



Handbuch

Qognify VMS 7.4

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Abbildungsverzeichnis	11
Impressum	12
Support	13
Funktionsübersicht	15
Intuitive Bedienbarkeit	15
Schnittstellen und Integrationen	16
Clients und Zugriffsmöglichkeiten	18
Konfiguration und Administration	20
Kerndienste und Filialen	22
Schutz von Privatsphäre und Daten: gemäß den gesetzlichen Bestimmungen	23
Konzept	24
Administrative Rechte und Benutzerrechte	24
Hierarchische Administration	24
Profile	25
Qognify VMS-Verschlüsselung	25
Umgang mit Zeitzonen	27
Der QogniFinder	27
Installation	29
Systemvoraussetzungen	31
Allgemeine Empfehlungen	32
Standardinstallation	35
Client-Installation	38
Installation eines abgesetzten Servers	38
Angepasste Installation	41
System mit dem AutoUpdater aktualisieren	45

Von SeeTec 5.4.x auf Qognify VMS aktualisieren/migrieren	50
Empfohlene Schritte vor der Migration	51
Migrationsvorgang	52
Nach dem Upgrade	54
Anmeldung	57
Die Benutzeroberfläche	65
Die Funktionsleiste	67
Die Menüelemente	68
Menü „Datei“	68
Ansicht	91
Tools	104
Info	126
Hilfe	135
Benutzer wechseln	136
Die Modusleiste	136
Die Steuerleiste	137
Suche	138
Überwachungsmodus	141
Arbeitsfläche	142
Sequenzielles Alarmfenster	145
Click-2-Track	145
Benutzerdefinierte Ansichten	147
Kamerabildsteuerung	151
Symbole der Kamerabildsteuerung	151
Miniarchiv Player	153
Manuelle Alarmaufzeichnung	154
Kamera im Bild schwenken	155
Kamerabild-Statistik	156
Lagepläne	156
Webseiten	158

Übersicht	159
Kamerasteuerung	160
Alarmliste und Systemmeldungen	170
Alarmmeldungen	170
Systemmeldungen	173
Suchen im Überwachungsmodus	174
Archivmodus	177
Archiv Player	178
Jog Dial verwenden	180
Zeitleiste / Zeitstrahl	180
Bereich bearbeiten	181
Click-2-Track	182
Verwenden des QogniFinder	183
Aufzeichnungen exportieren	186
Exportieren des Click-2-Track-Verlaufs mit dem Export Designer	187
Exportierte Videodaten auswerten	188
Schreibschutz	189
Alarme suchen	190
Mit Bookmarks arbeiten	193
Edge-Speicher-Import	195
iSearch	196
Ereignisauswertung	201
Konfigurationsmodus	207
Funktionen	208
Tastenkürzel für die Konfiguration	210
Geräte suchen	210
Suchergebnisse filtern	211
Einzelne Geräte hinzufügen	212
Mehrere Geräte hinzufügen	213

Kamera-Import per CSV- oder XML-Datei	213
Suchen im Konfigurationsmodus	217
Unternehmen und Filialen	217
Beziehung zwischen der Hauptfiliale und ihren Unterfilialen	218
Mit Filialen arbeiten	226
Mit der Sitemap arbeiten	227
Bearbeitungsmenü im Steuerelement Administration	229
Kameras	231
Kamera manuell anlegen	231
Kamera mit dem Assistenten anlegen	234
Die am Körper getragene AXIS-Kamerasteuerung	239
Kamera konfigurieren	242
Archivkamera konfigurieren	290
Mehrere Kameras konfigurieren	291
Mehrere Kameras gleichzeitig auswählen und deselektieren	292
Bewegen von Kameras	292
Kamera duplizieren	293
Kamera löschen	295
Kamera umwandeln	295
Sonstige Hardware	296
Neue Hardware anlegen	296
Hardware konfigurieren	298
Hardware löschen	298
Third Party Interface	298
Qognify	309
Qognify Video Analytics	315
Advantech	339
AXIS	342
W&T	344
Wago	346
Event Interfaces	349
Event Interface anlegen	350

Generische Zutrittskontrolle erstellen	351
Event Interfaces konfigurieren	352
Symbole für mehrere Zustände anlegen	356
Event Interfaces löschen	356
Benutzer	357
Benutzer anlegen	357
Benutzer konfigurieren	358
Benutzer löschen	367
Benutzer duplizieren	367
Gruppen	367
Neue Gruppe anlegen	368
Gruppe konfigurieren	368
Gruppe löschen	375
Gruppe duplizieren	375
Profile	375
Allgemein	376
Bildeinstellungen	377
Videowand-Modulmapping	380
Zeitverwaltung	381
Betriebskalender	385
Betriebskalender bearbeiten	385
Alarmer	386
Alarmszenario anlegen	387
Alarmszenario mit dem Assistenten anlegen	387
Alarm konfigurieren	391
Alarm löschen	403
Alarm duplizieren	403
Ansichten	404
Lagepläne und „Erweiterte Lagepläne“	407
Neuen Lageplan anlegen	408
Konfiguration eines Standardlageplans	408
Konfiguration eines erweiterten Lageplans	412

Lageplan löschen	416
Lageplan duplizieren	416
Buttons	416
Neuen Button anlegen	417
Button konfigurieren	417
Button löschen	419
Button duplizieren	419
Webseiten	420
Neue Webseite anlegen	420
Webseite konfigurieren	421
Webseite löschen	421
Webseite duplizieren	422
Wächterrundgänge	422
Neuen Wächterrundgang erstellen	422
Wächterrundgang konfigurieren	422
Wächterrundgang löschen	426
Wächterrundgang duplizieren	426
Sequenzen	426
Neue Sequenz erstellen	427
Sequenz konfigurieren	427
Sequenz löschen	430
Sequenz duplizieren	430
Videowände	430
Neue Videowand erstellen	430
Videowand konfigurieren	431
Videowand löschen	431
Videowand duplizieren	432
Kennzeichengruppen	432
Neue Kennzeichengruppe anlegen	432
Kennzeichengruppe konfigurieren	433
Kennzeichengruppe löschen	433
Kennzeichengruppe duplizieren	434

Server	434
Konfigurieren des Hauptdienstes	435
Device Manager (DM) konfigurieren	436
Globale OCR-Einstellungen konfigurieren	444
LPR-Modul konfigurieren	446
Qognify Analytics Server 3D-Modul konfigurieren	450
Analytics Interface-Modul konfigurieren	450
Gateway-Service-(SGS-)Modul konfigurieren	452
Transcoding-Modul konfigurieren	453
Bewegungserkennungsmodul konfigurieren	455
Konfiguration des QMM-Server-Moduls	455
Modul „Generischer DVR“ konfigurieren	456
Generisches Zutrittskontrollmodul konfigurieren	457
Qognify Event Interface-(QEI-)Modul konfigurieren	457
Konfigurieren eines Body-Worn Camera Connector Moduls	458
System	462
Videoklassifikation konfigurieren	463
Konfigurieren der Alarm-Klassifizierungen	465
Backup konfigurieren	466
Ereignisverwaltung konfigurieren	468
SMTP-Server konfigurieren	476
E-Mail-Verwaltung konfigurieren	477
SNMP-Server konfigurieren	477
NAT-Liste konfigurieren	479
Entitäten-Nummerierung konfigurieren	479
Alarm-WatchDog konfigurieren	481
Ton- und Symboldateien mit benutzerdefinierten Medien verwalten	482
Benutzer-Sicherheitseinstellungen konfigurieren	484
Erstellen von Entitätsetiketten	485
LPR-Modus	487
AdminTools	491
UpdateService Konfigurationstool	492

UpdateService konfigurieren	493
Gruppe konfigurieren	495
Globale Datenquelle	497
Serverkonfiguration bearbeiten	499
Updates und Patches auf den UpdateAgent importieren	501
Qognify Administrationstool	501
Allgemeine Einstellungen	502
Verwaltungsdatenbank (MaxDB)	503
MultimediaDatabase	505
OPC-Dienst	509
Sicherheit	510
Qognify ServiceManager	511
Displaysprache umstellen	511
Einstellungen bearbeiten	512
Dienste starten und stoppen	512
Qognify VMS VA Administrationstool	513
Displaysprache umstellen	514
Neue Konfigurationsdatei erstellen	514
LPR-Modul hinzufügen	515
Analytics Server-Modul hinzufügen	516
Transcodierungs-Engine-Modul hinzufügen	518
Gateway-Service-Modul (SGS) hinzufügen	519
Analytics Interface-Modul hinzufügen	521
Modul zur serverbasierten Bewegungserkennung hinzufügen	522
Generisches Zutrittskontrollmodul hinzufügen	524
AV-Export-Modul konfigurieren	525
Qognify Event Interface-Modul hinzufügen	527
Hinzufügen eines Body-Worn Camera Connector Moduls	529
Konfigurationseinstellungen exportieren	531

Kommandozeilenparameter	533
Tastenkürzel	537
Anywhere Viewer	539
Sprache der Benutzeroberfläche umstellen	540
Aufzeichnung importieren und abspielen	540
Aufzeichnung exportieren	544
Qognify VMS Web Client	545
Web Client-Dienste auf dem Qognify-Server installieren	546
Mit Qognify Web Client verbinden	546
Anmerkungen, Einschränkungen und bekannte Probleme	547
IIS härten	548
Der Qognify VMS Mobile Client	551
Mobile Client-Dienste auf dem Qognify-Server installieren	552
Mobile Client auf einem Mobilgerät installieren	552
Qognify Mobile Client auf dem Mobilgerät konfigurieren	553
Anmerkungen, Einschränkungen und bekannte Probleme	553
Mit Qognify Mobile Client verbinden	554
Installation des Qognify Metadata Manager (QMM)	555
Installation und Upgrade	556
Kameraeinstellungen	570
Fehlerbehebung	572
Der Alarm-WatchDog	573

Abbildungsverzeichnis

Lagepläne - Kamerasymbol-Einstellungen	410
Lagepläne - Buttonsymbol-Einstellungen	411
Lagepläne - Alarmsymbol-Einstellungen	411
Lagepläne - Kamerasymbol-Einstellungen	414
Lagepläne - Buttonsymbol-Einstellungen	415
Lagepläne - Alarmsymbol-Einstellungen	415

Impressum

Das vorliegende Dokument ist Bestandteil der von Qognify - nachstehend Hersteller genannt - gelieferten Software und beschreibt die Verwendung und Konfiguration der Software und der zugehörigen Komponenten.

Die englische Fassung der Anleitung ist die Originalanleitung. Alle Übersetzungen wurden auf der Grundlage der Originalanleitung erstellt.

Urheberrecht

Dieses Dokument ist urheberrechtlich geschützt. Die Weitergabe der darin enthaltenen Informationen an Dritte ist ohne ausdrückliche Genehmigung durch den Hersteller nicht zulässig. Zuwiderhandlungen ziehen Schadensersatzforderungen nach sich.

Patent- und Kopierschutz

Im Falle der Erteilung eines Patent-, Gebrauchsmuster- oder Geschmacksmusterschutzes sind alle Rechte vorbehalten. Marken- und Produktnamen sind Marken oder registrierte Marken ihrer jeweiligen Unternehmen oder Organisationen.

Adresse

Qognify GmbH
Werner-von-Siemens-Str. 2-6
D-76646 Bruchsal, Deutschland
Tel.: +49 (0)7251/9290-0
Telefax: +49 (0)7251/9290-815
E-Mail: info.emea@qognify.com
Internet: <https://www.qognify.com>

Haftungsausschluss

Änderungen vorbehalten. Vorschläge zur Verbesserung dieser Dokumentation nehmen wir gerne entgegen. Beachten Sie dazu den Abschnitt „[Support](#)“ auf der [gegenüberliegenden Seite](#).

Version

Das vorliegende Handbuch bezieht sich auf Qognify VMS 7.4 (Version 7.4.x).

Support

Softwareproblem melden

Wenn Sie ein Softwareproblem entdecken, melden Sie dies bitte über das Helpdeskportal unter:

<https://www.qognify.com>.



Wenn Sie Hilfe zu diesem Handbuch benötigen, geben Sie auch die Versionsnummer des Handbuchs an, da dieses regelmäßig aktualisiert wird und die installierte Version möglicherweise veraltet ist (siehe „[Version](#)“ auf der [vorherigen Seite](#)).

Wenn der AutoUpdater installiert und konfiguriert ist (siehe „[System mit dem AutoUpdater aktualisieren](#)“ auf [Seite 45](#)), prüft der UpdateClient automatisch auf neue Versionen der Software und der Onlinehilfe.

Funktionsübersicht

Dieser Abschnitt bietet eine Übersicht über die Funktion der verschiedenen Teile des Qognify VMS-„Ökosystems“ und deren Einbindung.

Intuitive Bedienbarkeit

Qognify VMS ist intuitiv und ohne lange Einarbeitungszeit nutzbar - damit Sie sich auf das Wesentliche konzentrieren können. Das fängt schon bei der modernen Benutzeroberfläche an: aufgeräumt und klar strukturiert. Qognify VMS kombiniert damit die Vorteile moderner Bedienkonzepte mit bewährter Funktionalität und Ergonomie - wie zum Beispiel im blendfreien Nachtmodus.

So behalten Sie den Überblick und können schnell auf Ereignisse reagieren - egal, ob Sie gerade im Überwachungs-, Archiv- oder Konfigurationsmodus arbeiten. Ein Vorteil, der immer größer wird, je mehr Bildquellen und Standorte in einem Unternehmen gleichzeitig im Blick behalten werden müssen.

Effizientes Alarm-Management

- Mit Alarmzähler und Toast Messages bleiben auch im Archivmodus alle aktuellen Alarme jederzeit „auf dem Schirm“.
- Mehr Übersichtlichkeit durch Klassifizierung der Alarme: Alarmarten lassen sich im Archivmodus durch verschiedenfarbige Alarmspuren auf einen Blick unterscheiden.
- Besseres Verständnis von Ereignissen dank der Alarmansicht, in der auf einem Bildschirm angezeigt wird, was vor dem Alarm geschehen ist, wodurch der Alarm ausgelöst wurde und was im Moment passiert.

Zeitsparende Funktionen

- Mehrfachkonfiguration für gleichzeitiges Bearbeiten mehrerer Kameras in einem Arbeitsschritt - auch über mehrere Standorte hinweg
- Kameraauswahl per Lasso direkt im Lageplan - für schnelles Erfassen von Situationen
- Aufschaltung von Ansichten auf Videowände per Drag & Drop

Schnittstellen und Integrationen

Qognify VMS lässt sich über Schnittstellen nahtlos in bestehende und neue Systemumgebungen einbinden. Besonders in großen Projekten mit mehreren untereinander kommunizierenden Anwendungen oder vielen Standorten ist dies eine wesentliche Voraussetzung. Hier lässt Qognify VMS keine Wünsche offen: Neben der direkten Integration einer Vielzahl von Hardware- und Software-Lösungen wird eine Reihe von Standards und Protokollen unterstützt - auch jenseits klassischer Sicherheitsanwendungen.

Das bietet auch wirtschaftliche Vorteile: Bei Neuinstallationen fällt der Aufwand gering aus, denn Qognify VMS integriert sich mühelos in bestehende Systemumgebungen. Durch die große Integrationsbreite können auch ältere Geräte und Systeme weiter verwendet werden - für nachhaltige Lösungen.

Hardware-Integration

- Qognify VMS ist herstellerunabhängig, über 1.000 Kameramodelle von etwa 40 Herstellern werden unterstützt. Wir verfolgen den Ansatz einer möglichst tiefen Integration und unterstützen z. B. Funktionen wie Multi Streaming, virtuelle Kameras oder Bewegungserkennung auf dem Endgerät.
- Zusätzlich können viele weitere Kameramodelle über den ONVIF-Standard eingebunden werden.
- Analogkameras und -systeme werden über Videosever integriert und können so weiter genutzt werden.
- Über I/O-Module können Steuersignale gesendet und empfangen werden - so lassen sich beispielsweise Türen über einen Klick in der Qognify-Oberfläche öffnen.

Systemintegration

- Branchenspezifische IT-Systeme wie Kassen- und Warenwirtschaftslösungen werden über ein treiberbasiertes Konzept einfach und schnell integriert.
- Sicherheitssysteme wie Gebäudemanagement- und PSIM-Systeme, Zutrittskontrollsysteme, Einbruch- und Brandmeldesysteme sowie Wachzentralen- und Leitstandslösungen werden über Schnittstellen eingebunden.
- Weitere Drittsysteme sind über Network I/Os und TCP-Trigger integrierbar - so kann beispielsweise ein Ereignis in der Zutrittskontrolle einen Alarm in Qognify VMS auslösen.
- VoIP-fähige Geräte können über die Integration verschiedener SIP-Server angebunden werden - dies ermöglicht bidirektionale Sprachkommunikation zwischen Clients und Sprechstellen direkt in Qognify VMS.
- Qognify VMS unterstützt über eine Serverschnittstelle den führenden systemübergreifenden Standard in der Automatisierungs- und Sicherheitstechnik: OPC UA. So lassen sich beispielsweise Anbindungen an Zutrittskontroll- oder Gebäudemanagementsysteme realisieren.

Analytics-Integration

Server- oder kamerabasierte Analyse-Anwendungen anderer Hersteller können flexibel über das standardisierte Qognify Analytics Interface integriert werden. Derzeit

sind Plugins der folgenden Anbieter zertifiziert:

- Agent VI
- CogVis
- Securiton IPS (ACAP-basierte Analyse)
- Axis Perimeter Defender
- Digital Barriers SafeZone Edge

Es sind auch weitere Plugins verfügbar. Weitere Informationen finden Sie im Abschnitt [„Generischer VCA-Kanal“ auf Seite 316](#).

SDK - Software Development Kit

Qognify VMS kann auch in Fremdsysteme integriert werden - mit Hilfe eines detailliert dokumentierten Software Development Kits.

Clients und Zugriffsmöglichkeiten

Qognify VMS bietet Zugriffsmöglichkeiten und Übertragungslösungen, die es Ihnen erlauben, Ihr Unternehmen stets und von überall aus zu überwachen. Ihre Daten sind stets sicher - geschützt durch unsere umfassenden Funktionen für Datenschutz und Verschlüsselung.

Windows Client

Windows-basierter Client, der die vollständige Systembedienung und -verwaltung ermöglicht- im Überwachungs-, Archiv- und Konfigurationsmodus. Der Client ist für 64-Bit-Systeme verfügbar.

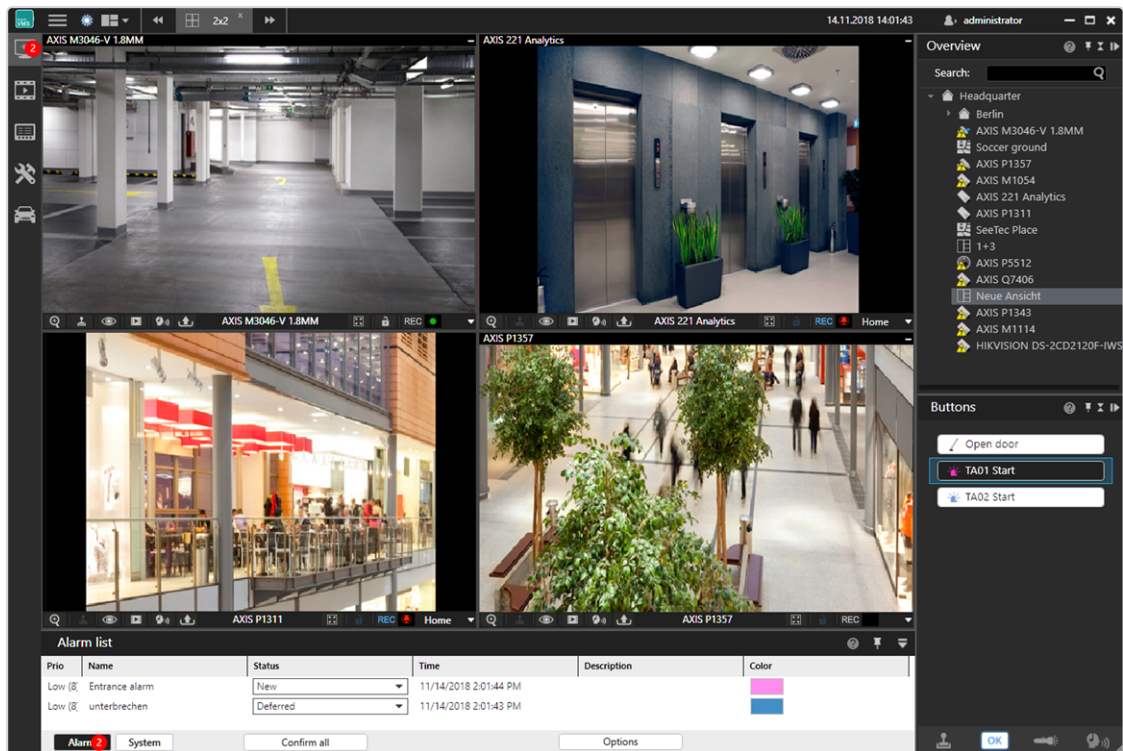


Abb. 1: Windows Client

Web Client

Der Web Client ermöglicht einen plattformunabhängigen Zugriff auf Installationen mit Qognify VMS von einem mit dem Internet verbundenen PC aus - im Überwachungs- und Archivmodus. Er kann unter Microsoft Windows, Mac OS X und Linux betrieben werden und benötigt lediglich einen aktuellen Webbrowser. Zusätzliche Plugins sind nicht erforderlich, da alle Eingangsformate (z. B. Motion JPEG, MPEG-4, H.264) über den Qognify TranscodingService in ein einheitliches Format gebracht werden.

Mobile Client

Der Mobile Client bietet über Tablets und Smartphones (iOS und Android) einen schnellen Systemzugriff von unterwegs. Neben der Live-Ansicht von Kamerabildern ermöglicht er die Archivrecherche sowie die Bearbeitung von Alarmen. Damit kann das Sicherheitspersonal zum Beispiel auch während eines Rundgangs auf Ereignisse reagieren.

Display Agent/Virtuelle Matrix

Großbildsysteme und Videowände verschiedener Hersteller können entweder über herstellerspezifische Split-Rechner oder mit Hilfe des Qognify Display Agent angebunden werden. Die Videowände können über einen herkömmlichen Qognify-Client

gesteuert werden, Ansichten und Kameras lassen sich einfach per Drag & Drop aufschalten.

Multi Installation Login

Ein Qognify Client kann mit 50 unabhängigen Qognify Installationen mit insgesamt maximal 5000 Geräten verbunden werden - mit Zugriff auf alle Kameras, Ansichten und Alarme. Dies ist die ideale Lösung für kleine Alarmzentralen oder für Gewerbebetriebe mit zentralen Sicherheitsdiensten.

Qognify VMS Anywhere Client

Der Qognify VMS Anywhere Client kann ohne vorherige Software-Installation auf jedem Windows-basierten Rechner gestartet werden. Der Qognify VMS Anywhere Client bietet alle Funktionen eines installierten Clients wie etwa Live- und Archivansicht sowie Administration und Systemkonfiguration - selbstverständlich unter Berücksichtigung der individuellen Benutzerrechte.

Konfiguration und Administration

Qognify VMS passt sich der Struktur Ihres Unternehmens an - und unterstützt so Systeme von einer bis hin zu mehreren tausend Kameras. Durch die verteilte Installation der Software auf mehreren Servern lässt sich das Gesamtsystem optimal dimensionieren und jederzeit erweitern. Dabei können die Server je nach Bedarf auch an verschiedenen Standorten stehen.

Die Architektur von Qognify VMS beruht auf einer strikten physischen Trennung von Clients und Servern. Die Speicherung der Bilddaten und die Kommunikation mit den Kameras sind als Systemdienste integriert. Deshalb muss auf dem Server weder ein eigenes Programm gestartet werden noch ist eine lokale Anmeldung nötig.

Hierarchische Administration

Jedem Benutzer können individuell und detailliert Rechte auf Kameras, deren Steuerelemente (z. B. PTZ-Steuerung) und zusätzliche Qognify VMS-Komponenten wie Buttons oder Lagepläne zugewiesen werden. Die Rechtematrix bildet das Organigramm Ihres Unternehmens ab: Selbst weltweit verzweigte Systeme mit mehreren tausend Kameras und zahlreichen Standorten lassen sich so mit Qognify VMS zentral verwalten und steuern.

Alarmszenarien - so individuell wie Ihr Unternehmen

Auch wenn sich viele Abläufe innerhalb einer Branche gleichen - jedes Unternehmen hat seine eigenen Prozesse. Qognify VMS erlaubt es Ihnen deshalb, komplexe Alarmroutinen individuell zu definieren. In einer Art Matrix können beliebige Startereignisse (z. B. Bewegungsmeldung, Ereignisse aus der Videoanalyse, I/O-Kontakt, Network I/O, Button) eine Vielzahl verschiedener Aktionen auslösen. Dazu zählen Alarmaufzeichnung und Visualisierung, Senden von Triggern an Drittsysteme über physische I/O-Kontakte oder Network I/Os, Senden von Videosequenzen per E-Mail und FTP sowie das Starten externer Programme. Für jede Alarmsituation lässt sich somit ein maßgeschneiderter Arbeitsablauf einrichten, der das Sicherheitspersonal optimal unterstützt und eine schnelle Reaktion ermöglicht.

Um das Anlegen eines Alarmszenarios so einfach wie möglich zu gestalten, bietet Qognify VMS einen Alarmassistenten, der den Benutzer Schritt für Schritt ans Ziel führt. Selbstverständlich basieren auch die Alarmszenarien auf dem detaillierten Rechkonzept von Qognify VMS und können individuellen Benutzern oder Benutzergruppen zugewiesen werden.

Ausfallsicherheit durch Failover-Konzept

Bei Qognify VMS sorgen im Störfall zwei Funktionen dafür, dass das Videosystem weiter läuft und stets erreichbar bleibt:

- Bei Ausfall eines oder mehrerer Aufzeichnungsserver übernimmt sofort ein Hot-Standby-Server die Bildaufzeichnung. Die Bilddaten müssen später nicht zurückgespielt werden (verfügbar für Qognify VMS Infinity X).
- Ist der zentrale Management-Server nicht mehr erreichbar, springt ein Proxy-Server ein, der alle relevanten Konfigurationsdaten und Zugriffsrechte zwischenspeichert. Das System arbeitet weiter im „Inselmodus“ und kann störungsfrei bedient werden.

Zusätzlich werden Microsoft Cluster und Virtualisierung unterstützt.

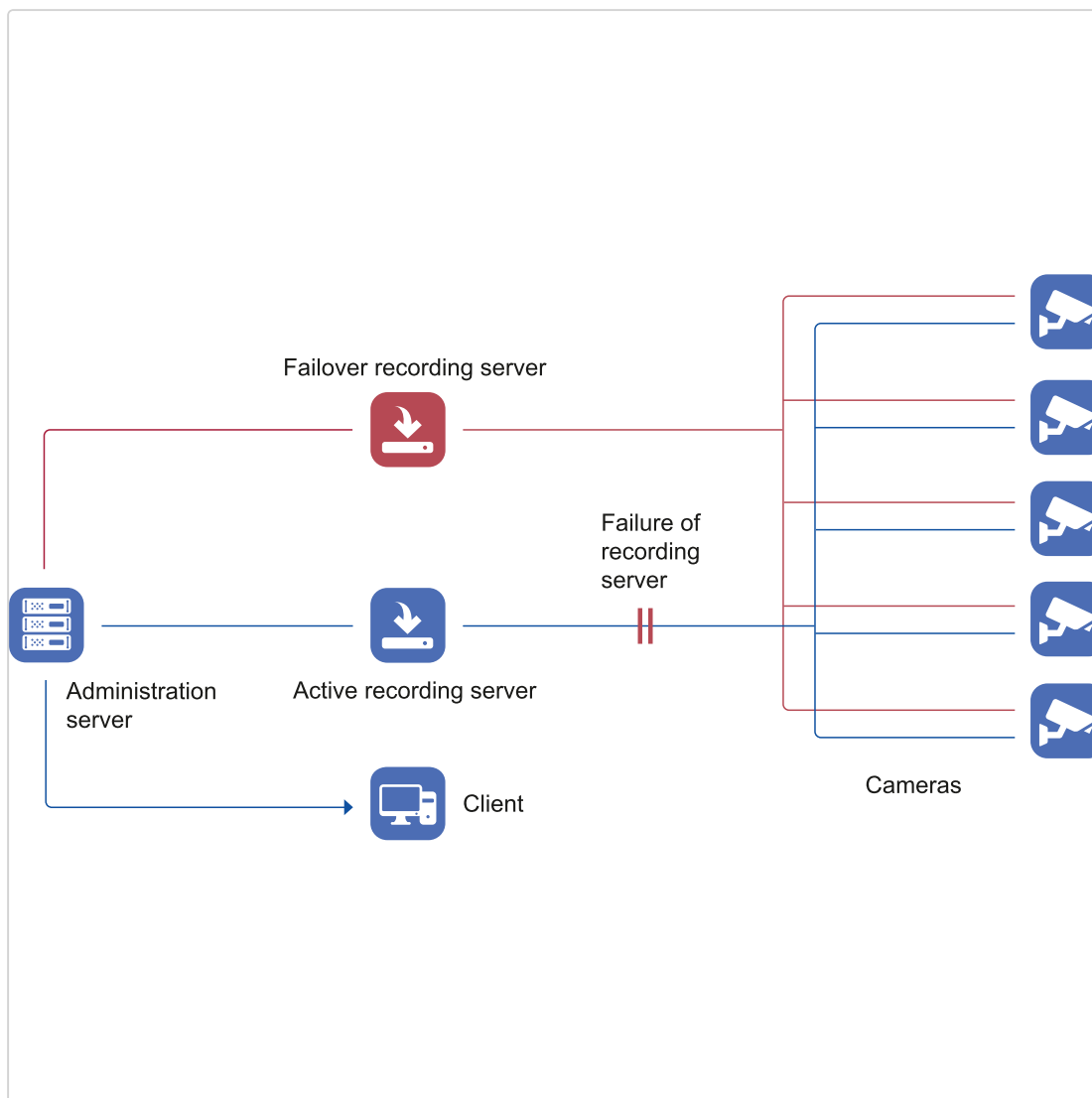


Abb. 2: Ausfallsicherheit durch Failover-Konzept

Kerndienste und Filialen

Der CoreService-Server des Unternehmens wird als „CoreService Main“ (CSM) in der Hauptfiliale installiert, konfiguriert und verwaltet. Die CoreServices der Filialen können den CSM oder einen CoreService in einer anderen Unterfiliale weder verwalten noch konfigurieren. Die CoreServices der Unterfilialen werden als „Core Service Sub“-Dienste (CSS) bezeichnet. Alle CSS werden vom CSM konfiguriert (Informationen zur Konfiguration finden Sie unter [„Konfigurieren des Hauptdienstes“ auf Seite 435](#)).

Bei einem Ausfall des CSM wechselt der CSS automatisch in einen „Inselmodus“ und stellt so die erforderlichen Dienste für die betreffende Unterfiliale bereit. Im „Inselmodus“ kann der CSS nicht konfiguriert werden. Daher sind der Konfigurationsmodus und die Ereignisauswertung nicht verfügbar.

Sobald der CSM in den Normalbetrieb zurückkehrt, kann der CSS wieder vom CSM verwaltet werden.

Schutz von Privatsphäre und Daten: gemäß den gesetzlichen Bestimmungen

Qognify VMS bietet verschiedene Mechanismen, um die Privatsphäre von Mitarbeitern, Kunden und Besuchern zu schützen. So können sensible Bildbereiche ausgeblendet oder bewegte Objekte anonymisiert werden. Zusätzlich kann der Systemzugriff über das Vier-Augen-Prinzip (Eingabe eines zweiten Passworts) abgesichert werden.

Auch auf Systemebene ist Qognify VMS gut geschützt: Die Daten zwischen Server und Client werden verschlüsselt übertragen - ein Grund, warum Qognify VMS über verschiedene Zertifizierungen z. B. für den Einsatz im Finanzsektor verfügt (siehe Zertifikate).

Privacy-Masking

Sensible Bildbereiche werden durch eine frei definierbare Fläche maskiert und im Live- und Archivbild rechteabhängig ausgeblendet. So lassen sich beispielsweise Sozialräume, öffentliche Bereiche oder Eingabefelder für Geheimzahlen aus der Videoüberwachung ausnehmen (Details finden Sie unter [„Privacy-Masking“ auf Seite 284](#)).

Motion Scrambling

Bewegte Objekte oder Objekte, die sich von einem im Vorab definierten Referenzbild unterscheiden, werden im Livebild verpixelt dargestellt und dadurch anonymisiert (Details finden Sie unter [„Privacy-Masking“ auf Seite 284](#)).

Verschlüsselung

Die Datenübertragung zwischen den Diensten in einer Qognify VMS-Umgebung wird verschlüsselt (Details siehe [„Qognify VMS-Verschlüsselung“ auf Seite 25](#)).

Zertifikate

Insbesondere für den Einsatz in der Finanzbranche verfügt Qognify VMS über die relevanten Zertifizierungen - so z. B. über das BGV-/UVV-Kassen-Zertifikat, das in Deutschland die Anforderungen für Videoüberwachung in Finanzinstituten definiert. Zudem hat die Fiducia IT AG, der größte IT-Dienstleister für Genossenschaftsbanken, Qognify VMS für die Verwendung auf ihren IT-Systemen freigegeben.

Konzept

Administrative Rechte und Benutzerrechte

In Qognify VMS können zwei Typen von Benutzern konfiguriert werden:

- **Administrator.** Standardmäßig werden ein Administrator und eine Administratorgruppe installiert. Beide können weder gelöscht noch deaktiviert werden. Beim Administrator handelt es sich um einen Benutzer mit Konfigurationsrechten, der zur Administratorgruppe gehört. Die Rechte der Administratorgruppe werden auf den Administrator vererbt. Zur Verwaltung von Filialen können Benutzern eingeschränkte administrative Rechte zugewiesen werden, sodass diese nur die Objekte (z. B. Kameras) innerhalb der Filiale verwalten, jedoch auf keine anderen Filialen zugreifen können.
- **Benutzer.** Der Benutzer hat eingeschränkte Rechte und kann Mitglied einer oder mehrerer Benutzergruppen sein. Auf einen Benutzer werden die Rechte der Gruppe bzw. Gruppen vererbt, zu der bzw. denen er gehört. Die Rechte der Benutzergruppe werden im Steuerelement Gruppe definiert (siehe „[Gruppen](#)“ auf Seite 367). Darüber hinaus kann der Benutzer über spezifische Rechte verfügen, die nicht Teil der Rechte seiner Gruppe(n) sind. Diese zusätzlichen Rechte werden im Steuerelement Benutzer definiert (siehe „[Benutzer](#)“ auf Seite 357). Die Gruppenrechte stehen über den einzelnen Benutzerrechten. Das bedeutet, dass ein Benutzer innerhalb einer Gruppe keine Ausnahmen (d. h. weiteren Einschränkungen oder „negativen Rechte“) erhalten kann, sondern nur zusätzliche Einschränkungen. Die Zugehörigkeit des Benutzers zu bestimmten Gruppen ist erkennbar an den Farbfeldern (für die Konfiguration der Farbgebung von Gruppen, siehe „[Gruppen](#)“ auf Seite 367).

Hierarchische Administration

Qognify VMS verfügt über eine mehrstufige Administration, sodass einem Benutzer Administrationsrechte für lediglich einen Teil der Installation bzw. einen Teil der Funktionen gegeben werden können.

- Eine allgemeine Beschreibung der administrativen Rechte und Benutzerrechte finden Sie unter „[Administrative Rechte und Benutzerrechte](#)“ oben.

- Informationen zum Definieren von Benutzerrechten und spezifischen Benutzerrechten finden Sie unter „[Benutzerrechte verwalten](#)“ auf Seite 361.

Das System erlaubt dazu eine Unterteilung der administrativen Rechtstufen und eine Aufteilung in eine Hauptfiliale und beliebig viele Unterfilialen. Die Unterfilialen werden als logische Einheiten mit eigenem Konfigurationskontext definiert und können nicht verschachtelt werden.

- Benutzer oder andere Entitäten wie Benutzergruppen, Lagepläne, Device Manager oder Kameras, **die zu einer Unterfiliale gehören**, werden strikt auf ihre Zugehörigkeit beschränkt, damit Benutzer nur Zugriff auf Videodaten und Konfiguration der zugehörigen Filiale erhalten.
- Benutzer oder andere Entitäten wie Benutzergruppen, Lagepläne, Device Manager oder Kameras, **die zur Hauptfiliale gehören**, sind in der Lage, auch mit Unterfilialen zu interagieren. Administrationsrechte für die relevanten Unterfilialen können explizit Benutzern oder Benutzergruppen zugewiesen werden, die zur Hauptfiliale gehören.

Das System vermeidet eine simultane Konfiguration einer Filiale durch zwei oder mehr Benutzer, erlaubt jedoch eine simultane Konfiguration unterschiedlicher Filialen durch unterschiedliche Benutzer.

Profile

Jede Benutzergruppe wird automatisch einem Profil zugeordnet, das in der Softwarekonfiguration definiert wird (siehe „[Profile](#)“ auf Seite 375). Das Profil einer Gruppe wird auf die Benutzer in der Gruppe vererbt, die Benutzer können jedoch über weitere Profile verfügen, je nachdem, zu welchen Gruppen sie gehören oder welche Profile den einzelnen Benutzern zugewiesen wurden. Wenn sich ein Benutzer anmeldet, wird er gebeten, ein Profil auszuwählen (falls mehrere Profile verfügbar und aktiviert sind). Der Administrator kann Profile für Benutzer und Benutzergruppen aktivieren bzw. deaktivieren.

Qognify VMS-Verschlüsselung

Qognify bestätigt, dass die Kommunikation zwischen den Qognify VMS-Clients und dem Qognify VMS-Server in allen Versionen der Qognify-Video-Management-Serie verschlüsselt wird.

Qognify VMS verwendet die AES-Verschlüsselung mit einer Schlüssellänge von 128 Bit.

Für die verschlüsselte Kommunikation zwischen Qognify VMS-Clients und Qognify VMS-Server (und umgekehrt) sind folgende Funktionen verfügbar:

- **Verschlüsselte**

Die verschlüsselte Übertragung ist standardmäßig aktiviert, wobei die o. g. AES-Verschlüsselung verwendet wird. Die Verschlüsselung ist immer aktiviert.

- **Passwort**

Das Passwort wird stets vom Qognify VMS-Client an den Qognify VMS-Server als „gesalteter SHA-512-Hash“ übermittelt.

- **Kamera - Audio- und Videostreaming**

Die Sicherung der Übertragung mittels Verschlüsselung hängt vom verwendeten Kameramodell ab. Die Streaming-Methode „RTSP over RTP over HTTPS“ muss unterstützt werden. TLS 1.2 wird verwendet, sofern von der Kamera unterstützt.

- **Audio- und Videostreams speichern**

An den Qognify VMS DeviceManager (DM) gesendete eingehende Streams werden an die lokale Qognify VMS MultimediaDatabase (MDB) weitergeleitet. Die Übertragung vom DM an die MDB erfolgt auf demselben Server (lokaler TCP STACK). Daher ist keine Verschlüsselung erforderlich. Qognify VMS speichert die Streams in einem oder in mehreren Dateisystemen gleichzeitig. Die Dateisysteme können vom Administrator konfiguriert werden. Der Datenspeicher in der Qognify MDB wird in einem proprietären Format verschlüsselt. Es wird vorausgesetzt, dass der physische und logische Zugriff auf den Speicherserver durch administrative Maßnahmen eingeschränkt wird. Der Export von der MDB wird verschlüsselt, wodurch sichergestellt wird, dass ein Zugriff auf den Stream ohne Passwort nicht möglich ist, da jegliche Änderung der exportierten Daten dazu führt, dass das Passwort nicht mehr funktioniert. Außerdem wird die Gültigkeit der exportierten Daten überprüft. Durch den Schutz der Rohdaten wird eine Manipulation verhindert und die Echtheit der Daten sichergestellt.

- **Audio- und Videostreaming auf die Qognify VMS-Clients**

Streams werden nur bei Bedarf an die Qognify VMS-Clients gesendet (z. B. wenn ein Kamerabild im Überwachungsmodus oder Archivmodus angezeigt wird).

Die Streams werden über TCP oder UDP an die Qognify VMS-Clients gesendet und unter Verwendung unseres eigenen proprietären Übertragungsprotokolls übertragen.

Umgang mit Zeitzonen

Zeitzoneinformationen (Datum und Uhrzeit) werden als Zeitzoneinformationen im Format UTC-Coordinated¹ gespeichert. Wenn ein Qognify VMS-Client ein Datum und eine Uhrzeit anzeigt, verwendet er in der Regel die lokale Zeitzone des Rechners, die sich von der Zeitzone des Servers unterscheiden kann, der die Informationen wie Aufnahme datum und -zeit speichert.

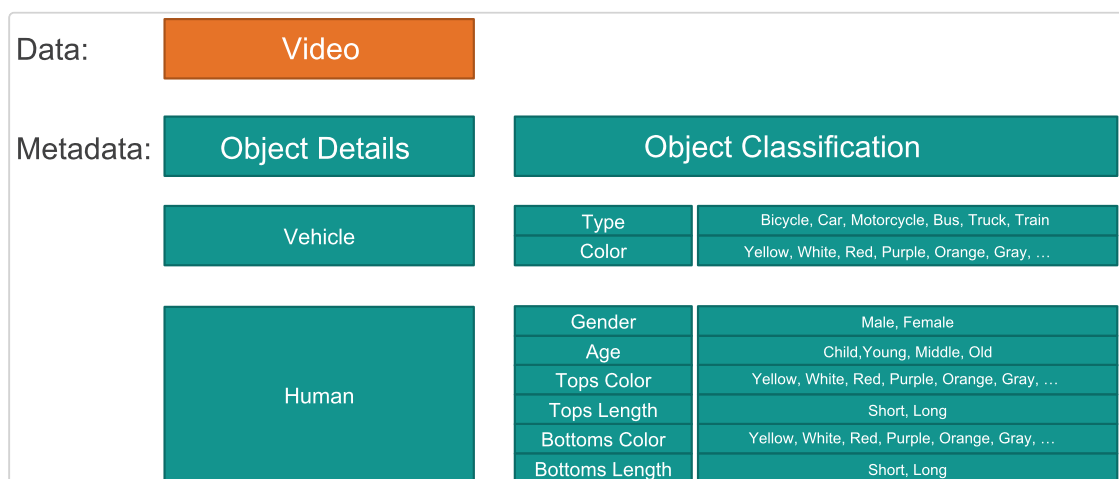
Beim Laden und Betrachten von Bildern oder Dateien im Archivmodus wird der Zeitstempel der geladenen Informationen immer in der lokalen Zeitzone des Clients angezeigt.

Beispiel

Der Server befindet sich in Europa und speichert ein Video um 22:00 Uhr Ortszeit, die auch im Zeitstempel innerhalb des Videos angezeigt wird. Wenn ein Kunde in Kalifornien (USA) dieses Video im Archivmodus anschaut, zeigt der Client 2 pm an, d. h. die Ortszeit des Kunden. Daher zeigt die Zeitleiste im Archivmodus 14 Uhr an und die Uhr im Video zeigt 22:00 Uhr an.

Der QogniFinder

Der QogniFinder erweitert die Suchfunktion für Objekte in Bildern durch eine erhöhte Verwendung von Metadaten. Metadaten bieten Informationen über andere Daten wie „rot“ oder „blau“ (Adjektive) ein Hemd (Nomen) beschreiben. Das folgende Diagramm bezeichnet diese Metadatenkonstruktion für Objekte in einem Video-Stream.



¹Universal Time

Qognify VMS verwaltet die Metadaten, die an Objekten in Bildern angewandt werden. Die Software entdeckt die Objekte in einem Bild und wendet die vorhandenen Metadaten an den gefundenen Objekten an. Dadurch wird die Suche nach Objekten in Bildern entsprechend ihrer Metadaten erheblich verbessert.

Installation

Installationshinweise

Bei der Migration von SeeTec 5 auf Qognify VMS 7.4 muss der CoreService Main festgelegt werden. Dieser kann später nicht mehr geändert werden (z. B. Core Service Sub), da dies zu Datenverlust führen würde.

- Qognify VMS darf nicht auf ein komprimiertes Laufwerk installiert werden, da dies zu Problemen mit der Datenbank führen kann. Ein Laufwerk, auf dem Qognify VMS bereits installiert ist, darf im Nachhinein nicht komprimiert werden.
- Während der Installation wird Microsoft .NET Framework 4.6.2 installiert, was bei einer Erstinstallation eventuell einen Neustart erfordert.

Ab Qognify VMS 7.4 wird DirectX 9 nicht mehr installiert, da DirectX bei aktuellen Windows-Betriebssystemen bereits standardmäßig installiert ist.

- Der Qognify AutoUpdater wird in einem separaten Ordner installiert.

Informationen zu Rollbacks

Möglicherweise ist es erforderlich, das System auf eine zuvor installierte Version von Qognify VMS zurückzusetzen (Rollback), um einen möglichst reibungslosen Systembetrieb sicherzustellen. Die Deinstallation der vorherigen Version und anschließende Installation der neuen Version erfolgen „im Verborgenen“. Bei einem Installationsfehler werden alle Schritte wieder rückgängig gemacht.

Um die Rollback-Funktion zu verwenden, muss eine neue Version von Qognify VMS installiert werden, OHNE die vorherige Version zu entfernen. Rollback ist verfügbar für Qognify VMS Version 16 und neuer.

Virens Scanner

Auf Qognify VMS-Systemen dürfen kein Webguard und keine Funktionen für Internetsicherheit installiert werden.

- Damit die Qognify VMS-Software ordnungsgemäß ausgeführt wird, schließen Sie bestimmte Verzeichnisse, Prozesse und bestimmten Netzwerkverkehr aus, da Virens Scanner möglicherweise eine große Menge an Systemressourcen nutzen.
- Der Scanvorgang kann dazu führen, dass Dateien vorübergehend gesperrt werden. Dies kann zu einer Unterbrechung der Aufzeichnung oder sogar zur Beschädigung der Datenbank führen.
- Führen Sie keine Echtzeit- und Systemscans von Qognify VMS-Verzeichnissen durch, in denen sich Aufzeichnungsdatenbanken befinden (standardmäßig C:\Programme\Qognify sowie alle Unterordner).
- Führen Sie keine Echtzeit- und Systemscans in archivierten Speicherzeichnissen durch.
- Richten Sie die folgenden zusätzlichen Ausschlüsse ein:
 - C:\Programme\Qognify und alle Unterverzeichnisse
 - Pfad zu Zone(n) der MultimediaDatabase
- Ausschluss von Echtzeit-Netzwerkscans auf TCP-Ports.
- Schließen Sie Netzwerkscans von Prozessen aus, die mit „VMS_“ beginnen (z. B. VMS_Client.exe).

Firewalls

Dem Standard entsprechend müssen Multiple Ports auf Server-Computern verfügbar sein, um der Qognify VMS Software die korrekte Funktion in einer Netzwerkumgebung

mit einer Firewall zu ermöglichen.

Setup-Typen

- **Client & Server.** Mit dieser Installation werden auf dem Rechner die Client- und die Server-Module installiert (siehe „[Standardinstallation](#)“ auf Seite 35).
- **Client.** Mit dieser Installation werden nur die Client-Module installiert (siehe „[Client-Installation](#)“ auf Seite 38).
- **Abgesetzter Server.** Mit dieser Installation werden nur der Client und Serverdienste für die Kameras (DM/MDB) auf dem gewählten Rechner installiert (siehe „[Installation eines abgesetzten Servers](#)“ auf Seite 38).
- **Benutzerdefiniert.** Bei einer benutzerdefinierten Installation besteht die Möglichkeit, auf einem Rechner nur einzelne Komponenten zu installieren (siehe „[Angepasste Installation](#)“ auf Seite 41).

Systemvoraussetzungen

Die Übersicht über die Software- und Hardware-Anforderungen findet sich auf unserer Support-Seite: <https://www.qognify.com/support-training/>

Bekannte Einschränkungen

- Die Leistungsanforderungen der Qognify-Serverdienste sind vor allem vom transferierten Videovolumen bzw. der Speicher-Hardware abhängig.
- **Die Installation der Server-Software darf nur auf Rechnern mit NTFS-Dateisystem durchgeführt werden.**
- Für jede zu visualisierende Kamera sollten zusätzliche 25 MB RAM für den Server verfügbar sein.

- Die Hardware-Anforderungen hängen von der Konfiguration ab. Qognify VMS basiert auf einer erweiterten Software-Architektur, als Antwort auf den technologischen Fortschritt. Qognify empfiehlt ein 64-bit-Betriebssystem für datenintensive Clients, um die Verwendung des Qognify 64-bit Client zu ermöglichen.

Wenden Sie sich im Zweifelsfall an den Qognify Support (siehe „Support“ auf Seite 13).

Voraussetzungen für die Onlinehilfe

- Aktueller Internetbrowser mit aktiviertem JavaScript
- Für die Hilfe im PDF-Format wird Adobe Reader oder ein vergleichbares Programm empfohlen.

Allgemeine Empfehlungen

Virtuelle Umgebungen

Die neuesten aktualisierten Systemvoraussetzungen und -parameter werden auf <https://www.qognify.com/support-training/hardware-recommendations/> veröffentlicht.

- Qognify rät davon ab, Clients in virtuellen Umgebungen einzusetzen, da die Rendering-Leistung wesentlich geringer ist.
- Qognify empfiehlt dedizierte Netzwerkschnittstellen.
- Für eine Virtualisierung wird u. U. mehr CPU-Leistung benötigt als für physische Umgebungen.
- Qognify empfiehlt ein Direct Attached Storage oder iSCSI.
- Da Virtualisierung zu einer Leistungsverringerung führt, empfiehlt Qognify, die geplante Serverumgebung zu testen.

- Qognify VMS ist kompatibel mit Citrix XEN, VMware vSphere und Microsoft Hyper-V.

Thin Clients

Thin Client-Umgebungen werden nicht unterstützt.

Empfehlungen für die CPU

- Die Videoverarbeitung benötigt viel CPU-Leistung. Qognify empfiehlt, stets die neuesten leistungsstärksten CPU-Modelle zu verwenden.
- Einen Vergleich finden Sie auf https://www.cpubenchmark.net/high_end_cpus.html.
- Es wird empfohlen, einen Single-Socket-Server mit bis zu 10 physischen Kernen zu verwenden.

Windows-Clustering und -Betriebssystem

- Es wird empfohlen, stets die aktuellsten Systemupdates zu installieren.
- Es werden 64-Bit-Versionen empfohlen.

Netzwerklayout

- Abhängig von der Anzahl an Kameras in Ihrem System und der sich daraus ergebenden erforderlichen Netzwerkbandbreite muss die Verwendung mehrerer separater Netzwerke für die Kameras, die Clients und den Speicher in Erwägung gezogen werden, um eine Überlastung des Netzwerks zu vermeiden.
- Da der Qognify-Client keine direkte Verbindung zu den Kameras benötigt, erfordert nur der Qognify-Server Zugriff auf beide Netzwerke.

Kombinieren oder verbinden Sie keine Netzwerkschnittstellen.

Verwendung von Kameras

- Kameras dürfen nur einmal referenziert werden. Die mehrfache Konfiguration einer Kamera pro Installation oder in verschiedenen Installationen führt bei einigen Kameratypen zu Problemen.
- Für weitere Informationen wenden Sie sich an Qognify Project Engineering.

Benchmark-Ergebnisse

Benchmark-Ergebnisse für einen Qognify Qognify VMS-Client mit empfohlenem Hardware-Setup und 4 Anzeigen:

H.264

- 48 Kameras, 320 x 240 bei 512 kbit/s CBR und 25 fps
- 40 Kameras, 640 x 480 bei 1024 kbit/s CBR und 25 fps
- 30 Kameras, 704 x 480/704 x 576 bei 2048 kbit/s CBR und 25 fps
- 18 Kameras, 720p bei 4096 kbit/s CBR und 25 fps
- 12 Kameras, 1080p bei 4096 kbit/s CBR und 25 fps
- 12 Kameras, 3 Megapixel bei 4096 kbit/s CBR und 25 fps

H.265

- 48 Kameras, 320 x 240 bei 200 kbit/s ~VBR und 25 fps
- 32 Kameras, 640 x 480 bei 400 kbit/s ~VBR und 25 fps
- 16 Kameras, 720p bei 600 kbit/s ~VBR und 25 fps
- 8 Kameras, 1080p bei 2000 kbit/s ~VBR und 25 fps

Standardinstallation

Das System wird in der Standardinstallation als Einplatzinstallation mit Client und Server installiert.

Vorbereitung

1. Kopieren Sie das ZIP-Archiv mit den Installationsdateien auf den Rechner, auf dem die Software installiert werden soll, und entpacken Sie das Archiv.
2. Starten Sie die Installation durch Doppelklick auf **setup.exe**.
3. Wählen Sie die Sprache für die Installation aus. Die Sprache der Benutzeroberfläche können Sie nach der Installation konfigurieren (siehe „[Sprache ändern](#)“ auf Seite 85).
4. Starten Sie die Installation mit **OK** und wählen Sie **Weiter**.
5. Lesen Sie den Softwarelizenzvertrag durch und wählen Sie **Weiter**.

Die Software kann nur installiert werden, wenn Sie dem Softwarelizenzvertrag (EULA) zustimmen.

6. Wählen Sie den Zielordner und dann **Weiter**.

Standardinstallation

1. Wählen Sie für die Standardinstallation den Setup-Typ „Client & Server“ und dann **Weiter**.

2. Wählen Sie **Gefundene IP-Adressen/Hostnamen** als Netzwerkadresse für die Serverkommunikation.

Server services
Specify connection settings for the server services

Qognify VMS

Management service

Host: localhost Port: 60000

IP address/host name for server communication

Host: 10.0.80.51 IP addresses/host names found: 10.0.80.51

InstallShield < Back Next > Cancel

Abb. 3: Standardinstallation - 1

Es wird empfohlen, die Portnummer des Verwaltungsdienstes unverändert bei „60000“ zu lassen. Wenn die Portnummer geändert werden muss, wenden Sie sich an den Qognify-Support, bevor Sie irgendwelche Änderungen vornehmen.

Das Installationsprogramm zeigt Ihnen alle vorhandenen Netzwerkadressen und Hostnamen des PCs bzw. Servers an. Es dürfen weder die IP 127.0.0.1 noch der Hostname „localhost“ für die Kommunikation mit dem Server verwendet werden.

3. Wenn der UpdateServer auf einem anderen Host als die CoreService Main installiert wird, geben Sie die IP-Adresse für den Host des **UpdateService** an (siehe [„UpdateAgent konfigurieren und aktualisieren“ auf Seite 47](#)). Der UpdateAgent kann sich an der angegebenen IP-Adresse mit dem UpdateService verbinden.

Der UpdateService verwendet für die Kommunikation mit den UpdateAgents standardmäßig Port 63000 und 63001.

4. Wählen Sie **Weiter**.

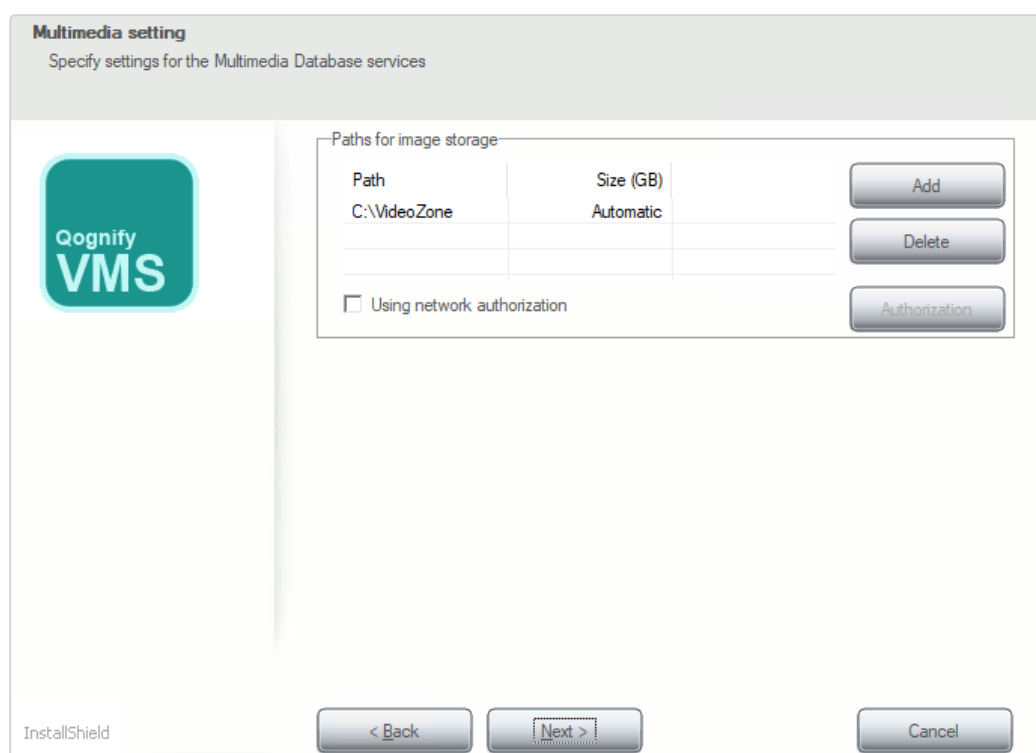


Abb. 4: Standardinstallation - 2

5. Passen Sie den vorhandenen Pfad zur Bildspeicherung an oder löschen bzw. fügen Sie weitere Verzeichnispfade hinzu. Falls das Verzeichnis auf einem Netzlaufwerk angelegt ist, geben Sie den vollständigen UNC-Pfad ein.

Beispiel, „\\IP-Adresse\Freigabename\Pfad...“

6. Falls das Netzlaufwerk durch Benutzernamen und Passwort geschützt ist, aktivieren Sie **Verwende Netzwerkautorisierung** und klicken Sie auf **Autorisierung**.
7. Geben Sie den Benutzernamen und das Passwort für den Zugriff auf das Netzlaufwerk an und bestätigen Sie mit **OK**. Stellen Sie sicher, dass der angegebene Benutzer lokal verfügbar ist und die Domäne im Feld „Benutzername“ aufgeführt wird (z. B. „Domain\\Benutzername“).
8. Wählen Sie **Weiter**.
9. Wählen Sie **Installieren**. Qognify VMS wird nun auf Ihrem Rechner installiert. Wenn der UpdateService installiert wurde, verbindet sich der Dienst jetzt mit dem UpdateServer und lädt die neuesten Patch-Dateien herunter, sofern vorhanden. Zum Starten des Programms und der Module siehe [„Anmeldung“ auf Seite 57](#).
10. Konfigurieren Sie das System mit dem Qognify VMS-Client (siehe [„Konfigurationsmodus“ auf Seite 207](#)).

Client-Installation

In der Client-Installation wird nur der Client auf dem Rechner installiert.

Vorbereitung

1. Kopieren Sie das ZIP-Archiv mit den Installationsdateien auf den Rechner, auf dem die Software installiert werden soll, und entpacken Sie das Archiv.
2. Starten Sie die Installation durch Doppelklick auf **setup.exe**.
3. Wählen Sie die Sprache für die Installation aus. Die Sprache der Benutzeroberfläche können Sie nach der Installation konfigurieren (siehe „[Sprache ändern](#)“ auf Seite 85).
4. Starten Sie die Installation mit **OK** und wählen Sie **Weiter**.
5. Lesen Sie den Softwarelizenzvertrag durch und wählen Sie **Weiter**.

Die Software kann nur installiert werden, wenn Sie dem Softwarelizenzvertrag (EULA) zustimmen.

6. Wählen Sie den Zielordner und dann **Weiter**.

Client-Installation

1. Wählen Sie den Setup-Typ „Client“ (siehe „[Installation](#)“ auf Seite 29).
2. Klicken Sie auf **Installieren**.

Der Client wird auf dem Rechner installiert. Wenn der UpdateService installiert wurde, verbindet er sich jetzt mit dem UpdateServer und lädt die neuesten Patch-Dateien herunter, sofern vorhanden. Zum Starten des Programms und der Module siehe „[Anmeldung](#)“ auf Seite 57.

Installation eines abgesetzten Servers

In der „Abgesetzter Server“-Installation werden zusammen mit dem Client nur die Datenbankmodule für die Bilddatenbank auf einem anderen Rechner installiert als der bereits installierte Client und Core-Server. Der abgesetzte Server dient dazu, die Auslastung des Core-Servers zu verringern, indem die Bilddatenbank ganz oder teilweise auf den abgesetzten Server ausgelagert wird.

Um den Server konfigurieren zu können, benötigen Sie einen installierten und konfigurierten Client und Core-Server (siehe „[Standardinstallation](#)“ auf Seite 35).

Die benötigten Ports 60000 - 60008 für die Kommunikation zwischen dem abgesetzten Server und dem Hauptserver müssen geöffnet sein.

Vorbereitung

1. Kopieren Sie das ZIP-Archiv mit den Installationsdateien auf den Rechner, auf dem die Software installiert werden soll, und entpacken Sie das Archiv.
2. Starten Sie die Installation durch Doppelklick auf **setup.exe**.
3. Wählen Sie die Sprache für die Installation aus. Die Sprache der Benutzeroberfläche können Sie nach der Installation konfigurieren (siehe „[Sprache ändern](#)“ auf Seite 85).
4. Starten Sie die Installation mit **OK** und wählen Sie **Weiter**.
5. Lesen Sie den Softwarelizenzvertrag durch und wählen Sie **Weiter**.

Die Software kann nur installiert werden, wenn Sie dem Softwarelizenzvertrag (EULA) zustimmen.

6. Wählen Sie den Zielordner und dann **Weiter**.

Installation

1. Wählen Sie den Setup-Typ „Abgesetzter Server“ (siehe „[Installation](#)“ auf Seite 29).

The screenshot shows the 'Server services' configuration window. The title bar reads 'Server services' and the subtitle is 'Specify connection settings for the server services'. On the left side, there is a logo for 'Qognify VMS'. The main content area is divided into two sections. The first section, 'Management service', has a 'Host' field containing 'localhost' and a 'Port' field containing '60000'. The second section, 'IP address/host name for server communication', has a 'Host' field containing '10.0.80.51' and an 'IP addresses/host names found' dropdown menu containing '10.0.80.51'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel!'. The 'InstallShield' logo is visible in the bottom left corner.

Abb. 5: Installation eines abgesetzten Servers - Servereinstellungen

1. Geben Sie im Bereich „Verwaltungsdienst“ als **Host** die IP-Adresse des Haupt-servers (CoreService Main, CSM) an.

Es wird empfohlen, die Portnummer des Verwaltungsdienstes unverändert bei „60000“ zu lassen. Wenn die Portnummer geändert werden muss, wenden Sie sich an den Qognify-„Support“ auf Seite 13, bevor Sie irgendwelche Änderungen vornehmen.

2. Wählen Sie **IP-Adresse/Hostname** für **Serverkommunikation** als Netzwerkadresse. Das Installationsprogramm zeigt Ihnen alle vorhandenen Netzwerkadressen und Hostnamen des PCs bzw. Servers an.

Es dürfen weder die IP 127.0.0.1 noch der Hostname „localhost“ für die Kommunikation mit dem Server verwendet werden.

3. Wenn NAT (Network Address Translation) verwendet wird, aktivieren Sie „Aktivieren, wenn NAT (Network Address Translation) benutzen soll“ und geben Sie die IP-Adresse des NAT-Routers ein.
4. Geben Sie die IP-Adresse für den Host des **UpdateService** an (siehe „[UpdateAgent konfigurieren und aktualisieren](#)“ auf Seite 47).

Der UpdateService verwendet für die Kommunikation mit den UpdateAgents standardmäßig Port 63000 und 63001.

5. Wählen Sie **Weiter**.

Multimedia setting
Specify settings for the Multimedia Database services

Qognify VMS

Path	Size (GB)
C:\VideoZone	Automatic

Using network authorization

< Back Next > Cancel

Abb. 6: Installation eines abgesetzten Servers - Multimedia-Einstellungen

7. Passen Sie den vorhandenen **Pfad zur Bildspeicherung** an oder löschen bzw. fügen Sie weitere Verzeichnispfade hinzu. Falls das Verzeichnis auf einem Netzlaufwerk angelegt ist, geben Sie den vollständigen UNC-Pfad ein.

Beispiel „\\Servername\Freigabename\Pfad ...“ bzw. „\IP-Adresse\Freigabename\Pfad ...“

8. Falls das Netzlaufwerk durch Benutzernamen und Passwort geschützt ist, aktivieren Sie **Verwende Netzwerkautorisierung** und klicken Sie auf **Autorisierung**.
9. Geben Sie den Benutzernamen und das Passwort für den Zugriff auf das Netzlaufwerk an und bestätigen Sie mit **OK**. Stellen Sie sicher, dass der angegebene Benutzer lokal verfügbar ist und die Domäne im Feld „Benutzername“ aufgeführt wird (z. B. „Domain\Benutzername“).
10. Wählen Sie **Weiter**.
11. Wählen Sie **Installieren**. Der Server wird nun auf Ihrem Rechner installiert. Wenn der UpdateService installiert wurde, verbindet sich der Dienst jetzt mit dem UpdateServer und lädt die neuesten Patch-Dateien herunter, sofern vorhanden.
12. Konfigurieren Sie das System mit dem Qognify-Client (siehe „[Konfigurationsmodus](#)“ auf Seite 207).

Angepasste Installation

In einer benutzerdefinierten Installation können ausgewählte Module installiert werden. Darüber hinaus ist es möglich, einen weiteren Core-Server im Sub-Core-Modus zu installieren, der als redundanter Server dient und damit die Ausfallsicherheit des Core-Servers erhöht.

Vorbereitung

1. Kopieren Sie das ZIP-Archiv mit den Installationsdateien auf den Rechner, auf dem die Software installiert werden soll, und entpacken Sie das Archiv.
2. Starten Sie die Installation durch Doppelklick auf **setup.exe**.
3. Wählen Sie die Sprache für die Installation aus. Die Sprache der Benutzeroberfläche können Sie nach der Installation konfigurieren (siehe „[Sprache ändern](#)“ auf Seite 85).
4. Starten Sie die Installation mit **OK** und wählen Sie **Weiter**.

5. Lesen Sie den Softwarelizenzvertrag durch und wählen Sie **Weiter**.

Die Software kann nur installiert werden, wenn Sie dem Softwarelizenzvertrag (EULA) zustimmen.

6. Wählen Sie den Zielordner und dann **Weiter**.

Angepasste Installation

1. Wählen Sie den Setup-Typ „Benutzerdefiniert“ (siehe „[Installation](#)“ auf Seite 29).
2. Wählen Sie die gewünschten Dienste und Features aus. Nicht benötigte Dienste und Features können Sie durch Deaktivieren abwählen.

Wird ein zuvor installierter Dienst deaktiviert, wird er entfernt. Die Installation des UpdateService auf dem Server und des UpdateAgent auf dem Client wird unter „[UpdateAgent konfigurieren und aktualisieren](#)“ auf Seite 47 beschrieben.

3. Wählen Sie **Weiter**.
4. Wählen Sie **Installieren**.

Die Dienste und Features werden auf Ihrem Rechner installiert.

Komponenten für die angepasste Installation

Folgende Komponenten sind für eine benutzerdefinierte Installation verfügbar.

Client-Komponenten

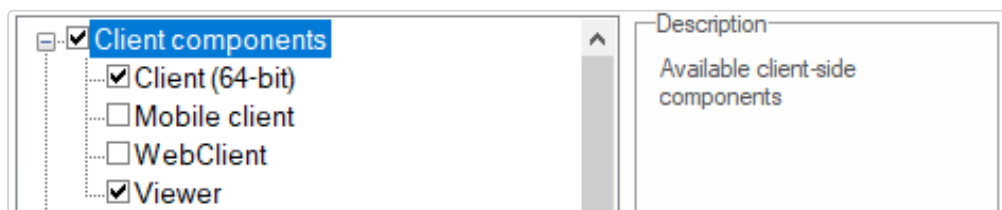


Abb. 7: Angepasste Installation - Client-Komponenten

- **Client (64 Bit):** der Client nur für 64-Bit-Betriebssysteme
- **Mobile Client:** die serverseitigen Mobile Client-Komponenten (Transcoding-Modul und Gateway Service) zur Verbindung mit mobilen Applikationen auf iOS- und Android-Plattformen (siehe „[Der Qognify VMS Mobile Client](#)“ auf Seite 551)

- **Web Client:** die serverseitigen Web Client-Komponenten (Transcoding-Modul, Gateway Service und Microsoft IIS-Webserver mit Website) zur Verbindung mit Webbrowsern (siehe „[Qognify VMS Web Client](#)“ auf Seite 545)
- **Viewer:** der OfflineViewer zur Anzeige exportierter Bilder (siehe „[Anywhere Viewer](#)“ auf Seite 539)

Server-Komponenten

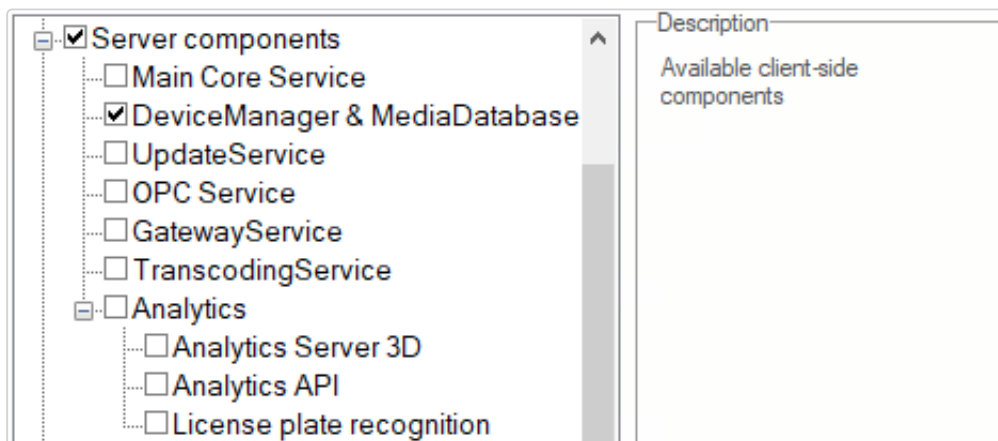


Abb. 8: Angepasste Installation - Server-Komponenten

- **Core Service Main:** Die Main Core-Dienste und Verwaltungsdatenbank
- **Core Service Sub:** Die Sub Core-Dienste und die Verwaltungsdatenbank für das redundante System-Management

Sub Core und Main Core können auf der gleichen Maschine nicht gleichzeitig installiert werden.

- **Device Manager & MediaDatabase:** die Dienste für den Device Manager und die MediaDatabase. Diese Dienste sind hauptsächlich für das Bildhandling zuständig.
- **UpdateService:** Der UpdateService verwaltet die automatischen Update- und Patchprozesse auf dem Qognify-System (siehe „[UpdateService Konfigurationstool](#)“ auf Seite 492).

- **OPC-Dienst:** Die „Open Platform Communications“-Schnittstelle ermöglicht einen standardisierten Datenaustausch zwischen Applikationen und Geräten in Echtzeit (siehe Technisches Handbuch zum OPC-Dienst für Qognify VMS R3 oder höher).
- **GatewayService:** Der GatewayService wird zur Verwendung des Mobile und Web Client benötigt (siehe [„Mobile Client-Dienste auf dem Qognify-Server installieren“ auf Seite 552](#)).
- **TranscodingService:** Der TranscodingService wird zur Verwendung des Mobile und Web Client benötigt (siehe [„Transcoding-Modul konfigurieren“ auf Seite 453](#)).
- **Analytics:** Die serverseitigen Komponenten für Qognify Video Analytics-Features
 - **Analytics Server 3D:** die serverseitigen Analytics Server 3D-Komponenten für auf dem Rechner verwendete Drittanbieter-Videoanalyse-Software (siehe [„Qognify Analytics Server 3D-Modul konfigurieren“ auf Seite 450](#))
 - **Analytics (alt):** die auf dem Rechner installierten serverseitigen Analysekomponenten (siehe [„Qognify Analytics“ auf Seite 327](#))
 - **Analytics API:** die serverseitigen Komponenten der Analytics API für auf dem Rechner installierte Drittanbieter-Videoanalyse-Software
 - **Kennzeichenerkennung:** die auf dem Rechner installierte serverseitige Kennzeichenerkennung (siehe [„Kennzeichenerkennung“ auf Seite 318](#))

Extras

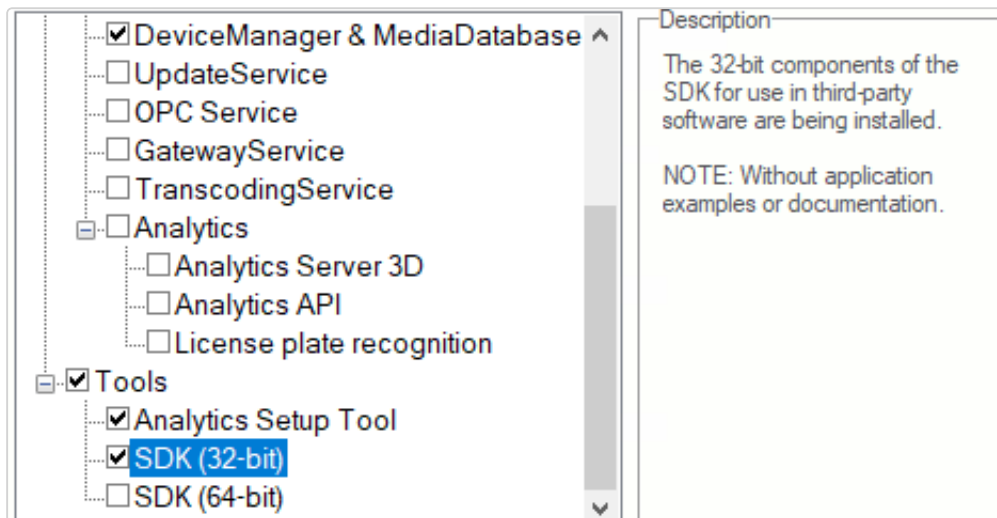


Abb. 9: Angepasste Installation - Extras

- **Analytics Setup Tool:** das Tool zur Konfiguration und Kalibrierung von Szenarien für den Qognify Analytics Server 3D (siehe „[Qognify Analytics Server-Modul konfigurieren](#)“ auf Seite 338)
- **SDK (32 Bit):** Die 32-Bit-Komponenten des SDK zur Verwendung in Software von Drittanbietern
- **SDK (64 Bit):** die 64-Bit-Komponenten des SDK zur Verwendung in Dritthersteller-Software

System mit dem AutoUpdater aktualisieren

Mit dem Qognify VMS AutoUpdater können Sie alle Systemkomponenten auf dem aktuellen Stand halten, ob es sich um eine „All-in-one“-Einzelninstallation auf einem Rechner oder eine verteilte Installation mit mehreren Servern und Clients handelt. Das Qognify VMS AutoUpdater-System besteht aus zwei Komponenten, dem UpdateService and dem/den UpdateAgent(s).

- Der **UpdateService**: Der UpdateService prüft unmittelbar nach der Installation und anschließend in regelmäßigen Abständen nach neuen Patches oder Updates und verteilt diese an die verbundenen UpdateAgents. Bei einer Standardinstallation wird der UpdateService auf dem Hauptserver des Kerndienstes installiert. Optional kann der UpdateService auf einem anderen Server installiert werden (siehe „[Angepasste Installation](#)“ auf Seite 41).

Für den UpdateService ist eine reguläre Lizenz mit einem gültigen Service Maintenance Agreement (SMA) oder eine noch nicht abgelaufene Demolizenz erforderlich.

- Der/Die **UpdateAgent(s)**: Mit jeder Qognify VMS-Komponente (Dienste, Clients, Tools usw.) wird automatisch ein UpdateAgent installiert. Abhängig von der Konfiguration des UpdateService empfängt ein UpdateAgent Updates und Patches vom UpdateServer entweder automatisch oder per manuellem Trigger. Dies ermöglicht die automatische oder benutzerdefinierte Installation von Updates und Patches für mehrere Clients.

Qognify VMS-UpdateService installieren

Der UpdateService wird standardmäßig auf dem Core Service Main installiert. Wenn Sie den UpdateService auf einer anderen Hardware als dem Core-Server installieren müssen, folgen Sie den unten stehenden Schritten.

- Der UpdateService verwendet für die Kommunikation mit den UpdateAgents standardmäßig Port 63000 und 63001.
- Überprüfen Sie, dass die Ports 63000 und 63001 nicht von einer Firewall blockiert werden.
- Nur ein Server sollte als der UpdateService-Server fungieren. Die Verwendung mehrerer UpdateService-Server wird nicht empfohlen.
- Um den UpdateService auf einem anderen Server als dem CoreService Main zu installieren und auszuführen, sollte er vor der Installation vom Hauptserver entfernt werden (siehe „[Ändern, Reparieren und Entfernen](#)“ auf Seite 49).

Aktualisieren Sie alle UpdateAgents mit dem aktuellen UpdateService (z. B. Qognify VMS7.4), bevor Sie Updates mit dem UpdateService installieren (z. B. von Qognify VMS R3 auf Qognify VMS7.4).

1. Wählen Sie den Server aus, auf dem der Qognify VMS UpdateService läuft.
2. Geben Sie die IP-Adresse des Servers für den UpdateService an. Alle UpdateAgents müssen sich über die angegebene IP-Adresse mit dem UpdateService verbinden.
3. Starten Sie eine benutzerdefinierte Installation und wählen Sie „UpdateService“ in den Serverkomponenten (siehe [„Angepasste Installation“ auf Seite 41](#)).

Qognify VMS UpdateService konfigurieren

Der UpdateService und das Update-Verhalten der UpdateAgents können mit dem Qognify VMS UpdateServer Konfigurationstool verwaltet werden. Das UpdateServer Konfigurationstool wird automatisch zusammen mit dem UpdateService auf dem Server installiert.

Die Konfigurationseinstellungen werden unter [„UpdateService Konfigurationstool“ auf Seite 492](#) beschrieben.

UpdateAgent konfigurieren und aktualisieren

Der UpdateAgent wird automatisch auf jedem Rechner installiert, auf dem eine Qognify VMS-Komponente (z. B. Basisdienst, Client, Device Manager, VA-Service usw.) installiert ist. Während des Installationsvorgangs muss die IP-Adresse des UpdateService angegeben werden (siehe [„Standardinstallation“ auf Seite 35](#)). Nach der Installation wird der UpdateAgent vom Installationsprogramm standardmäßig aktiviert und konfiguriert.

Wenn sich die IP-Adresse des UpdateServer geändert hat, muss der UpdateAgent in der Konfigurationsdatei des UpdateAgent manuell konfiguriert werden.

IP-Einstellungen des UpdateAgent manuell ändern

1. Stoppen Sie den UpdateAgent mit dem Qognify ServiceManager (siehe [„Dienste starten und stoppen“ auf Seite 512](#)).
2. Öffnen Sie die Konfigurationsdatei „/conf/updateclient.conf.xml“ im Installationsverzeichnis mit einem Texteditor.
3. Legen Sie die neue IP-Adresse des UpdateService fest. Die IP-Adresse entspricht der Netzwerkadresse des Clients, auf dem der UpdateService installiert ist.
4. Speichern Sie die Einstellungen.
5. Starten Sie den UpdateAgent mit dem Qognify ServiceManager (siehe [„Dienste starten und stoppen“ auf Seite 512](#)).

Beispiel

```
updateclient.conf.xml
<?xml version="1.0"?>
<ServerInformation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd-d="http://www.w3.org/2001/XMLSchema">
<ip>10.0.8.131</ip><port>63000</port>
</ServerInformation>
```

Manuelle Aktualisierung

Updates und Patches im Qognify VMS-System können vom AutoUpdater automatisch installiert werden. Wenn der AutoUpdater ordnungsgemäß konfiguriert ist, muss die ältere Version von Qognify VMS vor der Aktualisierung auf eine neuere Version nicht deinstalliert werden.

Ältere Versionen als SeeTec 5.4 müssen vor dem Upgrade jedoch entfernt werden (siehe [„Von SeeTec 5.4.x auf Qognify VMS aktualisieren/migrieren“ auf Seite 50](#)).

Vergewissern Sie sich vor der manuellen Aktualisierung des Systems, dass Ihr System die Hardware- und Softwareanforderungen erfüllt (siehe [„Systemvoraussetzungen“ auf Seite 31](#)).

1. Sichern Sie das CONF-Verzeichnis (C:\Programme\Qognify\Conf) manuell.
2. Sichern Sie die Verwaltungsdatenbank MaxDB (C:\Programme\Qognify\SAPDB\backup) manuell.
3. Deinstallieren Sie die aktuelle Qognify-Version über die Windows®-Systemsteuerung. Die Verzeichnisstruktur des Installationsverzeichnisses und die Datenbank bleiben erhalten.
4. Installieren Sie die neue Qognify VMS7.4-Software.
5. Importieren Sie die neue Lizenzdatei (siehe [Lizenzdatei importieren](#)).

Die neue Lizenzdatei kann auch vor der Aktualisierung importiert werden.

Ändern, Reparieren und Entfernen

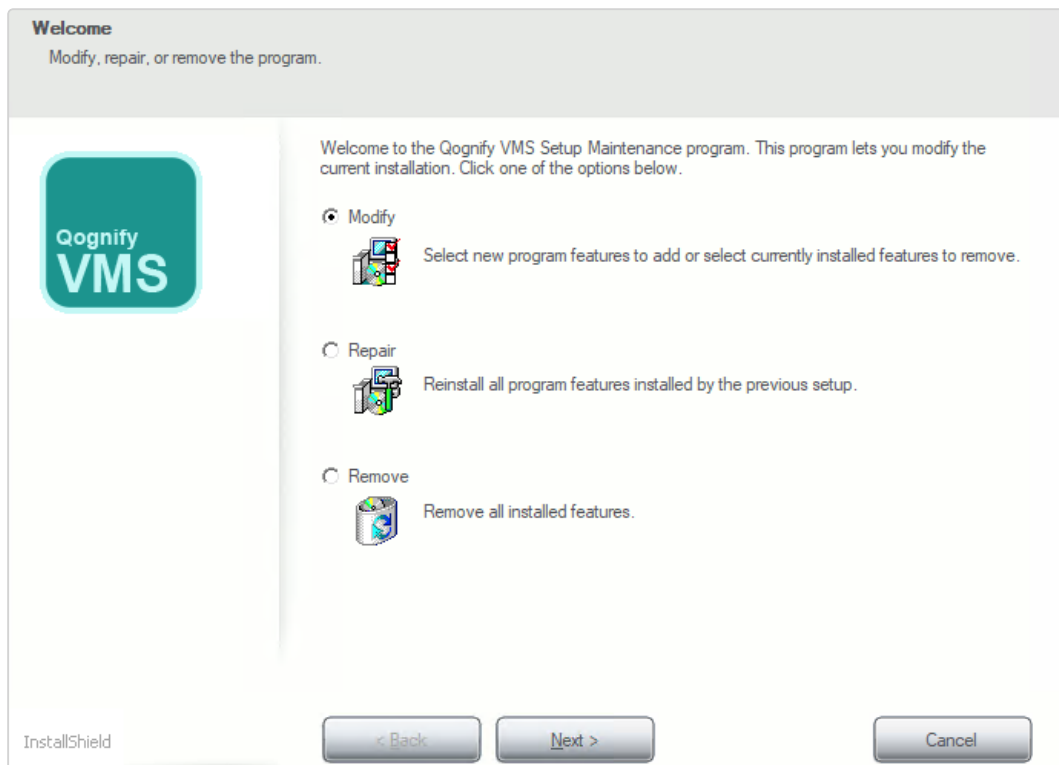


Abb. 10: Ändern, Reparieren und Entfernen

1. Starten Sie die Systemsteuerung und wechseln Sie in die Kategorie **Programme**.
2. Klicken Sie auf **Programme und Funktionen**.
3. Wählen Sie **Qognify VMS**.
4. Wählen Sie **Ändern** oder **Reparieren**.

5. Wählen Sie eine der folgenden Optionen:

- Um zusätzliche Qognify VMS-Komponenten zu installieren oder deinstallieren, wählen Sie „Ändern“ und dann **Weiter**. Sie werden dann zur „Benutzerdefinierten Installation“ geleitet, bei der Sie die gewünschten Module und Dienste installieren bzw. deinstallieren können (siehe [„Angepasste Installation“ auf Seite 41](#)).
- Um das Programm zu reparieren, wählen Sie „Reparieren“ und dann **Weiter**. Qognify VMS wird versuchen, eventuell beschädigte Programmbestandteile selbstständig zu reparieren und zu installieren.
- Um das Programm von der Festplatte zu entfernen, wählen Sie „Entfernen“ und **Weiter**. Alle Programmbestandteile bis auf die Konfigurationseinstellungen werden von der Festplatte gelöscht und aus den Verzeichnisdiensten entfernt.

Für das vollständige Entfernen nach der Deinstallation löschen Sie den verbliebenen Qognify-Ordner in „C:\Programme“ von Hand.

Von SeeTec 5.4.x auf Qognify VMS aktualisieren/migrieren

Im folgenden Abschnitt wird die Vorbereitung und Implementierung einer Migration von SeeTec 5.4.x auf Qognify VMS7.4 beschrieben. Es werden die erforderlichen Schritte für die Überprüfung und den grundlegenden Vorgang erläutert.

Beachten Sie, dass die Vorbereitung, abhängig von den technischen Spezifikationen des bestehenden Systems, lange vor der eigentlichen Migration beginnen sollte, da unter Umständen die Lieferzeiten für Hardwarekomponenten berücksichtigt werden müssen.

Vor der Migration komplexer Installationen (z. B. Logistik, CIT, BVI usw.) kann das Qognify-Supportteam kontaktiert werden (siehe [„Support“ auf Seite 13](#)).

Zu beachtende Dokumente

- Qognify VMS 7.4-Readme-Datei
- Systemvoraussetzungen für Qognify VMS 7.4 (siehe „[Systemvoraussetzungen](#)“ auf Seite 31)
- [Unterstützte Third Party Interfaces](#)

Empfohlene Schritte vor der Migration

Eine Migration auf Qognify VMS ist erst ab Qognify 5.4.0 oder höher möglich. Ältere Versionen müssen vor der Migration auf Qognify 5.4.x aktualisiert werden. Die Migration erfordert unter Umständen den Austausch von Hardwarekomponenten.

