

KONFIGURATION

DALLMEIER DEVICE MANAGER

TLS-SETUP

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 ® gekennzeichnete Marken sind eingetragene Marken von Dallmeier electronic.

Mit *) 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.

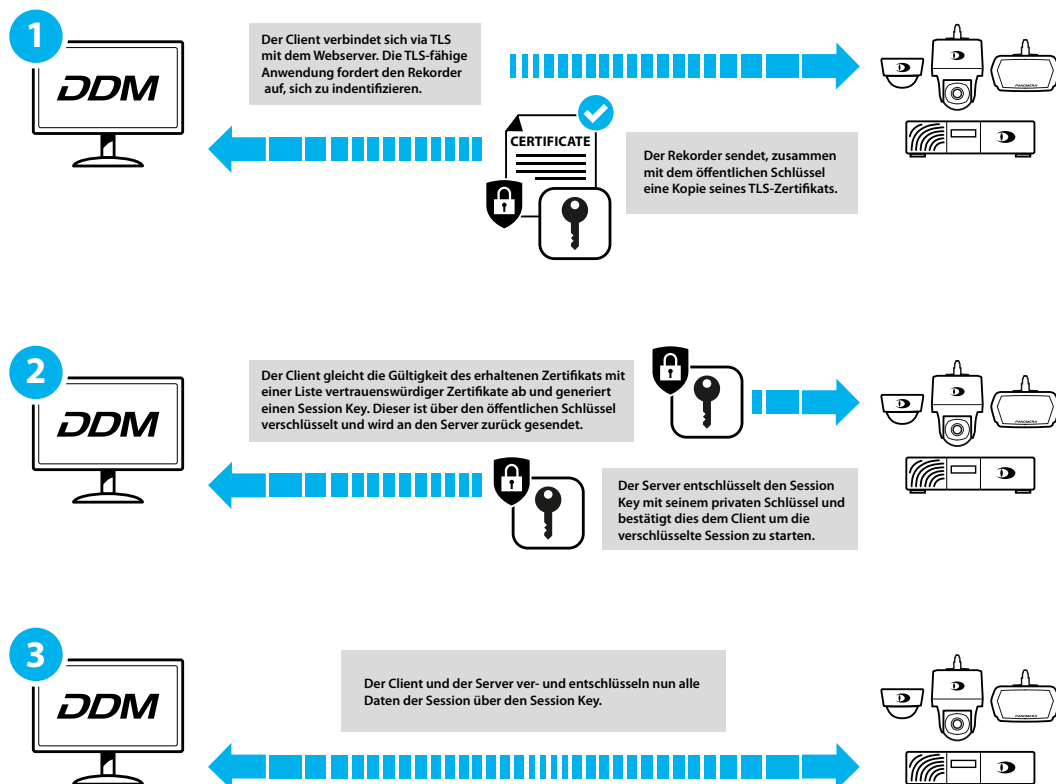
ALLGEMEINE HINWEISE

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® 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 Authority, 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.

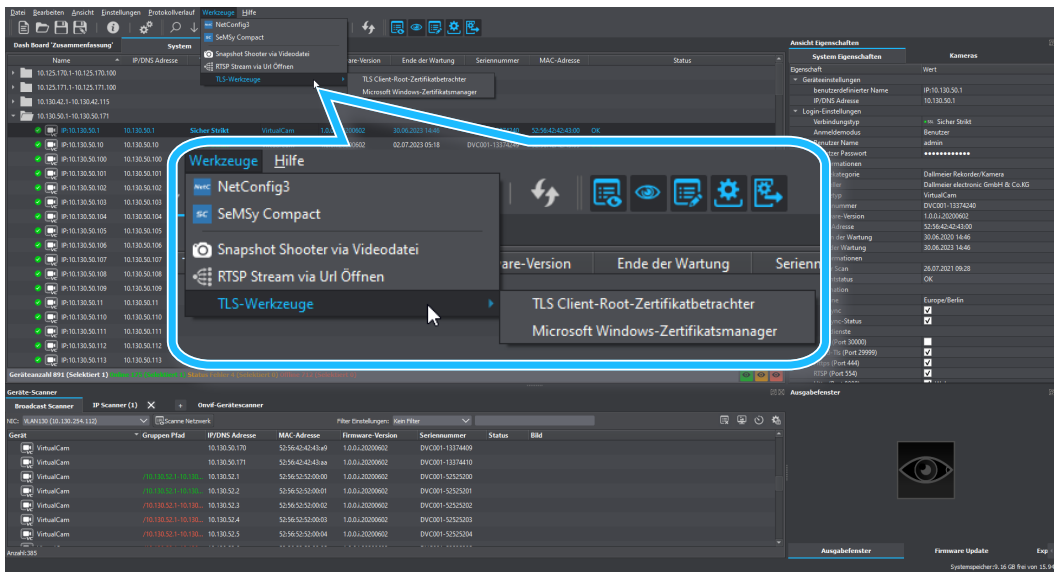


Abb. 3-1

- ▶ 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.

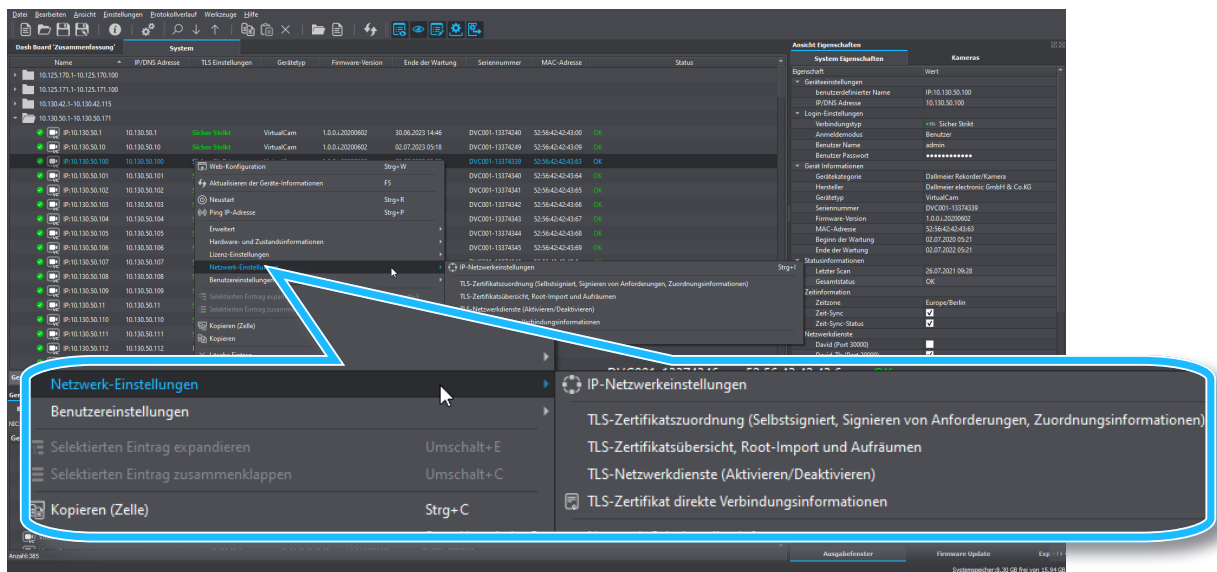


Abb. 3-2

- ▶ 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 Zertifikatszuweisungen 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 Bearbeiten, Erzeugen und Verwalten von Zertifikaten zur Verfügung.

- ▶ Wählen Sie den Tab **OpenSSL**.

