.

🗳 Configurations - Dallmeier Device N	Manager 1.0.10						>
Filter	Certification Authority						
🚰 Global	OpenSsl	Certifica	tion Authority	Subject 1	Template	Issuer Ter	nplate
😪 System Configuration	Select CA Root Certificate and	Private Key					
Device Scanner	CA Certificate:	C:\Users\martin\Downloads	\CAFolder\ca_DDM.crt				Browse
Report	CA Private Key:	C: \Users\martin\Downloads\	CAFolder\ca_DDM.key				Browse
Advanced	CA Private Key Password:						
Certification Authority	CA Root Certificate Informatio	n		CA Root Key Inform	nation		
-86							
	Issuer	DDM		Key Type:	Private		
	Common Name (CN):	DDM		Key Algorithm:	RSA		
	Country (C):			Key Length:	4096		
	State (ST):	N/A					
	Locality (L):	N/A					
	Organization (O):	N/A					
	Organizational Unit (OU):	N/A					
	Email:	N/A					
	Valid From:						
	Valid Till:						
	Create Root CA How to	create a root CA					
							Cancel

Fig. 3-4

Option A – Use Own Root Certificate

- Open the Settings menu item *a* 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.

📌 Configurations - Dallmeier Device Manager 1.0.10 X										
Filter	Certification Authority									
🚓 Global	OpenSsl	Certificatio	on Authority	Subject 1	Issuer Ten	nplate				
System Configuration	Select CA Root Certificate and									
Device Scanner	CA Certificate: C:\Users\martin\Downloads\CAFolder\ca_DDM.crt									
≣ Report	CA Private Key:	C:\Users\martin\Downloads\CA	Folder\ca_DDM.key				Browse			
Advanced	CA Private Key Password: •••••••									
Certification Authority	CA Root Certificate Informatio			CA Root Key Inform	ation					
	Issuer	DDM		Key Type:	Private					
	Common Name (CN):	DDM		Key Algorithm:	RSA					
	Country (C):	DE		Key Length:	4096					
	State (ST):	N/A								
	Locality (L):	N/A								
	Organization (O):	N/A								
	Organizational Unit (OU):	N/A								
	Email:	N/A								
	Valid From:									
	Valid Till:									
		n 🔪								
Cr	eate Root CA	CA CA								
						ОК	Cancel			
						- OK				

Fig. 3-5

Click Create Root CA.

The Create Root CA dialog is displayed.

Configurations - Da	allmeier Device Mar	nager 1.0.10							×
Filter		ertification A	Authority						
🛵 Global		Op	enSsl	Certificati	on Authority	Subjec	t Template	Issuer Ten	nplate
😪 System Configu	ration	Select CA Root Ce	ertificate and Private Key						
Device Scanne	🔅 Create Root CA	- Dallmeier Dev	ice Manager 1.0.10					×	Browse
📰 Report	Target Directory:							Select Target Directory	Browse
Advanced	CA Root Certificate I	information			CA Root Key Inform	nation		outer in get on term y	
Certification A	* Common Name	(CN):			Key Type:	Private			
	* Country (C):	. (0.1).		_	Key Algorithm:	RSA			
	State (ST):				Key Length:	4098			
	Locality (L):				Password:				
	Organization (O)								
	Organizational U	Init (OU):							
	Email:								
	* Valid From	31.08.	2021 10:46						
	* Valid Till:	31.08.	2041 10:46	Ē					
		Create Root CA	How to create a ro	ot CA					
:									Cancel
									Cancer

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.

image: certificates - Local Computer Trusted Root Certification Authonties] File Action View Help Image: Certificates - Local Computer Object Type Image: Certificates - Local Computer Object Type Image: Certificates - Local Computer Image: Certificates Image: Certification Authonities Enterprise Twatt Intermediate Certification Authonities Find Certificates Image: Trusted Reeple View Image: Trusted Reeple CurrentUser Image: Trusted Receple CurrentUser Image: Trusted Receple CurrentUser Image: Trusted Receple CurrentUser Image: Trusted Receple CurrentUser Image: Trusted Receple Receple CurrentUser Image: Trusted Receple Receple CurrentUser			 Right Trust ficati entry conte Selec Impo 	ed Root Certi- on Authorities to display the ext menu. t All Tasks > ort
 Fig. 3-7 ✓ Certificate Import Wizard Welcome to the Certificate Import Wizard Melcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certificate or to establish eacore network connections. A certificate store is the system area where certificates are kept. Store Location Current User © Local Machine To continue, dick Hext. 	>	Certificate Import Wizard File to Import Specify the file you want to import. File name: C:\User'Downloads\CAFolder\ca_DDM.crt Note: More than one certificate can be stored in a single file in the fo Personal Information Exchange= RKCS #12 (PFX,P12) Cryptographic Message Syntax Standard=RKCS #7 Certificates (. Microsoft Senaized Certificate Store (.SST)	Promse Nowing formats: P7B)	•