1. Sichern Sie die vorhandene Verwaltungsdatenbank MaxDB sowie das Konfigurationsverzeichnis (siehe „[Manuelle Aktualisierung](#)“ auf Seite 48).
2. Überprüfen Sie das bestehende System lange vor dem eigentlichen Migrationsdatum, um sicherzugehen, dass Hardware und/oder Betriebssystem die Anforderungen erfüllen (siehe „[Systemvoraussetzungen](#)“ auf Seite 31). Für Qognify VMS 7.4 ist ein 64-Bit-Betriebssystem erforderlich.
3. Vergewissern Sie sich, dass alle Geräte der Konfiguration im Dokument zu den unterstützten Third Party Interfaces (PDF) aufgeführt sind, und überprüfen Sie die unterstützten Funktionen.
4. Stellen Sie sicher, dass Sie über eine gültige Lizenz für Qognify VMS 7.4 verfügen.
5. Erfassen Sie die Spezifikationen der vorhandenen Server- und Client-Hardware und vergleichen Sie sie mit den im Abschnitt „[Systemvoraussetzungen](#)“ auf Seite 31 beschriebenen Anforderungen.

Mindestvoraussetzungen für Grafikkarten

Einige Grafikkarten, die in Qognify 5.4.x verwendet werden, sind nicht für die Verwendung mit Qognify VMS geeignet, da sie DirectX nicht oder nur teilweise unterstützen (z. B. Grafikkarten von Matrox, Nvidia Quadro NVS 290 oder 420).

- Dedizierte Grafikkarte ohne Shared Memory, 16 Mio. Farben, unterstützt DirectX 9.0 oder höher
- Speichergröße: 2 GB
- Speicherbandbreite mit 100 GB/s
- Mindest-Bildschirmauflösung:
 - 1280 x 768 (bei Textgröße 100 %)
 - 1600 x 960 (bei Textgröße 125 %)
 - 1920 x 1152 (bei Textgröße 150 %)

Nur Microsoft Windows Server 2012

1. Überprüfen Sie, ob das Windows-Feature „Desktop Experience“ installiert ist (bei Microsoft Windows Server 2008 erfolgt dies automatisch).
2. Wenn nicht, installieren Sie das Feature wie folgt: Server-Manager => Verwalten => Rollen und Features hinzufügen => Features => Benutzeroberflächen und Infrastruktur (installiert) => Desktop Experience => Features hinzufügen => Weiter => Installieren.

Migrationsvorgang

Hardware und Betriebssystem erfüllen die Anforderungen bereits

1. Führen Sie ein Backup der MaxDB-Datenbank und des Konfigurationsverzeichnisses aus.
 - Wechseln Sie in der Qognify Administration (Startmenü -> Programme -> SeeTec5) zur Verwaltungsdatenbank (MaxDB) und erstellen Sie über **Sichern** ein Backup. Das Backup wird unter „C:\Programme\SeeTec\SAPDB\backup“ gespeichert.
 - Das Konfigurationsverzeichnis lautet: C:\Programme\SeeTec\conf

2. Deinstallieren Sie SeeTec 5.x über die Windows-Systemsteuerung.
 - Die Verzeichnisstruktur bleibt gleich.
 - Die Datenbank bleibt gleich.
3. Installieren Sie Qognify VMS7.4.
4. Installieren und aktivieren Sie eine neue Lizenz (siehe „Info“ auf Seite 126).

Migration auf neue Hardware und/oder neues Betriebssystem

1. Überprüfen Sie, dass die bestehende Qognify VMS-Installation mindestens die Version 5.4.0 hat. Ist dies nicht der Fall, führen Sie ein Update auf Version 5.4.8 durch.
2. Führen Sie ein Backup der MaxDB-Datenbank aus.
 - Wechseln Sie in der Qognify Administration (Startmenü -> Programme -> Qognify5) zur Verwaltungsdatenbank (MaxDB) und erstellen Sie über **Sichern** ein Backup. Das Backup wird unter „C:\Programme\Qognify\SAPDB\backup“ gespeichert.
3. Installieren Sie Qognify VMS7.4.
4. Starten Sie das Qognify Administrationstool (Startmenü > Programme > Qognify) auf dem neu installierten System und stellen Sie das Backup des bestehenden Systems in der Verwaltungsdatenbank (MaxDB) wieder her.

Beachten Sie, dass das Backup lokal verfügbar sein muss und nicht entpackt werden darf.

5. Installieren und aktivieren Sie eine neue Lizenz (siehe „Info“ auf Seite 126).

Nach dem Upgrade

Änderungen

- Alle Benutzer mit Ausnahme des Administrators sind deaktiviert.
- Das Passwort des Administrators wird auf „pass“ zurückgesetzt. (Die Passwörter aller anderen Benutzer müssen während der Aktivierung neu vergeben werden.)
- Die Dienste SeeTec5_ENT, SeeTec5_EVT, SeeTec5_AUTH, SeeTec5_ALARM und SeeTec5_EXT werden in einen einzigen Dienst namens VMS_CORE migriert. Das bedeutet, es gibt nur ein Logfile (core.log) und nur eine Konfigurationsdatei (core.conf.xml).
- Die Namen aller Dienste beginnen nun mit „VMS_“.
- Die Angabe des Speichervolumens bei der Kamerakonfiguration/Bildspeicherung ist nicht mehr möglich. Es kann nur für die Zeitbegrenzung konfiguriert werden. Bei Kameras, für die ein Speichervolumen konfiguriert wurde, wird eine Zeitbegrenzung von 9999 Tagen festgelegt.
- Die Unterteilung zwischen ExpansionPackage und CorePackage besteht nicht mehr.
- Das Installationsprogramm verschiebt alle Applikationskomponenten in ein einziges Verzeichnis: „C:\Programme\Qognify“.
- Die Monitorwand wird durch Display Agent ersetzt.
- Die verschlüsselte Serverkommunikation ist Standard, es ist keine weitere Konfiguration erforderlich.
- Flyout-Fenster sind nicht mehr verfügbar.
- Andockbare Benutzeroberflächenelemente sind nicht mehr verfügbar.
- Alarmunterdrückung ist nicht mehr verfügbar.
- Qognify-Gateway-Services (SGS/SAG) ist nur HTTPS.
- BlackBerry Mobile ist nicht mehr verfügbar.

Prüfungen

1. Überprüfen Sie die Konfiguration der Dienste AvExport und Gateway Service nach der Migration im SeeTec VA Administrationstool, da die Konfiguration von SeeTec 5 nicht migriert wird.
2. Kalibrieren Sie den Qognify Analytics-Kanals neu und richten Sie alle Qognify Analytics-Regeln ein.
3. Überprüfen Sie die serverseitige Bewegungserkennung und konfigurieren Sie sie bei Bedarf neu.
4. Überprüfen Sie die Konfiguration der Videoklassifikationen.

Anmeldung

Nachdem das System installiert wurde, müssen Sie sich am Client anmelden, um die installierten Dienste nutzen zu können.

Um den Start des Clients zu automatisieren, können Kommandozeilenparameter definiert werden, um den Client z. B. mit einer anderen Sprache oder mit vorgegebenen Passwörtern zu starten (siehe „[Kommandozeilenparameter](#)“ auf Seite 533).

DAS PASSWORT DES ADMINISTRATORS AN EINEM SICHEREN ORT AUFBEWAHREN!

Falls Sie das Passwort des Administrators vergessen und der Administratorgruppe keine weiteren Benutzer hinzugefügt wurden, ist kein Zugriff auf die Konfigurationseinstellungen des Systems mehr möglich. Das Administratorpasswort kann nicht wiederhergestellt werden.

1. Starten Sie den **Qognify VMS-Client** im Verzeichnis **Qognify** im Startmenü oder auf dem Desktop.



Abb. 11: Anmeldung

2. Wählen Sie die Methode für die **Authentifikation** aus. Folgende Authentifikationsmethoden stehen zur Verfügung:
 - Basisauthentifizierung mit dem in der Konfiguration in Qognify VMS festgelegten Benutzernamen und Passwort.
 - Windows-Authentifizierung mit den Anmeldedaten des aktuellen Benutzers des Windows-Betriebssystems, d. h. denselben Anmeldedaten, die zur Anmeldung am System erforderlich sind. Der Benutzer verfügt über die Rechte der Gruppen, zu denen er gehört (siehe „[Gruppen](#)“ auf Seite 367).
 - Windows-Authentifizierung mit den Active Directory-(AD-)Anmeldedaten des Benutzers. Der Benutzer verfügt über die Rechte der Gruppen, zu denen er gehört (siehe „[Gruppen](#)“ auf Seite 367).

Diese Funktion kann nur verwendet werden, wenn die Nutzung von Active Directory (AD) Teil der Qognify VMS-Lizenz ist.

3. Falls **Basisauthentifizierung** ausgewählt wird, geben Sie den **Benutzernamen** und das **Passwort** ein.

Vergewissern Sie sich, dass der Benutzername und das Passwort korrekt eingegeben werden, da das System zwischen Groß- und Kleinschreibung unterscheidet (Groß- und Kleinschreibung beachten).

4. Bestätigen Sie durch Klicken auf den Pfeil. Der Client wird im Überwachungsmodus gestartet (siehe „Überwachungsmodus“ auf Seite 141).

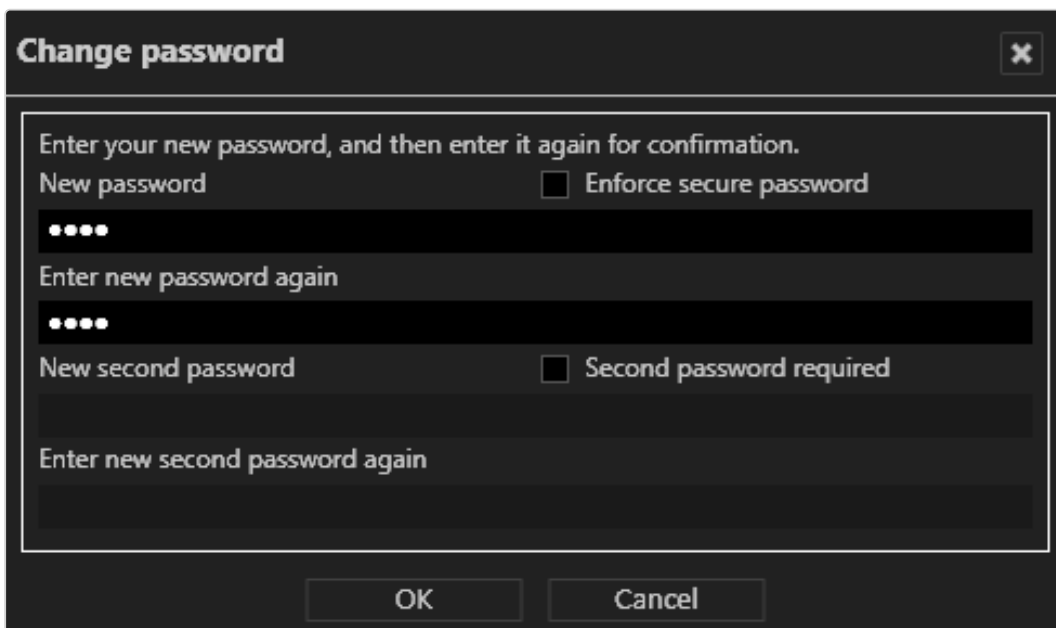
Im Viewer-Modus wird Qognify VMS zur Anzeige exportierter Daten im Archivmodus verwendet (siehe „Anywhere Viewer“ auf Seite 539).

Alle Anmeldeversuche (erfolgreiche und fehlgeschlagene) werden in der Berichtsansicht des Berichtsmodus zusammen mit der IP oder dem Namen des verwendeten Computers protokolliert.

Die Anzahl der fehlgeschlagenen Anmeldeversuche wird vom Administrator im Konfigurationsmodus festgelegt. Außerdem kann ein fehlgeschlagener Anmeldeversuch eine Benachrichtigung auslösen, die ebenfalls im Konfigurationsmodus festgelegt wird (siehe „Benutzer-Sicherheitseinstellungen konfigurieren“ auf Seite 484).

Passwort ändern

Wenn Sie sich zum ersten Mal anmelden, müssen Sie das Standard-Benutzerpasswort ändern.



Change password [X]

Enter your new password, and then enter it again for confirmation.

New password Enforce secure password
••••

Enter new password again
••••

New second password Second password required

Enter new second password again

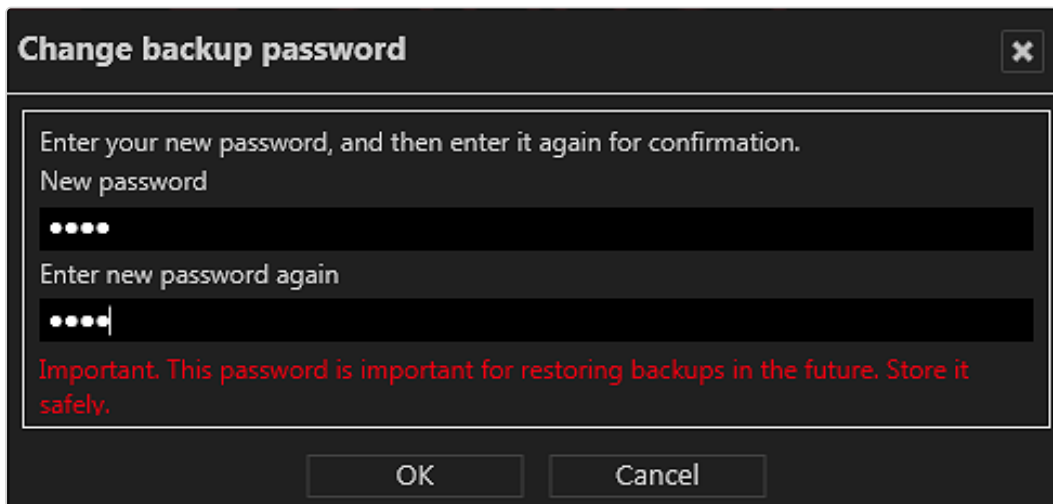
OK Cancel

Abb. 12: Passwort ändern

1. Geben Sie den **Benutzernamen** („administrator“) und das Standard-**Passwort** („pass“) ein.
2. Geben Sie Ihr neues Passwort ein.
3. Deaktivieren Sie **Sicheres Passwort erzwingen**, falls keine erhöhte Passwortsicherheit erforderlich ist (siehe „[Benutzer konfigurieren](#)“ auf Seite 358).
4. Geben Sie gegebenenfalls ein zweites Passwort ein (siehe „[Benutzer konfigurieren](#)“ auf Seite 358).
5. Klicken Sie auf **OK**.

Backup-Passwort der Datenbank ändern

Datenbank-Backups werden verschlüsselt und erfordern ein Passwort. Wenn Sie sich zum ersten Mal anmelden, müssen Sie das Standard-Backup-Passwort der Datenbank ändern.



Change backup password [X]

Enter your new password, and then enter it again for confirmation.

New password
••••

Enter new password again
••••

Important. This password is important for restoring backups in the future. Store it safely.

OK Cancel

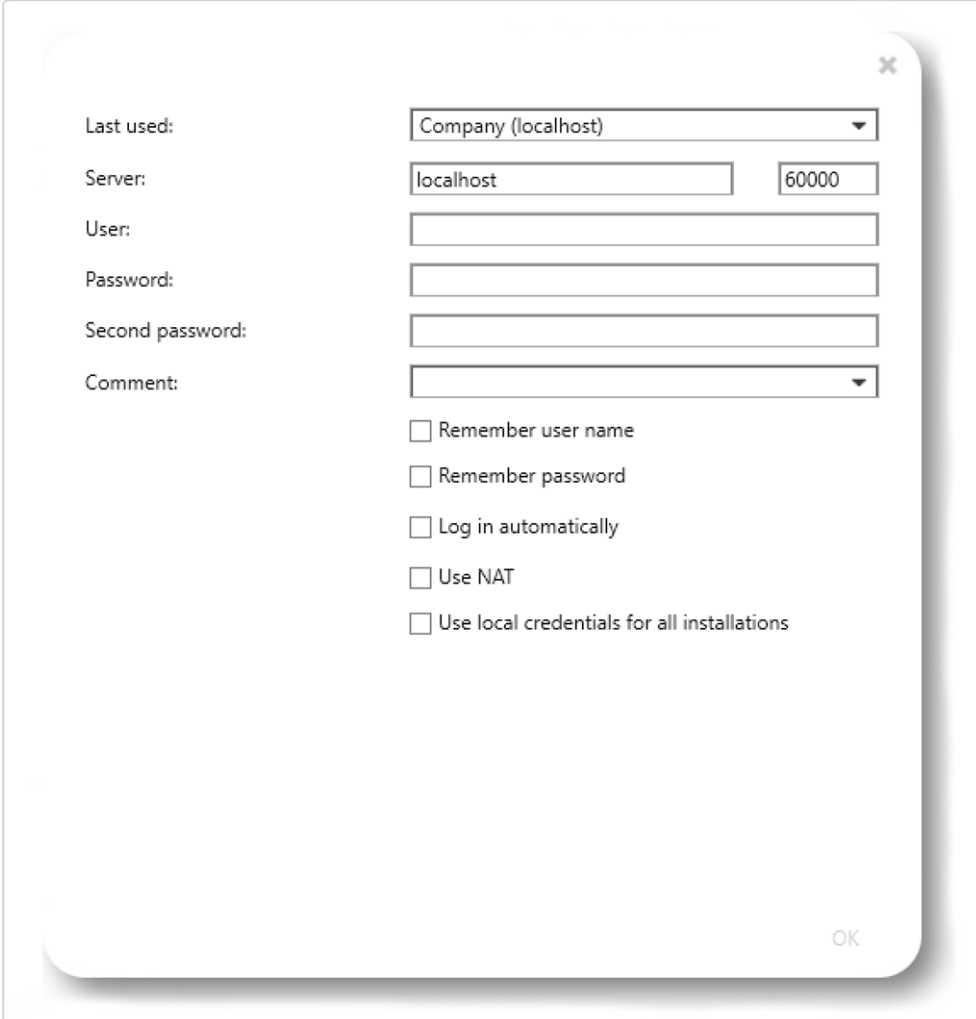
Abb. 13: Backup-Passwort der Datenbank ändern

1. Backup-Passwort der Datenbank eingeben.
2. Geben Sie das neue Backup-Passwort für die Datenbank erneut ein.
3. Klicken Sie auf **OK**.

Erweiterte Anmeldeoptionen

In den erweiterten Optionen des Anmeldebildschirms können zusätzliche Funktionen zur Benutzerverwaltung oder die Anmeldung als Benutzer mit zwei Passwörtern konfiguriert werden.

1. Klicken Sie auf **Erweiterte Optionen** im Anmeldefenster.



The image shows a dialog box titled "Erweiterte Anmeldeoptionen" (Advanced Login Options). It contains the following fields and options:

- Last used:** A dropdown menu showing "Company (localhost)".
- Server:** A text input field containing "localhost" and a port input field containing "60000".
- User:** An empty text input field.
- Password:** An empty text input field.
- Second password:** An empty text input field.
- Comment:** A dropdown menu.
- Remember user name
- Remember password
- Log in automatically
- Use NAT
- Use local credentials for all installations

An "OK" button is located at the bottom right of the dialog.

Abb. 14: Erweiterte Anmeldeoptionen

Folgende Optionen stehen zur Verfügung:

- **Zuletzt verwendet:** Liste der bereits verbundenen Server
- **Server:** Name und Port eines anderen Servers
- **Zweites Passwort,** falls zur Anmeldung benötigt
- **Kommentar::** zusätzliche Informationen für den ausgewählten Login

- **Benutzername merken** und **Passwort merken**: verhindert, dass Sie die Benutzerdaten für die Anmeldung eingeben müssen. Das System trägt den angegebenen Benutzernamen und das Passwort in das Anmeldefenster ein.

Aufgrund gesetzlicher Bestimmungen dürfen in Frankreich der Benutzername und das Kennwort nicht für Installationen gespeichert werden.

- **Benutzer automatisch anmelden**: Zeigt die Benutzeroberfläche an, wenn das Programm gestartet wird (ohne Anmeldung).
- **NAT verwenden**: Ermöglicht es dem Client, auf einen anderen Server über das Internet zuzugreifen. Deaktivieren Sie diese Option, wenn keine Internetverbindung benötigt wird. Für diese Option müssen NAT-Einstellungen im Konfigurationsmodus vorgenommen werden (siehe „[NAT-Liste konfigurieren](#)“ auf Seite 479).
- Um sich bei allen Installationen mit demselben Benutzernamen und Passwort anzumelden, aktivieren Sie **Lokale Anmeldedaten für alle Installationen verwenden**. Optional kann diese Option im Installationsmanager aktiviert werden (siehe „[Qognify-Installation trennen und erneut verbinden](#)“ auf Seite 90).

Achten Sie darauf, dass die Remote-Anmeldedaten den lokalen Anmeldedaten entsprechen.

DAS PASSWORT DES ADMINISTRATORS AN EINEM SICHEREN ORT AUFBEWAHREN!

Falls Sie das Passwort des Administrators vergessen und der Administratorgruppe keine weiteren Benutzer hinzugefügt wurden, ist kein Zugriff auf die Konfigurationseinstellungen des Systems mehr möglich. Das Administratorpasswort kann nicht wiederhergestellt werden.

Im Viewer Mode anmelden

Im Viewer Mode kann auf einen beschränkten Satz von Funktionen in Qognify VMS zugegriffen werden, ohne dass eine Verbindung zur Datenbank und zu den Benutzerverzeichnissen besteht. So können exportierte Daten offline angezeigt werden.

1. Starten Sie Qognify VMS neu und wählen Sie **Viewer Mode** aus.
2. Bestätigen Sie durch Klicken auf den Pfeil auf dem Anmeldebildschirm. Der Client wird im Viewer Mode gestartet.

Die Benutzeroberfläche

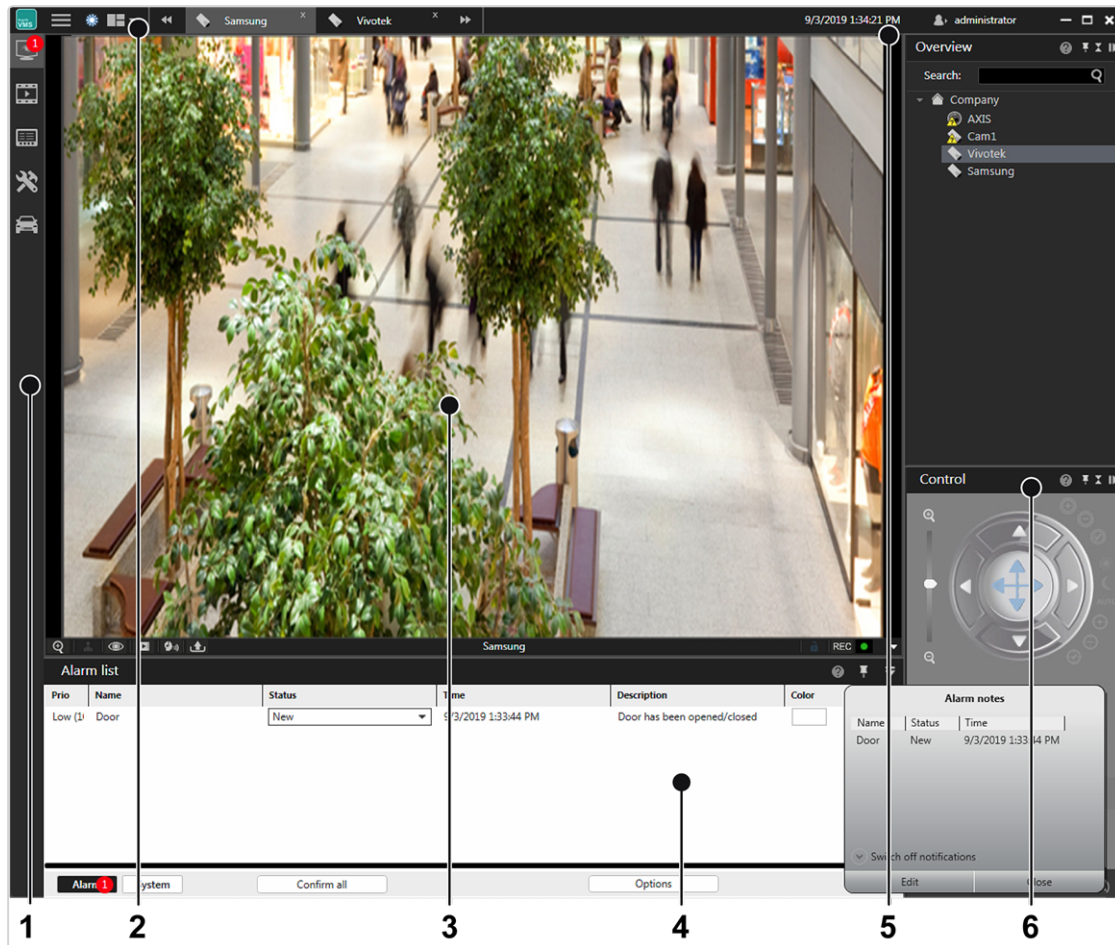


Abb. 15: Die Benutzeroberfläche

Die Benutzeroberfläche gliedert sich in verschiedene Bereiche:

- Mit der **Modusleiste** (1) können Sie zwischen Überwachungsmodus, Archivmodus, Ereignisauswertung, Konfigurationsmodus und LPR-Modus wechseln (siehe „Die Modusleiste“ auf Seite 136).
- Die **Funktionsleiste** (2) enthält grundlegende Bedienfunktionen, die je nach dem verwendeten Modus variieren können (siehe „Die Funktionsleiste“ auf der gegenüberliegenden Seite). Die Funktionsleiste enthält auch das Menü (siehe „Die Menüelemente“ auf Seite 68).
- Die **Arbeitsfläche** (3) ist das Hauptfenster für die Anzeige der ausgewählten Modusfunktionen. Die Arbeitsfläche kann in mehrere Tabs mit unterschiedlichen Inhalten wie Kameras, Ansichten, LPR-Funktionen usw. unterteilt sein (siehe „Arbeitsfläche“ auf Seite 142).



- Das Steuerelement **Information** (4) wird im unteren Teil der Arbeitsfläche angezeigt. Das Steuerelement „Information“ dient zur Anzeige der Alarmliste und Systemmeldungen (siehe „[Alarmliste und Systemmeldungen](#)“ auf Seite 170) im Überwachungsmodus sowie zur Anzeige der Suchergebnisse im Konfigurationsmodus (siehe „[Suchen im Konfigurationsmodus](#)“ auf Seite 217).
- **Anmeldeinformationen** (5) zeigen an, welcher Benutzer derzeit angemeldet ist, und bieten Funktionen zum Benutzerwechsel und zur einfachen Abmeldung (siehe „[Benutzer wechseln](#)“ auf Seite 136).
- Die **Steuerleiste** (6) beinhaltet die Tabs für die Steuerung der Inhalte auf der Arbeitsfläche (siehe „[Die Steuerleiste](#)“ auf Seite 137)

Die Funktionsleiste



Abb. 16: Die Funktionsleiste

Die Funktionsleiste enthält grundlegende Bedienfunktionen, die je nach dem ausgewählten Modus geringfügig variieren können:

- **Logo-Umschalter** (): Löst eine Aktion aus, wenn darauf geklickt wird. Die Logoaktion kann im Menü „Extras“ konfiguriert werden (siehe „[Logoaktion konfigurieren](#)“ auf Seite 122).
- **Navigation** (): Öffnet oder schließt das Navigationsmenü für die Menüs Datei, Ansicht, Tools, Info, Hilfe (siehe „[Die Menüelemente](#)“ auf der nächsten Seite).
- **Umschalter für Tag-/Nachtmodus** (): Stellt den Hintergrund der Benutzeroberfläche dunkler (Nachtmodus) oder heller (Tagmodus) ein. Diese Funktion steht in allen Modi mit Ausnahme des Konfigurationsmodus zur Verfügung.
- **Ansichtsmenü** (): Mit dieser Funktion kann der Benutzer benutzerdefinierte Ansichten im Überwachungsmodus anlegen und anordnen (siehe „[Benutzerdefinierte Ansichten](#)“ auf Seite 147).
- **Benutzerinformation** (): Zeigt den aktuellen Benutzer an und bietet Funktionen zum Abmelden oder Wechseln des Benutzers (siehe „[Benutzer wechseln](#)“ auf Seite 136).
- **Aktuelle Zeit**: Zeigt die aktuelle Uhrzeit und das aktuelle Datum des Client an.

- **Tabauswahl:** Zeigt alle geöffneten Ansichten für einen schnellen Zugriff in Tabs an (siehe „[Ansichten einrichten](#)“ auf Seite 143).

Die Menüelemente

Die Menüelemente sind in allen Modi verfügbar. Die Anzeige einiger Menüelemente hängt von den Benutzerrechten ab:

- **Datei:** Optionen zum Ändern der Einstellungen des Clients, der Sprache, des Passworts, des Profils, der Installation und des Installationsmanagers sowie zum Wechseln des Benutzers (siehe „[Menü „Datei“](#)“ unten).
- **Ansicht:** Verwaltet die Einstellungen der angeschlossenen Bildschirme und der Videowand sowie die LPR-Stammdaten (siehe „[Ansicht](#)“ auf Seite 91).
- **Extras:** Zeigt den Schreibschutz von Aufzeichnungen an und entfernt diesen, konfiguriert den Mehrfachexport von Bilddaten und definiert die Logoaktion (siehe „[Tools](#)“ auf Seite 104).
- **Info :** Zeigt die Informationen zum System und zur Lizenz an (siehe „[Info](#)“ auf Seite 126).
- **Hilfe:** Ruft die Onlinehilfe und Möglichkeiten zur Problemlösung auf (siehe „[Hilfe](#)“ auf Seite 135).

Menü „Datei“

Im Menü „Datei“ werden folgende Optionen angezeigt:

- Client-Konfiguration
- Sprache ändern
- Passwort ändern
- Profil wechseln
- Benutzer wechseln
- Installation wechseln
- Installationsmanager
- Beenden

Client-Konfiguration

Mit der Client-Konfiguration können Sie Einstellungen für Visualisierungsoptionen, Verhalten bei Benutzereingabe, Netzwerkauslastung usw. festlegen.

Es stehen Bearbeitungsoptionen für die folgenden Kategorien zur Verfügung:

Die Einstellungen des Clients werden lokal im Windows-Benutzerprofil abgelegt. Sie dürfen nur von einem Benutzer mit Administratorrechten verändert werden.

1. Starten Sie nach der Änderung der Client-Konfiguration den Client neu, damit die Änderungen wirksam werden.

Client

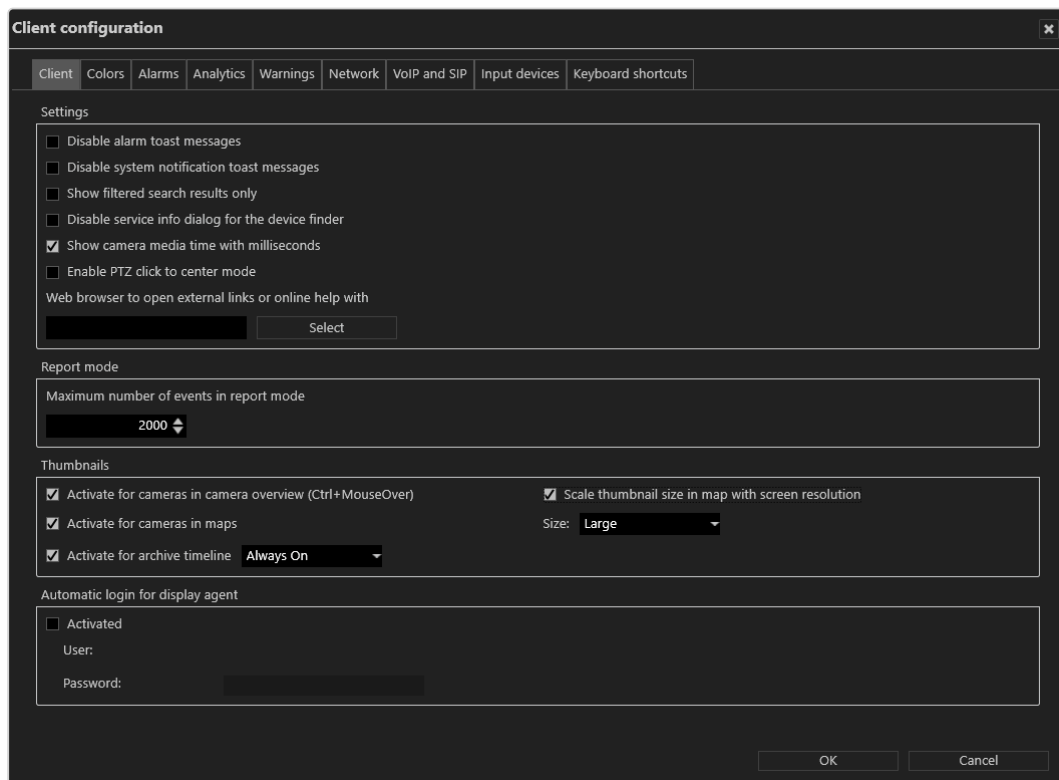


Abb. 17: Client-Konfiguration - Client

Einstellungen

- **Alarm Toast Messages deaktivieren**, um die Alarmbenachrichtigung bei Toast Messages zu unterdrücken (siehe „[Alarmbenachrichtigung](#)“ auf Seite 172).
- **Systembenachrichtigungen mittels Toast Messages deaktivieren**, um Systembenachrichtigungen bei Toast Messages zu unterdrücken (siehe „[Systemmeldungen](#)“ auf Seite 173).
- **Nur gefilterte Suchergebnisse anzeigen**, um in der Liste mit den Suchergebnissen nur die relevanten Suchergebnisse anzeigen zu lassen. (Wenn die Option deaktiviert ist, werden die Suchergebnisse in der Steuerleiste hervorgehoben, es werden jedoch alle Elemente angezeigt.)
- **Dialog mit Dienstinformationen für Gerätesucher deaktivieren**, um die Statusinformationen über den „SSDP Discovery“-Dienst (SSDPSRV) zu unterdrücken, der auf dem Betriebssystem möglicherweise nicht installiert ist. Dieser Dienst bietet UPnP(Universal Plug and Play)-Unterstützung für den Gerätesucher. Wenn das Kontrollkästchen aktiviert wird, wird der Benutzer gebeten, den Dienst zu installieren, wenn er nicht bereits vorhanden ist.
- **Kamera-Medienzeit in Millisekunden anzeigen**, um die Zeit im Archiv Player mit mehr Details anzuzeigen (siehe „[Archiv Player](#)“ auf Seite 178).
- **PTZ-Zentriermodus aktivieren**, um bei Klicken auf das Live-Bild einer Kamera den gewählten Punkt durch Schwenken/Neigen in die Bildmitte zu verschieben.
- **Alarmliste und Systemmeldungen zusammenführen**, um Alarme und Systemmeldungen in einer einzigen Liste anzuzeigen (siehe „[Alarmliste und Systemmeldungen](#)“ auf Seite 170).
- **Webbrowser zum Öffnen externer Links oder der Online-Hilfe**

Ereignisauswertung

- **Maximale Anzahl der Ereignisse im Modus Ereignisauswertung**, um die Anzahl der in der Ereignisauswertung angezeigten Ereignisse zu begrenzen.

Miniaturvorschau

- **Für Kameras in Kameraübersicht aktivieren**, um die Miniaturansicht des jeweiligen Kamerabilds in der Kameraübersicht zu aktivieren. Sie können die Miniaturansichten öffnen, wenn Sie bei gedrückter STRG-Taste mit dem Mauszeiger über die Namen der Kameras in der Übersicht streichen.
- **Für Kameras in Lageplänen aktivieren**, um die Miniaturansicht des jeweiligen Kamerabilds in den Lageplänen zu aktivieren. Sie können die Miniaturansicht öffnen, indem Sie im Lageplan mit dem Mauszeiger über den Namen der Kamera streichen.
- **Größe der Miniaturansichten im Lageplan gemäß Bildschirmauflösung skalieren**. Durch die Skalierung wird die Größe der Miniaturansichten an die Bildschirmauflösung angepasst. Je höher die Bildschirmauflösung, desto höher ist die Auflösung der Miniaturansichten.
- **Aktivieren für Archiv-Zeitleiste** zeigt ein kleines Vorschaubild des ausgewählten Zeitabschnitts an, wenn Sie die Maus im Archivmodus über die Zeitleiste bewegen. Die Optionen sind „Aus“, „Immer an“ und „Steuerungstaste gedrückt“, wobei „Immer an“ die Standardeinstellung ist.

Automatisches Anmelden für Display Agent

- Wenn **aktiviert**, müssen der **Benutzername** und das **Passwort** eingegeben werden, um den Display Agent beim Start des Clients automatisch zu starten.

Farben

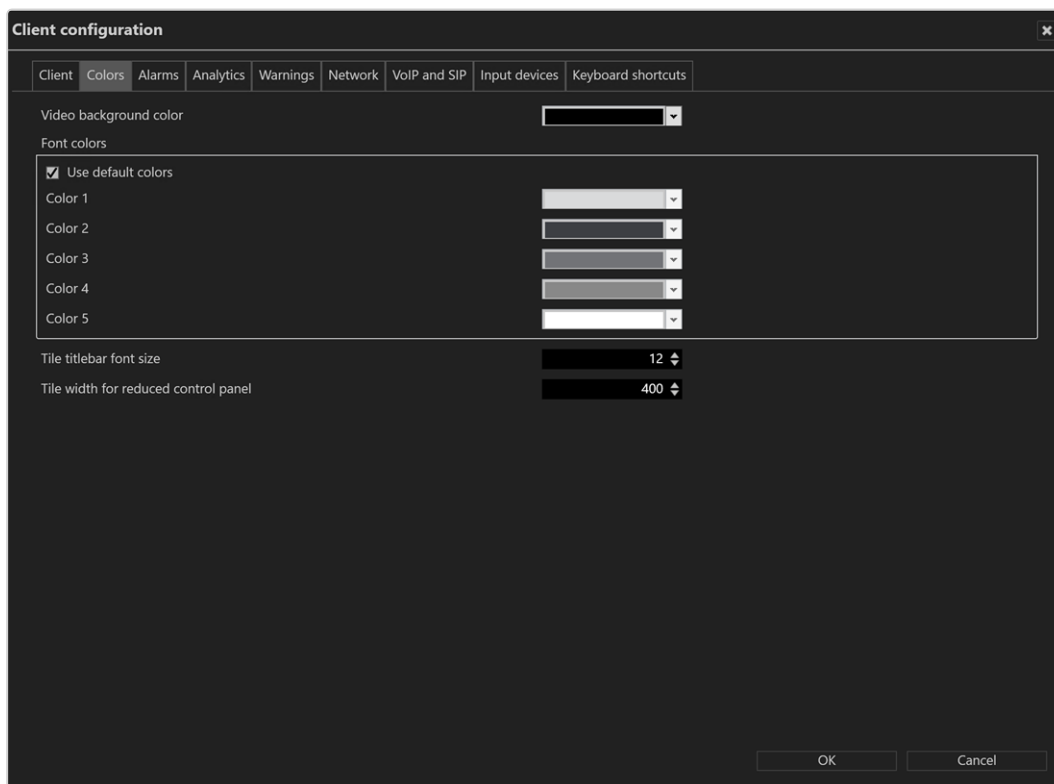


Abb. 18: Client-Konfiguration - Farben

- Die **Video-Hintergrundfarbe** wird um ein Videobild herum angezeigt, wenn sein Seitenverhältnis nicht dem Seitenverhältnis einer Ansicht oder Kachel entspricht.
- **Textfarben**. Die Standard-Textfarben können geändert werden.
 - **Farbe 1** auf dunklem Hintergrund
 - **Farbe 2** auf hellem Hintergrund
 - **Farbe 3** auf einem gemischten Hintergrund wie dem Hauptmenü

- **Farbe 4** auf einem gemischten Hintergrund wie Tabellenüberschriften
- **Farbe 5** auf einem Video-Player-Rahmen (schwarzer Hintergrund)
- Mit **Standardfarben verwenden** werden die Standardeinstellungen wiederhergestellt.
- **Schriftgröße der Kachel-Titelleiste:** Die Schriftgröße des Titels von Ansichten oder Kacheln kann geändert werden.

Alarmer

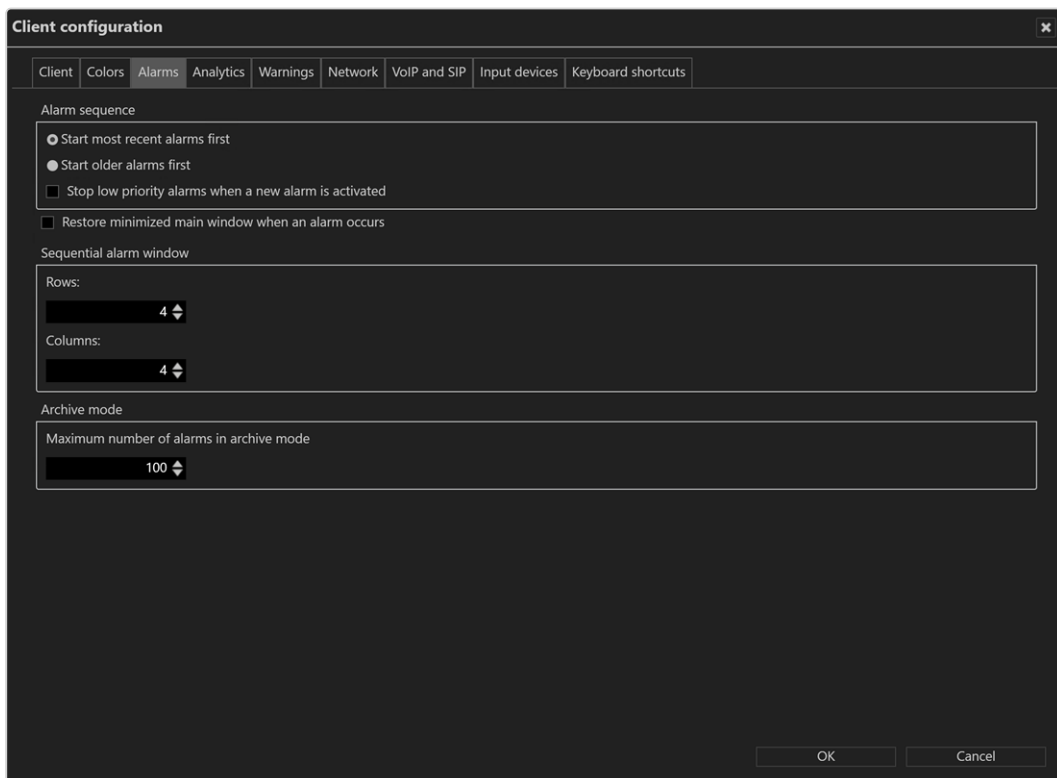


Abb. 19: Client-Konfiguration - Alarmer

- **Alarmreihenfolge** zur Festlegung, ob neuere Alarmer oder ältere Alarmer beim Abarbeiten der Alarmliste zuerst gestartet werden sollen.
- **Alarmer mit niedriger Priorität beenden, wenn ein neuer Alarm aktiviert wird**, um Alarmer mit niedriger Priorität (Priorität 1-4) vor dem Ende des festgelegten Alarmintervalls zu beenden (siehe „[Alarm konfigurieren](#)“ auf [Seite 391](#)).

Alarmer mit hoher Priorität können nicht beendet werden.

- **Minimiertes Hauptfenster wiederherstellen, wenn ein Alarm auftritt**, um das Hauptfenster im Alarmfall wiederherzustellen. Ist diese Option nicht aktiviert, wird das Hauptfenster im Alarmfall nicht wiederhergestellt.
- **Sequenzielles Alarmfenster** zur Angabe der gewünschten Anzahl an Zeilen und Spalten, die angezeigt werden sollen (siehe „[Sequenzielles Alarmfenster hinzufügen](#)“ auf Seite 92).
- **Maximale Anzahl der Alarme im Archivmodus** zur Angabe der maximalen Anzahl der angezeigten Alarme im Archivmodus (siehe „[Archivmodus](#)“ auf Seite 177).

Analytics

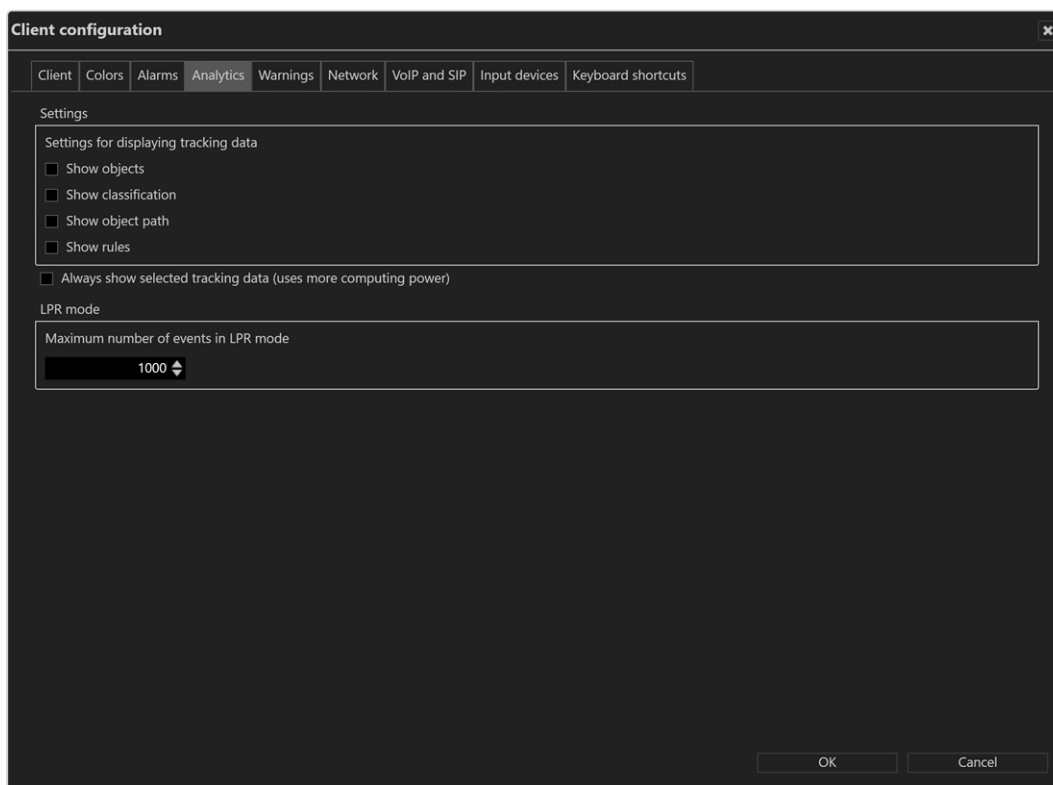


Abb. 20: Client-Konfiguration - Analytics

Die Einstellungen für die Trackingdaten werden als globale Einstellungen im Konfigurationsmodus definiert (siehe „[Qognify Analytics](#)“ auf Seite 327). Sie können separat aktiviert werden.

1. Legen Sie fest, welche Trackingdaten in den ausgewählten Kamerabildern immer angezeigt werden sollen:

- Objekte
 - Klassifikation
 - Zählungen
 - Objektpfad
 - Regeln
2. Aktivieren Sie **Ausgewählte Trackingdaten immer anzeigen**, um Trackingdaten auch in nicht ausgewählten Kamerabildern anzuzeigen. Diese Option verbraucht mehr Leistung auf dem Client.
 3. Legen Sie die **maximale Anzahl der Ereignisse im LPR-Modus** für die Suche nach Kennzeichen fest. Wenn die maximale Anzahl erreicht ist, wird eine Warnung eingeblendet.

Wird die Anzahl erhöht, kann dies zu einer Leistungsminderung und längeren Ladezeiten führen.

Warnungen

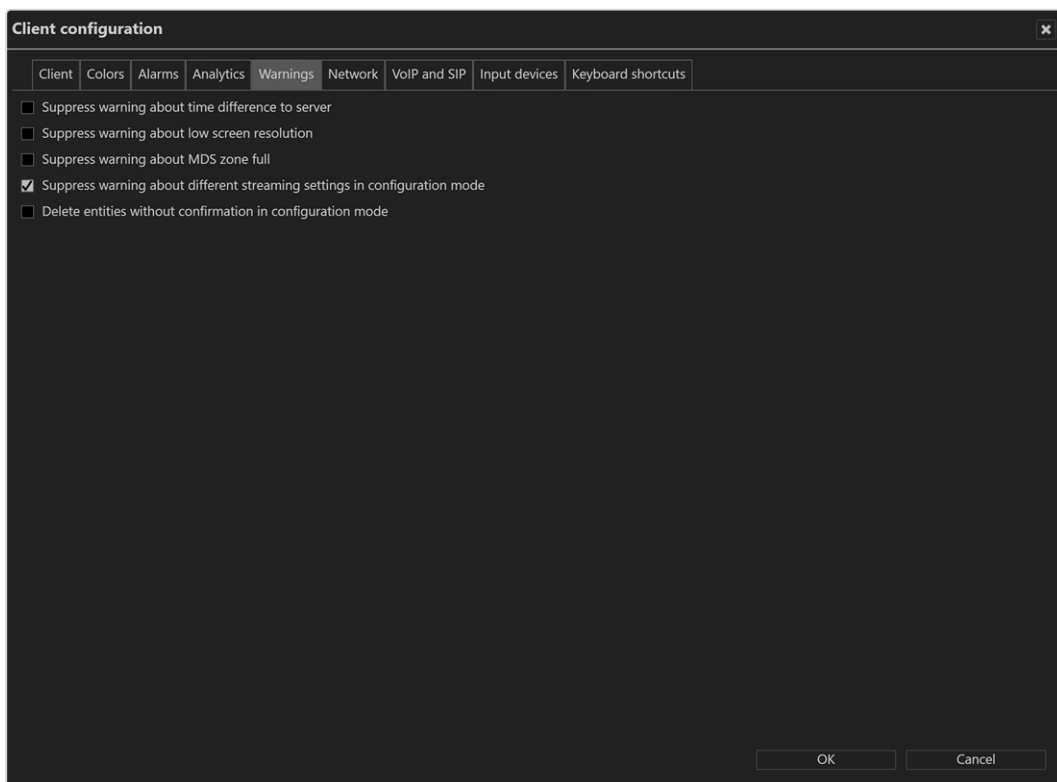


Abb. 21: Client-Konfiguration - Warnungen

- **Warnung bei Zeitdifferenz mit Server unterdrücken**, um eine Meldung zu unterdrücken, falls zwischen Client und Server mehr als zehn Sekunden Zeitdifferenz besteht.
- **Warnung zu niedriger Bildschirmauflösung unterdrücken**, um eine Meldung zu unterdrücken, falls der verwendete Bildschirm nicht über eine ausreichende Auflösung verfügt (siehe „[Systemvoraussetzungen](#)“ auf Seite 31).
- **Warnung bei voller MDS-Zone unterdrücken**, um die Ausgabe einer Meldung zu unterdrücken, wenn die Grenze für die Speichertiefe der MultimediaDatabase erreicht ist (siehe „[Qognify Administrationstool](#)“ auf Seite 501).
- **Warnung zu unterschiedlichen Streaming-Einstellungen im Konfigurationsmodus unterdrücken**, um die Warnung zu unterdrücken, dass bei unterschiedlichen Einstellungen für Standard- und Alarmaufzeichnung Aufzeichnungsverluste auftreten können, wenn für die Alarmaufzeichnung kein zweiter Stream verwendet wird (siehe „[Videostreams](#)“ auf Seite 263).
- **Im Konfigurationsmodus Entitäten ohne Rückfrage löschen**, um die jeweilige Entität (Kamera, Zeitschablone, Alarm, Button usw.) ohne Nachfrage zu löschen, sobald Sie im Konfigurationsmodus **Löschen** wählen.

Netzwerk

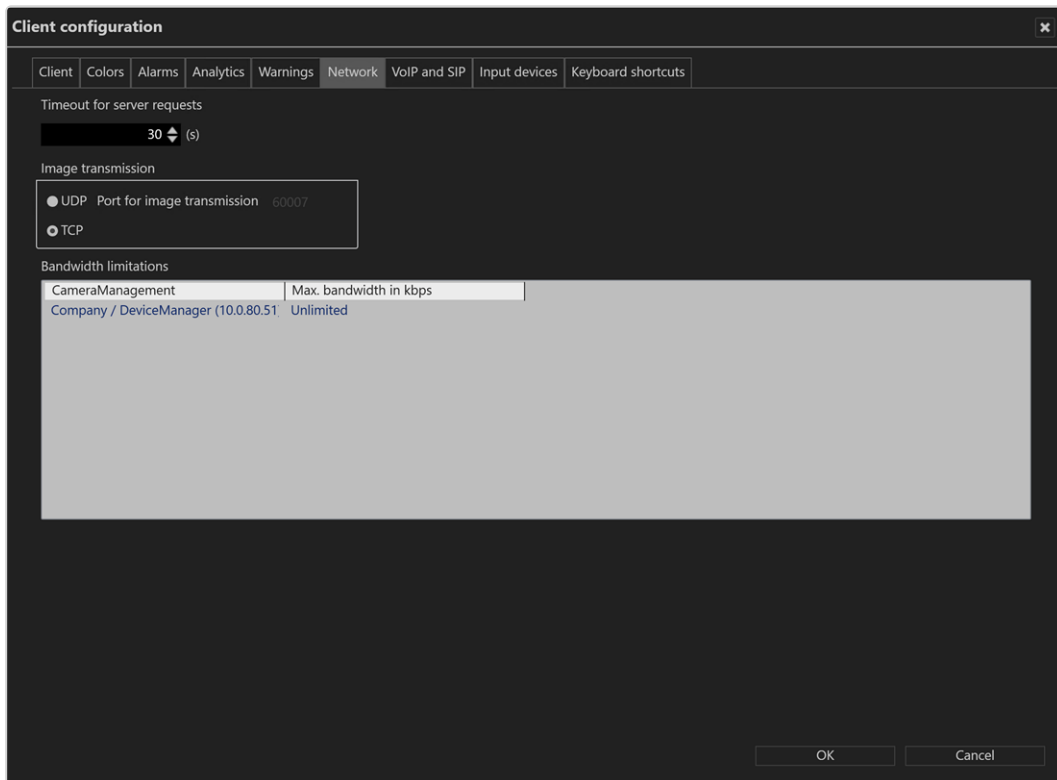


Abb. 22: Client-Konfiguration - Netzwerk

Folgende Optionen stehen zur Verfügung:

- **Timeout für Serveranfragen** zur Erhöhung der Zeitbegrenzung in Sekunden, wenn der Server nicht ausreichend schnell antwortet.
- **Bildübertragung** über den UDP- oder Standard-TCP-Port. Der UDP-Port ist frei wählbar.

Wählen Sie UDP nur bei 100%ig zuverlässigen Netzwerkverbindungen.

- **Bandbreitenbegrenzungen** zur Begrenzung der Bandbreite, wenn auf schmalbandig angebundene Device Manager-Server zugegriffen wird, um eine Überlastung des Netzwerks zu vermeiden.

Es wird davon abgeraten, die Bandbreite zwischen einem Client und dem Server zu begrenzen. Bei begrenzter Bandbreite werden Bilder ausgelassen.

VoIP und SIP

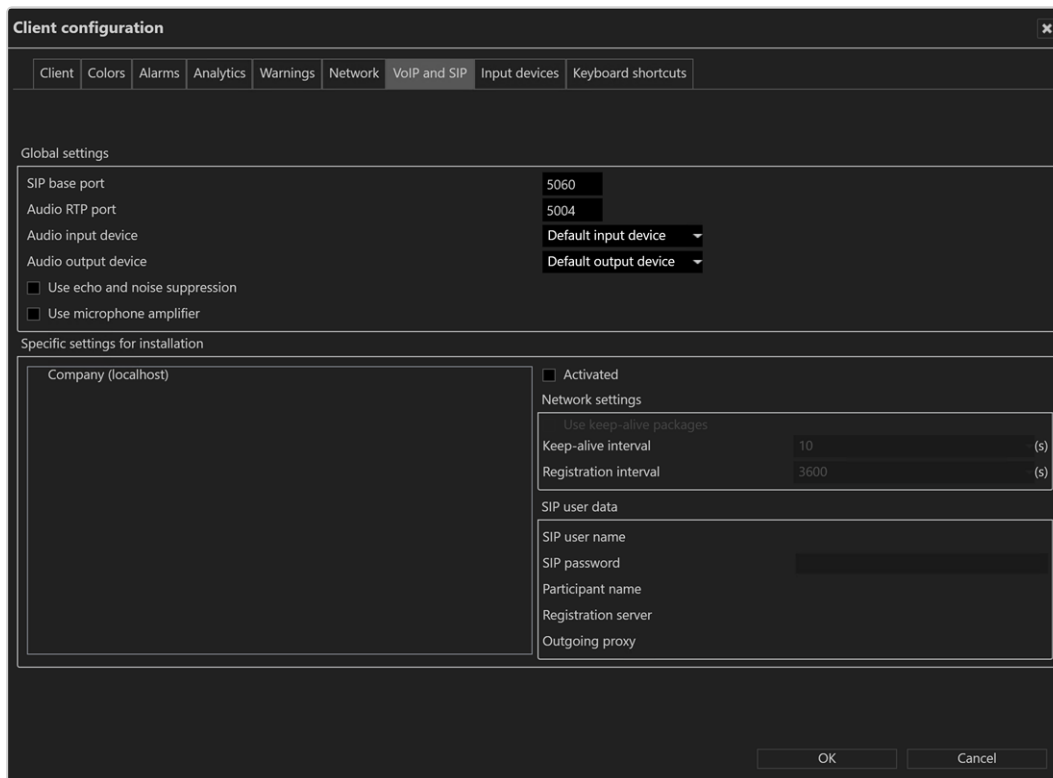


Abb. 23: Client-Konfiguration - VoIP und SIP

Der Qognify VMS-Client kann als SIP-Client fungieren, um mit anderen Clients oder Sprechereinheiten, die den SIP-Standard unterstützen, zu kommunizieren.

- **SIP-Basis-Portnummer** (Standard: 5060)
- **Audio-RTP-Portnummer** (Standard: 7000)
- **Audioeingabegerät** und **Audioausgabegerät**. Eingehende Anrufe werden davon unabhängig über das Standard-Audioausgabegerät des Betriebssystems signalisiert.
- **Echo-/Rauschunterdrückung verwenden**, um die Tonqualität zu verbessern.
- **Mikrofonverstärker verwenden**, um die Lautstärke des Eingabegeräts zu erhöhen.
- **Spezifische Einstellungen für Installation** zeigt alle bestehenden Qognify-Installationen an.

- **Keep-Alive-Pakete verwenden**, um die Intervalle anzupassen, nach denen sich der Client erneut am SIP- oder VoIP-Server anmelden soll. Der Standardwert für das **Keep-Alive-Intervall** ist 10 (s), für das **Registrierungsintervall** 3600 (s).
- **SIP-Benutzername** und **SIP-Passwort** für den SIP-Server.
- **Teilnehmername**: Der Teilnehmername wird im Archivmodus als ange-rufener Teilnehmer angezeigt.
- **Registrierungsserver** und **Ausgehender Proxy**: IP-Adresse des SIP-Ser-vers.

Es wird ein SIP-Server benötigt (siehe [VoIP](#)).

Eingabegeräte

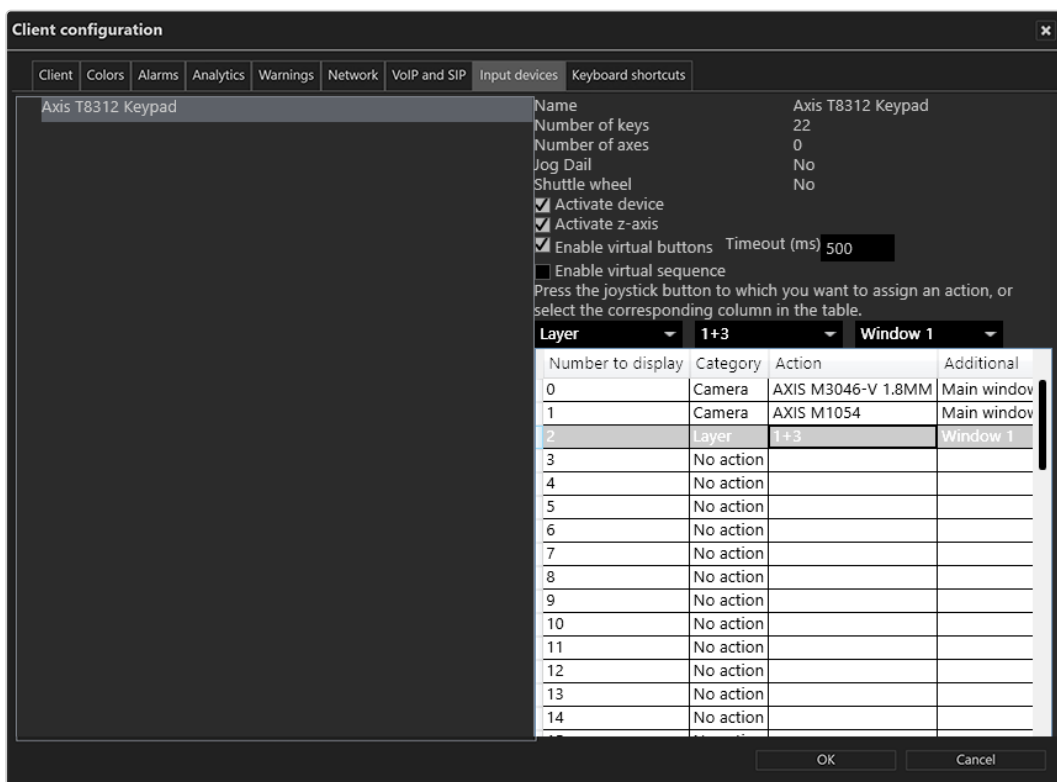


Abb. 24: Client-Konfiguration - Eingabegeräte

In diesem Bereich der Client-Konfiguration werden Eingabegeräte wie Jog Dials, Joysticks oder Tastaturen konfiguriert.

Das Eingabegerät oder die entsprechenden Gerätetreiber müssen auf dem Windows-System installiert sein, bevor es konfiguriert werden kann.

Das Eingabegerät muss mit dem Client-Computer verbunden sein, bevor der Client startet. Anderenfalls wird es in der Client-Konfiguration nicht angezeigt.

Entitäten mit Tasten eines Eingabegeräts auswählen und anzeigen

1. Schließen Sie das Gerät am USB-Anschluss des Client-Computers an.
2. Wählen Sie das Gerät aus. Auf der rechten Seite des Dialogfensters werden die Funktionen des Geräts in einer Liste angezeigt.
3. Aktivieren Sie **Gerät aktivieren**.
4. Aktivieren Sie die Funktionen, z. B. virtuelle Schaltflächen oder virtuelle Sequenzen (siehe [„Konfigurieren von virtuellen Tasten oder Sequenzen des Axis T8312-Bedienfelds“ unten](#)).
5. Aktivieren Sie gegebenenfalls die Z-Achse (hardwareabhängig, für gewöhnlich an Joysticks verfügbar).
6. Drücken Sie die Eingabegerät-Taste, der Sie eine Aktion zuweisen wollen, oder wählen Sie in der Liste die Tastennummer aus.
7. Wählen Sie die gewünschte Aktion aus (z. B. wenn eine bestimmte Taste des Joysticks gedrückt wird, solle eine Kamera oder ein Lageplan in einem bestimmten Fenster der Qognify-Konfiguration angezeigt werden).

Nach Bestätigung der Änderungen muss der Client neu gestartet werden, damit die Änderungen wirksam werden.

Konfigurieren von virtuellen Tasten oder Sequenzen des Axis T8312-Bedienfelds

Mit der Axis T8312-Tastatur kann eine Kamera in einem lokalen Qognify-Fenster oder auf einem Qognify GmbH Display Agent angezeigt werden (siehe [„Display Agent“ auf Seite 93](#)). Um die Anzahl der zu konfigurierenden Buttons zu verringern, ist jede Kamera nummeriert. Siehe die Dokumentation des Tastaturherstellers.

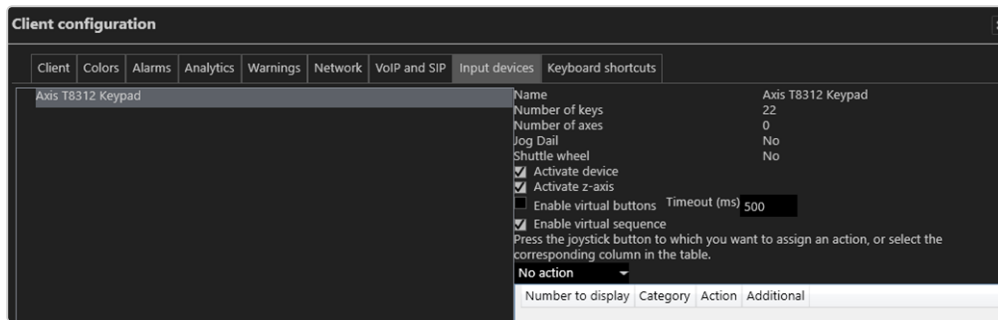


Abb. 25: Konfigurieren von virtuellen Tasten oder Sequenzen des Axis T8312-Bedienfelds
Es kann nur eine der folgenden Optionen zugewiesen werden:

- Wenn die Option **Virtuelle Buttons** wird, können für die Axis T8312-Tastatur bis zu 1000 virtuelle Buttons für das Berufen auf bis zu 1011 Aktionen konfiguriert werden.
- Für die **Verwendung virtueller** Sequenzen ist eine korrekt konfigurierte Entitäten-Nummerierung erforderlich (siehe „[Entitäten-Nummerierung konfigurieren](#)“ auf Seite 479). Im Überwachungs- oder Archivmodus können virtuelle Sequenzen auf der Tastatur gestartet werden (siehe Beispiele unten).

Eine ausführliche Beschreibung der Axis T8312-Tastatur finden Sie in der Dokumentation des Herstellers.

1. Wählen Sie **Virtuelle Schaltflächen** oder **virtuelle Sequenzen** aktivieren.
2. Wenn die virtuellen Schaltflächen aktiviert sind, geben Sie einen Wert für die Zeitüberschreitung (ms) ein. Der Benutzer muss die Schaltflächen innerhalb dieses Zeitraums drücken, um die konfigurierte Aktion auszuführen.
3. Für Tasten oder virtuelle Tasten wählen Sie eine beliebige Taste auf der Tastatur, um die zugewiesene Taste in der Liste in der Spalte „Anzuzeigende Nummer“ anzuzeigen und die Aktion aus dem Dropdown-Menü zu definieren.

Camera Fisheye Camera Main window





Nach Bestätigung der Änderungen muss der Client neu gestartet werden, damit die Änderungen wirksam werden.

Die Tasten des Axis T8312-Bedienfeldes sind wie folgt belegt:


▪ **Erste Reihe:**

- F1: Lokales Display
- F2: Display Agent
- F5: Webseite

▪ **Zweite Reihe:**

-  : Vordefinierte Ansicht
-  : Kamera
-  : Kachel
-  : Temporäre Ansicht
-  : Lagepläne

▪ **Tastenfeld:**

- 0 - 9: Vordefinierte Sequenzen, Schaltflächen oder virtuelle Schaltflächen 0...999
-  : Schalten Sie zwischen den Tasten 0...999 und den virtuellen Tasten 1000...1011 um:

▪ Alt-Taste: 1001

▪  : 1002

▪  : 1003

▪  : 1004

▪  : 1005

▪  : 1006

▪ F1: 1007






▪ F2: 1008

▪ F3: 1009

▪ F4: 1010



▪ F5: 1011

Virtuelle Tasten oder Sequenzen zuweisen

1. Drücken Sie die Tastenkombinationen auf dem Ziffernblock. Der erste Schlüssel wählt die Entität oder die Nummer aus, die zweite Nummer gibt den Entitätstyp oder den Gerätetyp an, z. B.:
 - Durch Drücken der Tasten 0 - F1 - 5 -  zeigt die Kameranummer 5 auf dem Display (F1) Nummer 0, dem lokalen Hauptdisplay, an.
 - Durch Drücken der Tasten 3 - F2 - 1 -  wird die vordefinierte Ebene Nummer 1 auf dem Display Agent (F2) Nummer 3 angezeigt.
 - Durch Drücken der Tasten 1 - F1 - 5 -  wird die Ebene Nummer 5 (eine 2x2-Ebene) auf dem Display (F1) Nummer 1 (dem lokalen sekundären Display) angezeigt.
 - Durch Drücken der Tasten 0 - F1 - 5 -  - 45 -  wird die Kameranummer 45 auf dem Display (F1) Nummer 0 (das lokale Hauptdisplay) in Kachel Nummer 5 angezeigt.

Um die Effizienz bei der Zuweisung der virtuellen Schaltflächen oder Sequenzen zu verbessern, „merkt“ sich die Software die zuvor zugewiesene Position, z. B. Fenster oder Kacheln.

Beispiel

Die Tasten 0 - F1 - 5 -  wurden zugewiesen, um Kamera 5 auf Display 0 anzuzeigen (siehe oben). Die Eingabe der nächsten 6 -  wird die Kamera 6 auf demselben Display angezeigt.

Einschränkungen und Sonderfälle

- Jog Dial und Shuttle Wheel werden für die Tastatur T8312 von Axis im Archivmodus unterstützt.

- Wenn mehrere Joysticks des gleichen Typs verwendet werden, können die Joystick-Einstellungen nach der Aktualisierung auf Version VMS 7.4 verschoben sein. Ändern Sie die physische Verbindung in diesem Fall entsprechend.
- Es muss sichergestellt werden, dass keine andere Anwendung Zugriff auf den Joystick hat, um ein fehlerhaftes Verhalten zu vermeiden.
- Die Steuerungseinheit DCZ von Videotec wird ebenfalls mit folgenden Einschränkungen unterstützt:
 - Es sind nur 32 von 38 Buttons nutzbar.
 - Nur das äußere Jog Dial ist im Archivmodus nutzbar.

Tastenkombinationen

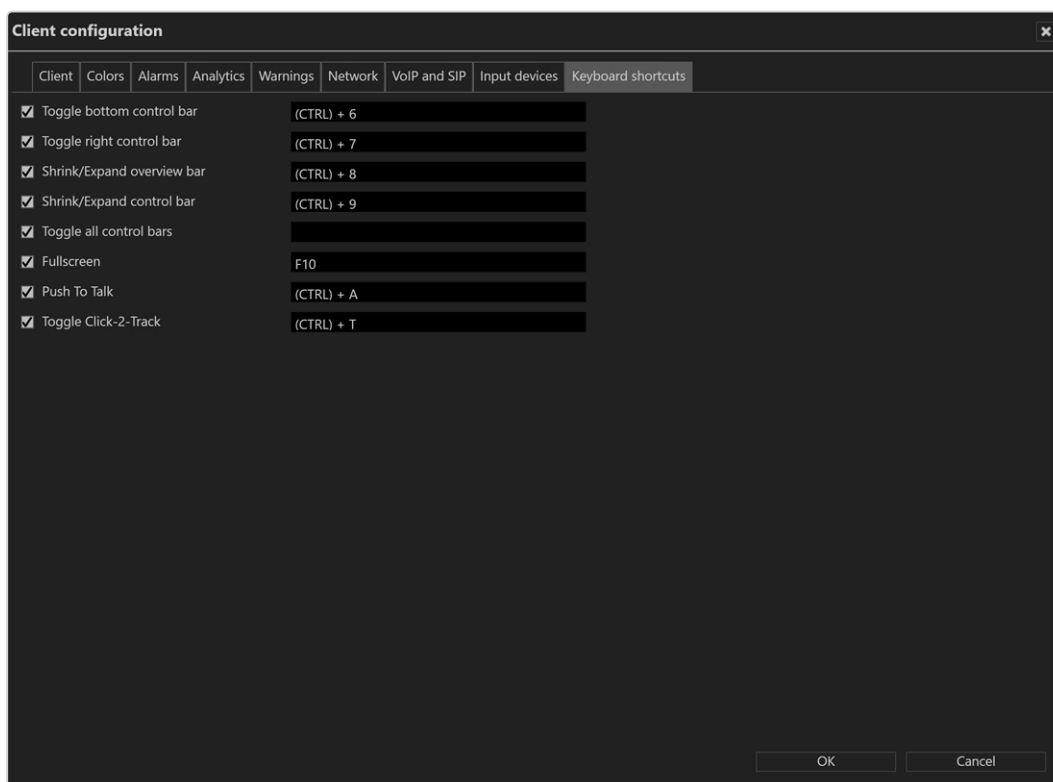


Abb. 26: Client-Konfiguration - Tastenkombinationen

Es können benutzerdefinierte Tastenkombinationen zur Neuordnung der Client-Oberfläche definiert werden.

Folgende Funktionen können konfiguriert werden:

- Untere Steuerleiste umschalten (Standard: (CTRL) + 6)
- Rechte Steuerleiste umschalten (Standard: (CTRL) + 7)

- Übersichtsleiste verkleinern/erweitern (Standard: (CTRL) + 8)
- Steuerleiste verkleinern/erweitern (Standard: (CTRL) + 9)
- Alle Steuerleisten umschalten (Standard: ESC)
- Vollbild (Standard: F10)
- Push To Talk (Standard: (STRG) + A)

Weitere Tastenkombinationen finden Sie unter „[Tastenkürzel](#)“ auf [Seite 537](#).

Sprache ändern

Die Benutzeroberfläche und die Onlinehilfe sind in folgenden Sprachen verfügbar:

- Englisch
- Tschechisch
- Dänisch (nur Benutzeroberfläche)
- Niederländisch
- Französisch
- Deutsch
- Griechisch (nur Benutzeroberfläche)
- Hebräisch
- Italienisch
- Japanisch (nur Benutzeroberfläche)
- Norwegisch (nur Benutzeroberfläche)
- Polnisch
- Portugiesisch (nur Benutzeroberfläche)
- Russisch
- Rumänisch
- Spanisch
- Schwedisch (nur Benutzeroberfläche)
- Thai (nur Benutzeroberfläche)
- Türkisch

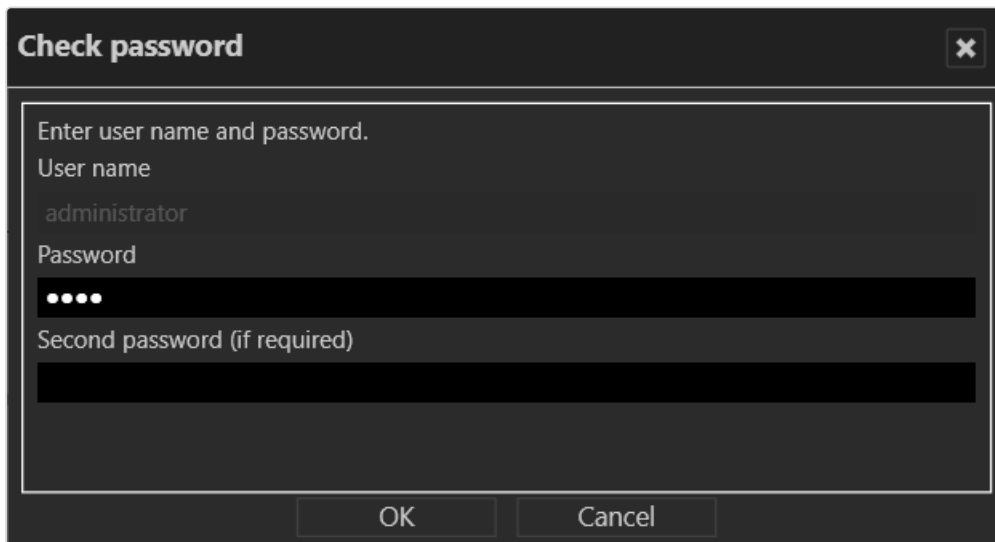
Darüber hinaus können Sie die Benutzeroberfläche mit einer benutzerdefinierten Sprache konfigurieren (siehe „[Technical_Guides_Qognify_Qognify VMS_7.4_DE.pdf](#)“).

1. Wählen Sie **Sprache ändern** auf dem **Datei**-Menü.
2. Wählen Sie die gewünschte Sprache. Mit **Windows-Standard** wird die Sprache des Betriebssystems verwendet.
3. Bestätigen Sie die Auswahl mit **OK** und starten Sie den Client neu.

Passwort ändern

Abhängig von den Benutzerrechten können Sie das Passwort des Benutzers nachträglich ändern.

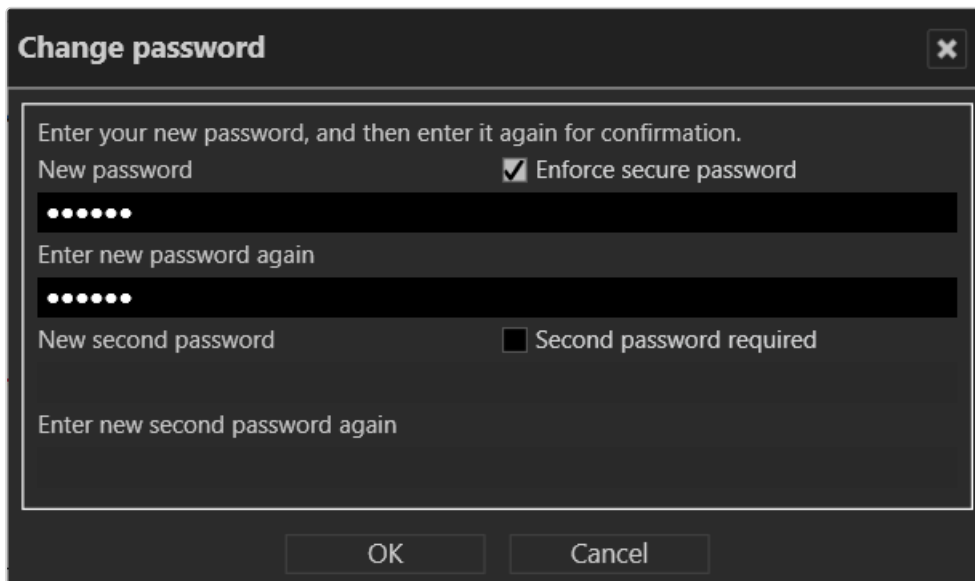
1. Wählen Sie **Passwort ändern** im Menü **Datei**.



The screenshot shows a dialog box titled "Check password" with a close button (X) in the top right corner. The main area contains the text "Enter user name and password." followed by two input fields. The first is labeled "User name" and contains the text "administrator". The second is labeled "Password" and contains four black dots. Below these is a third input field labeled "Second password (if required)" which is empty. At the bottom of the dialog are two buttons: "OK" and "Cancel".

Abb. 27: Passwort ändern - 1

2. Geben Sie das Passwort des aktuellen Benutzers ein und klicken Sie auf **OK**.



The screenshot shows a dialog box titled "Change password" with a close button (X) in the top right corner. The main area contains the text "Enter your new password, and then enter it again for confirmation." followed by two input fields. The first is labeled "New password" and contains six black dots. To its right is a checked checkbox labeled "Enforce secure password". The second input field is labeled "Enter new password again" and contains six black dots. Below these is a third input field labeled "New second password" which is empty. To its right is an unchecked checkbox labeled "Second password required". Below this is a fourth input field labeled "Enter new second password again" which is empty. At the bottom of the dialog are two buttons: "OK" and "Cancel".

Abb. 28: Passwort ändern - 2

3. Geben Sie das neue Passwort an.
4. Bestätigen Sie das Passwort mit **OK**.

Profil wechseln

Falls mehrere Profile (Benutzerprofil, Gruppenprofil usw.) verwendet werden, können Sie zu einem anderen Profil wechseln. Die Profile können im Konfigurationsmodus verwaltet werden (siehe „[Profile](#)“ auf Seite 375).

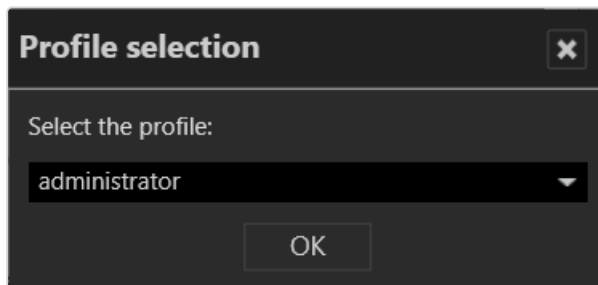


Abb. 29: Profil wechseln

1. Wählen Sie **Profil wechseln** und wählen Sie das gewünschte Profil aus.
2. Bestätigen Sie mit **OK**. Das aktuelle Profil wird abgemeldet und das gewählte Profil wird aktiviert.

Benutzer wechseln

Ein anderer Benutzer kann sich anmelden, ohne den Qognify VMS-Client zu schließen.

1. Wählen Sie **Benutzer wechseln** im Menü **Datei** und wählen Sie den Benutzer aus.
2. Bestätigen Sie die Auswahl mit **OK**. Der aktuelle Benutzer wird abgemeldet und der neue Benutzer muss sich mit Benutzernamen und Passwort anmelden (siehe „[Anmeldung](#)“ auf Seite 57).

Alternativ kann der Benutzer auch über das Benutzersymbol in der Funktionsleiste gewechselt werden (siehe „[Benutzer wechseln](#)“ auf Seite 136).

Qognify VMS-Installation wechseln

Wenn Sie mehrere unabhängige Qognify-Server installiert haben, können Sie eine Verbindung zu einem anderen Qognify-Server herstellen.

1. Wählen Sie **Installation wechseln** im Menü **Datei**. Der Anmeldebildschirm wird angezeigt (siehe „[Anmeldung](#)“ auf Seite 57).
2. Geben Sie den Servernamen oder die IP-Adresse ein sowie den Benutzernamen und das Passwort. Die aktuelle Installation wird beendet und die gewählte Installation wird gestartet.

Installationsmanager

Der Installationsmanager verwaltet und definiert Verbindungen zu mehreren Installationen (Hauptserver). Der aktuelle Verbindungsstatus wird angezeigt.

Die Verbindung mit mehreren Installationen kann zu einer hohen Client- und Netzwerkauslastung führen.

Wenn Sie die bandbreitenoptimierte Archivwiedergabe von mehreren Installationen verwenden, stellen Sie sicher, dass alle Installationen entsprechend konfiguriert sind (siehe „Bandbreitenoptimierung“ auf Seite 464).

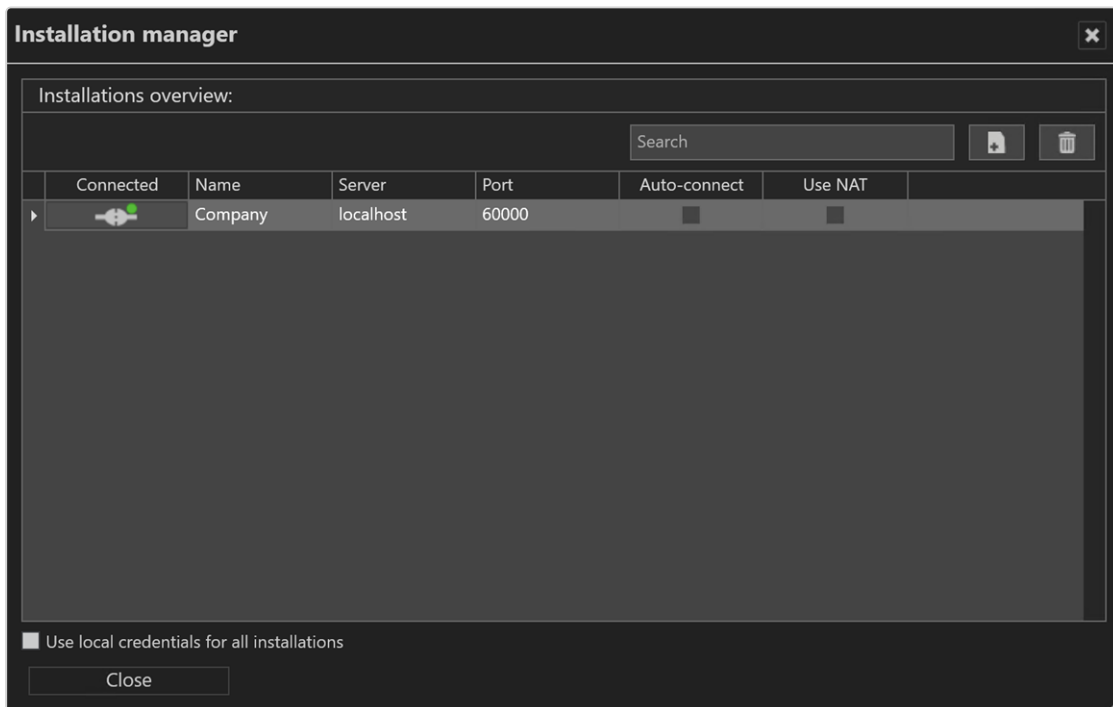


Abb. 30: Installationsmanager

- **Automatisch verbinden:** Aktiviert oder deaktiviert die automatische Verbindung des Clients mit der gewählten Installation.
 - **Suchen:** Suche nach verfügbaren Installationen
 - **Neu** (): Hinzufügen einer neuen Installation
 - **Löschen** (): Entfernt die Installation aus der Liste.
1. Zum Bearbeiten einer Verbindung klicken Sie auf den Namen der entsprechenden Installation.
 2. Um eine Installation hinzuzufügen, klicken Sie auf **Neu** () und bearbeiten Sie die Verbindung. Die neue Installation wird nicht automatisch verbunden.

3. Wenn Sie eine Verbindung zu einer vorhandenen Installation herstellen möchten, aktivieren Sie **Automatisch verbinden**.

Voraussetzungen

- Die Serverversion aller Server, zu denen eine Verbindung hergestellt werden soll, darf nicht höher (aktueller) als die des Clients sein.
- Jeder Server muss Multi Installation Login unterstützen. Es muss eine Lizenz für Qognify Multi Installation Login verfügbar sein.

Installation hinzufügen

1. Wählen Sie **Installationsmanager** im Menü **Datei** und aktivieren Sie die gewünschten Server.
2. Wenn der Server nicht angezeigt wird, fügen Sie die Installation hinzu. Geben Sie dazu den Namen der Installation, die IP-Adresse oder den Hostnamen und die Portnummer des Servers an.
3. Klicken Sie auf **Hinzufügen**.