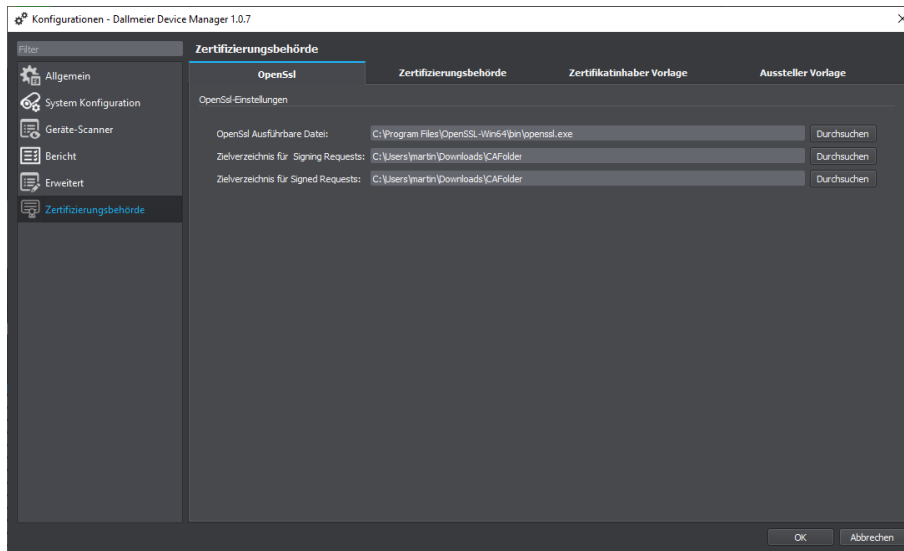


Abb. 3-3

- ▶ 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.

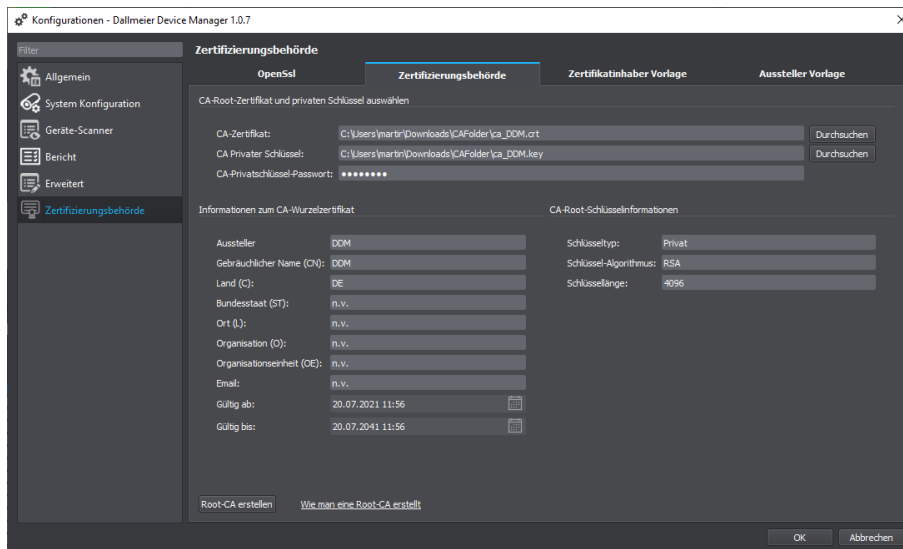



Abb. 3-4

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**.

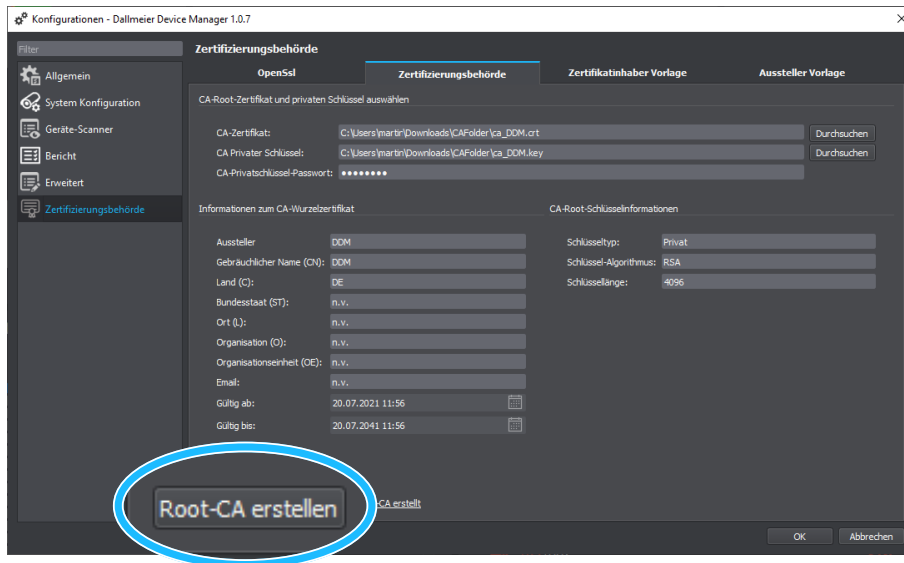


Abb. 3-5

- ▶ Klicken Sie **Root-CA erstellen**.

Der Dialog **Root-CA erstellen** wird angezeigt.

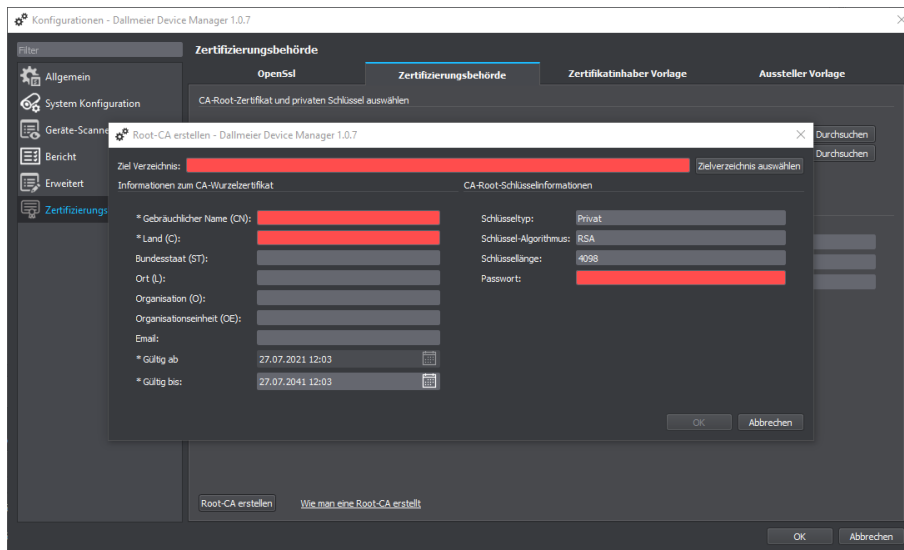


Abb. 3-6

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 angegebenen Zielverzeichnis werden folgende Dateien erstellt:

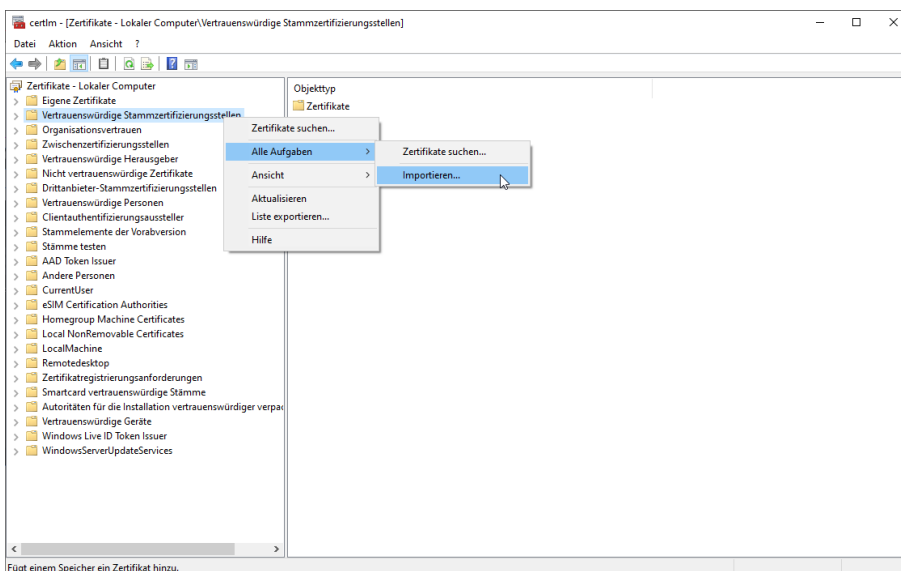
- **ca_common-name.crt** – das Root-Zertifikat
- **ca_common-name.key** – der private Schlüssel

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**.