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

	← 😺 Certificate Import Wizard	×	←
	Certificate Store Certificate stores are system areas where certificates are kept.		Completing the Certificate Import Wizard
→	Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse	>	The certificate will be imported after you click Finish. You have specified the following settings: Certificate Store Selected by User Content Certificate File Name C:\Users\martin.keidel\Downloads\CAFolder\cs_DDM <<
	Next Next Cancel		Finish Cancel

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.

* Configurations - Dallmeier Device	Manager 1.0.10			×
Filter	Certification Authority			
🚓 Global	OpenSsl	Certification Authority	Subject Template	Issuer Template
System Configuration	Subject			
Revice Scanner	Alias:	System TLS		
E Report	* Country (C):	DE		
Advanced	State (ST):	Bayern		
Certification Authority	Locality (L): Organization (O):	Regensburg Dalmeier		
-	Organizational Unit (OU):	TechDoku		
	Email:	info@dallmeier.com		

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.

Create Certificates and A	sign to Network Services - E	Dallmeier Device Manager 1	1.0.10					×
OpenSSL Settings for Signing					Subject Settings			
OpenSsl Executable: Target Directory for Signin	C:\Program File:	:\OpenSSL-Win64\bin\openssl keidel\Downloads\CAFolder	l.exe	Browse	Alias: * Country (C): State (ST):	System TLS DE Bayern		
Target Directory for Signe	Issuer CA Root Certificate and Private Key				Locaty (): Regenskung Organization (0): Delimeer			
CA Certificate: CA Private Key:	C: \Users\martin.keidel\Down C: \Users\martin.keidel\Down	loads\CAFolder\ca_DDM.crt loads\CAFolder\ca_DDM.key		Browse Browse	Organizational Unit (OU): Email:	: TechDoku info@dallmeier.com		
CA Private Key Password:	•••••				Assign Certificate and Actival	te Network Service		
Issuer Information from Certifi CA Root Certificate		CA Root Key			David-TLS		HTTPS (only Cameras)	
Issuer Common Name (CN): Country (C): State (ST): Locality (L):	DDM DDM DE N/A N/A	Key Type: Key Algorithm: Key Length:	Private RSA 4096		Activate Network	Service A	Activate Network Service CamProxy for Tunneling (only Recor Assign Certificate Activate Network Service	ders)
Organizatori (U): Organizational Unit (OU) Email: Valid From: Valid Till:	N/A N/A 20.07.2021 11:56			В	Delete 'Signing Reques	st' after signing d Certificates' after import		
Issuer Validity Days 1096 🗘			Validity in years 3 🗘	Apply				
* mandatory							(OK Cancel

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.

Elle Edit Yiew Options Logging 1	‱s ⊞elp ¢ ⁰ Ω↓	↑ @ ()	× 🖿	🖹 49 🔜 (≥ 🗊 🖄 🖳							
Summary Dash Board	System	TLS Cert	ificate Assignment					Pro	operty View			88
Device Name IP/DNS Addree	MAC Address	Deri	-1110							vslue	Cameras	Î
HD-DN	Secure Stric	Service		Path ID	Alias		Used By	Valid From	1	Valid Io		
		. 🕑 I	https	CP-2	DallmeierDM_2	0.07.2021 17:04:4	14 https david_tl	s 20.07.2021	15:04:44			1054 days
		- 🥑 (david_tls	CP-2	DallmeierDM_2	0.07.2021 17:04:4	14 https david_tl	s 20.07.2021	15:04:44			1054
									Time Zone Time Supr	CX Europ	e/Berlin	
									Time Sync Statu Network Services David (Port 300	s 2		
faretes.						New Self-Sinned Certificate	Trasta Gonino Dan wet Demova C	ertificate Aminoment	David-TIs (Port Https (Port 443)	29999) 🗸		
-Justier									RTSP (Port 554)	2		
Broadcast Scanner IP Scanner (1) X + 04	wif Device Scanner						18100 UV	e View			101.00
NEC: Vien 150 (10. 150. 0.65)	Scan Network			Pilter Settings: No Filter				R				
Device	* Group Path	IP/DNS Address	MAC Address	Firmware Version	Serial Number	Status Ima	ıge					
CF5200HD-DN			00:06:02:53:16:05									
CF4900HD											2	
DF4510HD			00-08-02:50:33:7F									
DDZ4230-HD												
00Z4220-HD												
DDZ4120-HD Count: 23 (Selected Count: 1)									Live View	r fir	mware Update	Exp < (>)
											System Memory:8.91	GB free from 15.94 GB

