

REV. 1.0.0 | 2021-10-25

KONFIGURATION

# DALLMEIER DEVICE MANAGER



VERBINDUNGEN VON KAMERAS, RECORDERN UND CLIENTS IM NETZWERK VERSCHLÜSSELN UND ABSICHERN



Copyright © 2021 Dallmeier electronic GmbH & Co.KG

Weitergabe sowie Vervielfältigung dieses Dokuments, Verwertung und Mitteilung seines Inhalts sind verboten, soweit nicht ausdrücklich gestattet. Zuwiderhandlungen verpflichten zu Schadenersatz.

Alle Rechte für den Fall der Patent-, Gebrauchsmuster- oder Geschmacksmustereintragung vorbehalten.

Der Hersteller übernimmt keine Haftung für Sach- oder Vermögensschäden, die aus geringfügigen Mängeln des Produkts oder geringfügigen Mängeln in der Dokumentation, z. B. Druck- oder Schreibfehler, entstehen und bei denen der Hersteller nicht vorsätzlich oder grob fahrlässig handelt.

Darstellungen (z. B. Screenshots) in diesem Dokument können vom tatsächlichen Produkt abweichen. Änderungen der technischen Daten ohne Vorankündigung vorbehalten. Irrtümer und Druckfehler vorbehalten.

Mit <sup>®</sup> gekennzeichnete Marken sind eingetragene Marken von Dallmeier electronic.

Mit \*<sup>)</sup> gekennzeichnete Marken sind Marken oder eingetragene Marken folgender Eigentümer: Microsoft, Microsoft Edge und Windows von Microsoft Corporation mit Hauptsitz in Redmond, Washington, USA;

Die Nennung von Marken Dritter dient lediglich Informationszwecken.

Dallmeier electronic respektiert das geistige Eigentum Dritter und ist stets um die Vollständigkeit bei der Kennzeichnung von Marken Dritter und Nennung des jeweiligen Rechteinhabers bemüht. Sollte im Einzelfall auf geschützte Rechte nicht gesondert hingewiesen werden, berechtigt dies nicht zu der Annahme, dass die Marke ungeschützt ist.

Darüber hinaus sind die nachfolgend aufgeführten rechtlichen Hinweise zu dem in diesem Dokument beschriebenen Produkt bzw. der zugrunde liegenden Software zu beachten:

Dieses Produkt enthält Software, die vom OpenSSL Project für die Verwendung im OpenSSL Toolkit entwickelt wurde (http://www.openssl.org/). Dieses Produkt enthält von Eric Young (eay@cryptsoft.com) geschriebene kryptografische Software. Dieses Produkt enthält von Tim Hudson (tjh@cryptsoft.com) geschriebene Software.

Teile dieser Software basieren auf der Arbeit der Independent JPEG Group.

# **INHALTSVERZEICHNIS**

KAPITEL 1:	EINFÜHRUNG	4
1.1	Gültigkeit	4
1.2	Dokumente	4
1.2.1	Dieses Dokument	4
1.2.2	Mitgeltende Dokumente	4
1.3	Darstellungskonventionen	5
1.4	Rechtliche Hinweise	5
KAPITEL 2:	ALLGEMEINE HINWEISE	6
2.1	Bestimmungsgemäße Verwendung	6
2.2	Weitere Features und Funktionen	7
2.3	Gewährleistung	7
KAPITEL 3:	TLS-KONFIGURATION	8
3.1	Empfohlene Vorgehensweise	8
3.2	Übersicht	9
3.2.1	TLS-Werkzeuge	9
3.2.2	TLS-Konfiguration und -Verwaltung	10
3.3	Zertifizierungsstelle	11
3.4	Verbindungen verschlüsseln	18
3.5	Recorder-zu-Kameras Verbindungen	21
3.6	Unsichere Ports deaktivieren	26

# EINFÜHRUNG

## 1.1 GÜLTIGKEIT

Dieses Dokument ist gültig für die Software Dallmeier Device Manager in der Software-Version 1.0.10.

Abbildungen (Screenshots) in diesem Dokument können vom tatsächlichen Produkt abweichen.

## 1.2 DOKUMENTE

Die Produktdokumentation zur jeweiligen Software umfasst verschiedene Dokumente, die gedruckt und/ oder in digitaler Form, beispielsweise über die Webseite www.dallmeier.com, bereitgestellt werden.

Lesen Sie die gesamte Produktdokumentation zu Ihrer Software sorgfältig und vollständig, bevor Sie diese verwenden. Beachten Sie immer die enthaltenen Anweisungen, Hinweise und Warnungen sowie die technischen Daten in der aktuell gültigen Produktspezifikation.

Bewahren Sie alle gedruckten Dokumente zu Ihrer Software in einem gut lesbaren Zustand und an einem geeigneten Ort auf, um ein späteres Nachschlagen zu ermöglichen. Archivieren Sie digitale Dokumente zu Ihrer Software (z.B. die technische Produktspezifikation) auf einem geeigneten Speichermedium. Prüfen Sie regelmäßig die Webseite www.dallmeier.com auf mögliche Aktualisierungen der Produktdokumentation sowie der jeweiligen Software-Versionen.

## 1.2.1 Dieses Dokument

Das Dokument "Konfiguration" (dieses Dokument) enthält detaillierte Beschreibungen zur Konfiguration und Bedienung der oben aufgeführten Software.

Zielgruppe dieses Dokuments sind geschulte Systemintegratoren (Errichter von Videosicherheitssystemen).

## 1.2.2 Mitgeltende Dokumente

## Produktspezifikation

Die Produktspezifikation enthält detaillierte technische Daten, Leistungsmerkmale und Eigenschaften der jeweiligen Software.

Zielgruppe des Dokuments sind geschulte Systemintegratoren (Errichter von Videosicherheitssystemen).

## Technische Mitteilung

Das Dokument "Technische Mitteilung" enthält Informationen zu Neuerungen und Änderungen, die mit dem jeweiligen Update der Software-Version eingeführt werden.

## 1.3 DARSTELLUNGSKONVENTIONEN

Zur Verbesserung der Übersichtlichkeit und Lesbarkeit dieses Dokuments werden verschiedene Textformatierungen und Hervorhebungen verwendet:

## ACHTUNG

*ACHTUNG* kennzeichnet Maßnahmen zur Vermeidung von Geräte- und/oder Sachschäden durch unsachgemäße Konfiguration des Geräts oder fehlerhafte Bedienung.

Handlungsanweisungen sind durch Pfeile (▶) gekennzeichnet.

Führen Sie Handlungsanweisungen stets in der beschriebenen Reihenfolge aus.

**Ausdrücke**, die fett und dunkelgrau hervorgehoben sind, beziehen sich in der Regel auf den Namen einer Anwendung, eines Produkts oder einer Funktion oder weisen auf ein Bedienelement der webbasierten grafischen Benutzeroberfläche hin (Schaltfläche, Checkbox, Drop-down-Liste, Menüpunkt etc.).



Kursiv formatierte Absätze bieten Informationen zu Grundlagen, Besonderheiten und effizienter Vorgehensweise sowie allgemeine Empfehlungen.

## **1.4 RECHTLICHE HINWEISE**

Beachten Sie die unten aufgeführten rechtlichen Hinweise zu dem in diesem Dokument beschriebenen Produkt bzw. der zugrunde liegenden Software:

- Dieses Produkt enthält Software, die vom OpenSSL Project für die Verwendung im OpenSSL Toolkit entwickelt wurde (http://www.openssl.org/).
- Dieses Produkt enthält von Eric Young (eay@cryptsoft.com) geschriebene kryptografische Software.
- Dieses Produkt enthält von Tim Hudson (tjh@cryptsoft.com) geschriebene Software.
- Teile dieser Software basieren auf der Arbeit der Independent JPEG Group.

Lesen und beachten Sie in diesem Zusammenhang auch die im Info-Dialog Ihres Geräts bereitgestellten Lizenztexte zu sonstigen auf Ihrem Gerät verwendeten Third-Party-Softwarekomponenten.

# **ALLGEMEINE HINWEISE**

## 2.1 BESTIMMUNGSGEMÄSSE VERWENDUNG

Dallmeier Device Manager (DDM) ist eine leistungsfähige Applikation für die komfortable Konfiguration und Verwaltung umfangreicher VideoIP-Systeme von Dallmeier. DDM scannt das Videonetzwerk nach Dallmeier-Geräten, erkennt diese automatisch und stellt sie in einer Übersicht bereit. Dadurch können sowohl Kameras als auch Aufzeichnungssysteme komfortabel verwaltet werden. Die umfangreichen Funktionen reichen von der Änderung von IP-Adressen über Updates der integrierten Software bis hin zur direkten Öffnung der Konfigurationsdialoge.