Installationen neu anordnen

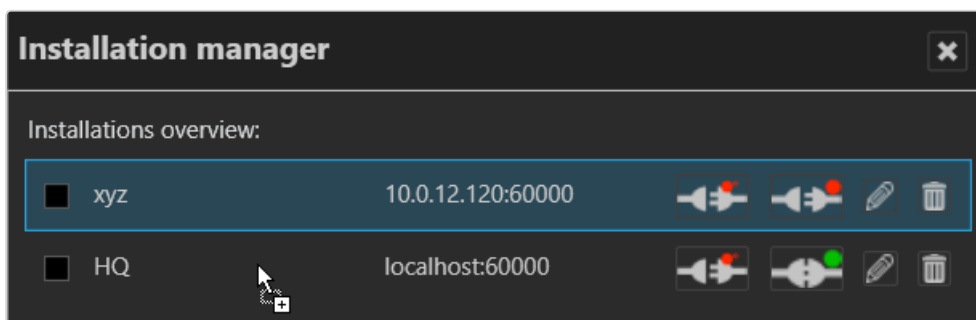


Abb. 31: Installationen neu anordnen

1. Ordnen Sie die Liste der Installationen neu, indem Sie ein Objekt auswählen und es an die gewünschte Position in der Liste ziehen.

Qognify-Installation trennen und erneut verbinden


Die Farbmarkierung im Symbol gibt den Verbindungsstatus an. Ein grüner Punkt gibt an, dass das System verbunden ist, ein roter Punkt bedeutet, dass das System getrennt ist.

1. Klicken Sie auf **Automatisch verbinden**, damit der Client beim Start automatisch mit dem ausgewählten Server verbunden wird.
2. Zur manuellen Verbindung oder Trennung klicken Sie auf **Verbinden** bzw. **Trennen**.
3. Um sich bei allen Installationen mit demselben Benutzernamen und Passwort anzumelden, aktivieren Sie **Lokale Anmeldedaten für alle Installationen verwenden**. Optional kann diese Option im Anmeldefenster aktiviert werden (siehe „[Erweiterte Anmeldeoptionen](#)“ auf Seite 61).

Achten Sie in diesem Fall darauf, dass die Remote-Anmeldedaten den lokalen Anmeldedaten entsprechen.


Qognify-Installationen bearbeiten

Ändert die IP-Adresse, den Hostnamen und die Portnummer des gewählten Servers.

1. Klicken Sie auf **Bearbeiten**  für die Qognify-Installation, die Sie ändern möchten. Der gewählte Server wird unten im Fenster angezeigt.
2. Bearbeiten Sie den Namen der Installation, die IP-Adresse bzw. den Hostnamen und die Portnummer des Servers.
3. Klicken Sie auf **Übernehmen**.

Gespeicherte Qognify-Installationen löschen

Bereinigt die Liste der gespeicherten Qognify-Installationen, die zuletzt vom Client aufgerufen wurden (siehe „[Anmeldung](#)“ auf Seite 57).

1. Klicken Sie auf **Löschen**  für die Qognify-Installation, die nicht mehr zur Auswahl verfügbar sein soll.
2. Um mehrere Installationen gleichzeitig zu löschen, wählen Sie die zu löschenden Installationen aus und klicken Sie auf **Markierte Obj. löschen**.

Ansicht

Im Menü „Ansicht“ werden folgende Optionen angezeigt:

- Fenster hinzufügen
- Sequenzielles Alarmfenster hinzufügen
- Seitenverhältnis beibehalten
- Rahmenlose Darstellung
- Display Agent
- Videowall Dispatcher
- LPR-Stammdateneditor
- Zählungsauswertung
- Editor für Zutrittskontrolldaten

Die im Menü „Ansicht“ vorgenommenen Einstellungen werden lokal abgelegt und müssen an jedem Client und für jedes Windows®-Anmeldeprofil individuell vorgenommen werden.

Ausgenommen hiervon sind:

- Einstellungen für den „LPR-Stammdateneditor“ auf Seite 94
- Daten der Zählungsauswertung
- Zutrittskontrolldaten

Diese Daten werden von den entsprechenden Diensten auf den Servern gespeichert.

Fenster hinzufügen

Mit dieser Funktion können Sie die Darstellung der Arbeitsfläche auf mehrere angeschlossene Monitore verteilen.

1. Wählen Sie **Fenster hinzufügen** im Menü **Ansicht**. Ein zweites Fenster wird geöffnet.
2. Verschieben Sie das Fenster auf den angeschlossenen Monitor. Der Client speichert die Einstellung und stellt sie auch nach der erneuten Anmeldung wieder zur Verfügung.
3. Um mehrere angeschlossene Monitore zu nutzen, wiederholen Sie die Schritte.

Sequenzielles Alarmfenster hinzufügen

Im Fall eines Alarmszenarios werden die als Alarmkameras in einem aktiven Alarmszenario definierten Kameras (siehe „[Alarme](#)“ auf Seite 386) in einem separaten Alarmfenster angezeigt. Der Name der Kamera wird angegeben und die Farbe des Bildrahmens im Fenster entspricht der Farbe des Alarmszenarios.

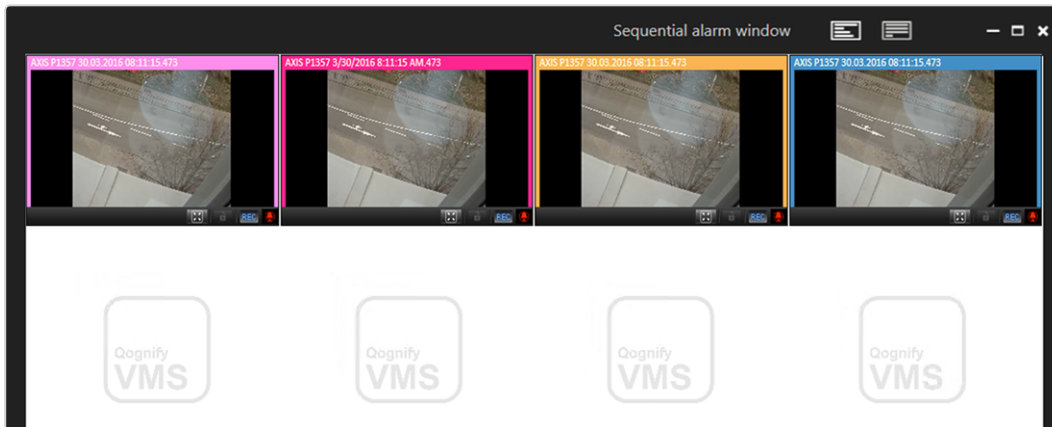




Abb. 32: Sequenzielles Alarmfenster hinzufügen

1. Wählen Sie **Sequenzielles Alarmfenster hinzufügen**, um alle alarm-relevanten Kameras in einem neuen, eigenen Fenster anzuzeigen.
2. Wählen Sie eine der folgenden Optionen:
 - **Zeilenmodus** , um Bilder mit einem Alarm pro Zeile anzuzeigen
 - **Fortlaufender Modus** , um mehrere Alarme pro Zeile anzuzeigen

Seitenverhältnis beibehalten

1. Wählen Sie **Seitenverhältnis beibehalten**, um das Kamerabild auf das Ansichtsfenster anzupassen. Das Kamerabild wird gegebenenfalls verzerrt dargestellt.
2. Deaktivieren Sie **Seitenverhältnis beibehalten**, um das Kamerabild wieder im originalen Seitenverhältnis anzuzeigen.

Rahmenlose Darstellung

1. Wählen Sie **Rahmenlose Darstellung**, um in Ansichten mit mehreren Kameras die jeweiligen Steuerelemente und die Stege zwischen den Kamerabildern auszublenden. Wird eine Kamera ausgewählt, wird der Rahmen eingeblendet.
2. Deaktivieren Sie **Rahmenlose Darstellung**, um in Ansichten mit mehreren Kameras die jeweiligen Steuerelemente und die Stege zwischen den Kamerabildern einzublenden.

Display Agent

Mit dem Qognify Display Agent können Sie handelsübliche PCs und die daran angeschlossenen Monitore in eine vollwertige fernsteuerbare Videowand umwandeln, die mit dem Videowall Dispatcher gesteuert werden kann (siehe „[Videowände](#)“ auf Seite 430).

Der Videowall Dispatcher wird zur Steuerung eines Display Agent benötigt.

Videowall Dispatcher

Der Videowall Dispatcher kann verbundene Bildschirme dynamisch steuern. Per Drag & Drop können Kamerabilder, Ansichten, Lagepläne und Webseiten auf Videowänden angezeigt werden, z. B. QognifyDisplay Agents oder eyevis Videowänden.

Editor für Zutrittskontrolldaten

In der Liste können die Ausweisinhaber nach Kennzeichengruppen sortiert und angezeigt werden.

Informationen zum Arbeiten mit dem Zutrittskontrollsystem finden Sie im Dokument „[Technical_Guides_Qognify_Qognify VMS_7.4_DE.pdf](#)“ oder wenden Sie sich an den Support (siehe „[Support](#)“ auf Seite 13).

1. Klicken Sie auf den Pfeil neben dem Namen der Ausweisinhaberguppe, um diese einzuklappen.

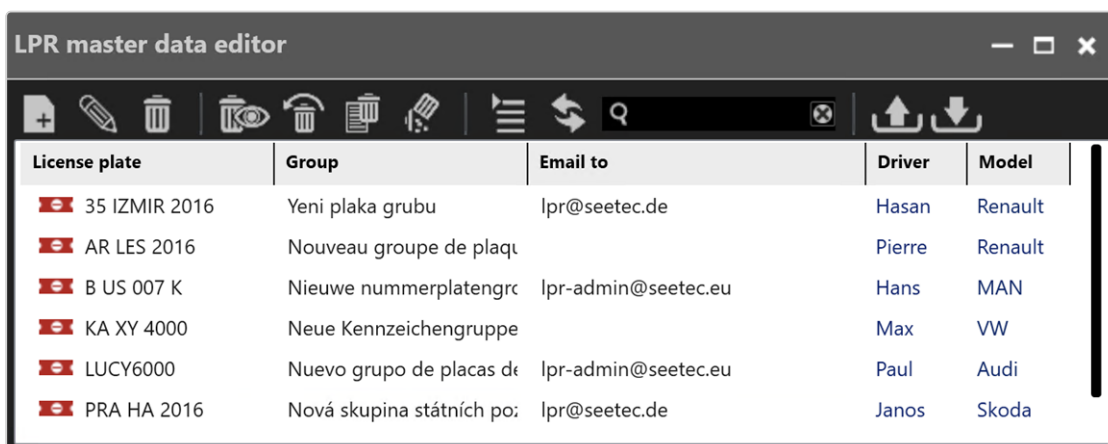
2. Klicken Sie erneut auf den Pfeil, um die Ausweisinhabergruppe wieder aufzuklappen.

LPR-Stammdateneditor

Im LPR-Stammdateneditor (Kennzeichenerkennung) können Kennzeichen hinzugefügt oder gelöscht sowie die zugehörigen Daten wie Name des Fahrers, Tickets, Historie und Benachrichtigungen bearbeitet werden.

Die Kennzeichenerkennung muss vor der Nutzung im Qognify VA Administrationstool (siehe „[Qognify VMS VA Administrationstool](#)“ auf [Seite 513](#)) sowie im Konfigurationsmodus konfiguriert werden (siehe „[Globale OCR-Einstellungen konfigurieren](#)“ auf [Seite 444](#) und „[LPR-Modul konfigurieren](#)“ auf [Seite 446](#)).

Der LPR-Stammdateneditor ist nur verfügbar, wenn mindestens eine LPR-Gruppe mit den entsprechenden Rechten konfiguriert wurde (siehe „[Kennzeichengruppen](#)“ auf [Seite 432](#)).



The screenshot shows a window titled "LPR master data editor" with a toolbar and a table of license plate data. The table has columns for License plate, Group, Email to, Driver, and Model. The data rows are as follows:







License plate	Group	Email to	Driver	Model
 35 IZMIR 2016	Yeni plaka grubu	lpr@seetec.de	Hasan	Renault
 AR LES 2016	Nouveau groupe de plaqu		Pierre	Renault
 B US 007 K	Nieuwe nummerplategrc	lpr-admin@seetec.eu	Hans	MAN
 KA XY 4000	Neue Kennzeichengruppe		Max	VW
 LUCY6000	Nuevo grupo de placas de	lpr-admin@seetec.eu	Paul	Audi
 PRA HA 2016	Nová skupina státních po:	lpr@seetec.de	Janos	Skoda

Abb. 33: LPR-Stammdateneditor

Zur Verwaltung von Kennzeichen stehen folgende Optionen zur Verfügung:

Neues Kennzeichen anlegen

Abhängig von der Konfiguration wird das Fenster für die Eingabe neuer Daten automatisch geöffnet, sobald ein Kennzeichen von der entsprechenden Kamera erkannt wird (siehe „[Globale OCR-Einstellungen konfigurieren](#)“ auf [Seite 444](#)).

Der LPR-Stammdateneditor kann über das Menü „Ansicht“ gestartet werden.

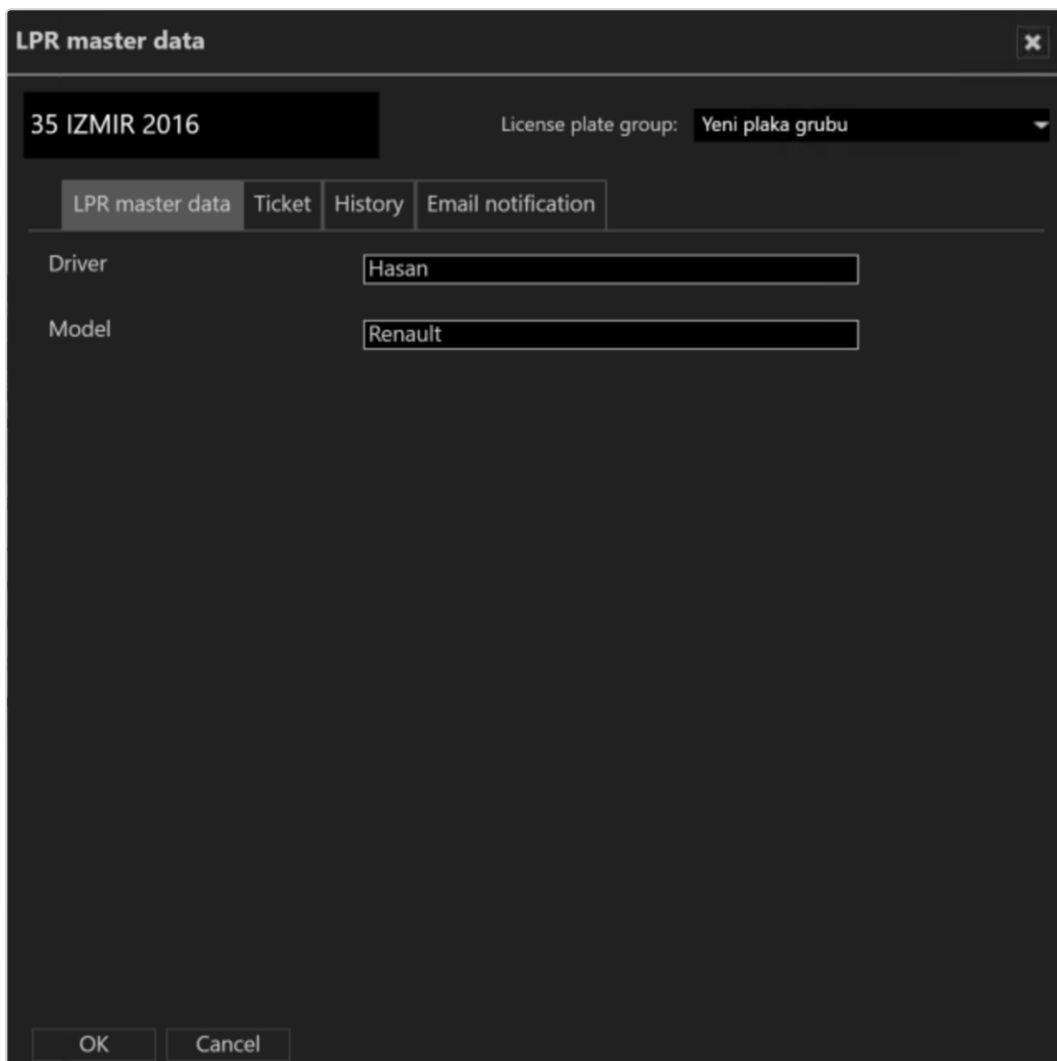




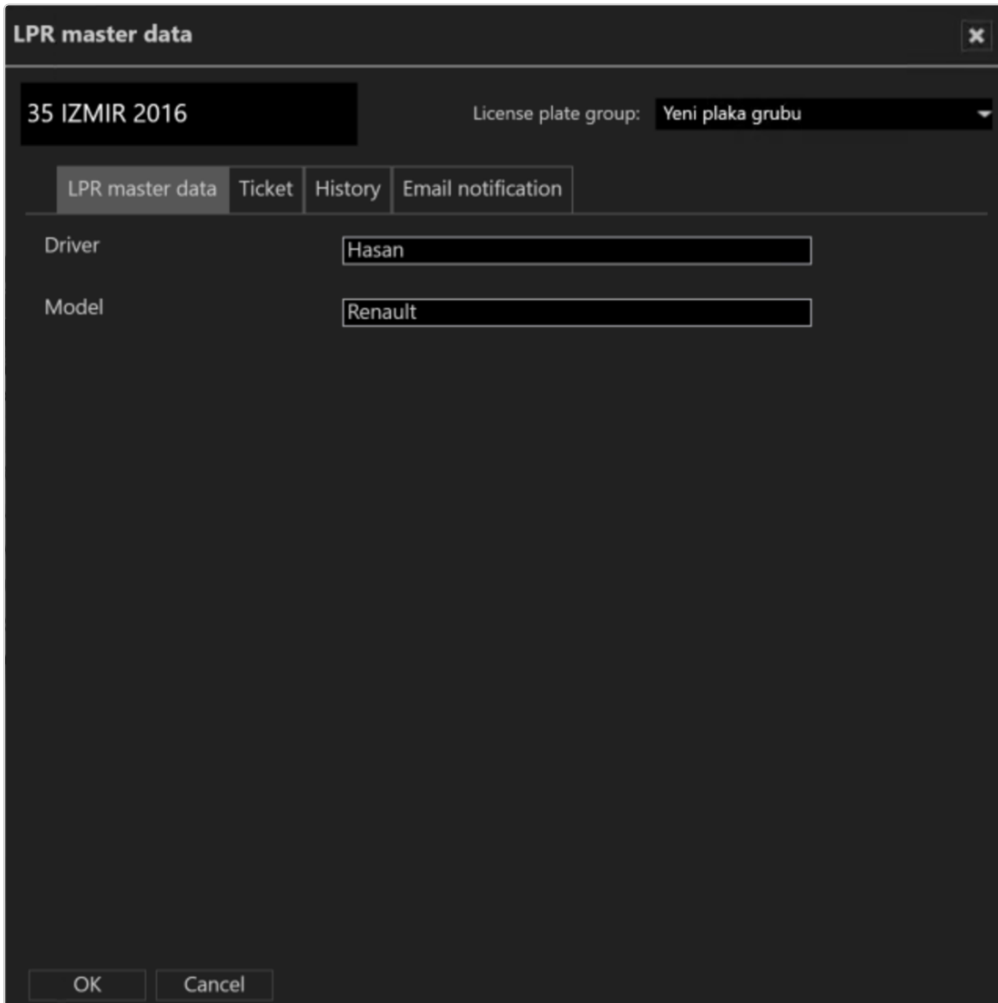
Abb. 34: Neues Kennzeichen anlegen

1. Wählen Sie im Stammdateneditor **Neu**  aus.
2. Geben Sie das neue Kennzeichen in das Textfeld oben links ein, falls es noch nicht angezeigt wird.
3. Weisen Sie dem Kennzeichen eine **Kennzeichengruppe** zu. Kennzeichengruppen werden im Konfigurationsmodus im Bereich „Kennzeichengruppen“ angelegt (siehe „[Kennzeichengruppen](#)“ auf Seite 432).
4. Optional können Sie die Beschreibungen für das Kennzeichen hinzufügen. Die Bezeichnung und die Anzahl der Textfelder werden im Konfigurationsmodus im Bereich „Server“ definiert (siehe „[Globale OCR-Einstellungen konfigurieren](#)“ auf Seite 444).
5. Bestätigen Sie die Einstellungen mit **OK**.

Kennzeichen bearbeiten

1. Wählen Sie ein Kennzeichen in der Liste des Stammdateneditors aus.
2. Wählen Sie **Bearbeiten** , um die Angaben zum Kennzeichen zu ändern.

LPR-Stammdaten



The screenshot shows a dialog box titled "LPR master data" with a close button (X) in the top right corner. The main content area displays the license plate "35 IZMIR 2016" and the license plate group "Yeni plaka grubu" in a dropdown menu. Below this, there are four tabs: "LPR master data", "Ticket", "History", and "Email notification". The "LPR master data" tab is selected. Underneath the tabs, there are two input fields: "Driver" with the value "Hasan" and "Model" with the value "Renault". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Abb. 35: LPR-Stammdaten

1. Bearbeiten Sie das Kennzeichen.
2. Klicken Sie auf **OK**, um die Einstellungen zu übernehmen.

Ticket

Tickets definieren den Gültigkeitszeitraum bestimmter Kennzeichen, z. B. dass ein Kennzeichen eine Schranke nur zu den Bürozeiten passieren darf.

LPR master data [X]

35 IZMIR 2016 License plate group: Yeni plaka grubu

LPR master data | **Ticket** | History | Email notification

Valid from: Saturday, December 3, 2016 12:00:00 A [Activate]

Valid until: Saturday, December 3, 2016 11:59:59 P

Validity: Always

Visualization in LPR list:

- Valid ticket
- Ticket expired
- Future ticket
- (none) Season ticket (not an individual ticket)

Always Today Tomorrow Current week Next week Never

OK Cancel

Abb. 36: Ticket

1. Wählen Sie einen vordefinierten **Gültigkeitszeitraum** für das Kennzeichen aus. Die vordefinierten Gültigkeitszeiträume werden auf der linken Seite angezeigt.
2. Um einen bestimmten Zeitraum anzugeben, klicken Sie auf **Aktivieren** und geben Sie den gewünschten Zeitraum ein. Der in der LPR-Liste angegebene Status des Tickets wird durch die unterschiedliche Textfarbe und ein Icon angezeigt. Wenn ein Zeitraum bereits definiert ist, ist die Aktivierung nicht mehr aktiv.
3. Klicken Sie auf **OK**, um die Einstellungen zu übernehmen.

Historie

Im Tab „Historie“ werden die Erstkonfiguration des Kennzeichens und alle späteren Änderungen angezeigt. Für eine bessere Lesbarkeit können Sie die Spalten der Liste an den Stegen verschieben.

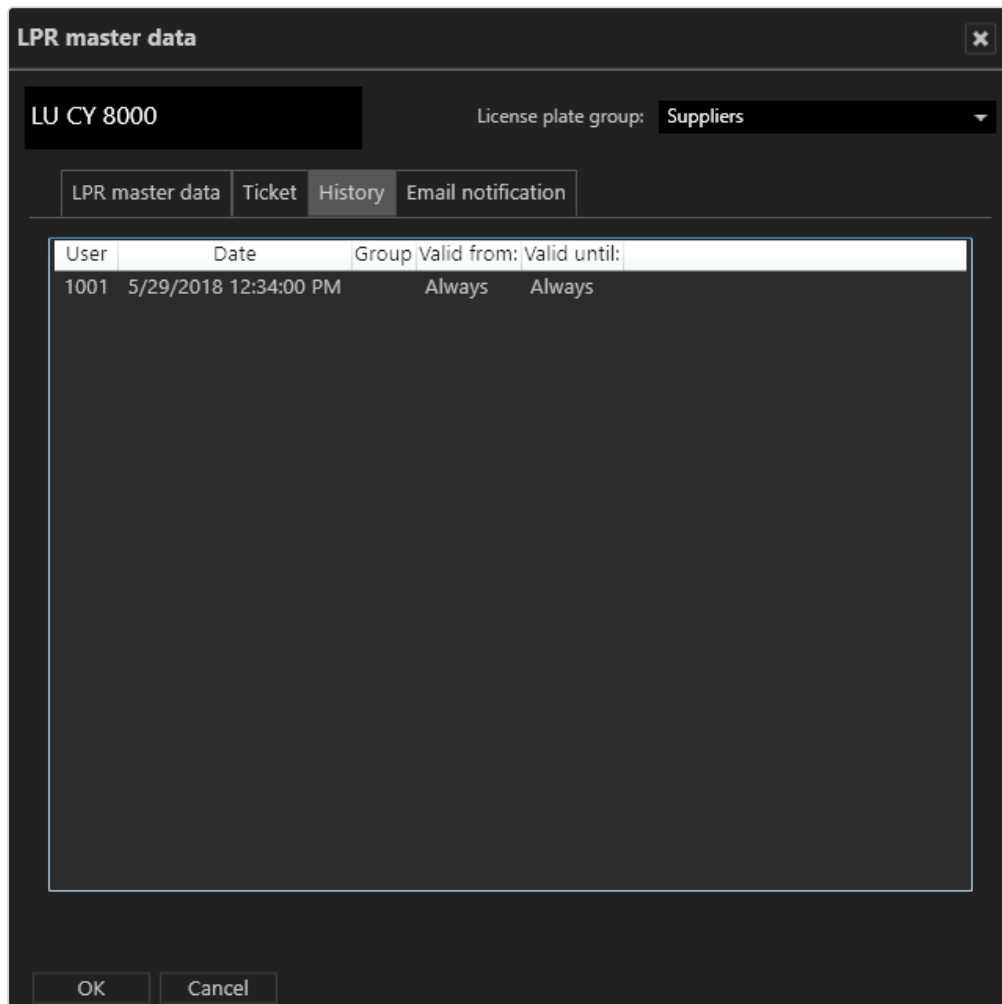


Abb. 37: Historie

1. Klicken Sie auf **OK**, um das Fenster zu schließen.

E-Mail-Benachrichtigung

Sie können E-Mail-Benachrichtigungen an bestimmte Empfänger senden, sobald das Fahrzeug mit dem angegebenen Kennzeichen erkannt wird.

LPR master data [X]

35 IZMIR 2016 License plate group: Yeni plaka grubu

LPR master data Ticket History Email notification

Recipient:
lpr@seetec.de
Separate multiple recipients with a semicolon.

Message:
[1] plakası [4] tarihinde saat [5] itibariyle tanımlandı.

Macros:
[0] Image
[1] License plate
[2] Group
[3] Unknown status
[4] Date
[5] Time
[6] Lane name
[7] Module name
[10] Master data field 1
...
[19] Master data field 10

OK Cancel

Abb. 38: E-Mail-Benachrichtigung


1. Geben Sie die E-Mail-Adressen der Empfänger durch Semikolons getrennt an.
2. Geben Sie den Text der E-Mail ein. Die Nummern auf der rechten Seite sind Platzhalter für Variablen (d. h. Kennzeichen-Details), die automatisch gesendet werden.
3. Klicken Sie auf **OK**, um die Einstellungen zu übernehmen.

Beispiel: Der Text im Nachrichtenfeld „Kennzeichen [1] ist am [4] um [5] erkannt worden.“ ergibt in der E-Mail „Kennzeichen LU CY 8000 ist am 15.04.2010 um 16:25 Uhr erkannt worden.“.

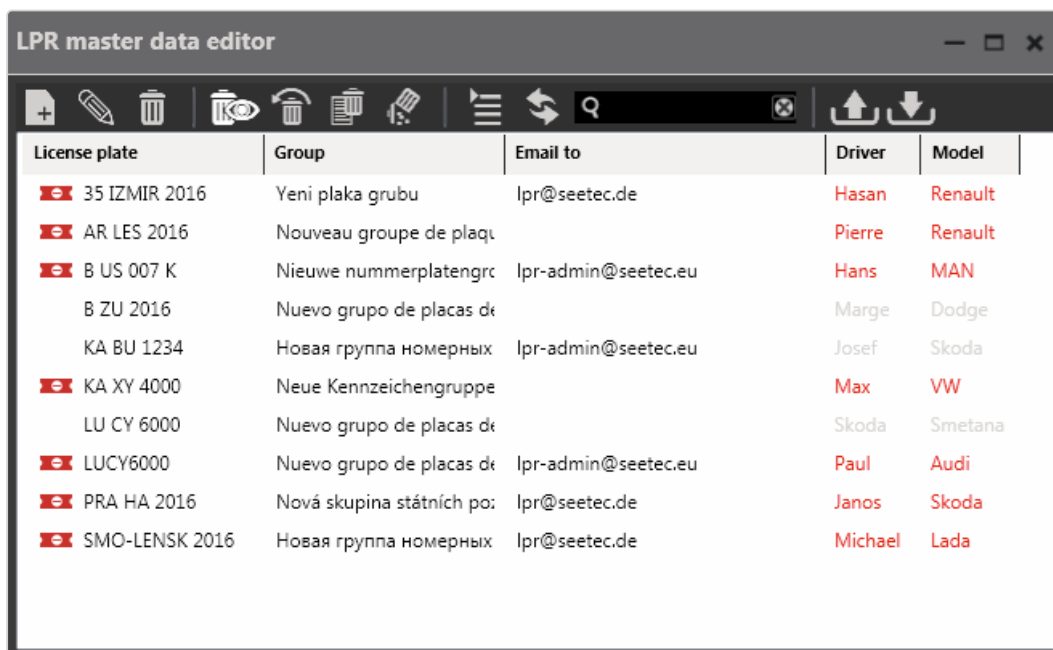
Kennzeichen löschen

Kennzeichen können aus der Liste der gültigen Kennzeichen entfernt werden.

Wenn Kennzeichen aus der Liste entfernt werden, verlieren sie ihre Gültigkeit, werden aber nicht aus der Datenbank entfernt. Gelöschte Kennzeichen können daher wiederhergestellt werden.

1. Wählen Sie ein Kennzeichen in der Liste des Stammdateneditors aus.
2. Wählen Sie **Löschen** , um das gewählte Kennzeichen aus der Liste zu entfernen. Das Kennzeichen wird ausgeblendet.

Gelöschte Kennzeichen anzeigen und wiederherstellen













License plate	Group	Email to	Driver	Model
 35 IZMIR 2016	Yeni plaka grubu	lpr@seetec.de	Hasan	Renault
 AR LES 2016	Nouveau groupe de plaq		Pierre	Renault
 B US 007 K	Nieuwe nummerplategrc	lpr-admin@seetec.eu	Hans	MAN
B ZU 2016	Nuevo grupo de placas de		Marge	Dodge
KA BU 1234	Новая группа номерных	lpr-admin@seetec.eu	Josef	Skoda
 KA XY 4000	Neue Kennzeichengruppe		Max	VW
LU CY 6000	Nuevo grupo de placas de		Skoda	Smetana
 LUCY6000	Nuevo grupo de placas de	lpr-admin@seetec.eu	Paul	Audi
 PRA HA 2016	Nová skupina státních po:	lpr@seetec.de	Janos	Skoda
 SMO-LENSK 2016	Новая группа номерных	lpr@seetec.de	Michael	Lada

Abb. 39: Gelöschte Kennzeichen anzeigen und wiederherstellen

1. Wählen Sie **Gelöschte Einträge anzeigen** , um die Liste einschließlich der gelöschten (d. h. ausgeblendeten) Kennzeichen anzuzeigen.
2. Wählen Sie das gelöschte Kennzeichen aus (angezeigt mit grauem Text) und wählen Sie **Wiederherstellen** . Das Kennzeichen wird wieder in der Kennzeichenliste angezeigt.

Historie löschen


Bei Bedarf können Sie die Historie eines Kennzeichens löschen.

1. Markieren Sie das Kennzeichen, dessen Historie Sie löschen möchten, und klicken Sie auf **Historie löschen** .
2. Bestätigen Sie den Löschvorgang mit **Ja**.


Kennzeichen endgültig löschen

Um Kennzeichen aus der Datenbank zu entfernen, müssen sie zunächst gelöscht (d. h. aus der Liste entfernt) werden.


Kennzeichen können nur von Mitgliedern der Administratorgruppe endgültig gelöscht werden (siehe „Administrative Rechte und Benutzerrechte“ auf Seite 24).

1. Wählen Sie das Kennzeichen aus, das endgültig gelöscht werden soll. Um mehrere Kennzeichen zu löschen, wählen Sie die Kennzeichen mit gedrückter STRG-Taste aus.
2. Wählen Sie **Permanent löschen**  und bestätigen Sie den Löschvorgang. Die Kennzeichen werden endgültig gelöscht.

Ansicht aktualisieren

1. Klicken Sie auf **Ansicht aktualisieren** , um gegebenenfalls ausgeblendete Kennzeichen in der Liste anzuzeigen.

Kennzeichen suchen

1. Um ein Kennzeichen in der Liste zu suchen, geben Sie einen Teil des Stammdatensatzes des Kennzeichens in die **Suche**  ein. Die Suche wird automatisch gestartet und das Ergebnis in der Liste angezeigt.
2. Um die Suche aufzuheben und ungefilterte Ergebnisse anzuzeigen, klicken Sie in der Suche auf das **X**.

3. Wenn die konfigurierte maximale Anzahl an Suchergebnissen überschritten wird, kann das Ergebnis als CSV-Datei exportiert werden.


Kennzeichen-Stammdaten exportieren

Die Stammdaten ausgewählter Kennzeichen können als CSV-Datei (eine Textdatei mit durch Semikolon getrennten Werten) exportiert werden, um sie auszuwerten oder für den weiteren Import in Datenbanken vorzubereiten.

1. Wählen Sie das Kennzeichen aus, dessen Stammdaten Sie exportieren möchten. Um mehrere Kennzeichen zu exportieren, wählen Sie die Kennzeichen mit gedrückter STRG-Taste aus.
2. Wählen Sie **Exportieren** , um die Stammdaten als CSV-Datei zu exportieren (siehe „[Datenfelder für den Export und Import](#)“ auf der [gegenüberliegenden Seite](#)).


Kennzeichen-Stammdaten importieren

Die Stammdaten von Kennzeichen können aus einer CSV-Datei (eine Textdatei mit durch Semikolon getrennten Werten) importiert werden.

1. Wählen Sie **Importieren**  und wählen Sie eine CSV-Datei mit den zu importierenden Kennzeichen-Stammdaten aus (siehe „[Datenfelder für den Export und Import](#)“ auf der [gegenüberliegenden Seite](#)).

Kennzeichengruppen anzeigen

In der Liste können die Kennzeichen nach Kennzeichengruppen sortiert angezeigt werden.

1. Klicken Sie auf **Ansicht wechseln** , um Kennzeichen gruppiert oder ungruppiert anzuzeigen.
2. Klicken Sie auf den Pfeil neben dem Namen der Kennzeichengruppe, um diese einzuklappen.
3. Klicken Sie erneut auf den Pfeil, um die Kennzeichengruppe wieder aufzuklappen.

Datenfelder für den Export und Import

Die Export- und Importdatei muss folgende Datenfelder enthalten:

```
LicencePlate;reserved;Group;
...;AlwaysValid;ValidFrom;ValidTill;
Email;EmailText;ValidityName;modify
```

Feldname	Wert	Hinweis
LicensePlate		Das Kennzeichen
reserved		
Group	Text	Name der konfigurierten Kennzeichengruppe (siehe „ Kennzeichengruppen “ auf Seite 432) Wenn es keinen Eintrag gibt, wird dieser als „unknown“ (unbekannt) definiert.
;;;;;	Text	Platzhalter für benutzerdefinierte Stammdatenfelder (siehe „ Globale OCR-Einstellungen konfigurieren “ auf Seite 444)
ValidFrom	Datum-Zeit-Wert	Datum/Zeit als Unix-Datum-Zeit-Wert (seit 1970 Millisekunden)
ValidTill	Datum-Zeit-Wert	Datum/Zeit als Unix-Datum-Zeit-Wert (seit 1970 Millisekunden)
AlwaysValid	1	„immer gültig“ (Werte in den Feldern ValidFrom und ValidTill gleich)
	0	Werte in den Feldern ValidFrom und ValidTill unterschiedlich

Feldname	Wert	Hinweis
ValidityName	negativer Wert, z. B. -1	Immer
	positiver Wert	ID der zugehörigen Zeit- schablone
Modify	<ul style="list-style-type: none"> ▪ „0“: Modifizieren Sie die vorhandenen Kennzeicheninformationen wie Gruppe, spezifische Felder usw. ▪ „1“: Fügen Sie ein neues Kennzeichen in die Datenbank ein. ▪ „-1“: Entfernt die ausgewählten Kennzeicheninformationen vom Editor, aber löscht nicht die Position in der Datenbank. 	Wertänderung ist möglich (siehe „ Kennzeichen-Stammdaten importieren “ auf Seite 102).

Beispiel

```
LicencePlate;reserved;Group;
;;;;;;;;;;AlwaysValid;ValidFrom;ValidTill;
Email;EmailText;TimePattern;modify
```

```
QV MS 8285;;Unbekannt;;;;;;;;;;1;1/9/2023 2:55:30 PM;1/9/2023 2:55:30
PM;;;-1;0
```

```
QV MS 8286;;Testen;;;;;;;;;;1;1/9/2023 2:55:30 PM;1/9/2023 2:55:30 PM;;;-
1;1
```

```
QV MS 8287;;Testen;;;;;;;;;;1;1/9/2023 2:55:30 PM;1/9/2023 2:55:30 PM;;;-1;-
1
```

Tools

In diesem Menü werden folgende Optionen angezeigt:

- Mehrfachexport von Bilddaten (siehe „[Mehrfachexport von Bilddaten](#)“ auf [Seite 114](#))
- Schreibschutz von Aufzeichnungen (siehe „[Schreibschutz von Aufzeichnungen mehrerer Kameras entfernen](#)“ auf [Seite 121](#))
- Logoaktion konfigurieren (siehe „[Logoaktion konfigurieren](#)“ auf [Seite 122](#))
- Statusbericht für automatischen Bildexport (siehe „[Statusbericht für automatischen Bildexport](#)“ auf [Seite 123](#))
- Manueller Referenzbildvergleich (siehe „[Manueller Referenzbildvergleich](#)“ auf [Seite 124](#))

Der Export Designer

Der Export Designer in Qognify VMS dient zum Konfigurieren des Bildexports. Damit lassen sich Formen hinzufügen, um bestimmte Bereiche der exportierten Bilder auszublenken und so einen besseren Datenschutz zu bieten. Außerdem kann ein Zeitbereich definiert werden.

Neuen Export erstellen

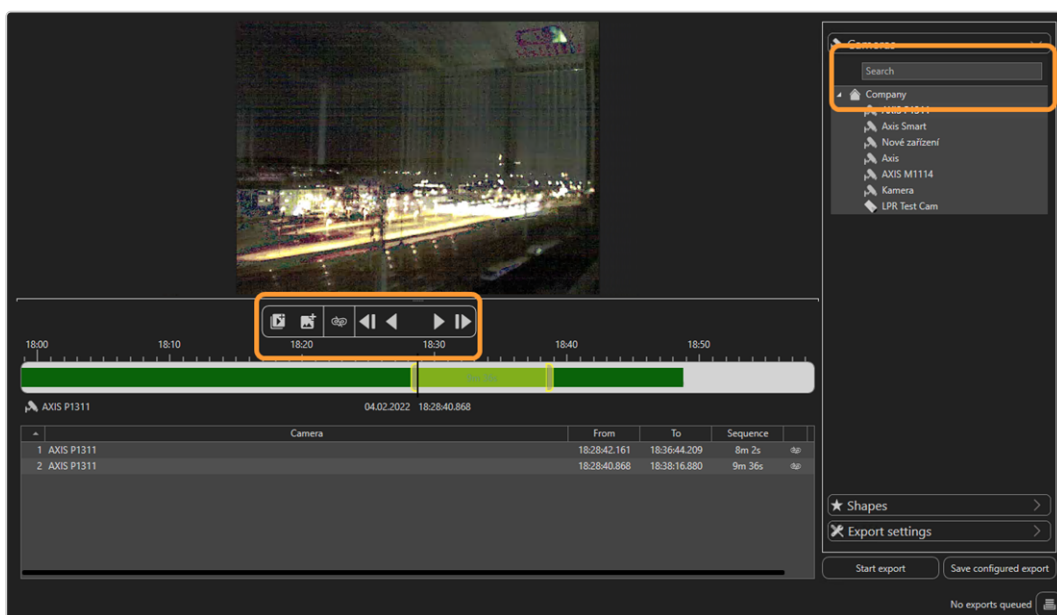


Abb. 40: Der Export Designer



Bild oder Bildsequenz definieren

1. Wählen Sie im Export Designer **Neu erstellen** im Menü **Extras**.
2. Wählen Sie aus der Liste eine Kamera aus oder suchen Sie mit dem Suchfeld oberhalb der Liste nach einer Kamera.
3. Verschieben Sie die Zeitleiste an die gewünschte Position. Das entsprechende Bild wird angezeigt. Vergrößern oder verkleinern Sie die Zeitleiste mit dem Mausrad, um mehr Details anzuzeigen.
4. Wählen Sie **Sequenz hinzufügen** , um den Startpunkt einer Bildsequenz einzustellen.
5. Ziehen Sie den Ziehpunkt der Begrenzungslinie der Sequenz nach rechts. Damit wird der Zeitbereich für den Export festgelegt.
6. Um nur ein einziges Bild für den Export zu kennzeichnen, wählen Sie **Einzelnes Bild hinzufügen**  und ziehen Sie den Marker zur Position auf der Zeitleiste.

Anzeigen von Privacy-Masks

Um festzustellen, ob Privacy-Masks in einem Bild verwendet werden, kann eine Privacy-Mask vor dem Export im Vorschaufenster markiert werden.

Ohne Berechtigung zum Ausblenden von Privacy-Masks (oder im Offline-Modus) ist die Schaltfläche deaktiviert und Privacy-Masks werden immer angezeigt und exportiert.

1. Um eine Privacy-Mask im Bild zu markieren, wählen Sie im Menü **Extras** die Option **Mask** . Alle Privacy-Masks des aktuellen Bildes im Vorschaufenster werden angezeigt.
2. Bevor Sie eine Datei mit deaktivierter oder aktivierter Privacy-Mask exportieren, schalten Sie die **Mask**  für eine ausgewählte Kamera in der Liste ein oder aus (zum Exportieren siehe „[Exporteinstellungen definieren](#)“ auf Seite 108).

Formen hinzufügen

Bereiche des Bilds oder der Bildsequenz können im Export ausgeblendet werden, um zu verhindern, dass Informationen im Exportergebnis angezeigt werden, wie etwa Kennzeichen oder sensible Objekte.

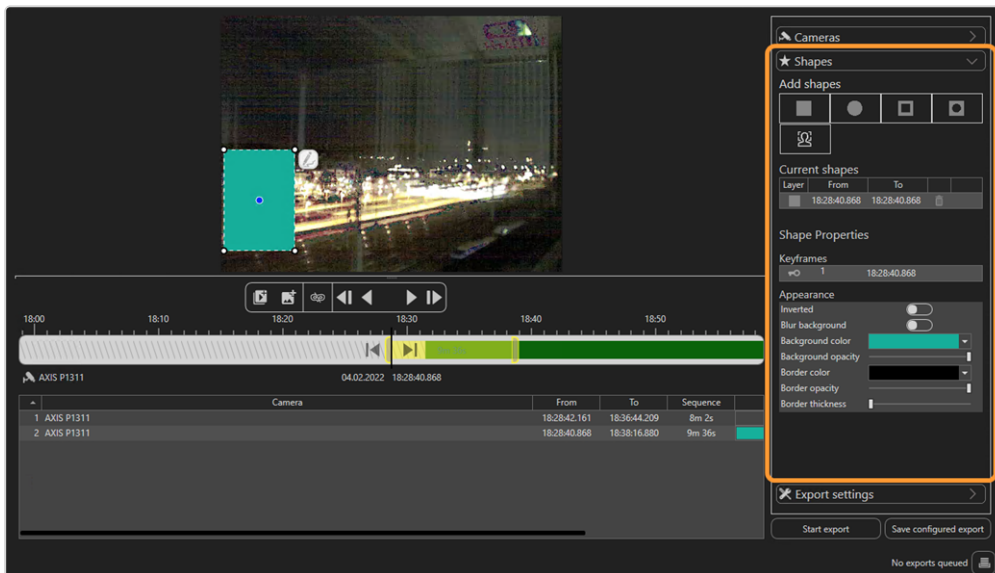




Abb. 41: Hinzufügen von Formen im Exportdesigner

1. Um eine Form hinzuzufügen, öffnen Sie in der Symbolleiste rechts das Aufklappmenü **Formen** und wählen Sie eine Form aus. Die ausgewählte Form wird in der linken oberen Ecke platziert.
2. Ziehen Sie die Form auf das Bild oder die Sequenz und passen Sie ihre Größe an.
3. Legen Sie die Farbe und Transparenz des Hintergrunds sowie die Farbe und Transparenz des Rahmens fest.
4. Verschieben Sie das Formsymbol auf der Zeitleiste, um das zu maschierende Objekt im Zeitbereich zu definieren.
5. Um eine Form aus dem Bild zu löschen, wählen Sie **Löschen**  neben der Form in der Liste der „Aktuellen Formen“.
6. Um einen Keyframe zu löschen, wählen Sie **Keyframe löschen** neben dem Keyframe in der Liste der „Keyframes“.

Hinzufügen einer Maske mit „Click2Mask“

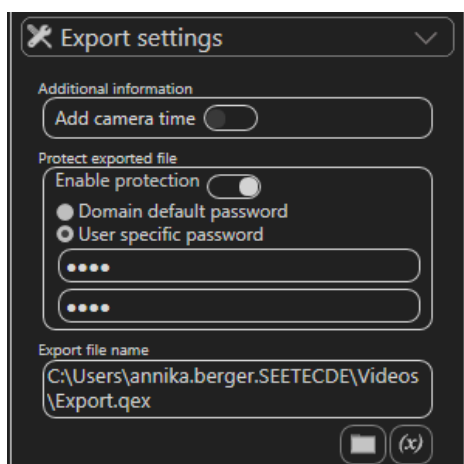
Um den Schutz der Privatsphäre zu bestätigen, können Personen in einer Szene vor dem Export automatisch maskiert werden. Diese Funktion wird „Click2Mask“ genannt.

Um „Click2Mask“ zu verwenden, muss das BVI-Servermodul installiert sein. Diese Funktion erfordert den 64bit-Modus und kann nicht mit dem Paket Qognify VMS S50 verwendet werden.

1. Um eine Maske hinzuzufügen, wählen Sie eine Kamera und fügen eine Bildsequenz hinzu.
2. Öffnen Sie **Formen** in der Symbolleiste auf der rechten Seite und wählen Sie **Analysieren** . Qognify VMS analysiert die Sequenz für eine Person. Die resultierende Sequenz wird im Abschnitt „Keyframes“ angezeigt.
3. Passen Sie bei Bedarf die Form an.

Exporteinstellungen definieren

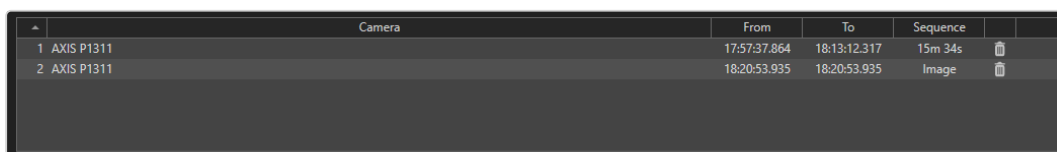
1. Um die Exporteinstellungen, z. B. einen Passwortschutz, zu definieren, öffnen Sie in der Symbolleiste rechts das Aufklappmenü **Exporteinstellungen**.



2. Aktivieren Sie die Anzeige der Kamerazeit als zusätzliche Information im Bild.

3. Aktivieren Sie bei Bedarf den Passwortschutz und legen Sie entweder ein Standardpasswort für den Geschäftsbereich oder ein benutzerspezifisches Passwort fest.
4. Klicken Sie auf das Ordnersymbol und wählen Sie den Speicherort für den Export der Datei aus.
5. Wenn Sie dem Namen der Exportdatei eine Variable hinzufügen möchten, klicken Sie auf **(x)** und wählen Sie die Variable aus. Sie können Variablen einfügen, die beim Export im Dateinamen angegeben werden sollen, z. B.:
 - Variable für Kameranamen einfügen: Im exportierten Dateinamen wird der Name der ausgewählten Kamera angegeben.
 - Variable für Exportzeit einfügen: Der Zeitpunkt des Exports wird im Dateinamen automatisch angegeben. Er kann als Zeitstempel, Datum, Tag, Uhrzeit usw. definiert werden.
 - GUID: Im Dateinamen wird der globale eindeutige Bezeichner (Global Unique Identifier) der Datei angegeben.
6. Speichern Sie die Exporteinstellungen.
7. Wählen Sie **Exportieren** aus.
8. Öffnen Sie die Exportverwaltung, um die exportierte Datei zu öffnen.

Bildexport fortsetzen



	Camera	From	To	Sequence	
1	AXIS P1311	17:57:37.864	18:13:12.317	15m 34s	🗑️
2	AXIS P1311	18:20:53.935	18:20:53.935	Image	🗑️

Export fortsetzen

Exporte werden im Export Designer in eine Warteschlange eingereiht. Bei einem Ausfall können die Exporteinstellungen wiederhergestellt werden. Die Einstellungsdatei, die zuvor im Export Designer konfiguriert wurde, wird erneut in die Exportwarteschlange geladen.


1. Wählen Sie im Export Designer **Fortsetzen** im Menü **Extras**.
2. Optional können Sie die Exporteinstellungen neu konfigurieren.
3. Starten Sie den Export.
4. Öffnen Sie die Exportverwaltung, um die exportierte Datei zu öffnen oder zu löschen.

Datei für den Export laden

Alle konfigurierten und gespeicherten Einstellungen können ohne Neukonfiguration in den Export Designer geladen werden. Die Einstellungen ersetzen die aktuelle Konfiguration in der Warteschlange.

1. Wählen Sie im Export Designer **Laden** im Menü **Extras**.
2. Optional können Sie die Exporteinstellungen neu konfigurieren.
3. Starten Sie den Export.

Marker löschen

1. Um einen Marker aus der Datei zu löschen, wählen Sie in der Zeile des entsprechenden Elements **Löschen** .

Eine Kamera freigeben

Außer einem Benutzer mit Administratorrechten kann jeder Benutzer eine Kamera freigeben, wenn die Benutzerrechte festgelegt sind (siehe „[Benutzerrechte verwalten](#)“ auf [Seite 361](#)).

Wenn eine freigegebene oder empfangende Partei gelöscht oder deaktiviert wird oder während der Freigabe von Kameras die Freigabe- oder Live-Ansichtsrechte verliert, wird die Freigabe beendet.

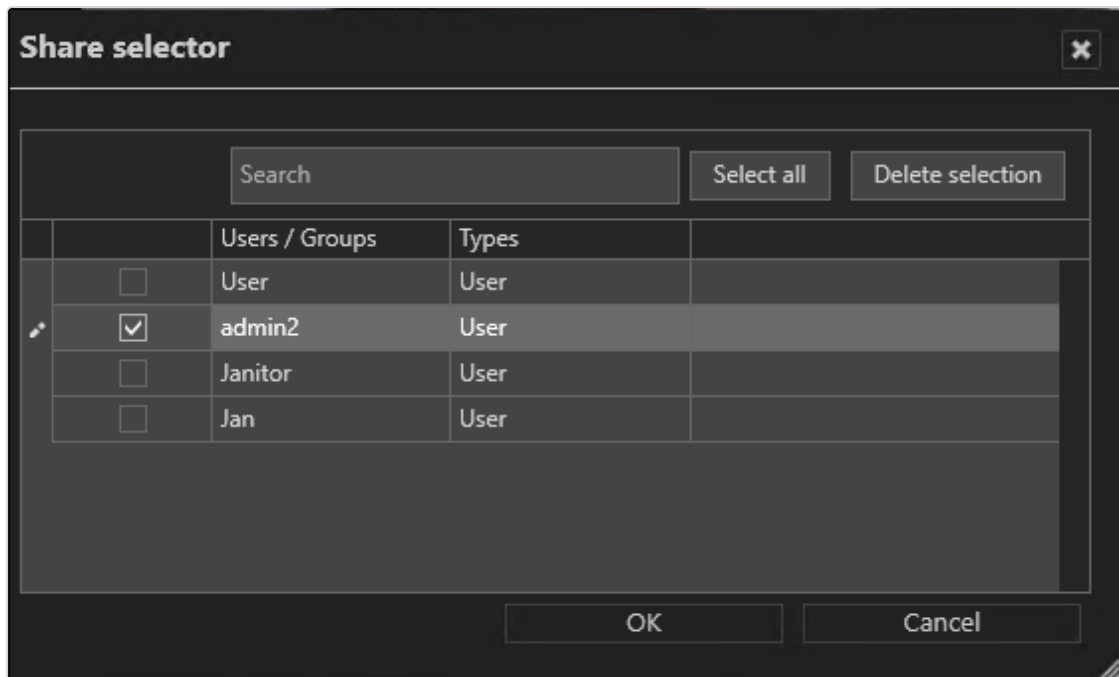


Abb. 42: Eine Kamera freigeben

Starten Sie die gemeinsame Nutzung einer Kamera

1. Öffnen Sie die Kamera im Arbeitsbereich im Überwachungs-Modus.
2. Wählen Sie **Manager freigeben > Freigabe starten** vom Menü **Extras** aus.
3. Wählen Sie den Benutzer oder die Gruppe.
4. Bestätigen Sie mit **OK**.

Beenden Sie die gemeinsame Nutzung einer Kamera

1. Öffnen Sie die Kamera im Arbeitsbereich im Überwachungs-Modus.
2. Wählen Sie **Manager freigeben > Freigabe beenden** vom Menü **Extras** aus.

Einschränkungsmanager

Der Zugriff für einen Benutzer oder eine Gruppe auf Kameras mit dem „Einschränkungsmanager“ vorübergehend eingeschränkt werden. Dies kann erforderlich sein, um den Zugang für Benutzer oder Gruppen zu begrenzen, die normalerweise Bilder ansehen dürfen, indem der Zugang zu Bilddaten, die vertrauliche private Daten (z. B. Unfälle) enthalten, für einen bestimmten Zeitraum beschränkt wird.

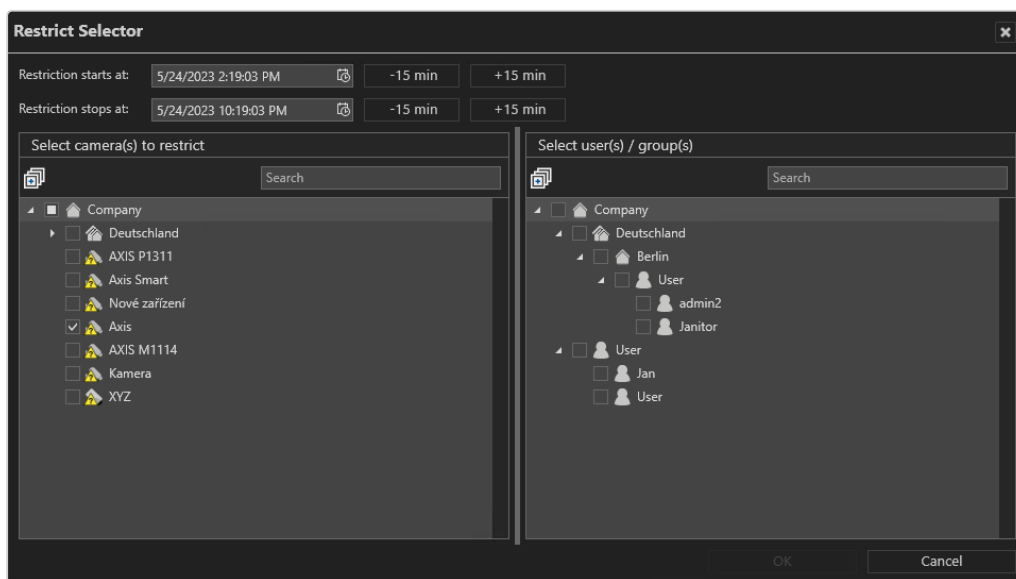
Die Beschränkung der Ansicht von Bilddaten für andere Benutzer erfordert die entsprechenden Erlaubnisse (siehe [„Benutzerrechte verwalten“ auf Seite 361](#)).

Bekannte Einschränkungen

- Wenn ein Benutzer oder eine Gruppe, der/die andere Benutzer oder Gruppen beschränkt, gelöscht wird, bleibt die Beschränkung erhalten.
- Wenn ein Benutzer oder eine Gruppe, der/die andere Benutzer oder Gruppen beschränkt, deaktiviert wird, bleibt die Beschränkung erhalten.
- Wenn ein Benutzer über Erlaubnisse von mehreren Gruppen verfügt und eine Gruppe beschränkt ist, wird auch der Benutzer eingeschränkt.
- Ein Administrator kann beschränkt werden, kann seine Beschränkung aber aufheben.
- Die Beschränkung hat Vorrang vor einer Freigabe, d. h. ein beschränktes Bild kann nicht angezeigt werden, wenn es für den Benutzer oder die Gruppe beschränkt ist.
- Ein Benutzer oder eine Gruppe kann sich selbst beschränken.
- Wenn ein Benutzer berechtigt ist, eine Kamera zu konfigurieren, aber beschränkt ist, kann der Benutzer die Kamera zwar konfigurieren, aber kein Video ansehen.

Beschränkung einer Kamera

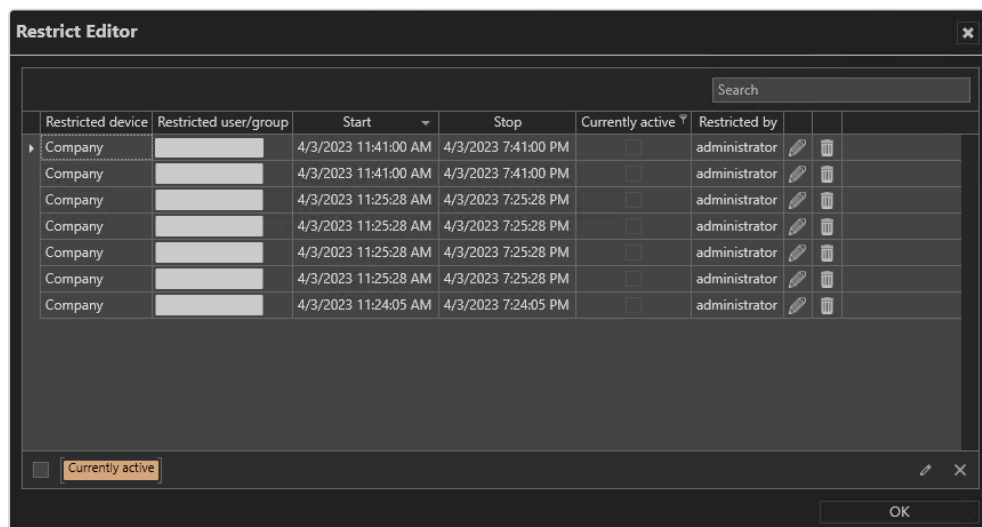
1. Wählen Sie im Überwachungsmodus **Manager beschränken > Beschränkung starten** vom Menü **Extras** aus. Alle Kameras in der aktiven Ansicht sind vorab ausgewählt.




2. Definieren Sie die Start- und Stoppzeit der Beschränkung.
 - Wenn das Zeitintervall in der Vergangenheit liegt, kann der Benutzer im Überwachungsmodus weiterhin auf das Video zugreifen, es jedoch nicht im Archivmodus ansehen.
 - Wenn das Zeitintervall in der Zukunft liegt, sieht der Benutzer das Video im Überwachungs- oder Archivmodus nicht.
3. Legen Sie bei Bedarf das Beschränkungsintervall vor und nach dem Beschränkungszeitraum fest.
4. Wählen Sie eine oder mehrere Kameras zur Beschränkung aus.
5. Wählen Sie die Benutzer aus, denen der Zugriff verweigert werden soll.
6. Wählen Sie **OK**.

Bearbeitung von Beschränkungen

1. Wählen Sie **Manager beschränken > Beschränkungen bearbeiten** vom Menü **Extras**.



2. Wählen Sie **Derzeit aktiv**, um nur die derzeit aktiven Beschränkungen anzuzeigen.
3. Wählen Sie die Beschränkung und wählen Sie **Bearbeiten** .
4. Definieren Sie die Start- und Endzeiten der Beschränkung und klicken Sie auf **OK**.

Mehrfachexport von Bilddaten

Bilddaten können mit zwei unterschiedlichen Verfahren exportiert werden:

- Verwendung von „Mehrfachexport von Bilddaten“ im Überwachungsmodus.
- Exportieren von Videos aus den geöffneten Kacheln im Archivmodus (siehe „[Aufzeichnungen exportieren](#)“ auf Seite 186).

Beim Export von Videoaufzeichnungen werden die exportierten Daten verschlüsselt abgelegt und können dann durch den Qognify Viewer auf einem PC ohne eigene Qognify-Installation abgespielt werden. Der **Qognify Viewer** befindet sich im Exportverzeichnis.

Die Setup-Dateien für den **Qognify Viewer** und das Programm zum Brennen des exportierten Videomaterials auf ein Speichermedium befinden sich ebenfalls im Verzeichnis „Tools“ der Qognify-Installation (siehe „[Anywhere Viewer](#)“ auf Seite 539).

Während des Exportvorgangs wird die Installationsdatei des Qognify Viewers ebenfalls in den Exportordner kopiert. Dadurch können die Dateien nur mit dem installierten Qognify Viewer auf einem PC ohne Qognify VMS-Installation abgespielt werden. Der Qognify Viewer importiert die Dateien und zeigt sie als separate Zeitintervalle an.

1. Wählen Sie **Mehrfachexport von Bilddaten** im Menü **Extras**.
2. Wählen Sie eine der folgenden Optionen.

AVI-Export zum Client

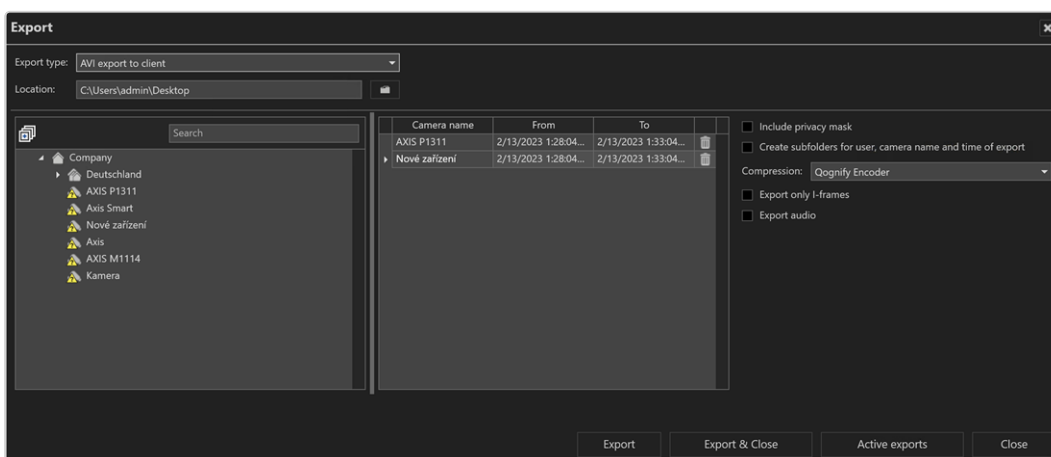




Abb. 43: AVI-Export der Bilddaten

1. Stellen Sie sicher, dass für den Bilddatenexport auf den Client ein temporäres Verzeichnis konfiguriert und verfügbar ist (siehe „[Video-Backup](#)“ auf [Seite 442](#)).
2. Um die Liste zu öffnen oder zu schließen, wählen Sie **Alle erweitern/zusammenklappen** .
3. Ziehen Sie die zu exportierenden Kameras per Drag & Drop in die rechte Spalte. Alle markierten Zeitspannen werden für jede Kamera angezeigt.
4. Um eine Zeitspanne zu löschen, wählen Sie in der entsprechenden Reihe die Option **Markierte Elemente löschen** .
5. Geben Sie an, ob die Bilddaten mit oder ohne **Privacy-Masks** exportiert werden sollen.

Falls Sie den Export ohne Privacy-Masks durchführen, kann dies zu einem Verstoß gegen die Datenschutzgesetze führen.

6. Um die exportierten Bilddaten nach Benutzer, Kameraname und Exportzeitpunkt in entsprechenden Ordnern abzulegen, aktivieren Sie **Unterordner für Benutzer, Kameraname und Zeitpunkt für Export anlegen**.
7. Wählen Sie das Videokomprimierungsformat:
 - Qognify Encoder
 - DV Video Encoder
 - MJPEG Compressor
 - Quellformat
8. Geben Sie an, ob **nur I-Frames** exportiert werden sollen.
9. Aktivieren Sie **Audio**, wenn die Videoquelle Audiokanäle enthält, die in den Export einbezogen werden sollen.
10. Um den Export sofort durchzuführen, klicken Sie auf **Exportieren**. Die Einstellungen werden nach dem Export oder beim Schließen des Fensters gespeichert.

Der Dateiname der AVI-Datei hat folgendes Format:
<Kameraname>_<abDatum>-<abZeit>_<bisDatum>-<bisZeit>.avi
Der Name kann nicht geändert werden. Sollte der Name bereits existieren, wird automatisch eine fortlaufende Nummer angehängt.

JPEG-Export zum Client

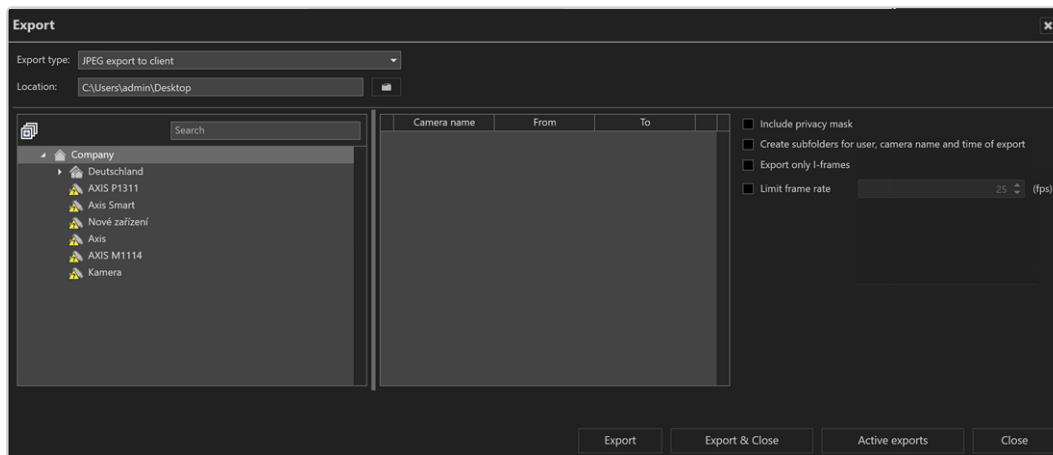




Abb. 44: JPEG-Export der Bilddaten

1. Stellen Sie sicher, dass für den Bilddatenexport auf den Client ein temporäres Verzeichnis konfiguriert und verfügbar ist (siehe „[Video-Backup](#)“ auf [Seite 442](#)).
2. Um die Liste zu öffnen oder zu schließen, wählen Sie **Alle erweitern/zusammenklappen** .
3. Ziehen Sie die zu exportierenden Kameras per Drag & Drop in die rechte Spalte. Alle markierten Zeitspannen werden für jede Kamera angezeigt.
4. Um eine Zeitspanne zu löschen, wählen Sie in der entsprechenden Reihe die Option **Markierte Elemente löschen** .
5. Geben Sie an, ob die Bilddaten mit oder ohne **Privacy-Masks** exportiert werden sollen.

Falls Sie den Export ohne Privacy-Masks durchführen, kann dies zu einem Verstoß gegen die Datenschutzgesetze führen.

6. Um die exportierten Bilddaten nach Benutzer, Kameraname und Exportzeitpunkt in entsprechenden Ordnern abzulegen, aktivieren Sie **Unterordner für Benutzer, Kameraname und Zeitpunkt für Export anlegen**.
7. Geben Sie an, ob **nur I-Frames** exportiert werden sollen.
8. Um die Anzahl der exportierten Bilder festzulegen, aktivieren Sie die Option **Bildrate begrenzen** und geben Sie die Anzahl der Bilder pro Sekunde des Video Streams an (Standard ist 25 fps).

- Um den Export sofort durchzuführen, klicken Sie auf **Exportieren**. Die Einstellungen werden nach dem Export oder beim Schließen des Fensters gespeichert.

Export von nativen Daten zum Client

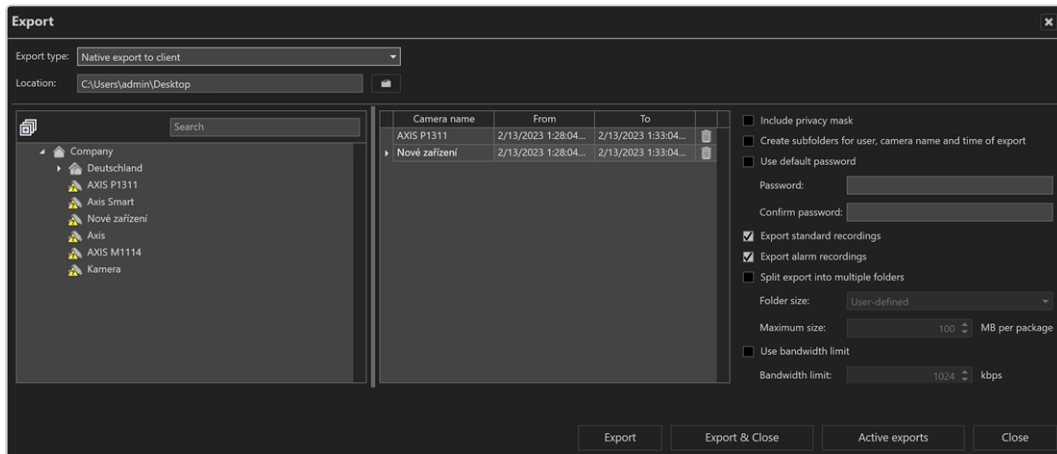




Abb. 45: Export von nativen Bilddaten zum Client

- Stellen Sie sicher, dass für den Bilddatenexport auf den Client ein temporäres Verzeichnis konfiguriert und verfügbar ist (siehe „[Video-Backup](#)“ auf [Seite 442](#)).

Während des Exports werden die vom Failover-Server exportierten Bilddaten an den Produktionsserver übertragen. Vergewissern Sie sich, dass der Produktionsserver über ausreichend Speicherkapazität verfügt.

- Um die Liste zu öffnen oder zu schließen, wählen Sie **Alle erweitern/zusammenklappen** .
- Ziehen Sie die zu exportierenden Kameras per Drag & Drop in die rechte Spalte. Alle markierten Zeitspannen werden für jede Kamera angezeigt.
- Um eine Zeitspanne zu löschen, wählen Sie in der entsprechenden Reihe die Option **Markierte Elemente löschen** .

5. Geben Sie an, ob die Bilddaten mit oder ohne **Privacy-Masks** exportiert werden sollen.

Falls Sie den Export ohne Privacy-Masks durchführen, kann dies zu einem Verstoß gegen die Datenschutzgesetze führen.

6. Um die exportierten Bilddaten nach Benutzer, Kameraname und Exportzeitpunkt in entsprechenden Ordnern abzulegen, aktivieren Sie **Unterordner für Benutzer, Kameraname und Zeitpunkt für Export anlegen**.
7. Um die exportierten Bilddaten mit dem vorgegebenen Standard-Passwort zu sichern, aktivieren Sie **Standard-Passwort verwenden**.

Diese Option ist deaktiviert, wenn die Verwendung des Standardpassworts in den Profileinstellungen im Konfigurationsmodus durchgesetzt wird.

8. Falls Sie statt des Standard-Passworts ein eigenes **Passwort** verwenden möchten, geben Sie dieses an und wiederholen Sie es. Das Standard-Passwort wird im Konfigurationsmodus im Bereich „Device Manager (DM)“ eingerichtet (siehe „[Video-Backup](#)“ auf Seite 442).
9. Geben Sie an, ob nur Standardaufzeichnungen oder auch **Alarmaufzeichnungen** exportiert werden sollen.
10. Um die exportierten Bilddaten aufgrund der zu erwartenden Dateigröße in Verzeichnisse annähernd gleicher Größe abzulegen, aktivieren Sie **Export in mehrere Verzeichnisse aufteilen** und legen Sie die **Verzeichnisgröße** und die **maximale Größe** der Bilddatei fest. Bilddaten, die die festgelegte Größe überschreiten, werden in mehrere Dateien aufgeteilt, um sie auf Datenträger wie CD-ROM oder DVD ablegen zu können.
11. Falls die Bilddaten auf einen Client exportiert werden sollen, der nur schmalbandig angebunden ist, aktivieren Sie **Bandbreitenbegrenzung verwenden** und legen Sie die Bandbreitenbegrenzung fest.
12. Um den Export sofort durchzuführen, klicken Sie auf **Exportieren**. Die Einstellungen werden nach dem Export oder beim Schließen des Fensters gespeichert.

Exportieren nativer Bilddaten auf den Server

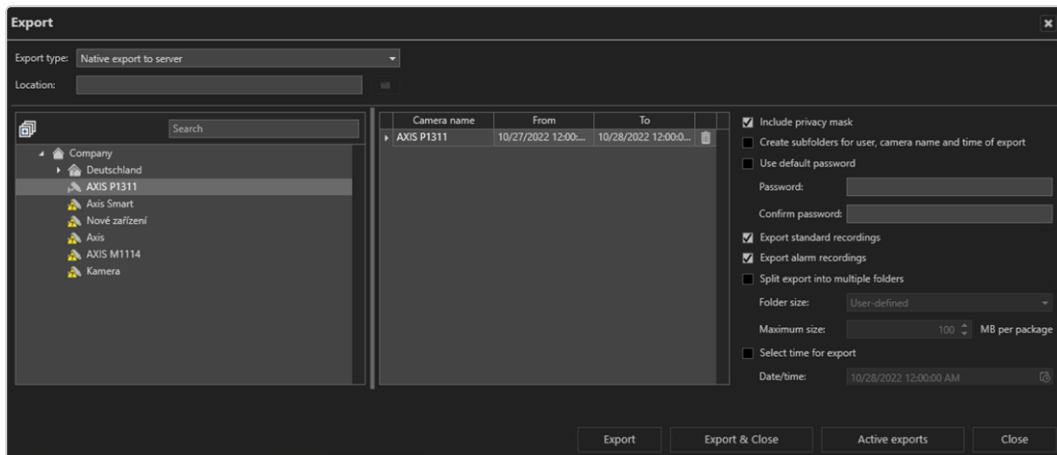




Abb. 46: Exportieren nativer Bilddaten auf den Server

1. Stellen Sie sicher, dass für den Bilddatenexport auf den Server ein temporäres Verzeichnis konfiguriert und verfügbar ist (siehe „[Video-Backup](#)“ auf [Seite 442](#)).

Während des Exports werden die vom Failover-Server exportierten Bilddaten an den Produktionsserver übertragen. Vergewissern Sie sich, dass der Produktionsserver über ausreichend Speicherkapazität verfügt.

2. Um die Liste zu öffnen oder zu schließen, wählen Sie **Alle erweitern/zusammenklappen** .
3. Ziehen Sie die zu exportierenden Kameras per Drag & Drop in die rechte Spalte. Alle markierten Zeitspannen werden für jede Kamera angezeigt.
4. Um eine Zeitspanne zu löschen, wählen Sie in der entsprechenden Reihe die Option **Markierte Elemente löschen** .
5. Geben Sie an, ob die Bilddaten mit oder ohne **Privacy-Masks** exportiert werden sollen.

Falls Sie den Export ohne Privacy-Masks durchführen, kann dies zu einem Verstoß gegen die Datenschutzgesetze führen.

6. Um die exportierten Bilddaten nach Benutzer, Kameraname und Exportzeitpunkt in entsprechenden Ordnern abzulegen, aktivieren Sie **Unterordner für Benutzer, Kameraname und Zeitpunkt für Export anlegen**.

7. Um die exportierten Bilddaten mit dem vorgegebenen Standard-Passwort zu sichern, aktivieren Sie **Standard-Passwort verwenden**.
8. Falls Sie statt des Standard-Passworts ein eigenes **Password** verwenden möchten, geben Sie dieses an und wiederholen Sie es. Optional können Sie das Standard-Passwort verwenden. Das Standard-Passwort wird im Konfigurationsmodus im Bereich „Device Manager (DM)“ eingerichtet (siehe [„Video-Backup“ auf Seite 442](#)).
9. Legen Sie fest, ob nur **Standardaufzeichnungen** exportiert werden sollen oder ebenso **Alarmaufzeichnungen**.
10. Um die exportierten Dateien zur Speicherung auf mehreren Datenträgern wie CD-ROMs oder DVDs aufzuteilen, wählen Sie **Export in mehrere Verzeichnisse aufteilen**.

Die Mindestgröße der Datei beträgt 100 MB.

11. Wählen Sie die gewünschte **Verzeichnisgröße** entsprechend dem Exportmedium (z. B. CD, DVD, Blue-Ray Disk).
12. Legen Sie die **maximale Größe** der Bilddatei fest.
13. Um den Export zu einem bestimmten Zeitpunkt durchzuführen, aktivieren Sie **Zeitpunkt für Export wählen** und legen Sie Datum und Uhrzeit für den Export fest.
14. Geben Sie das **Datum/die Zeitspanne** für die zu exportierenden Bilddaten an.
15. Klicken Sie auf **Auswählen** und geben Sie den **Speicherort** der exportierten Bilddaten an.

Während des Exports werden die vom Failover-Server exportierten Bilddaten an den Produktionsserver übertragen. Vergewissern Sie sich, dass der Produktionsserver über ausreichend Speicherkapazität verfügt.

16. Um den Export sofort durchzuführen, klicken Sie auf **Exportieren**. Die Einstellungen werden nach dem Export oder beim Schließen des Fensters gespeichert.

Exportierte Dateien anzeigen

- Um die exportierten Dateien zu betrachten, verwenden Sie bitte den „VMS_PortableViewer“. Mit dem Viewer können die exportierten Dateien ohne Änderung und ohne Installation von Qognify VMS geöffnet und angezeigt werden.
- Alternativ können Sie den Offline-Modus des Qognify VMS-Clients verwenden.

Schreibschutz von Aufzeichnungen mehrerer Kameras entfernen

Der Schreibschutz von aufgezeichneten Bilddaten kann entfernt werden (siehe „Schreibschutz“ auf Seite 189).

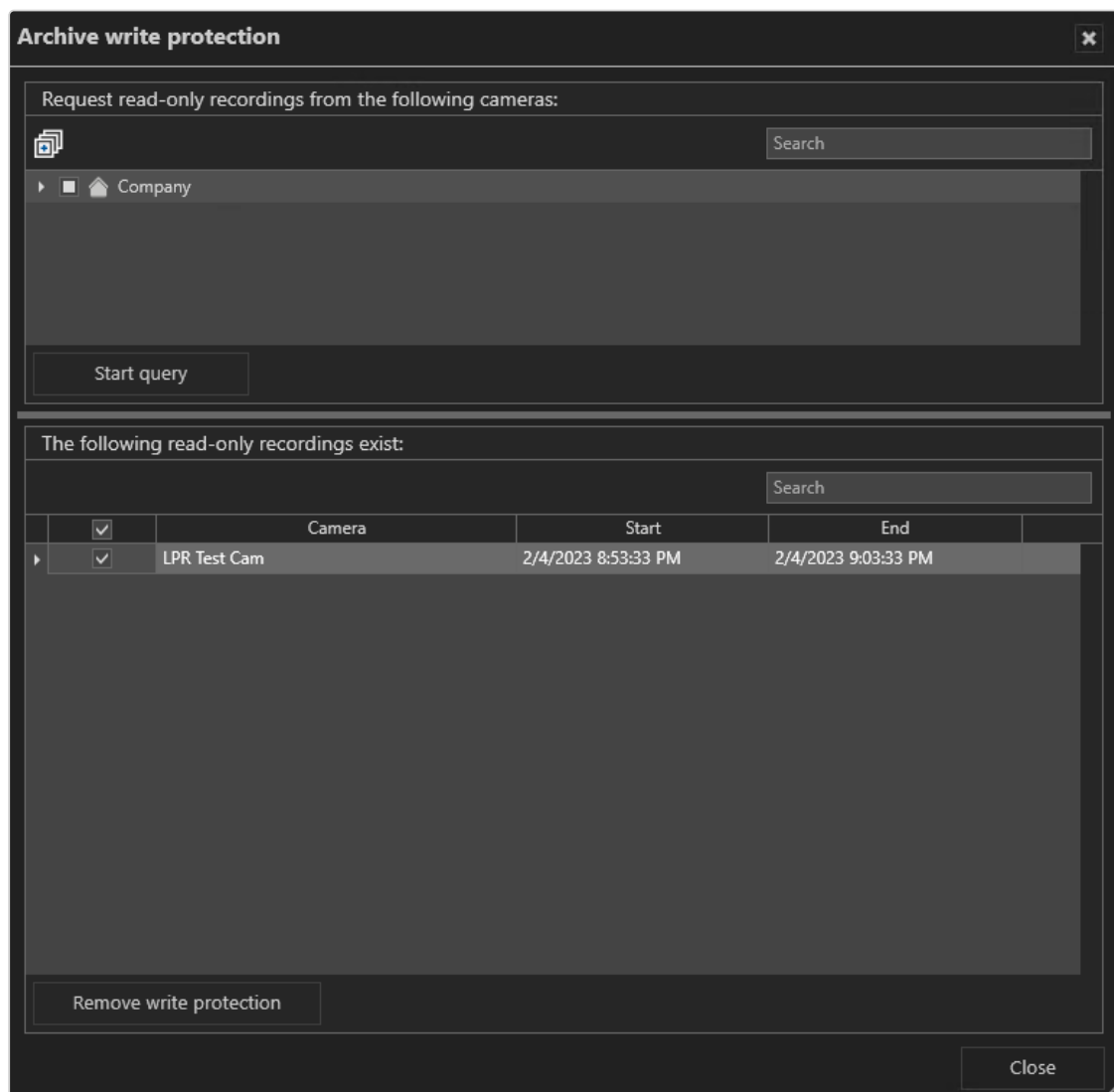


Abb. 47: Schreibschutz von Aufzeichnungen mehrerer Kameras entfernen

1. Wählen Sie **Schreibschutz von Aufzeichnungen** im Menü **Extras**.
2. Wählen Sie die zu prüfenden Kameras, um sicherzustellen, dass ein schreibgeschützter Aufnahmebereich vorhanden ist.
3. Klicken Sie auf **Abfrage starten**, um eventuell schreibgeschützte Aufzeichnungen der gewählten Kameras anzeigen zu lassen.
4. Wählen Sie die Bereiche aus, in deren Aufzeichnungen der Schreibschutz entfernt werden soll.
5. Wählen Sie **Schreibschutz entfernen**.
6. **Schließen** Sie das Fenster.

Logoaktion konfigurieren

Mit der Logoaktion legen Sie fest, welche Ansicht angezeigt werden soll, wenn Sie auf das Qognify-Logo am oberen Bildschirmrand klicken.

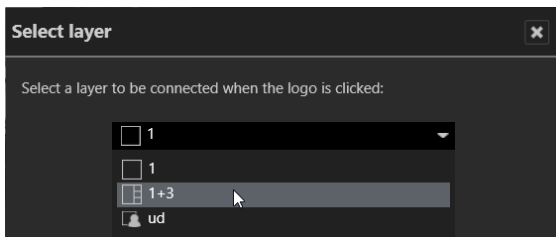


Abb. 48: Logoaktion konfigurieren

1. Wählen Sie **Logoaktion konfigurieren** im Menü **Extras**.
2. Wählen Sie die definierten Ansichten im Aufklappmenü. Die Ansichten werden im Konfigurationsmenü gespeichert (siehe „[Ansichten](#)“ auf Seite 404).
3. Bestätigen Sie mit **OK**.

Statusbericht für automatischen Bildexport

Dieses Menüelement ist nur im „Konfigurationsmodus“ auf Seite 207 verfügbar.

Der Statusbericht für den automatischen Bildexport zeigt Probleme an, die beim automatischen Bilddatenexport aufgetreten sind.

Sind während des Exports von Bilddaten Probleme aufgetreten, können die gescheiterten Exporte neu gestartet oder aus der Liste gelöscht werden.