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.

International Note Note Note Note Note Note International of the NASS 10 NASS 10 Note Name Note	Ele Edit View Options Logging	Teols Help ∣ ∧⁰ Ω ↓	ிலிடை	× 🖿 🖻	{ •	> ■ . ♥ ℝ.						
The number Type	Summary Deeb Board	- ** /- *								Property View		
Image: State 1	Name A	IP/DNS Address			ion Maintenan	ce End Secial Number	MAC Address			System Properties	Cameras	
************************************			ics beine	10012020602		Director 13374340	046404044					
0 000000000000000000000000000000000000			secure strict - virtuarcam							 Device Settings 		
•••••••••••••••••••••••••••••	💙 🛄 IP:10.130.50.11									IP/DNS Address	10.130.50.116	
Image: State in the State	💙 🔲 IP:10.130.50.110									 Device Login Settings 		
Image:	2 III III III III III III		Samue Strict Midwalface	100:30300602			52/56/2020/204			TLS		
MAXXA112 MAXXA112 MAXXA11										User Name	• Secure	
Image: Provide and Prov	IP:10.130.50.112	10.130.50.112	Secure Strict VirtualCam	1.0.0.1.20200602		DVC001-13374351	52:56:42:42:43:6f			User Password	<u>∕</u> k	
Image: Control of the state of the stat	🥝 🛄 IP:10.130.50.113	10.130	ACCORD.	1.0.0.i.20200602						Device Information	Dallmaiar Recorder/Camera	
Image:	2 III IP-10 133 50 115			10.0 ; 20200502		DV/C001-13374354	52-56-42-42-43-72			150 116	Dallmeier electronic GmbH & C	
Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image:		<i>.</i>								011.00.00	VirtualCam	
•••••••••••••••••••••••••••••	S [10:10.130.50.116	ç li	nactive	1.03.20200602			52.5643.05 0.00			10.130.50.116 🖊	The Internation	
Image: Control of the Control of th	🕗 💽 IP:10.130.50.117 🔪			1.0.03.20200602			² D	I in C-min				
Image: Strate Strate No.000-111 No.	Imil 10:100.50.118	10.130		1.0.0.1.20200602		DVC001-13374357	Devi	ce Login Settings				
 								15		•14 Inactive		
with 10,80,20	P:10.130.50.119		inactive VirtualCam	10.03.20200602		DVC001-13374358	~			- indeave		
Image: Processing of the Status Name (New Construction of the Status) Name (New Construction of the Status) Name (New Construction of the Status) Image: Processing of the Status Name (New Construction of the Status) Image: Processing of the Status Name (New Construction of the Status) Image: Processing of the Status Name (New Construction of the Status) Name (New Constructio	💙 🛄 IP:10.130.50.12						52: L	.ogin Mode		• TAS Secure		
•••••••••••••••••••••••••••••	💙 🔲 IP:10.130.50.120						52 L	lser Name				
Marked Market Ma	III IB-10 120 50 121		learthea VirtualCare	10.0120200502							N	