- ▶ Rechtsklicken Sie den Eintrag **Vertrauenswürdige Stammzertifizierungsstellen**, um das Kontextmenü anzuzeigen.
- ▶ Wählen Sie **Alle Aufgaben > Importieren....**

Abb. 3-7

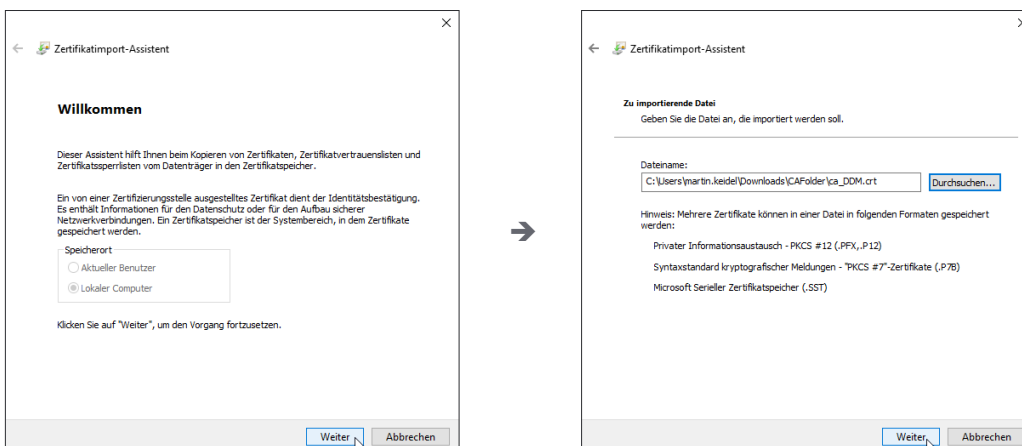


Abb. 3-8

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

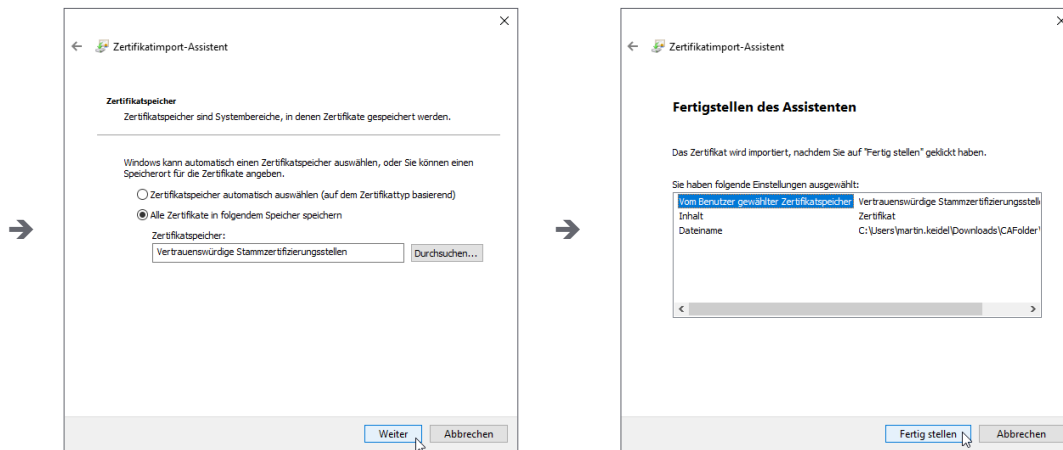


Abb. 3-9

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

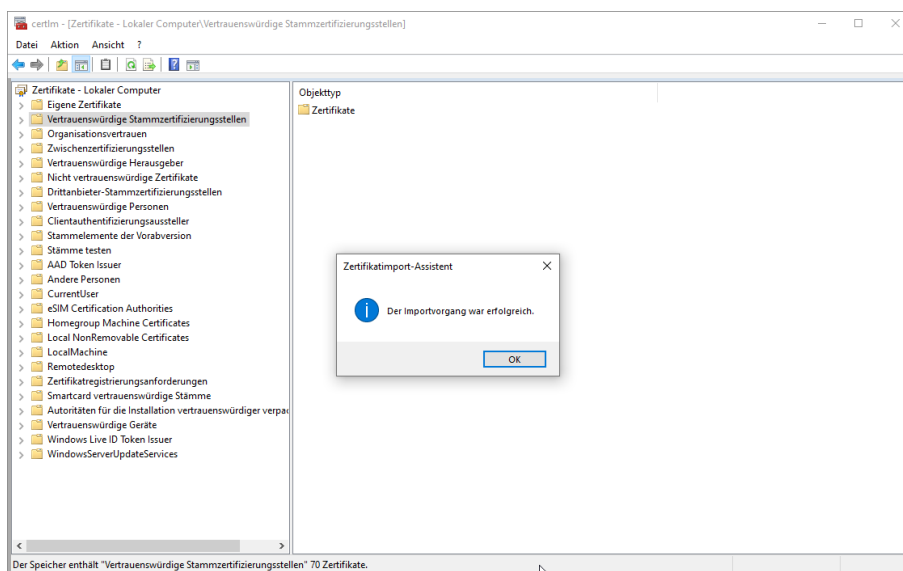


Abb. 3-10

- ▶ 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.

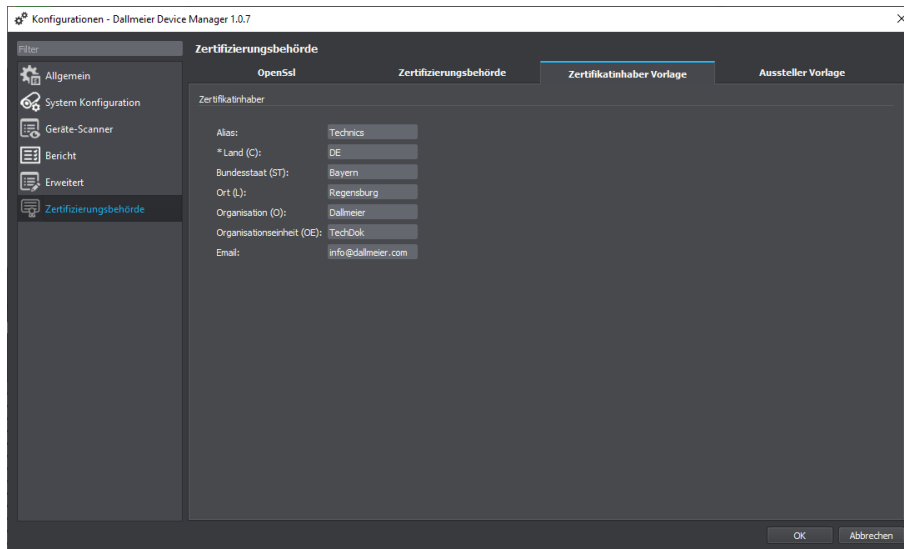


Abb. 3-11

- ▶ 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.