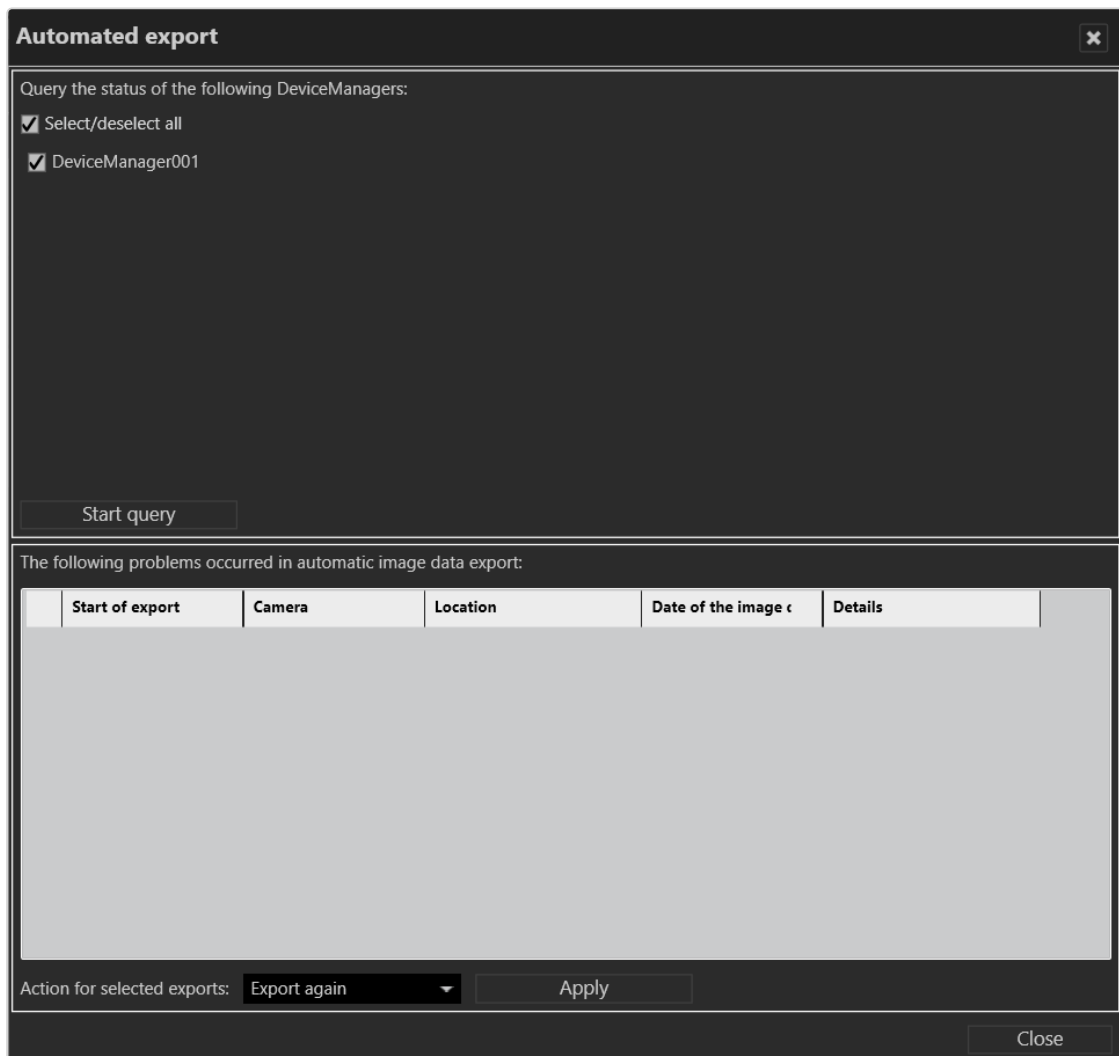


Abb. 49: Statusbericht für automatischen Bildexport

Der Statusbericht für den automatischen Bildexport zeigt eine Liste der gescheiterten automatischen Exporte an.

1. Wählen Sie die Device Manager aus, die in die Abfrage nach gescheiterten automatischen Exporten eingeschlossen werden sollen.
2. Klicken Sie auf **Abfrage starten**. Die am ausgewählten Device Manager aufgetretenen Fehler und Probleme werden angezeigt.
3. Wählen Sie ein oder mehrere Elemente in der Liste aus und wählen Sie eine **Aktion für die ausgewählten Exporte** aus.

4. **Erneut exportieren.** Der ausgewählte Bilddatenexport wird erneut durchgeführt.
5. **Aus Liste löschen.** Die ausgewählten Elemente werden aus der Ergebnisliste entfernt.
6. Klicken Sie auf **Übernehmen**, um die ausgewählte Aktion durchzuführen.
7. Klicken Sie auf **Schließen**.

Manueller Referenzbildvergleich

Für die Erstellung von Referenzkamerabildern und den Vergleich von Kamerabildern muss der Benutzer berechtigt sein, Live-Bilder im Überwachungsmodus anzuzeigen (siehe „[Administrative Rechte und Benutzerrechte](#)“ auf Seite 24).

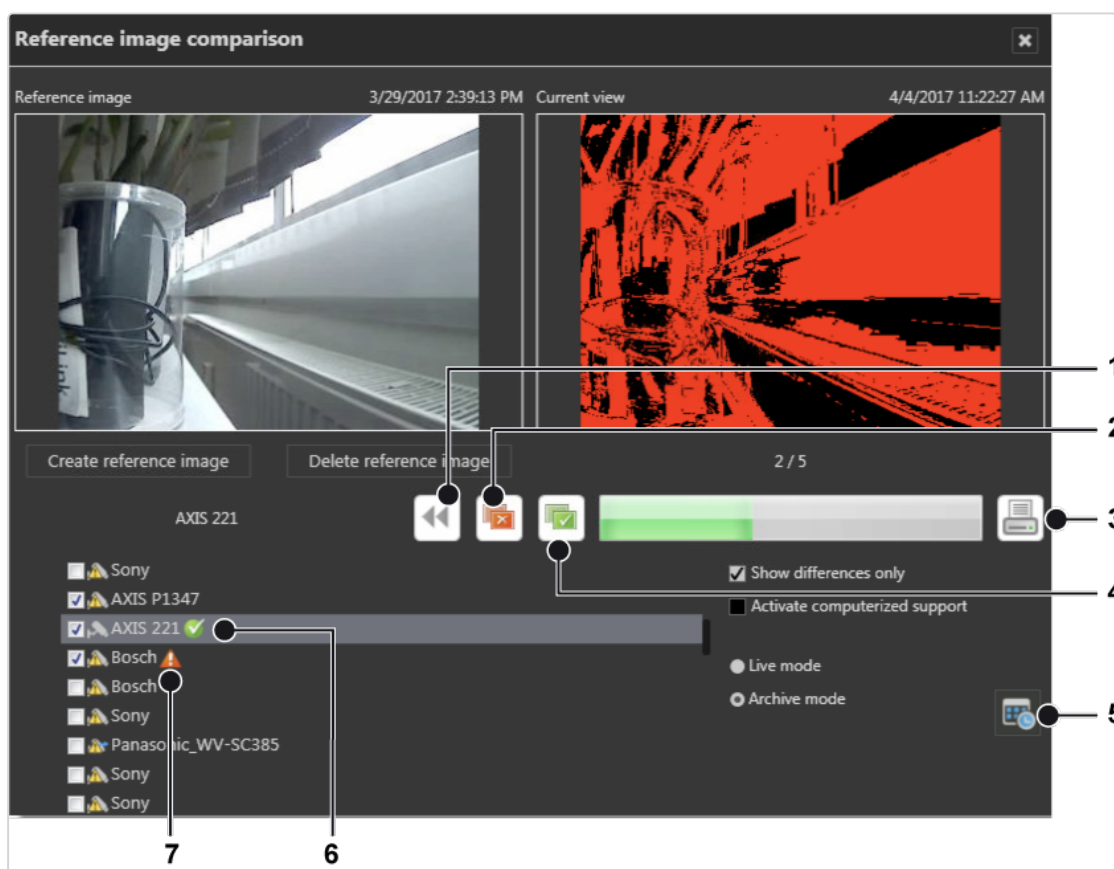


Abb. 50: Manueller Referenzbildvergleich

Mithilfe des manuellen Referenzbildvergleichs können Veränderungen des statischen Objekts erkannt werden.

Mobotix-Kameras werden nur für Motion JPEG unterstützt. Der Referenzbildvergleich funktioniert nicht bei Bildern, die mit einer Fisheye-Kamera aufgenommen wurden.

1. Wählen Sie eine Kamera aus der Liste aus und klicken Sie auf **Referenzbild erstellen**. Das aktuelle Kamerabild wird als Referenzbild verwendet. Die aktuelle Ansicht zeigt das jeweilige Live-Bild der Kamera oder ein archiviertes Bild.

2. Um ein Referenzbild zu löschen, wählen Sie die Kamera aus der Liste aus und klicken Sie auf **Referenzbild löschen**.
3. Wählen Sie die gewünschte Kamera aus und überprüfen Sie beide Bilder auf Veränderungen.
4. Wählen Sie **Abweichungen** (2), um die Bilder abzulehnen und als nicht identisch zu markieren. Nach dem Kameranamen wird das rote Symbol (7) angezeigt.
5. Wählen Sie **Übereinstimmung** (4), um die Bilder zu akzeptieren und als identisch zu markieren. Nach dem Kameranamen wird das grüne Symbol (6) angezeigt.
6. Wenn die Veränderungen schwer zu erkennen sind, aktivieren Sie **Nur Unterschiede anzeigen**. Die von der Bildverarbeitungssoftware erkannten Veränderungen werden in der aktuellen Ansicht als hervorgehobene Bereiche dargestellt. Werden keine Veränderungen festgestellt, wird die aktuelle Ansicht schwarz.
7. Deaktivieren Sie **Nur Unterschiede anzeigen**, um wieder das eigentliche Kamerabild anzeigen zu lassen.
8. Aktivieren Sie **Rechnerunterstützung aktivieren**, um eine Schwellenwertskala einzublenden. Um die Schwellenwerte zu ändern, verschieben Sie den Zeiger auf der Skala. Dadurch werden die Schwellenwerte des aktuellen Bilds geändert, um mögliche Veränderungen im Bild besser erkennen zu können.
9. Wählen Sie **Live-Modus** oder **Archivmodus**. Wenn Archivmodus ausgewählt wird, kann das Referenzbild mit einem aufgezeichneten Bild verglichen werden.
10. Wählen Sie **Kalender** (5) und wählen Sie Datum und Uhrzeit des archivierten Bilds aus.
11. Um einen Bericht mit den Ergebnissen zu drucken, wählen Sie **Drucken** (3).

Bericht für Referenzbildvergleich drucken

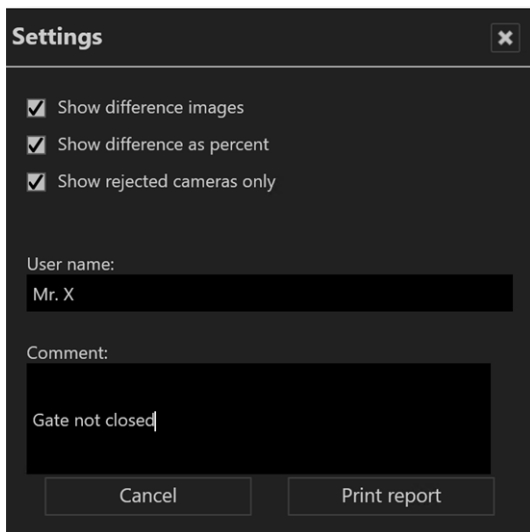


Abb. 51: Bericht für Referenzbildvergleich drucken

1. In den Einstellungen können die Druckoptionen angegeben werden:
 - Wählen Sie **Differenzbilder anzeigen**, um die aktuellen Ansichten mit hervorgehobenen Differenzen auszudrucken.
 - Wählen Sie **Differenz in Prozent anzeigen**, um die erkannten Unterschiede in jedem Bild als Prozentsatz zu drucken.
 - Wählen Sie **Nur abgelehnte Kameras anzeigen**, um den Bericht ohne die angenommenen Kameras zu drucken.
2. Geben Sie den **Benutzernamen** ein und fügen Sie bei Bedarf einen **Kommentar** hinzu.
3. Wählen Sie **Bericht drucken**.

Info

Im Menü **Info** werden Informationen über das System und die beiden Methoden zum Abrufen einer Lizenz für Qognify VMS 7.4 angezeigt. Die Installation muss innerhalb von 30 Tagen aktiviert werden. Dazu müssen Sie einen automatisch generierten Aktivierungsschlüssel, die Produkt-ID, an Qognify schicken.

In diesem Menü werden folgende Optionen angezeigt:

- Software aktivieren
- Informationen über die Software anzeigen

Qognify VMS-Lizenz online aktivieren

Das Produkt wird online aktiviert, um eine Lizenz zu personalisieren oder eine Lizenzdatei herunterzuladen.

Für die Online-Aktivierung wird eine Internet-Verbindung benötigt.

Lizenz personalisieren

License activation: HQ	
<input checked="" type="radio"/> Personalize license <input type="radio"/> Download license	
INR	132465
Name	Mr. Smith
Email	smith@smith.qq
Phone	001-123 456
Address 1	Runa way 12
Address 2	
Postal code	12345
City	Berlin
Country	Germany
OK Cancel	

Abb. 52: Lizenz personalisieren

1. Wählen Sie im Menü **InfoProdukt aktivieren**.
2. Wählen Sie **Online**.
3. Wählen Sie **Lizenz personalisieren**, wenn Sie die Lizenz mit Ihren Benutzerdaten registrieren möchten und sie noch nicht registriert wurde.
4. Geben Sie Ihre Installationsnummer (**INR**) und Benutzerdaten ein.
5. Bestätigen Sie die Angaben mit **OK**. Der Client verbindet sich mit dem Registrierungsserver von Qognify und überträgt den Lizenzschlüssel auf den Rechner.

Lizenz herunterladen

Sie können eine neue Lizenz herunterladen, wenn ein Update durchgeführt wurde und die Lizenz erneut benötigt wird.

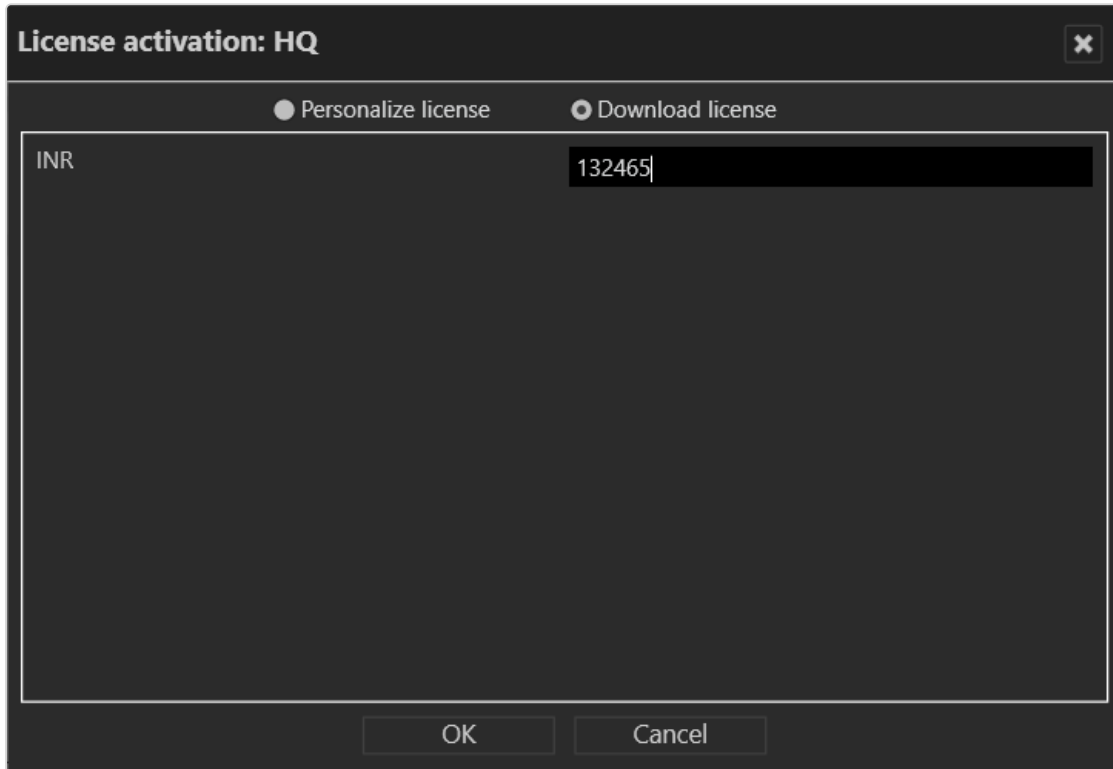


Abb. 53: Lizenz herunterladen

1. Wählen Sie **Lizenz herunterladen**.
2. Geben Sie Ihre Installationsnummer (**INR**) ein.
3. Bestätigen Sie die Angaben mit **OK**. Der Client verbindet sich mit dem Registrierungsserver von Qognify und überträgt den Lizenzschlüssel auf den Rechner.

Falls sich die Produkt-ID geändert hat (z. B. aufgrund von Änderungen an der Server-Hardware), kontaktieren Sie den Qognify-Support (siehe „[Support](#)“ auf [Seite 13](#)).

Produkt offline aktivieren

Wenn der Client keinen Internetzugang hat, aktivieren Sie den Client, indem Sie zunächst per E-Mail eine Lizenz beantragen. Nachdem Sie die Lizenzdatei per E-Mail erhalten haben, muss diese importiert werden.

Lizenz beantragen

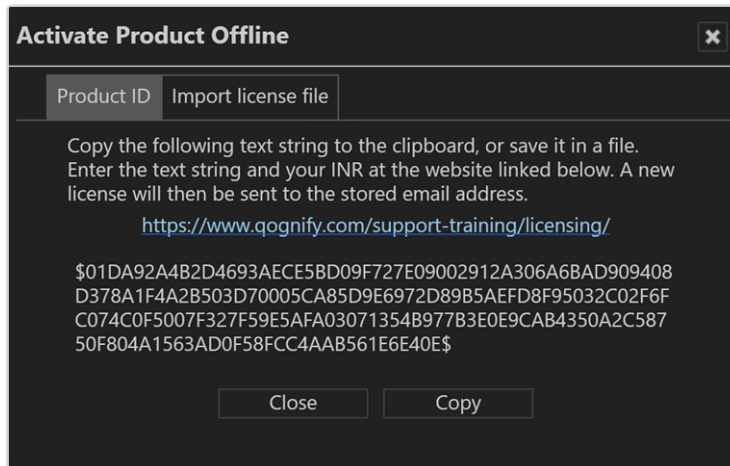


Abb. 54: Lizenz beantragen

1. Wählen Sie im Menü **InfoProdukt aktivieren**.
2. Wählen Sie **Offline**.
3. Öffnen Sie den Tab **Produkt-ID**. Die Software erstellt eine eindeutige Produkt-ID.
4. Klicken Sie auf **Kopieren**, um die angezeigte Produkt-ID in die Zwischenablage zu kopieren.
5. Öffnen Sie die Qognify-Internetseite und navigieren Sie zum Bereich „Support“ und „**Lizenzierung**“.
6. Klicken Sie auf „Neuer Lizenzschlüssel“.
7. Geben Sie dort neben den weiteren benötigten Angaben Ihre Produkt-ID an. Sie erhalten die Lizenzdatei per E-Mail.

Lizenzdatei importieren

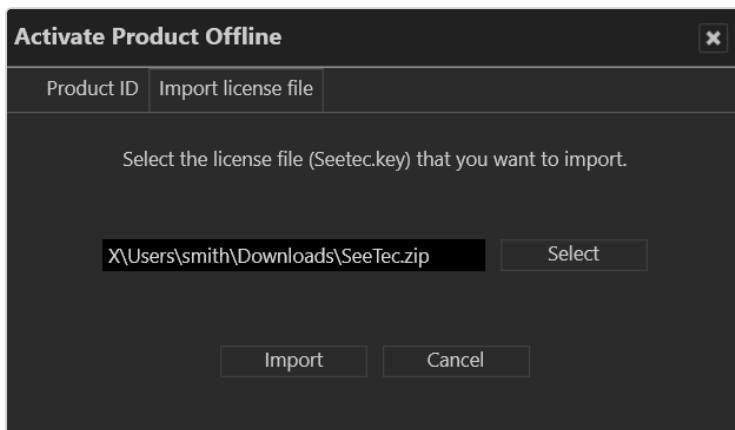


Abb. 55: Lizenzdatei importieren

1. Wählen Sie im Menü **InfoProdukt aktivieren**.
2. Wählen Sie **Offline**.
3. Öffnen Sie den Tab **Lizenzdatei importieren**.
4. Klicken Sie auf **Auswählen** und navigieren Sie zum Speicherort der Lizenzdatei.
5. Wählen Sie die Lizenzdatei aus. Beim Import wird die gezippte Datei automatisch entpackt.
6. Klicken Sie auf **Importieren**, um den Lizenzschlüssel zu verwenden.

Lizenz anzeigen

Während der Installation wird eine Testlizenz installiert, die 30 Tage gültig ist. Eine Demolizenz ist bis zum angezeigten Datum gültig. Ohne gültige Lizenz ist keine Anmeldung möglich. Bei weiteren Fragen wenden Sie sich an den Qognify-Support (siehe „[Support](#)“ auf Seite 13).

1. Wählen Sie im Menü **InfoInformationen anzeigen**.
2. Wählen Sie **Lizenz anzeigen**. Informationen zur Lizenz werden in drei Tabs angezeigt.
3. Öffnen Sie den Tab **Übersicht**, um allgemeine Informationen zum Produkt anzuzeigen, wie die INR (Installationsnummer), SMA (Software Maintenance Agreement) und den Gültigkeitszeitraum der Lizenz (bei einer Demolizenz).

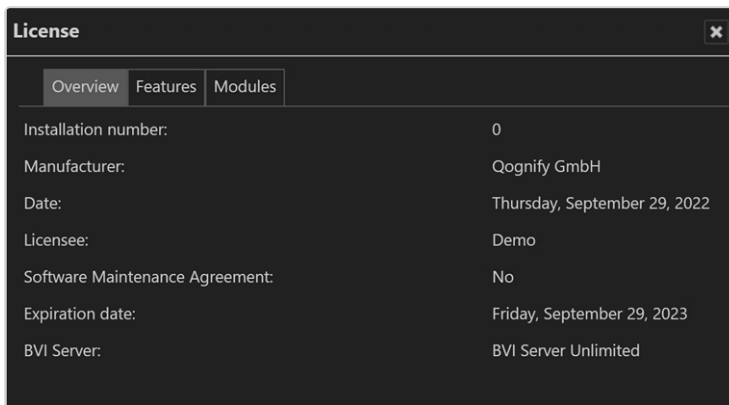


Abb. 56: Lizenz anzeigen - Übersicht

4. Wählen Sie **Features**, um die durch die installierte Lizenzdatei aktivierten Features anzuzeigen.

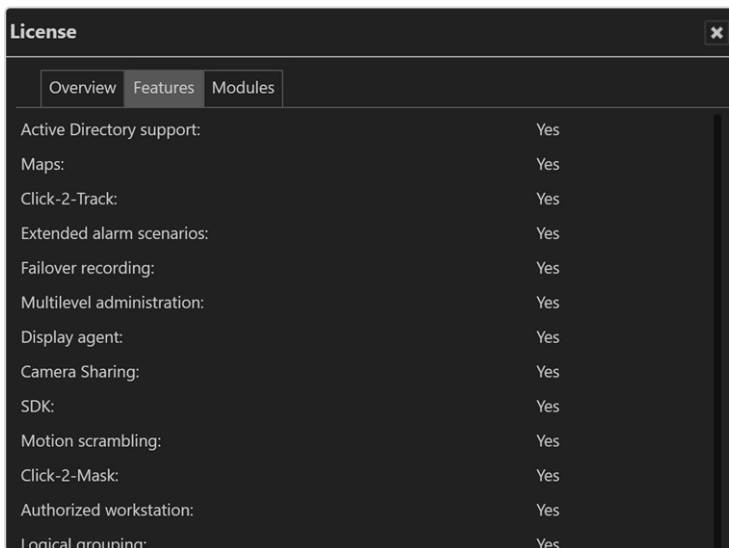
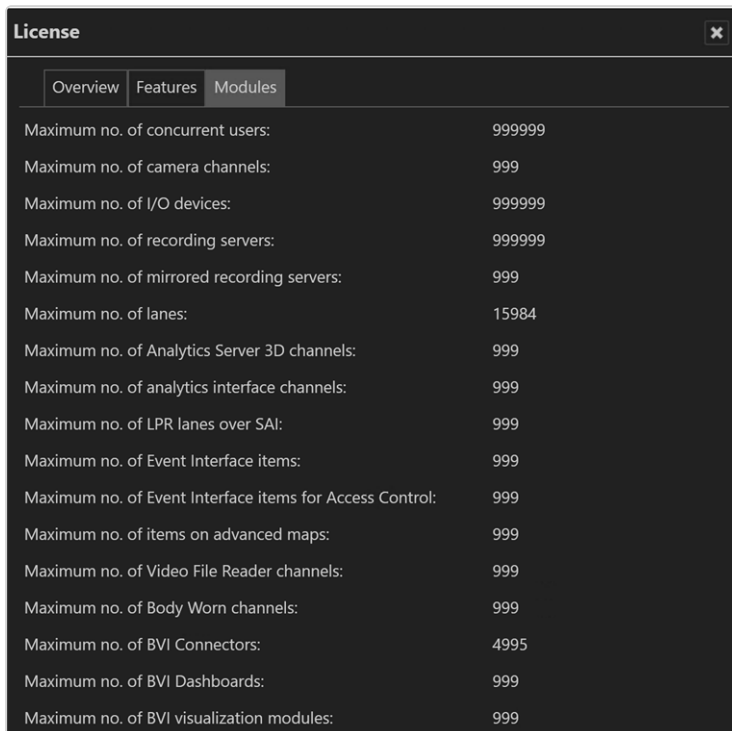


Abb. 57: Lizenz anzeigen - Features

5. Wählen Sie **Module**, um anzuzeigen, wie viele Module wie Kameras (Geräte), Server, Analytics-Kanäle usw. durch die installierte Lizenzdatei aktiviert werden.



Overview	Features	Modules
Maximum no. of concurrent users:		999999
Maximum no. of camera channels:		999
Maximum no. of I/O devices:		999999
Maximum no. of recording servers:		999999
Maximum no. of mirrored recording servers:		999
Maximum no. of lanes:		15984
Maximum no. of Analytics Server 3D channels:		999
Maximum no. of analytics interface channels:		999
Maximum no. of LPR lanes over SAI:		999
Maximum no. of Event Interface items:		999
Maximum no. of Event Interface items for Access Control:		999
Maximum no. of items on advanced maps:		999
Maximum no. of Video File Reader channels:		999
Maximum no. of Body Worn channels:		999
Maximum no. of BVI Connectors:		4995
Maximum no. of BVI Dashboards:		999
Maximum no. of BVI visualization modules:		999

Abb. 58: Lizenz anzeigen - Module

Programminformationen anzeigen

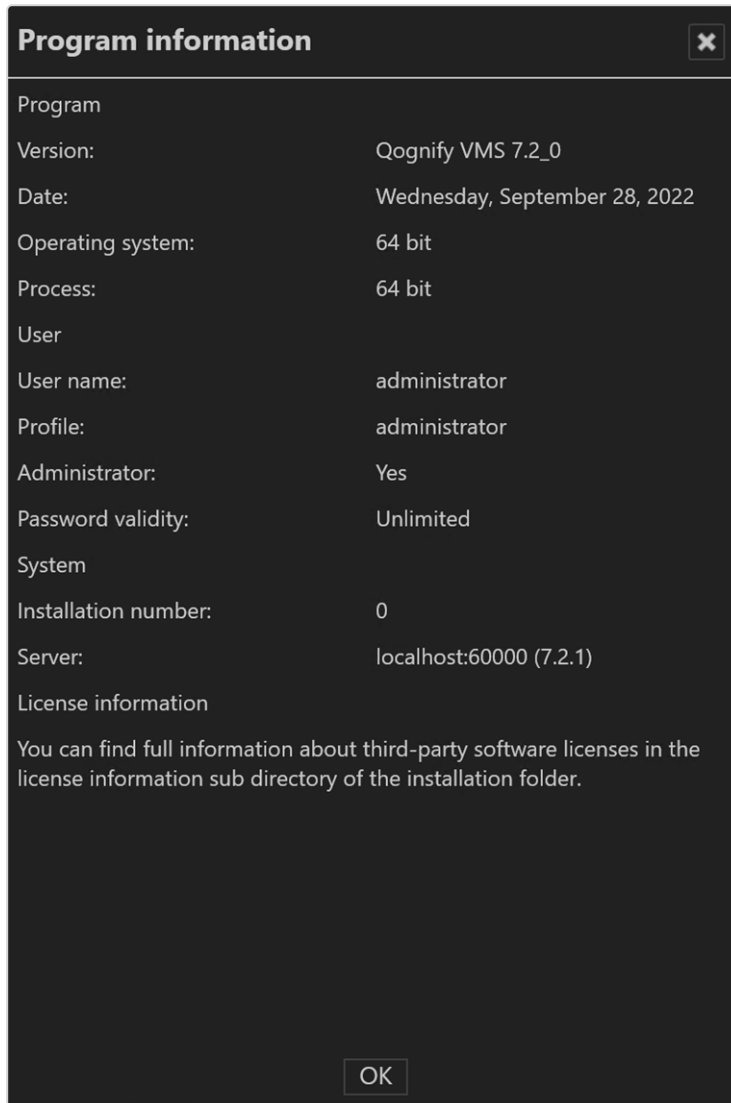


Abb. 59: Programminformationen anzeigen

1. Wählen Sie **Programminformationen anzeigen** im Menü **Info**. Die Informationen unter anderem zur Programmversion, zum aktuellen Benutzer und Profil sowie der Passwortgültigkeit werden angezeigt.

Systeminformationen anzeigen



Abb. 60: Systeminformationen anzeigen

1. Wählen Sie **Systeminformationen anzeigen** im Menü **Info**. Die Informationen unter anderem zum CoreService Main, zur Anzahl der aktivierten Device Manager und zu den Videoquellen (Kameras) werden angezeigt.
2. Klicken Sie auf **Kopieren**, um die Systeminformationen in die Zwischenablage zu kopieren. Sie können die Daten aus der Zwischenablage in Ihr E-Mail-Programm einfügen, um sie an den Support zu schicken (siehe „[Support](#)“ auf [Seite 13](#)).

Hilfe

Im Hilfemenü werden folgende Optionen angezeigt:

Online Hilfe

Startet die Onlinehilfe auf der Startseite. Darüber hinaus besteht über direkte Verknüpfungen auch Zugriff auf einzelne Themen direkt aus den jeweiligen Steuerelementen und Dialogfenstern. Das System prüft automatisch auf aktuelle Versionen der Onlinehilfe. Der Benutzer wird benachrichtigt, wenn die installierte Version nicht aktuell ist.

Wenn Sie die Onlinehilfe zum ersten Mal starten, werden Sie möglicherweise vom Browser dazu aufgefordert, ActiveX zu aktivieren oder JavaScript zuzulassen. Die Onlinehilfe funktioniert nicht ordnungsgemäß, wenn diese Dienste blockiert sind.

Problemaufzeichnung starten

Falls es zu Problemen bei Abläufen kommen sollte, können Sie mit der Funktion „Problemaufzeichnung starten“ diese auch direkt aufzeichnen, kommentieren und speichern. Die Problemaufzeichnung ist Teil des Betriebssystems.

1. Wählen Sie **Problemaufzeichnung starten** im Menü **Hilfe**.
2. Aktivieren Sie **Aufzeichnung starten** und führen Sie die Schritte durch, die zu dem Problem geführt haben.
3. Sobald Sie die Schritte durchgeführt haben, beenden Sie die Aufzeichnung.
4. Klicken Sie auf **Kommentar hinzufügen** und fügen Sie der Aufzeichnung gegebenenfalls einen Kommentar hinzu (z. B. Zeitpunkt, Verhalten des Clients und der Geräte usw.).
5. Geben Sie den Ablageort der Datei an.

Hilfesymbole anzeigen

1. Die Hilfesymbole sind kleine graue Kreise mit Fragezeichen innerhalb der Programmkomponenten, die Sie direkt auf die entsprechende Stelle in der Onlinehilfe führen.
2. Aktivieren oder deaktivieren Sie **Hilfesymbole anzeigen** im Menü **Hilfe**.

Benutzer wechseln

Der aktuelle Benutzer wird in der Funktionsleiste der Benutzeroberfläche angezeigt.

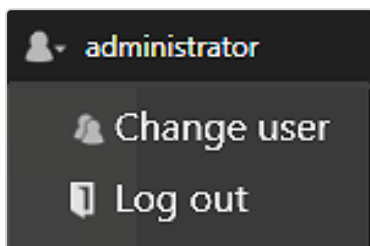


Abb. 61: Benutzer wechseln

1. Klicken Sie auf das Benutzersymbol in der Funktionsleiste.
2. Um sich beim Server als ein anderer Benutzer anzumelden, klicken Sie auf **Benutzer wechseln**. Alternativ können Sie den Benutzer auch über das Menü „Datei“ wechseln (siehe „[Benutzer wechseln](#)“ auf Seite 87).
3. Um den aktuellen Benutzer vom Server abzumelden, klicken Sie auf **Abmelden**.

Die Modusleiste

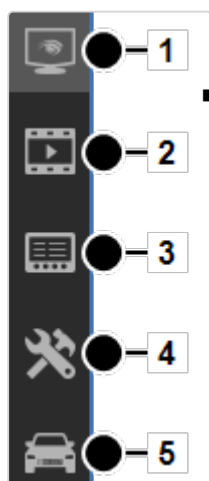


Abb. 62: Die Modusleiste

In der Modusleiste können Sie zwischen den Modi der Anzeige wechseln.


- **Überwachungsmodus (1)**: Nach der Anmeldung startet das System im Überwachungsmodus (siehe „[Überwachungsmodus](#)“ auf Seite 141). Die Anzahl der aufgetretenen Alarme und Systemereignisse wird durch eine Nummer im Symbol angezeigt. Darüber hinaus wird die Anzahl der Alarme und Systemereignisse durch eine Nummer im jeweiligen Tab in der Alarmliste angezeigt (siehe „[Alarmliste und Systemmeldungen](#)“ auf Seite 170).
- **Archivmodus (2)**: Im Archivmodus können aufgezeichnete Bilddaten verwaltet und angezeigt sowie nach Alarmereignissen gesucht werden (siehe „[Archivmodus](#)“ auf Seite 177). Die Anzahl der laufenden Exportvorgänge wird durch eine Nummer im Symbol **Archiv** angezeigt.
- **Ereignisauswertung (3)**: Die Ereignisauswertung zeigt eine Liste der angefallenen Ereignisse an (siehe „[Ereignisauswertung](#)“ auf Seite 201).

- **Konfigurationsmodus (4)**. Der Konfigurationsmodus dient zur Administration und Konfiguration der Videoquellen und Benutzer sowie Standorte (siehe „[Konfigurationsmodus](#)“ auf [Seite 207](#)).
- **LPR-Modus (5)**: Der LPR-Modus dient zur Zeichenerkennung in den Bilddaten der entsprechenden Kameras (siehe „[LPR-Modus](#)“ auf [Seite 487](#)).


Die Steuerleiste

Die Steuerleiste beinhaltet die Tabs, die je nach Modus zur Steuerung der Anzeige oder zur Konfiguration benötigt werden. Eine Beschreibung der Tabs erhalten Sie in den Abschnitten des entsprechenden Modus. Tabs können nicht verschoben werden. Sie bleiben in der Steuerleiste verankert.

Elemente in der Baumansicht anzeigen



1. Klicken Sie auf der linken Seite des oberen Elements im Tab auf , um die untergeordneten Elemente anzuzeigen oder auszublenden.

Kontextspezifische Hilfe öffnen



1. Klicken Sie auf **Hilfe** , um die Online-Hilfe im Standard-Webbrowser anzeigen zu lassen. Der Webbrowser kann in der Client-Konfiguration ausgewählt werden (siehe „[Client-Konfiguration](#)“ auf [Seite 69](#)). Die Online-Hilfe kann auch über das Hilfemenü aufgerufen werden (siehe „[Hilfe](#)“ auf [Seite 135](#)).

Steuerleiste verankern



Die Steuerleiste ist standardmäßig immer sichtbar (verankert). Es ist eine Funktion zum automatischen Ausblenden verfügbar.

- Klicken Sie auf die Reißzwecke , um die Funktion zum automatischen Ausblenden zu aktivieren. In diesem Zustand wird die Steuerleiste automatisch nach rechts hin minimiert, wenn der Mauszeiger aus der Steuerleiste weg bewegt wird. Sobald der Mauszeiger auf die minimierte Steuerleiste bewegt wird, wird diese automatisch wieder eingeblendet.
- Klicken Sie erneut auf die Reißzwecke , um die Funktion zum automatischen Ausblenden zu deaktivieren. In diesem Zustand ist die Steuerleiste immer sichtbar (Standardeinstellung).

Steuerelement minimieren und maximieren

- Klicken Sie auf das doppelte Dreieck , um ein Steuerelement nach oben hin in die Steuerleiste zu minimieren.
- Klicken Sie auf das doppelte Dreieck , um ein Steuerelement zu maximieren.

Steuerleiste minimieren und maximieren

- Klicken Sie auf das graue Dreieck  im rechten oberen Eck eines Steuerelements, um die Steuerleiste nach rechts hin zu minimieren. Das Hauptfenster vergrößert sich dadurch.
- Klicken Sie auf das graue Dreieck  in der minimierten Steuerleiste, um die Leiste zu maximieren.

Suche

Qognify VMS bietet modusspezifische Such- und Abfragefunktionen:

- Suchen im Überwachungsmodus (siehe „Suchen im Überwachungsmodus“ auf Seite 174)

Die Suche nach Elementen in der Steuerleiste ist auch im Archivmodus und LPR-Modus verfügbar.

- Suchen nach Alarmen im Archivmodus (siehe „Alarme suchen“ auf Seite 190)
- Suchen (Abfrage) in der Ereignisauswertung (siehe „Abfrage filtern“ auf Seite 202)
- Suchen im Konfigurationsmodus (siehe „Suchen im Konfigurationsmodus“ auf Seite 217)
- Suche (Abfrage) im LPR-Modus (siehe „LPR-Modus“ auf Seite 487)

Überwachungsmodus

Der Überwachungsmodus dient zur Darstellung von Live-Bildern, Webseiten, Lageplänen, Ansichten, Alarmen und Wächterrundgängen sowie zum Steuern von PTZ-Kameras und sonstiger angeschlossener Peripherie, wie z. B. Türöffnern (siehe „Die Benutzeroberfläche“ auf Seite 65).

1. Um in den Überwachungsmodus zu wechseln, klicken Sie auf **Überwachungsmodus** in der Modusleiste.

Kamerabedienung

Sie können die Funktionen der Kamera über die Steuerleiste bedienen (siehe „Kamerabildsteuerung“ auf Seite 151) oder mit der **Steuerung** (siehe „Kamerasteuerung“ auf Seite 160).

Um eine Kamera zu bedienen, wählen Sie die Kamera auf der Arbeitsfläche aus. Sie erkennen eine Standardaufzeichnung daran, dass am rechten unteren Rand des Kamerabildes im Überwachungsmodus ein grüner Punkt zu sehen ist. Eine Alarmaufzeichnung erkennen Sie daran, dass am rechten unteren Rand des Kamerabildes ein roter Punkt zu sehen ist.

Wenn keine Aufzeichnung vorhanden ist, wird anstelle eines roten oder grünen Punkts ein schwarzes Quadrat angezeigt.

Tabs

Mit den Tabs öffnen und schließen Sie die Ansichten (siehe „[Arbeitsfläche](#)“ unten).

Steuerleiste

In der Steuerleiste können Sie folgende Aktionen durchführen:

- die gewählten PTZ-Kameras bewegen und den Bildausschnitt verändern (siehe „[PTZ-Steuerung](#)“ auf Seite 160),
- Aktionen (Buttons) auslösen (siehe „[Buttons](#)“ auf Seite 164),
- Wächterrundgänge durchführen (siehe „[Wächterrundgang](#)“ auf Seite 165),
- die optional installierten Kommunikationsmöglichkeiten (Kamera und Audio) nutzen (siehe „[Audio](#)“ auf Seite 166),
- den Dispatcher-Modus aufrufen (sofern installiert, siehe „[Videowall Dispatcher](#)“ auf Seite 93). Der Dispatcher-Modus wird über das Menü „Ansicht“ ein- und ausgeschaltet.
- die für jeden Standort angelegten Kameras auswählen (siehe „[Übersicht](#)“ auf Seite 159),
- nach bestimmten installierten Kameras suchen.

Arbeitsfläche

Die Arbeitsfläche ist das Hauptfenster für die Anzeige von Kacheln mit Elementen wie Kamerabildern oder Wächterrundgängen (siehe „[Die Benutzeroberfläche](#)“ auf Seite 65). Die Arbeitsfläche zeigt bis zu 100 Kacheln gleichzeitig an. Dabei können die Kacheln unterschiedlich angeordnet sein:

- gleichmäßig als Gitternetz
- mit einer Hauptkachel und kleineren Kacheln

Der Name des Kamerabenzers wird oben im Bild für alle Zuseher angezeigt , wenn diese Funktion konfiguriert wurde (siehe „[Benutzer-Sicherheitseinstellungen konfigurieren](#)“ auf Seite 484).

Alarmbenachrichtigung („Toast-Benachrichtigung“)

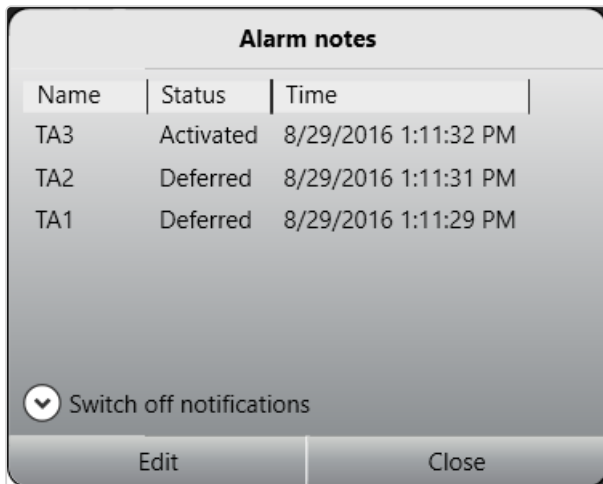


Abb. 63: Alarmbenachrichtigung („Toast-Benachrichtigung“)

Abhängig von der Einstellung werden aufgetretene Alarmer und Systemmeldungen in einem eigenen Meldungsfenster (Alarmbenachrichtigung) am unteren Bildschirmrand angezeigt. Weitere Informationen finden Sie im Abschnitt „Alarmmeldungen“ auf Seite 170.

Ansichten einrichten

Ansichten können im Konfigurationsmodus im Bereich „Ansichten“ eingestellt werden (siehe „Ansichten“ auf Seite 404). Optional können auch temporäre Ansichten zusammengestellt werden, die nur für den Benutzer vorhanden sind und nicht gespeichert werden.

Bei einigen Ansichten können die zur Verfügung stehenden Objekte wie Kameras oder Lagepläne beliebigen Kacheln auf der Arbeitsfläche zugewiesen werden.

1. Ziehen Sie die gewünschte Ansicht aus dem Steuerelement **Übersicht** auf die Arbeitsfläche. Um die Ebenen zu konfigurieren, siehe „Ansichten“ auf Seite 404.
oder klicken Sie auf das **Menü Ebene** in der Funktionsleiste (siehe „Die Funktionsleiste“ auf Seite 67) und wählen Sie **Ebene hinzufügen**. Sie können die gewünschte Anzahl der Kacheln auswählen bzw. eine benutzerdefinierte Ansicht erstellen. Oder wählen Sie **Persönliche Ansicht laden**, um eine zuvor gespeicherte vom Benutzer definierte Ansicht zu laden. Die gewählte Ansicht wird rechts neben dem Symbol für das Ansichtsmenü in der Tabauswahl angezeigt.
2. Klicken Sie auf das Kreuzchen im Tab, um diese Ansicht zu schließen.

3. Ziehen Sie das gewählte Objekt auf die gewünschte Kachel auf der Arbeitsfläche. Um Objekte auf der Arbeitsfläche zu bewegen, ziehen Sie ein Objekt auf der Arbeitsfläche auf die Kachel, in der es angezeigt werden soll. Ein dort bereits vorhandenes Objekt wird in die bisherige Kachel des bewegten Objekts verschoben.
4. Wählen Sie **Ansicht in Nebenfenster öffnen**, um die neue Ansicht auf einem zweiten Bildschirm anzeigen zu lassen (siehe „[Ansicht](#)“ auf Seite 91).
5. Wählen Sie den **Automatischen Ansichtenwechsel** und das gewünschte **Intervall**, um zwischen den geöffneten Ansichten nach Ablauf eines Intervalls automatisch zu wechseln.


Der automatische Ansichtenwechsel wird bei einem Alarmszenario gestoppt und nach einem Alarm automatisch fortgesetzt.

Ansichtsmodus in mehreren Fenstern einstellen

Die Ansichtsmodus-Funktion ist verfügbar, wenn mehrere Client-Fenster verwendet werden, und dient dazu, die Fenster in unterschiedlichen Modi zu belassen. Wenn an den Client mehrere Displays angeschlossen sind, können die Client-Fenster auf diese verteilt werden. Der Ansichtsmodus jedes Fensters kann separat eingestellt werden, das heißt, Displays können im Überwachungsmodus bleiben, selbst wenn das Haupt-Display in einen anderen Modus (z. B. Archivmodus oder Konfigurationsmodus) umgeschaltet wird.



Abb. 64: Ansichtsmodus-Symbol „Fenster in Überwachungsmodus belassen“

1. Wechseln Sie in den Überwachungs- oder Archivmodus und ziehen Sie die gewünschte Kameraansicht auf das sekundäre Fenster. Die Drag & Drop-Funktion funktioniert zwischen Überwachungs- und Archivmodus und umgekehrt.
2. Klicken Sie im sekundären Fenster auf **Fenster in Überwachungsmodus belassen** (). Die Kameraansicht am sekundären Fenster bleibt im Überwachungsmodus mit Live-Bild, selbst wenn das primäre Fenster in einen anderen Modus umgeschaltet wird.
3. Um den Ansichtsmodus im sekundären Fenster zurückzusetzen, klicken Sie erneut auf das Monitorsymbol.



4. Wenn Sie **nach** Umschalten des Ansichtsmodus im primären Fenster auf das Monitorsymbol im sekundären Fenster klicken, wird im sekundären Fenster wieder die letzte Live-Bildansicht angezeigt.

Sequenzielles Alarmfenster

Die Einstellungen für das sequenzielle Alarmfenster werden im Menü „Ansicht“ definiert (siehe „[Sequenzielles Alarmfenster hinzufügen](#)“ auf Seite 92).



Abb. 65: Sequenzielles Alarmfenster

1. Um in den sequenziellen Modus zu wechseln, wählen Sie **Zeilenmodus** (). Die Alarme werden in einer einzigen Zeile angezeigt. Wenn die Anzahl der Alarmkameras die festgelegte Spaltenanzahl übersteigt, werden die restlichen Alarmkameras ignoriert.
2. Um zum **Fortlaufenden Modus** zu wechseln, wählen Sie  . Wenn die Anzahl der Alarmkameras die festgelegte Spaltenanzahl übersteigt, werden die zusätzlichen Kameras in der Zeile darunter hinzugefügt.

Click-2-Track

Eine Person oder ein Objekt, das sich über verschiedene Kameraansichten hinweg bewegt, kann auch ohne Angabe des Kameranamens der folgenden Ansicht verfolgt werden. Stattdessen wird der Weg der Person oder des Objekts im Überwachungsmodus definiert, indem der Bereich aktiviert wird, der von der benachbarten Kamera abgedeckt wird.

Diese Funktion wird in „[Click-2-Track](#)“ auf Seite 288 konfiguriert. Es ist auch im Archivmodus verfügbar (siehe „[Click-2-Track](#)“ auf Seite 182) und kann mit dem Mini-Archiv-Player aufgerufen werden (siehe „[Miniarchiv Player](#)“ auf Seite 153).

Diese Funktion erfordert eine entsprechende Lizenz und ist nicht im Standardpaket enthalten.

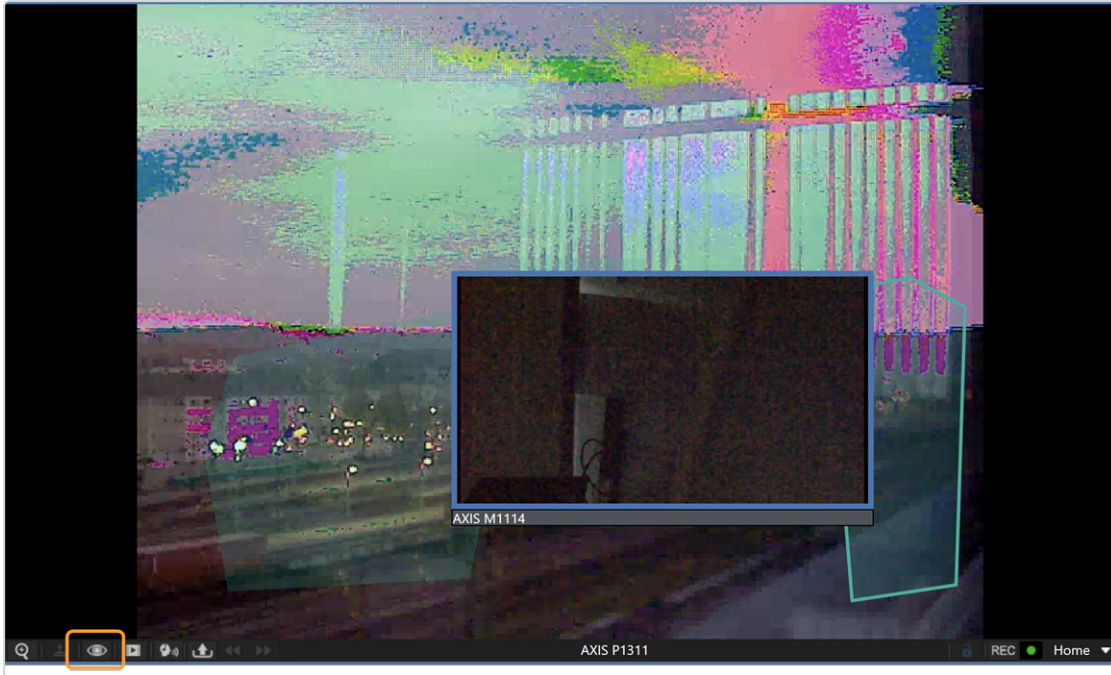
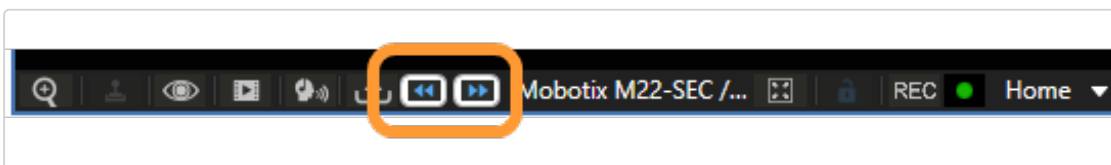


Abb. 66: Click-2-Track im Überwachungsmodus

1. Um Click-2-Track zu starten, wählen Sie die Kachel aus und klicken Sie auf die Kameraoptionen.
2. Wählen Sie **Aktivieren**.
3. Wählen Sie den Bereich auf dem Bild aus, in den sich die Person oder das Objekt bewegt. Das verknüpfte Kamerabild wird in der Vorschau angezeigt.
4. Um das Bild in der Einfügung in die Kachel zu bringen, klicken Sie auf die Vorschau. Click-2-Track bleibt aktiviert.

Historie



Sobald mehrere Kameraregionen besucht wurden, sind die Verlaufsschaltflächen aktiv. Sie werden verwendet, um vorwärts und rückwärts durch den Verlauf dieser Kachel zu navigieren, da jede Kachel eine eigene Geschichte hat.

Wenn Sie den Click-2-Track-Verlauf im Überwachungsmodus verwenden, wird die Kachel zum Mini-Archivplayer umgeschaltet.

Die im Miniarchivmodus angezeigten Vorschaukamas zeigen dieselbe Zeit an wie der Miniarchivplayer.

Benutzerdefinierte Ansichten

Wenn Sie im Überwachungs- oder Archivmodus arbeiten, können Sie benutzerspezifische Ansichten hinzufügen und für jeden Benutzer separat speichern. Diese benutzerdefinierten Ansichten können vom Benutzer ohne zusätzliche Benutzerrechte definiert und gelöscht werden.

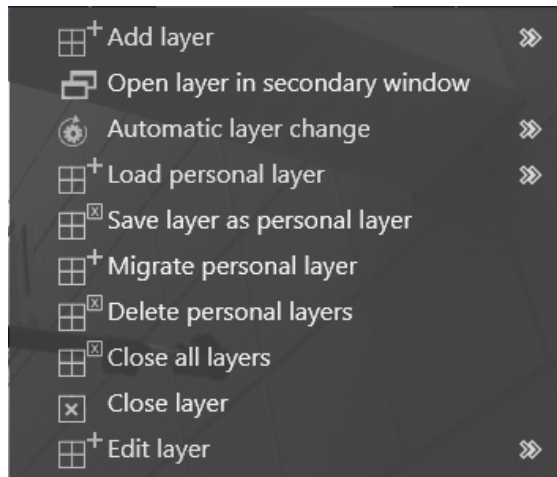
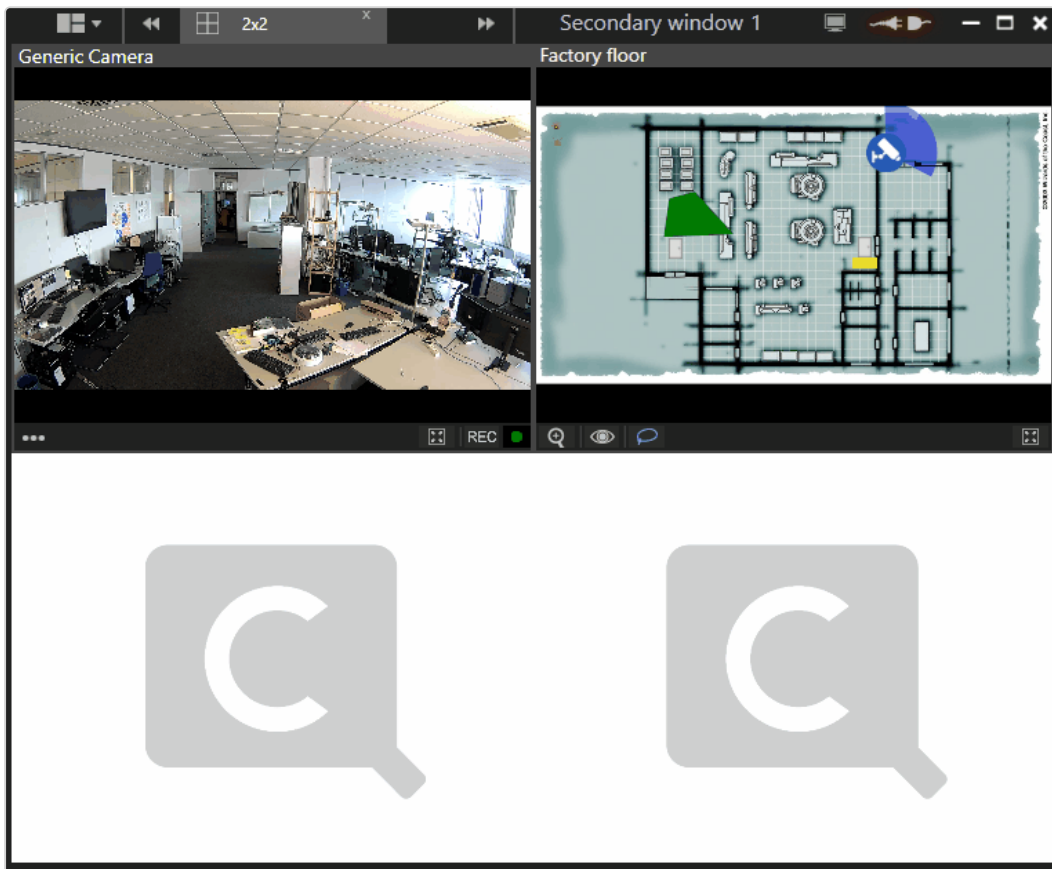


Abb. 67: Benutzerdefinierte Ansichten

1. Um eine Ansicht zu öffnen, wählen Sie **Ansicht** in der oberen Leiste.

Ansicht direkt in einer benutzerdefinierten Ansicht öffnen und schließen



1. Doppelklicken Sie auf ein Fenster, um die Ansicht zu vergrößern.
2. Doppelklicken Sie auf eine vergrößerte Ansicht, um sie auf die voreingestellte Größe zurückzusetzen.

Ansicht hinzufügen

1. Wählen Sie **Ansicht hinzufügen** und wählen Sie die gewünschte Anordnung der Ansichtsfelder aus oder wählen Sie eine benutzerdefinierte Anordnung von Zeilen und Spalten aus. Die neue Ansicht wird angezeigt.
2. Ziehen Sie die Kachel (z. B. Kameraansichten, Webseiten oder Karten) aus der Steuerleiste in die Felder und klicken Sie auf **Ansicht als persönliche Ansicht speichern**, um die neue Ansicht für den aktuellen Benutzer auf dem Server zu speichern.

Migration von lokalen Ansichten

Persönliche Ansichten wurden zuvor als „lokale Ansichten“ benannt. Persönliche Ansichten werden auf dem Server für jedes Benutzerkonto gespeichert, so dass man von jedem Client, in den der Benutzer eingeloggt ist, zugreifen kann.

1. Wählen Sie **Persönliche Ansicht migrieren**, um alle lokalen Ansichten, die sich in `localappdata/qognify` (oder `localappdata/seetec`, wenn es sich um eine ältere Installation handelt) befinden, in die neuen persönlichen Ansichten zu konvertieren. Die `.xml`-Dateien der alten Ansichten-Einstellungen werden nach erfolgreichem Abschluss des Prozesses **ENTFERNT**.

Ansicht erweitern

1. Wählen Sie **Ansicht hinzufügen** und wählen Sie die gewünschte Anordnung der Ansichtsfelder aus oder wählen Sie eine benutzerdefinierte Anordnung von Zeilen und Spalten aus. Die neue Ansicht wird angezeigt.
2. Wählen Sie **Ansicht bearbeiten** und wählen Sie jede optionale Ansicht, die zusätzliche Kacheln bietet (nicht verfügbare Platten werden deaktiviert). Der Tab mit der aktuellen Ansicht wird auf das neue Layout eingestellt.

Ansicht im Nebenfenster öffnen

1. Klicken Sie auf **Ansicht im Sekundärfenster öffnen**, um die neue Ansicht zu einem Sekundärfenster zu verschieben.

Ansicht automatisch wechseln

1. Klicken Sie auf **Automatischer Ansichtenwechsel** und wählen Sie ein Zeitintervall, nach dem die nächste geöffnete Ansicht angezeigt werden soll.

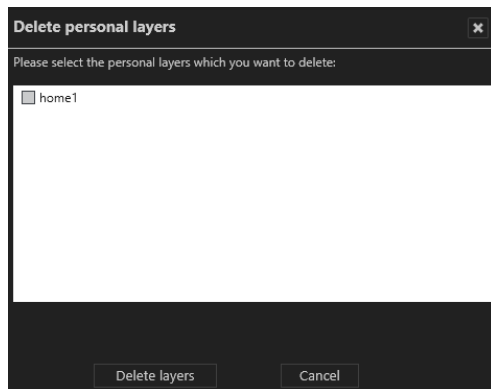
Persönliche Ansicht laden

1. Um eine vorhandene Ansicht zu öffnen, klicken Sie auf **Persönliche Ansicht laden** und wählen Sie die Ansicht.

Persönliche Ansicht löschen

Lokale Ansichten müssen zu persönlichen Ansichten migriert werden, bevor sie gelöscht werden können (siehe [„Migration von lokalen Ansichten“ auf der vorherigen Seite](#)).

1. Um eine Ansicht zu löschen, klicken Sie auf **Persönliche Ansichten löschen**.



2. Wählen Sie die zu löschende(n) Ansicht(en) aus und klicken Sie auf **Ansichten löschen**.

Ansichten schließen

1. Um eine einzelne Ansicht zu löschen, wählen Sie **Ansicht löschen** oder klicken Sie auf die Registerkarte „x“ der Ansicht.
2. Um alle offenen Ansichten zu schließen, wählen Sie **Alle Ansichten schließen**. Nicht gespeicherte Ansichten werden ohne weitere Benachrichtigung geschlossen.

Kamerabildsteuerung

Die Bilder der angeschlossenen und konfigurierten Kameras werden direkt in der Kameraansicht auf der Arbeitsfläche bedient.

Diese Funktionen beziehen sich nur auf die Steuerungsmöglichkeiten mithilfe von Qognify VMS.

Symbole der Kamerabildsteuerung

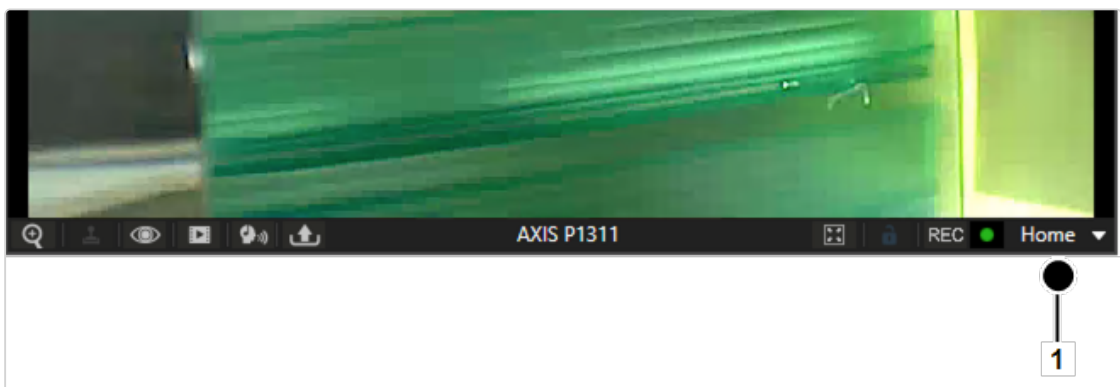











Abb. 68: Symbole der Kamerabildsteuerung

- **Zoom**  . Vergrößert den Bildausschnitt mit Hilfe des digitalen oder optischen Zooms.
 - Der Bildausschnitt wird durch Bewegen des Mausekzes vergrößert oder verkleinert.
 - Bei gedrückter mittlerer Maustaste kann das gezoomte Bild verschoben werden.
 - Optional kann mit gedrückter linker Maustaste im Bild ein Rechteck gezeichnet werden, wodurch in den eingeschlossenen Bereich hineingezoomt wird.
 - PTZ-Kameras können mit der Steuerung oder einem angeschlossenen Joystick bedient werden. Bei einigen PTZ-Kameras ist das Zoomen in einen definierten rechteckigen Bereich in einem Bild mittels optischen Zooms aktiviert.

Der optische Zoom ist nur möglich, wenn er vom jeweiligen Kameramodell unterstützt wird.

- **PTZ**  . Verschiebt den Bildausschnitt in der Ansicht. Der Bildausschnitt kann durch Klicken und Bewegen des Mauszeigers im Bild verändert werden (siehe „Kamerabildsteuerung“ auf der vorherigen Seite). PTZ-Kameras können mit der Steuerung oder einem angeschlossenen Joystick bedient werden (siehe „Kamera im Bild schwenken“ auf Seite 155).
- **Ansichtsoptionen**  . Blendet zusätzliche Optionen ein:
 - **Trackingdaten**: Zeigt die festgelegten und erkannten Regeln für diese Kamera (z. B. Tripwires) in der Ansicht an. Informationen zur Konfiguration finden Sie unter „Qognify Analytics“ auf Seite 327.
 - **Statistik anzeigen**: Zeigt statistische Daten über den Bildstrom zwischen Kamera und Device Manager-Server sowie zwischen Device Manager-Server und Client an (siehe „Kamerabild-Statistik“ auf Seite 156).
 - **Privacy-Masking aktivieren**: Aktiviert oder deaktiviert Privacy-Masking. Die Einstellungen für die Kamera werden im Konfigurationsmodus im Bereich „Kameras“ vorgenommen (siehe „Kameras“ auf Seite 231).
 - **Deselektieren**: Hebt die Auswahl der ausgewählten Kamera auf.
 - **Bild drehen (180°)**: Zeigt das Kamerabild um 180° gedreht an, wenn das ursprüngliche Kamerabild auf dem Kopf stehend angezeigt wird.
 - **In neuem Tab öffnen**: Zeigt die Kamera in einer eigenen Ansicht an.
 - **In Nebenfenster öffnen**: Zeigt die Kamera in einer eigenen Ansicht im ersten Nebenfenster an.
 - **Schließen**: Schließt die aktive Ansicht.
- **Miniarchivmodus**  . Zeigt die Aufzeichnungen des gewählten Intervalls (siehe „Miniarchiv Player“ auf der gegenüberliegenden Seite).
 - Das Intervall kann zwischen 5 und 60 Sekunden betragen und wird durch Klicken auf das Symbol angezeigt bzw. ausgewählt.
 - Bei Auswahl von **Zu Zeitpunkt springen** können Sie direkt zu einem bestimmten Zeitpunkt in der Aufzeichnung springen.
- **Audiomodus**  . Steuert die Audiofunktion der Kameras (Lautstärke/Lautlos/Immer an).
- **Export**  . Exportiert das aktuelle Standbild („Videoframe“) als JPEG oder druckt das angezeigte Standbild.

- **Kachel auf 1x1 Ansicht**  . Vergrößert die Kachel auf die komplette Bildschirmgröße der Arbeitsfläche. Diese Option ist nur verfügbar, wenn die Kachel nicht im Vollbildmodus angezeigt wird.
- **Kamerasperre**  . Sperrt die Kamera für den Benutzer. Durch erneutes Klicken auf das Symbol wird die Kamera für andere Benutzer freigegeben. Die Kamerasperre muss in den Benutzereinstellungen im Konfigurationsmodus aktiviert werden (siehe „Benutzer“ auf Seite 357).
- **REC.** Startet und stoppt die manuelle Aufzeichnung. Eine rote Schaltfläche rechts daneben zeigt, ob die Alarmaufzeichnung gestartet ist.
- **Aufzeichnung Status**  . Zeigt das Aufzeichnungsverhalten für die Kamera an. Ein grüner Punkt steht für Standardaufzeichnung, ein roter Punkt steht für Alarmaufzeichnung (siehe „MultimediaDatabase“ auf Seite 252). Ein rein schwarzer Hintergrund steht für „keine Aufzeichnung“.
- **Positionen (1):** Zeigt die eingestellten Preset-Positionen der gewählten Kamera an. Die Kamerapositionen werden im Konfigurationsmodus im Bereich „Kameras“ eingestellt (siehe „Kamerapositionen/Digitale Presets“ auf Seite 271). Zum Ansteuern der eingestellten Positionen siehe „Kamerasteuerung“ auf Seite 160.

Miniarchiv Player

Der Miniarchiv Player ermöglicht die Steuerung des Abspielvorgangs von einer ausgewählten Kamera. Im Archivmodus sind umfangreichere Archivfunktionen verfügbar (siehe „Archivmodus“ auf Seite 177).

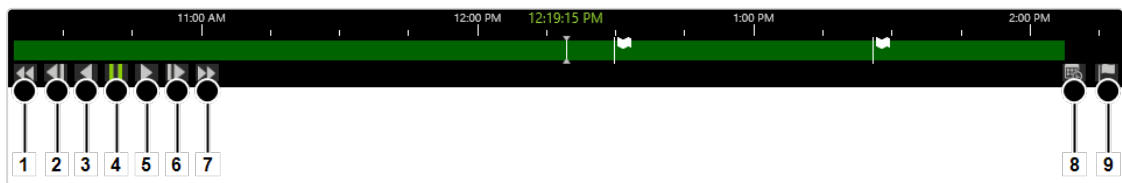


Abb. 69: Miniarchiv Player

Der Miniarchiv Player bietet die folgenden Funktionen:

- **Schneller Rücklauf (1):** Klicken Sie einmal, um die Aufzeichnung in zweifacher Geschwindigkeit rückwärts abzuspielen. Klicken Sie zweimal, um die Aufzeichnung in vierfacher Geschwindigkeit abzuspielen.
- **Einzelschritt rückwärts (2):** Springt einen Einzelschritt oder ein JPEG-Bild des Ereignisses rückwärts.

- **Rückwärts abspielen** (3): Spielt den archivierten Videostream in umgekehrter zeitlicher Reihenfolge ab.
- **Pause** (4): Unterbricht den Abspielvorgang.
- **Vorwärts abspielen** (5): Spielt die archivierte Aufzeichnung in der zeitlich korrekten Reihenfolge ab.
- **Einzelschritt vorwärts** (6): Springt zum nächsten I-Frame oder JPEG-Bild des Ereignisses.
- **Schneller Vorlauf** (7): Klicken Sie einmal, um die Aufzeichnung in zweifacher Geschwindigkeit vorwärts abzuspielen. Klicken Sie zweimal, um die Aufzeichnung in vierfacher Geschwindigkeit abzuspielen.
- **Kalender** (8): Öffnet ein Kalenderfenster, um zu einem bestimmten Zeitpunkt zu springen.
- **Bookmark hinzufügen** (9): Fügt ein Bookmark zum aktuellen Bild hinzu (siehe [„Mit Bookmarks arbeiten“ auf Seite 193](#)).

Manuelle Alarmaufzeichnung

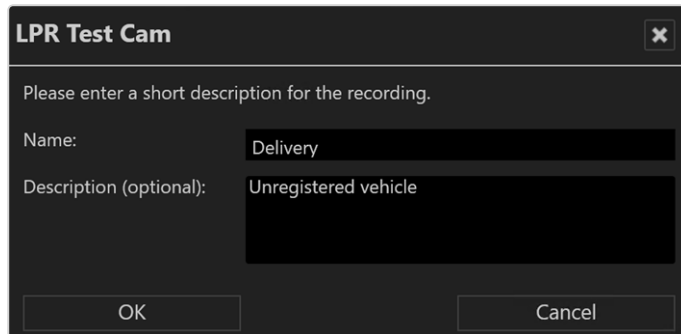
Alarmaufzeichnungen können manuell gestartet und von dem Benutzer, der sie gestartet hat, gestoppt werden. Darüber hinaus können Bookmarks zur Aufzeichnung hinzugefügt werden. Bookmarks können für die Suche im Archivmodus verwendet werden (siehe [„Alarme suchen“ auf Seite 190](#)).

Manuelle Alarmaufzeichnung starten

1. Klicken Sie auf die Schaltfläche **REC** (10, siehe oben). Eine rote Glocke zeigt rechts daneben, ob die Alarmaufzeichnung gestartet ist.

Um eine unbegrenzte Aufnahme zu verhindern, muss im Konfigurationsmodus in den Kameraeinstellungen die maximale Nachalarm-Dauer festgelegt werden (siehe [„MultimediaDatabase“ auf Seite 252](#)).

- Optional können Sie auf **Bookmark hinzufügen** klicken. Ein Fenster mit Bookmark-Informationen wird angezeigt.





- Geben Sie den Namen und eine kurze Beschreibung für das Bookmark ein.
- Fügen Sie das Bookmark mit **OK** zur Aufzeichnung hinzu.

Manuelle Alarmaufzeichnung stoppen

- Klicken Sie erneut auf die Schaltfläche **REC**. Die Aufnahme wird gestoppt.
- Optional können Sie ein Bookmark hinzufügen.



Kamera im Bild schwenken

Die Kamera kann im Bild geschwenkt und geneigt werden (Pan/Tilt Modus). Das Drehen der Kamera zur Seite wird als „Schwenken“ bezeichnet (erzeugt einen Panoramaeffekt) und das Drehen der Kamera nach oben oder unten als „Neigen“.

- Klicken Sie auf **PTZ** . In der Mitte des Bilds erscheint ein rotes Kreuz.
- Klicken Sie auf eine Stelle neben dem Kreuz. Die Entfernung des Klicks zum Mittelpunkt des Kreuzes bestimmt die Geschwindigkeit des Schwenkvorgangs in die jeweilige Richtung.
- Aktivieren Sie gegebenenfalls die Zoom-Funktion der PTZ-Kamera. Zoomen Sie das Bild mit dem Mausrad hinein bzw. heraus.
- Klicken Sie erneut auf **PTZ** , um die Schwenkfunktion im Bild zu deaktivieren.

Wenn diese in der PTZ-Kamera konfiguriert ist, wird der Name des Benutzers während des Vorgangs im Bild angezeigt. Bei Interaktionen, die nicht vom Benutzer ausgeführt werden, wie Alarmszenarien oder Sequenzen, wird „System“ angezeigt.

Kamerabild-Statistik

1. Wählen Sie in der Symbolleiste der Kamera die **Ansichtsoptionen** .
2. Wählen Sie **Statistik anzeigen**. Das Statistikfenster bleibt offen.
3. Schließen Sie das Statistikfenster, indem Sie in den **Ansichtsoptionen**  die Option **Statistik anzeigen** abwählen.

Die Kamerabild-Statistik zeigt Informationen über Folgendes:

- Die Videobilder, die vom Client dargestellt werden. Der Wert für **Dekodierung (fps)** sollte dem Wert für **Rendern (fps)** entsprechen.
- Die Videobilder, die auf dem Server aufgezeichnet werden
- Die Qualität des Audiostreams
- Die Netzwerkqualität. Das **Paketverlustverhältnis (%)** sowie der **Maximalwert. Jitter (ms)**-Wert sollten so niedrig wie möglich sein. Hohe Werte weisen auf Netzwerkprobleme hin, z. B. kann Jitter durch elektromagnetische Störungen und durch das Übersprechen mit Trägern anderer Signale hervorgerufen werden.

Lagepläne

Ein Lageplan stellt einen zu überwachenden Bereich dar. Er wird im Konfigurationsmodus als einfache Grafik in die Software eingefügt (siehe „[Lagepläne und „Erweiterte Lagepläne“](#)“ auf Seite 407 im Konfigurationsmodus). In diese Grafik werden dann die jeweiligen Kameras und andere Funktionssymbole eingebunden. Der Lageplan kann somit die unterschiedlichsten Unternehmensbereiche grafisch darstellen, angefangen beim Betriebsgelände bis hin zu voll automatisierten Produktionsstraßen.

Der Lageplan zeigt die Kameras an, die der Benutzer bedienen kann.

Ist eine Kamera ausgefallen (Stromausfall, keine Netzwerkverbindung o. Ä.), wird das Kamerasymbol mit einem gelben Warnsymbol dargestellt.

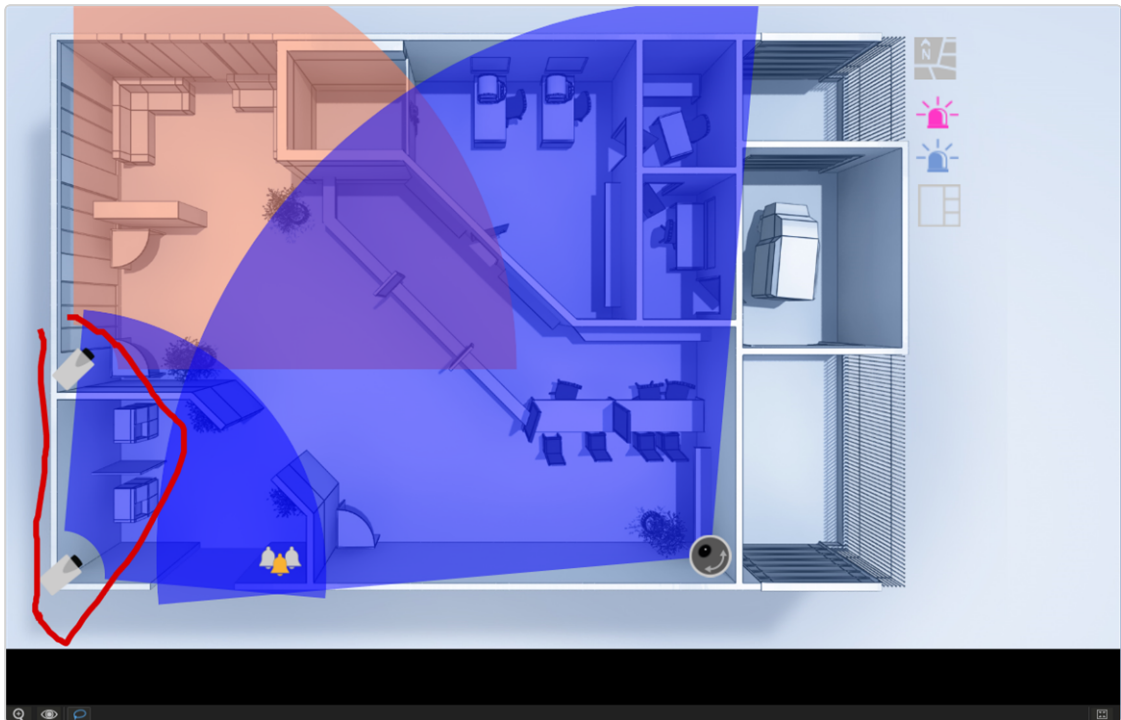






Abb. 70: Lagepläne

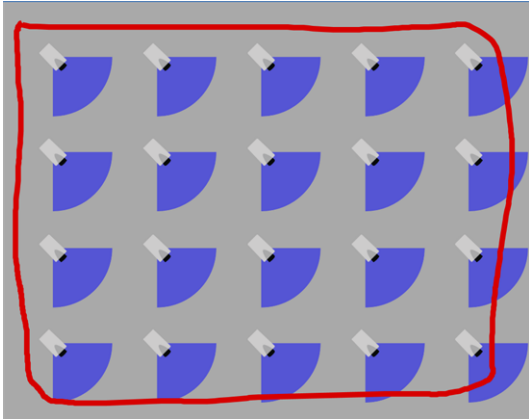
1. Wählen Sie **Digitaler Zoom** (), um die Zoom-Funktion für den Lageplan zu aktivieren.
2. Vergrößern bzw. verkleinern Sie die Details im Lageplan durch Drehen des Mausekkrads, während sich der Mauszeiger auf dem Lageplanbereich befindet.
3. Wählen Sie **Ansichten-Optionen** (), um den Lageplan auf einer neuen Registerkarte oder in einem neuen Fenster zu öffnen oder die Ansicht zu schließen.
4. Wählen Sie **Lasso-Auswahl erstellen** (), um die Lasso-Funktion zu aktivieren. Die Lasso-Funktion ist standardmäßig aktiviert.
5. Zeichnen Sie ein Lasso um die Kameras, die in einer Ansicht angezeigt werden sollen (siehe „Lasso“ verwenden“ auf der nächsten Seite).
6. Wählen Sie **Window auf 1x1 Ansicht** (), um die Größe des Bildes zu vergrößern, um den gesamten Arbeitsbereich zu füllen.


Kameravoransicht anzeigen

1. Bewegen Sie den Mauszeiger im Lageplan auf die gewünschte Kamera. Eine Voransicht des Kamerabilds wird angezeigt.
2. Klicken Sie auf das Kamerasymbol, um das Kamerabild in einer neuen Ansicht zu öffnen.

„Lasso“ verwenden

Bis zu 16 Kameras können mit der Lasso-Auswahl „eingefangen“ werden.








1. Klicken Sie auf **Lasso-Auswahl erstellen** , um die Lasso-Funktion zu aktivieren.
2. Bewegen Sie den Mauszeiger mit gedrückter linker Maustaste um die Kameras, die Sie auswählen möchten. Die Mauszeigerbewegung wird mit einer roten Linie hervorgehoben.
3. Lassen Sie die Maustaste los. Die gewählten Kamerabilder werden in einer neuen Ansicht angezeigt.

Webseiten

In der Webseitenansicht kann der Benutzer innerhalb festgelegter Kacheln bestimmte Webseiten aufrufen, um beispielsweise Informationen zum Unternehmen zu erhalten. Die angezeigten Webseiten (Internet oder Intranet) werden im Konfigurationsmodus festgelegt (siehe „[Webseiten](#)“ auf Seite 420).

1. Navigieren Sie innerhalb der Webseiten wie in einem Browser. Die browserartige Navigationsleiste wird nicht angezeigt.

- Um die Seite in einer eigenen Ansicht anzuzeigen, klicken Sie auf **Vollbild**. Folgende Navigationselemente stehen zur Verfügung:
 - **Zurück**  : Wechselt zur vorherigen Seite.
 - **Nächste**  : Wechselt zur nächsten Seite.
 - **Startseite**  : Kehrt zur Startseite zurück. Die Startseite ist die im Konfigurationsmodus definierte Seite.
 - **Neu laden**  oder **Laden abbrechen**  : Lädt erneut die angezeigte Seite oder stoppt das Laden der Seite. Ein erneutes Laden ist erst möglich, nachdem die Seite geladen wurde. Wenn die Seite zu langsam lädt, kann das Laden abgebrochen werden.

Übersicht

Im Steuerelement **Übersicht** werden alle vorhandenen Kameras, Lagepläne, Ansichten und Webseiten nach den Standorten des Unternehmens gegliedert angezeigt.

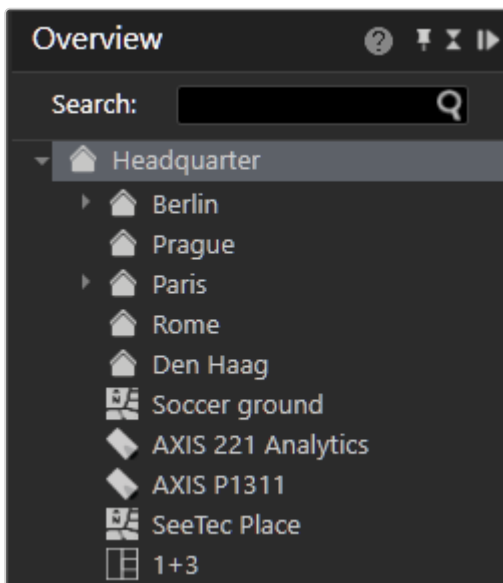


Abb. 71: Übersicht

- Klicken Sie auf das kleine Dreieck vor dem Namen des Standorts, um alle Objekte anzuzeigen, die diesem Standort zugewiesen sind.
- Wählen Sie ein Objekt aus der Liste aus, um nur dieses anzeigen zu lassen.

Element suchen

Bei der Konfiguration des Systems sollte jedes Element eine eigene Bezeichnung erhalten haben.



Abb. 72: Objekt suchen






1. Um ein bestimmtes Element zu suchen, geben Sie die Bezeichnung des Elements in das Textfeld **Suchen** ein (siehe „Suchen im Überwachungsmodus“ auf Seite 174).

Kamerasteuerung



Abb. 73: Kamerasteuerung

Mit der **Kamerasteuerung** kontrollieren Sie die aktiven Kameras, die auf der Arbeitsfläche angezeigt werden.

- **PTZ**  : startet die PTZ-Steuerung, um PTZ-Kameras zu bedienen
- **Buttons**  : startet die Button-Funktion, zum Triggern von Preset-Prozessen
- **Wächterrundgang**  : startet die Wächterrundgang-Funktion zum Starten verschiedener Überwachungsvorgänge
- **Audio-Modus**  : startet den Audio-Modus für die Kommunikation
- **Dispatcher**  : startet den Dispatcher-Modus zum Bedienen der Videowand

PTZ-Steuerung

Ausgewählte PTZ-Kameras werden mit Hilfe der PTZ-Steuerung bedient. PTZ-bezogene Funktionen sind nur für PTZ-Kameras verfügbar. Wenn keine PTZ-Kamera ausgewählt oder die PTZ-Funktion der Kamera deaktiviert ist, sind nur Digitalzoom und die Auswahl digitaler Presets möglich.

PTZ-Steuerung verwenden

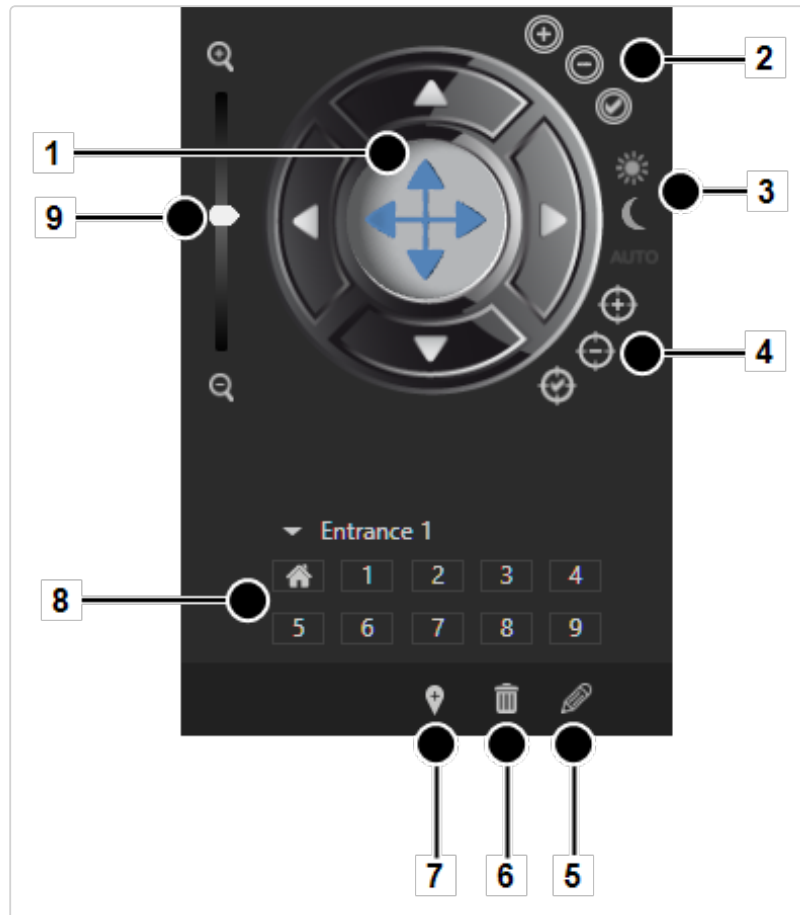


Abb. 74: PTZ-Steuerung verwenden

1. Klicken Sie in der Menüleiste des Steuerelements auf das **PTZ-Steuerung**, um in den Bedienmodus der Kameras zu wechseln.
2. Markieren Sie das Kamerabild und bewegen Sie die Kamera mit der **PTZ-Steuerung** (1), indem Sie die helle Fläche in die gewünschte Richtung verschieben.
3. Ziehen Sie den Regler **Zoom** (9) nach oben oder unten, um das Bild mit Hilfe der Kamera zu vergrößern oder zu verkleinern. Optional können Sie die Kamera schrittweise mit Hilfe der vier Richtungspfeile an der PTZ-Steuerung bewegen.

Preset-Positionen verwenden

Einschließlich der Standardposition sind im Nummernfeld (8) zehn Preset-Positionen zur direkten Auswahl verfügbar. Im Aufklappmenü stehen möglicherweise

noch mehr zur Verfügung. Die maximale Anzahl der Presets ist abhängig von der Kamera. Informationen zum Bearbeiten von Preset-Positionen im Überwachungsmodus finden Sie unter [„Kamera-Preset-Positionen bearbeiten“ auf der gegenüberliegenden Seite](#). Im Allgemeinen werden die Positionen von einem Administrator im Konfigurationsmodus (siehe [„Konfigurationsmodus“ auf Seite 207](#)) im Bereich **Kamera** eingestellt (siehe [„Kameras“ auf Seite 231](#)).