Operation Operation <t< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Jser Password</th><th></th><th>•••••</th><th>× _</th><th></th></t<>								Jser Password		•••••	× _	
No. 00.000 No. 00.0000 No. 00.00000 No.	IP:10.130.50.122		Inactive VirtualCam	1.0.0.7.20200602		DVC001-13374361	52:50					/
Deck Court Dit (Selected 1) Understand 1 (Selected 2) Understand 1 (Selected 2) Understand 2 (Selected 2) Unde	💙 🛄 IP:10.130.50.123									David-TIs (Port 29999)		
Normal Science Openance (1) N <th>Device Count 891 (Selected 1) Infine</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>000</th> <th>RTSP (Port 554)</th> <th>v ⊻</th> <th></th>	Device Count 891 (Selected 1) Infine								000	RTSP (Port 554)	v ⊻	
Witchest Statum Witchest S	Device Scanner								21.50	Live View	-	
NE: Ne: <th>Broadcast Scanner IP Scanner</th> <th>(II) × +</th> <th>Onvif Device Scanner</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	Broadcast Scanner IP Scanner	(II) × +	Onvif Device Scanner									
Deck: * Group Path 10/06/ 54/eres Numerar Version Serial Humber State Image 10 15/300-0PM 10/05/ 54/20 0.00/02/31/60 5.33.2x 0.00/07/20/200 Image Imag	NEC: Vien150 (10.150.0.65)	Scen Networ		rit	er Settings: No Filter	~			n B B O M			
1 (15)00-04 10.150.123 000x01551/h8 13.32x 0+00174002056 1 (16)00-05 10.150.123 000x01551/h 4.11.7x 0+0005 110067 1 (16)00-05 10.150.13 000x01551/h 4.41.4 0+0005 110067 1 (16)00-05 10.150.13 0.021 01031/h 0.001 01011/h 0+000 110067 1 (2025H0 10.150.122 0.424000000 10.150.123 0+014 0200000 1 (2025H0 10.150.122 0.4360.16464 92.03 0+014 0200000 10.150.122 0+014 0200000 1 (2022H0 10.150.123 0.4360.16464 92.03 0+014 0200000 10.150.122 0+014 0200000 1 (2022H0 10.150.123 0.4360.16464 92.03 0+014 0200000 10.150.122 0+014 0200000 1 (2022H0 10.150.123 0.4360.16464 92.03 0+014 0200000 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.150.126 10.	Device	* Group Path	IP/DNS Address	MAC Address Fi	rmware Version	Serial Number		Status Image				
Construint Constru	DF5200HD-DN			00:06:02:53:16:05 8.								
Image: Control Contro Control Contrecontrol Control Control Control Control Control Con	-											
■ # #1080 USU 00000000000000000000000000000000000	OF4900HD OF4900HD									<pre></pre>		
ECX203H0 10.150.123 285Necd46H 82.03 PH019-500H194 ECX203H0 10.150.12 eLineK0646 82.03 PH019-500H194 eCX203H0 eCX20H0	DF4510HD											
	DDIZ4230-HD											
Interactive Interactive Interactive												
1 (2010)-10 (201				042194303015 9.		0H018-3200/4438						
	DDZ4120-HD Count: 23 (Selected Count 1)			c4:2f:90:19:ef:d4 9.						Live View	Firmware Update	Exp < 1
System Memory: 7.60 GB free from 15.94 G											System Memory: 7.60 GB 1	ree from 15.94 G