Darüber hinaus stellt DDM in der aktuellen Version alle Werkzeuge bereit, um die Netzwerk-Kommunikation zwischen Dallmeier Aufzeichnungssystemen, Kameras und Workstation-Clients mittels Transport Layer Security (TLS) zu verschlüsseln.

TLS ist ein Mechanismus zur Verschlüsselung der Daten, die über das Netzwerk gesendet oder empfangen werden. Die übertragenen Daten sollen durch die Verschlüsselung vor unbefugtem Zugriff Dritter und vor Manipulation oder Fälschung geschützt werden.



Der Ablauf eines TLS-Verbindungsaufbaus besteht in vereinfachter Form aus folgenden Einzelschritten. Im ersten Schritt des Verbindungsaufbaus weist sich der Server gegenüber dem Client mit seinem Zertifikat aus. Der Client validiert die Vertrauenswürdigkeit des Zertifikats und prüft unter anderem, ob der Servername mit dem Servernamen des Zertifikats übereinstimmt. Optional kann sich der Client gegenüber dem Server mit einem Zertifikat ausweisen. Im letzten Schritt leiten die beiden Kommunikationspartner mit dem öffentlichen Schlüssel des Servers einen Sitzungsschlüssel ab.

## 2.2 WEITERE FEATURES UND FUNKTIONEN

- Kompatibel mit allen Dallmeier Aufzeichnungssystemen
- Kompatibel mit allen Panomera<sup>®</sup> Multifocal-Sensorsystemen
- Kompatibel mit allen Dallmeier Netzwerkkameras
- Unabhängige Definition von virtuellen Systemen
- Definition von Kameragruppen in einem System
- Einstellung der IP-Adressen
- Durchführung von Updates

# 2.3 GEWÄHRLEISTUNG

Es gelten die bei Vertragsabschluss gültigen Allgemeinen Geschäftsbedingungen (AGB).

# **TLS-KONFIGURATION**

Der Dallmeier Device Manager (DDM) stellt alle notwendigen Werkzeuge bereit, um Netzwerk-Verbindungen von Dallmeier-Geräten (Kameras, Recorder, Workstations-Clients) über das Standard-Protokoll Transport Layer Security (TLS) zu verschlüsseln und die dafür erforderlichen Zertifikate zu verwalten.

## 3.1 EMPFOHLENE VORGEHENSWEISE

Folgende Reihenfolge der Installationsschritte und Vorgehensweise wird bei einer Einrichtung von TLS-Verbindungen in einem Netzwerk empfohlen:

- **1.** Erstellen Sie mit dem Dallmeier Device Manager ein selbst-signiertes Root-Zertifikat und richten mit diesem eine Zertifizierungsstelle (Certificate Authosity, CA) in DDM ein.
- 2. Erstellen Sie nun Signierungsanfragen für Kameras, lassen diese durch die DDM-CA signieren und laden die daraus resultierenden Zertifikate auf die Kameras.
- 3. Importieren Sie das unter Punkt 1 erstellte Root-Zertifikat auf Ihre Aufzeichnungssysteme.
- **4.** Aktivieren Sie in Kameras (HTTPS 443, DaVid-TLS 29999) und Aufzeichnungssystemen (DaVid-TLS 29999) die Ports für verschlüsselte Netzwerkdienste.
- 5. Stellen Sie die Verbindung zu den Geräten auf TLS um.
- 6. Nach erfolgreicher Herstellung der TLS-Verbindungen können Sie abschließend die Ports (HTTP 80, DaVid 30000) für unverschlüsselte Verbindungskommunikation in Kameras und Aufzeichnungssystemen deaktivieren.

## ACHTUNG

Beachten Sie, dass Geräte nach dem Deaktivieren der Ports 80 (HTTP) und 30000 (DaVid) über das Netzwerk nicht mehr erreichbar sein können, wenn die Verbindung über TLS-Ports vorher nicht richtig eingerichtet wurde.

Deaktivieren Sie die Ports 80 und 30000 auf Geräten erst, nachdem Sie die Verbindungen über die Ports 443 (HTTPS) und 29999 (DaVid-TLS) zu diesen Geräten erfolgreich hergestellt haben.

## 3.2 ÜBERSICHT

DDM bietet verschiedene Tools, um Root-Zertifikate zu importieren, selbst-signierte Zertifikate zu erstellen oder Zertifikate auf Netzwerk-Geräten zu administrieren.

## 3.2.1 TLS-Werkzeuge

Das **TLS-Werkzeuge** Menü bietet die Möglichkeit den Zertifikatsspeicher auf dem eigenen Windows-Client anzuzeigen und die vorhandenen Zertifikate einzusehen. Der Zertifikatsspeicher steht über das Menü in der normalen Windows-Ansicht oder im Stil der DDM-Benutzeroberfläche zur Verfügung.



Abb. 3-1

- Öffnen Sie das Menü TLS-Werkzeuge über Werkzeuge.
- ▶ Wählen Sie die für Ihre Zwecke geeignete Option:

### • TLS Client-Root-Zertifikatsbetrachter

Übersichtliche Anzeige aller Zertifikate im Zertifikatsspeicher mit Such- und Sortierfunktion

#### • Microsoft Windows-Zertifikatsmanager

Windows-Zertifikatsmanager zur Anzeige der Zertifikate im Zertifikatsspeicher mit Such-, Sortier- und Bearbeitungsfunktion (z. B. Löschen, Kopieren)

## 3.2.2 TLS-Konfiguration und -Verwaltung

In den Netzwerk-Einstellungen zu einem Gerät finden Sie die Optionen für eine TLS-Konfiguration und zur Zertifikatsverwaltung.



Abb. 3-2

- ▶ Wählen Sie ein Gerät aus der System Liste.
- ▶ Rechtsklicken Sie, um das Kontextmenü anzuzeigen.
- > Wählen Sie Netzwerk-Einstellungen, um das Untermenü anzuzeigen.
- Öffnen Sie die TLS-Option, mit der Sie arbeiten möchten:

#### • TLS-Zertifikatszuordnung

Selbstsigniertes Root-Zertifikat erstellen; Erstellen von Signieranfragen für Geräte mit anschließender Signierung und Installation der Geräte-Zertifikate; Entfernung von Zertifikatzuweisungen zu Diensten

#### • TLS-Zertifikatsübersicht

Übersicht, welche Zertifikate auf einem Gerät installiert sind; Zertifikat-Status-Informationen (gültig von/bis etc.)

#### • TLS-Netzwerkdienste

Übersicht aktivierte/deaktivierte Netzwerkdienste; Konfiguration der Dienste (ein-/ausschalten)

### • TLS-Zertifikat Verbindungsinformationen

Status-Information zur aktuellen TLS-Verbindung des ausgewählten Geräts

## 3.3 ZERTIFIZIERUNGSSTELLE

Um eigene Zertifikate ausstellen und signieren zu können, muss zunächst eine Zertifizierungsstelle (Certificate Authority, CA) eingerichtet werden. Dabei handelt es sich um ein spezielles Root-Zertifikat, mit dessen Hilfe weitere Zertifikate signiert werden können.

Dallmeier Device Manager (DDM) kann über eine eigene Zertifizierungsstelle (Root CA) Client- und Server-Zertifikate verwalten. Eine eigene Root CA ermöglicht DDM Zertifikate zu erstellen, zu signieren und auf Geräten (Kameras, Recorder) im Netzwerk zu installieren. Auf dieser Grundlage können Sie dann Geräte-Verbindungen über HTTP und DaVid (Dallmeier Video Protokoll) mit dem Transport Layer Security (TLS) Protokoll verschlüsseln.

Zur Einrichtung einer Zertifizierungsstelle können eigene Zertifikate verwendet werden, die beispielsweise von anerkannten Zertifizierungsstellen ausgestellt wurden. DDM generiert aber auch ein selbst signiertes Root-Zertifikat.

## ACHTUNG

Das Einrichten einer Zertifizierungsstelle mit selbst signiertem Root-Zertifikat wird nur für den Übergang, bis ein Zertifikat einer anerkannten Zertifizierungsstelle vorliegt, empfohlen. Und auch nur innerhalb eines lokalen Netzwerks.