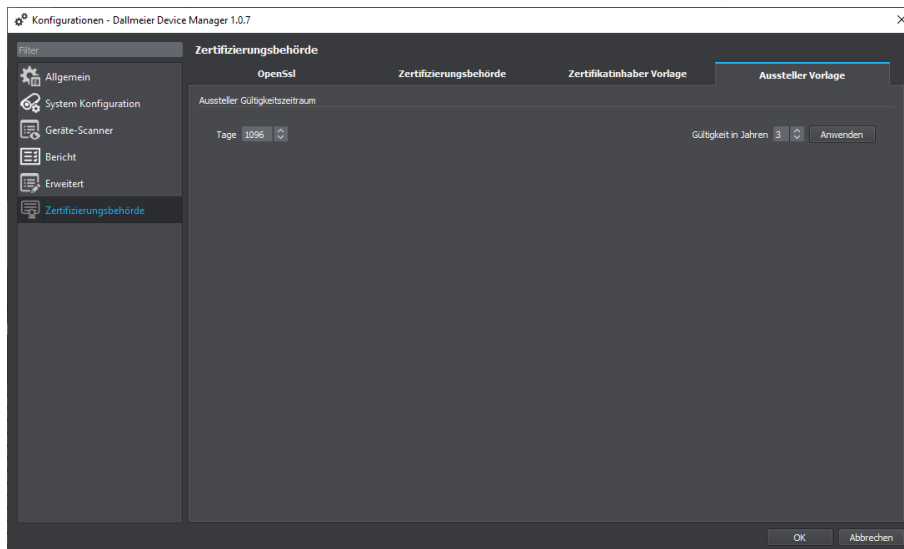


Abb. 3-12

- ▶ 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.

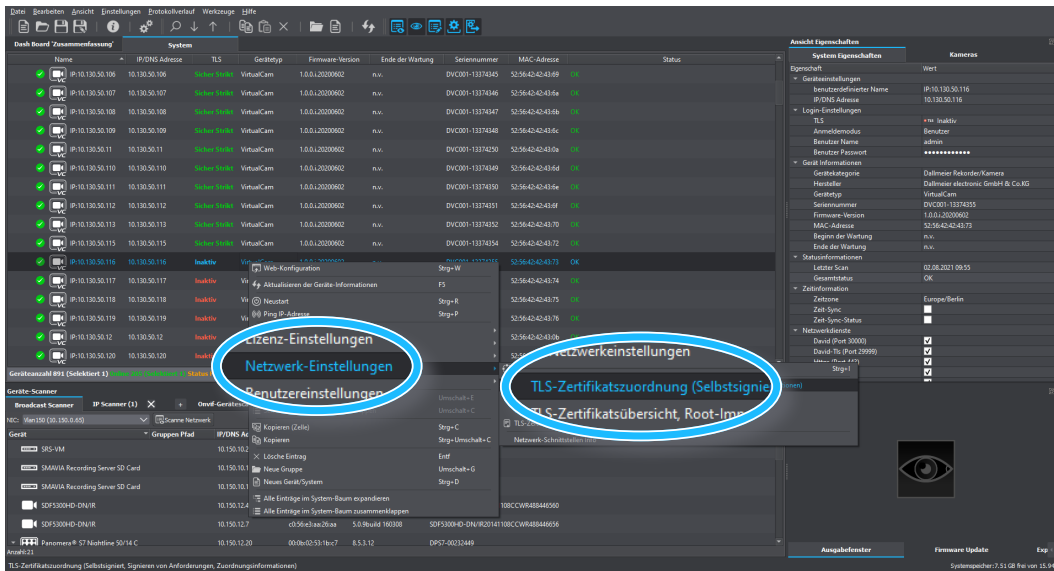


Abb. 3-13

- ▶ 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.

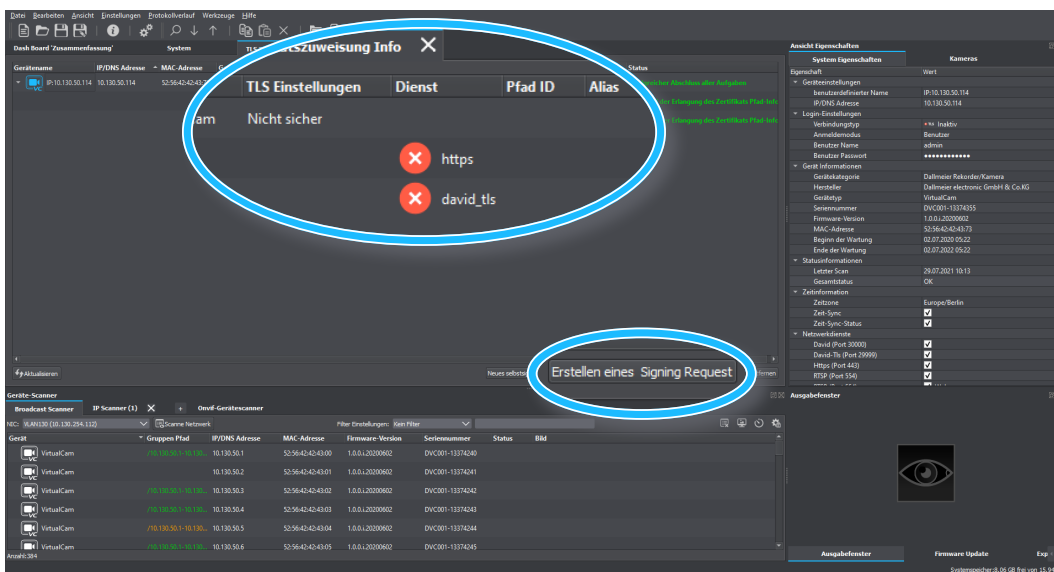
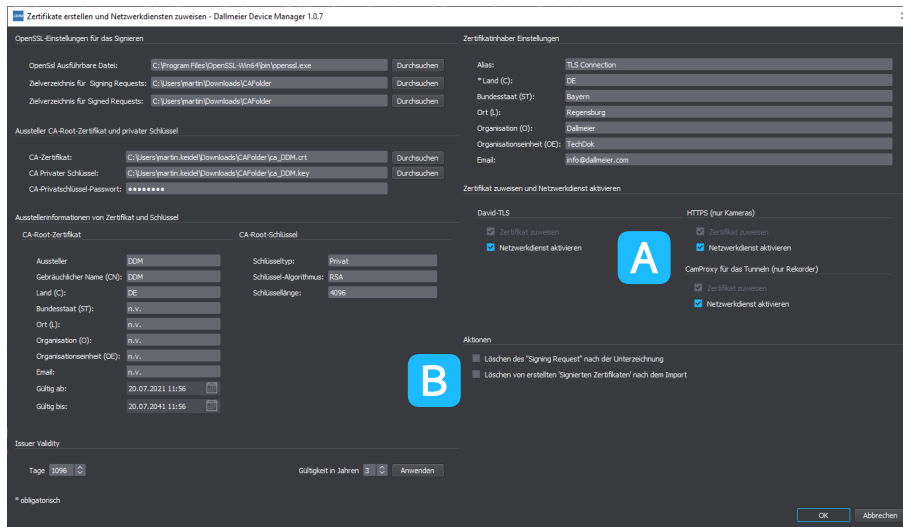


Abb. 3-14

- Klicken Sie **Erstellen eines Signing Request**.