1. Klicken Sie im Nummernfeld (8) auf die gewünschte Kameraposition, um einen Kameraschwenk auf die gewählte Position durchzuführen.
2. Optional können Sie auf das Dreieck neben dem Positionsnamen klicken und im Aufklappmenü die gewünschte Position auswählen. Die Position wird sofort angefahren.

Preset-Positionen einer Kamera in einer einzigen Ansicht verwenden

Statt für eine 360°-Ansicht eine Fisheye-Kamera zu verwenden, können mehrere Kamerastandbilder in einer einzigen Ansicht kombiniert werden (Informationen zu Ansichten im Überwachungsmodus finden Sie unter [„Benutzerdefinierte Ansichten“ auf Seite 147](#)).

Beim Speichern einer Ansicht wird auch die Kameraposition (digitales Preset, Digitalzoom, Dewarping-Position) gespeichert. Wenn die Ansicht wieder geöffnet wird, wird an derselben Position fortgefahren.

Dies gilt für gespeicherte Ansichten im Konfigurationsmodus sowie für persönliche Ansichten. Ansichten, die per Drag & Drop in eine Videowand eingefügt werden, behalten die digitale Kameraposition auf der Videowand bei.

Einstellung von Belichtung und Fokus

Die folgenden Belichtungs- und Fokuseinstellungen sind nur verfügbar, wenn sie von der Kamera unterstützt werden.

- **Iris-Einstellungen (2)**
 - **Iris +, Iris -:** Öffnet oder schließt die Iris der Kamera, um die Helligkeit zu regeln.
 - **Auto Iris:** Passt die Irisöffnung automatisch an die optimale Helligkeit der Umgebung an.
 - **AutoFokus:** Passt die Bildschärfe automatisch an die Gegenstände im Kamerafokus an.

- **Einstellungen für Tag- und Nachtmodus (3)**
 - **Tagmodus, Nachtmodus:** Die Kamera wendet einen Filter an, wenn die Lichtverhältnisse schlecht sind.
 - **Auto:** Die Kamera schaltet automatisch zwischen Tag- und Nachtsicht um.
- **Fokuseinstellungen (4)**
 - **Fokus nah, Fokus fern:** Passt die Bildschärfe abhängig vom Abstand des Gegenstands zum Sensor-Chip der Kamera an die Gegenstände im Kamerafokus an.
 - **AutoFokus:** Passt die Bildschärfe automatisch an die Gegenstände im Kamerafokus an.

Kamera-Preset-Positionen bearbeiten

Kamera-(Preset-)Positionen können abhängig von den Benutzerrechten definiert (4), gelöscht (5) und bearbeitet (6) werden (siehe „[Benutzerrechte verwalten](#)“ auf [Seite 361](#)).

Preset der Kameraposition anlegen

1. Bewegen Sie die Kamera mit der PTZ-Steuerung (1) in die gewünschte Position.
2. Klicken Sie auf **Neue Kameraposition hinzufügen** (7). Die neue Kameraposition wird auf die nächste freie Positionsnummer gelegt.
3. Geben Sie einen Namen für die Position ein und klicken Sie auf **OK**. Die neue Kameraposition wird auf die nächste freie Positionsnummer gelegt.

Preset der Kameraposition löschen

1. Wählen Sie die Position aus dem Nummernfeld oder aus dem Aufklappmenü aus.

2. Klicken Sie auf **Löschen** (6). Die gelöschte Kameraposition wird freigegeben und nachfolgende Positionen „rutschen“ nach.

Beispiel Position 3 wird gelöscht. Daraufhin wird Position 4 auf 3 und 5 auf 4 usw. verschoben.

Preset der Kameraposition bearbeiten

1. Wählen Sie die Position aus dem Nummernfeld oder aus dem Aufklappmenü aus.
2. Klicken Sie auf **Aktuelles Preset bearbeiten** (5).
3. Bearbeiten Sie die Position, indem Sie den Namen der Position, die PTZ-Einstellungen, die Fokuseinstellungen usw. ändern.
4. Klicken Sie auf **Aktuelle Änderungen speichern**.

Buttons

Aktionen und Prozesse über Buttons starten

Aktionen oder definierte Prozesse wie Kameraaufzeichnungen oder Alarmszenarien werden mit Hilfe von Buttons gestartet.

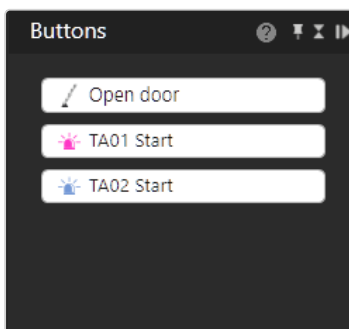


Abb. 75: Buttons

1. Klicken Sie in der Menüleiste des Steuerelements **Steuerung** auf **OK**, um zur Anzeige der angelegten Buttons zu wechseln. Zur Konfiguration der Buttons siehe „Buttons“ auf Seite 416.


2. Es werden die Buttons angezeigt, die der Benutzer entsprechend seiner Berechtigung verwenden darf.
3. Aktivieren Sie die gewünschte Aktion durch Klicken des Buttons.

Wächterrundgang


Wächterrundgänge können Kameras, eingestellte Positionen, Lagepläne und Ansichten nacheinander für einen bestimmten Zeitraum anzeigen. Zusätzlich ist es möglich, innerhalb eines Rundgangs digitale Ausgänge zu öffnen oder zu schließen und Kontrollpunkte zu bestätigen.

1. Klicken Sie in der Menüleiste der Steuerung auf **Wächterrundgang**, um zur Übersicht der konfigurierten Wächterrundgänge zu wechseln. Zur Konfiguration der Wächterrundgänge siehe „[Wächterrundgänge](#)“ auf Seite 422.


Wächterrundgang starten

1. Wählen Sie den gewünschten Rundgang und klicken Sie auf **Abspielen** . Die festgelegten Kameras, Presetpositionen, Lagepläne und Ansichten werden nacheinander für den angegebenen Zeitraum angezeigt.



Wächterrundgang stoppen

1. Wählen Sie **Stopp** , um den gewählten Rundgang abubrechen.



Wächterrundgang anhalten

1. Wählen Sie **Pause** , um den Rundgang zu unterbrechen. Der Wächterrundgang wird angehalten.

Wächterrundgang wiederholen

1. Wählen Sie **Schleife** . Der Rundgang wird wiederholt.
2. Wählen Sie erneut **Schleife** . Die Wiederholung wird aufgehoben und der Wächterrundgang nach dem aktuellen Durchlauf gestoppt.

Zwischen Positionen des Wächterrundgangs navigieren

1. Wählen Sie **Zurück**  oder **Vorwärts** , um zum vorherigen oder nächsten Element in der Liste zu springen.

Audio

1. Klicken Sie in der Menüleiste des Steuerelements **Steuerung** auf **Audio**, um in den Audiomodus zu wechseln.

Für Audio sind folgende Optionen verfügbar (sofern von der Hardware unterstützt):

VoIP

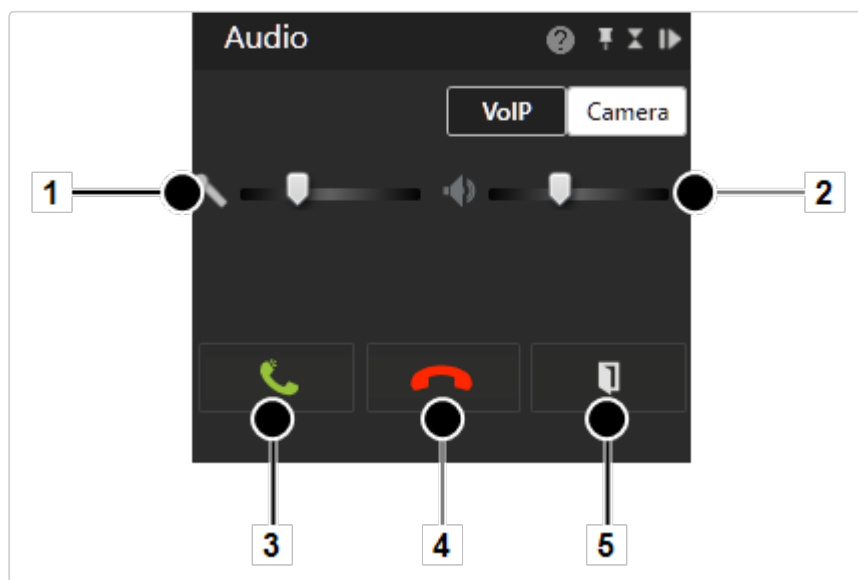


Abb. 76: VoIP

1. Wählen Sie **VoIP**, um die Sprachausgabe im Netzwerk („Voice over IP“) auszuwählen.

2. Verschieben Sie die Regler für **Mikrofon** (1) und **Lautsprecher** (2), um die Lautstärke anzupassen. Die Lautstärkeeinstellung wird für jeden Client lokal gespeichert.
3. Um mit einer Person aus dem Adressbuch der vorhandenen Benutzer zu sprechen, geben Sie den Namen der Person im Textfeld ein und klicken Sie auf das Lupensymbol oder wählen Sie eine Person aus der Liste aus.
4. Beginnen Sie das Gespräch, indem Sie auf den **grünen Telefonhörer** (5) klicken.
5. Beenden Sie das Gespräch, indem Sie auf den **roten Telefonhörer** (4) klicken. Der Name des Gesprächspartners, sein Standort und die Dauer des Gesprächs werden angezeigt (2).
6. Klicken Sie auf **DTMF** (3), um eine DTMF-Sequenz zu senden oder eine Buttonaktion aufzurufen. Die Sequenz oder Buttonaktion wird von einem Administrator in der VoIP-Konfiguration festgelegt (siehe [VoIP](#)).

Kamera

Wenn von der Kamera unterstützt, ist eine Audioübertragung vom Client zur Kamera möglich (zur Konfiguration der Push-to-Talk-Funktion siehe „[Audio](#)“ auf [Seite 271](#)).

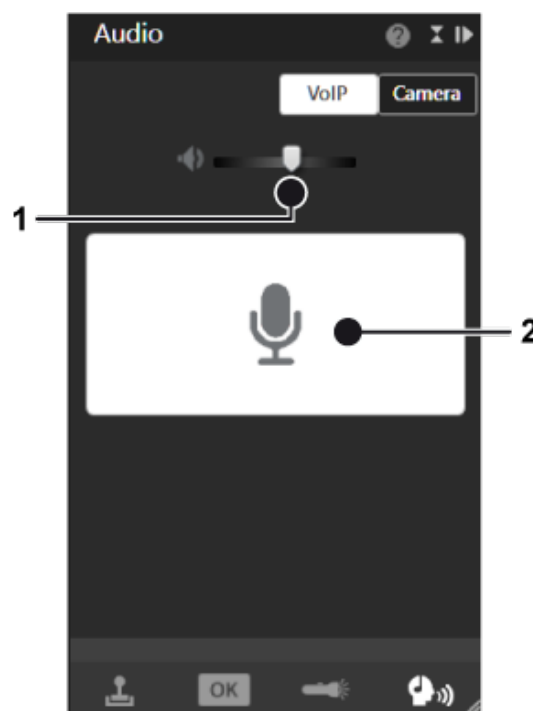


Abb. 77: Kamera

1. Wählen Sie **Kamera**, um das direkte Audiosystem der Kamera auszuwählen (sofern verfügbar).
2. Verschieben Sie den Regler für den Lautsprecher (1), um die Lautstärke anzupassen. Die Lautstärkeeinstellung wird für jede Kamera lokal gespeichert.
3. Um die Audiokommunikation mit der Kamera zu starten, halten Sie die Sprechtaste (2) gedrückt.
4. Um die Audiokommunikation mit der Kamera zu stoppen, lassen Sie die Sprechtaste (2) wieder los.

Dispatcher-Modus

Der Dispatcher-Modus wird nur angezeigt, wenn der Videowall Dispatcher im Menü „Ansicht“ aktiviert ist (siehe „[Videowall Dispatcher](#)“ auf Seite 93). Darüber hinaus muss mindestens eine Videowand im Konfigurationsmodus angelegt worden sein (siehe „[Videowände](#)“ auf Seite 430).

Dispatcher-Modus verwenden

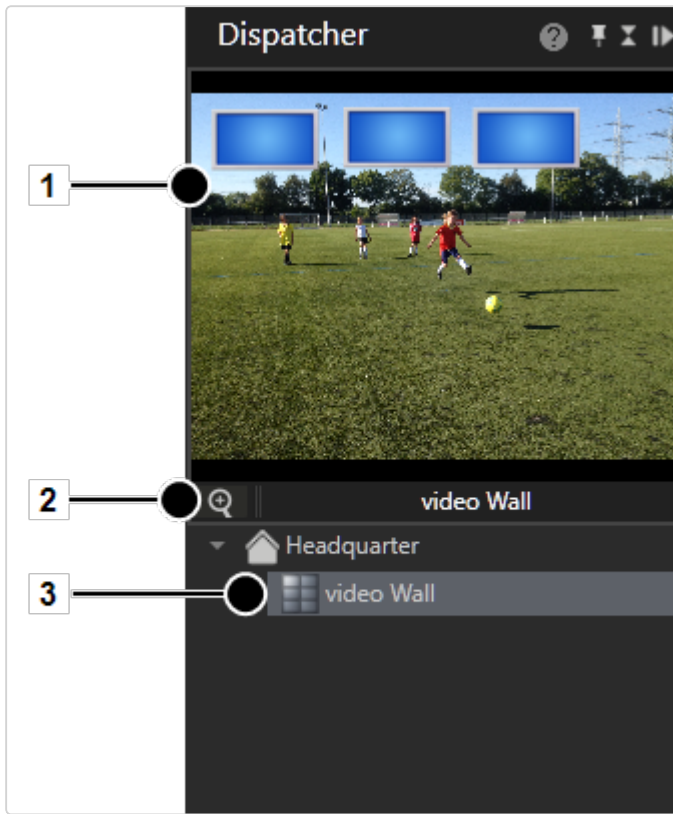
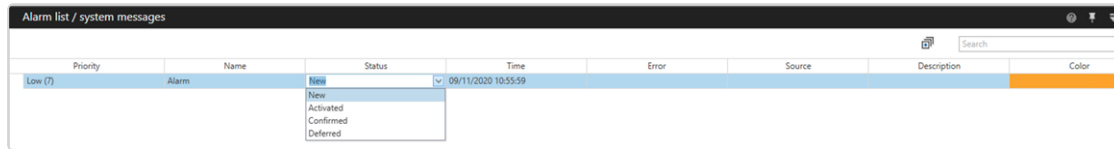


Abb. 78: Dispatcher-Modus

1. Klicken Sie in der Menüleiste des Steuerelements auf **Dispatcher-Modus**, um in die Steuerung der Videowände zu wechseln.
2. Wählen Sie die eingestellte Videowand (3) aus. Die Videowand wird einschließlich der darin befindlichen Monitore (1) angezeigt.
3. Klicken Sie zum Vergrößern oder Verkleinern des Bildausschnitts auf **Digitalzoom** (2) und drehen Sie das Mausrad.
4. Drücken Sie die Maustaste und ziehen Sie die Anzeigesymbole nach links oder rechts, um die angrenzenden Anzeigen zu sehen.
5. Ziehen Sie die gewünschten Videoquellen, Ansichten und Lagepläne auf den jeweiligen Monitor in der Miniaturansicht (1).
6. Öffnen Sie gegebenenfalls die Darstellung des jeweiligen Monitors durch Klicken auf den Monitor. Der Monitor mit den darin aufgeschalteten Ansichten wird in der Arbeitsfläche dargestellt. Sie können auch die Videoquellen, Ansichten und Lagepläne direkt in die Arbeitsfläche ziehen, wenn der Monitor der Videowand angezeigt wird.


Alarmliste und Systemmeldungen



Priority	Name	Status	Time	Error	Source	Description	Color
Low (7)	Alarm	New	09/11/2020 10:55:59				

Abb. 79: Alarmliste und Systemmeldungen

Die Alarmliste befindet sich am unteren Bildschirmrand und kann bei Bedarf ein- oder ausgeklappt werden. Sie zeigt die Alarm- und Systemmeldungen in der Reihenfolge ihres Auftretens an. Die neuesten Alarme werden zuerst angezeigt. Zusätzlich wird im Icon Überwachungsmodus in der Modusleiste die Anzahl der aufgetretenen Alarme angezeigt.

1. Um die Alarm- bzw. Systemmeldungen nach der Kategorie der Spalte zu sortieren, klicken Sie auf die jeweiligen Spaltentitel.
2. Um den Status der Alarmmeldungen zu ändern, wählen Sie das Objekt in der Spalte **Status** aus und wählen Sie dann im Aufklappmenü den Status aus.
3. Um die Alarmliste zu minimieren oder zu erweitern, klicken Sie auf **Alles erweitern/minimieren**  .

Alarmmeldungen

In den Alarmmeldungen werden alle offenen Alarme angezeigt, die dem aktuell angemeldeten Profil zugeordnet wurden (siehe „[Beteiligte Personen](#)“ auf Seite 398). Die Art der Alarme kann farblich unterschieden werden. Die angezeigte Farbe des Alarms legen Sie im Konfigurationsmodus im Steuerelement Alarme fest (siehe „[Alarme](#)“ auf Seite 386).

Alarmstatus ändern

Ein Alarm besitzt die folgenden Statuszustände:

- **Aktiviert:** Dieser Alarm ist gerade aktiv.
- **Bestätigt:** Diese Alarme wurden gesichtet und werden aus der Alarmliste entfernt. Bestätigte Alarme werden bei allen Benutzern aus der Liste entfernt.

- **Zurückgestellt:** Diese Alarme wurden bereits gesichtet und vom jeweiligen Benutzer (z. B. Wachmann) als wichtig deklariert, da er diese (evtl. für seinen Wachbericht) zu einem späteren Zeitpunkt noch benötigt. Diese Alarme werden weiterhin in der Alarmliste gehalten. Zurückgestellte Alarme sind beim nächsten Start wieder als offen deklariert.
- **Abgelehnt:** Diese Alarme werden aus der Alarmliste entfernt und vom Benutzer als unwichtig bzw. ihm nicht zugehörig angesehen.

1. Klicken Sie in der Alarmliste auf den Eintrag in der Spalte **Status**, um den Status der Alarmmeldungen zu ändern.
2. Optional können Sie auf **Alle bestätigen** klicken, um die Alarme zu bestätigen. Dadurch wird der rote Kreis, in dem die Anzahl der unbestätigten Alarme angezeigt wird, ausgeblendet.

Klassifizierung eines Alarms

Jeder Alarm in der Alarmliste kann anhand der definierten Kategorien klassifiziert werden (siehe „[Konfigurieren der Alarm-Klassifizierungen](#)“ auf Seite 465).

1. Wählen Sie den Alarm in der Alarmliste aus.
2. Wählen Sie die Kategorie aus der Dropdown-Liste in der Spalte **Klassifizierung**.

Meldungsfenster (Pop-Up)

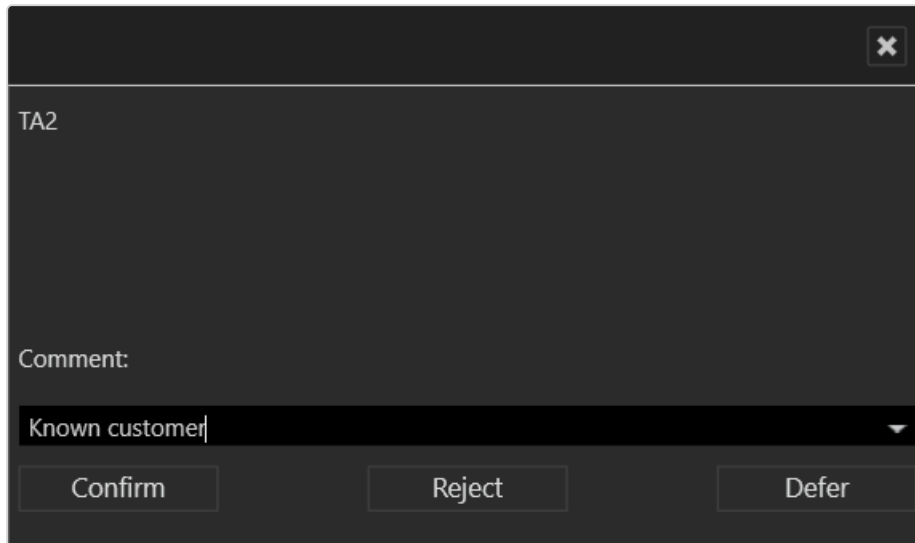


Abb. 80: Meldungsfenster (Pop-Up)

Sobald ein Alarm auftritt, wird bei Alarmen mit hoher und mittlerer Priorität ein Meldungsfenster angezeigt.

Alarme mit niedriger Priorität werden nach Alarmende aus der Alarmliste gelöscht, wenn sie bestätigt sind und ein anderer Alarm auftritt. Alarme mit niedriger Priorität besitzen keinen Alarmstatus.

Sie können einen Kommentar für diesen Alarm angeben. Der Kommentar wird in der Ereignisauswertung und im Archivmodus angezeigt.

1. Um den Alarm zu bestätigen, klicken Sie auf **Bestätigen**. Der Alarm wird aus der Alarmliste gelöscht und der nächste Alarm wird angezeigt.
2. Sie können den Alarm **ablehnen**. Der Alarm wird aus der Alarmliste gelöscht und der nächste Alarm wird angezeigt.
3. Sie können den Alarm **zurückstellen**. Der Alarm wird in der Alarmliste als zurückgestellt markiert. Es wird kein weiterer Alarm angezeigt, bis entweder ein Alarm aus der Alarmliste aufgerufen oder bestätigt wird. Dies gibt die Möglichkeit, mehrere Alarme gleichzeitig zu bestätigen.

Alarmbenachrichtigung

Ein neu aufgetretener Alarm wird in einem hellen Meldungsfenster angezeigt, das vom unteren Bildschirmrand aufklappt (Alarmbenachrichtigung).

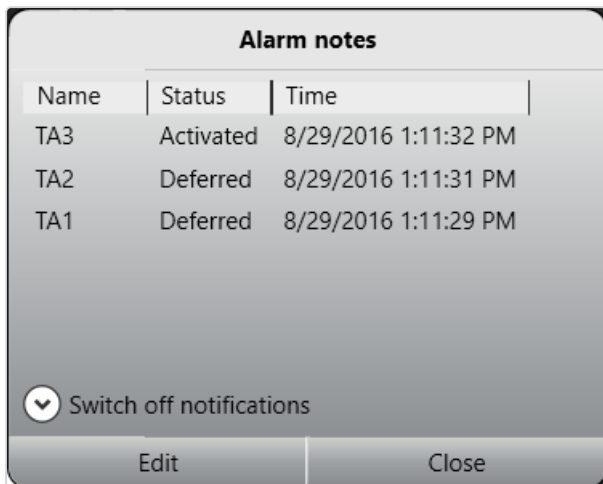


Abb. 81: Alarmbenachrichtigung

Im Meldungsfenster werden der Name, der Status und der Zeitpunkt des Auftretens des Alarms angezeigt.

1. Wenn keine Alarmbenachrichtigungen am Bildschirm angezeigt werden sollen, klicken Sie auf **Benachrichtigungen ausschalten**.
2. Wählen Sie aus, wie lange die Alarmbenachrichtigungen ausgeblendet werden sollen („Snooze“). Nach Ablauf der gewählten Zeitspanne werden die Alarmbenachrichtigungen wieder angezeigt.
3. Wählen Sie den Alarm aus und klicken Sie auf **Bearbeiten**, um das Meldungsfenster zur Bearbeitung anzeigen zu lassen.
4. Klicken Sie auf **Schließen**, um das Meldungsfenster zu schließen.

Systemmeldungen

In den Systemmeldungen werden die Fehler angezeigt, die vom System gemeldet wurden, beispielsweise der Ausfall eines Servers, einer Datenbank oder einer Kamera, sowie Verbindungsverluste.

Die Fehler werden nach dem Zeitpunkt ihres Auftretens in absteigender Reihenfolge einschließlich ihrer Beschreibung, der jeweiligen internen Fehlernummer, der Nachricht und der Fehlerquelle angezeigt.

1. Wählen Sie eine oder mehrere Systemmeldungen aus und klicken Sie auf **Entfernen ausgewählt**, um die Meldung(en) aus der Liste zu entfernen. Die Zahl im roten Kreis, in dem die Anzahl der unbestätigten Meldungen angezeigt wird, verringert sich entsprechend.

- Optional können Sie auf **Alle entfernen** klicken, um alle Systemmeldungen aus der Liste zu entfernen. Dadurch wird der rote Kreis, in dem die Anzahl der unbestätigten Systemmeldungen angezeigt wird, ausgeblendet.

Suchen im Überwachungsmodus

Die Suche unterhalb des Tabs „Übersicht“ in der Steuerleiste hilft Ihnen dabei, die Inhalte der jeweils aktiven Steuerleiste schneller zu finden.

Wenn Entitäten, wie z. B. Kameras, Etiketten zugewiesen wurden, können diese für die Suche verwendet werden, um sie einzugrenzen.

Die Suche nach Etiketten wird nicht angezeigt, wenn keine Etiketten konfiguriert sind oder keine Entitäten einer Etikette zugewiesen wurden.

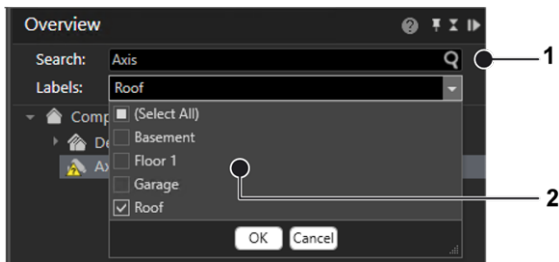


Abb. 82: Suchen im Überwachungsmodus

- Geben Sie im Suchfeld (1) einen Suchbegriff ein. Der erste gefundene Begriff in der Übersicht wird hervorgehoben.
- Klicken Sie auf die Lupe rechts neben dem Suchfeld oder drücken Sie [Enter] auf der Tastatur, um den nächsten Begriff in der Übersicht hervorzuheben.

3. Falls konfiguriert, wählen Sie eine oder mehrere Etiketten aus der Dropdown-Liste „Etiketten“ (2) und wählen dann **OK**. Sie können die Suche im Suchfeld und die Etikettenfilterung kombinieren, um die Ergebnisse einzugrenzen. Es werden nur Ergebnisse angezeigt, die sowohl den Suchtext als auch die Etiketten enthalten (UND Zuordnung).
 - Das Filtern nach einer Entität anhand einer Etikette zeigt die Entitäten für diese Etikette an, auch wenn sie mit mehr als einer Etikette versehen sind.
 - Wenn Sie nach einer Entität mit Mehrfachetiketten filtern, werden die Entitäten angezeigt, denen eine oder mehrere Etiketten zugeordnet sind.
 - Die gleichzeitige Verwendung des Suchbegriffs und der Etiketten zeigt die Entitäten mit dem Suchbegriff und die Entitäten mit den zugeordneten Etiketten an.

Sie können nur Etiketten für Entitäten sehen, für die Sie die entsprechenden Benutzerrechte besitzen.

Anzeige der Suchergebnisse in einer temporären Ebene

1. Verschieben Sie per Drag & Drop die Entität oder den dort enthaltenden Ordner oder Zweig auf den Arbeitsbereich. Das Suchergebnis öffnet eine neue Ebene. Wenn sich die Ergebnisse in einem Ordner oder einem Zweig befinden, können Sie den gesamten Zweig oder den Ordner per Drag & Drop auf den Arbeitsbereich ziehen. Es werden jedoch nur die gefilterten Ergebnisse angezeigt.

Wenn 4 Ebenen mit jeweils bis zu 16 Suchergebnissen eingetragen sind, müssen Sie dem Hinzufügen weiterer Ebenen zustimmen. Das Öffnen von mehr als 64 Ergebnissen kann um einiges länger dauern.

Archivmodus

Der Archivmodus dient zur nachträglichen Auswertung von Aufzeichnungen. Im Archivmodus können nur aufgezeichnete Daten angezeigt werden. Zur Auswahl der relevanten Bilddaten muss in der Kameraübersicht oder in der „[Alarmliste und Systemmeldungen](#)“ auf [Seite 170](#) eine Kamera ausgewählt werden.

Die Aufzeichnungszeiträume für die gewählte Kamera (grüner Rahmen) werden auf einem Zeitstrahl im „[Archiv Player](#)“ auf [der nächsten Seite](#) angezeigt. Die Symbole für Digitalzoom und Lautstärkeregelung werden ebenfalls angezeigt (nur für Kameras mit aktivierter Audioaufnahme).

1. Um in den Archivmodus zu wechseln, klicken Sie in der „[Die Modusleiste](#)“ auf [Seite 136](#) auf **Archivmodus**.
2. Wählen Sie die Kamera oder die Ansicht aus, deren archivierte Bilddaten angezeigt werden sollen, oder wählen Sie einen Alarm aus der Alarmliste aus.

Kameraübersicht

In der Kameraübersicht werden alle installierten Kameras, Lagepläne und Ansichten angezeigt, auf die Sie Zugriff haben. Kameras mit integrierten exportierten Bilddaten werden wie folgt angezeigt: „<Kameraname> [Archiv]“.

1. Klicken Sie auf die entsprechende Kamera. Die Kamerabilder werden im Hauptfenster angezeigt.

Archiv Player

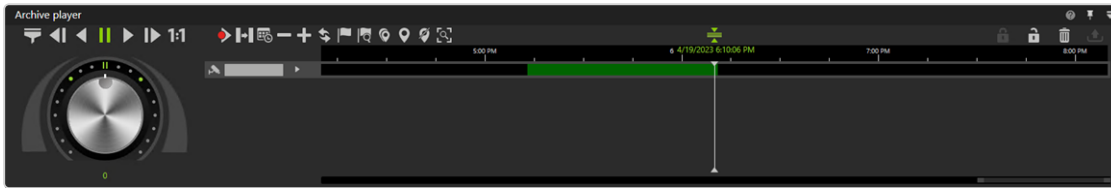



















Abb. 83: Archiv Player




Der Archiv Player ermöglicht die Steuerung des Abspielvorgangs von einer ausgewählten Kamera. Der Player gliedert sich in zwei Bereiche. Der eigentliche Archiv Player wird links angezeigt und der Zeitstrahl rechts.

Der Archiv Player besitzt die folgenden Funktionen:

- **Optionen zur Bandbreitenoptimierung** (): Abhängig von der Lizenz und der Konfiguration kann ein optimierter Videostream ausgewählt werden, um die Client- und Netzwerkauslastung zu reduzieren (siehe „[Bandbreitenoptimierung](#)“ auf [Seite 464](#)).
- **Einzelschritt rückwärts** (): Springt zum vorangegangenen Videoframe der Aufzeichnung.
- **Rückwärts abspielen** (): Spielt den archivierten Videostream in umgekehrter zeitlicher Reihenfolge ab.
- **Pause** (): Unterbricht den Abspielvorgang.
- **Vorwärts abspielen** (): Spielt die Videoaufzeichnung in der zeitlich korrekten Reihenfolge ab.
- **Einzelschritt vorwärts** (): Springt zum nächsten Videoframe der Aufzeichnung.
- **Echtzeit** (): Spielt das Ereignis in Echtzeit ab.
- **Nächste Alarmaufzeichnung** (): Springt zur nächsten Alarmaufzeichnung der ausgewählten Kamera.
- **Pause überspringen** (): Überspringt die Pause zwischen zwei Aufzeichnungen im Abspielmodus.
- **Kalender** (): Öffnet ein Kalenderfenster, um zu einem bestimmten Kalenderzeitpunkt (Datum und Uhrzeit) zu navigieren.

- Aus der Zeitleiste **herauszoomen** () oder **hineinzoomen** (): Vergrößert oder verkleinert die Darstellung der Zeitleiste. Durch einen Klick in die Zeitleiste und anschließendem Drehen des Mauseisens können Sie ebenfalls innerhalb des Aufzeichnungszeitraums zoomen.
- **Zeitleiste aktualisieren** (): Aktualisiert die Zeitleiste der Kamera. Um eine manuelle Synchronisierung mit Edge-Speicherung vorzunehmen (siehe „[Vollständiger Import](#)“ auf Seite 258), klicken Sie bei gedrückter STRG-Taste auf das Symbol.
- **Bookmark hinzufügen** (): Fügt ein Bookmark zum aktuellen Bild hinzu.
- **Bookmark-Übersicht** (): Zeigt die Übersicht aller Bookmarks an (siehe „[Mit Bookmarks arbeiten](#)“ auf Seite 193).
- **Multiselektionsmodus** (): Setzt eine Markierung über mehrere Zeitströme.
- **Marker setzen** (): Setzt die Start- und Endmarkierung für einen ausgewählten Bereich auf der Zeitleiste (siehe „[Bereich bearbeiten](#)“ auf Seite 181).

Bookmarks werden im Viewer-Modus/ Qognify Viewer nicht unterstützt.

- **Markierung löschen** (): Löschen Sie die ausgewählte Markierung.
- **QogniFinder** (): Startet die forensische Suche, wenn die entsprechenden Nutzungsrechte vorhanden sind (siehe „[Verwenden des QogniFinder](#)“ auf Seite 183).
- **Synchronisierter Modus** (): Alle sichtbaren Kameras werden standardmäßig auf die Zeit der ausgewählten Kamera synchronisiert. Wenn der synchronisierte Modus deaktiviert ist, kann jede Kamera einen anderen Zeitpunkt anzeigen.
- **Schreibschutz** ( / ): Setzt den Schreibschutz für den markierten Bereich auf der Zeitleiste. Siehe „[Schreibschutz](#)“ auf Seite 189.
- **Bereich löschen** (): Löscht den markierten Bereich aus der Zeitleiste.
- **Bereich exportieren** (): Startet den AVI-Export bzw. den Qognify-Videodatei-Export (siehe „[Aufzeichnungen exportieren](#)“ auf Seite 186).

Der Export in das Qognify-Dateiformat wird nicht unterstützt.

- **Jog Dial**: Spielt die Sequenz vorwärts und rückwärts ab. Je weiter das Jog Dial nach rechts oder links gedreht wird, desto schneller wird vorwärts oder rückwärts abgespielt. Die Abspielgeschwindigkeit wird unter dem Jog Wheel angezeigt.

- **Zeitleiste / Zeitstrahl:** Siehe „[Zeitleiste / Zeitstrahl](#)“ unten.

Jog Dial verwenden

1. Drehen Sie das Jog Dial mit der Maus nach links oder rechts, um die Sequenz rückwärts bzw. vorwärts abzuspielen. Wenn Sie das Jog Dial loslassen, kehrt es wieder in die Mittelstellung zurück.
2. Klicken Sie auf einen der Punkte, die um das Jog Dial herum angeordnet sind, um es in dieser Stellung zu positionieren.
3. Klicken Sie auf den doppelten Balken über dem Jog Dial, um es loszulassen.

Zeitleiste / Zeitstrahl

Die in der Zeitleiste angezeigte Zeit kann aufgrund der Art und Weise, wie die Qognify VMS Zeitstempelinformationen gespeichert werden, von der im Video angezeigten Zeit abweichen „[Umgang mit Zeitzonen](#)“ auf Seite 27).

Mithilfe der Zeitleiste / des Zeitstrahls können Sie den gesamten Aufzeichnungszeitraum nach relevantem Bildmaterial durchsuchen. Folgende wichtige Farbmarkierungen werden verwendet:

- Grün (Standardaufzeichnung)
- Rot (Alarmaufzeichnung) oder eine andere Farbe als grün

1. Zoomen Sie in den Aufzeichnungszeitraum hinein, indem Sie in die Zeitleiste klicken und das Mousrad drehen. Dies bietet eine bessere Übersicht über den Aufzeichnungsbeginn der Kamera.
2. Doppelklicken Sie auf einen beliebigen Punkt in der Zeitleiste, um den ausgewählten Punkt in die Mitte der Zeitleiste zu verschieben.




Vorschau

1. Bewegen Sie die Maus über die Zeitleiste oder verschieben Sie die Zeitleiste, um die Vorschau des Kamerabildes zum ausgewählten Zeitpunkt anzuzeigen. Die Einstellung in der Client-Konfiguration muss als „Immer ein“ definiert sein (siehe „[Client-Konfiguration](#)“ auf Seite 69).

- Optional können Sie die Steuerungstaste gedrückt halten, während Sie die Maus über die Zeitleiste bewegen oder die Zeitleiste verschieben. Dadurch wird die Vorschau nur bei gedrückter Steuerungstaste angezeigt. Dazu muss die Einstellung in der Client-Konfiguration als „Strg + MouseOver“ definiert werden.

Die Vorschaufunktion ist im Miniarchivmodus einer Kachel nicht verfügbar.

Bereich bearbeiten

- Klicken Sie auf den Kamera-Zeitstrahl neben dem Jog Dial. Wenn eine Kamera abgespielt wird oder mehrere Kameras synchron abgespielt werden, wird neben dem Abspielkopf die aktuelle Uhrzeit des Archivs angezeigt. Wenn mehrere Kameras asynchron abgespielt werden, wird die aktuelle Uhrzeit des Archivs nicht angezeigt.
- Wählen Sie auf der Zeitleiste **Startmarkierung einstellen** , um den Anfang des Abschnitts zu kennzeichnen. Wenn Sie die Markierungen gleichzeitig auf mehreren Zeitleisten einstellen, wählen Sie zuerst den **Multiselektionsmodus** . Wenn der Multiselektionsmodus aktiv ist, ist das Symbol grün.
- Bewegen Sie die Zeitleiste bis ans Ende des Abschnitts.
- Wählen Sie **Endmarkierung einstellen** , um das Ende des Abschnitts festzulegen.
- Wählen Sie **Bereich löschen** , um den Abschnitt von der Zeitleiste zu entfernen.
- Klicken Sie auf **Bereich exportieren** , um den Abschnitt zu exportieren.
- wählen Sie das erforderliche Datenformat (**Typ**), wählen Sie **OK**. Folgende Exportformate stehen zur Verfügung:
 - Qognify-Datenformat: Die exportierten Daten besitzen einen Passwortschutz und können nur mit dem Viewer betrachtet werden.
 - AVI: Die exportierten Dateien besitzen keinen Passwortschutz und können mit jeder beliebigen Filmsoftware betrachtet werden. Dies stellt ein erhöhtes Datenschutzrisiko dar.
- Legen Sie die gewünschten Exporteinstellungen fest (siehe „[Mehrfachexport von Bilddaten](#)“ auf Seite 114).

Click-2-Track

Diese Funktion wird im Archivmodus verwendet, um von einer Kamera zur nächsten zu navigieren, indem Sie auf die Click-2-Track-Regionen im Bild klicken.

Die Vorschau der Click-2-Track-Region zeigt denselben Zeitpunkt an wie die aktuelle Archiv-Zeitleiste. Wenn sich das Archiv im Wiedergabemodus befindet, wird die Vorschau mit der gleichen Geschwindigkeit wie das Hauptbild abgespielt. Die aktuelle Geschwindigkeit und Richtung bleibt gleich, auch wenn Sie zwischen Click-2-Track-Regionen wechseln und die Kamera wechseln.

Die Funktion funktioniert sowohl bei der Wiedergabe vorwärts und rückwärts in verschiedenen Geschwindigkeiten als auch bei Standbildern.

Die Verlaufsfunktion

Click-2-Track speichert eine Historie der Kamera nach den folgenden Kriterien:

- Jede Kamera speichert die Zeit, zu der sie geöffnet wurde, sowie den Zeitpunkt, zu dem sie durch die nächste Kamera ersetzt wurde.
- Wenn Sie zum nächsten Eintrag in der Historie navigieren, zeigt die Kamera die Öffnungszeit an.
- Wenn Sie zum vorherigen Eintrag in der Historie navigieren, zeigt die Kamera die Schlusszeit an.
- Nur die Click-2-Track-Nutzungen der aktuellen Kachel werden in der Verlaufsfunktion gespeichert. Alle Kacheln weisen ihren eigenen Verlauf auf.


Beispiel

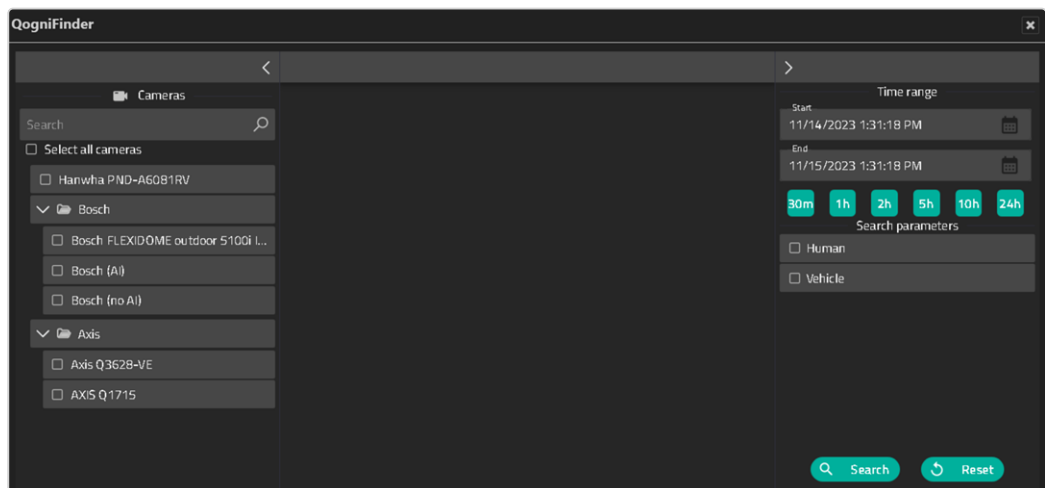
1. Kamera A wird von 8:00 bis 8:01 betrachtet, dann wird der Bereich für Kamera B ausgewählt.
2. Kamera B wird von 8:01 bis 8:02 betrachtet, dann wird der Bereich für Kamera C ausgewählt.
3. Kamera C wird von 8:02 bis 8:03 betrachtet, dann wird die Schaltfläche **Zurück** im Verlauf verwendet. Die Ansicht springt um 8:02 Uhr auf Kamera B mit einem Standbild, unabhängig von der vorherigen Geschwindigkeit.
4. Wenn Sie die Schaltfläche **Zurück** im Verlauf erneut verwenden, springt die Ansicht zu Kamera A bei 8:01 mit einem Standbild.

5. Wenn Sie in der Historie die Taste **Vorwärts** drücken, springt die Ansicht zu Kamera B bei 8:01, wenn Sie sie erneut drücken, springt sie zu Kamera C bei 8:02.

Verwenden des QogniFinder

Der QogniFinder muss für die ausgewählte Kamera im Konfigurationsmodus aktiviert sein (siehe „Kamera - Allgemein“ auf Seite 246).

1. Wählen Sie im Archiv-Modus die Kamera und **QogniFinder**  in der Symbolleiste des Archiv Player. Wenn mehrere Kameras konfiguriert sind, werden Sie als Gruppen angezeigt und nach dem Hersteller benannt.



2. Wählen Sie die Kamera(s), die für die Suche nach Objekten benutzt wird/werden.

- Wenn eine Kamera einige Suchkriterien nicht unterstützt, werden die entsprechenden Suchkriterien markiert.
- Wenn eine Kamera keines der Suchkriterien unterstützt, wird die Kamera markiert.

- Definieren Sie den **Zeitbereich** für die Suche, indem Sie Start- und Enddatum eingeben oder einen der vordefinierten Filter auswählen:
- Aktivieren Sie die primären Suchparameter:

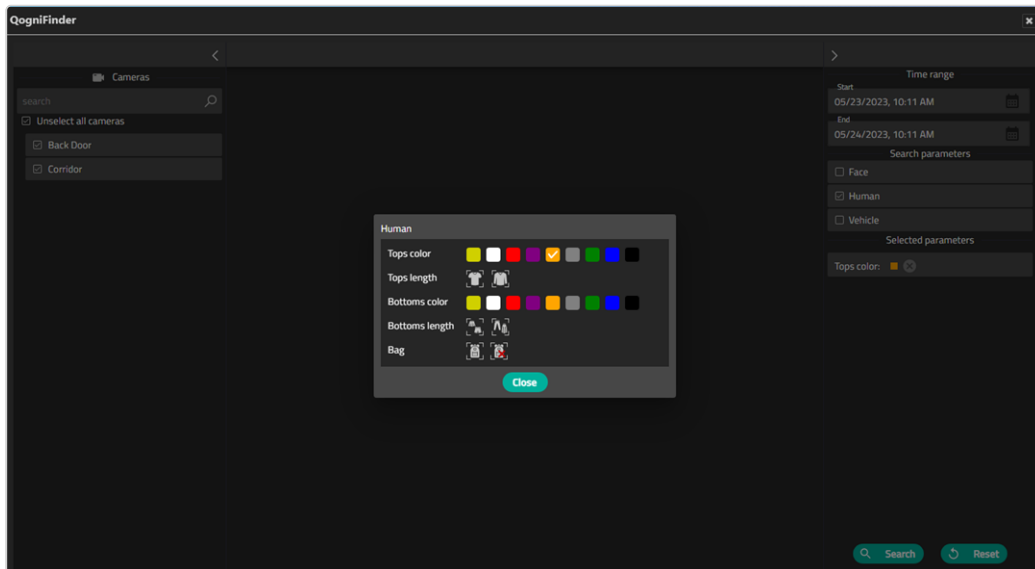
- Mensch (Kombination aus Gesicht und Körper)

Bei unterstützten Kameras von Hanwha umfasst das Suchkriterium „Mensch“ auch Kriterien wie „Hut“, „Tasche“, usw.

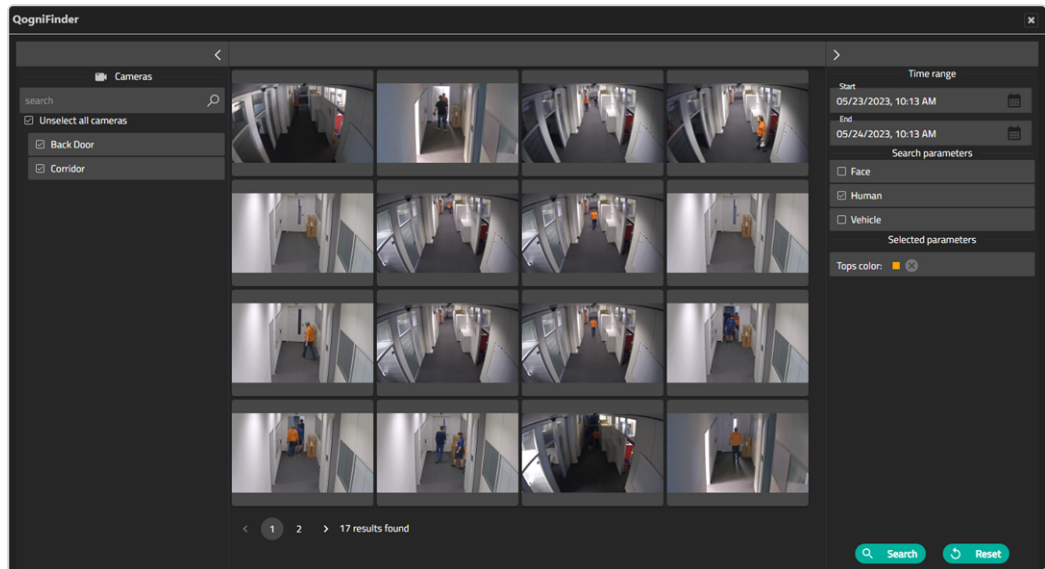
- Fahrzeug


Bei unterstützten Kameras wie bestimmten Kameras von Hanwha, Axis oder Bosch werden bei der Suche nach „Fahrzeug“ auch Kriterien zum Fahrzeugtyp angezeigt.

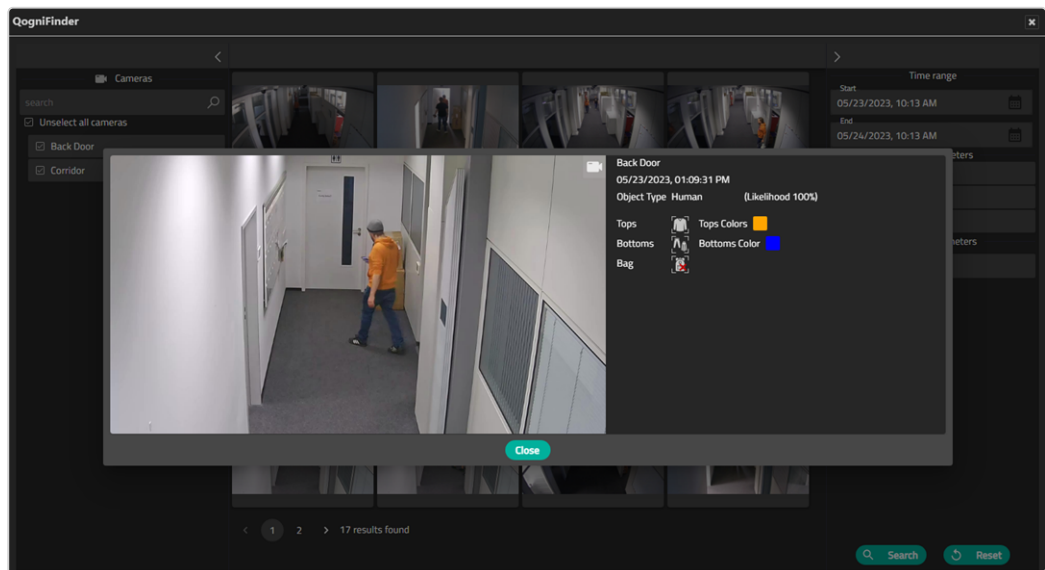
- Um die Suchparameter zu definieren, klicken Sie auf den/die aktivierten Parameter und spezifizieren Sie weitere Metadaten, wie z. B. Kleiderfarbe oder Fahrzeugtyp.





- Schließen Sie das Auswahlfenster und klicken Sie auf **Suchen**. Die Objekte innerhalb des spezifizierten Zeitbereichs und alle Bilder, die die spezifizierten Suchkriterien erfüllen, werden angezeigt.



- Wenn mehr als 16 Ergebnisse gefunden werden, verwenden Sie die Paging-Funktion im unteren Bereich des Fensters, um zu mehr Objekten zu navigieren oder engen Sie die Suche durch das Hinzufügen von Parametern oder die Änderung der Zeitleiste ein.
- Um die Details eines Ergebnisses aufzurufen, bewegen Sie die Maus über die Vorschau und klicken Sie auf das Kamerasymbol . Die Suchparameter werden entlang der ausgewählten Szene angezeigt.




- Wenn mehr als ein Ergebnis gefunden wird, können Sie mit den Schaltflächen  und  zum vorherigen oder nächsten Ergebnis navigieren.

10. Um eine Suche mit anderen Parametern zu starten, wählen Sie **Zurücksetzen** und definieren Sie die neuen Suchparameter.

Aufzeichnungen exportieren

Einzelbild exportieren

1. Wählen Sie in der Bilderkachel unterhalb der Kachel **Exportieren** aus. 
2. Wählen Sie das Exportformat aus:
 - **Videoframe in Datei speichern:** Damit wird das ausgewählte Bild als statische Bilddatei (JPG) gespeichert.
 - **Videoframe drucken:** Damit wird das ausgewählte Bild als Hardcopy mit zusätzlichen Informationen wie Kamera und Aufnahmezeit gedruckt.

Videodatei exportieren

1. Legen Sie den Zeitbereich für den Export fest, indem Sie den aufgezeichneten Abschnitt verschieben und die Markierung  an den Start- und Endpunkten setzen.
2. Verwenden Sie die Mehrfachauswahlmarkierung , um mehrere Zeitleisten gleichzeitig auszuwählen, indem Sie diese auf der Zeitleiste einer Kamera platzieren. Alle Kamerazeitleisten mit derselben vertikalen Auswahl sind markiert.
3. Um einen Zeitbereich zu entfernen, wählen Sie **Markierung löschen**  und wählen Sie den/die zu entfernenden Zeitbereich(e).
4. Wählen Sie in den Steuerelementen des Archiv-Players die Option **Exportieren** .

5. Wählen Sie als Exporttyp **Videodaten-Export** (passwortverschlüsseltes Cognify-spezifisches Format) oder AVI-Export (unverschlüsseltes Datenformat) aus.

Wenn Videodaten-Export ausgewählt wird, werden die Aufzeichnungen auf den Server oder den Client exportiert (siehe „[Mehrfachexport von Bilddaten](#)“ auf Seite 114).

Wenn der Exportvorgang unterbrochen wird, z. B. wegen eines Netzwerkfehlers, wird er automatisch so bald wie möglich fortgesetzt.

6. Fahren Sie entsprechend den gewünschten Zielen fort (zu den folgenden Vorgehensweisen siehe „[Mehrfachexport von Bilddaten](#)“ auf Seite 114).

Exportieren des Click-2-Track-Verlaufs mit dem Export Designer

Wenn Sie ein Ereignis mit dem Export Designer exportieren, kann auch der Click-2-Track-Verlauf exportiert werden.

Bei Kameras, bei denen Click-2-Track aktiviert ist, funktioniert diese Übergabefunktion auch im „[Anywhere Viewer](#)“ auf Seite 539.

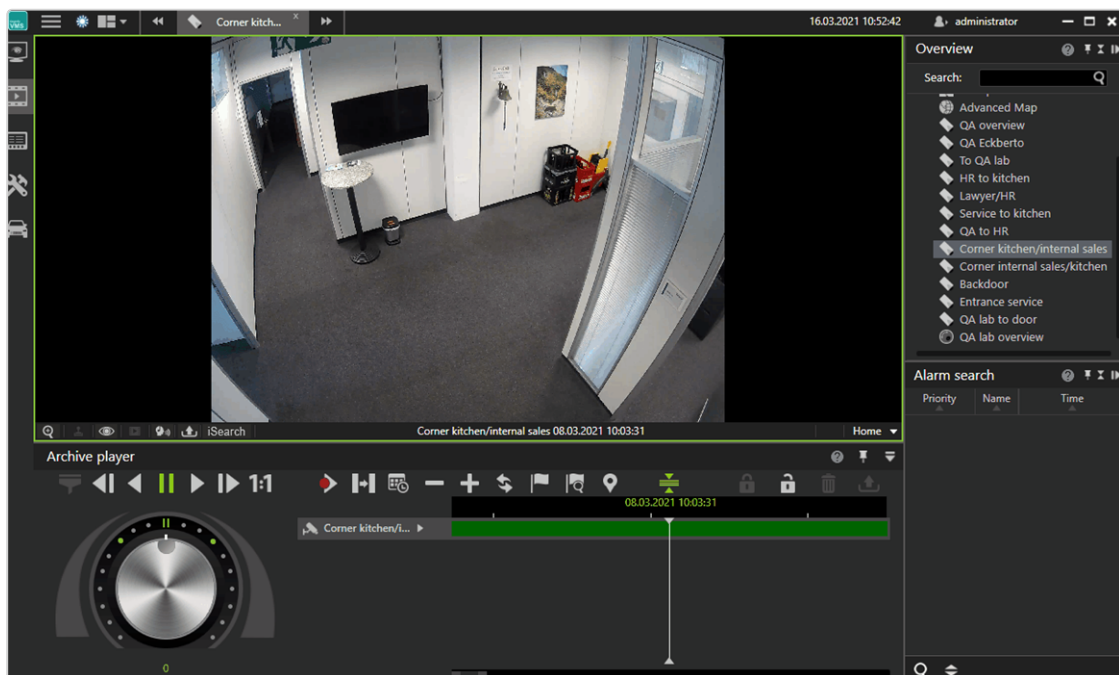

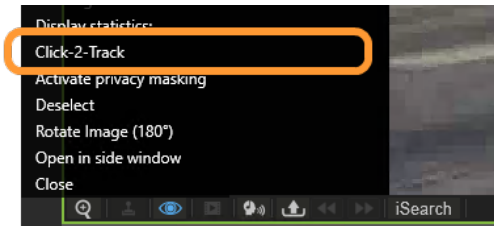


Abb. 84: Beispiel für die Verfolgung einer Person im Archivmodus mit Click2Track

1. Öffnen Sie die Kamera im Archivplayer.
2. Wählen Sie **Click-2-Track** in den **Auszug-Optionen** .




3. Wählen Sie **Aktivieren** und folgen Sie den Formen in der Bildfolge, indem Sie auf die jeweilige Form klicken. Dies öffnet die Kamerasequenz der zugewiesenen Kamera.
4. Wählen Sie **Click-2-Track > Verlauf im Export Designer öffnen**, um den Export Designer zu starten (siehe „[Der Export Designer](#)“ auf Seite 105). Der Click-2-Track-Verlauf der Kamera wird in einer Liste als Sequenzen angezeigt.

	Camera	From	To	Sequence	
1	Corner kitchen/internal sales	14:02:20.282	14:02:25.202	4s	
2	Service to kitchen	14:02:25.202	14:02:35.132	9s	
3	QA to HR	14:02:35.132	14:03:12.482	37s	

5. Klicken Sie auf eine Privacy-Mask , um die Privacy-Mask in den Export einzubeziehen oder auszuschließen.

Datenschutzmasken können im Offline-Modus nicht ausgeblendet werden.

6. Um eine Kamera aus der Export zu entfernen, markieren Sie die Kamera und klicken Sie auf **Löschen** . Standardmäßig werden alle Sequenzen exportiert.

Exportierte Videodaten auswerten

Es gibt zwei Möglichkeiten zur Auswertung der exportierten Videodaten:

- Auf einem System ohne Qognify VMS-Installation können die Videodaten mit dem Qognify VMS Viewer (siehe „[Anywhere Viewer](#)“ auf Seite 539) ausgewertet werden.
- Um die Videodaten in eine Qognify VMS-Installation einzubinden, muss im Konfigurationsmodus eine „Archivkamera“ angelegt werden (siehe „[Kamera manuell anlegen](#)“ auf Seite 231).


Schreibschutz

Schreibgeschützte Aufzeichnungen werden im Zonenverzeichnis vorgehalten und werden nicht gelöscht. Stellen Sie sicher, dass auf der Zonenpartition ausreichend Speicherplatz vorhanden ist.

Aufgrund gesetzlicher Vorschriften darf der Schreibschutz bei Installationen in Frankreich nicht verwendet werden.

Schreibschutz setzen

Der geschützte Bereich in der Zeitleiste ist mindestens so weit wie der vom Benutzer ausgewählte Bereich, Qognify VMS kann aber auch einen größeren Bereich schützen, um beispielsweise die Leistung der Multimedia-Datenbank (mdb) zu optimieren. Der tatsächlich geschützte Zeitbereich wird nach der Einstellung des Schreibschutzes angezeigt.

1. Wählen Sie auf der Zeitleiste **Markierungen setzen**, um den Anfang des zu schützenden Abschnitts zu markieren.
2. Verschieben Sie den Zeitbalken an das Ende des zu schützenden Abschnitts.
3. Wählen Sie erneut **Markierungen setzen**, um den Abschnitt festzulegen.
4. Um Aufzeichnungen vor Überschreiben oder Löschen zu schützen, klicken Sie auf das geschlossene **Schloss** .

Schreibschutz entfernen

1. Wählen Sie **Schloss öffnen** () im Archiv Player.

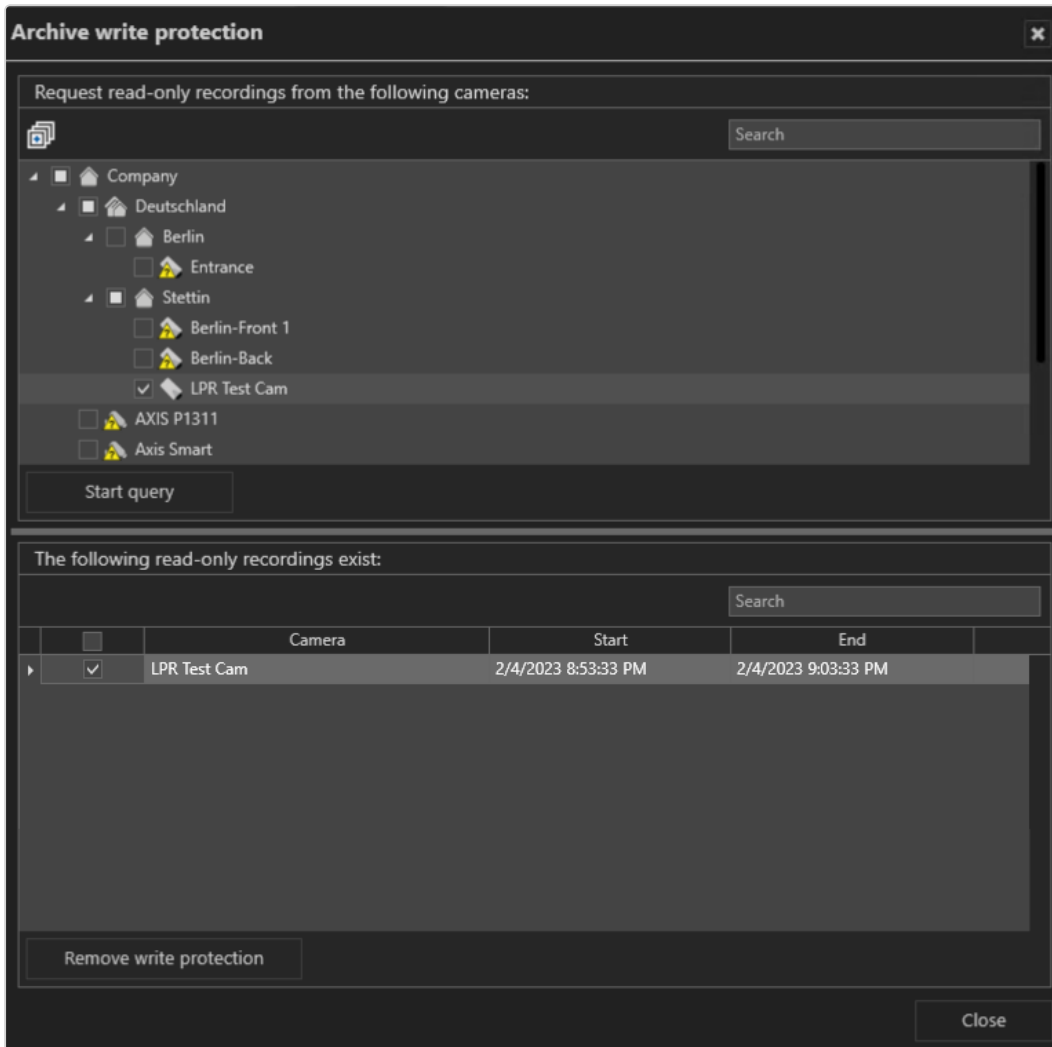


Abb. 85: Schreibschutz entfernen

2. Wählen Sie **Abfrage starten**.
3. Wählen Sie die schreibgeschützten Sequenzen aus. Wenn Sie mehrere Sequenzen auswählen möchten, halten Sie gleichzeitig die STRG-Taste gedrückt.
4. Wählen Sie **Schreibschutz entfernen**.

Alarmer suchen

Die in der Zeitleiste angezeigte Zeit kann aufgrund der Art und Weise, wie die Qognify VMS Zeitstempelinformationen gespeichert werden, von der im Video angezeigten Zeit abweichen „[Umgang mit Zeitzonen](#)“ auf Seite 27).

Mit der Alarmsuche können Sie in Abhängigkeit von konfigurierbaren Bedingungen nach einem bestimmten Alarm suchen.

Alarm-Abfrage anlegen

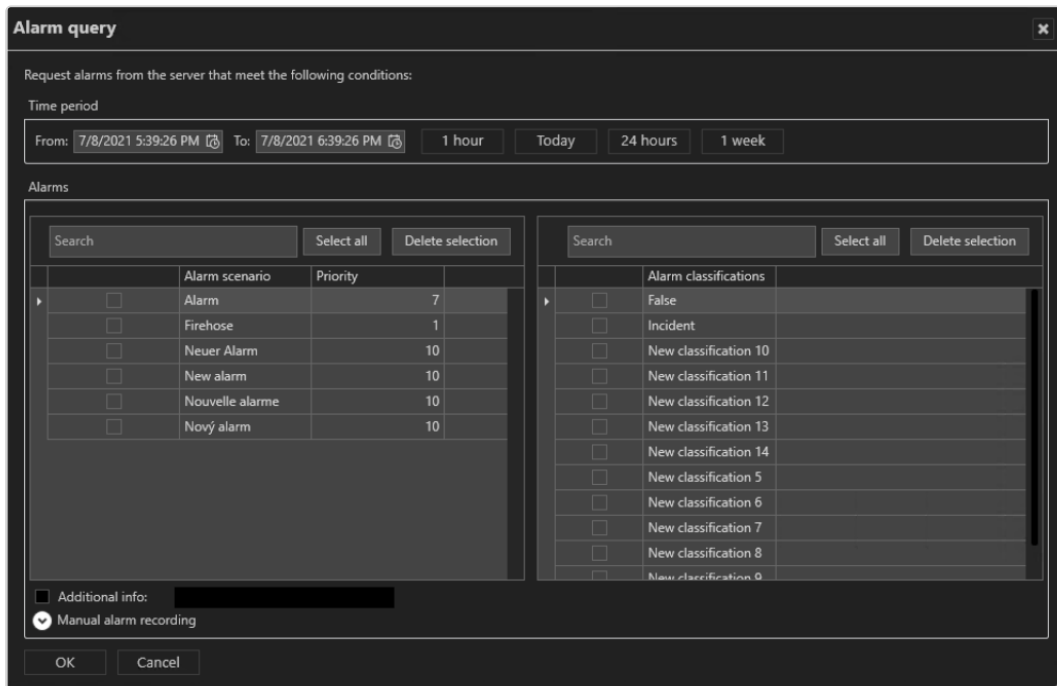


Abb. 86: Alarmer suchen

1. Klicken Sie im Steuerelement Alarmsuche auf **Neue Abfrage**. Die Alarm-Abfrage wird angezeigt.
2. Geben Sie den **Zeitraum** an, in dem nach dem Alarm gesucht werden soll.
3. Optional können Sie als Zeitraum die letzte Stunde, die letzten 24 Stunden, die letzte Woche oder den heutigen Tag wählen.
4. Legen Sie fest, ob Sie das Alarmszenario nach Name oder nach Priorität auswählen möchten.
 - Zur Auswahl aller Elemente klicken Sie auf **Alle auswählen**.
 - Um die Auswahl aufzuheben, klicken Sie auf **Auswahl löschen**.
5. Wählen Sie die „Alarm klassifizierung“ entweder durch direkte Auswahl oder durch Suche nach dem Klassifizierungsbegriff. Die Alarmkategorien werden in der Systemkonfiguration festgelegt (siehe [„Konfigurieren der Alarm-Klassifizierungen“ auf Seite 465](#)).
6. Falls verfügbar, geben Sie die zusätzlichen Informationen ein, die durch Netzwerkauslöser (z. B. Network IO) ermittelt werden, nach denen gesucht werden soll.

- Um manuelle Aufzeichnungen der verfügbaren Videoquellen bei der Suche zu berücksichtigen, aktivieren Sie **Manuelle Alarmaufzeichnung**.
- Wählen Sie die Aufzeichnungen der Kamera bzw. Kameras aus, die durchsucht werden sollen.
- Starten Sie die Suche mit **OK**.

Alarmsuchergebnisse

Die Ergebnisse der Alarm-Abfrage werden im Steuerelement „Alarmsuche“ angezeigt.

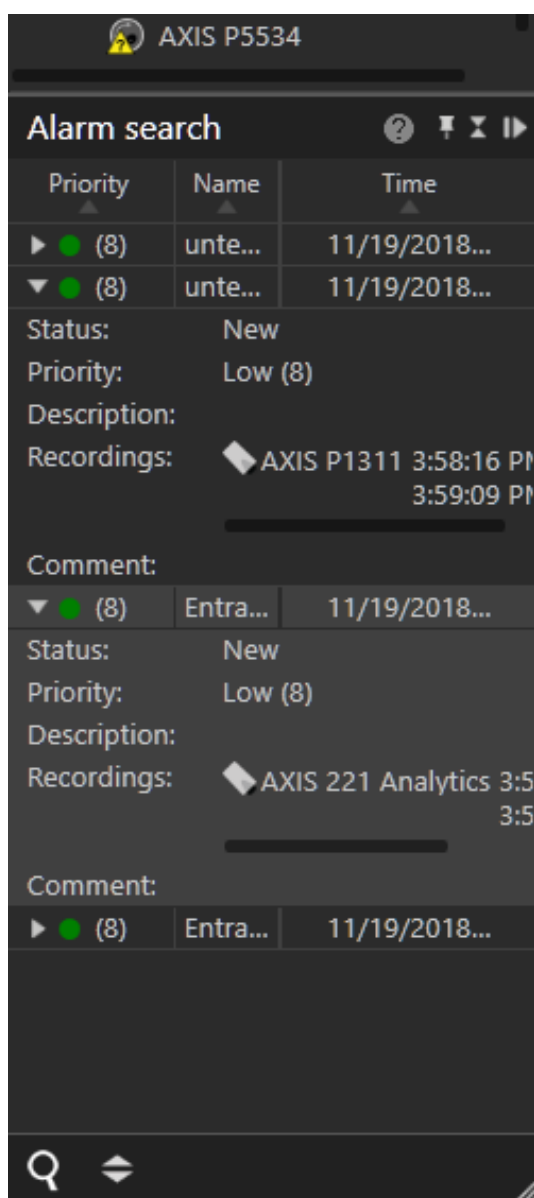


Abb. 87: Alarmsuchergebnisse

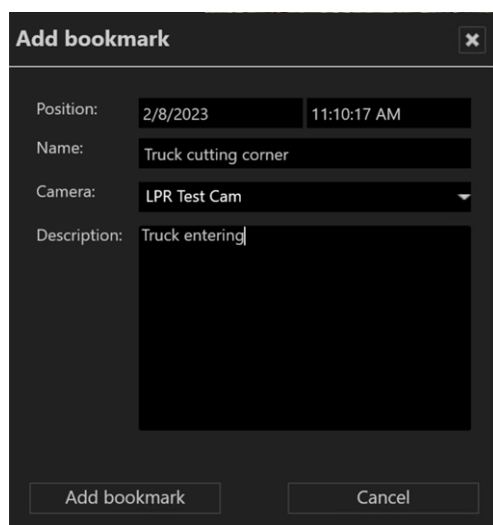
1. Klicken Sie auf einen der Spaltentitel **Priorität**, **Name** oder **Zeitpunkt**, um die Ergebnisse entsprechend zu sortieren.
2. Klicken Sie auf den Pfeil links neben einem Alarm, um Details anzuzeigen.

Mit Bookmarks arbeiten

Bookmarks können im Archivmodus oder beim Starten oder Beenden einer manuellen Alarmaufzeichnung gesetzt werden [siehe „[Manuelle Alarmaufzeichnung](#)“ auf [Seite 154](#)].

Bookmark hinzufügen

1. Bewegen Sie die Zeitleiste an die Position, an der Sie das Bookmark setzen möchten.
2. Wählen Sie **Bookmark hinzufügen** () im Archiv Player.



The screenshot shows a dark-themed dialog box titled "Add bookmark". It has a close button (X) in the top right corner. The dialog contains the following fields:

- Position:** A date field containing "2/8/2023" and a time field containing "11:10:17 AM".
- Name:** A text input field containing "Truck cutting corner".
- Camera:** A dropdown menu showing "LPR Test Cam".
- Description:** A text input field containing "Truck entering".

At the bottom of the dialog, there are two buttons: "Add bookmark" and "Cancel".

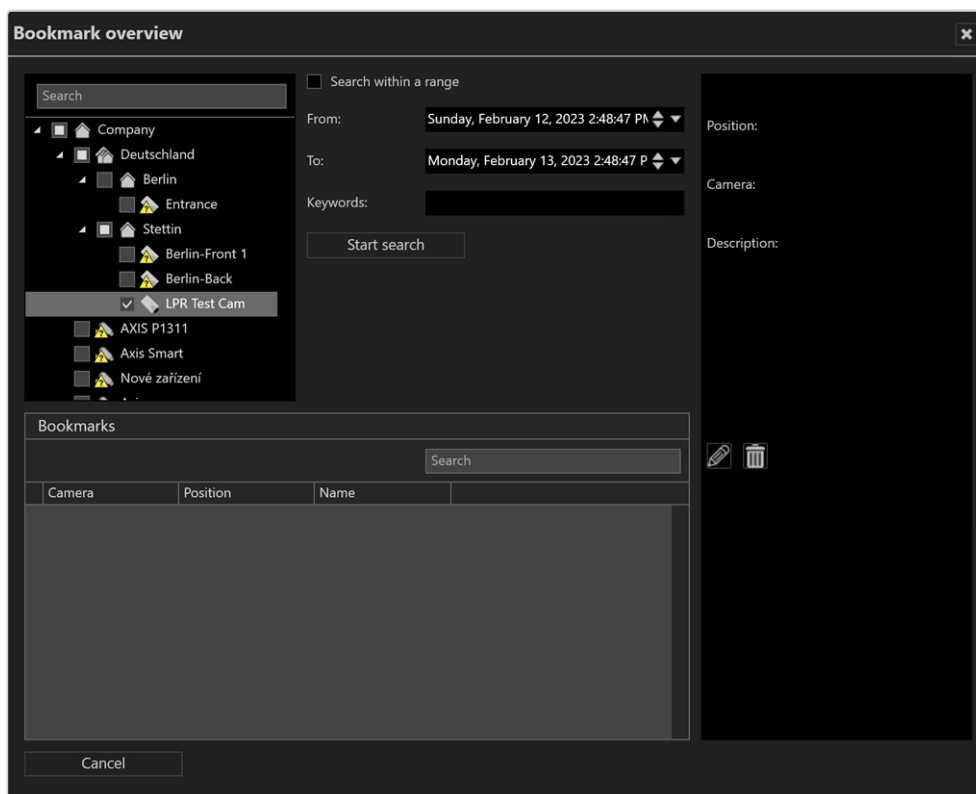
3. Geben Sie einen **Namen** für das Bookmark ein.
4. Wählen Sie die **Kamera**, für die Sie ein Bookmark zur Aufzeichnung hinzufügen möchten, aus dem Aufklappmenü aus. Das Aufklappmenü enthält alle Kameras, die derzeit im Archiv Player angezeigt werden. Standardmäßig ist die derzeit aktive Kamera im Archiv Player ausgewählt.
5. Geben Sie bei Bedarf eine Beschreibung ein.


6. Wählen Sie **Bookmark hinzufügen**. In der Zeitleiste der gewählten Kamera wird eine Markierung eingefügt.



Bookmark-Übersicht

In der Bookmark-Übersicht können Bookmarks angezeigt, bearbeitet und gelöscht werden.

1. Wählen Sie im Archiv Player **Bookmark-Übersicht** ().



2. Wählen Sie eine oder mehrere Kameras aus oder klicken Sie zur Auswahl aller angezeigten Kameras (d. h. Kameras mit verknüpften Bookmarks) auf **Alle auswählen**.
3. Optional können Sie nach dem Kameranamen oder dem Bookmark suchen.
4. Suchen Sie nach Bookmarks für alle Kameras, selbst wenn diese nur im Archiv sichtbar sind. Bookmarks von Kameras unterschiedlicher Installationen können gleichzeitig gesucht werden.
5. Um die Auswahl aufzuheben, klicken Sie auf **Auswahl aufheben** ().

6. Aktivieren Sie **Innerhalb der Reichweite suchen**, um das Zeitfenster für die Suche einzuengen und das Zeitintervall zu spezifizieren.
7. Wählen Sie **Suche starten**, um nur die Bookmarks innerhalb des angegebenen Zeitraums anzuzeigen. Die Bookmarks werden im Bereich „Bookmarks“ aufgelistet.
8. Wählen Sie im Bereich „Bookmarks“ ein Bookmark aus. Die zugehörigen Informationen des Bookmarks (Zeit, zugeordnete Kamera und Beschreibung) werden im rechten Bereich angezeigt.
9. Doppelklicken Sie auf das Bookmark, um zur entsprechenden Zeitmarke zu navigieren.
10. Zum Bearbeiten der Informationen klicken Sie auf **Bearbeiten** () (siehe [„Bookmark hinzufügen“ auf Seite 193](#)).
11. Zum **Löschen** des Bookmarks klicken Sie auf **Löschen** () .

Bookmarks werden nicht mit den Videodaten gelöscht, da sie in einer separaten Ereignisdatenbank gespeichert werden. Sie werden automatisch gelöscht, sobald das älteste Videobild jünger als der Zeitstempel des Bookmarks ist.

Edge-Speicher-Import

Bei der Edge-Speicherung werden die Bilder auf einem internen Speicher (z. B. SD-Karte) der Kamera gespeichert, um Verbindungsausfälle zwischen Kamera und Datenbankserver auszugleichen. Wenn die Verbindung zwischen Kamera und Server unterbrochen wird, kommt es auf dem Device Manager zu Aufzeichnungslücken.

Nach Wiederherstellung der Verbindung können die Aufzeichnungslücken auf dem Server mit den Aufzeichnungen vom internen Speicher der Kamera gefüllt werden. Zeitpläne für die Aufzeichnung und die maximale Aufzeichnungsgröße werden dabei berücksichtigt. (siehe [„Bildspeicherung“ auf Seite 252](#)).

Abhängig von der Konfiguration der Kamera (siehe [„Edge-Speicher“ auf Seite 260](#)) können die Edge-Speicherdaten automatisch oder manuell importiert werden.

Manueller Edge-Speicher-Import

1. Um einen manuellen Edge-Speicher-Import vorzunehmen, klicken Sie bei gedrückter STRG-Taste auf **Zeitleiste aktualisieren** () .

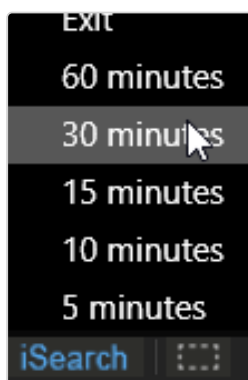
iSearch

iSearch im Archivmodus durchsucht Aufzeichnungen nach Bewegungen in bestimmten Bildbereichen. Der durchsuchbare Aufzeichnungszeitraum liegt zwischen 5 und 60 Minuten.

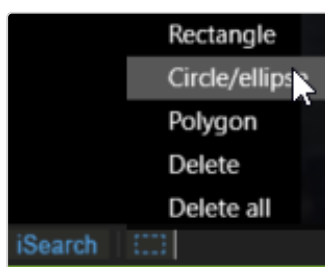
Die Leistung von iSearch ist von der Leistungsfähigkeit der Client-Hardware abhängig, da die Suche ausschließlich auf dem Client stattfindet.

iSearch konfigurieren

1. Wählen Sie die zugehörige Kamera aus.
2. Klicken Sie am unteren Rand des Videobilds auf **iSearch** und wählen Sie einen Zeitbereich zwischen 5 und 60 Minuten. Der maximal auswählbare Zeitbereich hängt von den Zugriffsbeschränkungen des Benutzers für das Archiv ab (siehe „[Rechte-Optionen](#)“ auf Seite 360).



Rechts neben der iSearch-Schaltfläche wird ein gestricheltes Rechtecksymbol angezeigt.



3. Klicken Sie auf das **Bereichssymbol** und wählen Sie die Form des Suchbereichs aus. Folgende Formoptionen stehen zur Verfügung:
 - Rechteck
 - Kreis / Ellipse
 - Polygon
 - Form löschen
 - Alle Formen löschen
4. Klicken Sie in das Kamerabild und ziehen Sie die ausgewählte Form an die gewünschte Stelle. Über das Bild wird an der gewählten Stelle ein halbtransparenter Bereich gelegt.

Falls Sie das Polygon als Ausschnitt gewählt haben, klicken Sie für jeden Eckpunkt in das Bild und schließen Sie das Polygon durch Doppelklick des letzten Punkts.

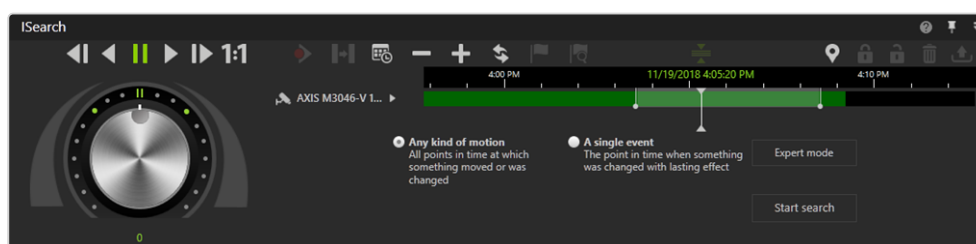


Abb. 88: iSearch konfigurieren

5. Wählen Sie im ausgewählten Bereich entweder **Alle Bewegungen** (Standardeinstellung) oder **Ein einzelnes Ereignis** aus.
 - **Alle Bewegungen:** Diese Suchmethode sucht nach allen Veränderungen im Bild im angegebenen Zeitraum. Die Suche kann auf dem ganzen Bild oder in vom Anwender zu definierenden Bereichen geschehen. Abhängig von der Auswahl kann die Suche einige Zeit dauern.
 - **Ein einzelnes Ereignis:** Diese Suchmethode ist besonders schnell. Es können mehrere Tage Bildmaterial in wenigen Sekunden durchsucht werden. Allerdings funktioniert die Methode nur, wenn ein nachhaltiges einzelnes Ereignis im gewählten Bereich der Kamera aufgetreten ist.
6. Optional können Sie **Expertenmodus** aktivieren, um die Suche zu präzisieren.

iSearch im Expertenmodus

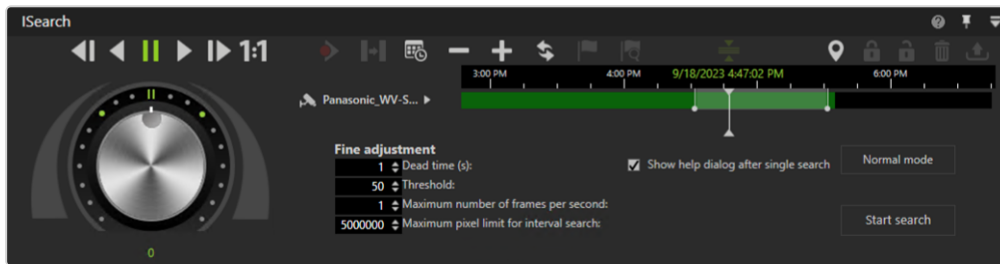


Abb. 89: iSearch im Expertenmodus

1. Nehmen Sie die gewünschten Einstellungen vor und starten Sie die Suche. Folgende Optionen stehen zur Verfügung:
 - Die **Totzeit** in Sekunden gibt an, wie lange nach Erkennung einer Bewegung im Bild bzw. Teilbereich ein erneuter Treffer in der Ergebnisliste angezeigt wird.
 - Mit dem **Schwellenwert** werden bei extremen Lichtverhältnissen der Kamera Veränderungen im Bild erkannt. Eine solche Veränderung im Bild interpretiert der Schwellenwert als Bewegung. Je höher der Schwellenwert, umso größer muss die Bildänderung sein, damit Sie einen Treffer erhalten.
 - **Maximale Anzahl von Frames pro Sekunde**, wenn nicht alle aufgezeichneten Bilder durchsucht werden müssen. Dies kann die Suche erheblich beschleunigen.
 - **Maximale Pixelgrenze bei Intervallsuche**: Die maximale Pixelgrenze bei einer Intervallsuche hat nur Auswirkungen bei der Suche nach einer nachhaltigen Veränderung. Es wird permanent zwischen dem von Ihnen definierten Start- und Endpunkt des zu durchsuchenden Zeitraums verglichen. Sollte der momentane Zustand von beiden Punkten um mehr als die angegebene Pixelgrenze abweichen, wird die Intervallhalbierung unterbrochen und es wird eine serielle Suche mit großer Schrittweite gestartet, bis die Pixelgrenze wieder unterschritten wird. Danach wird die Intervallsuche zu diesem Zeitpunkt wieder fortgesetzt. Diese Einstellung verbessert die Suche unter extremen Lichtverhältnissen (starker Kontrast zwischen hellen und dunklen Bereichen oder durchlaufende Objekte).

- Aktivieren Sie gegebenenfalls **Hilfsdialogfenster nach Einzelsuche anzeigen**. Nach dem Ende der Suche können Sie in einem Dialog auswählen, ob das Ereignis gefunden/nicht gefunden wurde und ob Sie mit dem gefundenen Ereignis in den Archivmodus wechseln möchten.
2. Um den Expertenmodus zu verlassen, wählen Sie **Normaler Modus**.

Suchbereich löschen

1. Klicken Sie auf den Suchbereich und wählen Sie **Löschen**, um nur den gewählten Bereich zu löschen.
2. Optional können Sie **Alle löschen** wählen, um alle Bereiche zu löschen.

Ereignisauswertung

Die Ereignisauswertung zeigt Ihnen eine Übersicht der vorgefallenen Ereignisse als Liste an. Es wird dabei unterschieden zwischen:

- Benutzerereignissen (Anzeige von Ereignissen, die bestimmte Benutzer betreffen),
- Alarmereignissen (aufgetretene Ereignisse),
- Kameranutzung (Anzeige von Ereignissen, die eine bestimmte Kamera betreffen)
- Systemmeldungen (Anzeige von Ereignissen, die bestimmte Dienste betreffen)

Zudem kann die Verwendung der Kamera durch die Benutzer verfolgt werden und der Benutzer kann sehen, welche Änderungen an der Konfiguration vorgenommen und von wem sie vorgenommen wurden.

Die maximal angezeigte Anzahl der Ereignisse kann in der Client-Konfiguration eingestellt werden (siehe „[Client-Konfiguration](#)“ auf Seite 69).