Besteht Zugriff aus öffentlichen, potentiell gefährlichen Netzen (z.B. aus dem Internet) auf das eigene System, sollten zum Verschlüsseln von Netzwerk-Verbindungen und zur Authentifizierung von Geräten von Anfang an nur Zertifikate von anerkannten Zertifizierungsstellen verwendet werden.

### Eine Zertifizierungsstelle (CA) einrichten

Dallmeier Device Manager kann als Zertifizierungsstelle mit extern ausgestelltem Root-Zertifikat verwendet werden ("Option A – eigenes Root-Zertifikat verwenden" auf Seite 13). Dazu müssen Sie das Zertifikat und den zugehörigen privaten Schlüssel auf ihrem lokalen Client-PC speichern. Das Zertifikat kann hier ein Root-Zertifikat oder ein untergeordnetes CA-Zertifikat sein.

Sie können Ihre DDM-Zertifizierungsstelle aber auch mit einem selbst signiertem Root-Zertifikat betreiben ("Option B – Root-CA generieren" auf Seite 14). In diesem Fall erstellen Sie in DDM eine eigene, selbst signierte Root-CA.

 Verfahren Sie zur Einrichtung einer DDM-Zertifizierungsstelle auf Ihrem Client-PC wie hier im Folgenden beschrieben.

> Zum Erstellen von TLS-Zertifikaten in DDM muss das freie Software-Toolkit "OpenSSL" in seiner aktuellen Version installiert sein. "OpenSSL" implementiert die entsprechenden Netzwerkprotokolle sowie die genutzten Kryptographiestandards. Weitere Informationen, Installationshinweise und Download der aktuellen Version unter www.openssl.org.

- Öffnen Sie den Menüpunkt Einstellungen \*\*
- Wechseln Sie zur Einstellungsoption Zertifizierungsbehörde.

#### **OpenSSL**

OpenSSL implementiert die Verschlüsselungsprotokolle SSL und TLS und stellt die Funktionen zum Beantragen, Erzeugen und Verwalten von Zertifikaten zur Verfügung.

▶ Wählen Sie den Tab **OpenSSL**.

* Konfigurationen - Dallmeier Device	Manager 1.0.7				×
Filter	Zertifizierungsbehörde				
🚓 Allgemein	OpenSsl	Zertifizierungsbehörde	Zertifikatinhaber Vorlage	Aussteller Vorlage	
😪 System Konfiguration	OpenSsl-Einstellungen				
🕞 Geräte-Scanner	OpenSsl Ausführbare Datei:	C:\Program Files\OpenSSL-Win64\bin\openssl.	exe	Durchsuche	n
📰 Bericht	Zielverzeichnis für Signing Requests:	C: \Users \martin \Downloads \CAFolder		Durchsuche	n
Erweitert	Zielverzeichnis für Signed Requests:	C:\Users\martin\Downloads\CAFolder		Durchsuche	n
Zertifizierungsbehörde					
				OK Abt	rechen

Abb. 3-3

- Geben Sie im ersten Feld den Pfad zur ausführbaren OpenSSL-Datei direkt ein oder nutzen Sie den Button Durchsuchen, um mit dem Datei-Manager in das erforderliche Verzeichnis zu navigieren.
- Geben Sie in den nächsten beiden Feldern jeweils den Pfad zu den Verzeichnissen für Signing Requests (Signieranfragen) und Signed Requests (signierte Anfragen) ein.

Die Verzeichnisse dienen Ihrer eigenen Übersicht und können beliebig gewählt werden.

Klicken Sie OK, um die Eingaben zu speichern und öffnen anschließend die Einstellungsoption Zertifizierungsbehörde erneut.

### Zertifizierungsbehörde

Auf diesem Tab sind alle Informationen zu Ihrer DDM-Zertifizierungsstelle enthalten. Hier können Sie den Pfad zu einem eigenen Root-Zertifikat und dem zugehörigen Privat-Schlüssel angeben oder ein selbst signiertes Root-Zertifikat generieren.

* Konfigurationen - Dallmeier Device	Manager 1.0.7						×				
Filter	Zertifizierungsbehörde										
Kallgemein	OpenSsl	Zertifizieru	ngsbehörde	Zertifikatinhaber Vo	orlage	Aussteller Vorlage					
System Konfiguration	CA-Root-Zertifikat und privaten Schlüssel auswählen										
Geräte-Scanner	CA-Zertifikat: C:\Users\martir\Downloads\CAFolder\ca_DOM.crt										
E Bericht	CA Privater Schlüssel:	C: \Users \martin\Downloads	\CAFolder\ca_DDM.ke			Durchsuchen					
Erweitert	CA-Privatschüssel-Passwort:										
Zertifizierungsbehörde	Informationen zum CA-Wurzelzertifikat CA-Root-Schlüsselnformationen										
	Aussteller	DDM		Schlüsseltyp:	Privat						
	Gebräuchlicher Name (CN):	DDM		Schlüssel-Algorithmus:							
	Land (C):			Schlüssellänge:	4096						
	Bundesstaat (ST):										
	Organisation (O):										
	Organisationseinheit (OE):										
	Email:										
	Gültig ab:										
	Gültig bis:	20.07.2041 11:56									
	Root-CA erstellen <u>Wie ma</u>	in eine Root-CA erstellt									

Abb. 3-4

#### **Option A – eigenes Root-Zertifikat verwenden**

- Öffnen Sie den Menüpunkt Einstellungen *\** und wechseln zu dem Tab Zertifizierungsbehörde.
- Geben Sie im Feld CA-Zertifikat den Verzeichnispfad zu Ihrem eigenen Root-Zertifikat ein, das für die Zertifizierungsstelle verwendet werden soll.
- Geben Sie im Feld **CA Privater Schlüssel** den Verzeichnispfad zur Datei mit dem privaten Schlüssel ein.
- ▶ Geben Sie im Feld **CA-Privatschlüssel-Passwort** die zugehörige Passphrase ein.

Die Informationen zum Root-CA-Zertifikat und -Schlüssel werden aus dem hinterlegten Zertifikat ausgelesen und in die entsprechenden Feldern automatisch eingetragen.

► Klicken Sie **OK**, um Ihre Eingaben zu speichern.

### **Option B – Root-CA generieren**

Öffnen Sie den Menüpunkt Einstellungen *\** und wechseln zu dem Tab Zertifizierungsbehörde.

🔅 Konfigurationen - Dallmeier Device	Manager 1.0.7								×
Filter	Zertifizierungsbehörde								
🚓 Allgemein	OpenSsl		Zertifizierungsbehörde		Zertifikatinhaber Ve	orlage	Aussteller	Vorlage	
System Konfiguration	CA-Root-Zertifikat und privaten	Schlüssel auswäh	nlen						
Geräte-Scanner	CA-Zertifikat:		tir\Downloads\CAFolder\ca_D	DM.art				Durchsuchen	
E Bericht	CA Privater Schlüssel:	C:\Users\mar	tin\Downloads\CAFolder\ca_E	OM.key				Durchsuchen	
	CA-Privatschlüssel-Passwor	t: •••••							
Zertifizierungsbehörde	Informationen zum CA-Wurzelze	rtifikat			A-Root-Schlüsselinformati	onen			
	Δussteller	DDM			Schlüsseltvn:	Privat			
	Gebräuchlicher Name (CN):	DDM			Schlüssel-Algorithmus:	RSA	_		
	Land (C):	DE			Schlüssellänge:	4096	_		
	Bundesstaat (ST):	n.v.							
	Ort (L):	n.v.							
	Organisation (O):	n.v.							
	Organisationseinheit (OE):	n.v.							
	Email:	n.v.							
	Gültig ab:								
	Gültig bis:	20.07.2041 11:							
Ro	ot-CA ersteller	n )car	erstellt						
							ок	Abbrecher	
							0.0	- Hobiled Ra	

Abb. 3-5

Klicken Sie Root-CA erstellen.

Der Dialog Root-CA erstellen wird angezeigt.