Der Dialog **Zertifikate erstellen und Netzwerkdienste zuweisen** wird angezeigt.



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 Checkboxes hier aktivieren.

- Klicken Sie **OK** und bestätigen Sie die nachfolgende Sicherheitsabfrage, um den Vorgang der Zertifikaterstellung zu starten.

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

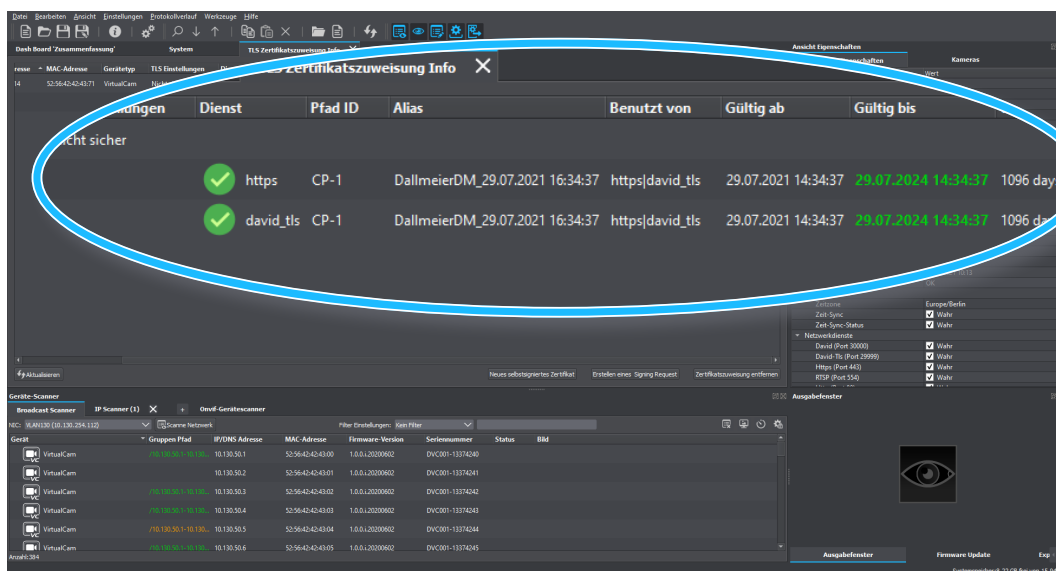


Abb. 3-16

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.

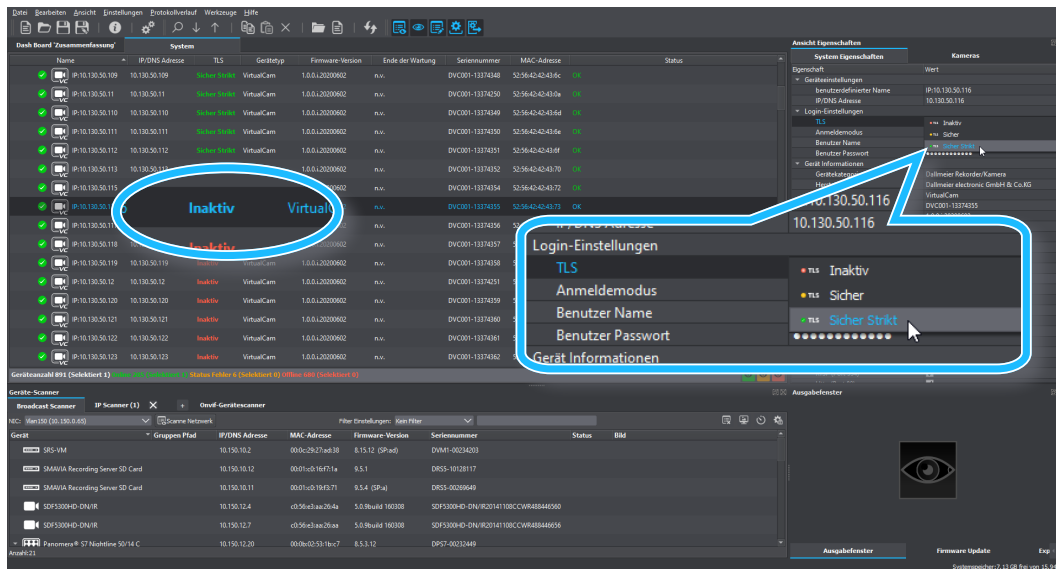


Abb. 3-17

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.

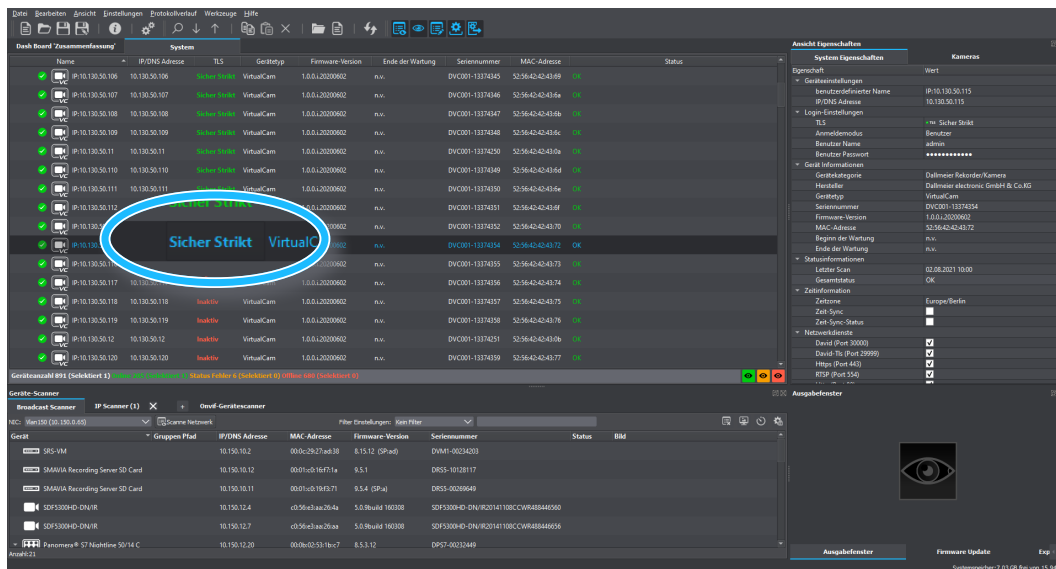


Abb. 3-18

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.

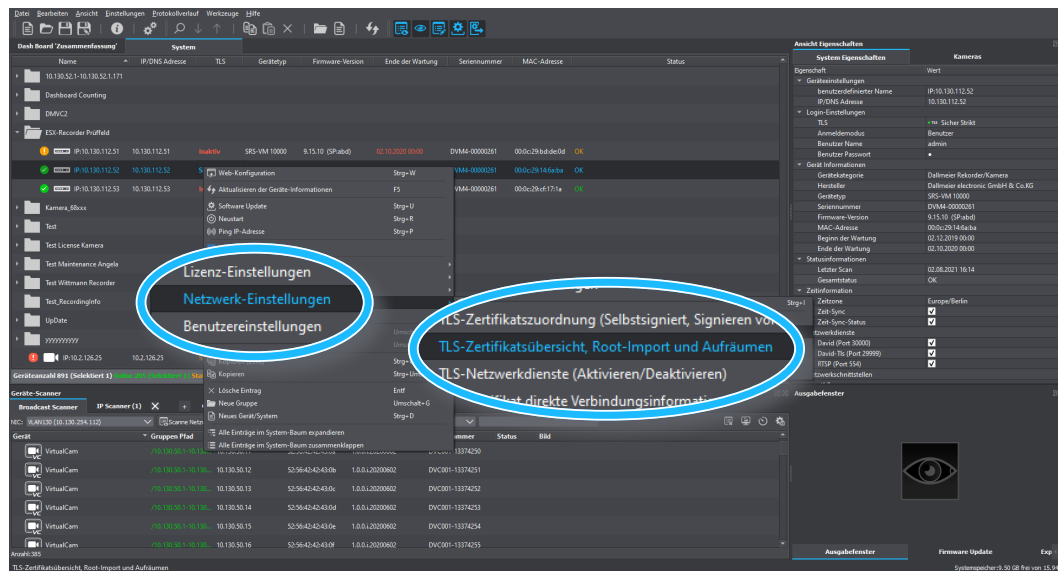


Abb. 3-19

- ▶ Wählen Sie **Netzwerk > TLS-Zertifikatsübersicht**.