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.

Ele Edit View Options Logging	Tools Help										
▐▆▐▀▐▀▌▐▓▏▏▐▋	∣ ☆° ♀ ↓	· ^ 🗈 🛍	🗙 🗁 🖹	🔸 🖪	≥ 💷 🖄 🖾						
Summary Dash Board	System								Property View		
Name	ID/DNS Address				re End Savial Number	MAC Address			A System Properties	Cameras	
									Property		
💙 🛄 IP:10.130.50.100		iecure Strict VirtualCam	1.0.0.1.20200602			52/56/42/42/43/63					
Image: 10 100 100 100 100 100 100 100 100 100		acure Strict - VirtualCare	10.0120200602		DWC001-12174240	52564254254264					
									IP/DNS Address		
🖌 💽 IP:10.130.50.102									 Device Login Settings 		
🕑 🛄 IP:10.130.50.103		iecure Strict VirtualCam	1.0.0.20200602		DVC001-13374342	52:56:42:42:43:66			Login Mode	User Login	
IP-10 133 50 104		ierure Strict - VirtualCam	10.0120200602		DVC001-13374343	5255642424243457			UserName	admin	
<u> </u>			_						User Password		
🕗 🛄 IP:10.130.50.105 🏒	000	ire stites	1,0,0,1,20200602						Device information		
	<u> </u>								Device Category	Dalimeier Necolue/Camera Dalimeier alastarais Grabbil & C	
			200002			52/56/42/42/43/69			Device Type	VirtualCam	
🖉 🔲 (P-10 13) 4	Secu	ire Strict	firtual Common						Serial Number	DVC001-13374346	
		ine ounce	and any second						Firmware Version	1.0.0.1.20200602	
🖌 💽 IP:10.130.50.1	<u> </u>		1020602							52:56:42:42:43:6e	
🕑 🛄 IP:10.130.50.109	10.130.00		1.0.03.20200602		DVC001-13374348	52:56:42:42:43:5c			Maintenance End		
Image: 100 (100 (100 (100 (100 (100 (100 (100			10012020002			5256424242426					
									Last Device Scan		
IP:10.130.50.110									Overall Status		
									 Time Information 		
🕑 🛄 IP:10.130.50.111		iecure Strict VirtualCam	1.0.0.20200602			52:56:42:42:43:6e			Time Zone	Europe/Berlin	
IP-10 130 50 112		incure Strict VirtualCare	10.0320200602			52-56-42-42-43-44			Time Sync		
-ve									With work Services		
IP:10.130.50.113									David (Port 30000)		
									David-Tis (Port 29999)	2	
💙 🛄 IP:10.130.50.115		iecure Strict VirtualCam	1.0.0.1.20200602		DVC001-13374354	52/56/42/42/43/72			 Https (Port 443) 	V	
Device Count 891 (Selected 1) China								00	RTSP (Port 554)	V	
										_	
Device Scanner									DO LA LIVE VIEW		
Broadcast Scanner IP Scanner	W X +	Onvir Device Scanner									
NIC: Vian 150 (10.150.0.65)	Scan Network			Settings: No Filter	~			R 4 0	¢.		
Device	Group Path	IP/DNS Address	MAC Address Firm	nware Version	Serial Number		Status Image				
DF5200HD-DN			00:06:02:53:16:05 8.5.								
C DF400HD					DHD90-12345678						
0F4510HD											
0.0074220-MD											
_											
DDZ4220-HD					DHD18-520074438						
ODZ4120-HD									Theo More	Genuenes Hedate	Sec. 115
Count: 23 (Selected Count 1)									Live Yes	Contractive Operate	- the state
										system Memory: 7.74 GB fr	ee moen 15,94 G

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.

Eile Edit View Options J	ogging Tools														
	6 3		↑ Ba fà	🗙 I 🖿 🖬	a 🗆 👫 📃 🥅	@ 🗐 🌣 🖻									
Summary Dash Soard		System			× /								Property View		
Junior y Cash Courte		STREET.	150	ruikate overview									System Properties	Cameras	
Device Name	IP/DNS Addre	ns * TLS	MAC Address	Device Type	Cert ID	Alias	Path ID	Used By		Organization	Common	Locality	Property		
▼ Ø □□□□ IP:10.2.101.83													 Device Settings 		
													User defined Name		
						rDM_20.07.2021 18:24:25									
													 Device Login Settings 		
													Login Mode	Group Login	
													Device Category		
													Manufacturer	Dalimeier electronic GmbH &	Co.KG
													Device Type	IPS-10000	
													Serial Number	DAX5-10210183	
													Firmware Version	9.7.10 (SP:abdeh)	
													MAC Address	90:1b:0e:de:7b:a2	
													Maintenance Start	23.02.2020 00:00	
													Maintenance End	22/07/2022 00:00	
													Status Information		
													Last Device Scan	04.06.202109536	
													 Time lefermation 		
													Time Zoos	Europa/Partin	
													Time Supr	curope berni	
										_			Time Sync Status		
													* Network Services	_	
													David (Port 30000)	V	
										/			David-Tls (Port 29999)	V	
									_ //	<i>,</i>			RTSP (Port 554)	V	
I •													ork Interfaces		
Refresh Certificate Information									te Al	Import	Root Cei	runcate			
Device Scanner											~		- / /		
Broadcast Scanner IP	Scanner (1)	< + o	wif Device Scanner									(m)//	//		
NEC: Vien150 (10.150.0.65)		Scan Network			Pilter Settings: No Pilter										
Device		Group Path	IP/DNS Address	MAC Address	Firmware Version	Serial Number		Status	Image			^			
OF5200HD-DN															
C DF4510HD															
D0Z4230-HD															
D0Z4220-HD						DHD18-520074438									
0074120-HD				of 2600 10 whold		DHD14-0000009									
Count: 23 (Selected Count 1)													Live View	Firmware Update	Exp ()
														System Memory: 7.67 GB	free from 15.94

Fig. 3-20

Click Import Root Certificate.

The Root Certificate Import dialog is displayed.