Konfigurationen	- Dallmeier Device M	anager 1.0.7					×
Filter		Zertifizierungsbehörde					
🗱 Allgemein		OpenSsl	Zertifizi	erungsbehörde	Zertifikatinhaber Vorlage	Aussteller V	orlage
System Konfig	uration	CA-Root-Zertifikat und privat	en Schlüssel auswählen				
Geräte-Scanne	<b>o<sup>o</sup></b> Root-CA erstel	len - Dallmeier Device Man	ager 1.0.7			×	Durchsuchen
E Bericht	Tel Vereilabeler		5			Taluana dabata anya Walay	Durchsuchen
Erweitert	Informationen zum	CA-Wurzelzertifikat		CA-Root-Schlüsselinformat	ionen	zierverzeichnis auswahien	
Zertifizierungs		(C))		a literation			
	* Gebrauchliche * Land (C):	r Name (CN):		Schlusseltyp: Schlüssel-Algorithmus:	Privat RSA		
	Bundesstaat (S	т):		Schlüssellänge:	4098		
	Ort (L):			Passwort:			
	Organisation (C	):					
	Organisationsei	nheit (OE):					
	Email:	27.07.2021.12	.02				
	* Cilitia bior	27.07.2021 12	.03				
	Guilg bis.	27.07.2041 12					
						OK Abbrechen	
		Root-CA erstellen Wie	man eine Root-CA erstellt				
							Abbrechen

Abb. 3-6

Die rot markierten Felder sind Pflichteingaben, die weiteren können optional ergänzt werden.

- Klicken Sie Zielverzeichnis auswählen und navigieren Sie mit dem Datei-Manager zu dem erforderlichen Verzeichnis.
- ▶ Geben Sie im Feld **Gebräuchlicher Name** die Benennung der Root-CA ein. Der Name ist frei wählbar.
- ▶ Geben Sie im Feld Land die erforderliche Länderkennung ein (z. B. "DE" für Deutschland).
- Legen Sie unter **Gültig bis** die Gültigkeitsdauer der Root-CA fest (Standardeinstellung: 20 Jahre).
- Legen Sie im Feld **Passwort** eine Passphrase für den privaten Schlüssel fest.
- Ergänzen Sie optional weitere Felder, falls erforderlich.
- Bestätigen Sie Ihre Eingaben mit **OK**.

Die Root-CA wird generiert und in dem angegebenem Zielverzeichnis werden folgende Dateien erstellt:

- ca\_common-name.crt das Root-Zertifikat
- ca\_common-name.key der private Schlüssel

Der private Schlüssel dient zum Signieren der Geräte-Anfragen und darf den Client-PC nicht verlassen, um die TLS-Sicherheitskette nicht zu unterbrechen.

#### Root-Zertifikat in Windows hinzufügen

Es wird empfohlen, das CA-Zertifikat immer auch zu Ihrem Windows Zertifikatsspeicher hinzuzufügen, damit der Webbrowser (beispielsweise beim Öffnen einer Kamera-Web-Konfiguration) keine Sicherheitswarnung über ein ungültiges Sicherheitszertifikat anzeigt und die Verbindung zu dem Gerät nicht blockiert wird. Ein Zertifikatsimport in Windows ermöglicht eine sichere HTTPS-Verbindung im Browser mit Ihren Geräten herzustellen.

Öffnen Sie den Windows Zertifikatsspeicher über Werkzeuge > TLS-Werkzeuge > Microsoft Windows Zertifikatsmanager.





- Klicken Sie Weiter.
- Klicken Sie **Durchsuchen...**, wählen das zu importierende Zertifikat aus und klicken Sie **Weiter**.



Abb. 3-9

- > Wählen Sie als Zertifikatspeicher Vertrauenswürdige Stammzertifizierungsstellen und klicken Weiter.
- ▶ Klicken Sie Fertig stellen, um den Importvorgang zu starten.

certIm - [Zertifikate - Lokaler Computer/Vertrauenswürdige S	tammzertifizierungsstellen]	-		×
Zertifikate - Lokaler Computer     Eligene Zertifikate     Gregene Zertifikate     Organisationsvertrauen     Zovichcarstridige Herausgeber     Zovichcaretifizierungsstellen     Dittanbieter-Stammzertifizierungsstellen     Vetrauenswürdige Zertifikate     Dittanbieter-Stammzertifizierungsstellen     Vetrauenswürdige Zertifikate     Stammenente der Vorabversion     Stammenente der Vorabversion     Stammenente der Vorabversion     Ad Ditens issuer     Ad Ditens issuer     Adhören State     Currentüser     Eetification Authonities     Local MonRemovable Certificates     Local MonRemovable Certificates     LocalMochine Certificates     Vetrauenswürdige Stammen     Autoritäten für die Installation vertrauenswürdige rverpar     Vetrauenswürdige Stammen     Vetrauenswürdige Stammen	Objekttyp Zetrifikate Zetrifikatimport-Assistent T Der Importvorgang war effolgreich. T K K K			
E			_	_

Abb. 3-10

Bestätigen Sie den Zertifikatimport-Assistent mit OK und beenden Sie den Zertifikatsmanager nach erfolgreichem Importvorgang.

#### Zertifikatinhaber Vorlage

Ihre DDM-Zertifizierungsstelle verwendet für die Erstellung der Geräte-Zertifikate bei Signieranfragen die Angaben aus diesem Dialog.

🇬 Konfigurationen - Dallmeier Device	e Manager 1.0.7			×
Filter	Zertifizierungsbehörde			
🚓 Allgemein	OpenSsl	Zertifizierungsbehörde	Zertifikatinhaber Vorlage	Aussteller Vorlage
System Konfiguration	Zertifikatinhaber			
🕞 Geräte-Scanner	Alias:			
📑 Bericht	*Land (C):			
Erweitert	Bundesstaat (ST):	Bayern		
Zertifizierungsbehörde	Ort (L): Organisation (O):	Regensburg Dalmeier		
	Organisationseinheit (OE):	TechDok		
	Email:	info@dallmeier.com		
				OK Abbrechen

Abb. 3-11

- Geben Sie die erforderlichen Angaben für den Zertifikatinhaber in den entsprechenden Feldern ein.
- Bestätigen Sie mit **OK**, um ihre Eingaben zu speichern.

#### Aussteller Vorlage

In diesem Dialog legen Sie die Gültigkeitsdauer für die Geräte-Zertifikate fest, die Ihre DDM-Zertifizierungsstelle bei Signieranfragen ausstellt.



Abb. 3-12

- Geben Sie im Feld **Gültigkeit in Jahren** den gewünschten Zeitraum ein.
- Klicken Sie Anwenden.

# 3.4 VERBINDUNGEN VERSCHLÜSSELN

Nach dem Einrichten einer Zertifizierungsstelle (Certificate Authority, CA) auf Ihrem Client-PC in Dallmeier Device Manager (DDM) können Sie nun damit beginnen, Verbindungen von Ihrem DDM-Client-PC zu Kameras und Recordern in Ihrem Netzwerk mit Transport Layer Security (TLS) zu verschlüsseln. Um die dafür erforderlichen Protokolle DaVid-TLS (Kameras, Recorder) und HTTPS (Kameras) zu aktivieren, muss auf einem Gerät ein Zertifikat installiert sein. DDM ermöglicht es als CA, entsprechende Zertifikate zu erstellen, zu signieren und auf den Geräten zu installieren. Das Vorgehen hierbei ist bei Kameras und Recordern gleich.