1. Um in die Ereignisauswertung zu wechseln, klicken Sie auf das Symbol **Ereignisauswertung** in der Modusleiste.

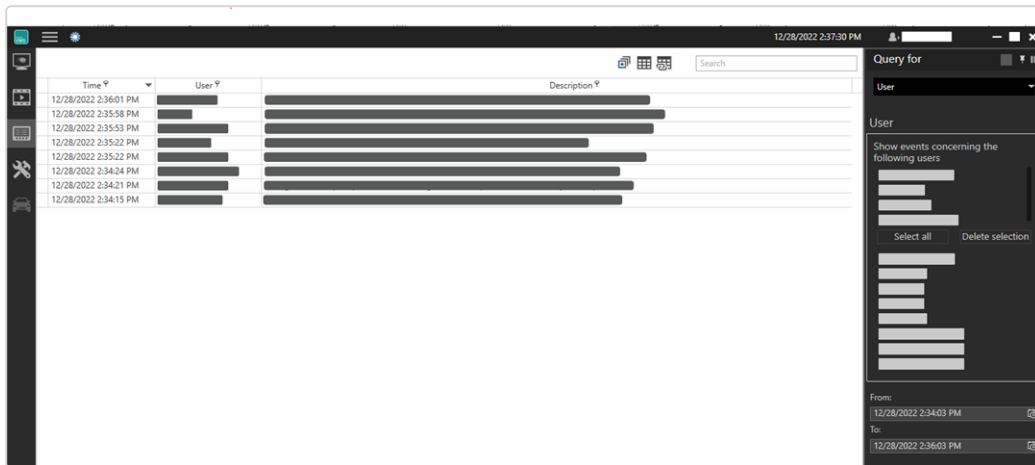


Abb. 90: Ereignisauswertung

2. Klicken Sie im Hauptfenster auf einen Spaltentitel, um die Ereignisse anhand der Kategorie der Spalte (Datum/Zeit, Benutzer, Beschreibung) aufsteigend oder absteigend zu sortieren.

Abfrage filtern

In der Ereignisauswertung können die folgenden Ereignistypen ausgewertet werden:

- Alarme können nach Alarmszenarien gefiltert werden.
- Benutzer können gefiltert werden nach:
 - Benutzer
 - Kamerakonfiguration
 - Archiv
 - Export
 - Wächterrundgänge
 - Aktionen
 - Anmelden oder Abmelden
 - Fehlgeschlagene Anmeldungen:
 - Modus ändern
 - Ereignisse freigeben und einschränken

- Kameranutzung kann gefiltert werden nach:
 - Kamera (nur, wenn der Device Manager die Kameranutzung aufzeichnet)
 - Benutzer
- System kann gefiltert werden nach:
 - Basisdienste
 - Bildspeicherung

Abhängig vom Bereich können die Abfrageergebnisse gefiltert werden.

1. Um die Ereignisse anhand vorgegebener Kriterien zu filtern, wählen Sie in der Steuerleiste **Abfrage nach** die Art des gesuchten Ereignisses aus.
2. Wählen Sie den bzw. die Benutzer aus, die in Beziehung zu dem gesuchten Ereignis stehen.
3. Aktivieren Sie die gewünschten Ereignisse. Die Elemente werden in der Liste darunter angezeigt.
4. Wählen Sie bestimmte Elemente durch Aktivieren des Kontrollkästchens vor dem Namen des jeweiligen Elements aus oder klicken Sie auf **Alle auswählen**.
5. Um die Auswahl aufzuheben, wählen Sie **Auswahl löschen**.
6. Um die Auswahl weiter einzugrenzen, legen Sie den Zeitraum (Datum und Uhrzeit) fest.
7. **Starten** Sie die Abfrage. Im Hauptfenster werden nur die Ereignisse angezeigt, die den gewählten Kriterien entsprechen.

Exportieren der Analyse als Tabellenkalkulationsdatei

Optional können Sie das Ergebnis auch als kommagetrennte Datei (*.csv) exportieren.

1. **Exportieren** Sie das Ergebnis, um es mit einem Tabellenkalkulationsprogramm auszuwerten.

Abfrage als Berichtvorlage speichern

Darüber hinaus können die Suchkriterien für zukünftige Abfragen gespeichert werden.

1. Wählen Sie im Berichtmodus-Fenster **Speichern**.

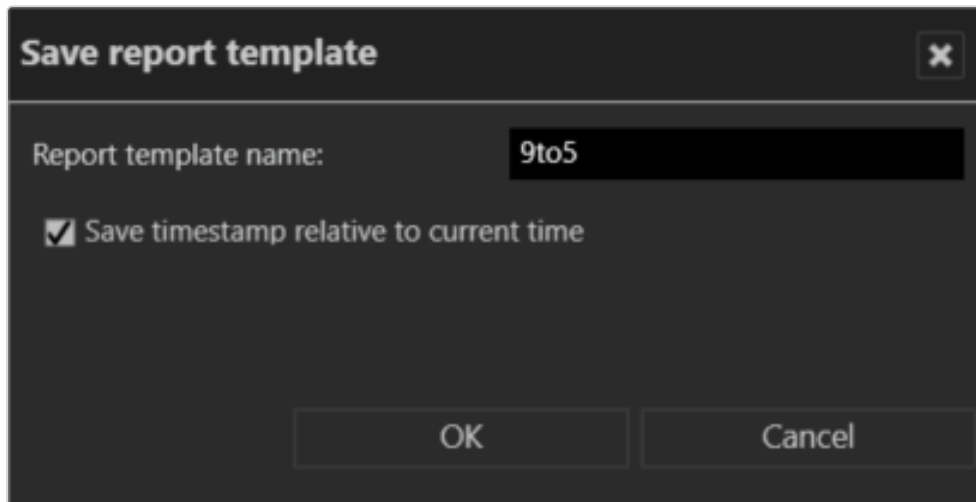


Abb. 91: Abfrage als Berichtvorlage speichern

2. Geben Sie den **Namen der Berichtvorlage** ein.
3. Optional können Sie **Zeitpunkt für aktuelle Zeit speichern** aktivieren. Bei Auswahl dieser Option wird das Zeitintervall der aktuellen Abfrage für die nächste Abfrage verwendet.
Beispiel Die aktuelle Abfrage sucht nach Ereignissen innerhalb der letzten 24 Stunden. Wenn die Abfrage mit dem entsprechenden Zeitpunkt gespeichert wird, sucht auch die nächste Abfrage innerhalb der letzten 24 Stunden - in Bezug auf die nächste Abfrage.
4. Speichern Sie die Abfrage mit **OK**.

Verwenden einer zuvor gespeicherten Abfrage

1. Wählen Sie den Namen der Abfrage im Aufklappmenü aus und dann **Abfrage starten**.

Löschen einer gespeicherten Abfrage

1. Um die gespeicherte Abfrage zu löschen, wählen Sie die Abfrage im Aufklappmenü aus und wählen dann **Löschen**.

Konfigurationsmodus

Für den Konfigurationsmodus werden ausreichende Administratorrechte benötigt.

Es wird dringend empfohlen, sich vor der Konfiguration des Systems mit dem Konzept der zugrunde liegenden Rechteverwaltung grundlegend vertraut zu machen (siehe „[Konzept](#)“ auf Seite 24).

Im Konfigurationsmodus werden alle Einstellungen, z. B. für die Hardware, das Netzwerk, das Unternehmen, Lagepläne sowie Alarmer und Benutzer, vorgenommen.

Im Steuerelement Administration können Sie der festgelegten Administration die entsprechende Hardware (z. B. Kameras), Aktionen und die Benutzerverwaltung zuweisen bzw. neue Objekte wie Alarmszenarien verwalten.

1. Um in den Konfigurationsmodus zu wechseln, klicken Sie auf das Symbol **Konfigurationsmodus** in der Modusleiste (siehe „[Die Modusleiste](#)“ auf Seite 136).

Weitere Einstellungen

- Für weitere Einstellungen zum Unternehmen siehe „[Unternehmen und Filialen](#)“ auf Seite 217.

Funktionen

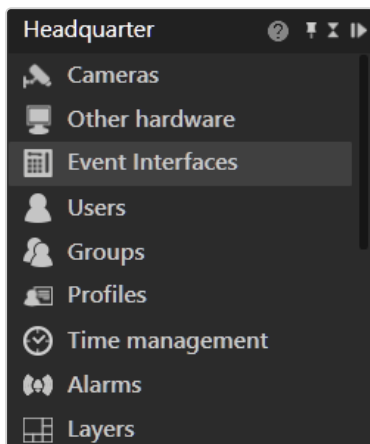


Abb. 92: Funktionen

Abhängig von der vorhandenen Hardware, der Netzwerkarchitektur sowie der Qognify VMS-Lizenz können die folgenden Funktionen konfiguriert werden:

- **Kameras:** Mit dieser Funktion konfigurieren und verwalten Sie die Kamera-Hardware und den dazugehörigen Videosever (siehe „[Kameras](#)“ auf Seite 231).
- **Sonstige Hardware:** Mit dieser Funktion konfigurieren und verwalten Sie zusätzliche Geräte (siehe „[Sonstige Hardware](#)“ auf Seite 296).
- **Event Interfaces:** Mit dieser Funktion können Sie Drittanbieter-Sicherheitssysteme konfigurieren, die mittels Plugins angebunden werden können (siehe „[Event Interfaces](#)“ auf Seite 349).
- **Benutzer:** Mit dieser Funktion konfigurieren und verwalten Sie die Benutzer (siehe „[Benutzer](#)“ auf Seite 357).
- **Gruppen:** Mit dieser Funktion konfigurieren und verwalten Sie die Benutzergruppen (siehe „[Gruppen](#)“ auf Seite 367).
- **Profile:** Mit dieser Funktion konfigurieren und verwalten Sie die Benutzer- und Gruppenprofile (siehe „[Profile](#)“ auf Seite 375).
- **Zeitverwaltung:** Mit dieser Funktion konfigurieren und verwalten Sie die Zeit-schablonen, um die Standardbildaufzeichnung einzelner oder mehrerer Kame-ras sowie die Gültigkeit in Alarmszenarien zeitlich zu koordinieren (siehe „[Zeitverwaltung](#)“ auf Seite 381).
- **Alarmer:** Mit dieser Funktion konfigurieren und verwalten Sie die Alarmszenarien (siehe „[Alarmer](#)“ auf Seite 386).

- **Ansichten:** Mit dieser Funktion konfigurieren und verwalten Sie die Ansichten, um im Überwachungsmodus mehrere Kameras oder Lagepläne anzuzeigen (siehe „[Überwachungsmodus](#)“ auf Seite 141).
- **Lagepläne:** Mit dieser Funktion konfigurieren und verwalten Sie die grafischen Übersichtskarten des überwachten Geländes bzw. Gebäudes, einschließlich des Anbringungsortes der Überwachungs-Hardware (siehe „[Lagepläne und „Erweiterte Lagepläne“](#)“ auf Seite 407).
- **Buttons:** Mit dieser Funktion konfigurieren und verwalten Sie die Aktionsfolgen, die im Überwachungsmodus in der Steuerung ausgelöst werden können (siehe „[Buttons](#)“ auf Seite 416).
- **Webseiten:** Mit dieser Funktion können beliebige Webseiten in die Ansicht eingebettet werden (siehe „[Webseiten](#)“ auf Seite 420).
- **Wächterrundgänge:** Mit dieser Funktion konfigurieren und verwalten Sie mehrere Kameras, eingestellte Positionen, Lagepläne und Ansichten nacheinander für eine frei definierbare Zeit (siehe „[Wächterrundgänge](#)“ auf Seite 422).
- **Sequenzen:** Mit dieser Funktion konfigurieren und verwalten Sie Aktionsreihenfolgen, in denen mehrere eingestellte Positionen nacheinander angefahren und/oder Aktionen ausgelöst werden (siehe „[Sequenzen](#)“ auf Seite 426).
- **Videowände:** Mit dieser Funktion konfigurieren Sie die Anordnung der Videowandbildschirme. Per Drag & Drop können Sie Kamerabilder, Ansichten, Lagepläne und Webseiten auf Videowänden anzeigen (zur Konfiguration der Bildschirme, siehe „[Sonstige Hardware](#)“ auf Seite 296).
- **Kennzeichengruppen:** Mit dieser Funktion konfigurieren und verwalten Sie die Kennzeichenerkennung des LPR-Moduls (siehe „[Kennzeichengruppen](#)“ auf Seite 432).
- **Server:** Mit dieser Funktion konfigurieren Sie die Gerätedienste (siehe „[Server](#)“ auf Seite 434).
- **System:** Mit dieser Funktion konfigurieren und verwalten Sie u. a. systemweite Einstellungen zum Netzwerk, zu automatischen Backups sowie zu Kommunikationseinstellungen und zur Ereignisverwaltung (siehe „[System](#)“ auf Seite 462).

Tastenkürzel für die Konfiguration

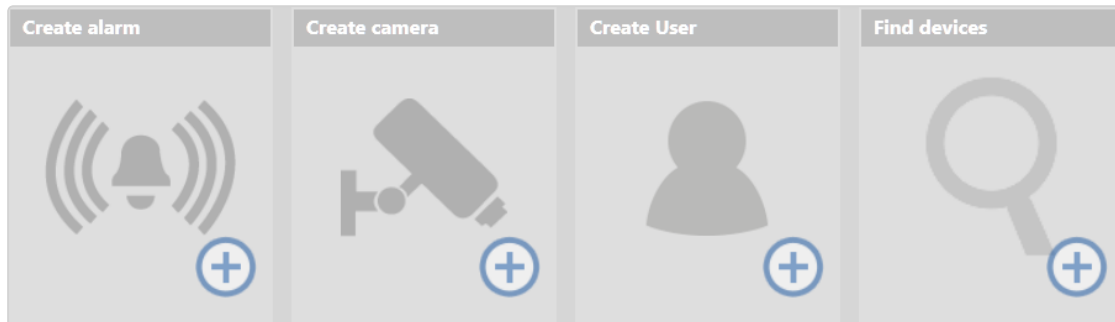


Abb. 93: Tastenkürzel für die Konfiguration

Sie finden die Tastenkürzel für die Konfiguration auf der Startseite des Konfigurationsmodus. Diese Tastenkürzel vereinfachen die Navigation zu den Einstellungen für neue Kameras und Alarmer sowie die Suche nach verfügbaren Geräten im Netzwerk. Sie können mit ihnen Einstellungen für die folgenden Aufgaben starten:

- Anlegen von Alarmen, siehe [„Alarme“ auf Seite 386](#)
- Anlegen von Kameras, siehe [„Kamera manuell anlegen“ auf Seite 231](#)
- Anlegen von Benutzern, siehe [„Benutzer anlegen“ auf Seite 357](#)
- Suchen verfügbarer Geräte, siehe [„Geräte suchen“ unten](#)

Geräte suchen

Anhand der IP-Adresse, die einem Netzwerkgerät (z. B. Kamera, Encoder) eindeutig zugewiesen ist, kann der Gerätesucher Netzwerkgeräte suchen und anzeigen. Mit dem Gerätesucher können IP-Kameras bequem in das Qognify VMS-System integriert werden.

1. Wählen Sie **Geräte suchen** in der Ansicht des Konfigurationsmodus. Alle erkannten Netzwerkgeräte (Kameras) werden im Fenster „Gerätesucher“ angezeigt. Unbekannte Netzwerkgeräte (d. h. noch nicht konfigurierte Kameras oder Router) werden mit grauer Schrift dargestellt.

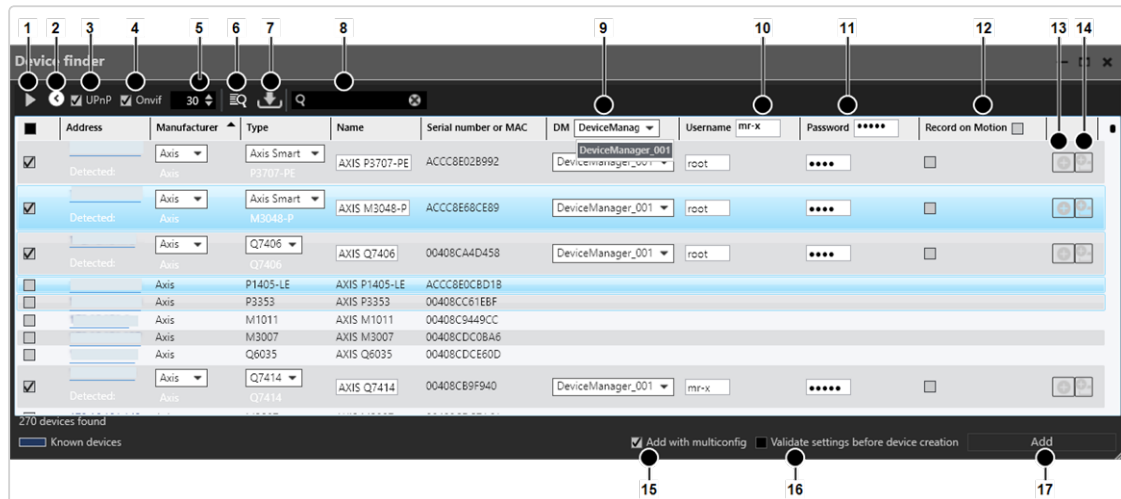


Abb. 94: Geräte suchen

Suchergebnisse filtern

1. Wenn nach dem ersten Suchlauf des Gerätesuchers nicht alle Netzwerkgeräte automatisch gefunden wurden, klicken Sie auf das **Dreieck** (1), um einen neuen Suchlauf im Netzwerk zu starten.
2. Um zusätzliche Netzwerkoptionen anzuzeigen, klicken Sie auf den **Kreis** (2). Der Gerätesucher unterstützt das ONVIF- (3), UPnP- (4) und Bonjour-Protokoll (verfügbar, wenn auf dem System installiert) zum Durchsuchen des Netzwerks nach Geräten.
3. Geben Sie das **Timeout** (in Sekunden) (5) für die Protokolle an. Damit wird festgelegt, wie lange jedes Protokoll nach neuen Geräten sucht. Nach dem Timeout muss die Suche manuell gestartet werden.
4. Klicken Sie auf den **Suchfilter** (6), um entweder alle verfügbaren oder alle unbekanntenen Geräte anzuzeigen.
5. Klicken Sie auf einen der Spaltentitel, um die Geräte nach **Adresse**, **Hersteller**, **Typ**, **Name** oder **Seriennummer oder MAC** (MAC-Adresse) zu sortieren.

6. Um die Ergebnisse zu filtern, geben Sie im Suchfeld einen der folgenden Suchbegriffe ein:
 - IP-Adresse
 - Hersteller
 - Gerätetyp
 - Name
 - Seriennummer oder MAC-Adresse

Einzelne Geräte hinzufügen

1. Wählen Sie die Kamera aus, die hinzugefügt werden soll, indem Sie das Kontrollkästchen in der ersten Spalte aktivieren.
2. Optional können Sie auf die IP-Adresse klicken, um die Geräte-Website in einem Webbrowser zu öffnen.
3. Ändern Sie bei Bedarf die Einstellungen für **Hersteller**, **Typ** und **DeviceManager** (DM).
4. Optional können Sie die Kamera benennen oder den Benutzernamen und das Passwort ändern.
5. Klicken Sie in der Kamerazeile auf **Hinzufügen** (13) oder klicken Sie auf **Hinzufügen und konfigurieren** (14). Nach Klicken auf **Hinzufügen und konfigurieren** wird das Fenster mit den Konfigurationseinstellungen für das betreffende Gerät angezeigt.
6. Konfigurieren Sie die Kamera (siehe „[Kameras](#)“ auf Seite 231).

Informationen zum Hinzufügen einer Kamera ohne den Gerätesucher finden Sie unter „[Kamera manuell anlegen](#)“ auf Seite 231.

Mehrere Geräte hinzufügen

Für alle ausgewählten Geräte können im Spaltentitel folgende Einstellungen vorgenommen werden:

- Device Manager (9)
- Benutzername (10)
- Passwort (11)
- Bewegungsabhängige Aufzeichnung (12)

1. Wählen Sie die Kameras aus, die hinzugefügt werden sollen, indem Sie die Kontrollkästchen in der ersten Spalte aktivieren.
2. Optional können Sie auf die IP-Adresse klicken, um die Geräte-Website in einem Webbrowser zu öffnen.
3. Ändern Sie bei Bedarf die Einstellungen für **Hersteller**, **Typ** und **DeviceManager** (DM).
4. Optional können Sie die Kamera benennen oder den Benutzernamen und das Passwort ändern.
5. Um die ausgewählten Kameras mit der Mehrfachkonfigurationsoption zu konfigurieren, wählen Sie **Mit Mehrfachkonfiguration hinzufügen** (15) (siehe „[Mehrere Kameras konfigurieren](#)“ auf Seite 291).
6. Optional können Sie **Einstellungen vor Anlegen von Geräten validieren** (16), um zu überprüfen, dass die konfigurierten Geräteeinstellungen korrekt sind.
7. Klicken Sie auf **Hinzufügen** (17).

Kamera-Import per CSV- oder XML-Datei

Mit der Kamera-Importfunktion können Kamerakonfigurationsdaten bequem mit Hilfe von strukturierten CSV- oder XML-Dateien importiert werden.

Voraussetzungen

Die Dateien müssen bestimmte Anforderungen erfüllen, bevor die Kameras importiert werden können.

Anforderungen an CSV-Dateien

Für die CSV-Importdatei gelten folgende Anforderungen:

- Die Einträge müssen durch ein Komma „**,**“ getrennt sein.
- Keine Leerzeichen vor oder nach einem Komma
- Die erste Zeile muss eine Kopfzeile sein.
- Die Kopfzeile muss die Strings **IPAddress** und **DisplayName** enthalten.
- Wenn Sonderzeichen (ß, ö, Ø, etc.) verwendet werden, muss die Datei im UTF-8-Format kodiert sein

Die Kopfzeilen-Strings werden automatisch erkannt. Die Reihenfolge spielt keine Rolle.

Darüber hinaus kann die CSV-Datei folgende Werte enthalten:

- MAC-Adresse
- DriverName: Der Wert für Treiber sollte derselbe sein wie in Qognify VMS für *Hersteller*, z. B. „Axis“ anstelle von „AxisDriver“
- Benutzername
- Passwort

Beispiel

```
DisplayName,MAC,IPAddress,Manufacturer,UserName,Password  
Front Door,,172.16.101.153,Axis,root,pass  
Back Door,0002D124EA0B,172.16.117.70,Vivotek,,  
Entrance,ABCDEFABCDEF,1.2.3.4,Test,UserName,Password
```

Anforderungen an XML-Dateien

Für die Importdatei mit XML-Struktur gelten folgende Anforderungen:

- Das erste Element muss **<config>** sein.
- Das erste untergeordnete Element muss **<Devices>** sein.
- Das Element **<Devices>** enthält alle Geräte.
- Jedes Gerät muss die Elemente **<IPAddress>**, **<Manufacturer>** und **<DisplayName>** enthalten.


Darüber hinaus kann die Datei „Device elements“ folgende Werte enthalten:

- MAC-Adresse
- DriverName
- Benutzername
- Passwort

Beispiel

```
<config>
  <Devices>
    <Device1>
      <DisplayName>ImportTest2 - Axis</DisplayName>
      <MAC/>
      <IPAddress>172.16.101.153</IPAddress>
      <Manufacturer>Axis</Manufacturer>
      <Cameras>
        <Camera1>
          <DisplayName>ImportTest - Axis</DisplayName>
        </Camera1>
      </Cameras>
    </Device1>
    <Device2>
      <DisplayName>ImportTest2 - Vivotek</DisplayName>
      <MAC>0002D124EA0B</MAC>
      <IPAddress>172.16.117.70</IPAddress>
      <Manufacturer>Vivotek</Manufacturer>
      <Cameras>
        <Camera1>
          <DisplayName>ImportTest - Vivotek</DisplayName>
        </Camera1>
      </Cameras>
    </Device2>
    <Device3>
      <DisplayName>ImportTest2 - Unbekannt</DisplayName>
      <MAC>ABCDEFABCDEF</MAC>
      <IPAddress>1.2.3.4</IPAddress>
      <Manufacturer>Test</Manufacturer>
      <Cameras>
        <Camera1>
          <DisplayName>ImportTest - Unbekannt 1</DisplayName>
        </Camera1>
        <Camera2>
          <DisplayName>ImportTest - Unbekannt 2</DisplayName>
        </Camera2>
      </Cameras>
    </Device3>
  </Devices>
</config>
```

CSV- oder XML-Datei importieren

1. Wechseln Sie in den Konfigurationsmodus und klicken Sie auf **Geräte suchen**.
2. Wählen Sie **Importieren** .

3. Wählen Sie die CSV- oder XML-Datei aus und importieren Sie sie.

Abhängig von der Anzahl und dem Typ der zu importierenden Geräte kann der Importvorgang eine Weile dauern.

- Solange der Gerätesucher eine Suche durchführt, erhalten Sie eine Meldung, dass die importierten Geräte noch nicht angezeigt werden.
- Wenn der Gerätesucher die Suche beendet hat, wird die importierte Konfiguration der Ergebnisliste des Gerätesuchers hinzugefügt.
- Bei Geräten, die in der importierten Konfiguration enthalten sind und die auch vom Gerätesucher gefunden werden, erfolgt das Hinzufügen der Konfiguration im Handumdrehen.
- Bei Geräten, die in der importierten Konfiguration enthalten sind, jedoch vom Gerätesucher nicht gefunden werden, versucht Qognify VMS, die Daten zu vervollständigen. Dies kann für jede Kamera einige Sekunden dauern.
- Der Fortschritt wird in einer Einblendung (kein Dialogfenster) angezeigt, sodass der Benutzer während des Imports weiter arbeiten kann.
- Nach Abschluss des Imports wird eine Meldung zum Importstatus und den verschiedenen Farben im Gerätesucher eingeblendet. Geräte, die vom Gerätesucher gefunden wurden, sind grün hervorgehoben, Geräte, die nicht gefunden wurden, sind rot hervorgehoben.

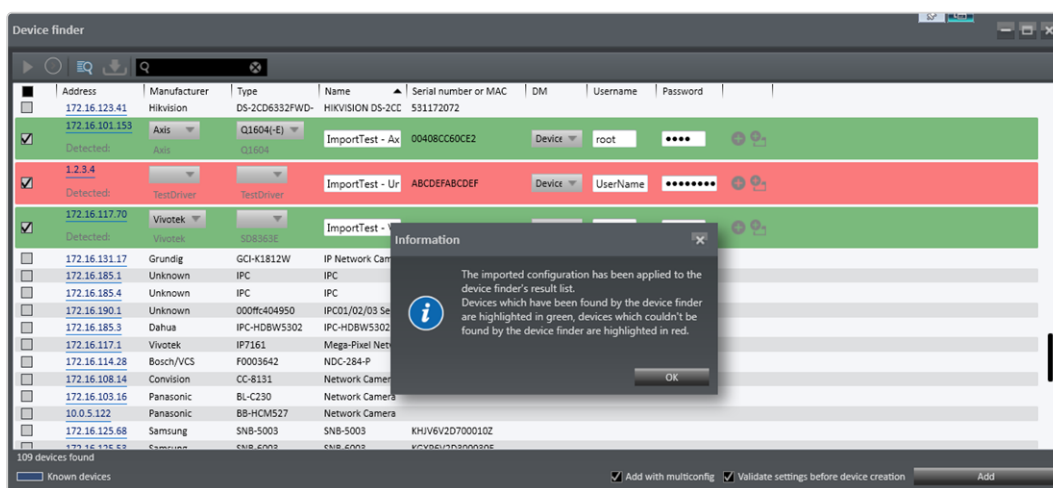


Abb. 95: CSV- oder XML-Datei importieren

Informationen zu weiteren Einstellungen finden Sie unter „Suchergebnisse filtern“ auf Seite 211.

Suchen im Konfigurationsmodus

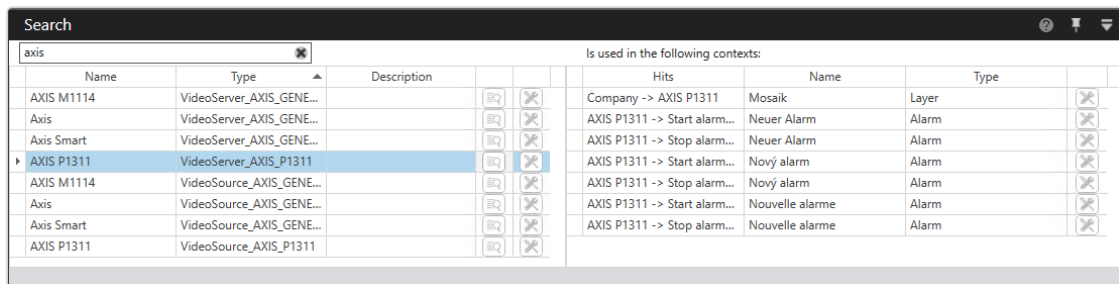




Abb. 96: Das Steuerelement Suchen im Konfigurationsmodus

Am unteren Rand der Arbeitsfläche befindet sich das Steuerelement **Suchen**, das Ihnen dabei hilft, die Inhalte der Serverdatenbank schneller zu finden. Die Suche startet ab der Eingabe des zweiten Zeichens und zeigt alle Ergebnisse in einer Liste an.

1. Geben Sie den Suchbegriff ein. Dabei kann es sich um einen Objektnamen oder eine Beschreibung handeln. Die Suche startet ab der Eingabe des zweiten Zeichens und zeigt alle Ergebnisse in einer Liste an. Zusätzlich erhalten Sie Informationen zum Typ.
2. Klicken Sie auf **Referenzen anzeigen** . In der rechten Spalte werden die zum gefundenen Begriff gehörenden Kontexte angezeigt.
3. Klicken Sie auf **Einstellung öffnen** . Die Einstellungen des Treffers werden geöffnet. Zum Bearbeiten von Elementen im Konfigurationsmodus sind möglicherweise Administrationsrechte erforderlich.
4. Zeigen Sie mit dem Mauszeiger auf den Spaltentitel, um den Filter für die ausgewählte Spalte festzulegen.

Unternehmen und Filialen

Dieses Steuerelement hilft Ihnen bei der Konfiguration der Filialen Ihres Unternehmens und der an jedem Standort eingesetzten Hardware (siehe „[Mit Filialen arbeiten](#)“ auf Seite 226). Bei der Installation des Programms wird ein „Unternehmen“ (Hauptfiliale) als Ausgangspunkt vorgegeben. Sie können den Namen der Hauptfiliale anpassen und ihr weitere Filialen und Filialgruppen zuordnen.

Die Hauptfiliale kann über Unterfilialen verfügen, Filialen können jedoch nicht über Unterfilialen oder Filialgruppen verfügen.

Informationen zu der Beziehung zwischen dem „Unternehmen“ und den Filialen finden Sie unter „[Beziehung zwischen der Hauptfiliale und ihren Unterfilialen](#)“ auf der nächsten Seite.

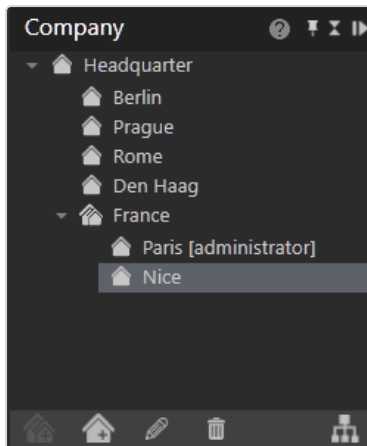


Abb. 97: Unternehmen und Filialen

In Qognify VMS sind Filialen dem „Unternehmen“ untergeordnet, das als Hauptfiliale angesehen werden kann. Daher kann die Verwaltung der Hauptfiliale auch die Verwaltung einer Unterfiliale umfassen, jedoch nicht umgekehrt. Entsprechend kann eine Unterfiliale auch nicht eine andere Unterfiliale oder die Hauptfiliale selbst verwalten. Mit Ausnahme von Kameras und DeviceManager-Servern gehören alle anderen Objekte zur Unterfiliale (beispielsweise kann ein Lageplan einer Unterfiliale nicht mit einer Kamera in der Hauptfiliale verbunden werden, der Lageplan der Hauptfiliale jedoch mit einer Kamera in der Unterfiliale).

Administrative Rechte vererben sich NICHT von der Hauptfiliale an die Unterfilialen und somit auch nicht an Filialgruppen. Doch Filialgruppen zugewiesene administrative Rechte werden für alle untergeordneten Filialen oder Filialgruppen übernommen.

Beziehung zwischen der Hauptfiliale und ihren Unterfilialen

Konzept

Zur Konfiguration der Hauptfiliale und ihrer Unterfilialen muss der Benutzer über administrative Rechte für alle relevanten Filialen verfügen. Um administrative Rechte für eine Unterfiliale zu besitzen, muss der Benutzer der Unterfiliale oder der Hauptfiliale zugewiesen werden.

Beispiel

- Benutzer „A“ verfügt über administrative Rechte für die Hauptfiliale „X“ und beide Unterfilialen „Y“ und „Z“. Er kann alle Filialen konfigurieren.

- Benutzer „B“ verfügt über administrative Rechte für die Unterfiliale „Y“, jedoch nicht für die anderen Filialen. Er kann nur Unterfiliale „Y“ konfigurieren.
- Benutzer „C“ verfügt über administrative Rechte für die Hauptfiliale „X“ und die Unterfiliale „Z“. Er kann Unterfiliale „Y“ und Filialen nicht konfigurieren.

Wie die Hauptfiliale können Unterfilialen Entitäten umfassen, die auf die Filiale selbst beschränkt sind. Entitäten der Hauptfiliale können nicht in einer Unterfiliale konfiguriert werden.

Entitäten wie Karten, Kameras oder Ebenen werden mit dem Core Service Main (CSM) der Hauptfiliale für alle Core Services konfiguriert. Die Entitäten „referenzieren“ daher einen Server (CSM oder CSS). Grundsätzlich sind nur Referenzen in der Unterfiliale bzw. von der Hauptfiliale zur Unterfiliale erlaubt.

Es gibt keine Referenzen zwischen Unterfilialen.

Für die Beziehung zwischen CSM und CSS siehe [„Kerndienste und Filialen“ auf Seite 22](#).

Die einzige Ausnahme für Referenzen vom CSS zum CSM sind Kameras und Device Management-Server. Hier kann die Kamera einer Unterfiliale über den Device Management-Server der Hauptfiliale verwaltet werden, sodass die Unterfilialen nicht ihren eigenen Device Management-Server installieren müssen.

Zulässige und unzulässige Referenzen

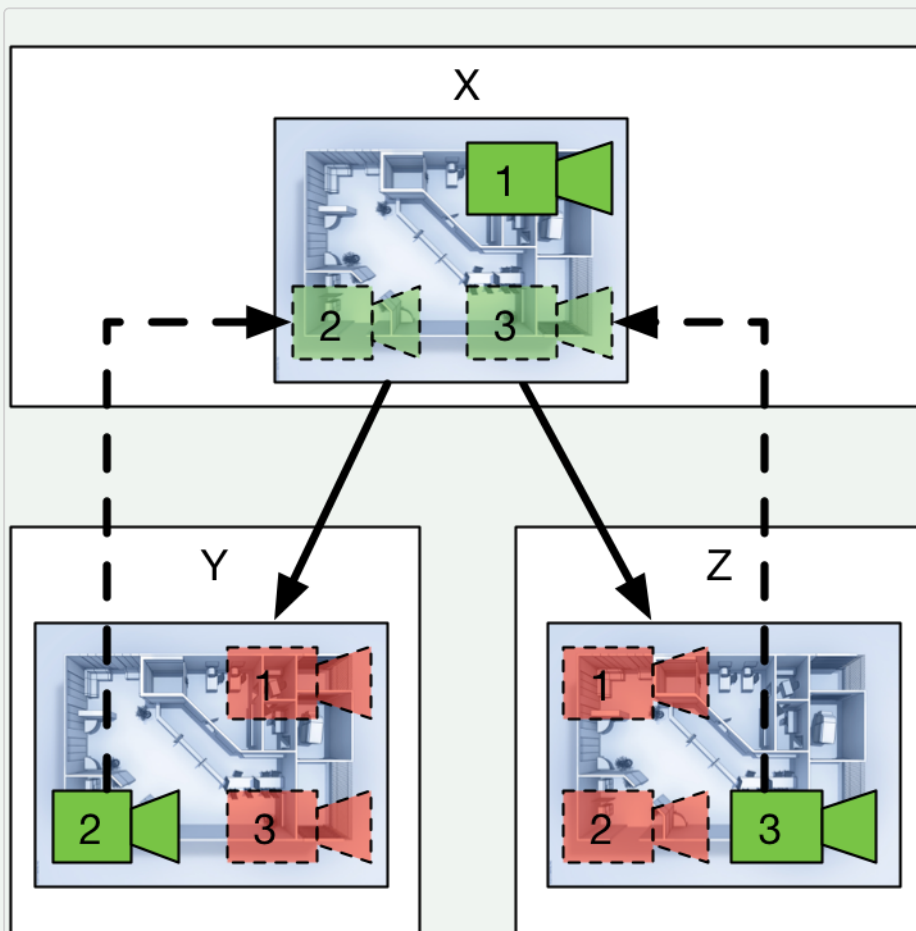
Wenn Entitäten oder Entitätengruppen (z. B. Lagepläne mit Kameras) zwischen Filialen verschoben wurden, müssen auch alle referenzierten Entitäten („Objekte“) verschoben werden. „Zulässige“ Referenzen sind nur möglich, wenn alle Entitäten einer Gruppe für die Unterfiliale, in die sie verschoben wurden, zugänglich sind. Anderenfalls entstehen „unzulässige“ Referenzen zur Hauptfiliale. Die einzige Ausnahme sind Entitäten in der Hauptfiliale, die Entitäten aus den Unterfilialen umfassen können.

Beispiel

In der Hauptfiliale „X“ wird Lageplan „A“ angelegt, der Kamera 1, 2 und 3 umfasst. Kamera 2 ist jedoch für die Unterfiliale „Y“ konfiguriert und Kamera 3 für die Unterfiliale „Z“. Daher werden die Kameras 2 und 3 in Lageplan „A“ referenziert.

Wenn Lageplan „A“ in die Unterfiliale „Y“ verschoben wird, sind Referenzen zu

Kamera 2 zulässig, Kamera 1 und 3 werden jedoch für Unterfiliale „Y“ unzulässig, da sich Kamera 1 noch in der Hauptfiliale „X“ befindet und in Unterfiliale „Y“ nicht referenziert werden kann. Ebenso befindet sich Kamera 3 noch in der Unterfiliale „Z“ und ist für Unterfiliale „Y“ nicht zugänglich, selbst wenn alle Kameras denselben Device Manager in der Hauptfiliale „X“ verwenden.



Beziehungstabelle

In der folgenden Tabelle werden die Elemente und deren Zugänglichkeit für die Hauptfiliale oder Unterfiliale im Konfigurationsmodus abhängig von dem Bereich, in dem das Element angelegt wurde, aufgeführt.

Erläuterungen zur Tabelle

- Eine Aktion für eine Kamera kann von der Unterfiliale nur aufgerufen werden, wenn sie in derselben Unterfiliale konfiguriert wurde. Aktionen, die in der Hauptfiliale konfiguriert wurden, können von der Unterfiliale nicht aufgerufen werden.
- Die Fahrspurkonfiguration des LPR-Moduls kann von der Unterfiliale aufgerufen werden, selbst wenn sie in der Hauptfiliale konfiguriert wurde. Die zugehörige Kamera muss jedoch in der Hauptfiliale konfiguriert werden.

Entität	Navigation im Konfigurationsmodus	Entitäten zugänglich für Unterfiliale, wenn in Hauptfiliale konfiguriert
Alle Intervalle (z. B. Alarmszenarien)		-
Hardware hinzufügen	Device Manager	x
Assistent	Device Manager	x
Kameraserver	Allgemein > Device Manager	x
Kamera	Allgemein > Aktion	-
	Aufzeichnung	-
Archiv	Allgemein > Device Manager	x
GND	Allgemein > Device Manager	x
SPS	Allgemein > Device Manager	x

Entität	Navigation im Konfigurationsmodus	Entitäten zugänglich für Unterfiliale, wenn in Hauptfiliale konfiguriert
SPC	Allgemein > Device Manager	x
Audioquelle	Allgemein > Device Manager	x
Fahrspur	Fahrspurkonfiguration > LPR-Modul	x
	Fahrspurkonfiguration > Kamera	-
	Fahrspurkonfiguration > Zugeordnete Kamera	-
Analytics	Allgemein > Analytics Modul	x
	Allgemein > Kamera	-
Analytics API	Allgemein > Analytics Modul	x
	Allgemein > Kamera	-
Buttons	Allgemein > Festgelegte Kamera	-
	Aktion	-
	2. Aktion	-
	Alarmszenario starten	-
	Alarmszenario beenden	-
	Wächterrundgang starten	-

Entität	Navigation im Konfigurationsmodus	Entitäten zugänglich für Unterfiliale, wenn in Hauptfiliale konfiguriert
Lagepläne		x ¹
Videowände		-
Ansichten		x ²
Benutzer	Allgemein > Gruppen	-
	Benutzerrechte	x ³
	Administrative Rechte Administrative Rechte vererben sich nicht auf die Filiale.	x ⁴
Gruppen	Allgemein > Trigger	-
	Benutzer	-
	Benutzerrechte	x ⁵

¹In der Unterfiliale definierte Lagepläne dürfen nur Entitäten aus der Unterfiliale umfassen. In der Hauptfiliale definierte Lagepläne können Entitäten aus der Hauptfiliale und den Unterfilialen umfassen.

²In der Unterfiliale definierte Ansichten dürfen nur Entitäten aus der Unterfiliale umfassen. In der Hauptfiliale definierte Ansichten können Entitäten aus der Hauptfiliale und den Unterfilialen umfassen.

³In der Unterfiliale definierte Benutzerrechte haben nur Zugriff auf Entitäten in der Unterfiliale. In der Hauptfiliale definierte Benutzerrechte haben Zugriff auf Entitäten aus der Hauptfiliale und den Unterfilialen.

⁴In der Unterfiliale definierte administrative Rechte haben nur Zugriff auf Entitäten in der Unterfiliale. In der Hauptfiliale definierte administrative Rechte haben Zugriff auf Entitäten aus der Hauptfiliale und den Unterfilialen.

⁵In der Unterfiliale definierte Benutzerrechte haben nur Zugriff auf Entitäten in der Unterfiliale. In der Hauptfiliale definierte Benutzerrechte haben Zugriff auf Entitäten aus der Hauptfiliale und den Unterfilialen.

Entität	Navigation im Konfigurationsmodus	Entitäten zugänglich für Unterfiliale, wenn in Hauptfiliale konfiguriert
	Administrative Rechte Administrative Rechte vererben sich nicht auf die Filiale.	x ¹
Profile	Allgemein > Ansichten	x
	Allgemein > Wächterrundgänge	x
	Videowand-Modulmapping > Mapping, definiert in Filiale	-
	Videowand-Modulmapping > Mapping, definiert im Unternehmen	x (Module)
Alarme	Start > Start Ereignisse	x
	Buttons	-
	Ende > Ende Ereignisse	x
	Ende > Buttons	-
	Visualisierung	x
	Profile	-
	Server > Aktionen Start	x
	Server > Aktionen Ende	x
	E-Mail und FTP	-

¹In der Unterfiliale definierte administrative Rechte haben nur Zugriff auf Entitäten in der Unterfiliale. In der Hauptfiliale definierte administrative Rechte haben Zugriff auf Entitäten aus der Hauptfiliale und den Unterfilialen.

Entität	Navigation im Konfigurationsmodus	Entitäten zugänglich für Unterfiliale, wenn in Hauptfiliale konfiguriert
Assistent, Kopierassistent	Start Ereignisse	x
	Kameras	x (Aktionen)
	Beteiligte Personen > Profile	-
	Kameras	x (Aktionen)
	Beteiligte Personen > Profile	-
Wächterrundgänge		x
Sequenzen		x
Server Failover-Server können nicht von einer anderen Unterfiliale übertragen werden. Der Failover Device Manager der Hauptfiliale kann nicht als Device Manager in einer Unterfiliale verwendet werden.	Transcoding-Server > Device Manager	x
	Device Manager > Allgemein > Failover	-
	LPR-Modul > Allgemein > Failover	-
	Analytics Modul > Allgemein > Failover	-
	Analytics API Modul > Allgemein > Failover	-
	Server Motion Detection Modul > Allgemein > Failover	-
	System	Ereignisverwaltung > Systemereignisse > Aktionen
	Ereignisverwaltung > Systemereignisse > E-Mail	-
	Ereignisverwaltung > Sys-	-

Entität	Navigation im Konfigurationsmodus	Entitäten zugänglich für Unterfiliale, wenn in Hauptfiliale konfiguriert
	temereignisse > Profile	
Client	Logoaktion > Ansichten	x

Mit Filialen arbeiten

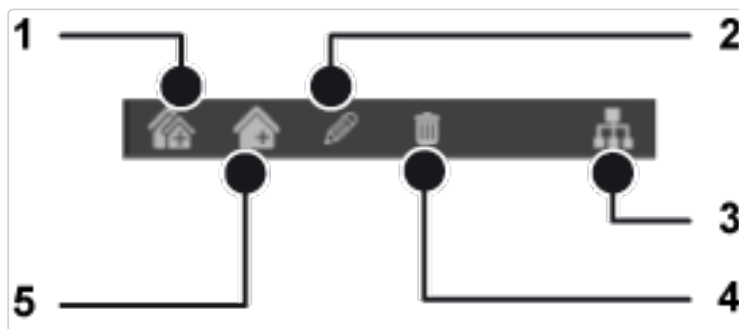


Abb. 98: Mit Filialen arbeiten

Filiale oder Filialgruppe anlegen

1. Um eine neue Filiale oder Filialgruppe anzulegen, klicken Sie auf **Neue Filialgruppe** (1) oder **Neue Filiale** (5).
2. Geben Sie den Namen der Filiale oder Gruppe an und bestätigen Sie mit **OK**. Die neue Filiale bzw. Gruppe wird angezeigt.

Namen einer Filiale oder Filialgruppe bearbeiten

1. Um den Namen einer angelegten Filiale oder Filialgruppe zu bearbeiten, wählen Sie die Filiale bzw. Gruppe im Fenster des Steuerelements aus.
2. Klicken Sie auf **Bearbeiten** (2).
3. Geben Sie der Filiale bzw. Gruppe einen neuen Namen und bestätigen Sie mit **OK**.

Filialen in Gruppen anordnen

Zur leichteren Navigation können Filialen in Filialgruppen angeordnet werden. Die Filialgruppen werden in den Baumansichten (Archivbaum, LPR-Baum usw.) im Steuerelement Unternehmen als Verzeichnisse angezeigt.

1. Um eine Filiale oder Filialgruppe in eine andere Filialgruppe zu verschieben, wählen Sie die Filiale (oder Filialgruppe) aus und ziehen Sie sie auf die Ziel-Filialgruppe.
2. Um eine Filiale aus einer Filialgruppe zu entfernen, wählen Sie die Filiale aus und ziehen Sie sie auf den Unternehmensnamen.

Filiale oder Filialgruppe löschen

1. Zum Löschen einer Filiale oder Filialgruppe wählen Sie diese aus und klicken Sie auf **Löschen** (4).

Wenn eine Filiale gelöscht wird, die mindestens eine Entität (Kamera, Button, Alarmszenario usw.) enthält, wird eine Warnung mit dem Hinweis angezeigt, dass diese Filiale nicht leer ist. Darüber hinaus wird eine Statistik zum Inhalt der Filiale angezeigt.

2. Klicken Sie auf **Löschen**.

Mit der Sitemap arbeiten

1. Klicken Sie auf **Lageplan** (3), um den Lageplan für die Installation anzuzeigen.

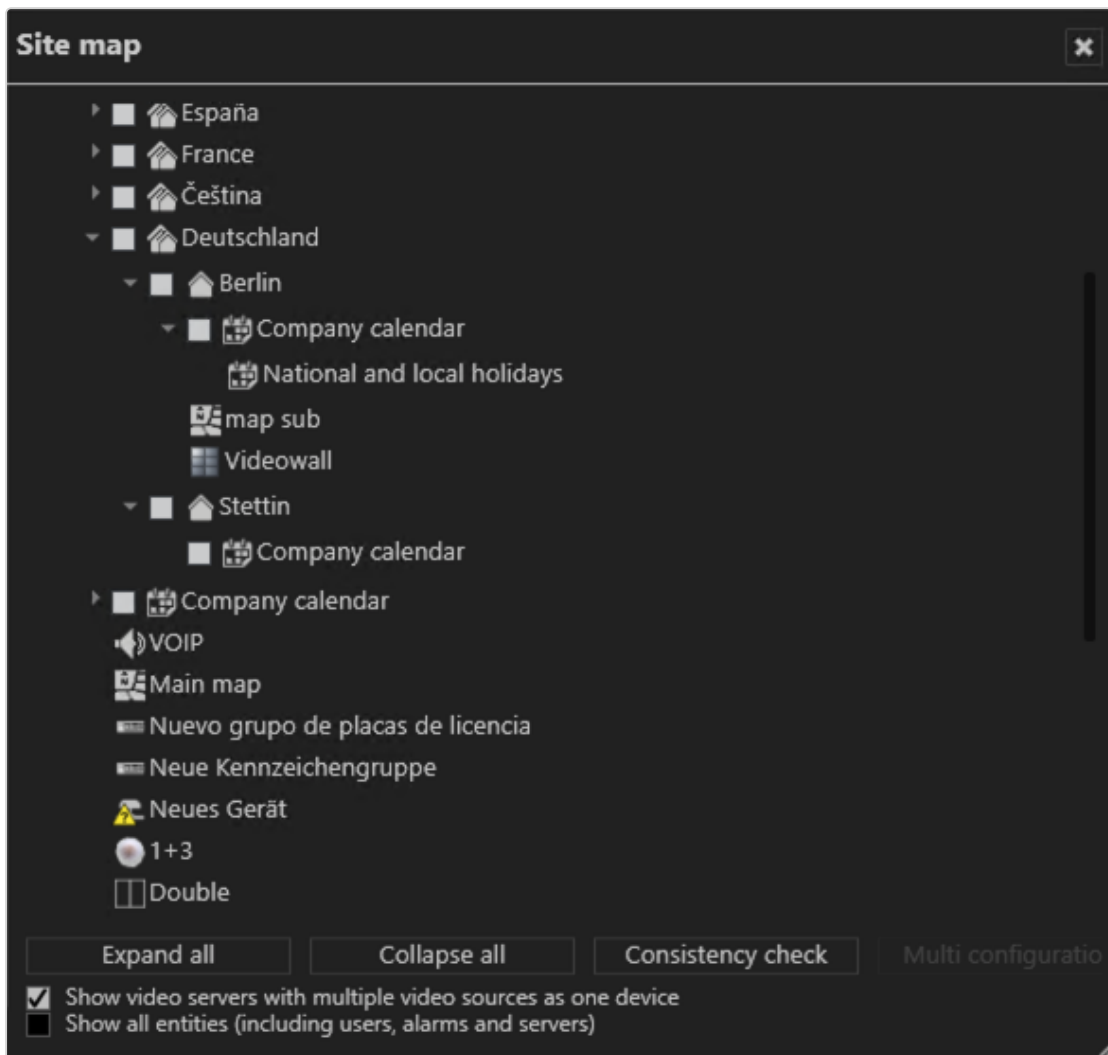


Abb. 99: Sitemap

Der Lageplan bietet die folgenden Funktionen:

- Anordnen von Objekten (Entitäten) in Filialen und Ordern mittels Drag & Drop
- Überprüfen, ob die Konsistenz der logischen Struktur der Beziehungen der in Filialen verteilten Objekte gültig ist (siehe „[Beziehung zwischen der Hauptfiliale und ihren Unterfilialen](#)“ auf Seite 218)

Objekte zwischen Filialen verschieben

Für das Verschieben von Objekten zwischen Filialen werden Administratorrechte für die Hauptfiliale benötigt. Administratoren von Unterfilialen haben keinen Zugriff auf die Hauptfiliale.

1. Um ein Objekt (Entität) von der Hauptfiliale („Unternehmen“) in eine Unterfiliale zu verschieben, wählen Sie die Hauptfiliale aus.

2. Wählen Sie das Objekt im Steuerelement Administration aus.
3. Ziehen Sie das ausgewählte Objekt per Drag &Drop in die Filiale.

Konsistenzcheck durchführen

Das Verschieben von Objekten zwischen Filialen kann zu inkonsistenten Bezügen führen. Es wird daher empfohlen, unmittelbar nach dem Verschieben von Objekten in eine andere Filiale einen Konsistenzcheck durchzuführen.

1. Wählen Sie **Videoserver mit mehreren Videoquellen als ein Gerät anzeigen**, um einen Encoder mit mehreren Kameras als ein Gerät anzeigen zu lassen. Anderenfalls werden alle zu einem Encoder gehörenden Kameras als separate Geräte angezeigt.
2. Wählen Sie **Alle Entitäten anzeigen**, um Objekte wie Benutzer, Alarme und Server anzuzeigen.
3. Klicken Sie auf **Konsistenzcheck**, um etwaige Inkonsistenzen anzeigen zu lassen. Informationen zu zulässigen und unzulässigen Referenzen finden Sie unter [„Beziehung zwischen der Hauptfiliale und ihren Unterfilialen“](#) auf Seite 218.

Bearbeitungsmenü im Steuerelement Administration

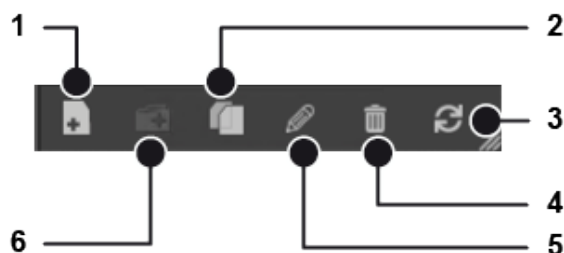








Abb. 100: Bearbeitungsmenü im Steuerelement Administration

Im Steuerelement **Administration** stehen Ihnen die folgenden Bearbeitungsmodi zur Verfügung:

- Objekt neu anlegen  (1)
- Objekt duplizieren  (2). Dazu darf nur ein Objekt ausgewählt sein.
- Ansicht aktualisieren  (3). Je nach Kontext wird ein Sortiersymbol angezeigt.

- Objekt löschen  (4).
- Objekt bearbeiten  (6). Dazu werden je nach Kontext viele einzelne Konfigurationsseiten oder eine Mehrfachkonfiguration geöffnet.
- Neuen Ordner anlegen  (2).

Kameras

Mit der Funktion **Kamera** in der Steuerleiste können Sie die Videohardware wie z. B. Kameras und Video-Encoder konfigurieren und verwalten.

Kamera manuell anlegen

Informationen zum schnellen Anlegen mehrerer Kameras mit dem Gerätesucher finden Sie unter [„Geräte suchen“ auf Seite 210](#).

1. Wählen Sie in der Kamera-Steuerleiste die Option **Objekt neu anlegen** aus.

Create camera [X]

Name:
Motion Detection Cam 1

Manufacturer:
Axis

Type:
Axis Smart Driver (H.264 Generation)

Use authorization

User name
root

Password
.....

Host (IP address or name): 10.0.111 Port: 80

DeviceManager:
DM1

OK Wizard Cancel

Validate settings before device creation

Abb. 101: Kamera anlegen

2. Geben Sie im Fenster „Kamera anlegen“ den Namen für die neue Kamera ein. Falls Sie die neue Kamera mit Hilfe des Konfigurationsassistenten einstellen möchten, wählen Sie **Assistent** (siehe „[Kamera mit dem Assistenten anlegen](#)“ auf Seite 234).

Mit dem Assistenten können keine Kameras angelegt werden, die den generischen Treiber verwenden. Der generische Treiber empfängt nur den Standard-Bildstrom (RTSP-Stream) von der Kamera.

3. Wählen Sie den **Hersteller** und den **Typ** der Kamera aus.

- **Generischer Videotreiber:** Mit dem generischen Videotreiber können Sie Kameras einbinden, die nicht in der Qognify-Software integriert sind. Die Funktionalität beschränkt sich dabei auf die Anzeige und die Aufzeichnung des Kamerabilds. Die Videoparameter müssen direkt auf der Kamera konfiguriert werden, z. B. die Auflösung und die Framerate. Qognify übernimmt keinerlei Gewährleistung für den einwandfreien Betrieb von Kameras, die über den Die Videoparameter müssen direkt auf der Kamera konfiguriert werden, z. B. die Auflösung und die Framerate-Videotreiber angebunden sind.
- **Intelligenter Kameratreiber:** Die herstellereigenen Kameratreiber beziehen die unterstützten Funktionen direkt von der Kamera. Qognify stellt Kameratreiber für verschiedene Hersteller bereit. Alle zum Zeitpunkt der aktuellen Freigabe verfügbaren Modelle werden unterstützt (für weitere Informationen sehen Sie sich das entsprechende PDF-Dokument im Download-Bereich der Qognify-Partner-Website an).

Bei manchen Modellen, die vom Herstellerstandard abweichen, kann der generische Kameratreiber ein anderes Verhalten zeigen. Alle Kameras, die mit einem generischen Treiber verwendet werden sollen, sollten getestet werden, bevor bindende Absprachen getroffen werden. Eine Liste zugelassener Geräte finden Sie im Dokument „Supported 3rd Party interfaces“ (Unterstützte Dritthersteller-Schnittstellen).

Generische Kameratreiber unterstützen keine Offline-Konfiguration. Bei Projekten mit vielen Kameras desselben Typs muss pro Modell mindestens eine Kamera angeschlossen und konfiguriert werden. Anschließend können die Kameras beliebig oft dupliziert und konfiguriert werden.

- **ONVIF-Treiber/ONVIF Profile-S-Treiber:** Mit dem ONVIF-Videotreiber können Sie Kameras einbinden, die nicht in der Qognify-Software integriert sind. Die Funktionalität beschränkt sich dabei auf die Anzeige und die Aufzeichnung des Kamerabilds. Die Videoparameter, z. B. Auflösung und Bildrate, sowie die Bewegungserkennung können abhängig von der ONVIF-Version konfiguriert werden. Qognify übernimmt keinerlei Gewährleistung für den einwandfreien Betrieb von Kameras, die über den ONVIF-Videotreiber angebunden sind.
 - **Qognify-Archiv:** Mit einer Qognify-Archivkamera können Aufzeichnungen importiert werden, die im Archivmodus als reguläre Kamera angezeigt werden (siehe „[Archivmodus](#)“ auf Seite 177).
 - **Qognify JPEG-Kamera-Emulator:** Videostreams können sich aus JPEG-Dateien zusammensetzen, die in einem bestimmten Ordner im Dateisystem gespeichert werden (z. B. laden Kameras ihre Bilder auf einen FTP-Server hoch). Daher ist der Videostream unabhängig von der Kamerahardware. Es sind auch sehr langsame Bildraten (z. B. 1 Bild pro Minute) möglich.
4. Aktivieren Sie gegebenenfalls eine erforderliche **Autorisierung** und geben Sie **Benutzernamen** und **Passwort** ein.
 5. Geben Sie den **Host**-Namen oder die IP-Adresse der Kamera ein.
 6. Wählen Sie gegebenenfalls den **Device Manager** aus. Falls mehrere Server für die Speicherung der Bilddaten installiert wurden (siehe „[Installation eines abgesetzten Servers](#)“ auf Seite 38), werden die verfügbaren Server angezeigt.
 7. Optional können Sie die Option **Einstellungen vor Anlegen von Geräten validieren** aktivieren. Diese prüft, ob die Kamera ordnungsgemäß implementiert werden kann.

Wenn die Prüfung fehlschlägt, kann die Kamera dennoch geladen werden und die Einstellungen können nachträglich geändert werden.

8. Bestätigen Sie die Angaben mit **OK**. Die neue Kamera wird in der Kamera-Steuerelemente angezeigt und kann konfiguriert werden (siehe „[Kamera konfigurieren](#)“ auf Seite 242).

Kamera mit dem Assistenten anlegen

Mit dem Kamerakonfigurationsassistenten können Sie eine Kamera mit wenigen Schritten integrieren. Die Einstellungen entsprechen den Schritten im Steuerelement

„Kameras“ (siehe „[Kamera manuell anlegen](#)“ auf Seite 231).

Mit dem Assistenten können keine Kameras angelegt werden, die den generischen Treiber verwenden. Der generische Treiber empfängt nur den Standard-Bildstrom von der Kamera.

Allgemeine Einstellungen

Camera configuration wizard

General settings

Do you want to activate digital inputs and/or outputs?

No
 Yes

Do you want to rotate the camera image?

No
 Yes

What data do you want to be displayed in the image?

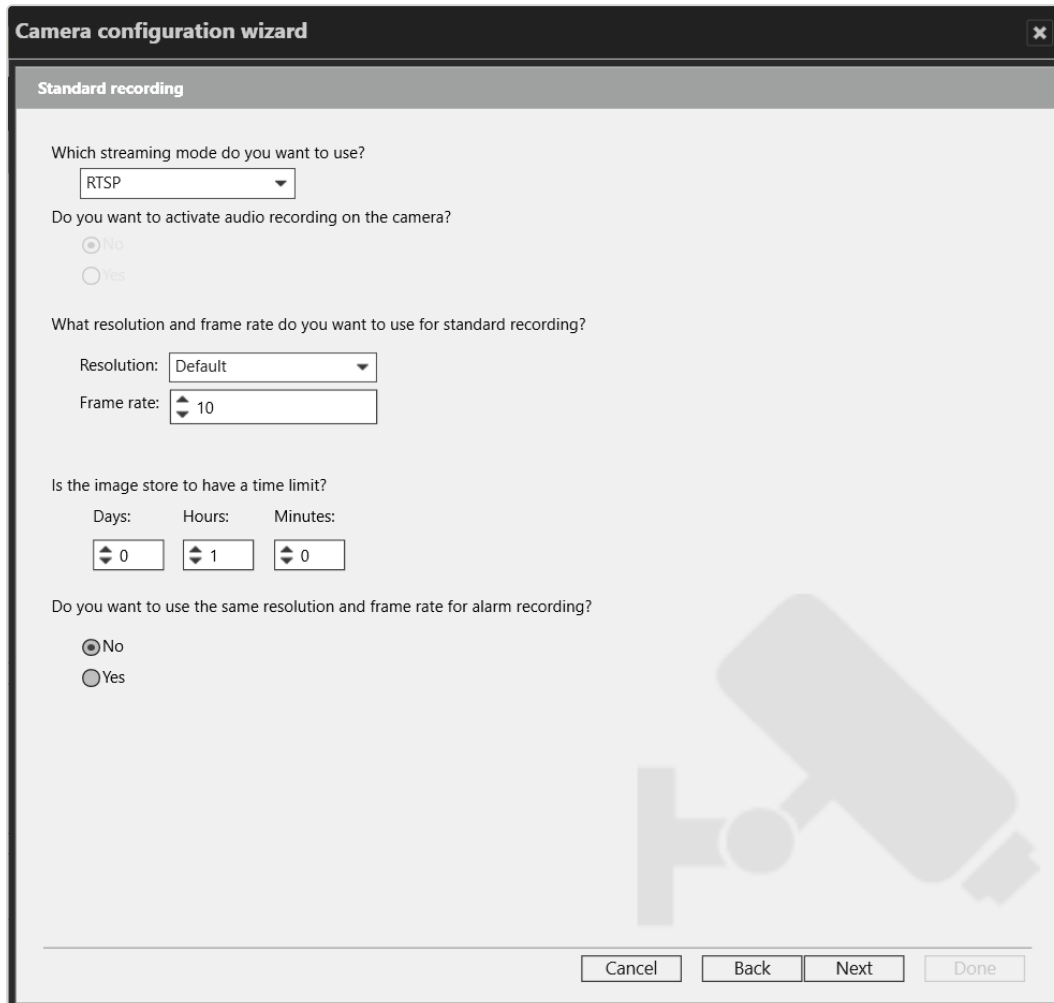
Title
 Date and time

Cancel Back Next Done

Abb. 102: Allgemeine Einstellungen

1. Wählen Sie **Ja**, um digitale Ein- oder Ausgänge zu aktivieren (sofern an der Kamera vorhanden), oder **Nein**, um sie zu deaktivieren.
2. Wenn die Kamera gedreht werden muss, wählen Sie den Drehwinkel aus.
3. Wählen Sie die Daten aus bzw. geben Sie die Daten ein, die im Kamerabild angezeigt werden.
4. Wählen Sie **Weiter**, um die Einstellungen für die Standardaufzeichnung zu definieren.

Standardaufzeichnung



The screenshot shows a 'Camera configuration wizard' window with a 'Standard recording' tab. The window contains the following settings:

- Which streaming mode do you want to use? (Dropdown menu): RTSP
- Do you want to activate audio recording on the camera? (Radio buttons): No (selected), Yes
- What resolution and frame rate do you want to use for standard recording?
 - Resolution: (Dropdown menu): Default
 - Frame rate: (Spin box): 10
- Is the image store to have a time limit?
 - Days: (Spin box): 0
 - Hours: (Spin box): 1
 - Minutes: (Spin box): 0
- Do you want to use the same resolution and frame rate for alarm recording? (Radio buttons): No (selected), Yes

At the bottom right, there are four buttons: Cancel, Back, Next, and Done.

Abb. 103: Standardaufzeichnung

1. Wählen Sie den Streaming-Modus aus (z. B. M-JPEG, H.264, H.265, RTSP).
2. Aktivieren Sie die Audioaufzeichnung (nur verfügbar in MPEG-4-, H.264- oder H.265-Streams).
3. Wählen Sie die **Auflösung** und **Bildrate** für die Standardaufzeichnung aus.
4. Legen Sie die Zeitbegrenzung für die Bildspeicherung fest.
5. Wählen Sie **Weiter**, um die Einstellungen für die Alarmaufzeichnung zu definieren.

Alarmaufzeichnung

Camera configuration wizard [X]

Alarm recording

What resolution and frame rate do you want to use for alarm recording?

Resolution:

Frame rate:

Is the image store to have a time limit?

Days: Hours: Minutes:

Abb. 104: Alarmaufzeichnung

1. Wählen Sie die **Auflösung** und **Bildrate** für die Alarmaufzeichnung aus.
2. Legen Sie die Zeitbegrenzung für die Bildspeicherung fest.
3. Wählen Sie **Weiter**, um eine Zusammenfassung Ihrer Einstellungen anzeigen zu lassen.

Zusammenfassung

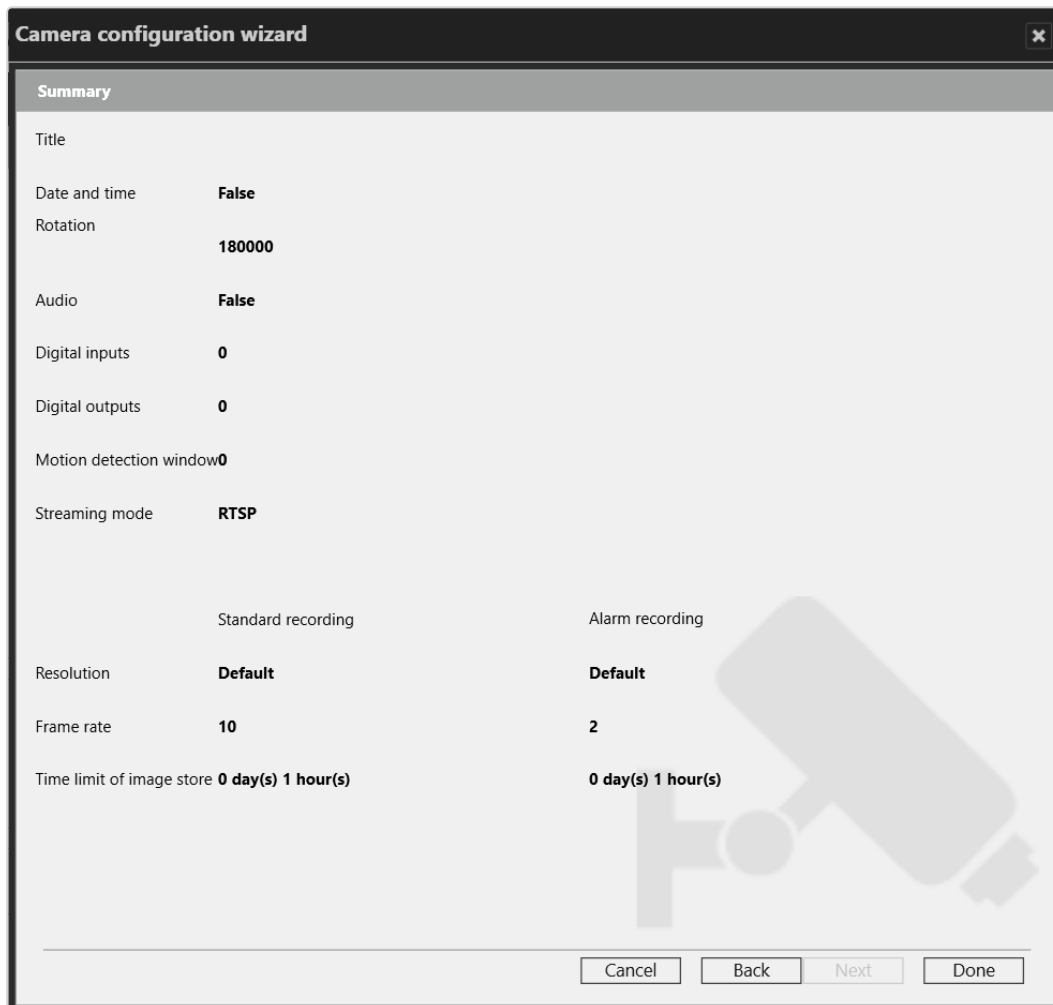
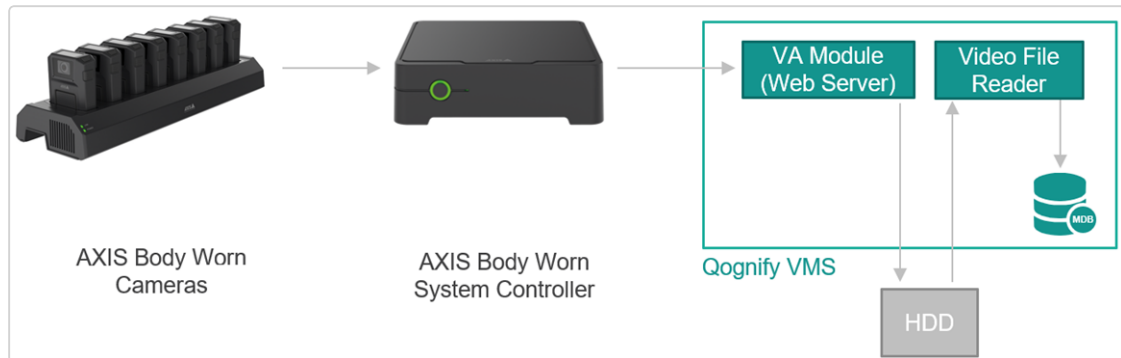


Abb. 105: Zusammenfassung

1. Überprüfen Sie die Einstellungen.
2. Um Änderungen vorzunehmen, wählen Sie **Zurück** und passen Sie die Einstellungen an.
3. Um die Einstellungen zu übernehmen, wählen Sie **Fertig**.

Die am Körper getragene AXIS-Kamerasteuerung



Der AXIS Body-Worn System Controller (BWSC) entlädt und speichert vorübergehend Videos von jeder am Körper getragenen AXIS-Kamera und sendet sie an Qognify VMS. Dazu muss bei der Einrichtung eine Verbindungsdatei erstellt werden, die in den BWSC hochgeladen werden muss.

Für die Nutzung des BWSC wird eine Lizenz benötigt. Ohne vorhandene Lizenz wird der Webserver-Port nicht geöffnet und es wird keine Verbindung zwischen der am Körper getragenen Steuerung und Qognify VMS hergestellt.

Nachdem der Videoimport abgeschlossen ist, werden die temporären Dateien von der lokalen Festplatte gelöscht.

Jeder Benutzer einer am Körper getragenen Kamera ist einem separaten Videokanal zugeordnet und benötigt eine Lizenz, auch wenn diese am Körper getragene Kamera gemeinsam mit anderen Benutzern verwendet wird (eine Lizenz pro Kanal).

Systemanforderungen und Voraussetzungen

- Achten Sie darauf, dass Sie für die am Körper getragenen Kamera genügend freien Speicherplatz für die temporäre Speicherung von Videodateien auf dem lokalen Laufwerk reservieren. Der Platzbedarf hängt von der Anzahl der verwendeten Kameras ab.
- Verwenden Sie einen Netzwerkadapter mit einer Übertragungsrage von mindestens 1 Gbit/s.
- Verwenden Sie einen NTP-Zeitserver, um die Zeit zwischen Qognify VMS und dem System der am Körper getragenen Kamera zu synchronisieren. Andernfalls könnten die Aufnahmen des Systems der am Körper getragenen Kamera mit einem falschen Zeitstempel importiert werden.

■ Die am Körper getragene Systemadministration (Kameras, Kameraeinstellungen, Benutzer usw.) muss durch den Body-Worn Manager erfolgen.

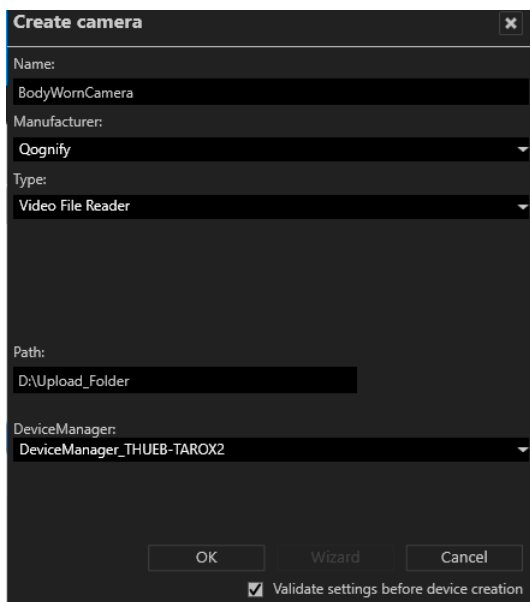
Sie können die Browseroberfläche des Body-Worn Managers als Website für Qognify VMS Administratoren hinzufügen.

Bekannte Einschränkungen

Die Kommunikation zwischen VMS und dem AXIS Body-Worn Camera System Controller kann nur über HTTPS erfolgen. Standardmäßig können alle TLS-Versionen für die HTTPS-Verbindung zwischen VA und Axis Controller verwendet werden. Wir empfehlen, SSL 3.0/TLS 1.0 und TLS 1.1 Windows-weit zu deaktivieren, wie in unserem Härteleitfaden beschrieben.

Konfigurieren des Anschlusses der am Körper getragenen Kamera

Voraussetzung: Im VA Administrationstool wurde ein „Body-Worn Camera Connector“ erstellt (siehe [„Hinzufügen eines Body-Worn Camera Connector Moduls“ auf Seite 529](#)).



1. Erstellen Sie eine neue Kamera und geben Sie „Qognify“ als **Hersteller** und „Videodatei-Leser“ als **Typ** ein.
2. Geben Sie ein Verzeichnis auf dem lokalen Laufwerk an, das vom Treiber überwacht werden soll. Dies ist das von Qognify VMS verwendete Verzeichnis, welches zum Videodateienimport verwendet wird.

3. Wählen Sie **OK**. Es wird eine neue virtuelle Kamera erstellt. Verwenden Sie das gleiche Verzeichnis wie für das AXIS Body Worn Camera VA Modul, in dem die Aufzeichnungen des am Körper getragenen Systems vorübergehend gespeichert werden.
4. Nehmen Sie ein Video mit einer AXIS Body-Worn Camera auf und stecken Sie diese in die Dockingstation, um die Videodateien in Qognify VMS zu importieren.
 - Für jeden Benutzer wird automatisch ein Videokanal erstellt, sobald seine erste Aufnahme importiert wird.
 - Jeder Benutzer einer am Körper getragenen Kamera erhält einen bereitgestellten Kanal, der ebenso im Archivmodus verfügbar ist.

Image storage			
Priority:	<input type="text" value="No"/>		
Standard recording:	<input type="text" value="Yes"/>		
Recording period:	<input type="text" value="Always"/>		
Time limit:	Days:	Hours:	Minutes:
	<input type="text" value="120"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Recording if:	<input type="text" value="Select"/>		
Show system message when last full frame is older than:	Days:	Hours:	Minutes:
	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Alarm recording:	<input type="text" value="No"/>		
Stream for Alarm recording	<input type="text" value="Stream 1/1"/>		
Time limit:	Days:	Hours:	Minutes:
	<input type="text" value="120"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Maximum pre-alarm buffer (s):	<input type="text" value="0"/>		

5. Legen Sie die Videoaufbewahrungsdauer für die **Bildspeicherung** fest. Der Anfangszeitraum beträgt 120 Tage.

Konfigurieren Sie eine zeitlich angemessene Aufbewahrungsfrist für Situationen, in denen ein Benutzer vergessen hat, eine Kamera für längere Zeit anzudocken oder eine Kamera verloren geht und wiedergefunden wurde. Falls die Aufbewahrungsfrist zu kurz ist, um den Zeitraum abzudecken, in dem eine Aufzeichnung erstellt wurde, wird diese direkt nach dem Import gelöscht.

Kamera konfigurieren

1. Wählen Sie die Kamera in der Übersicht aus. Die Einstellungen der Kamera werden im Hauptfenster angezeigt.

Netzwerkcameras bestehen aus einer Videosever-Einheit (Encoder) und mindestens einer Kameraeinheit. Entsprechend sind auch die Einstellungen einer Netzwerkkamera in Videosever-Einstellungen und Kameraeinstellungen getrennt. In den Videosever-Einstellungen werden alle verbindungspezifischen Parameter, in den Kameraeinstellungen alle Bildqualitäts- und Bildspeichereinstellungen vorgenommen.

Encoder/Kamera: Allgemein

General	
Activated:	<input type="text" value="Yes"/>
Name:	<input type="text" value="AXIS P1311"/>
Description:	<input type="text"/>
Manufacturer:	<input type="text" value="Axis"/>
Type:	<input type="text" value="P1311"/>
Firmware:	<input type="text" value="Undefined"/>
Host:	<input type="text" value="10.0.8.234"/>
HTTP port:	<input type="text" value="80"/>
HTTPS port:	<input type="text" value="443"/> <input type="text" value="No"/>
	<input type="button" value="Browser"/>
API version:	<input type="text" value="2.09"/>
DeviceManager server:	<input type="text" value="DeviceManager"/>
Authentication:	<input type="text" value="Yes"/>
User name:	<input type="text" value="root"/>
Password:	<input type="text" value="****"/>
Virtual cameras:	<input type="text" value="No"/>

Abb. 106: Encoder/Kamera: Allgemein

1. **Aktivieren** Sie die Kamera oder den Encoder.

Im Fall eines Mehrkanal-Encoders sind die angeschlossenen Kameras nicht mehr erreichbar.

2. Klicken Sie auf **Gerät abfragen**, beispielsweise wenn direkt an der Kamera Einstellungen geändert wurden.

Diese Funktion ist nur verfügbar, wenn die Kamera mit dem ONVIF-Treiber oder intelligenten Treiber integriert ist.

3. Geben Sie einen eindeutigen **Namen** für die Netzwerkkamera ein.

4. Geben Sie eine Beschreibung mit maximal 1.000 Zeichen ein. Die Beschreibung wird in den Export eingeschlossen und kann auch für mehrere Kameras festgelegt werden. Die Beschreibung ist auch im Konfigurationsexport-Tool verfügbar und wird in der Suche im Konfigurationsmodus angezeigt (siehe [„Suchen im Konfigurationsmodus“ auf Seite 217](#)).
5. Wählen Sie den Protokolltyp (**http** oder **https**) aus und ändern Sie gegebenenfalls die **Port**-Nummer.
6. Um das eingehende Kamerasignal zu testen, klicken Sie auf **Browser**. Der in den Systemeinstellungen festgelegte Browser („Standardbrowser“) wird gestartet und die Weboberfläche der Kamera direkt im Browserfenster angezeigt.
7. Die Programmschnittstelle (**API-Version**) wird automatisch erkannt.
8. Legen Sie einen **Videostrom-Netzwerk-Timeout(s)** zwischen 5 und 20 Sekunden fest. Legen Sie einen Wert für das Videostrom-Netzwerk-Timeout (s) zwischen 5 und 20 Sekunden fest. Wenn die Netzwerkverbindung zur Kamera vorübergehend unterbrochen ist, wird für die Dauer des festgelegten Werts eine Fehlermeldung unterdrückt und das zuletzt empfangene Bild wird weiterhin in der Kameraansicht angezeigt.

Diese Funktion ist nur verfügbar, wenn die Kamera mit dem ONVIF-Treiber oder intelligenten Treiber integriert ist.

9. Ändern Sie gegebenenfalls den **Device Manager-Server**.

Durch Ändern des Device Managers werden alle vorhandenen Aufzeichnungen gelöscht.

10. Wählen Sie aus, ob für die Kamera eine **Authentifizierung** erforderlich ist, und geben Sie gegebenenfalls einen **Benutzernamen** und ein **Passwort** ein.
11. Wählen Sie die Option **Virtuelle Kameras**, um von einer Kamera mehrere Bildausschnitte als eigenständige Kamera anzuzeigen und zu speichern.

Diese Funktion ist nur für bestimmte Kameramodelle verfügbar.

Nach dem Aktivieren der virtuellen Kamerafunktion werden automatisch mehrere virtuelle Kameras angelegt. Die Anzahl der virtuellen Kameras ist abhängig vom Kameramodell. Die Konfiguration erfolgt analog zu einer normalen Kamera. Die Bildausschnitte können dann in der virtuellen Kamerakonfiguration festgelegt werden (siehe [„Virtuelle Kamera \(Bildausschnitt\)“ auf Seite 250](#)).

Wartung

Diese Funktion gilt für Axis SD- und Bosch SD-Kameras.

Passwort übertragen

Die Wartungsfunktion ermöglicht es, das Kamerapasswort in einem Massenvorgang zu ändern, statt das Passwort für jede Kamera einzeln festzulegen.

The screenshot shows a 'Maintenance' window with the following fields and buttons:

- Label: 'Push new password to the camera: Password:' followed by an empty text input field.
- Label: 'Confirm password:' followed by an empty text input field.
- Button: 'Push password'.

Abb. 107: Wartung

1. Legen Sie das Kamerapasswort fest und geben Sie es zur Bestätigung erneut ein.
2. Wählen Sie **Passwort übertragen** aus. Die Kamera wird mit dem neuen Passwort neu gestartet.

Digitale Eingänge

Einige Kameras verfügen über digitale Eingänge, die kameraspezifische Funktionen auslösen können, wie etwa Neustarten der Kamera oder Einschalten des Kamerarlichts.


Input	Activated	Name for CLOSED	Icon	Name for OPEN	Icon	Dead time (s)
1	<input checked="" type="checkbox"/>	CLOSED: input 1		OPEN: input 1		1

Abb. 108: Digitale Eingänge

1. Aktivieren Sie die digitalen Eingänge und geben Sie jeweils einen eindeutigen **Namen für GESCHLOSSEN** und **Namen für OFFEN** an.
2. Geben Sie das Intervall für die **Totzeit** (in Sekunden) an, nach dem wieder ein Signal ausgewertet wird. Dies verhindert, dass sich bei kurz aufeinander folgenden Ereignissen die Ereignisdatenbank unnötig vergrößert. Diese Einstellung kann auch zum Auslösen eines Alarms verwendet werden (siehe [„Alarme“ auf Seite 386](#)).
3. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
4. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Digitale Ausgänge

Einige Kameras verfügen über digitale Ausgänge. Eine Zustandsänderung kann beispielsweise als Startereignis in einem Alarmszenario verwendet werden.

Digital outputs				
Output	Activated	Name for CLOSE	Name for OPEN	Hold time (s)
1	<input checked="" type="checkbox"/>	CLOSE: output 1	OPEN: output 1	3

Abb. 109: Digitale Ausgänge

1. Aktivieren Sie die digitalen Ausgänge und geben Sie jeweils einen eindeutigen **Namen für SCHLIESSEN** und **Namen für ÖFFNEN** an.
2. Geben Sie die **Haltezeit** für die Zeit (in Sekunden) an, in der ein Ausgang geöffnet oder geschlossen wird (0 = unendlich).

Kamera - Allgemein

General	
Activated:	Yes
Name:	AXIS M1114
Description:	
Stream audio/video:	Always
Camera ID:	1
Camera type:	Axis Smart Driver (H.2) Open converter
Display title:	Yes
Show date and time:	No
Custom icons :	
Streaming Priority:	Smooth video
Expose static URL:	Yes
	rtsp://<sgs ip>:<port>/video?staticentityid=4611967493619193569
Rotate image:	0°
Control camera:	No
360 lens:	No

Abb. 110: Kamera - Allgemeine Einstellungen - 1

1. Aktivieren oder deaktivieren Sie die Kamera.
2. Passen Sie gegebenenfalls den **Namen** der Kamera an.

3. Optional können Sie **Audio/Video streamen** wählen, um kontinuierliche oder On-Demand-Videostreams (Trigger-basiert) zu ermöglichen. Diese Funktion kann den Netzwerkverkehr reduzieren, z. B. in LTE-Umgebungen.
 - **Immer** (Standardeinstellung): Video-Streaming von der Kamera zum Device Manager ist verfügbar und die Streams können aufgezeichnet oder bei Bedarf sofort an den Client gesendet werden.
 - **On Demand**: Es wird kein Videostream von der Kamera gesendet. Video-Streaming kann beispielsweise durch ein Alarmereignis (siehe **Aktionen bei Alarmstart** unter „[Server](#)“ auf Seite 399) oder eine Button-Aktion (siehe „[Aktion](#)“ auf Seite 418) gestartet werden. Es keine eine Weile dauern, bis der Videostream aufgebaut ist.
 - **On Demand - Schnellstart**: Videostreams von der Kamera werden vom Device Manager verworfen. Video-Streaming kann beispielsweise durch ein Alarmereignis (siehe **Aktionen bei Alarmstart** unter „[Server](#)“ auf Seite 399) oder eine Button-Aktion (siehe „[Aktion](#)“ auf Seite 418) gestartet werden. Bei Bedarf ist der zugehörige Videostream sofort verfügbar.
4. Falls erforderlich, ändern Sie die **Kamera-ID** und passen Sie die ID der dazu gehörenden Kamera direkt an die Hardware an. Die Kamera-ID ist nur für bestimmte Kamerasteuerungen erforderlich.
5. Wählen Sie den **Kamera-Typ** aus:
 - **Kamera**: Die Kamera wird, abhängig vom Kameratyp, mit oder ohne PTZ-Steuerungsfunktionen verwendet.
 - **External PTZ**: Falls die Kamera über keine eigene PTZ-Steuerungseinheit verfügt, können Sie die Steuerungssignale eines Encoders an eine andere Kamera mit angebundener PTZ-Steuerungseinheit umleiten. Pro Umleitung wird ein eigenständiger RS-485-Port des Encoders benötigt.
6. Um den Kameratyp zu ändern, klicken Sie auf **Konverter öffnen** (siehe „[Kamera umwandeln](#)“ auf Seite 295).
7. Legen Sie fest, ob im Kamerabild ein Titel angezeigt werden soll, und geben Sie den **Titel** ein.
8. Wählen Sie, ob **Datum und Uhrzeit** im Kamerabild angezeigt werden sollen.
9. Wählen Sie für die Kamera ein **benutzerdefiniertes Symbol** aus (siehe „[Ton- und Symboldateien mit benutzerdefinierten Medien verwalten](#)“ auf Seite 482).