Eile Edit View Options Logg	ging Tools <u>H</u> el	¢ Ω↓	↑ 60 (â	× 🖿	े । 49 🛛 🗔	@ 🗊 🖄 🖏									
Summary Dash Board		System	TLS Ce	srtificate Overview	×								Property View		
													System Properties	Cameras	
Device Name II	P/DNS Address	 TLS 	MAC Address	Device Type	Cert ID	Alias	Path ID	Used By	CA	Organization	Common	Locality	Property		
▼ 2 000 10:2.101.83 10.2													 Device Settings 		
					CT-3 Dalimeter	DM 20.07/2021 18/24/25 C	P-3 cami	proxy[david_tls		Dallmeier		Regensburg			
					CT-1 DDM 201	Root Certificate Imort	 Dallmeier Device 	e Manager 1.0.10		×					
						Select CA Post Certificate									
													Login Mode		
						CA Root Certificate:							User Password		
						C: (Jsers (nar tri)Download	ds\CAFolder\ca_DDI	M.at					 Device Information 		
													Device Category	Dallmeier Recorder/Camera	
													Manufacturer	Dalimeier electronic GmbH 8	Co.NG
						CA Root Certificate Informa	8an						Device type	DAVE 10310182	
													Emuran Version	0.7.10 (SP shots)	
							DOM						MAC Address	90-1b-0a-da-7b-a2	
						Common Name (Ch):	DOM						Maintenance Start	23.02.2020.00-00	
							pe						Maintenance End	22.02.2022 00:00	
						State (ST):	NA						* Satus Information		
						Locality (1.):	NUS						Last Device Scan	04.05.2021.09.36	
							IN CO.	_	_				Overall Status		
						Organization (0):	N/A	_	_				 Time Information 		
						Organizational Unit (OU): N/A							Europe/Berlin	
							N/A								
						Valid From:									
							20.07.2041.114								
						Tens Inc.							David (Port 30000)		
													David-TIs (Port 29999)	<u> </u>	
(H)													RTSP (Port 554)	2	
Refresh Certificate Information											Inpo		 Network Interfaces 		
Dentes Commen															
Broadcast Scanner IP Scan	nner(1) 🗙	+ 04	vif Device Scanner										Live view		
NEC: Vien150 (10.150.0.65)	~ R	Scan Network			Pilter Settings: No Pilter						R	9 O 48			
Device	▼ Gro	up Path	IP/DNS Address	MAC Address	Firmware Version										
OF5200HD-DN														-	
0F4900HD						DHD90-12345678									
DF4510HD															
DDZ4230-HD															
00Z4220-HD						DHD18-520074438									
D074120-HD				e4/25/90:19:e5:d4		DHD14-0000009									
Count: 23 (Selected Count 1)													Live View	Firmware Update	Exp
														System Memory: 7.53 G	B free from 15.94

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.

Elle Edit View Options Logging	Tools Help		.	⊳								
	1 8 1 12	<u> </u>	\sim	E ••	60	° 🖙 🛎 🖼						
Summary Dash Board	System									Property View		
Name *										System Properties	Cameras	
10 120 52 1-10 120 52 1 171												
										 Device Settings 		
Dashboard Counting										User defined Name	IP:10.130.112.52	
-										IP/DNS Address		
DMVC2										* Dence Login Settings		
ESX-Recorder Prüffeld										Login Mode	User Login	
										User Name	admin	
 Kamera_68oox 										User Password		
* / lechDok										Device Category		
IP:10.130.112.52		Web Configuration		Ctrl+W							Dallmeier electronic GmbH &	
										Device Type	SRS-VM 10000	
🧭 🛄 IP:10.130.50.114		* Refresh Device Info					52:56:42:42:43:71			Serial Number	DVM4-00000261	
. In		. Software !!		_Ctrl+U						Firmware Version	9.15.10 (SP:a6d)	
r itsi			11							MAC Address	000002814/04/04	
Test License Kamera	/	ring IP a	address							Maintenance start	02.12.2019 00:00	
					\					* Satur Information	02.10.2020 00:00	
Test Maintenance Angela										Last Device Scan	04.08.2021 09.36	
> Test Wittmann Seconder		NetConf	ig3							Overall Status		
_			~		/							
Test_RecordingInfo		<u> </u>									Europe/Berlin	
		a dyance	ed									
+ UpDate		Netwo										
> •										 Network Services 	-	
_										David (Port S000)		
IP:10.2.126.25						DHID156-00419409				RTSD (Part 554)		
Device Count 891 (Selected 1)		😨 Copy (Cell)							00	* Network Interfaces		
Device Scanner		Rig Copy								Live View		
Broadcast Scanner IP Scanner												
NEC: Vien150 (10.150.0.65)	Scen Ne	🔚 New Group			No Filter	~			R 9 0 4			
Device	* Group Path				ersion	Serial Number		Status Image				
OF5200HD-DN												
CF4900HD		Collapse All Root Items	0000802:5000418	40.1./.rc								
DF4510HD												
D0/24230-HD												
00Z4220-HD												
00Z4120-HD										Line Mean	Generate Hedate	Sec. 115
Count: 23 (Selected Count 1)										LOVE YIEW	Control Manager 2 42 62	Exp III
											any states plantery (7.47 Ge	1001100110.94 08