Datei Bearbeiten Ansicht Einstellu													
🖻 🗁 💾 🕄 । 🚯	¢¶  ⊅ ↓		ک ش 🖻	🗁 🖹	fy	R @ F	🔅 🖲						
Dash Board 'Zusammenfassung'	System										Ansicht Eigenschaften		
Name A	IP/DNS Adresse					ie der Wartung	Secienciummer	MAC-Adresse			System Eigenschaften	Kameras	
											Bgenschaft		
P:10.130.50.106			VirtualCarn	1.0.0.1.20200602				52/56/42/42/43/09			<ul> <li>Geräteeinstellungen</li> </ul>		
IP-10 130 50 107			VirtualCarra	1.0.0 ( 20200602			01/001-13374346	52-56-42-42-42-64					
Gre											IP/DNS Adresse		
🥝 🛄 IP:10.130.50.108											<ul> <li>Login-Einstellungen</li> </ul>		
												•na Inaktiv	
			virtualCam	1.0.0.1.20200602			DVC001-13374348	52:56:42:42:45:66			Anmeldemodus	Benutzer	
Image: 10 10 10 10 10 10 10 10 10 10 10 10 10			VirtualCarro	1.0.0.120200602				52/56/42/42/43/06			Benutzer Name	admin	
											Benutzer Passwort		
😪 🛄 IP:10.130.50.110			VirtualCam								Garitakataooria	Dallmaiar Rekorder/Kamera	
											Hersteller	Dallmeier electronic GmbH & Co	
			virtualcam	1000120200802				363096969693706			Gerätetyp	VirtualCam	
IP:10.130.50.112			VirtualCam	1.0.0.120200602				52:56:42:42:43:66					
<u>Sec</u>											Firmware-Version	1.0.0.i.20200602	
💙 🛄 IP:10.130.50.113			VirtualCam				DVC001-13374352	52:56:42:42:43:70				52:56:42:42:43:73	
2 10 10 100 50 115				100:000000							Beginn der Wartung		
Current asserts											Ende der Wartung		
IP:10.130.50.116			Vinter								<ul> <li>Statusinformationen</li> </ul>		
			Web-Konti روا	guration			strg+W				Letzter Scan	02.08.2021.09.55	
🕑 🛄 IP:10.130.50.117			Vit 64 Aktualisien	en der Geräte-Informa							Gesamtstatus		
IB-10 120 50 119								52/56/42/42/42/75			Zeittope	Furona/Barlin	
			() Neustant				krg+к				Zeit-Sync	Corope ection	
IP:10.130.50.119			Vir 00 Ping IP-Ad	resse	-		strg+P				Zeit-Sync-Status		
						_							
P:10.130.50.12		inaktiv	cizenz-E	:instellung	en 🔨			52:56:42:42:43:06				<b>V</b>	
IP:10.130.50.120		laukti						2.5	tzwerkeinstelli	ungen	David-TIs (Port 29999)		
-ve			Netzwer	k-Finstelli		, <u>)</u>					Steel		
Geräteanzahl 891 (Selektiert 1)		stars (				· //		<b>//</b>				<u> </u>	
Garite-Scanner							^	TLS-Z	ertifikatszuord	Inuna (Selbstsianie)			
The second second	(n) ×	Owned Consider	enutze	reinstellur	Iden		Jmschalt+E						
broadcast Scanner in Scanner		Universities			and a second			VI C.7	artifikatsühars	icht Root-Imp			
NEC: Vian 150 (10. 150. 0.65)	Scame Nets		E Vanimum C					TLS-20	ertifikatsubers	acine, Root-Inc			
Gerat	* Gruppen Pfad	IP/DNS	Ac on the second										
100-11 SPS-VM			Eg Kopieren				strg+Umschalt+C	Netzwerk-Schnitt	tellen Inio				
												$\sim$	
SMAVIA Recording Server SD			0.1 💼 Neue Grup	pe								$\langle (\mathbf{a}) \rangle$	
			R Neues Geri	it/System			Rrq+D						
SMAVIA Recording Server SD													
SDES300HD-DN/IR			2.4 Alle Eintrög	ge im System-Baum e	xpandieren		1	08CCWR488446560					
			I≣ Alle Eintrag	ge im System-Baum z	usammenkl	appen							
SDF5300HD-DN/IR					0.96uild 160		5300HD-DN/IR201411						
→ FIII Panomera® S7 Nightline 50/											durant of control	Common Markets	
Anashi:21											Jungabelenster	- remware Opdate	Exp (1)
TLS-Zertifikatszuordnung (Selbstsigniert,	Signieren von Anforders	ungen, Zuordnu	ingsinformationen	)		_						Systemspeicher:7.51G8 f	reiven 15.94G

Abb. 3-13

- > Wählen Sie in Ihrem System das erforderliche Gerät.
- Rechtsklicken Sie das Gerät, um das Kontextmenü anzuzeigen.
- > Öffnen Sie den erforderlichen Dialog über Netzwerk-Einstellungen > TLS-Zertifikatszuordnung.

Der Dialog wird in einem neuen Tab angezeigt. An den rot markierten Diensten sehen Sie, dass HTTPS und DaVid TLS noch nicht aktiviert sind.





Klicken Sie Erstellen eines Signing Request.

Der Dialog Zertifikate erstellen und Netzwerkdienste zuweisen wird angezeigt.

Zertifikate erstellen und Ne	etzwerkdiensten zuweisen - D	allmeier Device Manager 1.0.						×			
OpenSSL-Einstellungen für das Si	gnieren				Zertifikatinhaber Einstellungen						
OpenSsl Ausführbare Datei:	C:\Program Files\Op	enSSL-Win64\bin\openssl.exe		Durchsuchen	Alas:	TLS Connection					
Zielverzeichnis für Signing Re	equests: C:\Users\martin\Dow	inloads\CAFolder		Durchsuchen		CE .					
Zielverzeichnis für Signed Rei	quests: C:\Users\martin\Dov	inloads\CAFolder			Bundesstaat (ST):	Bayern					
						Regensburg					
Aussteller CA-Root-Zertifikat und	privater Schlüssel				Organisation (O):	Dalmeier					
					Organisationseinheit (OE):	TechDok					
CA-Zerbfikat:	C:\Users\martin.keidel\Down	loads\CAFolder\ca_DDM.crt		Durchsuchen	Email:	info@dalmeier.com					
CA Privater Schlussel:	C: Users (martin keidel (Down	loads(CAholder)(ca_DDM.key		Durchsuchen							
CA+rivatschlussel+Passwort:	•••••				Zertifikat zuweisen und Netzwe	rkdienst aktivieren					
Ausstellerinformationen von Zerti	ifikat und Schlüssel				David-TLS		HTTPS (nur Kameras)				
CA-Root-Zertifikat		CA-Root-Schlüssel									
					🗹 Netzwerkdienst akti	vieren	🗹 Netzwerkdienst aktivieren				
Aussteller	DOM	Schlüsseltyp:	Privat				Cambrovy für das Turmalo (nur Dal	inertiar)			
Gebräuchlicher Name (CN):	: DOM	Schlüssel-Algorithmus	: RSA								
Land (C):	DE	Schlüssellänge:	4096				Zerbfikat zuweisen				
Bundesstaat (ST):	n.v.						Netzwerkdienst aktivieren				
	n.v.										
Organisation (O):	n.v.				Aktionen						
Organisationseinheit (OE):	n.v.				📄 Löschen des "Signing Re	quest" nach der Unterzeichnung					
Email:	n.v.			R	Löschen von erstellten 'S	Signierten Zertifikaten' nach dem Imp	xort				
Gültig ab:	20.07.2021 11:56										
Gültig bis:											
Issuer Validity											
Tage 1096 🗘		Gültigk	sit in Jahren 3 🗘	Anwenden							
* obligatorisch											
								OK Abbrechen			

Linke Seite: Informationen der Root CA; rechte Seite: Angaben für das auszustellende Geräte-Zertifikat wie in den DDM-Einstellungen vorgenommen (siehe Abschnitte "Zertifizierungsbehörde" auf Seite 13, "Zertifikatinhaber Vorlage" auf Seite 17, "Aussteller Vorlage" auf Seite 17).

Abb. 3-15

- A In der Standardeinstellung erfolgt mit der Zertifikatszuweisung auch die Aktivierung der entsprechenden Netzwerkdienste. Deaktivieren Sie diese, falls erforderlich.
- **B** Das Speichern des Signing Request und des Geräte-Zertifikats auf Ihrem lokalen Client-PC können Sie unterbinden und die Dateien nach dem Vorgang löschen, wenn Sie die Checkboxen hier aktivieren.
- Klicken Sie OK und bestätigen Sie die nachfolgende Sicherheitsabfrage, um den Vorgang der Zertifikatserstellung zu starten.

Ihre DDM Root CA signiert die Zertifikatsanfrage und installiert automatisch das entsprechende Zertifikat auf dem Gerät.

Datei Bearbeiten Ansicht Einstellun	gen <u>P</u> rotokollverlau	f Werkzeuge	Hite											
E 🖻 🖻 🕄 I 🚯 I	📌 🔎 🗸		🗈 î 🗙 I	🗁 🖹 I	🔸 🖪 <	e 📑 🗷 🖳								
Dash Board 'Zusammenfassung'	System		TLS Zertifikatszur	reisung tala							Ansicht Eigenschaf	Iten		88
resse + MAC-Adresse Gerätets	n TIS Finstellung	ien Di		Philikats	zuweisun	a Info 💙	٢					eschaften	Kameras	
14 52-56-42-43-71 VirtualCar	n Nicht			Tunkats	Zuweisun	g milo 🍾	`						ert	·
_														~
	ngen	Dienst		Pfad ID	) Alia	s			Benutzt vo	n Gültig ab		Gültig bis		
Cht sicher														
				00.4	~ "									1005 1
			nttps	CP-1	Dai	imeierDivi_	29.07.20	J21 10:34:37	nttps/david_	tis 29.07.2021	14:34:37			1096 days
														/
			david tls	CP-1	Dall	ImeierDM 3	29.07.20	021 16:34:37	https/david	tls 29.07.2021	14:34:37			1096 da
	_												/	
												_		
												0	K	
											Zeitzone Zeit-Swic	6	rope/Berlin Wahr	
												tatus	Wahr	
											<ul> <li>Netzwerkdienst</li> <li>David (Port</li> </ul>	e 300001	Wabr	
a -											David+TIs (P	ort 29999)	Wahr	
4) Altualisieren								gniertes Zertfikat E	istellen eines Signing Request		Https (Port - RTSP (Port 5	443)	Wahr Wahr	
														•
Geräte-Scanner		Omit Contin									Ausgabefenster			15.26
broadcast Scanner in Scanner (			scanner											
Gerst	<ul> <li>Gruppen Pfad</li> </ul>	IP/DNS I	Adresse MAC-	Filler Adresse D	rmware-Verilag	Serlessummer	Statur	034						
Vietuslána	(00.100.50.1-10	10 100 50	11 \$2.56	45454200 1	0.0120200602	DWC001-13374240	510105	010						
												6		
Virtua Kam		10.130.50	1.2 52:560	424243801 1.	0.0120200602	DVC001-13374241						C	//	
Virtua/Cam														
VirtualCam														
Virtua/Cam						DVC001-13374244								
				43-43-43-05 1	0.0:0000600									
Anzahi:384				10101010							Ausgabe	fenster	Firmware Update	Exp (1)
													Systemspeicher	3.22 G8 frei von 15.94 G8