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

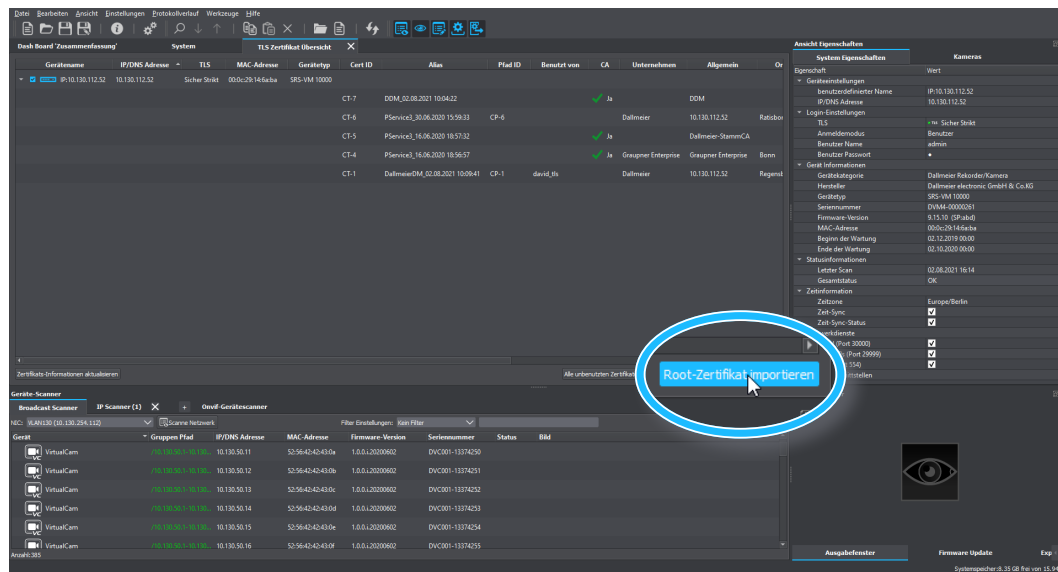


Abb. 3-20

- ▶ Klicken Sie **Root-Zertifikat importieren**.

Der Dialog **Stammzertifikat importieren** wird angezeigt.

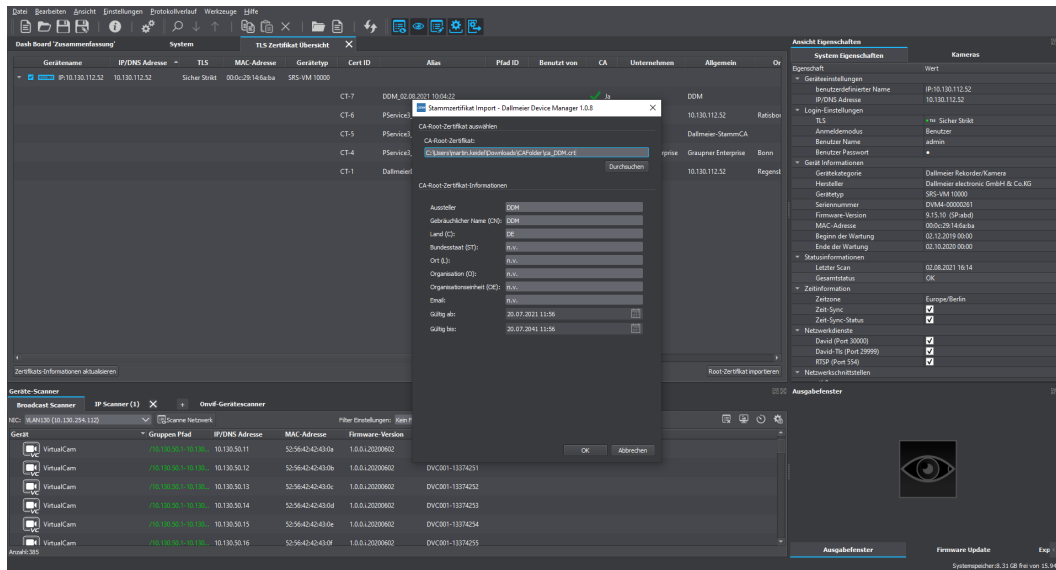


Abb. 3-21

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 DaVid TLS über Port 29999 aktivieren und den DaVid Port 30000 ausschalten, um unverschlüsselte Kamera-Verbindungen darüber nicht mehr zuzulassen.

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

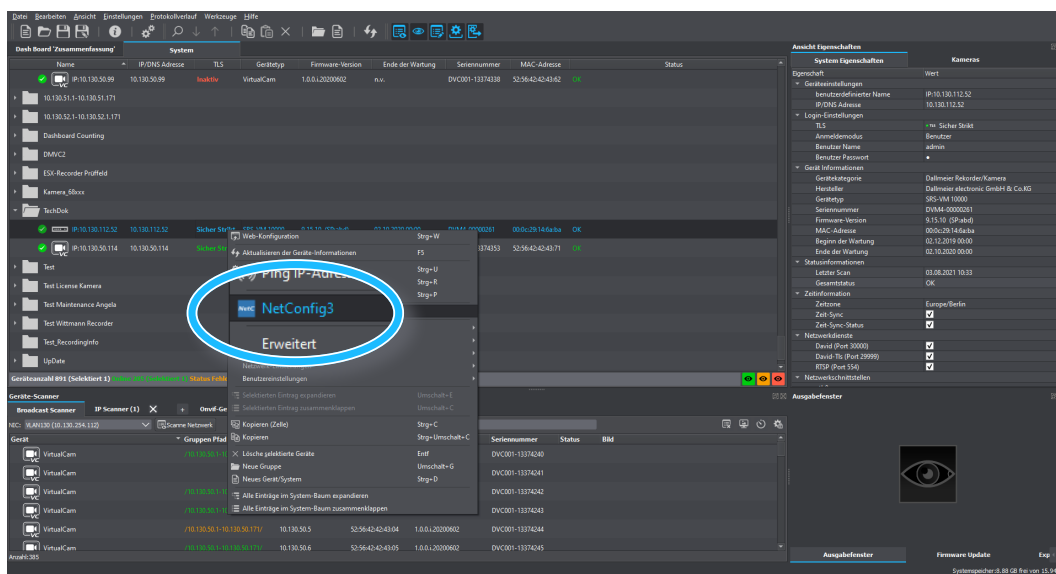
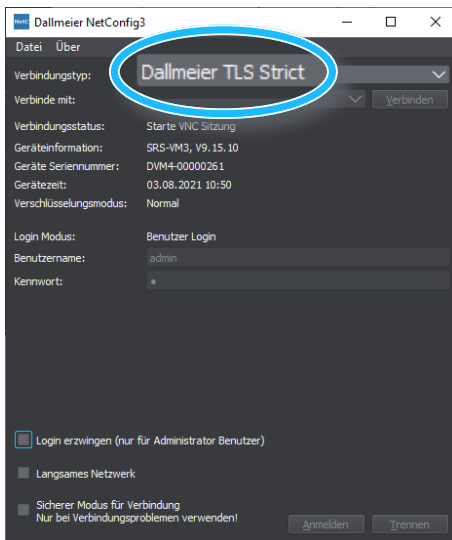