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

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



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

Fig. 3-23

The configuration interface of the recorder is displayed:

Dallmeier Netconfig 3 - 10.2.101.83				– 🗆 🗙
Logged in as Administrator			GPU Usage: 0%	CPU Usage: 3%
	Close Recording Ne	twork System Interfaces		
	Recording			
	Camera Timer	Areas HDD Management		
	Camera Descriptions	Search Criteria		
	Protect tracks	Reference Images		
	MaxAge			
				e more.

Fig. 3-24

Select Recording > Cameras / Tracks.

The camera configuration of the recorder is displayed:

Dallmeier Netconfi	g 3 - 10.130.112.52							-		×
Recording Settings	(100 channels activated)								
Cameras	Analysis									
	D. CO									
	Di 😱	Com 1								
	Di (C)	Call I								
	Di ஸ	Expert Mode								
	•••	Recording Mode		Settings						
	D (Permanent			Quality					
	Di 😱									
			Timer	Protection						
	Di (1)									
	Di 💽	Set marker on Camera Contact	odress		10.130.50.115		-			
	Di (1)		Protocol							
	Di 😱				No TI S (DaVid)			.))		
	Di (1)		User name		TLS only (David)					
			Assword		TLS only (Davids	/ 2) -		//		
			aphono -		TES SILICI (DITAID	" b				
					a					
				Encoder	1	\sim				
	D O									
				Eisheve						
	B (0)									
		Apply to all Dallmeler HD-IP of this model			√ ¢	K 🔮 Cancel				
	D									
V/A Bit rate	15Mbps (Max	:: 480Mbps) NetIF1 1	5Mbps (Max: 1000Mbps)			¢ ^o Sett		√ок	Ja Gan	

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 Proper-ties**.