Abb. 3-16

Die Dienste HTTPS und DaVid-TLS sind nun auf dem Gerät aktiviert und Sie können eine verschlüsselte Verbindung zu diesem aufbauen.

▶ Wechseln Sie dazu in den System Tab.

Datei Bearbeiten Arsicht Einstell	lungen <u>P</u> rotokoliveriau	uf Werkzeuge ⊟ife ↓ ↑   @⊋n	ñ x i 🖿 🖻	· 4 📃 👁						
Daub Board Zusammenfassund	1.941 / 2-							Ansicht Eigenschaften		
Name	IP/DNS Adresse		erätetyn Firmware-Ver	rsion Forde der Warts		M&C-Adresse Status		System Eigenschaften	Kameras	
2 1 19-10 120 50 109		Sicher Strike Mit 4	Cam 1.0.0120200602			52564242424362 01		Egenschaft		
								<ul> <li>Geräterinstellungen</li> </ul>	10.10 120 50 116	
P:10.130.50.11		Sicher Strikt Virtual			DVC001-13374250	52:56:42:42:43:0a OK		IP/DNS Adresse	10.130.50.116	
IP:10.130.50.110								<ul> <li>Login-Einstellungen</li> </ul>		
IP-10 133 50 111		Sicher Strikt - Mittal	Cam 1.0.0 i 20200602			52554242434s III		TLS Annaldemodur	••• Inaktiv	
								Benutzer Name	- Scher Strikt	
P:10.130.50.112		Sicher Strikt Mitual	Cam 1.0.0.1.20200602		DVC001-13374351	525642424388 01		Benutzer Passwort	<u> </u>	
🧭 🛄 IP:10.130.50.113	10.130.50.112		1.0.0.1.20200602					Gerät Informationen     Gerätekateggai	Dallmeier Rekorder/Kamera	
IP:10.130.50.115			40502					Here	Dallmeier electronic GmbH & C	
		and also	Minter and				_	.130.50.116	VirtualCam DVC001,13374355	
	2	nakuv	virtualy			A STREET, STRE		10 120 50 116		<u> </u>
S 📑 🕹 🖓 🖓					DVC001-13374356	S II / DI IS / GIESSE		10.130.50.110		
🥝 🔃 IP:10.130.50.118	The state	paletive	20200602			Login-Einstellungen				
< 🔃 IP:10.130.50.119	10.130.50.119	Inskiiv Virtual	Cam 1.0.0.i.20200602			те				
IP-10 193 50 12		Inaktiv Votnal	Cam 1.0.0 i 20200602			ILS		• TIS Inaktiv		
						Anmeldemodus		•114 Sicher		
		Inaktiv virtual	Cam 1.0.0.20200602		DVC001+13374359	Benutzer Name				
IP:10.130.50.121									N	
IP:10.130.50.122						Benutzer Passwort		•••••	~	
🥝 🛄 IP:10.130.50.123						Gerät Informationen				<del>」</del>
Geräteanzahl 891 (Selektiert 1)										<u> </u>
Geräte-Scanner								Ausgabefenster		
Broadcast Scanner IP Scanne	er (1) 🗙 🛛 +	Onvif-Gerätescanne								
NEC: Vien 150 (10. 150. 0.65)	Scame N			er Einstellungen: Kein Niter	~		R 9 0 4			
Gerat	* Gruppen Pfa	d IP/DNS Adres	se MAC-Adresse	Firmware-Version	Serlennummer	Status Bild				
SRS-VM										
THE SAMUA Recording Server SI	D Card		0001-001667-14		DRS5-10128117					
					DK33-00209049					
SDF\$300HD+DN/IR			c0:56:e3:aac26:4a	5.0.9build 160308	SDF5300HD-DN/IR201411	08CCWR488446560				
SDF5300HD-DN/IR										
→ IFFFFI Panomera® S7 Nightline 50										
Anzahi:21								Ausgabefenster	Firmwäre Update	Exp (1)
									Systemspeicher: 7.13 GE	3 frei von 15.94 GB

Abb. 3-17

Die TLS Einstellungen zeigen die Inaktiv Markierung für eine unverschlüsselte Verbindung.

- Öffnen Sie das Verbindungstyp Dropdown-Menü unter den Login-Einstellungen in den System Eigenschaften.
- Wählen Sie die Option Sicher Strikt.
- Aktualisieren Sie mit der Taste **F5** die Verbindung zu dem Gerät.

Beim erneuten Verbindungsaufbau validiert Ihre DDM Root CA das Geräte-Zertifikat und beide kommunizieren ab sofort über eine TLS verschlüsselte Verbindung.

Dotei Bearbeiten Ansicht Einstellu	ngen <u>P</u> rotokollverlauf	Werkzeuge	Hife											
	<b>∲</b>   ⊅ ↓		Bo Ca ×	🗁 🖹	- <del>6 y</del> - [	R @ F	🔅 🖳							
Dash Board 'Zusammenfassung'	System											Ansicht Eigenschaften		
Name +	IP/DNS Adresse					e der Warbung		MAC-Adresse				System Eigenschaften	Kameras	
												Boenschaft		
Image: 10 10 10 10 10 10 10 10 10 10 10 10 10			VirtualCam	1.0.0.1.20200602				52/56/42/42/43/09				<ul> <li>Geräteeinstellungen</li> </ul>		
IP-10 133 50 107			VirtualCarra	1.0.0 ( 2020)602			DVC001-13374346	52-56-42-42-42-64						
												IP/DNS Adresse		
🧭 🛄 IP:10.130.50.108												<ul> <li>Login-Einstellungen</li> </ul>		
													• na Sicher Strikt	
			virtualCam	1.0.0.120200602			DVC001-13374348	52:56:42:42:45:66				Anmeldemodus	Benutzer	
IP:10.130.50.11			VirtualCam	1.0.0.120200602				52:56:42:42:43:0a				Benutzer Name	admin	
												Benutzer Passwort		
💙 🦳 IP:10.130.50.110			VirtualCam									Garitakatanoria	Dallmaiar Rekorder (Kamara	
												Hersteller	Dallmeier electronic GmbH & Co.	0G
	10.150.30.111		ningaicam	1000120200802				3/2309/29/29/29/29				Gerittetyp	VirtualCam	
IP:10.130.50.112		er own	6.0	0.0.120200602				52:56:42:42:43:66						
												Firmware-Version	1.0.0.i.20200602	
🕗 🛄 IP:10.130.5				200602			DVC001-13374352						52:56:42:42:43:72	
2 III 10 10 100	Siche	er Strik	et Vintu	JalC								Beginn der Wartung		
												Ende der Wartung		
🔗 🥅 IP:10.130.50.1	<u> </u>		~	20200602								* Statusinformationen		
		-		/								Letzter scan	02.08.2021 10:00	
💙 🛄 IP:10.130.50.117	10.130.99		1000	1.0.0.120200602			DVC001-13374356	52:56:42:42:43:74				T Triticformation		
Image: 10 10 10 10 10 10 10 10 10 10 10 10 10			VirtualCam	1.0.0.120200402				52/56/42/42/43/75				Zeitzone	Europe/Berlin	
<u> </u>												Zeit-Sync		
😪 🛄 IP:10.130.50.119												Zeit-Sync-Status		
			virtualCam	1.000.20200602				52/30/42/42/43/00				David (Port 30000)	✓	
IP:10.130.50.120			VirtualCarm									David-TIs (Port 29999)	<u>≚</u>	
- ve												Https (Port 443)	~	
Geräteanzahl 891 (Selektiert 1)	n 305 (Selektert I) Sta	itus Felder 6 (S	Selektiert 0) Offi	ine 680 (Selektärrt G							<u> </u>	KISP (Port 554)		
Geräte-Scanner												Ausgabefenster		
Broadcast Scanner IP Scanner	(1) X +	Onvif-Gerates	icanner											
NEC: Vien150 (10.150.0.65)	Scame Netz				tinstelungen:		~				🛛 🖳 🖄 🖏			
Gerät	* Gruppen Pfad	IP/DNS	Adresse N	MAC-Adresse	Firmware-Vei	rsion Seri	lennummer		Status	Bild				
SRS-VM														
SMAVIA Recording Server SD	Card		0.12 0	0.01:c0:16:F7:1a		DRS								
							13-00209049							
SDF5300HD-DN/IR				0.56:e3:aa:26:4a	5.0.9build 160		5300HD-DN/IR2014110	38CCWR488446560						
SDF5300HD-DN/IR														
- FIFFI Panomera® S7 Nightline S0/												Ausoahefenster	Firmware Undate	Eventual
A12872.21													-	
	_		_										Systemspeicher: 7.03 GB fre	ii von 15.94 G8