10. Ändern Sie ggf. die **Streaming-Priorität** von „Video glätten“ in „Niedrige Latenz“:
 - **Video glätten** (Standardeinstellung): Die Videobilder von der Kamera werden zunächst im Arbeitsspeicher (RAM) auf dem Qognify-Client dynamisch zwischengespeichert, bevor sie angezeigt werden. Dadurch werden Schwankungen bei der Live-Videoanzeige, die durch Probleme wie Netzwerk-Jitter, begrenzte Bandbreite, ungleicher Abstand zwischen den Bildern, sprunghafte Bildraten etc. verursacht werden, normalisiert.
 - **Niedrige Latenz**: Die Videobilder von der Kamera werden ohne Zwischenspeicherung in Echtzeit angezeigt. Daher kann eine unzureichende Bandbreite zu einer ruckeligen Videowiedergabe führen.
11. Stellen Sie **Freigeben der statischen URL** auf „Ja“, um eine statische IP-Adresse für die Kamera für die URL des Videostreams zu aktivieren.
 - Die Platzhalter der IP-Adresse und der Portnummer müssen durch die Adresse und den Port des SGS-Gateways ersetzt werden, mit dem die Kamera verbunden ist (siehe [„Gateway-Service-\(SGS-\)Modul konfigurieren“ auf Seite 452](#)).
 - Vergewissern Sie sich bei Verwendung des RTSP-Protokolls, dass „RTP_Over_RTSP_Over_TCP“ als Übertragungsmodus ausgewählt ist (siehe [„Videostream bearbeiten“ auf Seite 264](#)).
12. Falls die Kamera nicht aufrecht montiert wurde, verwenden Sie die Funktion **Bild drehen**, um das Bild in 90°-Schritten (90°, 180°, 270°) zu drehen. Wenn sich die Kamera nicht selbst drehen kann, übernimmt der Client die Drehung. Die seitliche Kameradrehung hat jedoch immer Vorrang.

Einstellungen für PTZ-Kameras

1. Aktivieren Sie **Kamera steuern** (nur für PTZ-Kameras verfügbar), falls Sie eine PTZ-Kamera oder eine Steuereinheit konfigurieren, damit der Benutzer die Möglichkeit hat, im Überwachungsmodus die Kamera zu steuern.
2. Legen Sie die **PTZ-Empfindlichkeit** (nur für PTZ-Kameras verfügbar) der Kamerasteuerung fest.
3. Aktivieren Sie die **Kameraposition** (nur für PTZ-Kameras verfügbar), damit der Benutzer die Möglichkeit hat, im Überwachungsmodus voreingestellte Kamerapositionen zu definieren und zu verwenden.

4. Aktivieren Sie **PTZ-Steuerung invertieren** (nur für PTZ-Kameras verfügbar), um Kameras korrekt zu steuern, z. B. auf dem Kopf stehend montierte Kameras.
13. Falls die Kamera über ein **360°-Objektiv** (Weitwinkel- oder Fisheye-Objektiv) verfügt, wählen Sie den Hersteller des Objektivs und seine Parameter aus.
 - Wenn an der Kamera verfügbar, aktivieren Sie den **Dewarping Mode** und legen Sie die **Position der Kamera** fest. Der Dewarping Mode bestimmt die Entzerrung des Fisheye-Objektivs.
 - Nachdem Sie eine geeignete Kamera ausgewählt haben, legen Sie den Dewarping Mode auf **Panorama** oder **Virtuelle PTZ-Steuerung** und die Kameraposition auf **Decke, Tisch** oder **Wand** fest.

The screenshot displays a configuration window for a camera. At the top, there is a section for 'Store object metadata' with a dropdown menu set to 'No'. Below this, there are several sections for defining actions in different states:

- Action in the case of inactivity:** A button labeled 'Edit' is shown, with 'No action selected' below it.
- Timeout (s):** A numeric input field containing the value '60'.
- Action at start of video stream:** A button labeled 'Edit' is shown, with 'No action selected' below it.
- Action when the video stream stops:** A button labeled 'Edit' is shown, with 'No action selected' below it.
- Action in the event of a network error:** A button labeled 'Edit' is shown, with 'No action selected' below it.
- Dead time (s):** A numeric input field containing the value '3600'.

Abb. 111: Kamera - Allgemeine Einstellungen - 2

14. Spezifizieren Sie die Einstellung für **Objektmetadaten speichern**.
 - Wenn auf „Ja“ gestellt, wird der Device Manager die Metadaten an den QogniFinder weiterleiten.
 - Wenn auf „Nein“, gestellt, wird der Device Manager keine Metadaten weiterleiten und die Kamera wird im QogniFinder nicht gezeigt.
15. Legen Sie fest, welche **Aktion bei Inaktivität** erfolgen soll, wenn eine PTZ-Kamera nicht gesteuert wird. Die gewählte Aktion wird angezeigt.
16. Legen Sie fest, nach welchem **Timeout (s)** in Sekunden die Aktion bei Inaktivität der PTZ-Kamera durchgeführt werden soll.

17. Legen Sie fest, welche **Aktion beim Start des Videostreams** und welche **Aktion beim Stopp des Videostreams** erfolgen soll. Die gewählten Aktionen werden angezeigt.
 - Die **Aktion beim Start des Videostream** wird ausgelöst, wenn ein Benutzer die Kamera im Überwachungsmodus im Vordergrund hat, also das aktuelle Live-Bild dieser Kamera betrachtet.
 - Die **Aktion beim Stopp des Videostreams** wird ausgelöst, wenn die aktuelle Kamera geschlossen oder eine andere Ansicht in den Vordergrund geholt wird.
18. Wählen Sie die **Aktion bei Netzwerkfehler** aus, um festzulegen, welche Aktion bei Inaktivität der Kamera aufgrund eines Netzwerkfehlers durchgeführt werden soll. Die gewählte Aktion wird angezeigt.
19. Definieren Sie für die gewählte Aktion eine **Totzeit (s)** in Sekunden, innerhalb der ein Netzwerkfehler nicht zur erneuten Auslösung der Aktion führt. Der Standardwert ist 3600 s.

Geografische Koordinaten

Die Kamera kann auf einem Lageplan anhand von GPS-Koordinaten lokalisiert werden. Die Koordinaten werden als Web Mercator-Mappings angegeben. Der Längengrad ist die Ost-West-Position und der Breitengrad die Nord-Süd-Position. Die Koordinaten werden mit der Funktion „Erweiterte Lagepläne“ synchronisiert (siehe „[Lagepläne](#) und „[Erweiterte Lagepläne](#)“ auf Seite 407).

Geo coordinates	
Coordinate system	Web Mercator EPSG:3857
Longitude	<input type="text" value="52.5162556"/>
Latitude	<input type="text" value="13.37708568573"/>

Abb. 112: Geografische Koordinaten

1. Geben Sie die geografischen Koordinaten der Kamera für den Längengrad ein.
2. Geben Sie die geografischen Koordinaten der Kamera für den Breitengrad ein.

Virtuelle Kamera (Bildausschnitt)

Wenn die Funktion „Virtuelle Kamera“ aktiviert wird (siehe „[Encoder/Kamera: Allgemein](#)“ auf Seite 243), werden standardmäßig alle virtuellen Kameras bis auf die erste deaktiviert.

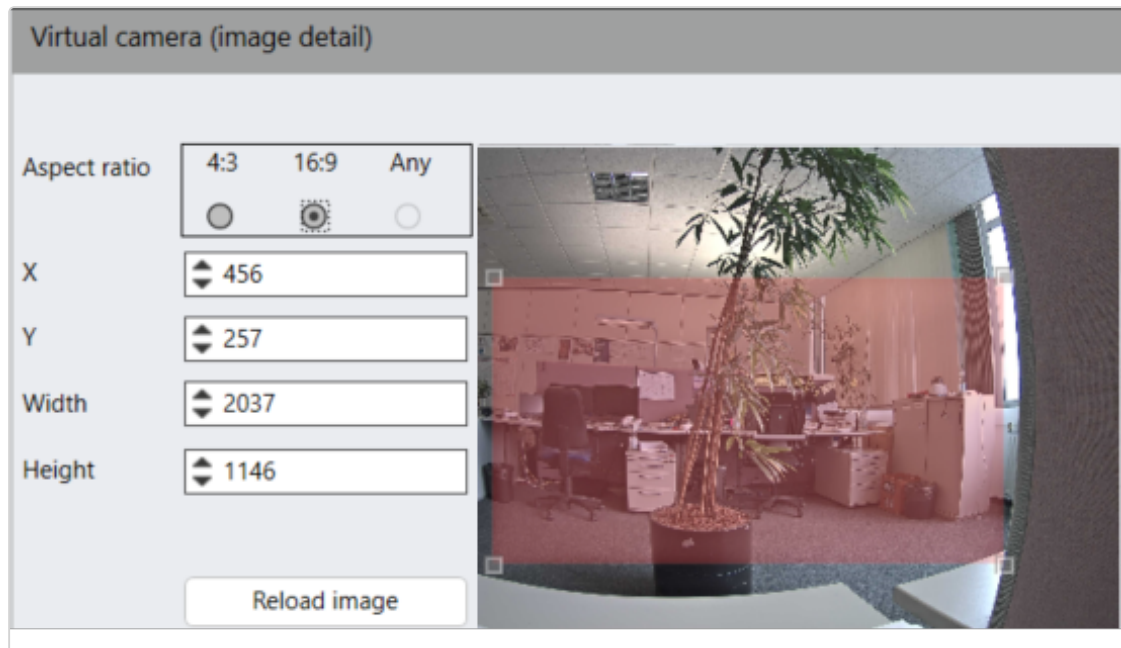


Abb. 113: Virtuelle Kamera (Bildausschnitt)

1. Wählen Sie das **Seitenverhältnis** der virtuellen Kamera (4:3, 16:9 oder Beliebig).

Die Option "Beliebig" ist nur verfügbar, wenn sie von der Kamera unterstützt wird.

Es wird empfohlen, in den Videostream-Einstellungen dasselbe Seitenverhältnis zu wählen (siehe „[Videostreams](#)“ auf Seite 263), da das Bild anderenfalls möglicherweise abgeschnitten wird.

2. Geben Sie die x- und y-Koordinate der rechten oberen Ecke des roten Rechtecks ein, das den Bildausschnitt definiert.
3. Geben Sie Breite oder Höhe des anzuzeigenden Bildausschnitts an.
 - Wird Breite gewählt, wird die Höhe in Abhängigkeit vom gewählten Seitenverhältnis automatisch skaliert.
 - Wird Höhe gewählt, wird die Breite in Abhängigkeit vom gewählten Seitenverhältnis automatisch skaliert.
 - Optional kann auch das Blickfeld durch Ziehen der Eckpunkte skaliert werden.
4. Um die Position des ausgewählten Bereichs im Bild zu ändern, klicken Sie auf den ausgewählten Bereich und verschieben Sie ihn mit gedrückter Maustaste.
5. Klicken Sie auf **Bild neu laden**, um eine neue Momentaufnahme der Szene zu erstellen.

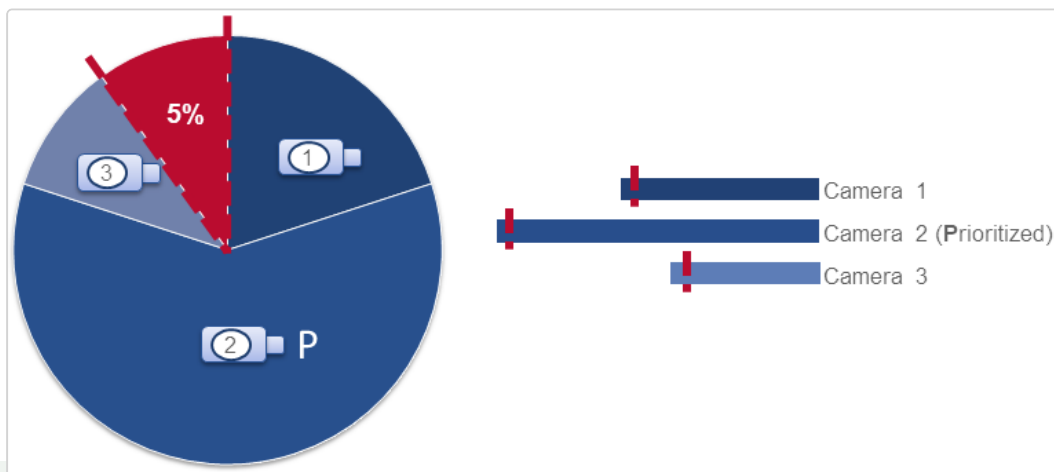
Bildspeicherung

In diesem Abschnitt wird die Konfiguration von Bedingungen für Standard- und Alarmaufzeichnungen sowie das Verhalten des Edge-Speichers und der bewegungsabhängigen Aufzeichnung beschrieben.

MultimediaDatabase

Videoaufzeichnungen werden in der MultimediaDatabase in einer Warteschlange auf Basis eines so genannten „Ringpuffers“ gespeichert. Die folgende Abbildung gibt einen kurzen Überblick.

Übersicht



Wenn die Speicherbelegung 85 % erreicht, wird per SNMP, E-Mail oder als Nachricht die Meldung **Zone fast voll** an den Client gesendet. Sobald die Speicherbelegung 95 % erreicht, beginnt das Ringpuffersystem damit, die ältesten Videodaten zu löschen, um Festplattenspeicher für neue Aufzeichnungen freizugeben. Die Bilddaten der priorisierten Kameras (P) werden als Letzte gelöscht.

Alle Einstellungen zur Bildspeicherung (z. B. die Größe des belegten Speichers einer Kamera auf der Festplatte) werden in diesem Bereich konfiguriert. Um das Überschreiben sensibler Bilddaten zu vermeiden, werden Standard- und Alarmaufzeichnungen getrennt konfiguriert.

Wenn die Speicherbelegung 95 % erreicht, werden die ältesten Aufzeichnungen in folgender Reihenfolge gelöscht:

1. Standardaufzeichnungen
2. Alarmaufzeichnungen
3. Priorisierte Standardaufzeichnungen
4. Priorisierte Alarmaufzeichnungen

Image storage

Priority:

Standard recording:

Recording period:

Time limit: Days: Hours: Minutes:

Recording if:

Show system message when last full frame is older than: Days: Hours: Minutes:

Alarm recording:

Stream for Alarm recording:

Time limit: Days: Hours: Minutes:

Maximum pre-alarm buffer (s):

Maximum post-alarm duration (s):

Show system message when last full frame is older than: Days: Hours: Minutes:

Standard recording data aging:

Alarm recording data aging:

Timespan with full data rate (days):

Frame rate (fps):

Abb. 114: MultimediaDatabase-Einstellungen

1. Wählen Sie **MultimediaDatabase** im Menü „Bildspeicherung“ aus.
2. Legen Sie fest, ob die Bildaufzeichnung über eine **Priorität** verfügt. Wenn die Speicherbelegung 95 % erreicht, beginnt das Ringpuffersystem damit, die ältesten Bilddaten zu löschen. Die aufgezeichneten Bilddaten der priorisierten Kameras werden als Letzte gelöscht (siehe Löschreihenfolge oben).
3. Aktivieren Sie, ob mit dieser Kamera **Standardaufzeichnungen** durchgeführt werden sollen.

4. Wählen Sie den **Aufnahmezeitraum** aus. Den genauen Zeitraum legen Sie mit einer Zeitschablone fest, die Sie in der Zeitverwaltung erstellen (siehe [„Zeitverwaltung“ auf Seite 381](#)). Standardmäßig wird eine Daueraufzeichnung („Immer“) gestartet.
5. Aktivieren Sie die **Zeitbegrenzung** und geben Sie die maximale Speicherdauer an. Bei Überschreiten der Zeitbegrenzung werden Aufzeichnungen, die älter als die festgelegte Zeitbegrenzung sind, gelöscht.
6. Im Bereich **Aufzeichnung wenn** können Sie eine Bedingung für verfügbare digitale Eingänge auswählen, bei der die Bildaufzeichnung gestartet werden soll.

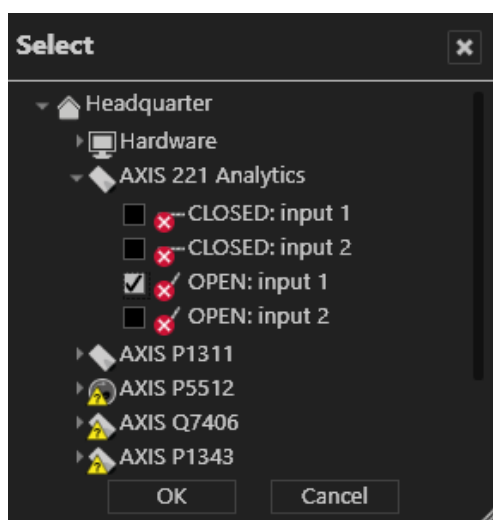


Abb. 115: MultimediaDatabase - Bedingung auswählen

7. Spezifizieren Sie das Zeitintervall, nach dem eine Mitteilung angezeigt wird, wenn das letzte Vollbild der Standardaufnahme erreicht ist. Dies hilft bei der Überwachung des für Standardaufnahmen erforderlichen Speicherplatzes.
8. Aktivieren Sie, ob mit dieser Kamera **Alarmaufzeichnungen** durchgeführt werden sollen.
9. Wählen Sie einen **Stream für Alarmaufzeichnung** aus. Zur Verwendung dieser Funktion muss die Multi-Stream-Funktion von der Kamera unterstützt und konfiguriert werden (siehe [„Videostreams“ auf Seite 263](#)).
10. Aktivieren Sie die **Zeitbegrenzung** und geben Sie die maximale Speicherdauer an. Bei Überschreiten der Zeitbegrenzung werden die Aufzeichnungen, die älter als die festgelegte Zeitbegrenzung sind, gelöscht.

11. Geben Sie einen **Max. Voralarm-Puffer** an (bis zu 3600 s), um einen Zeitraum aufzuzeichnen, wenn die Standardaufzeichnung deaktiviert oder ein zusätzlicher Stream für die Alarmaufzeichnung definiert ist. Der Voralarm-Puffer definiert die maximale Länge der Voralarmdauer, die in einem Alarmszenario konfiguriert werden kann (Informationen zur Alarmkonfiguration siehe Einstellungen unter „[Server](#)“ auf Seite 399). Die im Pufferspeicher aufgezeichneten Daten werden mit Beginn der manuellen Aufzeichnung in die Alarmaufzeichnungsspur übertragen (siehe „[Manuelle Alarmaufzeichnung](#)“ auf Seite 154).

Der Voralarm-Puffer wird nur berücksichtigt, wenn keine Standardaufzeichnung verfügbar ist.

12. Geben Sie eine **Maximale Nachalarmdauer** an, um bei einer manuellen Alarmaufzeichnung im Überwachungsmodus zusätzlich einen Zeitraum nach der Alarmauslösung aufzuzeichnen (siehe „[Manuelle Alarmaufzeichnung](#)“ auf Seite 154). Wird die manuelle Alarmaufzeichnung nicht beendet, stoppt die Aufzeichnung automatisch am Ende der festgelegten Nachalarm-Dauer.
13. Spezifizieren Sie das Zeitintervall, nach dem eine Mitteilung angezeigt wird, wenn das letzte Vollbild der Alarmaufzeichnung erreicht ist. Dies hilft bei der Überwachung des für die Alarmaufzeichnungen erforderlichen Speicherplatzes.
14. Aktivieren Sie das automatische Verringern der Bildrate der Standardaufzeichnungen bzw. Alarmaufzeichnungen nach einer bestimmten Zeitspanne (**Data Aging Standard Aufzeichnung** bzw. **Alarmaufzeichnung Data Aging**). Nach Ablauf der festgelegten Zeitspanne wird die Bildrate der gespeicherten Aufzeichnungen reduziert, um Speicherplatz zu sparen (Data-Aging).

Der Data Aging-Prozess komprimiert nur die Bilddaten des Tags vor dem konfigurierten Tag.

Beispiel Sie zeichnen einen H.264-Stream mit 20 Bildern pro Sekunde mit einem I-Frame-Abstand von einer Sekunde auf. Durch das Data Aging wird die Bildrate dann auf ein Bild pro Sekunde reduziert, da alle P-Frames gelöscht werden. Trackingdaten und Audioaufzeichnungen werden immer gelöscht.

15. Geben Sie die **Zeitbegrenzung** an, nach der die Aufzeichnungen komprimiert und von der Audiospur befreit werden sollen.
16. Geben Sie die **Bildrate** (in fps) an, mit der die Aufzeichnungen nach Überschreiten der Zeitbegrenzung gespeichert werden sollen. Damit werden die Bilddaten auf die eingestellte Bildrate reduziert.
 - Motion JPEG-Aufzeichnungen werden auf die angegebene Bildrate reduziert.
 - MPEG-4/H.264/H.265-Aufzeichnungen werden auf I-Frames reduziert (die P-Frames werden gelöscht).
17. Legen Sie einen Zeitrahmen fest, nachdem eine Systemmeldung ausgelöst wird, wenn das letzte aufgezeichnete Vollbild älter als die angegebene Zeit ist. Damit die Meldung „Das letzte Archivbild ist älter als der konfigurierte Wert“ ausgegeben wird, muss die Ereignisverwaltung entsprechend konfiguriert werden (siehe [„Ereignisverwaltung konfigurieren“](#) auf Seite 468).

Lückenfüllung

Die Lückenfüllung füllt Aufzeichnungslücken für die Zone mit den Aufzeichnungen aus dem Edge-Speicher.

Weitere Einstellungen werden unter „[Edge-Speicher](#)“ auf Seite 260 beschrieben.

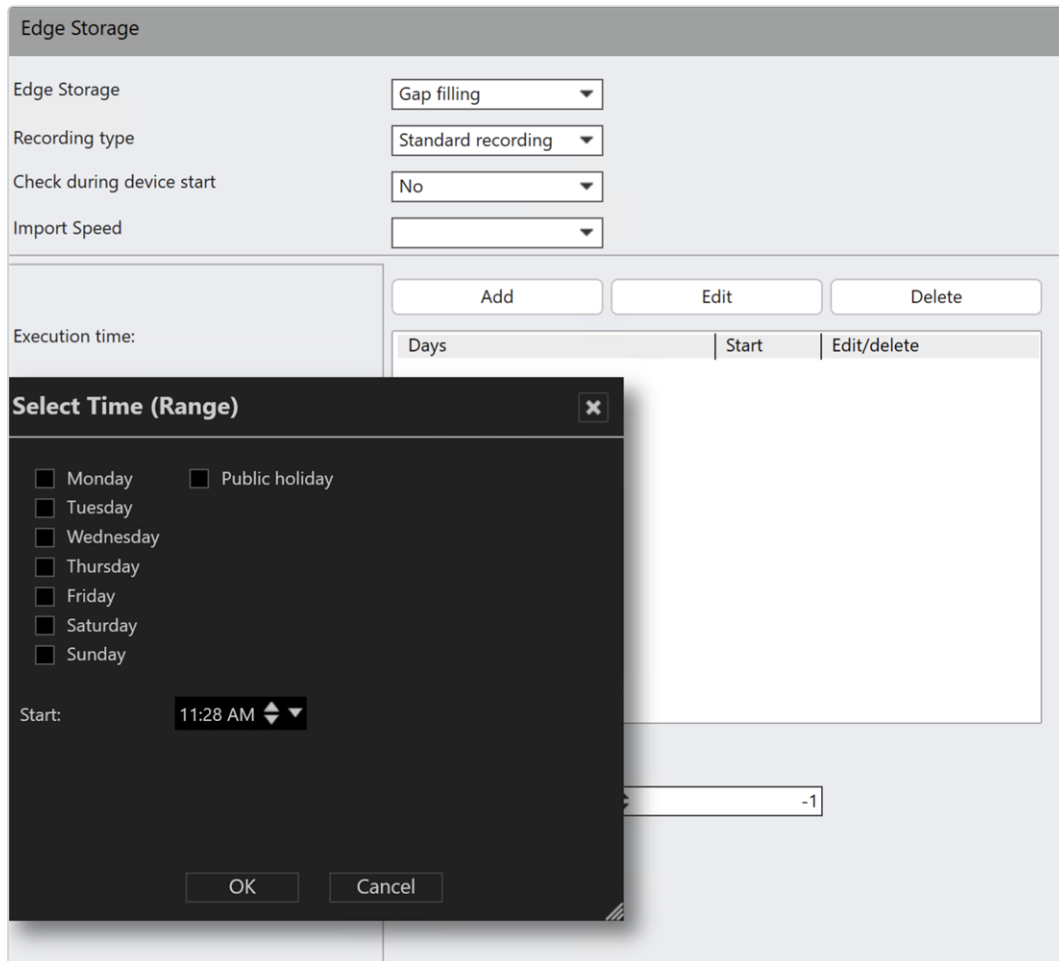
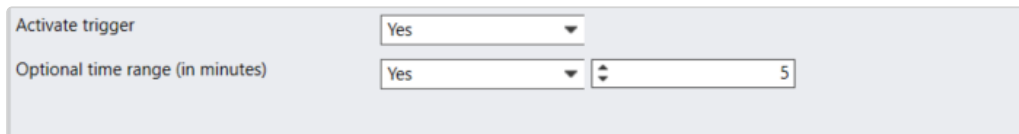


Abb. 116: Lückenfüllung - 1

1. Wählen Sie für den **Edge-Speicher** die Option **Lückenfüllung**.
2. Legen Sie bei **Aufzeichnungstyp** fest, ob die importierten Bilddaten als **Standardaufzeichnung** oder **Alarmaufzeichnung** behandelt werden sollen.

3. Fügen Sie bei **Ausführungszeit** mindestens einen Zeitplan hinzu und legen Sie den Zeitpunkt fest, zu dem Qognify VMS automatisch nach Aufzeichnungslücken suchen und diese füllen soll.

Es wird eine tägliche Systemprüfung empfohlen.



The screenshot shows a configuration panel with two rows. The first row is labeled 'Activate trigger' and has a dropdown menu set to 'Yes'. The second row is labeled 'Optional time range (in minutes)' and has a dropdown menu set to 'Yes' and a numeric input field containing the value '5'.

4. Zur Auslösung der Lückenfüllung durch ein Alarmszenario oder eine Sequenz legen Sie **Trigger aktivieren** auf **Ja** fest.
5. Aktivieren Sie **Optionaler Zeitbereich (in Minuten)** und geben Sie die zusätzliche Zeit vor und nach der eigentlichen Lückenfüllung in Minuten an. Die Daten von der Kamera liefern dann nicht nur das fehlende Zeitfenster, sondern noch zusätzliche Zeitbereiche, um Lücken zu vermeiden.

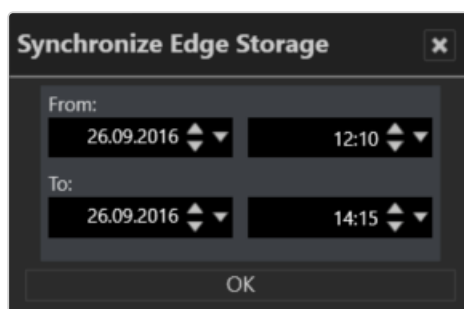
Vollständiger Import

Beim vollständigen Import werden alle Aufzeichnungen für die Zone mit den aus dem Edge-Speicher importierten Aufzeichnungen überschrieben.

Die Dateien können nur manuell im Archivmodus importiert werden (siehe „[Archivmodus](#)“ auf Seite 177).

1. Wählen Sie für den **Edge-Speicher** die Option **Vollständiger Import**.
2. Legen Sie bei **Aufzeichnungstyp** fest, ob die importierten Videosequenzen als **Standardaufzeichnung** oder **Alarmaufzeichnung** behandelt werden sollen.
3. Wechseln Sie in den Archivmodus.

- Drücken Sie die STRG-Taste und klicken Sie im Archiv Player auf **Zeitleiste aktualisieren** (↻) (siehe „Archiv Player“ auf Seite 178).



- Legen Sie im Aufklappmenü den Zeitbereich fest und klicken Sie auf **OK**.

Bewegungsabhängige Aufzeichnung

Die Funktion „Bewegungsabhängige Aufzeichnung“ ermöglicht eine schnelle und einfache Konfiguration einer Alarmaufzeichnung.

Die bewegungsabhängige Aufzeichnung ersetzt kein vollständiges Alarmzenario (siehe „Alarme“ auf Seite 386).

Record On Motion	
Enable record on motion:	Yes
Recording period:	Monday_8-To-13
pre-alarm (s):	7
post-alarm (s):	3
Camera side motion detection:	Disabled <input type="button" value="Configuration"/>
Server side motion detection:	Enabled <input type="button" value="Configuration"/>

Abb. 117: Bewegungsabhängige Aufzeichnung

- Siehe **Bewegungsabhängige Aufzeichnung aktivieren**:
 - Wählen Sie **Ja**, wenn im Fall einer server- oder kamerabasierten Bewegungserkennung eine Alarmaufzeichnung erfolgen soll.
 - Wählen Sie **Nein**. Sie werden gefragt, ob die serverbasierte Bewegungserkennung deaktiviert werden soll.

2. Wählen Sie den **Aufnahmezeitraum** aus, wie in der Zeitverwaltung angegeben (siehe „[Zeitverwaltung](#)“ auf Seite 381). Jeder Trigger außerhalb des ausgewählten Zeitraums wird ignoriert. Trigger, die den Schwellenwert erreichen, werden in der entsprechenden Vor- und Nachalarm-Aufzeichnung eingeschlossen.
3. Geben Sie eine **Voralarmdauer** in Sekunden an.
4. Geben Sie eine **Nachalarmdauer** in Sekunden an.

Edge-Speicher

Das Menüelement „Edge-Speicher“ wird nur angezeigt, wenn die ausgewählte Kamera Edge-Speicherung unterstützt.

Edge Storage

Edge Storage

Recording type

Check during device start

Import Speed

Execution time:

Days	Start	Edit/delete
------	-------	-------------

Activate trigger

Optional time range (in minutes)

Abb. 118: Edge-Speicher

Bei der Edge-Speicherung werden die Bilder auf einem internen Speicher (z. B. SD-Karte) der Kamera gespeichert, um Verbindungsausfälle zwischen Kamera und Daten-

bankserver auszugleichen. Wenn die Verbindung zwischen Kamera und Server unterbrochen wird, kommt es auf dem Device Manager zu Aufzeichnungslücken.

Nach Wiederherstellung der Verbindung können die Aufzeichnungslücken auf dem Server mit den Aufzeichnungen vom internen Speicher der Kamera gefüllt werden. Zeitpläne für die Aufzeichnung und die maximale Aufzeichnungsgröße werden dabei berücksichtigt.

Beide Anwendungsfälle müssen kameraseitig konfiguriert werden (siehe „Technical_Guides_Qognify_Qognify VMS_7.4_DE.pdf“). Für beide Anwendungsfälle ist eine Lizenz erforderlich, die Funktionen zur Edge-Speicherung beinhaltet.

Für die Konfiguration des Edge-Speichers im Konfigurationsmodus steht eine Reihe verschiedener Optionen zur Verfügung.

- Prüfung bei Gerätestart: Wenn ein Gerät nach einem Ausfall des Netzwerks gestartet oder neu verbunden wird, wird der Import ausgelöst.
- Importgeschwindigkeit: Abhängig vom Kamerahersteller und -modell können unterschiedliche Werte ausgewählt werden, zum Beispiel.
 - 1 s: Die Importgeschwindigkeit entspricht der Abspielgeschwindigkeit der Aufzeichnung.
 - 2 s: Die Importgeschwindigkeit entspricht der doppelten Abspielgeschwindigkeit der Aufzeichnung.
 - Max.: Abhängig vom Kamerahersteller ist bei einigen Kameras eine höhere Importgeschwindigkeit möglich. Wird dieser Wert ausgewählt, importiert der Qognify VMS-Client die Aufzeichnungen mit der höchstmöglichen Geschwindigkeit der Kamera (zu den Einstellungen in der Device Manager-Konfiguration siehe unten).
- Auslösung des Imports nach Zeitplan (siehe „[Lückenfüllung](#)“ auf Seite 257)
- Manueller Import eines Zeitbereichs im Archivmodus (siehe „[Vollständiger Import](#)“ auf Seite 258)
 - Optional kann ein Zeitbereich definiert werden. Wird kein Zeitbereich definiert, werden alle Daten seit dem letzten Import importiert.
 - Wird ein Zeitbereich definiert, werden nur die Daten innerhalb dieses Bereichs importiert.
- Auslösung des Imports durch ein Alarmszenario

Anmerkungen

- Um eine Überlastung des Netzwerks zu vermeiden, ruft nur jeweils ein Gerät Videodaten aus dem Edge-Speicher ab. Wenn der Import oder die Lückenfüllung für mehrere Geräte gleichzeitig ausgelöst wird, werden diese in eine Warteschlange eingereiht.
- Ändern Sie die Konfiguration des Geräts nicht, während die Lückenfüllung oder der vollständige Import aktiv ist, da es sonst zu Datenverlust kommen kann.
- Stellen Sie sicher, dass Datum/Uhrzeit der Kamera mit dem Datum, der Tageszeit, der Sommerzeit und der Uhrzeit auf dem Qognify-Server übereinstimmen.
- Der Edge-Speicher funktioniert nicht in einem Failover-Szenario (produktiver DM ist offline und der redundante DM zeichnet zu diesem Zeitpunkt Bilder auf).
- Lückenfüllung: Im Konfigurationsmodus -> Kamera -> Bildspeicherung -> MultimediaDatabase können Sie die Option **Aufzeichnen nur wenn** aktivieren: Diese Option wird bei der Prüfung auf fehlende Aufzeichnungen ignoriert. Wenn aufgrund dieser Funktion eine Aufzeichnungslücke besteht, wird die fehlende Aufzeichnung von der Kamera zur MDB übertragen, obwohl keine Aufzeichnung beabsichtigt ist.
- Es ist möglich, manuell nach fehlenden Aufzeichnungen zu suchen (und diese zu aktualisieren): Öffnen Sie die Kamera im Archivmodus und klicken Sie auf „Zeitstrahl aktualisieren“. Abhängig von den fehlenden Aufzeichnungen kann die Aktualisierung einige Zeit dauern.
- Zeitpläne, Feiertage und maximale Aufnahmezeit werden nicht ignoriert.
- Lückenfüllung: Wenn einmal täglich auf Lücken geprüft wird, stellen Sie sicher, dass sich auf dem Gerät Aufzeichnungen für zwei Tage befinden, damit die Funktion ordnungsgemäß funktioniert. Vergewissern Sie sich außerdem, dass die SD-Karte über ausreichend Speicherplatz für zwei Tage Aufzeichnungen verfügt.
- Aufzeichnungen mit Überschreibschutz werden nicht durch Edge-Speicher-Importe ersetzt.

- Eingefügte Aufzeichnungen im MDS werden in der Ereignisauswertung angezeigt.
- Lücken werden erst nach dem ersten Zugriff auf die Kamera gefüllt.
- Wenn es häufig zu einem Ausfall der Aufzeichnung kommt, kann Qognify nicht sicherstellen, dass die Edge-Speicherung ordnungsgemäß funktioniert. In diesem Fall muss das Kamera- oder Netzwerkproblem zuerst behoben werden.

Videostreams

Im Bereich für Videostreams sollten verschiedene Profile für die Übertragung von Bild-
daten von der Kamera festgelegt und konfiguriert werden. Qognify VMS erstellt bei der
Installation der Kamera einen Basis-Stream. Der Basis-Stream kann nicht gelöscht
werden.

Falls von der Kamera unterstützt, können mehrere Videostreams konfiguriert werden,
z. B. um eine unterschiedliche Videoqualität im Überwachungsmodus, für die Alarm-
aufzeichnung und für Analysezwecke zu verwenden.

Neuen Videostream erstellen

Falls von der Kamera unterstützt, können auf einen Videostream verschiedene Ein-
stellungen angewendet werden, z. B. die Verwendung einer unterschiedlichen
Videoqualität im Überwachungsmodus und für die Alarmaufzeichnung. Die ver-
schiedenen Aufzeichnungen werden aus dem Basis-Stream erfasst. Der Basis-
Stream kann nicht gelöscht werden.

1. Klicken Sie im Konfigurationsbaum auf „Videostreams“. Die konfigurierten
Videostreams werden aufgelistet.

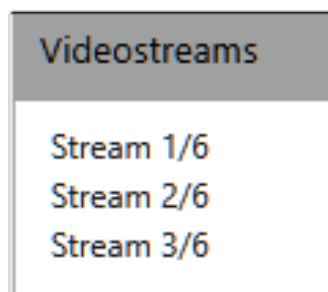


Abb. 119: Neuen Videostream erstellen

2. Klicken Sie auf **Neu**, um einen neuen Videostream anzulegen.

Die maximale Anzahl der Streams ist abhängig vom Kamerateyp.

Videostream bearbeiten

1. Wählen Sie den Videostream und klicken Sie auf **Bearbeiten**, um die erforderlichen Einstellungen vorzunehmen.
2. Wählen Sie den **Capture Mode** aus.

Der Capture Mode kann nur ausgewählt werden, wenn er von der Kamera unterstützt wird. Die verfügbaren Capture Modes hängen vom Kameratyp ab. Bei Mehrkanalgeräten oder virtuellen Kameras betrifft eine Änderung des Capture Modes alle Geräte dieses Video-servers. Daher kann der Capture Mode zwar nur für den Basis-Stream (angezeigt durch ein Home-Symbol) festgelegt werden, er betrifft jedoch alle nachfolgenden Streams der gewählten Kamera. Abhängig von der gewählten Einstellung liefert die Kamera dann unterschiedliche Bildraten und Auflösungen. Gegebenenfalls startet die Kamera neu und ist für mehrere Minuten nicht erreichbar.

3. Wählen Sie die Art des **Videostreams** aus. Folgende Videostreams stehen je nach Hardware zur Verfügung:

Motion JPEG (M-JPEG)

Stream 1/6	
Capture mode:	SMP 2560x1920 (4:3) ▼
Video stream:	Motion JPEG ▼
Video codec:	Motion JPEG
Transmission mode:	HTTP_Serverpush ▼
Activate audio:	No ▼
Standard recording	Alarm recording
Frame rate (fps):	2
Quality (%):	50
Resolution:	2048x1536 ▼
RTSP port:	554
DM/Client Multicast:	No ▼
Address:	<input type="text"/>
Port:	1
TTL:	1

Do you want to configure alarm recording individually?

Abb. 120: Motion JPEG (M-JPEG)

1. Wählen Sie den **Übertragungsmodus** aus: HTTP Server Push (einziger verfügbarer Modus für Motion JPEG) - auch als HTTP-Streaming bezeichnet - ist eine Methode zum Senden unangeforderter (asynchroner) Daten von einem (Kamera-)Webserver an den Device Manager.
2. Legen Sie die **Bildrate** (fps) für Standardaufzeichnungen fest.
3. Legen Sie separat die **Qualität** für Standardaufzeichnungen fest.
4. Wählen Sie eine geeignete **Auflösung** des Kamerabilds für Standardaufzeichnungen.
5. Geben Sie einen **RTSP-Port** an. Der Standard-RTSP-Port ist 544.

6. Optional können Sie die Alarmaufzeichnung separat konfigurieren.

Es wird davon abgeraten, andere Einstellungen für Alarmaufzeichnungen festzulegen. Unterschiedliche Einstellungen für Standard- und Alarmaufzeichnung können dazu führen, dass das Umschalten von der Standard- auf die Alarmaufzeichnung mehrere Sekunden benötigt. Die benötigte Zeit hängt von der Kamera ab. In diesem Zeitraum ist dann unter Umständen keine Aufzeichnung vorhanden.

Wenn für die Alarmaufzeichnung eine andere Videoqualität benötigt wird, wird empfohlen, einen separaten Videostream zu definieren, der in den Einstellungen für die Alarmaufzeichnung zugewiesen werden kann (siehe „[MultimediaDatabase](#)“ auf Seite 252).

H.264/H.265 (MPEG-4)

Stream 1/6	
Capture mode:	SMP 2560x1920 (4:3) ▼
Video stream:	H.264 ▼
Video codec:	H.264
Transmission mode:	RTP_Over_UDP_Unica ▼
Activate audio:	No ▼
Standard recording	Alarm recording
Frame rate (fps):	2
I-Frame distance (s):	1
Quality (%):	50
Resolution:	2048x1536 ▼
Bandwidth control:	Variable ▼
RTSP port:	554
DM/Client Multicast:	No ▼
Address:	<input type="text"/>
Port:	1
TTL:	1

Do you want to configure alarm recording individually?

Abb. 121: H.264/H.265 (MPEG-4)

1. Wählen Sie den **Übertragungsmodus** aus. Folgende Übertragungsmodi stehen je nach Kamera zur Verfügung:
 - **RTP over UDP Unicast** (Standardeinstellung): Die Kommunikation zwischen Qognify-Server und Kamera erfolgt über den TCP-Port 554 (= RTSP-Port). Die Bildübertragung von der Kamera zum Server erfolgt über einen ausgehandelten UDP-Port.
 - **RTP over UDP Multicast**: Die Kommunikation zwischen Qognify-Server und Kamera erfolgt über den TCP-Port 554 (= RTSP-Port). Die Bildübertragung erfolgt über eine Multicast-Adresse, die von der Kamera mitgeteilt wird. RTP over UDP Multicast sollte nur dann verwendet werden, wenn gleichzeitig Fremdsysteme (z. B. Barco oder eyevis) und der Server auf die Kamera zugreifen.
 - **RTP over RTSP over TCP**: Die Kommunikation zwischen Qognify-Server und Kamera und die Bildübertragung erfolgen über den TCP-Port 554 (= RTSP-Port). Diese Einstellung wird bei schlechter Netzwerkverbindung zwischen Server und Kamera empfohlen. Aufgrund der wiederholten Übertragung fehlerhafter Daten können Latenzzeiten auftreten.
 - **RTP over RTSP over HTTP Unicast**: Die Kommunikation und die Bildübertragung erfolgen über einen HTTP-Tunnel (Port 80 TCP). Diese Einstellung wird bei schlechter Netzwerkverbindung zwischen Server und Kamera empfohlen. Aufgrund der wiederholten Übertragung fehlerhafter Daten können Latenzzeiten auftreten.
2. Wählen Sie **Audio aktivieren** für die Übertragung von Audiosignalen. Diese Funktion steht nur zur Verfügung, wenn die Kamera Audiosignale in MPEG-4-basierten Videostreams verarbeiten kann.

Wenn aktiviert, wird der Audiostream ebenfalls aufgezeichnet und ist daher im Archivmodus verfügbar.

3. Legen Sie die **Bildrate** (fps) für Standardaufzeichnungen fest.
4. Definieren Sie den **I-Frame-Abstand** für MPEG-4/H.264./ H.265
5. Legen Sie separat die **Qualität** für Standardaufzeichnungen fest.
6. Wählen Sie eine geeignete **Auflösung** des Kamerabilds für Standardaufzeichnungen.

7. Wählen Sie die Art der **Bandbreitenkontrolle** für MPEG-4/H.264/H.265-Streams aus:
 - **Variable Bitrate:** VBR (variable bit rate) wird verwendet, wenn ausreichend Ressourcen und Bandbreite zur Verfügung stehen. VBR liefert eine gleichbleibende Bildqualität sowohl bei statischen Szenen als auch in Bewegung.
 - **Konstante Bitrate:** CBR (constant bit rate) wird verwendet, wenn nur begrenzte Bandbreite zur Verfügung steht. CBR liefert eine gute Bildqualität bei statischen Szenen und eine verminderte Bildqualität in Bewegung.
8. Geben Sie einen **RTSP-Port** an (Standardport: 554).
9. Optional können Sie die Alarmaufzeichnungen separat konfigurieren.

Es wird davon abgeraten, andere Einstellungen für Alarmaufzeichnungen festzulegen. Unterschiedliche Einstellungen für Standard- und Alarmaufzeichnung können dazu führen, dass das Umschalten von der Standard- auf die Alarmaufzeichnung mehrere Sekunden benötigt. Die benötigte Zeit hängt von der Kamera ab. In diesem Zeitraum ist dann unter Umständen keine Aufzeichnung vorhanden.

Wenn für die Alarmaufzeichnung eine andere Videoqualität benötigt wird, wird empfohlen, einen separaten Videostream zu definieren, der in den Einstellungen für die Alarmaufzeichnung zugewiesen werden kann (siehe „[MultimediaDatabase](#)“ auf Seite 252).

Videoklassifikationen

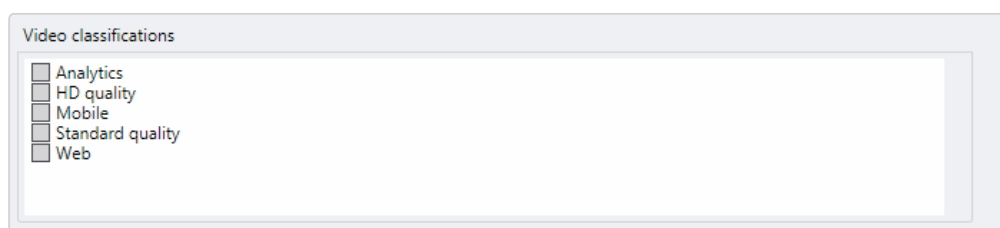
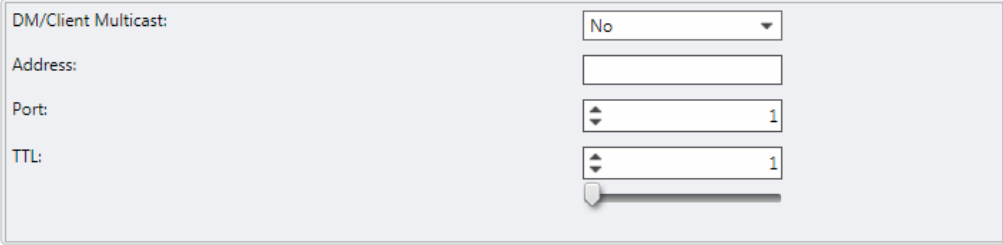


Abb. 122: Videoklassifikationen

Videoklassifikationen sind nur verfügbar, wenn für eine Kamera mehrere Videostreams festgelegt sind. In diesem Fall muss jeder Stream klassifiziert werden. Klassifizierte Streams können für verschiedene Zwecke verwendet werden. Beispielsweise wird die Klassifikation „Standard Qualität“ für Standard- und Alarmaufzeichnungen verwendet, die Klassifikation „HD Qualität“ hingegen für die Anzeige des Kamerabilds auf dem Client in Abhängigkeit vom Benutzerprofil (siehe „[Bildeinstellungen](#)“ auf Seite 377).

1. Wählen Sie die gewünschte Videoklassifikation (siehe „[Videoklassifikation konfigurieren](#)“ auf Seite 463).

DM/Client Multicast



DM/Client Multicast:	No
Address:	
Port:	1
TTL:	1

Abb. 123: DM/Client Multicast

1. Aktivieren Sie **DM/Client Multicast**-Streaming, um einen einzelnen Videostream auf mehreren Clients gleichzeitig anzeigen zu können. Multicast sollte nur verwendet werden bei einer schmalen Bandbreite zwischen Device Manager und Clients.

Für Multicast-Streaming wird eine Multicast-fähige Netzwerkhardware benötigt.

2. Geben Sie die **Netzwerk-Adresse** und die **Portnummer** des Multicast-Servers ein.
3. Geben Sie die **TTL-Dauer** („Time To Live“) an, nach der der Client sich erneut beim Multicast-Server anmelden muss. Eine kurze TTL führt zu höherer Netzwerkauslastung.

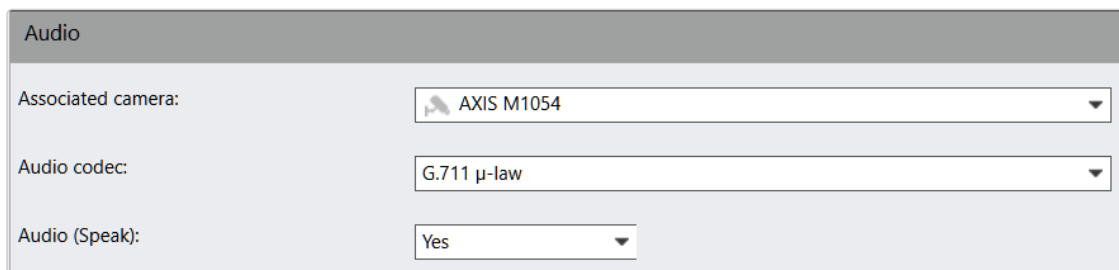
Videostream löschen

1. Klicken Sie im Konfigurationsbaum auf „Videostreams“. Die konfigurierten Videostreams werden aufgelistet.
2. Wählen Sie den Videostream aus und klicken Sie auf **Löschen**.

Audio

Sofern die Kamera eine Übertragung von Audiosignalen unterstützt, kann der Audio-codec eingestellt werden. Die Anpassungen im Steuerelement Kamera im Überwachungsmodus überschreiben jedoch die Kameraeinstellungen (siehe „[Audio](#)“ auf [Seite 166](#)). Um die Übertragung von Audiosignalen von der Kamera zum Client verwenden zu können, muss die Übertragung in den Videostream-Einstellungen aktiviert werden (siehe „[Videostreams](#)“ auf [Seite 263](#)).

Die Auswahl der Kamera ist nur bei Mehrkanalgeräten nötig.



Associated camera:	AXIS M1054
Audio codec:	G.711 μ-law
Audio (Speak):	Yes

Abb. 124: Audio

1. Wählen Sie in den Videostream-Einstellungen den MPEG-4/H.264/H.265-Modus für Videostreams aus (siehe „[Videostreams](#)“ auf [Seite 263](#)).
2. Wählen Sie die **zugehörige Kamera** aus.
3. Wählen Sie den entsprechenden **Audiocodec** aus.
4. Wenn von der Kamera unterstützt, wählen Sie **Audio (Sprechen)** aus. Wenn auf „Ja“ gesetzt, ist im Überwachungsmodus eine Audiokommunikation mit der Kamera möglich (siehe „[Audio](#)“ auf [Seite 166](#)).

Kamerapositionen/Digitale Presets

Wenn die gewählte Kamera PTZ unterstützt, lautet dieses Menüelement „Kamerapositionen“.

Wenn die gewählte Kamera PTZ nicht unterstützt, lautet dieses Menüelement „Digitale Presets“. Alle Kamerapositionen werden mithilfe des Digitalzooms eingestellt. Die Anzahl der Kamerapositionen wird durch die Kamera beschränkt.

Kamerapositionen können als „Presets“ sowohl vom Benutzer im Überwachungsmodus als auch vom Administrator im Konfigurationsmodus angelegt und gelöscht werden.

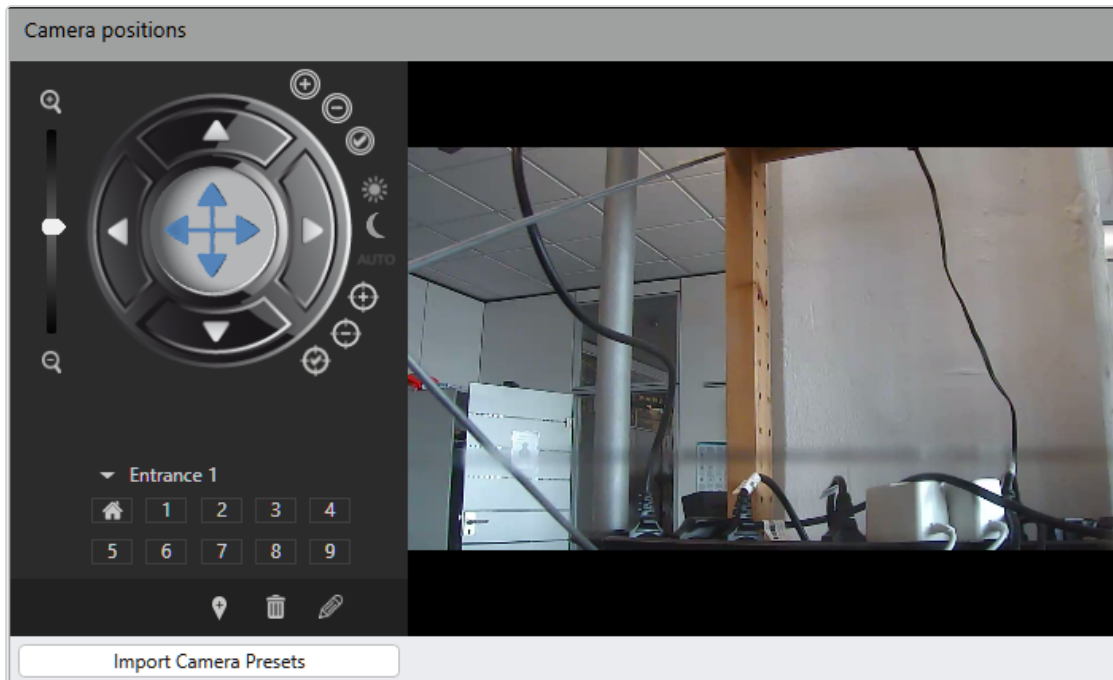


Abb. 125: Kamerapositionen/Digitale Presets

Je nach Kamera stehen folgende Funktionen zur Verfügung:

- Iris +
- Iris -
- Auto-Iris
- Tagmodus
- Nachtmodus
- Auto-Modus
- Fokus nah
- Fokus fern
- Auto-Fokus

Kamerapositionen/Digitale Presets anlegen

Admin-Presets werden vom Administrator angelegt und verwaltet.

1. Bewegen Sie die Kamera mit der PTZ-Steuerung oder einer externen Steuerung in die gewünschte Position.
2. Klicken Sie auf **Neue Kameraposition hinzufügen**.
3. Geben Sie den **Namen** der neuen Presetposition ein und bestätigen Sie mit **OK**. Der Name wird in der Spalte angezeigt und die Preset-Position der nächsten freien Positionsnummer zugewiesen. Stehen nicht genügend Positionsnummern zur Verfügung, werden die weiteren Positionen als Aufklappmenü hinzugefügt.

Preset-Positionen/digitale Presets bearbeiten

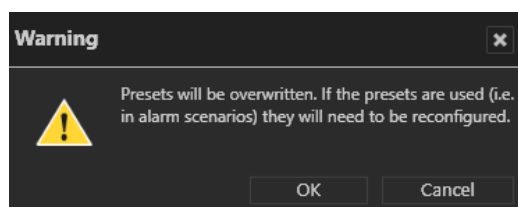
1. Klicken Sie auf die Position, die Sie bearbeiten möchten, oder wählen Sie sie aus der Liste aus.
2. Klicken Sie auf **Aktuelles Preset bearbeiten**.
3. Bewegen Sie die Kamera mit der PTZ-Steuerung oder einer externen Steuerung in die gewünschte Position.
4. Ändern Sie ggf. den Positionsnamen.
5. Klicken Sie auf **Aktuelle Änderungen speichern**.
6. Um eine Preset-Position zu löschen, klicken Sie auf die Auswahl, wählen Sie den Namen in der Liste aus und klicken Sie dann auf **Aktuelle Kameraposition löschen**.

Kamerapositionen/Digitale Presets importieren

Positionen, die in der Kamera bereits konfiguriert sind, können in die Qognify-Konfiguration importiert werden.

Die Option zum Importieren von Presets ist nur verfügbar, wenn der Benutzer über Rechte zum Anlegen von Presets verfügt (siehe „[Benutzerrechte verwalten](#)“ auf Seite 361). Außerdem muss die Kameraposition in der allgemeinen Kamerakonfiguration aktiviert werden (siehe „[Kamera - Allgemein](#)“ auf Seite 246).

1. Klicken Sie auf **Kamera-Presets importieren**.



Beim Importieren von Preset-Positionen aus einer Kamera werden alle Positionen in der Qognify-Konfiguration überschrieben!

2. Klicken Sie auf **OK**. Der Importvorgang wird gestartet.

Video-Backup/-Export

Video Backup/Export	
Automatic backup of image data from multimedia database server:	
Automatically backup standard recording:	<input type="text" value="Yes"/>
Automatically backup alarm recording:	<input type="text" value="Yes"/>
Time period:	<input type="text" value="Always"/>
The settings of the multimedia database server are used for the backup	
AV export	
Show camera name and time:	<input type="text" value="No"/>
Maximum resolution:	<input type="text" value="800x600"/>
Use maximum duration:	<input type="text" value="Yes"/>
Maximum duration (s):	<input type="text" value="2"/>
Video settings:	
Reduce frame rate:	<input type="text" value="No"/>
Single-image sequences:	
Reduce frame rate:	<input type="text" value="Yes"/>
Maximum frame rate (fps):	<input type="text" value="2"/>
Create ZIP file:	<input type="text" value="No"/>

Abb. 126: Video-Backup/-Export

Automatischer Bilddatenexport vom Datenbankserver

Aufzeichnungen können automatisch in einen Pfad auf dem Device Manager exportiert werden, beispielsweise zur Langzeit-Archivierung der Aufzeichnungen oder zu Sicherungszwecken.

Standardmäßig werden Sicherungen täglich als Sicherungsaufträge erstellt. Bevor die Übertragung beginnt, prüft Qognify VMS, ob der Pfad zum Sicherungsordner verfügbar ist. Wenn der Pfad nicht verfügbar ist oder der Backup-Prozess fehlschlägt, versucht Qognify VMS einmal pro Minute, eine Verbindung herzustellen und setzt den Backup-Prozess fort, sobald die Verbindung hergestellt ist. Wenn der Sicherungsinhalt nicht mehr verfügbar ist (z. B. wenn eine Kamera während einer nicht abgeschlossenen Sicherung entfernt wird), wird der Sicherungsauftrag entfernt.

Wenn der Exportvorgang unterbrochen wird, z. B. wegen eines Netzwerkfehlers, wird er automatisch so bald wie möglich fortgesetzt.

1. Legen Sie fest, ob Standardaufzeichnungen und Alarmaufzeichnungen automatisch gesichert werden sollen.

Der Verzeichnispfad für den automatischen Export muss in der Device Manager-Konfiguration festgelegt werden (siehe „[Device Manager \(DM\) konfigurieren](#)“ auf Seite 436). Anderenfalls ist kein automatischer Export möglich

2. Legen Sie den **Zeitraum** fest, der exportiert werden soll. Zeiträume können mithilfe von Zeitschablonen in der Zeitverwaltung definiert werden erstellen (siehe „[Zeitverwaltung](#)“ auf Seite 381).

AV-Export

Der AV-Export kann durch einen Alarm ausgelöst werden. Bei dem Vorgang werden Alarmaufzeichnungen in unverschlüsselte H.264 (MPG)- oder M-JPEG-Sequenzen konvertiert, die an eine E-Mail angehängt oder auf einem FTP-Server gespeichert werden können (siehe „[E-Mail und FTP](#)“ auf Seite 402).

Die Einstellungen für den FTP-Server müssen im VA Administrationstool festgelegt werden (siehe „[Qognify VMS VA Administrationstool](#)“ auf Seite 513).

1. Legen Sie fest, ob beim AV-Export auch der **Kameraname und Zeitpunkt** der Aufzeichnungen exportiert und angezeigt werden sollen. Kameraname und Zeitpunkt werden in der exportierten Sequenz am unteren Bildrand angezeigt.
2. Wählen Sie die **Maximale Auflösung** für den Export.
3. Legen Sie fest, ob die **Länge** der Aufzeichnung begrenzt werden soll.
4. Geben Sie die **Maximale Dauer (s)** des Exports an (in Sekunden).

Es wird empfohlen, die Größe der Exportdateien so stark wie möglich zu reduzieren, indem Auflösung und Dauer der Videosequenz verringert werden.

5. In den Videoeinstellungen (für MPG-basierte Streams, z. B. H.264) können Sie optional **Bildrate reduzieren** aktivieren, sodass nur I-Frames exportiert werden.
6. Bei Einzelbildsequenzen (MJPEG) können Sie optional **Bildrate reduzieren** aktivieren, damit die angegebene maximale Bildrate (fps) exportiert wird.

7. Aktivieren Sie **ZIP-komprimierten Ordner erstellen**, um die exportierten Daten nach dem Export zu komprimieren.

Serverseitige Funktionen

Zu den konfigurierbaren serverseitigen Funktionen zählen:

- Bewegungserkennung (siehe [„Bewegungserkennung“ auf der gegenüberliegenden Seite](#))
- Referenzbildvergleich (siehe [„Referenzbildvergleich“ auf Seite 279](#))
- Manipulationserkennung (siehe [„Manipulationserkennung“ auf Seite 280](#))

Die serverseitigen Funktionen erkennen Bewegungen innerhalb des Bilds, Manipulationsversuche an der Kamera sowie Unterschiede zu einem Referenzbild. Bei den serverseitigen Funktionen werden die Bilder durch Bewegungserkennungsmodule auf dem Server ausgewertet (siehe [„Modul zur serverbasierten Bewegungserkennung hinzufügen“ auf Seite 522](#)). Ein Ereignis der serverseitigen Bewegungserkennung kann beispielsweise als Auslöser für einen Alarm verwendet werden.

Die serverseitige Bildauswertung durch das Bewegungserkennungsmodul führt zu einer hohen Ressourcenauslastung. Daher wird empfohlen, die kameraseitige Bewegungserkennung zu verwenden (siehe [„Kameraseitige Funktionen“ auf Seite 281](#)).

1. Öffnen Sie das Menü „Serverseitiger Betrieb“.
2. Wählen Sie eine Videoklassifikation aus (siehe [„Videostreams“ auf Seite 263](#)).
 - Die Videoklassifikation bestimmt, welcher Videostream für die Bewegungserkennung verwendet wird.
 - Die Videostreams sind nach ihrer Nutzung der Netzwerkbandbreite angeordnet („HD Qualität“ erfordert eine Breitbandverbindung, während „Mobile“ die Bildqualität für langsame Netzwerke verringert).
3. Wählen Sie für Bildvergleiche einen Videostream für geringe Bandbreiten aus.

Für die Bewegungserkennung, den Referenzbildvergleich und die Manipulationserkennung werden größere Bilder intern auf 320 x 240 Pixel verkleinert.

Bewegungserkennung

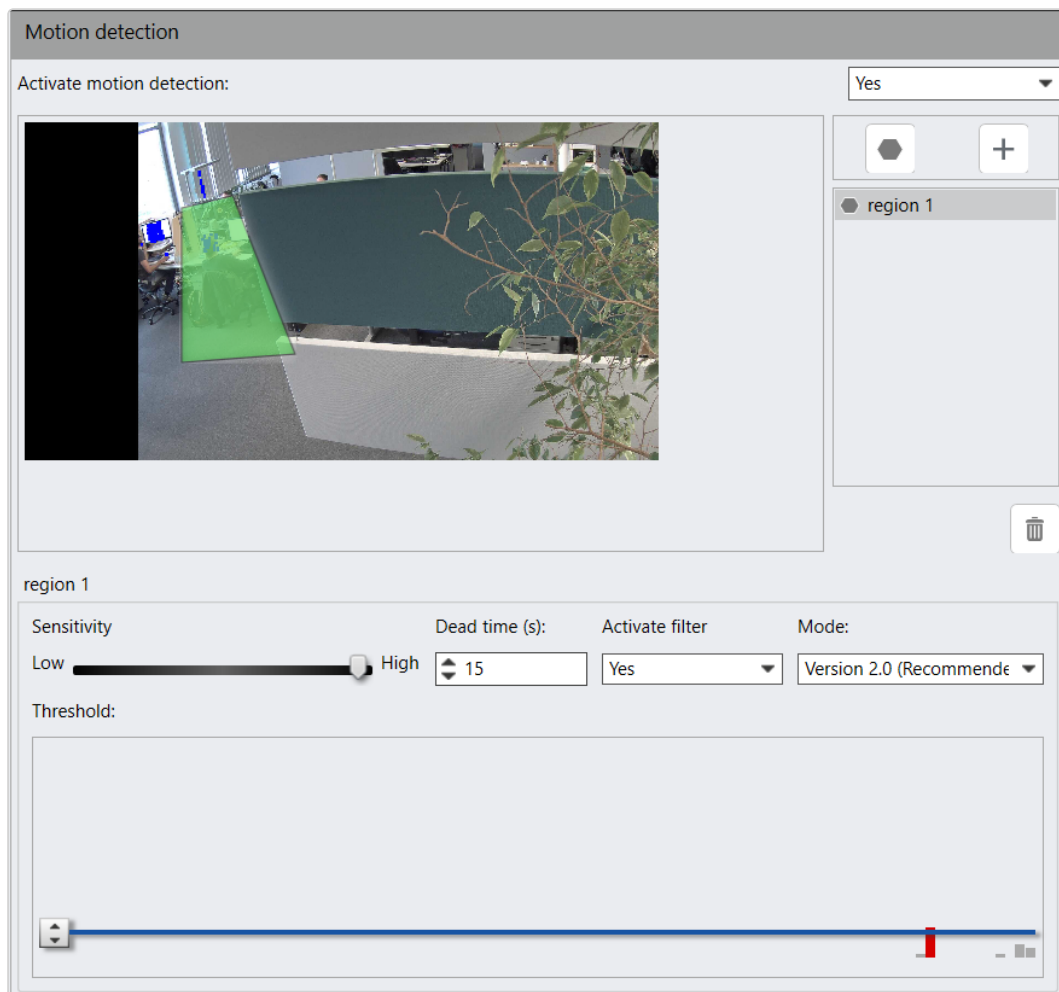


Abb. 127: Bewegungserkennung

Die serverseitige Bewegungserkennung wertet einen Graubildstrom aus einem einzelnen Kanal aus und ist somit äußerst effizient. Dennoch wird empfohlen, bevorzugt die kameraseitige Bewegungserkennung zu verwenden, um die Hardware-Anforderungen an den Server zu reduzieren (siehe „Systemvoraussetzungen“ auf Seite 31).

Die Bewegungserkennung liefert die besten Ergebnisse in Innenräumen. Sie können für jede Kamera bis zu zehn Regionen mit individuell konfigurierten Empfindlichkeits-, Totzeit- und Schwellenwerten anlegen

1. Wählen Sie **Bewegungserkennung** im Menü „Serverseitiger Betrieb“ (Sie müssen möglicherweise auf das Dreieck vor dem Menü klicken).
2. Um die Bewegungserkennung zu aktivieren, wählen Sie im Aufklappmenü **Ja**.
3. Klicken Sie auf das Plus-Zeichen rechts neben dem Kamerabild.

4. Zeichnen Sie mit Hilfe des Polygon-Werkzeugs die Region in das Kamerabild. Unterschiedliche Bereiche werden nur benötigt, wenn pro Bereich unterschiedliche Alarmszenarien ausgelöst werden sollen.
5. Geben Sie einen Namen für den/die Bereich(e) an.
6. Passen Sie die **Bewegungsempfindlichkeit** durch Verschieben des Schiebereglers an. Der Empfindlichkeitswert legt fest, wie klein oder groß ein Unterschied im Bild sein muss, damit dies als Bewegung gilt. Erhöhen Sie den Wert, wenn zu viele falsch-negative Ergebnisse ausgegeben werden, oder verringern Sie den Wert, wenn zu viele falsch-positive Ergebnisse ausgegeben werden.
 - Bei einem hohen Wert werden selbst kleine Veränderungen im Bild als Bewegung behandelt.
 - Bei einem niedrigen Wert werden nur große Veränderungen im Bild als Bewegung behandelt.
7. Geben Sie das Intervall für die **Totzeit** (in Sekunden) an, nach dem wieder ein Signal ausgewertet wird.
8. Wählen Sie die Option **Filter aktivieren**, um das Bild mit Hilfe eines Weichzeichners zu optimieren und so eventuelles Bildrauschen (z. B. aufgrund schlechter Lichtverhältnisse) zu reduzieren.
9. Wählen Sie im Aufklappmenü in der Mitte zwischen **Version 1.0** und **Version 2.0**.


Es wird dringend empfohlen, Version 2.0 zu verwenden, da sie eine wesentlich bessere Leistung bei nur geringfügig verringerter Qualität bietet. Für alle Regionen einer Kamera muss derselbe Modustyp verwendet werden.

10. Passen Sie den **Schwellenwert** durch Verschieben der blauen Linie an. Der Schwellenwert legt fest, wie groß die Bewegung im Bild sein muss, damit ein Alarm ausgelöst wird.
 - Legen Sie einen hohen Schwellenwert fest, wenn nur große Bewegungen einen Alarm auslösen sollen.
 - Legen Sie einen niedrigen Schwellenwert fest, wenn bereits kleine Bewegungen einen Alarm auslösen sollen. Die Rechtecke im Fenster mit dem Schwellenwert-Schieberegler dienen als visuelle Hilfe bei der Einstellung des Schwellenwerts. Sie zeigen die Bewegungsamplitude der letzten Sekunden und stellen diese rot dar, wenn beim aktuellen Schwellenwert ein Alarm ausgelöst worden wäre.
 - Die farbigen Pixel im Bild zeigen an, wo eine Bewegung erkannt wurde.
 - Ein blaues Pixel gibt an, dass eine Bewegung erkannt wurde.
 - Ein rotes Pixel gibt an, dass ein Alarm ausgelöst wurde.
11. Speichern Sie die Einstellungen.

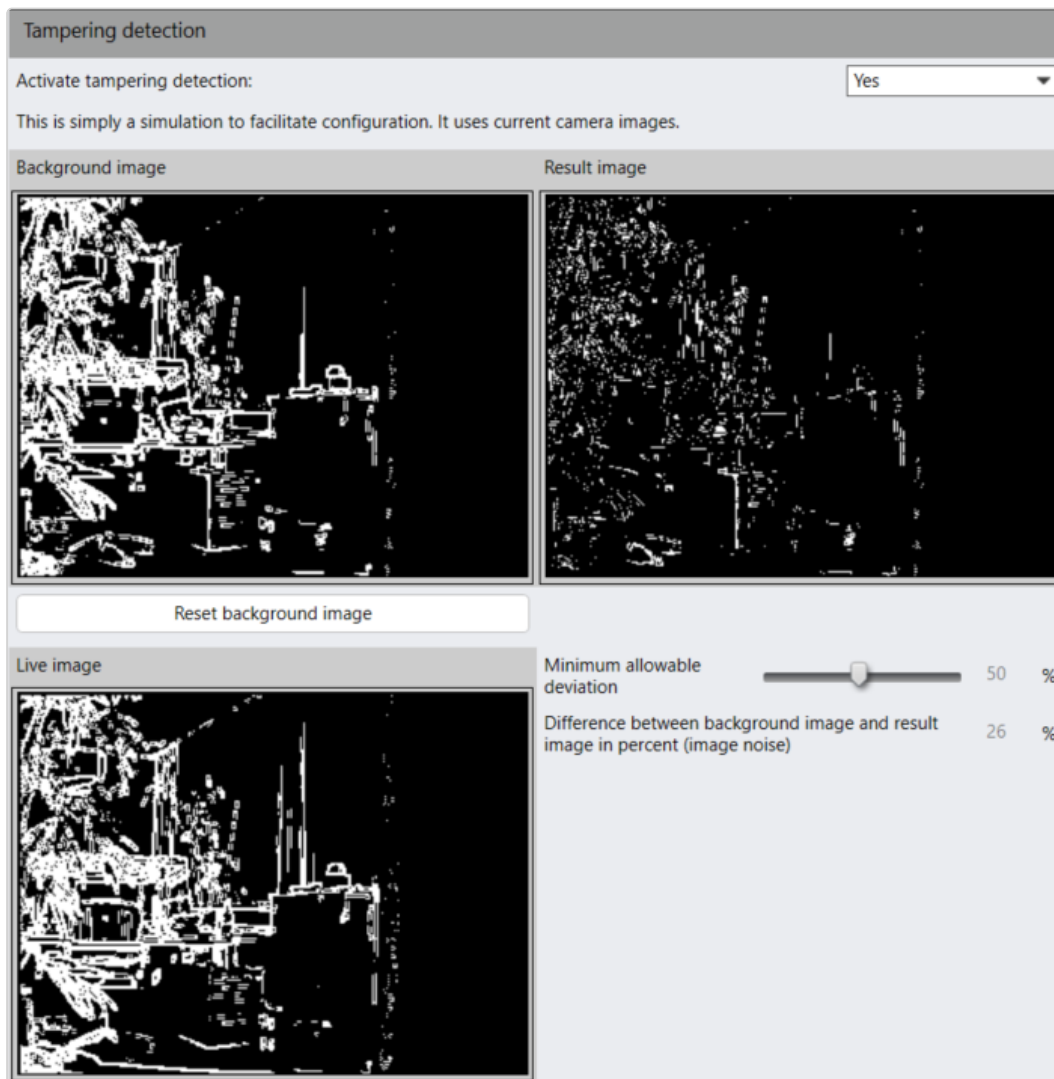
Referenzbildvergleich

Das Live-Kamerabild wird mit einem festgelegten Referenzbild der gleichen Kameraansicht verglichen (siehe [„Manueller Referenzbildvergleich“ auf Seite 124](#)). Wenn die Bilder nicht übereinstimmen, wird ein Alarm ausgelöst. Ein zweiter Alarm wird ausgelöst, wenn die ursprüngliche Kameraansicht wiederhergestellt wird.

1. Wählen Sie **Referenzbildvergleich** im Menü „Serverseitiger Betrieb“.
2. Um den automatische Referenzbildvergleich zu aktivieren, wählen Sie im Aufklappmenü **Ja**.
3. Wählen Sie **Referenzbild erstellen**, um ein Bild von der Kamera als Hintergrund für die Bewegungserkennung auszuwählen.
4. Wählen Sie **Nur Unterschiede anzeigen**, um nur die Unterschiede zwischen dem Live-Bild und dem Referenzbild anzeigen zu lassen.
5. Legen Sie die **Alarmschwelle in Prozent (Toleranz)** fest. Ein Alarm wird nur dann ausgelöst, wenn die Unterschiede zwischen dem Live-Bild und dem Referenzbild über dem Schwellenwert liegen.

- Legen Sie fest, ob für das zu vergleichende Bild ein Live-Bild im Überwachungsmodus oder ein aufgezeichnetes Bild aus dem Archivmodus verwendet werden soll. Das aufgezeichnete Bild muss durch Auswahl des Zeitpunkts und **Kalender-Direkteingabe**  festgelegt werden.
- Legen Sie die Werte für den **Ausführungszeitpunkt** fest, indem Sie das Zeitintervall (in Minuten, zu einer bestimmten Tageszeit oder an bestimmten Wochentagen zu einer bestimmten Uhrzeit) für den Abgleich von Referenzbild und Live-Bild angeben.

Manipulationserkennung



Tampering detection

Activate tampering detection: Yes

This is simply a simulation to facilitate configuration. It uses current camera images.

Background image

Result image

Reset background image

Live image

Minimum allowable deviation 50 %

Difference between background image and result image in percent (image noise) 26 %

Abb. 128: Manipulationserkennung

Die Manipulationserkennung erkennt eine Manipulation der Kameraausrichtung, verwendet jedoch Kantenerkennung für den Abgleich. Aus jedem Bild wird automatisch ein Referenzbild erstellt und mit dem folgenden verglichen. Bestimmte Manipulationsereignisse können als Auslöser für ein Alarmszenario verwendet werden. Nach einem Alarm wird das Referenzbild neu erstellt.

1. Um die Manipulationserkennung zu aktivieren, wählen Sie im Aufklappenmenü **Ja**.
2. Wählen Sie **Hintergrundbild zurücksetzen**, um ein neues Referenzbild festzulegen.
3. Legen Sie die **Minimal zulässige Abweichung** für das Live-Bild (in Prozent) fest, um den Schwellenwert für die Auslösung der Bewegungserkennung anzugeben. Je höher der Wert, desto weniger empfindlich ist die Bilderkennung.

Um einen Alarm auszulösen, muss für die Kamera ein Alarmszenario eingerichtet werden (siehe „Alarmszenario anlegen“ auf Seite 387).

4. Übernehmen Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
5. Speichern Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Kameraseitige Funktionen

Falls von der Kamera unterstützt, erkennen die kameraseitigen Funktionen Bewegungen innerhalb des Bilds sowie Manipulationsversuche an der Kamera.

Die kameraseitigen Funktionen müssen auf der Kamera selbst aktiviert und konfiguriert werden.

Ein Ereignis der Bewegungserkennung kann beispielsweise als Auslöser für einen Alarm verwendet werden.

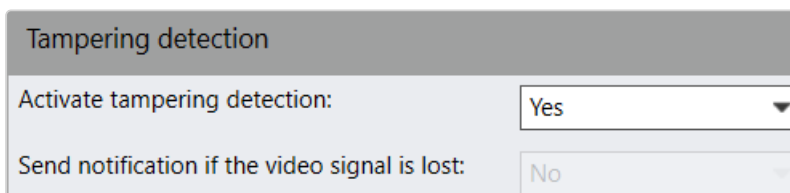
Bewegungserkennung

Camera motion detection			
Window	Activated	Name	Dead time
1	<input checked="" type="checkbox"/>	Window 1	15
2	<input checked="" type="checkbox"/>	Window 2	15
3	<input type="checkbox"/>	Window 3	15

Abb. 129: Bewegungserkennung

1. Wählen Sie **Bewegungserkennung** im Menü „Kameraseitiger Betrieb“.
2. Aktivieren Sie die entsprechende Anzahl der Fenster und geben Sie einen Namen sowie das Intervall für die **Totzeit** (in Sekunden) an, nach dem wieder ein Signal ausgewertet wird. Diese Einstellung kann auch zum Auslösen eines Alarms verwendet werden (siehe „[Alarme](#)“ auf Seite 386).

Manipulationserkennung



Tampering detection	
Activate tampering detection:	Yes
Send notification if the video signal is lost:	No

Abb. 130: Manipulationserkennung

Abhängig vom verwendeten Kameramodell können bestimmte Ereignisse als Auslöser für ein Alarmszenario verwendet werden (nähere Informationen über die kameraspezifischen Manipulationsfunktionen entnehmen Sie bitte dem Handbuch der jeweiligen Kamera).

Nach Erhalt einer Benachrichtigung kann dann eine Aktion gestartet werden. Diese Einstellung kann auch zum Auslösen eines Alarms verwendet werden (siehe „[Alarme](#)“ auf Seite 386).

1. Wählen Sie **Manipulationserkennung** im Menü „Kameraseitiger Betrieb“.
2. Wählen Sie **Ja**, um die kameraseitige Manipulationserkennung zu aktivieren.
3. Falls von der Kamera unterstützt, legen Sie **Bei Verlust des Videosignals Benachrichtigung senden** auf **Ja** fest. Dadurch wird in der Alarmliste eine Benachrichtigung ausgegeben, wenn das Videosignal ausfällt. Diese Einstellung kann auch zum Auslösen eines Alarms verwendet werden (siehe „[Alarme](#)“ auf Seite 386).

Ereignistrigger

Wenn die Kamera über einen intelligenten (generischen) Treiber integriert ist, können Trigger wie Bewegungserkennungs-, Manipulations- oder andere kameraseitige Ereignisse als Ereignistrigger konfiguriert werden.

Event trigger

Update generic event trigger

Activated	Name	Event trigger type	Dead time	Record On Motion
<input type="checkbox"/>	M0	M0	15	<input type="checkbox"/>
<input checked="" type="checkbox"/>	M1	M1	15	<input type="checkbox"/>
<input type="checkbox"/>	M2	M2	15	<input type="checkbox"/>
<input type="checkbox"/>	M3	M3	15	<input type="checkbox"/>
<input type="checkbox"/>	M4	M4	15	<input type="checkbox"/>
<input type="checkbox"/>	M5	M5	15	<input type="checkbox"/>
<input type="checkbox"/>	M6	M6	15	<input type="checkbox"/>
<input type="checkbox"/>	M7	M7	15	<input type="checkbox"/>
<input type="checkbox"/>	M8	M8	15	<input type="checkbox"/>
<input type="checkbox"/>	M9	M9	15	<input type="checkbox"/>
<input type="checkbox"/>	A0	A0	15	<input type="checkbox"/>
<input type="checkbox"/>	T0	T0	15	<input type="checkbox"/>

Show extended camera options

Activated	Name	Event trigger type	Dead time	Record On Motion
<input checked="" type="checkbox"/>	Device/Tampering/ShockDetec	Device/Tampering/ShockDetec	15	<input type="checkbox"/>
<input type="checkbox"/>	CameraApplicationPlatform/Ba	CameraApplicationPlatform/Ba	15	<input type="checkbox"/>
<input checked="" type="checkbox"/>	VideoSource/TamperingIchann	VideoSource/TamperingIchann	15	<input type="checkbox"/>

Abb. 131: Ereignistrigger

1. Wählen Sie **Ereignistrigger** im Menü „Kameraseitiger Betrieb“.
2. Wenn an der Kamera selbst Änderungen vorgenommen wurden oder wenn nicht alle erwarteten Ereignisse angezeigt werden, klicken Sie auf **Generischen Ereignistrigger aktualisieren**.

3. Aktivieren Sie die entsprechende Anzahl der Ereignisse und geben Sie einen **Namen** sowie das Intervall für die **Totzeit** (in Sekunden) an, nach dem wieder ein Signal ausgewertet wird. Diese Einstellung kann auch zum Auslösen eines Alarms verwendet werden (siehe „[Alarme](#)“ auf Seite 386).

Die Totzeit wird nur verwendet, wenn der Ereignistrigger beispielsweise für ein Alarmszenario verwendet wird. Wenn das Kontrollkästchen "Bewegungsabhängige Aufzeichnung" ebenfalls aktiviert ist, wird die Totzeit nicht auf die Funktion "Bewegungsabhängige Aufzeichnung" angewendet.

Abhängig vom Kameratyp und Treiber sind möglicherweise erweiterte Optionen verfügbar.

Privacy-Masking

Sensible Bereiche oder Bewegungen im Bild können durch eine Maske ausgeblendet werden. Damit wird verhindert, dass diese Bereiche für den Benutzer sichtbar sind. Die Maske wird, abhängig von den Benutzerberechtigungen, im Überwachungsmodus und im Archivmodus angezeigt.

Diese Funktion kann im Überwachungsmodus und im Archivmodus von Administratoren und Benutzern mit entsprechenden Rechten aktiviert und deaktiviert werden.

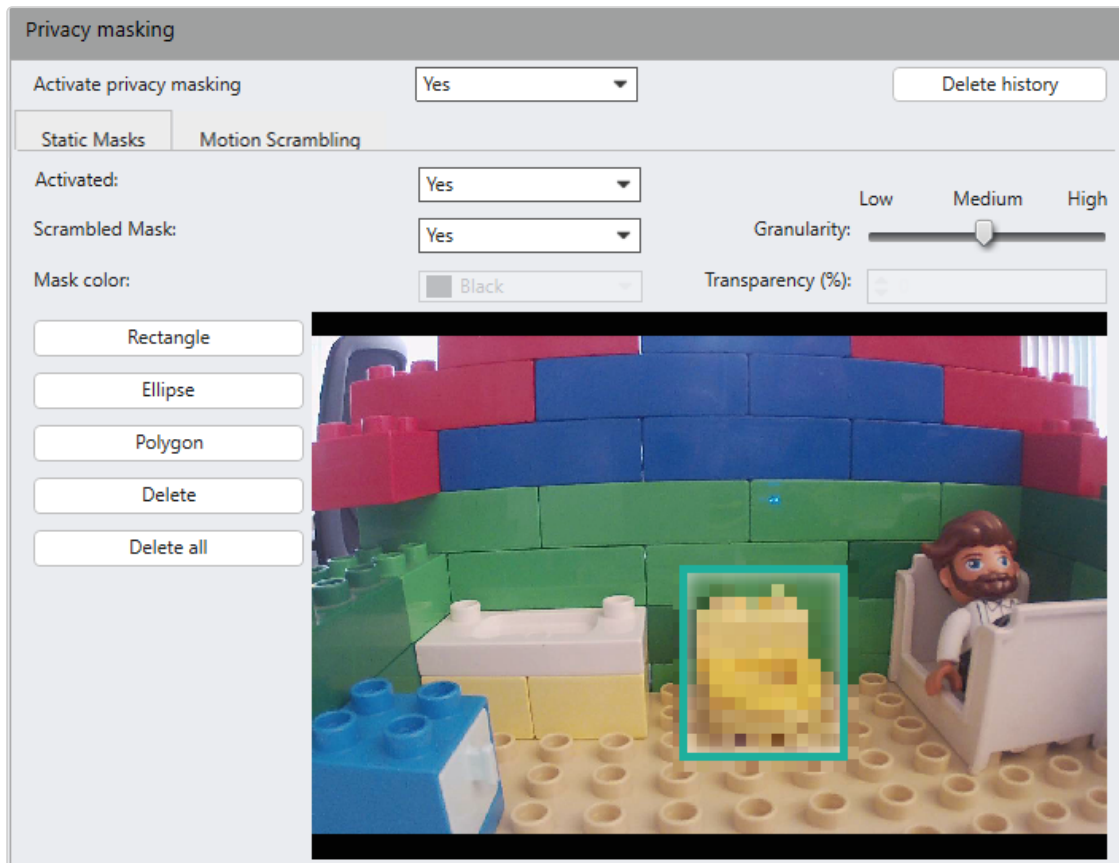


Abb. 132: Statische Objekte

1. Aktivieren Sie **Privacy-Masking**.
2. Wählen Sie **Static Masks** oder **Motion Scrambling**.
 - Sie können die Methode **Static Masks** verwenden, um einzelne Bereiche des Kamerabildes zu verbergen. Die Maskierung folgt der Kamera, sodass immer der gleiche Bildausschnitt maskiert wird.
 - Sie können das **Motion Scrambling** dazu verwenden, um die Änderung oder statische Informationen zu verbergen. Mit der Methode **Bewegte Objekte** der Funktion „Scrambling“ maskieren Sie alle Objekte, die sich bewegen, wie Personen oder Fahrzeuge (siehe „[Motion Scrambling](#)“ auf [Seite 287](#)). **Der Büromodus** der Scrambling-Funktion basiert auf dem Referenzbildvergleich und verbirgt alle Unterschiede von einem Referenzbild (siehe „[Büromodus](#)“ auf [Seite 288](#)).