Abb. 3-22

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

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



i 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:

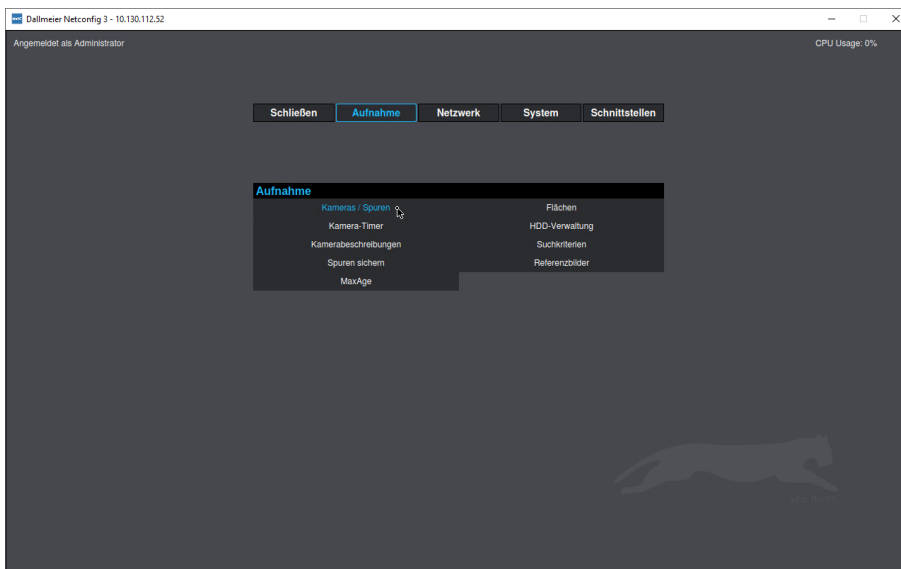


Abb. 3-24

► Wählen Sie **Aufnahme > Kameras / Spuren**.

Die Kamera-Konfiguration des Recorders wird angezeigt:

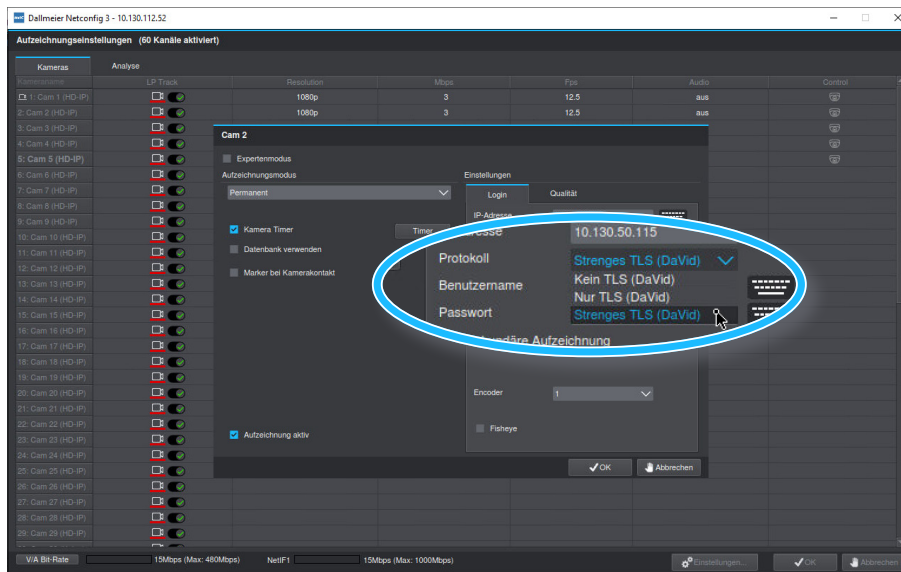


Abb. 3-25

- ▶ 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**.

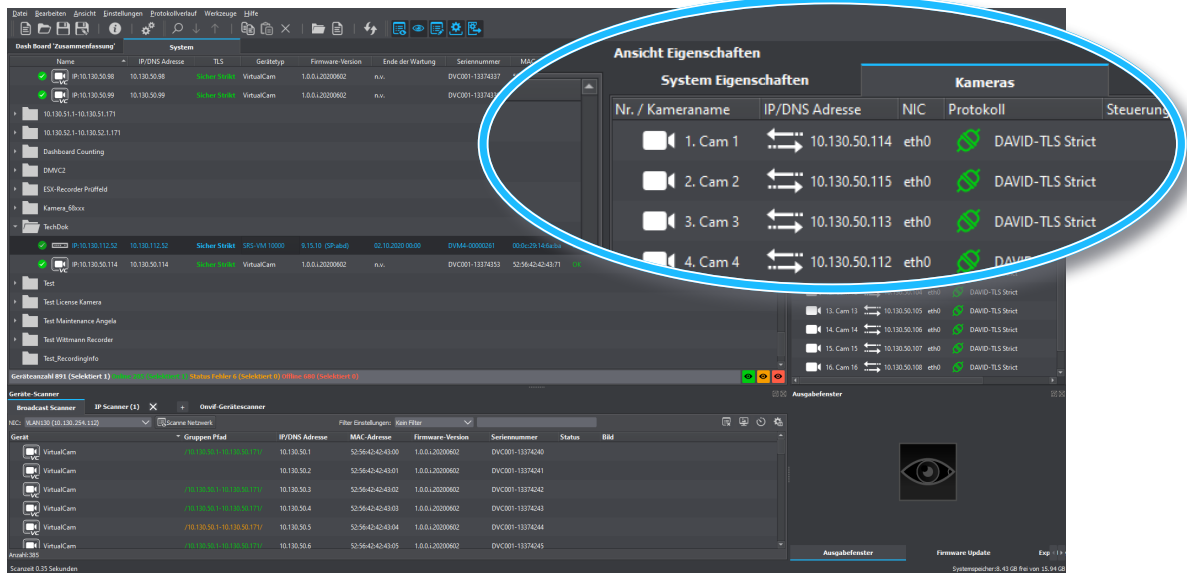


Abb. 3-26

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.

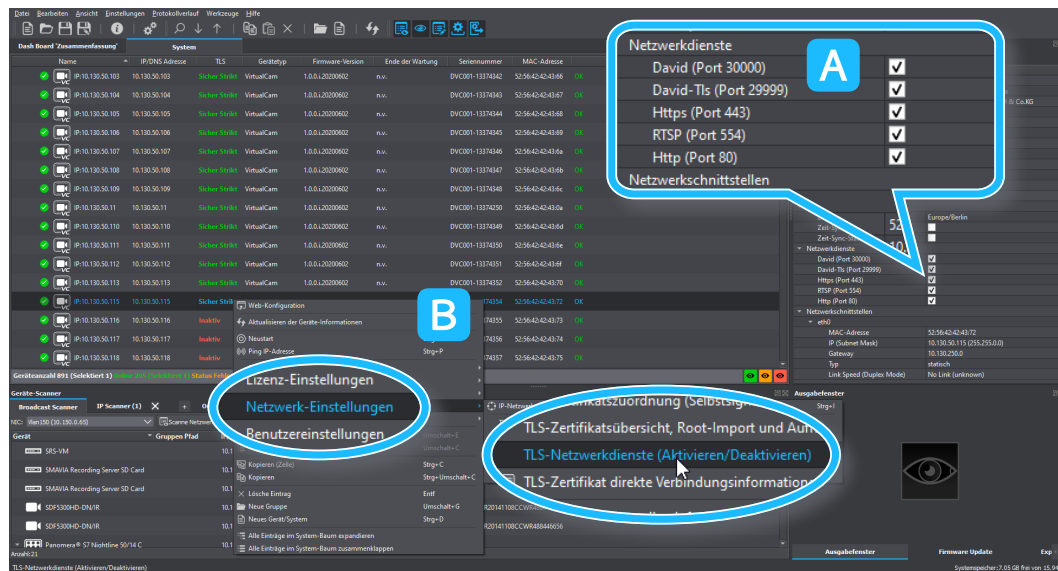


Abb. 3-27

▶ 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.