Abb. 3-18

Die TLS Einstellungen des Geräts zeigen nun Sicher Strikt.

## 3.5 RECORDER-ZU-KAMERAS VERBINDUNGEN

TLS-Verbindungen eines Aufzeichnungssystems (Recorder) zu seinen Kameras können mit dem Root-Zertifikat Ihrer DDM-Zertifizierungsstelle eingerichtet werden. Dazu importieren Sie das Zertifikat auf dem Recorder und dieser validiert damit die Kamera-Zertifikate, die Sie vorher mit diesem Root-Zertifikat über DDM auf den Kameras installiert haben.

 Rechtsklicken Sie den erforderlichen Recorder in der Ansicht System, um das Kontextmenü anzuzeigen.

Datei Bearbeiten Ansicht Einstellun	igen <u>P</u> rotokollverlauf	Werkzeuge Hilfe										
A 🖻 🖻 🖪 I 🚯	8 P I	/ ↑   🗈 டி	×   🗁 🖻	😽 📃	ې 📃 👁	E 🔍						
Dash Board 'Zusammenfassung'	Curture.									Ansicht Eigenschaften		
News	ID /DNIC A down									System Eigenschaften	Kameras	
Name -	IP/Diss Adresse	its dentery	p Pittiwate.	enue dei	wattong :	salamumia	Machadiese	Status		Bgenschaft		
10.130.52.1-10.130.52.1.171										<ul> <li>Geräteeinstellungen</li> </ul>		
Dashboard Counting										benutzerdefinierter Name		
										IP/DNS Adresse	10.130.112.52	
DMVC2										* Login-Einstellungen		
· FSL Becorder Pridleld										Anneklemodur	Reputter	
										Benutzer Name	admin	
IP:10.130.112.51			00 9.15.10 (SP:al							Benutzer Passwort		
		_										
9 Local 1911013011232		Web-Konfiguration			w 🖤	Me-0000261	0010022914068168			Gerätekategorie		
IP:10.130.112.53		🖌 🍫 Aktualisieren der Gerä	te-Informationen		v)							
										Gerätetyp	SRS-VM 10000	
<ul> <li>Kamera_68xxxx</li> </ul>		Software Update		Strg+						Seriennummer	DVM4-00000261	
> En ter		() Neustart			R					MAC-Adverse	9.15.10 (SP(800) 00.0x/29.14.6 s/ba	
		()() Ping IP-Adresse								Beging der Wertung	02 12 2019 00:00	
Test License Kamera	-									Ende der Wartung	02.10.2020 00:00	
										* Statusinformationen		
<ul> <li>Jest Insaintenance Angela</li> </ul>	117	enz-Finstellu	ngen 🦳		,							
Test Wittmann Recorder					,							
	/ N.	towark Einste			•			<b>J</b>		<ul> <li>Zeitinformation</li> </ul>		
Test_RecordingInfo			llungen							Strg+  Zeitzone	Europe/Berlin	
> DoDate						-7ertifik	catszu ordn	una (Selhstsianiert 4	Signieren vo	Zeit-Sync Zuit Sume Statum		
	Be	nutzereinstell	ungen		//····	Letter	auszaoran	ang (sensengmere,	Signician rol	tweekdienste	<u>u</u>	
>					🖊 те			ht. Doot loop at und	I.A., 6.8	David (Port 30000)	2	
0 10.10 2 126 25	10.2.126.26				11.5	-Zerunk		ni, Koot-import und	Auffaumen	David-TIs (Port 29999)	<b>V</b>	
0 IN: 10:2: 120-23		S. Koheren (receit)								RTSP (Port 554)		
Geräteanzahl 891 (Selektiert 1) (Intere		🖌 🕄 Kopieren			UN TLS	-Netzw	erkdienste	(Aktivieren/Deaktivi	eren) 🦯	tzwerkschnittstellen		
Geräte-Scanner						<u> </u>				Austabefenster		
The second second		Neue Gruppe		Umsc	halt-G		<del>est direkte</del>	Verbindungsinforma	the			
broadcast Scanner in Scanner	··· × ··	R Neues Gerät/System		Stro+	D							
NEC: VLAN130 (10.130.254.112)	Scame Net	n				~			R 8 0 8			
Gerät	* Gruppen Pfad	🗄 Alle Einträge im Syste	m-Baum expandierer		m	imer Sta	rtus Bild					
VitualCam		🗏 Alle Einträge im Syste	m-Baum zusammenk	lappen								
VirtualCam												
				1.0.0.2000000								
L. Virtuicam			100000000000000	10000200002								
VirtualCam												
UrtualCam				1.0.0.1.20200602	DVC001-13							
VirtualCam		30 10.130.50.16	52:55:42:42:43:06	1.0.0.120200602								
Anzehi:335										Ausgabefenster	Firmware Update	Exp (1)
TLS-Zertifikatsübersicht, Root-Import und	Aufräumen										Systemspeicher: 9.50 (	58 frei von 15.94 G

Abb. 3-19

▶ Wählen Sie Netzwerk > TLS-Zertifikatsübersicht.

Bit De line in partie line in partie line in partie

Partie

Bit De line in partie

Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Partie
Par

Der Dialog TLS-Zertifikatsübersicht wird in einem neuen Tab angezeigt.

Abb. 3-20

Klicken Sie Root-Zertifikat importieren.

Der Dialog Stammzertifikat importieren wird angezeigt.

Rotei Bearbeiten Ansicht Einstellung	en <u>P</u> rotokollverlauf Werkz	euge Bife	×   🖿	Ì   49		@ 📑 🖄 🖫								
Dash Board 'Zusammenfassung'	System	TLS Zerti	ifikat Übersicht									Ansicht Eigenschaften		
1												System Eigenschaften	Kameras	
Gerätename IP/DI	IS Adresse * 115	MAC-Adresse	Geratetyp	Cert ID		Ahas Pla	ed ID Benutzt vo	m CA (	Unternehmen	Allgemein		Egenschaft		
👻 🗹 🚥 IP:10.130.112.52 10.130.												<ul> <li>Geräteeinstellungen</li> </ul>		
												benutzerdefinierter Name		
					DDW_02.06	12021 10:04:22		وا 🏑	_					
						Stammzertifikat Import - D	Valimeier Device Manag	er 1.0.8	×			* Login-Einstellungen		
					Poenices.						Ratistical			
					DService3	CA-Root-Zertfikat auswählen				Dalmaire-StammCA		Anmeldemodus	Benutzer	
						CA-Root-Zertifikat:						Benutzer Name		
					PService3	C: Utera martri keidel Dowrk	ads/CAFolder/ca_DDM.cr	t		Graupner Enterprise		Benutzer Passwort		
									-			<ul> <li>Gerät Informationen</li> </ul>		
					Dalimeierl			Durchsut	orien		Regenst	Gerätekategorie	Dallmeier Rekorder/Kamera	
						CA-Root-Zertificat-Informationer						Hersteller	Dallmeier electronic GmbH &	Co.KG
												Gerätetyp	SRS-VM 10000	
						6	2014					Seriennummer	DVM4-00000251	
						HIMING	LON	_				Firmware-Version	9.15.10 (SP:abd)	
						Gebräuchlicher Name (CN):	DOM					MAC-Adresse	00:0c:29:14:6a:ba	
												Beginn der Wartung	02.12.2019 00:00	
						Bundesstaat (ST):	0.9					Ende der Wartung	02.10.2020 00:00	
												* Statusinformationen		
							11.44	_				Letzter Scan	02.08.2021 16:14	
						Organisation (0):	n.v.							
						Organisationseinheit (OE):						<ul> <li>Zeitinformation</li> </ul>		
						Enal:	n.v.						Europe/Berlin	
								r	100			Zeit-Sync	<b>V</b>	
						Guing ap:	20.07.2021 11:56					Zeit-Sync-Status	✓	
						Guiltig bis:								
												David (Port 30000)	✓	
												David+TIs (Port 29999)	<b>V</b>	
												RTSP (Port 554)	✓	
Zertifikats-Enformationen aktualisieren										Root-Zertifikat	mportieren	<ul> <li>Netzwerkschnittstellen</li> </ul>		
Geräte-Scanner Broadcast Scanner IP Scanner (1	i) 🗙 + Onvaf-G	Ferätescanner										0 Ausgabefenster		
NEC: W.AN130 (10.130.254.112)	Scame Netzwerk										0 🗞			
Gerät	* Gruppen Pfad IP/	DNS Adresse	MAC-Adresse	Firmware-	Version									
VirtualCam														
Virtue/Cerro														
VirtualCam														
VirtualCam														
Virtus/Cam														
Virtua/Cem														
Anzahi: 335												Aungabetenster	Systemspeicher:8.31 G	8 frei von 15.94