Ele Edit View Options Logging	Tools Help								_			
B 🖻 💾 🕄 🛛 🕄	∳ ⊅		è G ×	🗁 🖹	4y 🛛 🕄 🕗 🛛	B 🛎 📴 👘						
Summary Dash Board	System								Network Services			
Name *	IP/DNS Address		Device Type	Firmware Version	Maintenance En:	Serial Number	MAC Address	5	David (Port 30000)		✓	
Pin 130.50.109			VirtualCam	1.0.0.1.20200602		DVC001-13374348	52:55:42:42:43:56	e ok	David-TIs (Port 299		v	
P:10.130.50.11				1.0.0.120200602			52:56:42:42:43:0	• OK			-	
P:10.130.50.110			VirtualCarn	1.0.03.20200602		DVC001-13374349	52:56:42:42:43:6	d OK	Https (Port 443)		×	
2 IP:10.130.50.111			VirtualCam				52:56:42:42:43:6	e OK	RTSP (Port 554)		✓	
IP:10.130.50.112							52:56:42:42:43:6	OK	Http (Port 80)		✓	
IP:10.130.50.113								0 OK	Network Interfaces			
🥝 📑 IP:10.130.50.115		Secure Strict		1.0.03.20200602 Ctrl+V	N/A			2 OK	Including interfaces			
🥝 👥 IP:10.130.50.116		4+ Refresh De									furone/Retin	
💙 💽 IP:10.130.50.117		Reboot								Time	52	
🤗 💽 IP:10.130.50.118		🖌 🏟 Ping IP ad	ldress	Ctrl+F						Iime Sync Str Vetwork Services	10	
🥝 🛄 IP:10.130.50.119	10.130.50.119		C-++i		<u>`</u>	DVC001-13374358				David (Port 30000) David-Tis (Port 29999)		
🥝 🛄 IP:10.130.50.12	10.130.50.12		nse setui	ngs		251	52:56:42:42:43:0	ь ок		Https (Port 443)		
IP:10.130.50.120	10.130.50.120			ings	P IP Netwo	В			e Assignment (Sensis	Http (Port 80)	v V	
IP:10.130.50.121	10.130.50.121	N 11	C-112		TLS Centi TLS Centi	Selfs	TIS	Certificat	te Overview, Root Import a	nd http://		
🔮 🛄 IP:10.130.50.122	10.130.50.122	User	settings	moma	TLS Netw	ork Services (Er				AC Address Subnet Mask)	52:56:42:42:43:72 10.130.50.115 (255.255.0.0)	
IP:10.130.50.123		🖌 😡 Copy (Cell	0	Ctrl+0		t Certificate Co	TLS	Network	Services (Enable/Disable)	R Charles		
Device Count 891 (Selected 1) Traine		BB Copy			hift+C Network	Interfaces Info	TLS	Direct Ce	rtificate Connection Info	Link: Speed (Duplex N	tode) No Link (unknown)	
Device Scanner		× Delete Iter	m	Del	a			_		etten		
Broadcast Scanner IP Scanne	r(1) 🗙 +	New Devic	ce/System	Ctrl+[
NIC: Vien 150 (10.150.0.65)	Scen Netwo				o filter	~						
Device	- Group Path	E Collapse A 10.150.12.3	VI Root Items 00:0h:	02:53:16:05 8.5.3.2	on Ser	10117-00226745		Status	mage			
			00-08-		lee DH	Dan. 12345678						
			00.08	03602275 6464		0102-12245679						
		10110123										
				DECOMPANY 9/2/0.5	UH	019100241794						
0024220-HD			o4:21:5	9.2.0.	DH	018-520074438						
Count: 23 (Selected Count 1)				9.2.0.19tettd47 9.2.0.1	DH	014-00000009				Live View	Firmware Update	Exp (1)
TLS Network Services (Enable/Disable)												

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.

Elle Edit View Options Logging Te	ws⊞ep ∦ ⁰ D J	↑ Ba £≏	24			_				
			5					Property View		
Summary Cash Board	System	· ·						System Properties	Cameras	
Device Name IP/DNS Addin	ess TLS									-
Z		Http Port	Https Port	David Por	t DavidTls Port	R tsn Po	rt 🔪	 Device Settings 		
_	(IP	πωγιοιί	Inception		C Davians Forc	Rtap Pol		User defined Name		
	(Cam		- 🛃 N	12 📿 2	0000		554 //	 Device Login Settings 		
				" V J		· · · · ·				
		. —						Login Mode		
									Dallmeier Recorder/Camera	
								Device Type	DF5300HD-DN	
									00:06:02:40:21:56	
								Time Zone	Europe/Berlin	
									⊻	
								Time Sync Status		
								 Network Services 		
								David (Port 30000)	<u>-</u>	
								id+TIs (Port 29999)	<u>×</u>	
Defects								(Port 443)	2	
kerresn							Configure Network Services	[ort 554]	<u>×</u>	
Dender Courses										
Device Scaliner							R			
Broadcast Scanner IP Scanner (1)) X + -	Onvif Device Scanner								
NEC: Vien150 (10.150.0.65)	Scan Network			Pilter Settings: No Filter				30		
Device	* Group Path	IP/DNS Address	MAC Address	Firmware Version	Serial Number	Status	Image			
DF5200HD-DN										
			00.08.03.50.06.19		DUD00 12245679					
										i i i
DF4510HD			00:08:02:50:33:7F		DHD102-12345678					
00Z4230-HD										
00Z4220-HD										
D0Z4120-HD										
Count: 23 (Selected Count 1)								Live View	Firmware Update System Memory:7.73 GB free	Exp (1) (from 15.94 GB
Fig. 3-28										

Click Configure Network Services.

The Network Services Settings dialog is displayed.



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

Fig. 3-29

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

www Network Services Settings - Dallmeier Device Manager 1.0 🗙									
Protocol:	David (Port 30000)								
Enable/Disable	David TLS (Port 29999)								
	Http (Port 80)								
If you are connected with the David p protocol. The same applies to the Davi	Https (Port 443)								
so you can't lock yourself out.	Rtsp (Port 554)								
	DMVC (Port 3377)								
	DMVC TLS (Port 3443)								
	OK Cancel								

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

Fig. 3-30

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