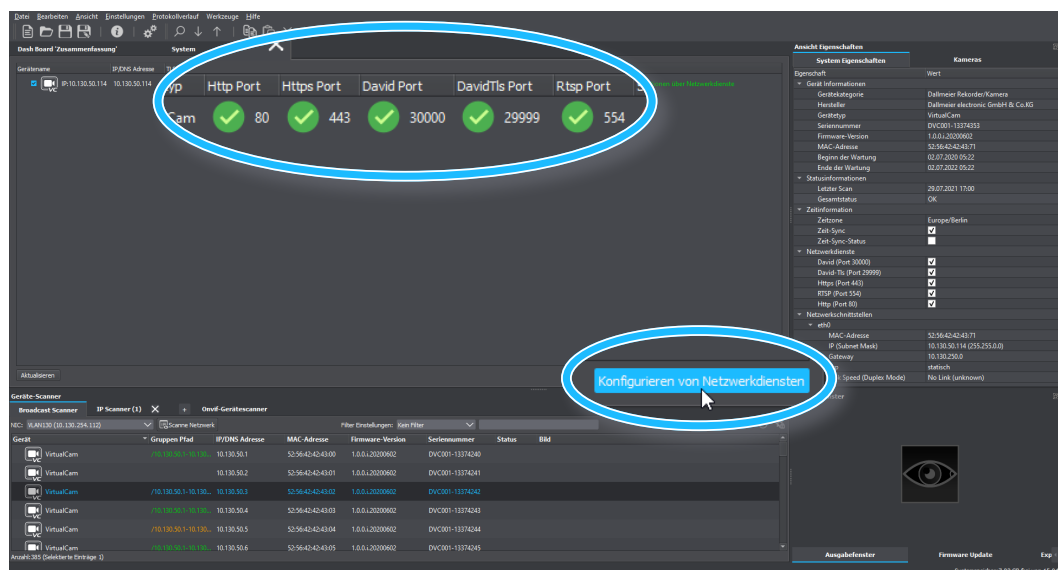


Abb. 3-28

▶ Klicken Sie **Konfigurieren von Netzwerkdiensten**.

Der **Network Services Settings** Dialog wird angezeigt.



Abb. 3-29

- ▶ 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.

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

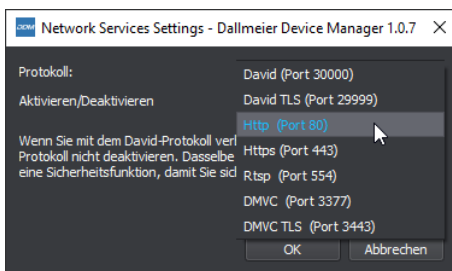


Abb. 3-30

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

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.

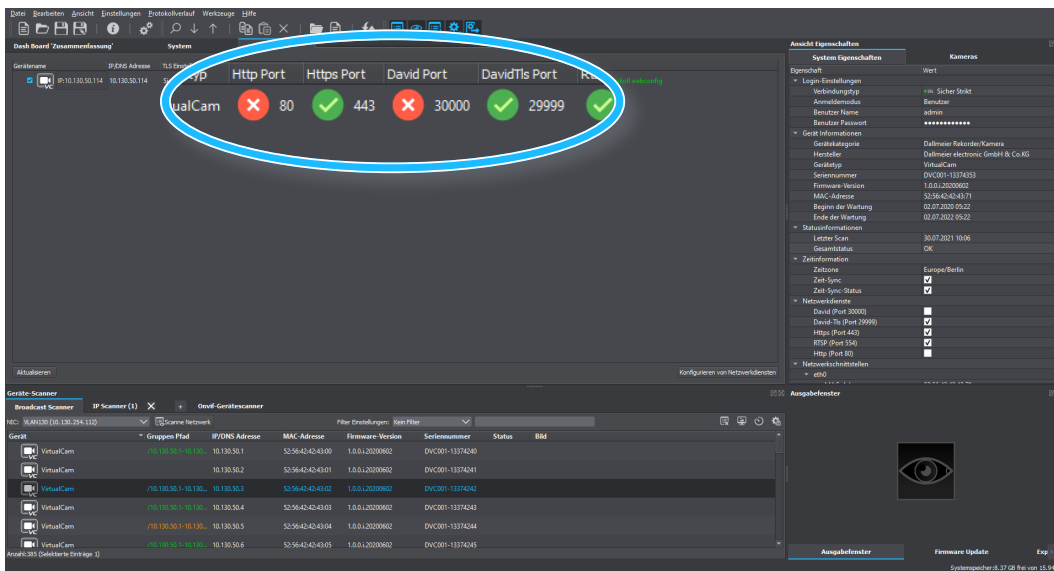


Abb. 3-31

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

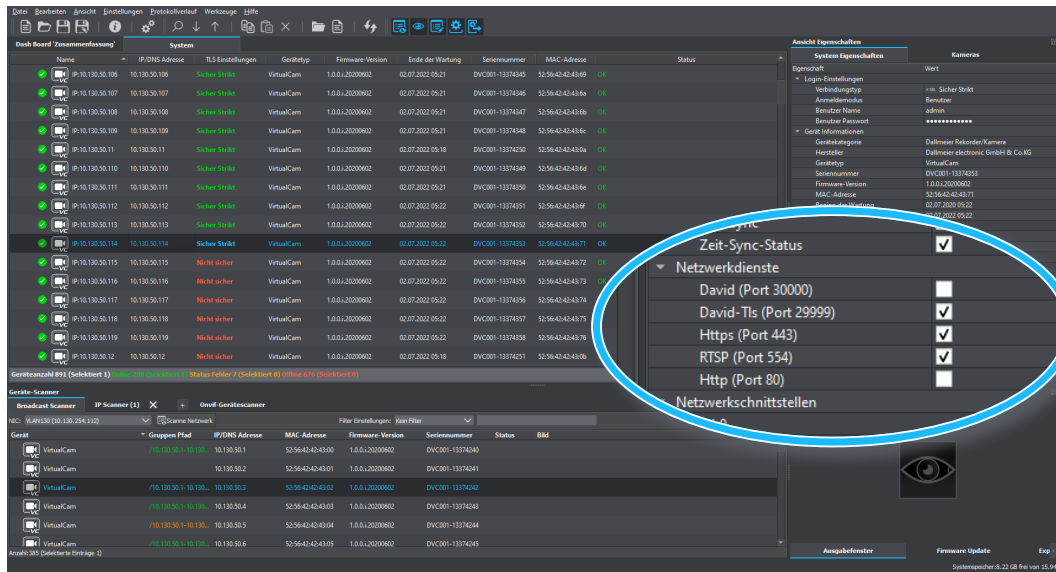


Abb. 3-32

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