Abb. 3-21

Der Dialog übernimmt automatisch das zuvor in den DDM-Einstellungen eingerichtete Root-Zertifikat.

- Klicken Sie OK.
- Bestätigen Sie den nachfolgenden Sicherheits-Dialog, um den Importvorgang zu starten.

Das Root-Zertifikat wird auf das Aufzeichnungssystem geladen.

#### DaVid TLS für Kamera-Verbindungen aktivieren

Für die Kamera-Verbindungen des Recorders können Sie nach dem Import des Root-Zertifikats nun Da-Vid TLS über Port 29999 aktivieren und den DaVid Port 30000 ausschalten, um unverschlüsselte Kameraverbindungen darüber nicht mehr zuzulassen.

 Rechtsklicken Sie den erforderlichen Recorder in der Ansicht System, um das Kontextmenü anzuzeigen.



Abb. 3-22

Wählen Sie **NetConfig3**, um die Recorder-Konfiguration zu öffnen.

Der **NetConfig3** Verbindungsdialog wird angezeigt und die Anmeldung am Recorder erfolgt automatisch.



*Beachten Sie den Verbindungstyp Dallmeier TLS Strict:* DDM-Client-PC und Recorder kommunizieren über eine verschlüsselte Verbindung. Login- und Konfigurations-Daten können nicht "mitgelesen" werden.

Abb. 3-23

Die Konfigurationsoberfläche des Recorders wird angezeigt:

Dallmeier Netconfig 3 - 10.130.112.52					– 🗆 🗙
Angemeldet als Administrator					CPU Usage: 0%
	Schließen Aufnahme	Netzwerk	System	Schnittstellen	
	Aufnahme		<b>Fileboo</b>		
	Kameras / Spuren		HDD-Verwaltu	ina	
	Kamerabeschreibungen		Suchkriterier	n.	
	Spuren sichern		Referenzbild		
	MaxAge				
					See more.

Abb. 3-24

► Wählen Sie Aufnahme > Kameras / Spuren.

Die Kamera-Konfiguration des Recorders wird angezeigt:



Abb. 3-25

- ▶ Klicken Sie auf eine Kamera in der Spalte LP Track, um den Aufnahme-Dialog der Kamera anzuzeigen.
- ▶ Wählen Sie aus dem Protokoll Dropdown-Menü die Option Strenges TLS (DaVid).
- Klicken Sie **Test**, um die Kameraverbindung zu prüfen, falls erforderlich.

Ist der Verbindungstest zur Kamera erfolgreich, schließen Sie den Aufnahme-Dialog der Kamera mit **OK**. Kann unter Verwendung des TLS-Protokolls keine Verbindung zur Kamera hergestellt werden, stellen Sie das Protokoll auf die Option **Kein TLS (DaVid)** zurück und überprüfen zunächst die Zertifikate auf den beteiligten Geräten.

> Verfahren Sie wie oben beschrieben, um für alle erforderlichen Kameras die TLS-Option zu aktivieren.

Sind alle Recorder-Kameras-Verbindungen auf diese Weise erfolgreich umgestellt, können Sie dies auch im Dallmeier Device Manager (DDM) überprüfen:

- > Wählen Sie den erforderlichen Recorder in der Ansicht System.
- Aktualisieren Sie mit der Taste F5 die Verbindung, falls nach der TLS-Konfiguration noch nicht vorgenommen.
- ▶ Wählen Sie in der Ansicht Eigenschaften den Tab Kameras.



Abb. 3-26

Auf dem Tab **Kameras** werden alle Infos zu den Kameraverbindungen des Recorders angezeigt, so auch über welches **Protokoll** die Kameras mit dem Recorder verbunden sind.

## 3.6 UNSICHERE PORTS DEAKTIVIEREN

Nach der Installation der Geräte-Zertifikate und der Herstellung der verschlüsselten TLS-Verbindungen können Sie nun auf den Geräten abschließend die Ports (HTTP Port 80, DaVid Port 30000) deaktivieren, über die unverschlüsselte Kommunikation noch möglich wäre, um unsichere Verbindungen hier nicht mehr zuzulassen. Die aktuell aktiven **Netzwerkdienste** des Geräts können Sie in seinen **System Eigenschaften** sehen A.



▶ Rechtsklicken Sie das Gerät, um sein Kontextmenü B anzuzeigen.

Abb. 3-27

Wählen Sie Netzwerk-Einstellungen > TLS-Netzwerkdienste (Aktivieren/Deaktivieren).

Der Dialog **Netzwerkdienste** wird in einem neuen Tab angezeigt. Sie sehen hier noch einmal übersichtlich die verfügbaren Kommunikations-Ports der aktiven Netzwerkdienste.



► Klicken Sie Konfigurieren von Netzwerkdiensten.

Der Network Services Settings Dialog wird angezeigt.



- Wählen Sie aus dem Dropdown-Menü Protokoll den Eintrag DaVid (Port 30000).
- Markieren Sie die Checkbox Aktivieren/Deaktivieren nicht, wenn Sie das ausgewählte Protokoll ausschalten möchten.
- Klicken Sie OK und bestätigen die nachfolgende Sicherheitsabfrage.

Abb. 3-29

Der DaVid Port 30000 ist deaktiviert. Schalten Sie nun noch Port 80 ab.

$\stackrel{\scriptstyle{\scriptstyle{\rm CM}}}{=}$ Network Services Settings - Dallmeier Device Manager 1.0.7 $ \times$								
Protokoll:	David (Port 30000)							
Aktivieren/Deaktivieren	David TLS (Port 29999)							
Wenn Sie mit dem David-Protokoll verl	Http (Port 80)							
Protokoll nicht deaktivieren. Dasselbe eine Sicherheitsfunktion, damit Sie sicl	Https (Port 443) Rtsp (Port 554)							
	DMVC (Port 3377)							
	DMVC TLS (Port 3443)							
	OK Abbrechen							

- Wählen Sie aus dem Dropdown-Menü Protokoll nun den Eintrag HTTP (Port 80).
- Markieren Sie die Checkbox Aktivieren/Deaktivieren <u>nicht</u>, wenn Sie das ausgewählte Protokoll ausschalten möchten.
- Klicken Sie OK und bestätigen die nachfolgende Sicherheitsabfrage.

Abb. 3-30

Das Gerät kann nun nicht mehr über die Ports 80 und 30000 erreicht werden und es somit auch keine unverschlüsselte Kommunikation mehr darüber möglich.

Im Dialog Netzwerkdienste sehen Sie, dass die entsprechenden Ports nun deaktiviert sind.

Abb. 3-31

Wechseln Sie in den System Tab und aktualisieren mit der Taste F5 die Geräte-Verbindnung, um auch die Anzeige der Netzwerkdienste in den System Eigenschaften zu aktualisieren.



Abb. 3-32

Hier sehen Sie, welche **Netzwerkdienste** zur Kommunikation verwendet werden.



#### 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