Statische Masken

Scrambled Mask

1. Wählen Sie **Static Masks** und aktivieren Sie.
2. Wählen Sie die Form des zu verschlüsselnden Bereichs, z. B. ein Rechteck oder eine Ellipse.
3. Wählen Sie **Scrambled Mask** und legen Sie die Granularität der Details fest. Je niedriger die Granularität, desto weniger grob wird der ausgewählte Bereich dargestellt.
4. Ziehen Sie die Form über das Kamerabild.

Maskenfarbe

1. Wählen Sie **Statische Objekte** und aktivieren Sie diese.
2. Wählen Sie die Form des zu verschlüsselnden Bereichs, z. B. ein Rechteck oder eine Ellipse.
3. Wählen Sie **Maskenfarbe** und legen Sie die Farbe und die Transparenz der Maske fest.
4. Ziehen Sie die Form über das Kamerabild.

Löschen einer Maske

1. Wählen Sie entweder **Löschen**, um eine einzelne Maske zu löschen, oder **Alle löschen**, um alle zu entfernen.

Motion Scrambling

Bewegte Objekte

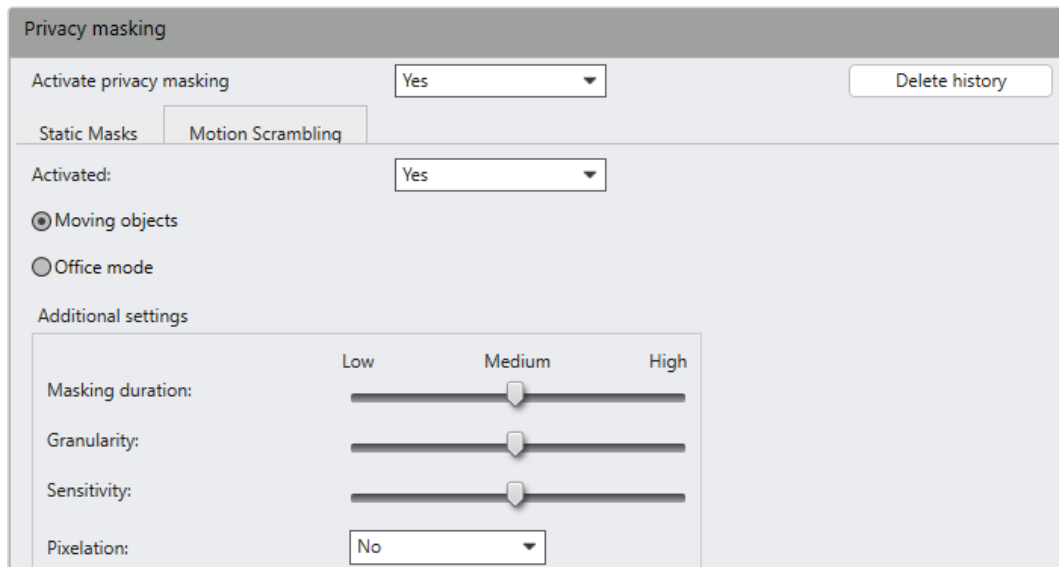


Abb. 133: Scrambling/Bewegte Objekte

1. Wählen Sie **Scrambling** und aktivieren Sie es.
2. Legen Sie fest, wie lange das Objekt nach seinem Stillstand maskiert werden soll (= **Maskierungsdauer**), welche Pixelgröße bei der Maskierung verwendet werden soll (**Granularität**) und wie empfindlich auf ein sich bewegendes Objekt reagiert wird (**Empfindlichkeit**).
3. Aktivieren Sie **Pixelung**, um die Maske in schwarz-weiß anzuzeigen. Andernfalls wird die Maske grobpixelig in den Originalfarben dargestellt.

Büromodus

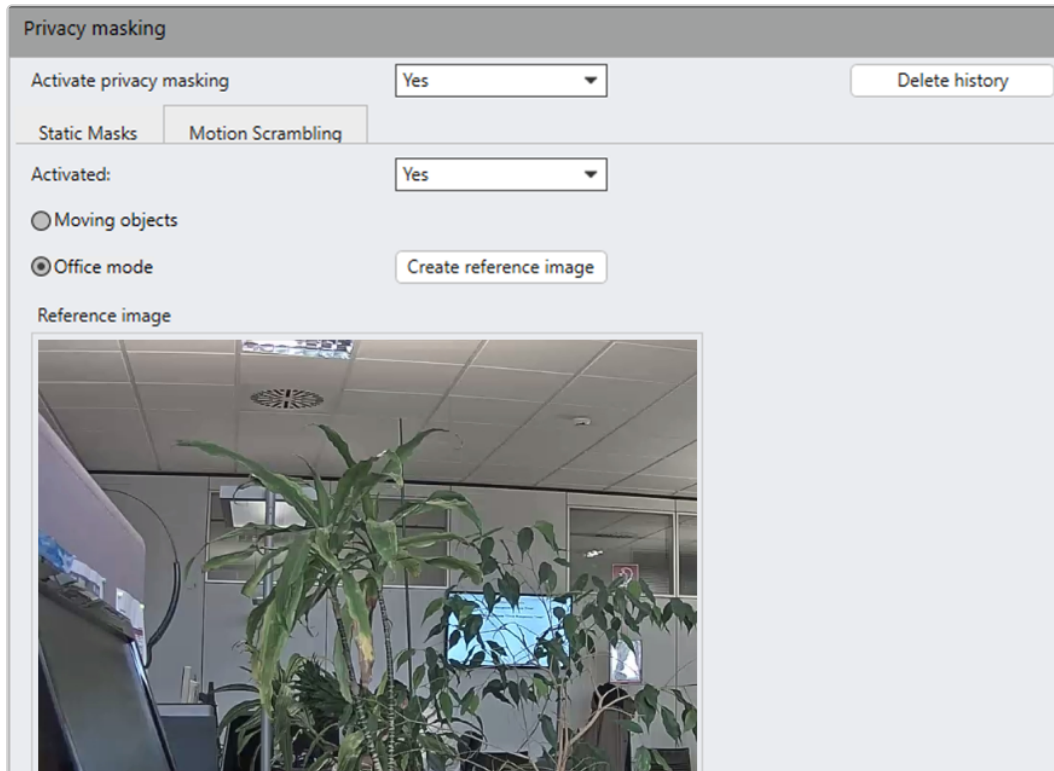


Abb. 134: Scrambling/Büromodus

1. Aktivieren Sie **Büromodus**.
2. Laden Sie ein Referenzbild. Alle Unterschiede zum hinterlegten Referenzbild werden dann maskiert dargestellt.
3. Um alle Masken im Archiv zu löschen, klicken Sie auf **Verlauf löschen**.
4. Bestätigen Sie mit **Ja**.

Wenn die Historie der Privacy-Masks nicht gelöscht wird, verbleiben die Privacy-Masks in den Aufzeichnungen, selbst wenn die Maskierungsfunktion deaktiviert wird. Daher können nur Benutzer mit den entsprechenden Berechtigungen die Aufzeichnungen ansehen.

Click-2-Track

Eine Person oder ein Objekt, das sich über verschiedene Kameraansichten hinweg bewegt, kann auch ohne Angabe des Kameranamens der folgenden Ansicht verfolgt werden. Stattdessen wird der Weg der Person oder des Objekts im Überwachungsmodus definiert, indem der Bereich aktiviert wird, der von der benachbarten Kamera abgedeckt wird (siehe „Click-2-Track“ auf Seite 145).

Diese Funktion erfordert eine entsprechende Lizenz und ist nicht im Standardpaket enthalten.

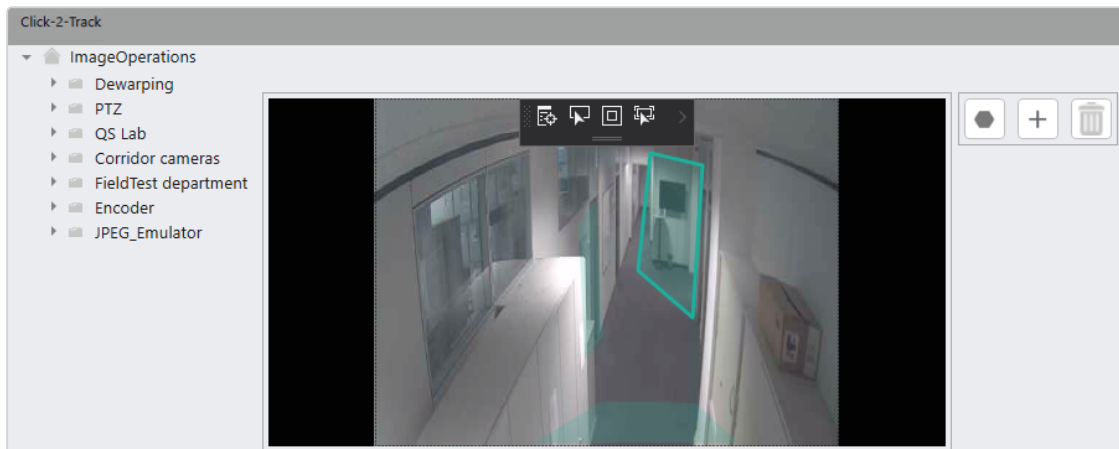




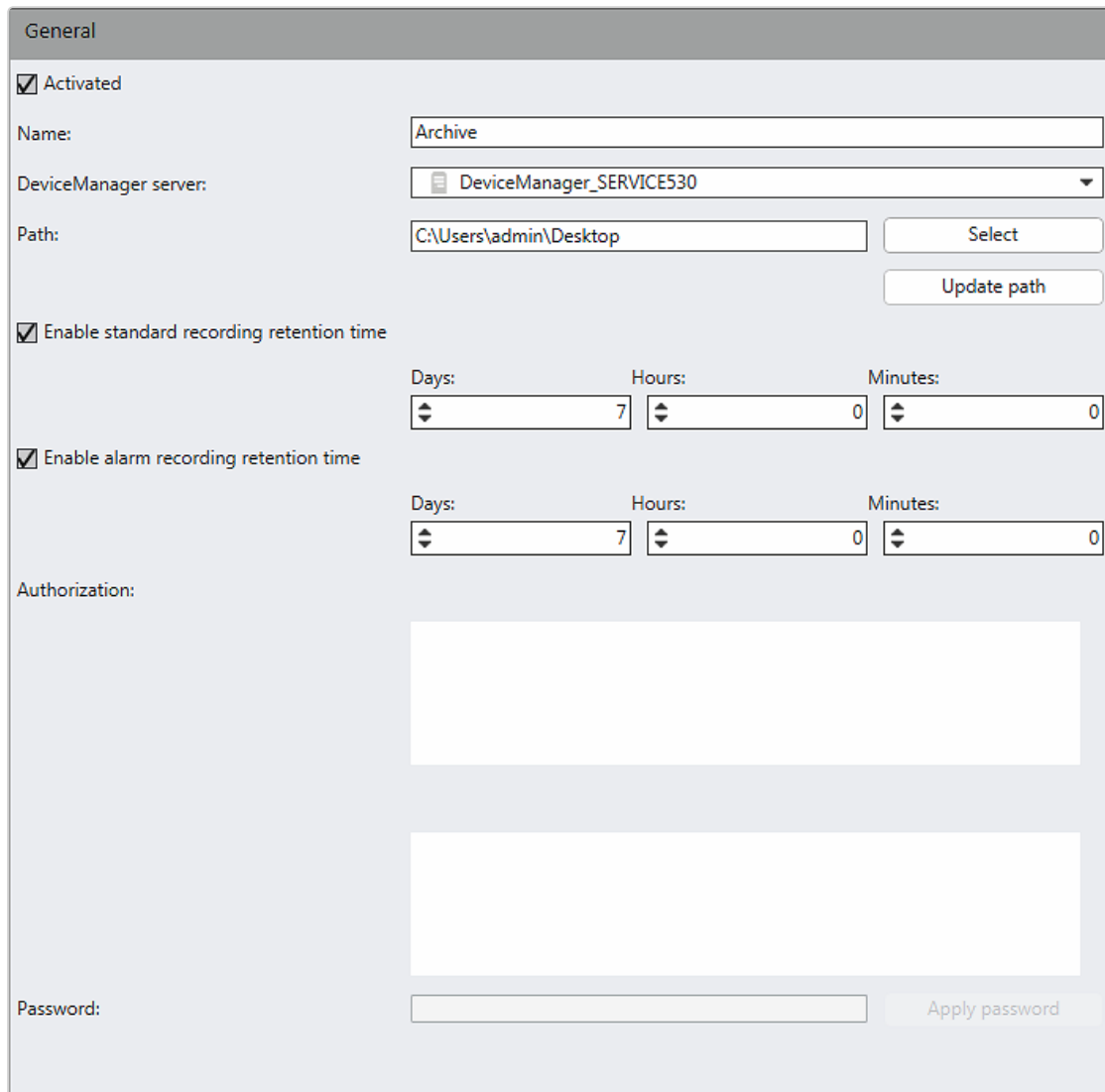


Abb. 135: Verfolgungsmodus

1. Klicken Sie auf **Hinzufügen**  und anschließend auf **Polygon** .
2. Zeichnen Sie ein Polygon in das Bild, indem Sie auf die Ecken klicken, um ihn zu definieren. Das Polygon definiert die Regionen für die Überwachung.
3. Schließen Sie das Polygon, indem Sie darauf doppelklicken.
4. Öffnen Sie den Kamerabaum links neben dem Bild und ziehen Sie eine Kamera in die Region.
5. Um eine Region zu ändern, klicken Sie auf **Polygon**  und definieren eine neue Region.
6. Um die Einstellungen zu überprüfen, fahren Sie mit der Maus über den Bereich, um eine Vorschau des verknüpften Kamerabildes zu erhalten.
7. Um einen Polygon zu löschen, wählen Sie den Polygon aus und klicken Sie auf **Löschen** . Das Polygon und die Verknüpfung mit der zugehörigen Kamera werden gelöscht.

Archivkamera konfigurieren



General

Activated

Name:

DeviceManager server:

Path:

Enable standard recording retention time

Days: Hours: Minutes:

Enable alarm recording retention time

Days: Hours: Minutes:

Authorization:

Password:

Abb. 136: Archivkamera - Allgemeine Einstellungen

1. Aktivieren oder deaktivieren Sie die Kamera.
2. Passen Sie gegebenenfalls den **Namen** der Kamera an.
3. Ändern Sie gegebenenfalls den **Device Manager-Server**.

Durch Ändern des Device Managers werden alle vorhandenen Aufzeichnungen gelöscht.

4. Definieren Sie die Eingabe **Pfad**, wo die Aufzeichnungen gespeichert werden. Mit **Auswählen** können Sie nach dem Verzeichnis suchen.
5. Wenn Sie den Dateipfad ändern möchten, klicken Sie auf **Pfad neu einlesen**.
6. Wenn Sie den Zeitraum für die Speicherung der Standardaufzeichnungen angeben möchten, wählen Sie die Option **Speicherzeit für Standardaufzeichnungen aktivieren**.

7. Legen Sie den Zeitraum in Tagen, Stunden und Minuten fest.
8. Wenn Sie den Zeitraum für die Speicherung der Alarmaufzeichnungen angeben möchten, wählen Sie die Option **Speicherzeit für Alarmaufzeichnungen aktivieren**.

In der Spalte **Autorisierung** werden die verifizierten und nicht verifizierten Kameras angezeigt, die am angegebenen Speicherort gefunden wurden.

9. Wählen Sie eine nicht verifizierte Kamera aus und legen Sie das entsprechende **Passwort** zur Validierung der Kamera fest. Dadurch werden Archivkameras vor unbefugtem Zugriff geschützt.

Die Verschlüsselung verwendet den GCM AES-256 mit PBKDF2Sha256 als Passwort-Hash-Algorithmus.

Mehrere Kameras konfigurieren

Zur Erleichterung der Kamerakonfiguration können mehrere Kameras gleichzeitig konfiguriert werden, selbst in verschiedenen Filialen. Es sind jedoch nicht alle Einstellungen verfügbar. Informationen zur Konfiguration bestimmter Kameras finden Sie im Abschnitt „[Kamera konfigurieren](#)“ auf Seite 242.

1. Schließen Sie alle Tabs für die Kamerakonfiguration.
2. Klicken Sie im Steuerelement Unternehmen auf **Kameras**.
3. Wählen Sie die Kameras aus, die Sie konfigurieren möchten.
4. Um mehrere Kameras gleichzeitig zu konfigurieren, schließen Sie alle Kamera-Tabs in der Arbeitsfläche.
5. Klicken Sie auf **Bearbeiten**. Die Ansicht für die Kamerakonfiguration wird angezeigt. Optionen, die nicht für alle gewählten Kameras verfügbar sind, sind ausgegraut. Bei der gleichzeitigen Konfiguration mehrerer Kameras können nur die Einstellungen geändert werden, die für alle Kameras gelten.
6. Aktivieren oder deaktivieren Sie die gewünschten Einstellungen. Details zu den Einstellungen finden Sie im Abschnitt „[Kamera konfigurieren](#)“ auf Seite 242.

Mehrere Kameras gleichzeitig auswählen und deselektieren

1. Um eine zusammenhängende Liste von Kameras auszuwählen, wählen Sie im Steuerelement „Kamera“ die erste Kamera durch Aktivieren des zugehörigen Kontrollkästchens aus. Im Kontrollkästchen wird ein Häkchen angezeigt.
2. Halten Sie die Umschalttaste gedrückt und wählen Sie die letzte Kamera in der Reihe durch Aktivieren des zugehörigen Kontrollkästchens aus. Alle dazwischen liegenden Kameras werden ausgewählt.
3. Um die Auswahl einer zusammenhängenden Liste von Kameras aufzuheben, deselektieren Sie im Steuerelement „Kamera“ die erste Kamera durch Deaktivieren des zugehörigen Kontrollkästchens. Das Kontrollkästchen ist leer.
4. Halten Sie die Umschalttaste gedrückt und deselektieren Sie die letzte Kamera in der Liste durch Deaktivieren des zugehörigen Kontrollkästchens. Die Auswahl aller dazwischen liegenden Kameras wird aufgehoben.
5. Halten Sie die Umschalttaste gedrückt und aktivieren Sie Kontrollkästchens vor dem Listennamen. Alle Kameras werden ausgewählt.

Bewegen von Kameras

Sie können eine oder mehrere Kameras auf einmal durch Ausschneiden und Einfügen verschieben.

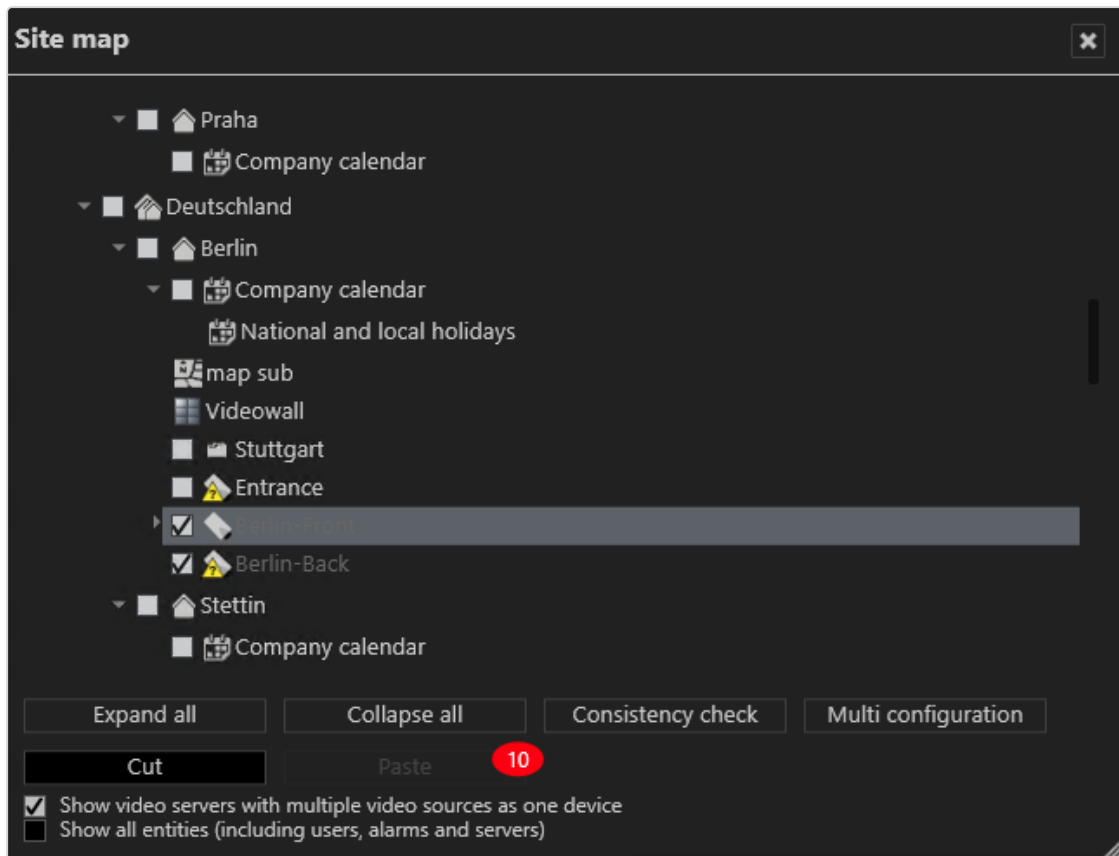



Abb. 137: „Bewegen“ einer Kamera

1. Wählen Sie im Bereich „Unternehmen“ die Option **Sitemap** .
2. Wählen Sie die Kameras durch Anklicken der Kontrollkästchen aus.
3. Wählen Sie **Ausschneiden**. Die ausgewählten Elemente werden ausgegraut und die Anzahl der ausgewählten Elemente wird angezeigt.
4. Wählen Sie eine Filiale oder einen Ordner. Einfügen ist aktiviert.

Wenn mehr als 100 Einträge ausgewählt sind, wird ein Hinweis zur Dauer des Vorgangs angezeigt. Das Verschieben einer großen Anzahl von Entitäten kann einige Minuten dauern.

5. Wählen Sie **Einfügen**, um die Kameras in die ausgewählte Filiale oder den ausgewählten Ordner zu verschieben.

Kamera duplizieren

Durch das Duplizieren einer Kamera mit dem „Kopierassistenten“ können Kameraeinstellungen auf eine größere Anzahl identischer Kameras zeitsparend übertragen werden.

Copying wizard [X]

The following settings are necessary:

Number of copies: 1

Camera name: AXIS 221 (Copy)

Address range: 10.0.8.139 - 10.0.8.139

DeviceManager: DeviceManager_SASCHA-HP

Which optional settings do you want to copy?

- User name and password
- Digital inputs
- Digital outputs
- Image rotation
- Standard recording
- Alarm recording
- Video profiles
- Motion detection

Select all

OK Cancel

Validate settings before device creation

Abb. 138: Kamera duplizieren

1. Wählen Sie die Kamera in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und legen Sie die Anzahl der Kopien fest.
3. Geben Sie den **Namen** für die duplizierte Kamera ein. Die Namen der Kameras erhalten gegebenenfalls eine Nummer, die automatisch hochgezählt wird. Sie können die Namen nach der Erstellung anpassen (siehe „[Kamera konfigurieren](#)“ auf Seite 242).
4. Geben Sie im **Adressenbereich** die IP-Adresse der ersten kopierten Kamera an. Die IP-Adressen werden anhand der Anzahl der Kopien automatisch hochgezählt.
5. Wählen Sie den **Device Manager** aus.
6. Aktivieren Sie die Eigenschaften, die auf die kopierten Kameras übertragen werden sollen.
7. Optional können Sie die Option **Einstellungen vor Anlegen von Geräten validieren** aktivieren.

- Bestätigen Sie den Namen mit **OK**. Die neue Kamera wird in der Übersicht angezeigt.

Kamera löschen

- Wählen Sie die Kamera in der Übersicht aus.
- Klicken Sie auf **Objekt löschen**.

Es werden alle gespeicherten Aufzeichnungen der Kamera gelöscht.

Kamera umwandeln

Eine installierte Kamera kann durch Übertragen der Kamerakonfiguration und der Kameraaufzeichnungen in eine neue Kamera umgewandelt werden (Treiberumwandlung). Alarme, Wächterrundgänge und andere Einstellungen werden auf die neue Kamera vererbt. Mit dieser Umwandlung kann eine neue Kamera installiert werden, um eine defekte zu ersetzen.

Kameras, die den intelligenten (generischen) Treiber verwenden, werden nicht vollständig unterstützt und können nur teilweise umgewandelt werden.

Wenn ein nativer Kameratreiber in einen intelligenten Treiber umgewandelt wird, muss in der Videostream-Konfiguration ein RTSP-Stream ausgewählt werden (siehe „[Videostream bearbeiten](#)“ auf Seite 264).

- Wählen Sie die Kamera in der Übersicht aus.
- Klicken Sie in den allgemeinen Einstellungen der ausgewählten Kamera auf **Konverter öffnen**.

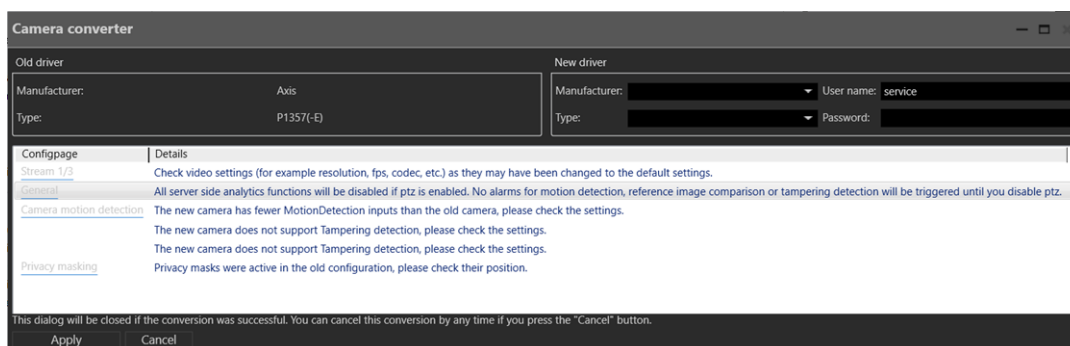


Abb. 139: Kamera umwandeln

- Wählen Sie den **Hersteller** und den **Typ** der neuen Kamera aus.
- Geben Sie bei Bedarf den **Benutzernamen** und das **Passwort** ein.

5. Klicken Sie auf **Konvertierung überprüfen**. Eine Liste potenzieller Konvertierungsprobleme wird angezeigt.
6. Beheben Sie die Probleme und klicken Sie dann auf **Übernehmen**, um die Konvertierung zu starten.

Sonstige Hardware

Mit der Funktion **Sonstige Hardware** im Steuerelement Administration können Sie zusätzliche Geräte konfigurieren und verwalten. Zu diesen Geräten gehören unter anderem Netzwerkschnittstellen, Videowände, Alarmanlagen und I/O-Module. Diese Geräte können teilweise mit Qognify VMS verwaltet und angesteuert werden, als auch mit Hilfe der Software von Drittherstellern.

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste der Steuerleiste angezeigt.
2. Wählen Sie **Sonstige Hardware** in der Steuerleiste.

Neue Hardware anlegen

Create new hardware [X]

Name:
Analytics 2D inside

Manufacturer:
SeeTec Video Analytics

Type:
SeeTec Analytics Server 3D

Analytics Server 3D Module:
Analytics Server Module 4 SASCHA-HP

Available IP installers:
[Dropdown]

IP setup

OK Wizard Cancel

Validate settings before device creation

Abb. 140: Neue Hardware anlegen

1. Legen Sie eine neue Hardware an.
 2. Geben Sie den **Namen** für die neue Hardware ein.
 3. Wählen Sie den **Hersteller** und **Typ** der Hardware aus. Folgende Hersteller und Typen stehen zur Verfügung:
 - **Third Party Interface:** eyevis wall, SPC Alarmanlage, Aritech-Alarmzentrale, Schneider Intercom ICX Connection, Siemens SPC 4000/5000/6000.
- Informationen zur Verwendung von Third Party Interfaces finden Sie unter „Sonstige Hardware integrieren“ oder fragen Sie den Qognify-Support.**
- **Qognify:** Network I/O, Display Agent und VoIP
 - **Qognify Video Analytics:** Generischer VCA-Kanal, Kennzeichenerkennung, LPR VCA, Qognify Analytics Basic / Enterprise / Premium, Qognify Analytics Server 3D, Qognify Counting Suite
 - **Advantech:** ADAM 6050/6050W, ADAM 6052, ADAM 6060/6060W/6066
 - **AXIS:** A9161, A9188
 - **W&T:** WEB-IO 2x Digital IN/OUT
 - **Wago:** Wago System 750 I/O-Modul
 4. Aktivieren Sie gegebenenfalls eine erforderliche **Autorisierung** und geben Sie **Benutzernamen** und **Passwort** ein.
 5. Geben Sie gegebenenfalls den Namen des **Hosts** oder die **IP-Adresse** des Geräts ein.
 6. Wählen Sie gegebenenfalls den **Device Manager** aus.
 7. Bestätigen Sie die Angaben mit **OK**. Die neue Hardware wird in der Übersicht angezeigt.

Hardware konfigurieren

1. Wählen Sie die Hardware in der Übersicht **Sonstige Hardware** aus.
2. Passen Sie die Einstellungen der Hardware an. Folgende Optionen stehen zur Verfügung:
 - „Third Party Interface“ unten
 - SeeTec
 - „Qognify Video Analytics“ auf Seite 315
 - „Advantech“ auf Seite 339
 - „AXIS“ auf Seite 342
 - „W&T“ auf Seite 344
 - „Wago“ auf Seite 346

Hardware löschen

1. Wählen Sie die Hardware in der Übersicht **Sonstige Hardware** aus.
2. Klicken Sie auf das Symbol **Objekt löschen**.

Third Party Interface

In diesem Abschnitt wird die Konfiguration folgender Module beschrieben:

- Aritech-Alarmzentrale
- eyevis Wand
- Schneider Intercom ICX Connection
- Siemens SPC 4000/5000/6000
- TDSi-Zutrittskontrolle

Third Party Interfaces (Dritthersteller-Schnittstellen) müssen im Allgemeinen auf der Seite der Drittherstellerkomponente vorkonfiguriert werden. In diesem Abschnitt wird nur die Konfiguration in Qognify Qognify VMS beschrieben.

Informationen zur Konfiguration der Third Party Interfaces der Komponenten finden Sie im Dokument „Technical_Guides_Qognify_Qognify VMS_7.4_DE.pdf“ oder wenden Sie sich an den Support (siehe „[Support](#)“ auf Seite 13).

Aritech-Alarmzentrale

Die Aritech-Alarmzentrale sendet Alarme und Ereignisse über den OH-Netzwerkempfänger an das Qognify-System, das die Ereignisse quittiert und sie im Rahmen von Alarmszenarien verarbeitet. Alle von der Aritech-Alarmzentrale an das Qognify-System übermittelten Nachrichten müssen von Qognify VMS quittiert werden, da sie ansonsten erneut gesendet werden. Der Verbindung ist unidirektional.

Die Systeme kommunizieren per TCP unter Verwendung des Sicherheitskommunikationsprotokolls (Protokoll „Format SIA“) für die Kommunikation zwischen Alarmanlagen (SIA DC-03-1990.01(R2003.10)).

Informationen zur Installation und Konfiguration der Aritech-Alarmzentrale finden Sie im Dokument „Technical_Guides_Qognify_Qognify VMS_7.4_DE.pdf“ oder wenden Sie sich an den Support (siehe „Support“ auf Seite 13).

General	
<input checked="" type="checkbox"/> Activated	
Name:	Aritec Alarm Center
DeviceManager server:	DeviceManager_SASCHA-HP
OH port:	60030
Central ID:	1212

Abb. 141: Aritech-Alarmzentrale konfigurieren - 1

1. Fügen Sie einen neuen **Sonstigen Hardware-Hersteller** hinzu, indem Sie „3rd Party Interface“ und als **Typ** „Aritech-Alarmzentrale“ wählen.
2. Wählen Sie den **Device Manager-Server** für die Verwaltung der Alarmzentrale aus. Das Aritech-System muss seine Ereignisse an diesen Server senden.
3. Geben Sie den **OH-Port** an, an den die Ereignisse vom OH-Netzwerkempfänger über den Logging-Appender gesendet werden sollen. Der Port ist in der Datei seetec.properties angegeben. Diese Datei befindet sich im Installationsverzeichnis des OH-Netzwerkempfängers.
4. Geben Sie die **Zentrale ID** ein.

Diese ID wird Ihnen vom Errichter der Aritech-Alarmzentrale mitgeteilt.

Regeln

Eine Regel setzt sich aus einem Namen, einer Zonen-ID, einer Bereichs-ID und einem Ereignis zusammen.

Folgende Elemente aus den Ereignissen der Aritech-Alarmzentrale können in einer Regel verwendet werden:

- Alarm [SIA-Code: BA]: Alarm
- Manipulation [SIA-Code: TA]: Manipulationsereignisse
- Scharf geschaltet [SIA-Code: CL]: Alarmzentrale wird scharf geschaltet
- Unscharf geschaltet [SIA-Code: OP]: Alarmzentrale wird unscharf geschaltet
- Maske [SIA-Code: BT]: Ein Sensor meldet, dass eine Zone maskiert ist.
- Ausgeschlossen [SIA-Code: BB]: Zone wurde gelöscht.
- Forciert scharf geschaltet [SIA-Code: CF]: Alarmzentrale wird scharf geschaltet, obwohl offene Probleme bestehen.

Regeln einrichten

Activated	Name	Zone ID	Area ID	1	2	3	4	5	6	7	All	Delete
<input checked="" type="checkbox"/>	Alarm	1	2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Mask	4	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

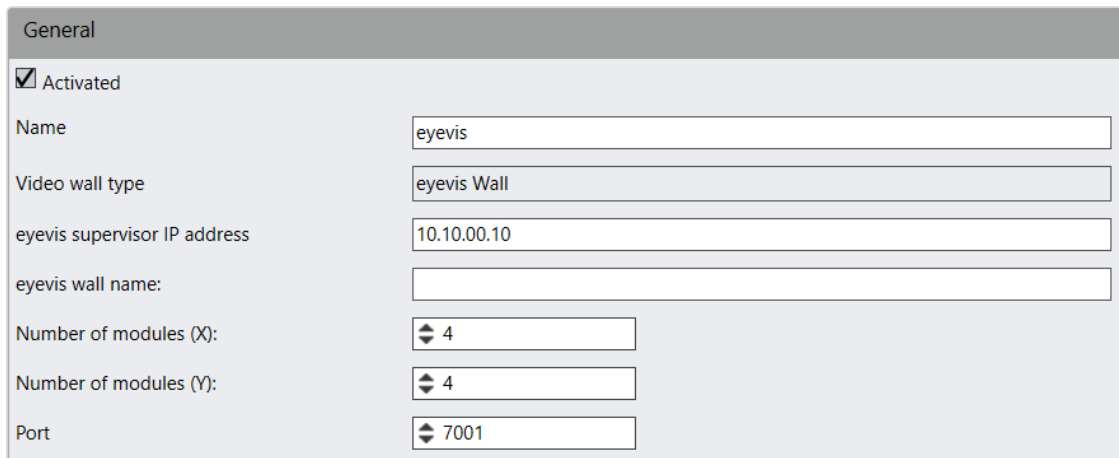
Abb. 142: Aritech-Alarmzentrale konfigurieren - 2

1. Wählen Sie **Eine Regel hinzufügen** bzw. **10 Regeln hinzufügen**.
2. Aktivieren Sie die Regel.
3. Geben Sie einen Namen für die Regel ein.
4. Geben Sie die **Zonen-ID** für die entsprechende Zone ein.
5. Geben Sie die **Bereichs-ID** für den entsprechenden Bereich ein.
6. Wählen Sie das gewünschte Ereignis (Spalte „1“ bis „7“). Eine Mehrfachauswahl ist möglich. Die Zonen- und Bereichs-ID werden Ihnen vom Errichter der Aritech-Alarmzentrale mitgeteilt.

eyevis Wand

eyevis bietet Videowandsysteme, die von einem Qognify VMS-Client gesteuert werden.

Allgemein



General	
<input checked="" type="checkbox"/> Activated	
Name	eyevis
Video wall type	eyevis Wall
eyevis supervisor IP address	10.10.00.10
eyevis wall name:	
Number of modules (X):	4
Number of modules (Y):	4
Port	7001

Abb. 143: Allgemein

1. Aktivieren oder deaktivieren Sie das Modul.
2. Passen Sie gegebenenfalls den **Namen** an.
3. Geben Sie die **eyevis-Supervisor IP-Adresse** an.
4. Legen Sie den **eyevis Wandnamen** fest.
5. Teilen Sie die auf der Videowand von eyevis zur Verfügung stehende Bildfläche in einzelne Videowand-Module auf, indem Sie Werte für **Anzahl Module X** und **Anzahl Module Y** eingeben.
6. Geben Sie den Port an, auf dem der **eyevis Supervisor** erreichbar ist.
7. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
8. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Weitere Einstellungen müssen in der Videowandkonfiguration festgelegt werden (siehe „Videowände“ auf Seite 430).

Schneider Intercom ICX Connection

Für die Kommunikation mit Schneider Intercom wird ein proprietäres Protokoll verwendet (ICX-Protokoll, Version 1.1/0910 „PRELIMINARY“). Die Ereignisse werden über dieses Protokoll bereitgestellt. Innerhalb des Protokollstreams gibt es keine Gesprächsdaten, sondern nur Informationen wie „X stellt eine Verbindung mit Y her“. Es sind keine aktiven Protokollfunktionen implementiert. Dieser Qognify-Server empfängt Ereignisse nur. Qognify ist nicht in der Lage, Befehle an den Schneider Intercom-Server zu senden.

Informationen zur Installation und Konfiguration der Schneider Intercom ICX Connection finden Sie im Dokument „Technical_Guides_Qognify_Qognify VMS_7.4_DE.pdf“ oder wenden Sie sich an den Support (siehe „Support“ auf Seite 13).

Allgemein

Der Schneider Intercom-Geräteserver wird durch die separat bereitgestellte Schneider-Software konfiguriert. Die Terminalidentifizierung erfolgt ebenfalls mithilfe der Schneider-Software.

General

Activated

Name:

DeviceManager server:

Schneider Intercom server:

Schneider Intercom port:

Use authorization

Password:

Abb. 144: Schneider Intercom ICX Connection - Allgemein

1. Legen Sie ein neues Modul mit den folgenden Einstellungen an:
 - Hersteller: 3rd Party Interface
 - Typ: Schneider Intercom ICX
2. Aktivieren Sie das Modul.
3. Wählen Sie den **Device Manager** für die Verwaltung des Schneider-Geräts aus.
4. Geben Sie bei **Schneider Intercom-Server** und **Schneider Intercom-Port** die IP-Adresse und den Port des Schneider Intercom-Servers ein.
5. Optional können Sie **Autorisierung verwenden** aktivieren, um den Zugriff einzuschränken, und das Passwort eingeben.

Regeln




Rules

Search

	Activated	Name	Events	Number of caller	Number of callee
▶	<input checked="" type="checkbox"/>	DA	Call request	F102	
	<input checked="" type="checkbox"/>	FDA	End of the call request	F101	
	<input checked="" type="checkbox"/>	AA	Call acceptance		
	<input checked="" type="checkbox"/>	FA	End of call		

Abb. 145: Schneider Intercom ICX Connection - Regeln

Eine Regel setzt sich aus einem Namen, einem Ereignistyp und der Nummer des Anrufers oder Angerufenen zusammen.

1. Um eine Regel hinzuzufügen, klicken Sie auf **Hinzufügen** .
2. Um mehrere Regeln (10) gleichzeitig hinzuzufügen, klicken Sie auf **Mehrere Regeln hinzufügen** .
3. Um eine oder mehrere Regeln zu löschen, wählen Sie die Regel(n) aus und klicken Sie auf **Löschen** .
4. Legen Sie fest, dass die folgenden Ereignisse von Qognify in einer Regel verwaltet werden sollen:
 - Nichts ausgewählt
 - Rufanforderung (ICX Code Task 5B Type 21)
 - Ende der Rufanforderung (ICX Code Task 5B Type 30)
 - Rufannahme (Verbindung wird gestartet) (ICX Code Task 42 Type 12)
 - Ende des Anrufes (ICX Code Task 42 Type 10)
 - Diskreter Anruf (ICX Code Task 42 Type 13)
 - Gruppenruf (ICX Code Task 42 Type 0B)
 - Rufanforderung Notfall (ICX Code Task 5B Type 22)

Ab Qognify VMS R12 wird "Anruf 2" in einem anderen Ereignis verarbeitet. Kunden müssen eventuell ihre bestehende Konfiguration ändern. Vor der Änderung war „Anruf 2“ im normalen „Anruf“-Ereignis enthalten, jetzt ist es ein separates Ereignis.

5. Geben Sie die Nummer des Anrufers und des Angerufenen ein. Es gibt zwei mögliche Datenformate: 4-stellige und 8-stellige hexadezimale Zahlen.
6. Füllen Sie die nicht verwendeten Ziffern mit „F“, um einen vollständigen Block zu bilden.

Beispiel

Nummer (= Terminal-ID)	> 4-stellig	8-stellig
101	F101	-
12321	-	FFF12321

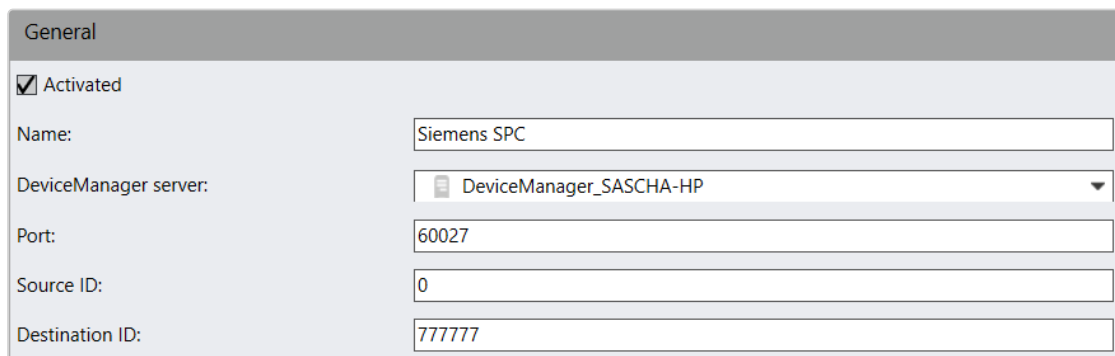
7. Legen Sie ein Alarmszenario an und wählen Sie die entsprechende Regel als Starterereignis aus (siehe „[Alarmszenario anlegen](#)“ auf Seite 387).

Siemens SPC 4000/5000/6000

Die Siemens-Alarmzentrale ist in der Lage, auftretende Alarme/Ereignisse an das Qognify-System zu übermitteln. Das Qognify-System quittiert die Ereignisse und ist in der Lage, diese im Rahmen von Alarmszenarien zu verarbeiten.

Die generelle Kommunikation der beiden Systeme erfolgt über TCP. Der Aufbau einer TCP-Verbindung wird immer von der Siemens-Alarmzentrale durchgeführt. Alle von der Siemens-Alarmzentrale an das Qognify-System übermittelten Nachrichten werden dabei von Qognify quittiert, da sie ansonsten erneut gesendet werden.

Allgemein



General	
<input checked="" type="checkbox"/> Activated	
Name:	Siemens SPC
DeviceManager server:	DeviceManager_SASCHA-HP
Port:	60027
Source ID:	0
Destination ID:	777777

Abb. 146: Allgemein

1. Aktivieren oder deaktivieren Sie das Modul.
2. Passen Sie gegebenenfalls den **Namen** an.
3. Ändern Sie gegebenenfalls den Server zur Verwaltung der Geräte (**Device Manager**). Die Alarmanlage übermittelt die Nachrichten an diesen Server.
4. Passen Sie gegebenenfalls den **IP-Port** des Empfängers für die Übertragung von Nachrichten von der Einbruchmeldezentrale an (Standard: 60027). Verwenden Sie pro Einbruchmeldezentrale einen separaten Port.
5. Geben Sie die Installations-ID als **Source ID** an. Diese ID wird zur Quittierung von Nachrichten verwendet. Die IDs in Qognify VMS und in der Siemens-Einbruchmeldezentrale müssen identisch sein. Die Source ID entnehmen Sie der Konfiguration der SPC-Alarmanlage.
6. Geben Sie die Empfänger-ID als **Destination ID** an. Die Destination IDs in Qognify VMS und in der Siemens-Einbruchmeldezentrale müssen identisch sein (Standard: 777777). Die 'Destination ID' entnehmen Sie der Konfiguration der SPC-Alarmanlage.

Die entsprechenden Moduleinträge der SPC Alarmanlage (Source ID) und die Einträge des Qognify-Systems (Destination ID) müssen identisch sein.

Bereiche

Sie können für jede Einbruchmeldezentrale bis zu 64 Bereiche aktivieren. Jeder Bereich kann scharf oder unscharf geschaltet und als Auslöseereignis für ein Qognify-Alarmszenario verwendet werden.

Areas			
Area	Activated	Name of arming	Name of disarming
1	<input checked="" type="checkbox"/>	Armed: area 1	Disarmed: area 1
2	<input checked="" type="checkbox"/>	Armed: area 2	Disarmed: area 2

Abb. 147: Bereiche

1. Aktivieren Sie den Bereich und geben Sie den **Namen der Scharfschaltung** und den **Namen der Unscharfschaltung** an. Bei Auslösen eines Ereignisses an der Alarmanlage wird statt einer Nummer der angegebene Begriff angezeigt (beispielsweise „Fenster offen“ / „Fenster geschlossen“).

Der Zustand eines Bereichs kann im Lageplan visualisiert werden (siehe „[Lagepläne](#) und „[Erweiterte Lagepläne](#)“ auf Seite 407). Der Bereich wird nach 10 bis 15 Sekunden rot (scharf) oder grün (unscharf) dargestellt.

Regeln

Eine Regel setzt sich aus einem Namen, einem Ereignistyp und einer zugehörigen Zone zusammen. Eine Regel stellt eine Zone dar. Sie wird als Regel bezeichnet, da jede Zone über einen Typ, jedoch zwei Ereignisse (Alarm/Wiederherstellung) verfügen kann. Daher sind in Qognify VMS zwei verschiedene Typen erforderlich, um sie mit Alarmszenarien zu verwenden.

Rules					
Add new rule		<input type="button" value="Add"/>			
Add 10 new rules		<input type="button" value="Add"/>			
Delete rules marked for deletion		<input type="button" value="Delete"/>			
Activated	Name	Type	Zone	Delete	
<input type="checkbox"/>	New rule			<input type="checkbox"/>	
<input type="checkbox"/>	New rule			<input type="checkbox"/>	
<input type="checkbox"/>	New rule	No events		<input type="checkbox"/>	
<input type="checkbox"/>	New rule	Burglar alarm (BA)		<input type="checkbox"/>	
<input type="checkbox"/>	New rule	Burglar alarm (restore) (BR)		<input type="checkbox"/>	
<input type="checkbox"/>	New rule	Holdup alarm (HA)		<input type="checkbox"/>	
<input type="checkbox"/>	New rule	Holdup alarm (restore) (HR)		<input type="checkbox"/>	

Abb. 148: Regeln

1. Klicken Sie auf **Neue Regel hinzufügen** bzw. **10 neue Regeln hinzufügen**, um eine bzw. zehn neue Regeln anzulegen.
2. Aktivieren Sie die gewünschte Regeln und passen Sie den **Namen** an.

3. Wählen Sie das **Ereignis** aus, das zu einer Alarmmeldung führen soll. Die Alarmanlage unterscheidet zwischen den zwei Ereignissen Einbruchsalarm und Panikalarm. In der Regel legen Sie fest, um welche Art von Alarm es sich handelt.
4. Geben Sie die **Meldergruppe** an, um die ID des Geräts anzugeben, das das Alarmsignal sendet.
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Die folgenden, von der Siemens-Einbruchmeldezentrale gesendeten Ereignistypen können von Qognify Qognify VMS als Regeln verarbeitet werden:

- Einbruchalarm (BA)
- Einbruchalarm Wiederherstellung (BR)
- Panikalarm (PA)
- Panikalarm Wiederherstellung (PR)
- Medizinischer Alarm (MA)
- Medizinischer Alarm Wiederherstellung (MR)
- Sabotagealarm (BT)
- Sabotagealarm Wiederherstellung (BJ)
- Sabotagealarm (TA)
- Sabotagealarm Wiederherstellung (TR)
- Technischer Alarm (UA)
- Technischer Alarm Wiederherstellung (UR)
- Störung Überfallzone (HT)
- Störung Überfallzone Wiederherstellung (HJ)
- Störung Panikzone (PT)
- Störung Panikzone Wiederherstellung (PJ)
- Störung medizinische Zone (MT)
- Störung medizinische Zone Wiederherstellung (MJ)
- Technische Störung/Sabotage (UT)
- Technische Störung/Sabotage Wiederherstellung (UJ)
- Netzwerk verbunden (NR)
- Netzwerk getrennt (NT)

Ausgänge

Outputs				
Output	Activated	Name for CLOSE	Name for OPEN	Hold time (s)
1	<input checked="" type="checkbox"/>	CLOSE: output 1	OPEN: output 1	5
2	<input checked="" type="checkbox"/>	CLOSE: output 2	OPEN: output 2	0
3	<input type="checkbox"/>	CLOSE: output 3	OPEN: output 3	0

Abb. 149: Ausgänge

Sie können für jede SPC-Zentrale bis zu 8 Ausgänge aktivieren. Jeder Ausgang kann auf „SCHLIESSEN“ oder „OFFEN“ festgelegt werden.

1. Aktivieren Sie den Ausgang.
2. Optional können Sie die Namen anpassen.

Haltedauer wird in Qognify VMS nicht verwendet, ist in der SPC-Zentrale jedoch konfiguriert.

TDSi-Zutrittskontrolle

TDSi ist ein Zutrittskontrollsystem von [Time and Data Systems International Limited](#).

Das TDSi-System wird durch den Export der Textdateien von TDSi verbunden, die vom Qognify-System gelesen werden.

TDSi-Verbindung konfigurieren

1. Legen Sie ein neues Modul mit den folgenden Einstellungen an:
 - Hersteller: 3rd Party Interface
 - Typ: TDSi-Zutrittskontrolle

Allgemein

General	
<input checked="" type="checkbox"/> Activated	
Name:	<input type="text" value="tdsi"/>
DeviceManager server:	<input type="text" value="DeviceManager_SASCHA-HP"/>
TDSi export directory:	<input type="text" value="\\10.0.1.1\tdsi_export"/>
TDSi export delimiter:	<input type="text" value=","/>

Abb. 150: TDSi-Zutrittskontrolle - Allgemein

1. Aktivieren Sie die Zutrittskontrolle.
2. Optional können Sie den **Namen** des Geräts ändern.
3. Wählen Sie den **Device Manager-Server** zur Verwaltung der TDSi-Verbindung aus.
4. Geben Sie das **TDSi-Exportverzeichnis** an, in dem der EXgarde Event Exporter Ereignisse speichert.
5. Falls das Verzeichnis nicht lokal auf dem Qognify-Server angelegt wurde, geben Sie den vollständigen UNC-Pfad ein.
6. Geben Sie das **Trennzeichen für TDSi-Export** an.

Ereignisgruppen

Das Anlegen von Ereignisgruppen ist optional. Ereignisgruppen dienen in einer Regel als Starterereignis für Alarmszenarien. Auf diese Weise kann unabhängig vom Ereignis stets dasselbe Alarmszenario gestartet werden.

The screenshot shows a web-based configuration interface for 'Event groups'. At the top, there's a header 'Event groups'. Below it, a large text input field contains 'Event group 1'. To the right of this field are two buttons: 'Add' and 'Delete'. Below the main input field is a section titled 'Event group' with a smaller text input field also containing 'Event group 1'. Underneath this is a list of events with checkboxes: 'Door opened (1001)', 'Door closed (1002)', 'Door forced (1003)', 'Door local alarm (1004)', 'Door remote alarm (1005)', and 'Door egress on (1006)'. All checkboxes are currently unchecked.

Abb. 151: TDSi-Zutrittskontrolle - Ereignisgruppen

1. Um eine neue Ereignisgruppe anzulegen, klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen der Ereignisgruppe im Textfeld an.
3. Wählen Sie in der Liste **Ereignisgruppe** ein oder mehr Ereignisse aus, die der Ereignisgruppe zugeordnet sind.

Regeln

Activated	Name	Events	Source	Detail 1	Detail 2	Detail 3	Delete
<input checked="" type="checkbox"/>	rule 1	[Dropdown]					<input type="checkbox"/>
<input checked="" type="checkbox"/>	New rule 2	No events					<input type="checkbox"/>

Abb. 152: TDSi-Zutrittskontrolle - Regeln

1. Klicken Sie auf **Eine Regel hinzufügen** bzw. **10 Regeln hinzufügen**, um eine bzw. zehn Regeln gleichzeitig hinzuzufügen.
2. Geben Sie den Namen der Regel in der Spalte **Name** der Tabelle ein.
3. Wählen Sie für das Ereignis entweder ein einzelnes Ereignis oder eine Ereignisgruppe aus, die Sie zuvor angelegt haben.
4. Optional können Sie die Felder **Quelle**, **Ausschnitt 1**, **Ausschnitt 2** und **Ausschnitt 3** ausfüllen. Die Felder entsprechen den Feldern in der EXgarde Explorer-Übersicht.

Groß- und Kleinschreibung in den Feldern „Quelle“ sowie „Ausschnitt 1“ bis „Ausschnitt 3“ muss genau der im EXgarde Event Exporter und in der Qognify-Konfiguration entsprechen. Anderenfalls wird das Alarmszenario nicht ausgelöst.

Beispiel

Tür geöffnet ist ausgewählt als Ereignis, Vordereingang ist ausgewählt als Quelle und Benutzer Testbenutzer als Ausschnitt 1.

Das entsprechende Alarmszenario wird nur gestartet, wenn Benutzer Testbenutzer die Tür öffnet Vorderer Eingang.

Qognify

Für sonstige Hardware von Qognify muss Folgendes konfiguriert werden:

- Netzwerk-Ein- und -Ausgang
- Display Agent-Videowand

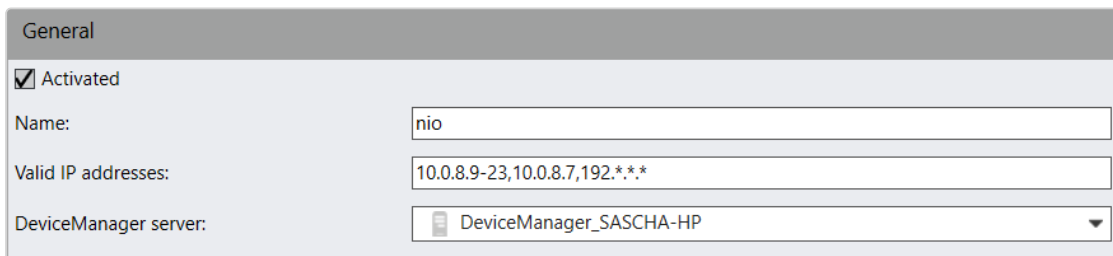
- VoIP

Informationen zur Konfiguration finden Sie in den folgenden Abschnitten.

Qognify Network I/O

Qognify kann Network I/O bereitstellen, beispielsweise zum Auslösen einer Hardwarefunktion über das Netzwerk.

Allgemein



General

Activated

Name:

Valid IP addresses:

DeviceManager server:

Abb. 153: Allgemein

1. Aktivieren oder deaktivieren Sie das Modul.
2. Passen Sie gegebenenfalls den Namen an.
3. Geben Sie gegebenenfalls die **Erlaubten IP-Adressen** oder IP-Adressbereiche an, um eine „Maske“ anzulegen, innerhalb derer Eingangsoperationen angenommen werden sollen. Diese Angabe ist optional. Sie können beliebig viele Masken kommagetrennt (ohne Leerzeichen) angeben. Innerhalb einer Maske können die Platzhalter „*“ und „-“ verwendet werden. Falls keine Maske vergeben wird, wird jede eingehende Verbindung akzeptiert.

Beispiel

10.0.8.9-23,10.0.8.7,192..**

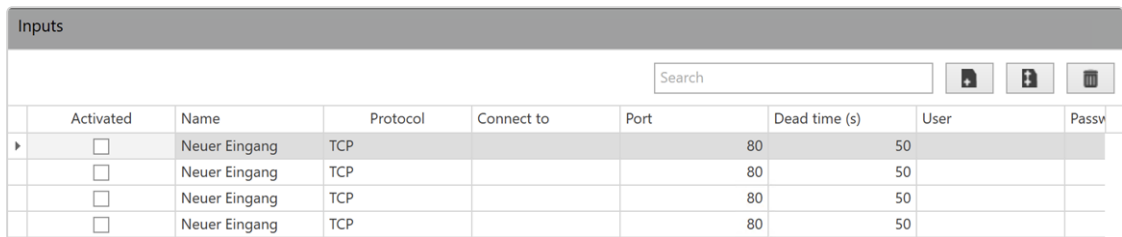
Es wurden drei einschränkende Masken definiert:

Maske 10.0.8.9-23 lässt alle IP-Adressen im Bereich 10.0.8.9 bis 10.0.8.23 zu. Maske 10.0.8.7 lässt die einzelne IP-Adresse zu.

Maske 192..* lässt das gesamte Subnetz 192 zu.*

4. Ändern Sie gegebenenfalls den Device Manager-Server (siehe [„Installation eines abgesetzten Servers“](#) auf Seite 38).

Eingänge



The screenshot shows a web-based configuration interface for 'Inputs'. At the top, there is a search bar and three icons (add, edit, delete). Below is a table with the following columns: 'Activated', 'Name', 'Protocol', 'Connect to', 'Port', 'Dead time (s)', 'User', and 'Passw'. The table contains four rows, each with a checkbox in the 'Activated' column and the text 'Neuer Eingang' in the 'Name' column. The 'Protocol' column for all rows is 'TCP'. The 'Port' and 'Dead time (s)' columns have values of 80 and 50 respectively for each row.

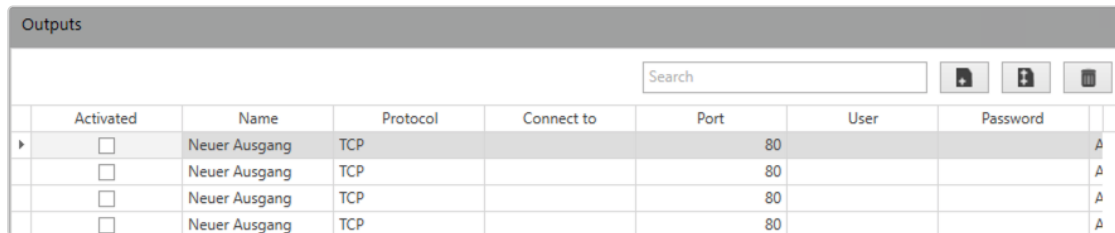
Activated	Name	Protocol	Connect to	Port	Dead time (s)	User	Passw
<input type="checkbox"/>	Neuer Eingang	TCP		80	50		
<input type="checkbox"/>	Neuer Eingang	TCP		80	50		
<input type="checkbox"/>	Neuer Eingang	TCP		80	50		
<input type="checkbox"/>	Neuer Eingang	TCP		80	50		

Abb. 154: Eingänge

1. Klicken Sie auf **Neuen Eingang hinzufügen** bzw. **10 neue Eingänge hinzufügen**, um einen bzw. zehn neue Eingänge anzulegen.
2. Klicken Sie auf **Aktiviert**, um einen Eingang zu aktivieren bzw. zu deaktivieren. Um den Aktivierungszustand für mehrere Eingänge festzulegen, halten Sie die Umschalt- oder Strg-Taste auf der Tastatur gedrückt, während Sie weitere Eingänge auswählen.
3. Ändern Sie den **Namen** des Eingangs.
4. Wählen Sie das Netzwerk-**Protokoll** für den Eingang aus. Folgende Protokolle stehen zur Verfügung:
 - TCP zur Verbindung innerhalb des Netzwerks,
 - TCP (permanent) zur permanenten Verbindung innerhalb des Netzwerks,
 - HTTP zur Verbindung über das Internet.
5. Geben Sie in der Spalte **Verbinden mit** die IP-Adresse und die **Portnummer** für die eingehende Eingangsverbindung an.
6. Geben Sie das Intervall für die **Totzeit** (in Sekunden) an, nach dem wieder ein Signal ausgewertet wird.
7. Wenn das HTTP-Protokoll ausgewählt ist, geben Sie den **Benutzernamen** und das **Password** für den Zugriff auf die Hardware an.
8. Wählen Sie den **Typ** des Texts, der übertragen werden kann, wenn eine Eingangsverbindung besteht. Mit der Option ASCII können nur Groß- und Kleinbuchstaben sowie Zahlen ohne Sonderzeichen verwendet werden. Bei HEX sind alle Zeichen erlaubt.
9. Geben Sie den **Text** ein, der angezeigt werden soll, sobald auf die Hardware zugegriffen wird.
10. Optional können Sie die **Steuerzeichen**-Kodierung festlegen, um beispielsweise Absatzwechsel im Text korrekt darzustellen.

- Um Eingänge zu löschen, markieren Sie die zu löschenden Eingänge und klicken Sie auf **Als „Löschen“ markierte Eingänge löschen**. Wenn Sie mehrere Eingänge löschen möchten, halten Sie die Umschalt- oder Strg-Taste gedrückt, während Sie die Eingänge auswählen.

Ausgänge



The screenshot shows a window titled 'Outputs' with a search bar and three icons (add, edit, delete). Below is a table with columns: Activated, Name, Protocol, Connect to, Port, User, Password, and a small icon column. The table contains four rows, all with 'Neuer Ausgang' as the name and 'TCP' as the protocol. The port is '80' for all. The 'Activated' column has checkboxes, and the icon column has a small 'A' icon.

Activated	Name	Protocol	Connect to	Port	User	Password	
<input type="checkbox"/>	Neuer Ausgang	TCP		80			A
<input type="checkbox"/>	Neuer Ausgang	TCP		80			A
<input type="checkbox"/>	Neuer Ausgang	TCP		80			A
<input type="checkbox"/>	Neuer Ausgang	TCP		80			A

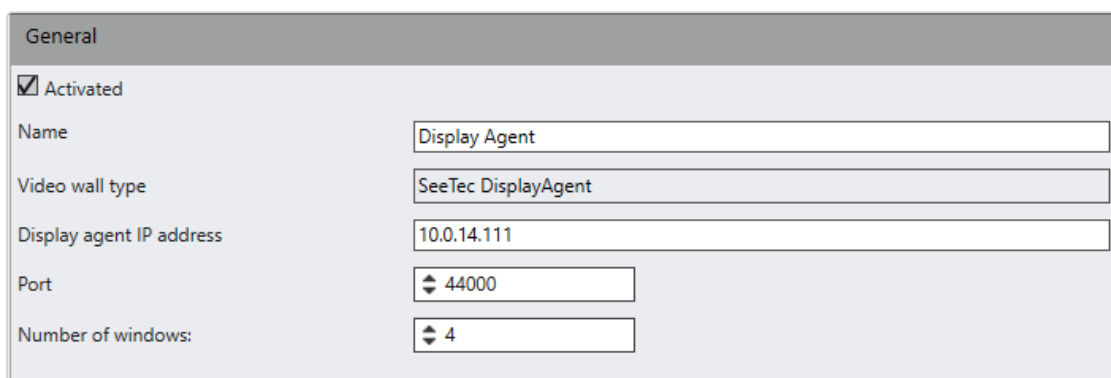
Abb. 155: Ausgänge

- Klicken Sie auf **Neuen Ausgang hinzufügen** bzw. **10 neue Ausgänge hinzufügen**, um einen bzw. zehn neue Ausgänge anzulegen.
- Klicken Sie auf **Aktiviert**, um einen Ausgang zu aktivieren bzw. zu deaktivieren. Um den Aktivierungszustand für mehrere Ausgänge festzulegen, halten Sie die Umschalt- oder Strg-Taste gedrückt, während Sie die Ausgänge auswählen.
- Ändern Sie den **Namen** des Ausgangs.
- Wählen Sie das Netzwerk-**Protokoll** für den Ausgang aus. Folgende Protokolle stehen zur Verfügung:
 - TCP zur Verbindung innerhalb des Netzwerks,
 - HTTP zur Verbindung über das Internet,
 - HTTPS zur verschlüsselten Verbindung über das Internet.
- Geben Sie die IP-Adresse und die Portnummer an, mit denen der Ausgang eine Verbindung aufbauen soll. Sie können mehreren Ausgängen die gleiche IP-Adresse zuweisen.
- Wenn das HTTP- oder HTTPS-Protokoll ausgewählt ist, geben Sie den **Benutzernamen** und das **Passwort** für den Zugriff auf die Hardware an.
- Wählen Sie den **Typ** der Passwortkodierung. Mit der Option ASCII können nur Groß- und Kleinbuchstaben sowie Zahlen ohne Sonderzeichen verwendet werden. Bei HEX sind alle Zeichen erlaubt.
- Geben Sie den **Text** ein, der angezeigt werden soll, sobald auf die Hardware zugegriffen wird.

- Um Ausgänge zu löschen, markieren Sie die zu löschenden Ausgänge und klicken Sie auf **Als „Löschen“ markierte Ausgänge löschen**. Wenn Sie mehrere Ausgänge löschen möchten, halten Sie die Umschalt- oder Strg-Taste gedrückt, während Sie die Ausgänge auswählen.

Qognify Display Agent (Videowand)

Der Qognify Display Agent ist im Qognify-Client integriert. Mit dem Display Agent kann jeder Client-Rechner (siehe „[Systemvoraussetzungen](#)“ auf Seite 31) und die angeschlossenen Monitore als voll funktionsfähige Videowand verwendet werden.



General	
<input checked="" type="checkbox"/> Activated	
Name	Display Agent
Video wall type	SeeTec DisplayAgent
Display agent IP address	10.0.14.111
Port	44000
Number of windows:	4

Abb. 156: Qognify Display Agent (Videowand)

- Aktivieren oder deaktivieren Sie das Modul.
- Passen Sie gegebenenfalls den **Namen** an.
- Passen Sie gegebenenfalls die **IP-Adresse** des Rechners an, auf dem der Qognify Display Agent installiert ist.
- Legen Sie die **Anzahl der Fenster** fest, um die der Monitore auf dem Rechner zu bestimmen, auf dem der Qognify Display Agent installiert wurde. Es wird empfohlen, ein Fenster pro Monitor anzugeben.

Weitere Einstellungen müssen in der Videowandkonfiguration festgelegt werden (siehe „[Videowände](#)“ auf Seite 430)

VoIP

Die Konfiguration setzt passende Hardware (VoIP-fähige Geräte wie beispielsweise entsprechende Mobotix-Kameras und Türsprechanlagen voraus).

Allgemein

General

Activated

Name:

SIP address:

DeviceManager server:

Activated

DTMF sequence

Button

DTMF sequence

Start of call

End of call

Abb. 157: Allgemein

1. Aktivieren oder deaktivieren Sie das Modul.
2. Passen Sie gegebenenfalls den **Namen** an.
3. Passen Sie gegebenenfalls die **SIP-Adresse** des Rechners an, auf dem das VoIP-Modul installiert ist.
4. Wählen Sie den **Device Manager** aus.
5. Wählen Sie **Aktivieren**. Wählen Sie aus, ob über die DTMF-Funktionstaste im Überwachungsmodus (siehe „[Audio](#)“ auf Seite 166) eine **DTMF-Sequenz** oder ein **Button** ausgelöst werden soll.
 - Geben Sie gegebenenfalls die DTMF-Sequenz an, die Sie dem Handbuch des Geräteherstellers entnehmen können, oder wählen Sie einen Qognify-Button aus (siehe „[Button konfigurieren](#)“ auf Seite 417).
6. Geben Sie die **DTMF-Sequenzen** für den Beginn und das Ende des Anrufs an. Die DTMF-Sequenz ist zu Beginn oder Ende eines Anrufs vom Client im Überwachungsmodus zu senden (siehe „[Audio](#)“ auf Seite 166).

VoIP-Aufzeichnung

Voice over IP-Sitzungen können als Standard-VoIP-Aufzeichnungen oder als Alarm-VoIP-Aufzeichnungen definiert werden.

Voice over IP recording

Standard VoIP recording Activated

Recording period

Days: Hours:

Alarm VoIP recording Activated

Days: Hours:

Abb. 158: VoIP-Aufzeichnung

1. Aktivieren Sie **Standard-VoIP-Aufzeichnung** und legen Sie den **Aufzeichnungszeitraum** mithilfe einer Zeitschablone fest (siehe „[Zeitverwaltung](#)“ auf Seite 381).
2. Geben Sie die maximale Anzahl an Tagen und Stunden für die gesamte Aufzeichnungszeit an.
3. Aktivieren Sie **Alarm-VoIP-Aufzeichnung**.
4. Geben Sie die maximale Anzahl an Tagen und Stunden für die gesamte Aufzeichnungszeit an.
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Qognify Video Analytics

Da mit der steigenden Anzahl zu beobachtender Monitore gleichzeitig die Aufmerksamkeit des Personals sinkt, haben Sie die Möglichkeit, eine intelligente Videoanalyse innerhalb der Qognify-Software durchzuführen. Durch eine intelligente Videoanalyse wird das Wachpersonal entlastet und somit die Überwachungsqualität erheblich gesteigert.

Im Abschnitt „SeeTec Video Analytics“ wird die Konfiguration von Folgendem beschrieben:

- Generischer VCA-Kanal (siehe „[Generischer VCA-Kanal](#)“ auf der nächsten Seite)

- Kennzeichenerkennung (siehe „[Kennzeichenerkennung](#)“ auf Seite 318)
- LPR VCA (siehe „[LPR VCA - Kennzeichenerkennung](#)“ auf Seite 322)
- Qognify Analytics (obsolet, wird nicht mehr verteilt) (siehe „[Qognify Analytics](#)“ auf Seite 327)
- Qognify Analytics Server (siehe „[Qognify Analytics Server](#)“ auf Seite 335)

Die Videoanalyse-Module sollten aus Performancegründen auf einem dedizierten Server installiert werden (siehe „[Angepasste Installation](#)“ auf Seite 41).

Generischer VCA-Kanal

Das Modul „Generischer VCA-(Video Content Analytics)-Kanal“ dient der Einbindung von APIs von Drittherstellern über die Qognify Programmschnittstelle (QAI). Dabei liefert die Schnittstelle Bilddaten an Qognify VMS und erhält Ereignisse zurück, um beispielsweise einen Alarm auszulösen.

Um ein Modul vom Typ „Generischer VCA-Kanal“ zu konfigurieren, muss es zunächst im Qognify VA Administrationstool angelegt werden (siehe „[Qognify VMS VA Administrationstool](#)“ auf Seite 513).

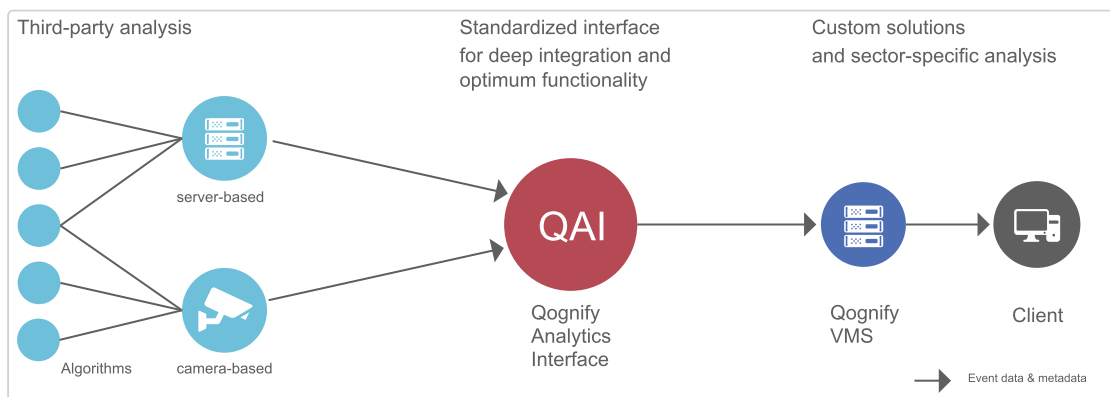


Abb. 159: Generischer VCA-Kanal

Die QAI (Qognify Analytics Interface) bietet die folgenden Plugins:

- **IPS/Axis:** für Kameras mit integrierter Bildanalyse; es werden Metadaten ausgelöst (Trackingdaten können in Qognify VMS visualisiert werden)
- **IVA/Bosch:** für Bosch-Kameras mit integrierter Bildanalyse
- **CogVis:** serverbasierte Bildanalyse
- **Traficon Flir:** Flir-Kameras mit integrierter Bildanalyse. Das Traficon-Plugin dient zur Verkehrsanalyse.
- **SafeZoneEdge** (kompatibel mit ACAP-Version 1.0.4521)
- **AxisPerimeterDefender** (kompatibel mit ACAP Axis Perimeter Defender-Version 2.7.2).

Um beim Starten von der Software korrekt erkannt zu werden, muss die API im Unterverzeichnis „\VersatileApplications\VCAPLugin“ im Installationsverzeichnis von Qognify abgelegt werden.

Allgemein

General

Activated

General

Name: CogVIS

Video analysis module: QAI CogVis Count

Camera: AXIS P1354

Video classification: Analytics

Frame rate for analysis (fps): 8

Authentication

Use authentication Use module settings for authentication

User name:

Password:

External service

Abb. 160: Generischer VCA-Kanal - Allgemein

1. Aktivieren Sie das Modul und passen Sie gegebenenfalls den **Namen** an.
2. Wählen Sie das **Videoanalyse-Modul** aus.
3. Wählen Sie die geeignete **Kamera** aus.
4. Wählen Sie die geeignete **Videoklassifikation** aus. Die Videoklassifikation bestimmt, welcher Videostream im Überwachungsmodus für die verschiedenen Modi (Normal, Ausgewählt, Alarm) verwendet wird.
5. Geben Sie die **Bildrate für Analyse (fps)** ein. Wird eine andere Bildrate als die in der ausgewählten Videoklassifikation konfigurierten verwendet, wirkt sich dies nur auf MJPG-basierte Videostreams aus.
6. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
7. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Informationen zum Konfigurieren von Drittanbieter-Analysesystemen finden Sie im Dokument „[Technical_Guides_Qognify_Qognify VMS_7.4_DE.pdf](#)“ oder wenden Sie sich an den Support (siehe „[Support](#)“ auf Seite 13).

Kennzeichenerkennung

Das Qognify LPR-Modul (License Plate Recognition, Kennzeichenerkennung) ist ein Zusatzmodul für Qognify VMS zur automatischen Erkennung von Kennzeichen im ruhenden oder fließenden Verkehr. Es kann internationale Kennzeichenformate, sogar mit arabischen und kyrillischen Schriftzeichen, in bis zu acht Fahrspuren pro Server auslesen.

Das Modul wird vollständig im Qognify VMS-Client konfiguriert und die Erkennung der Kennzeichen erfolgt entweder kontinuierlich oder triggergesteuert. Das LPR-Modul kann mit allen von Qognify VMS unterstützten IP-Kameras verwendet werden und wird in das System eingebunden. Für eine optimale Erkennung selbst bei schwierigen Lichtverhältnissen sollten spezielle LPR-Kameras (IP-Kameras oder Analogkameras über Video-Encoder) verwendet werden.

Alle LPR-bezogenen Ereignisse, wie Kennzeichen aus einer bestimmten Liste, unbekanntes Kennzeichen, Kennzeichen in der falschen Fahrspur usw., können zur Auslösung eines Alarms verwendet werden.

Um ein LPR-Modul zu konfigurieren, muss es zunächst im Qognify VMS VA Administrationstool angelegt werden (siehe „[Qognify VMS VA Administrationstool](#)“ auf Seite 513).

Fahrspurkonfiguration

Lane configuration

General

Activated

Name:

LPR module:

Camera:

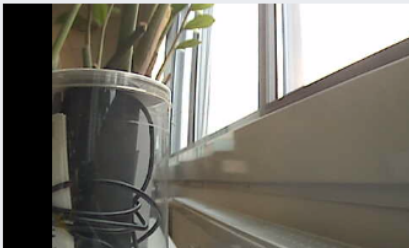
Video classification:

Role:

Frame rate for recognition (fps):

Delete LPR events after (number of days):

Area of interest



LPR archive

Assigned layer:

Assigned cameras:

- AXIS P5532-E
- AXIS Q1635
- Axis TestCam
- h.264
- multi
- Sony

Event-based recognition

Pre-delay (s):

Post-delay (s):

Continuous LPR

Time between same license plates (s):

Number of frames required:

Abb. 161: Fahrspurkonfiguration

1. Aktivieren Sie das Modul und passen Sie gegebenenfalls den **Namen** an.
2. Wählen Sie das geeignete **LPR-Modul** aus.
3. Wählen Sie die geeignete **Kamera** aus.
4. Wählen Sie die geeignete **Videoklassifikation** aus. Die Videoklassifikation bestimmt, welches Videoprofil im Überwachungsmodus für die verschiedenen Modi (Normal, Ausgewählt, Alarm) verwendet wird. Bei MPEG-4-, H.264- oder H.265-Streaming muss die Bildrate für die Erkennung der Bildrate für die Standardaufzeichnung der ausgewählten Kamera entsprechen, bei Motion JPEG kann ein beliebiger Wert eingetragen werden.
5. Wählen Sie die gewünschte **Rolle** aus. Im LPR-Modus können Sie dadurch z. B. die Suche auf alle Einfahrten begrenzen und müssen nicht jede Einfahrt-Fahrspur manuell auswählen.

6. Geben Sie die **Bildrate für Erkennung** an, um die Anzahl der Bilder pro Sekunde festzulegen, die an das Modul übertragen werden sollen. Bei MPEG-4/H.264-Streaming muss die Bildrate für die Erkennung der Bildrate für die Standardaufzeichnung der ausgewählten Kamera entsprechen, bei Motion JPEG kann ein beliebiger Wert eingetragen werden.
7. Legen Sie fest, nach wie vielen Tagen aufgetretene LPR-Ereignisse (erkannte Kennzeichen, Änderungen an den Stammdaten usw.) gelöscht werden sollen.
8. Wählen Sie die **Zugeordneten Kameras** und **Zugeordneten Ansichten** aus, die zusätzlich zur Kamera im LPR-Modus angezeigt werden sollen.
9. Wählen Sie **Ereignisgesteuerte Erkennung** oder **Ständige Erkennung**. Bei der ereignisgesteuerten Erkennung wird mit der Kennzeichenerkennung erst nach einem Ereignis begonnen, wenn z. B. ein Fahrzeug durch eine Lichtschranke fährt. Die ereignisgesteuerte Erkennung wird beispielsweise durch ein Alarmszenario ausgelöst.

Aus Leistungsgründen wird die Verwendung der ereignisgesteuerten Erkennung dringend empfohlen.

10. Geben Sie für die ereignisgesteuerte Erkennung die **Vorlaufzeit** und die **Nachlaufzeit** in Sekunden an. Dieser Zeitraum wird für die Erkennung des Kennzeichens verwendet, d. h., die Bilder dieses Zeitraums werden an die OCR-Erkennung weitergeleitet.
11. Aktivieren Sie **Beim nächsten Auslöseereignis exportieren**. Sobald diese Funktion aktiviert ist, werden beim nächsten Auslöseereignis die Bilder gemäß der Parameter Vorlaufzeit, Nachlaufzeit und Bildrate gleichzeitig sowohl an das LPR-Modul zur Kennzeichenerkennung geschickt, als auch im Verzeichnis „VersatileApplications“ abgelegt.

Beispiel Bildrate: 2 fps

Vorlaufzeit: 1s

Nachlaufzeit: 2s

*Beim nächsten Auslöseereignis werden sechs Bilder im Verzeichnis „VersatileApplications“ abgelegt (Vorlauf+Nachlauf * 2 fps).*

Diese Einstellung gilt nur für das kommende Ereignis und dient zur Kontrolle der eingestellten Parameter. Sie gilt nur für ein Ereignis und wird nach dem Export wieder deaktiviert.

12. Geben Sie für die ständige Erkennung die **Zeit zwischen gleichen Kennzeichen** an. Damit wird festgelegt, wie lange das gleiche Kennzeichen maximal zu sehen ist.

Beispiel Kennzeichenerkennung an einer Tankstelle: Die Zeit zwischen gleichen Kennzeichen ist auf 60 Sekunden eingestellt.

Scenario 1: Wagen 1 kommt an -> Kennzeichenerkennung wird gestartet - Wagen 1 fährt ab -> 60 Sekunden starten - Wagen 1 kommt innerhalb der 60 Sekunden wieder an -> Keine Kennzeichenerkennung, da der Wagen innerhalb von 60 Sekunden wieder angekommen ist.

Scenario 2: Wagen 1 kommt an -> Kennzeichenerkennung wird gestartet - Wagen 1 fährt ab -> 60 Sekunden starten - Wagen 1 kommt nach 60 Sekunden wieder an -> Erneute Kennzeichenerkennung, da der Wagen erst nach 60 Sekunden nochmals angekommen ist.

13. Definieren Sie im Feld **Anzahl von notwendigen Frames**, bei wie vielen Bildern das Kennzeichen eindeutig erkannt werden muss.
14. Klicken Sie auf **Neue Liste anlegen**, um eine oder mehrere Kennzeichenlisten anzulegen. Wählen Sie eine Liste aus und weisen Sie ihr eine Kennzeichengruppe zu, um diese auswerten zu können.
15. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Listenkonfiguration

Mithilfe von Listen können die Kennzeichen von Fahrzeugen bequem klassifiziert werden, z. B. in „Mitarbeiter“ und „Lieferanten“ oder „ungültige Kennzeichen“. Beispielsweise kann ein Alarm ausgelöst werden, wenn ein Kennzeichen aus der Liste „ungültige Kennzeichen“ erkannt wird.

Lane 1

Activated

General

Create new list

Name: Lane 1

3rd party ID:

Role: Not assigned

Delete LPR events after (number of days): 28

Offset (ms): 0

LPR archive

Assigned layer: No assignment

Assigned cameras:

- AXIS
- Cam1
- Vivotek
- Samsung

Abb. 162: Listenkonfiguration

1. Wählen Sie eine Liste aus.
2. Aktivieren Sie die Liste und passen Sie gegebenenfalls den **Namen** an.
3. Wählen Sie die **Kennzeichengruppen** aus, die ausgewertet werden sollen (siehe „**Kennzeichengruppen**“ auf Seite 432). Im dazugehörigen Alarmszenario kann damit festgelegt werden, dass z. B. bei einem Kennzeichen aus Liste 1 ein Alarm ausgelöst wird, bei einem Kennzeichen aus Liste 2 wird automatisch eine Schranke geöffnet.
4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

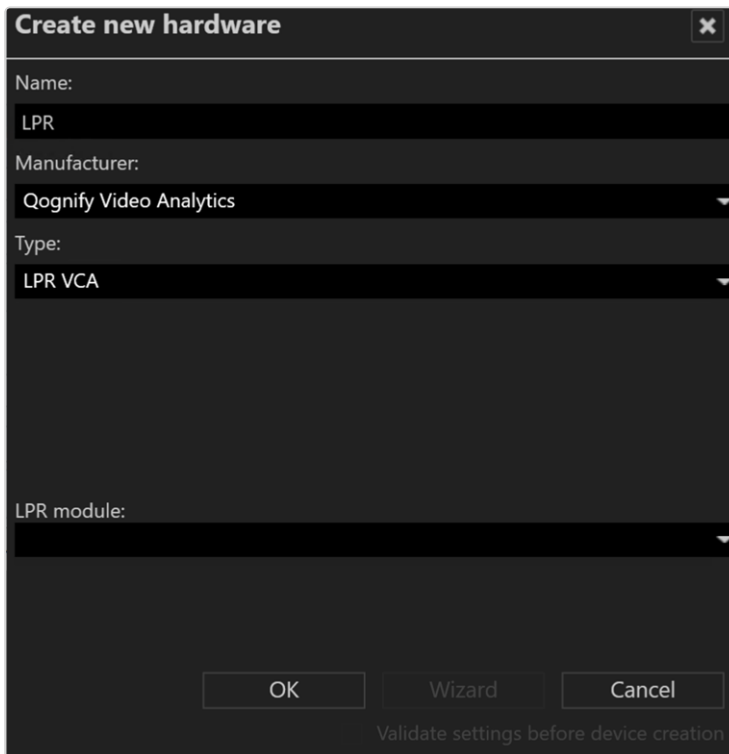
LPR VCA - Kennzeichenerkennung

Das Modul „LPR-VCA-(Video Content Analytics-)Kanal“ dient der Einbindung von APIs von LPR-Drittanbietern über die SeeTec-Programmschnittstelle (SAI). Dabei liefert die Schnittstelle Bilddaten und Ereignisse an Qognify Qognify VMS, die beispielsweise einen Alarm auslösen können.

Alle LPR-bezogenen Ereignisse, wie Kennzeichen aus einer bestimmten Liste, unbekanntes Kennzeichen, Kennzeichen in der falschen Fahrspur usw., können zur Auslösung eines Alarms verwendet werden.

Um beim Starten von der Software korrekt erkannt zu werden, müssen die API-Dateien und die signierte XML-Datei im Unterverzeichnis „\VersatileApplications\VCAPugin“ oder „\VersatileApplications64\VCAPugin“ im Installationsverzeichnis von Qognify abgelegt werden.

Neues LPR VCA-Modul hinzufügen



Create new hardware

Name:
LPR

Manufacturer:
Qognify Video Analytics

Type:
LPR VCA

LPR module:

OK Wizard Cancel

Validate settings before device creation

Abb. 163: Neue Hardware anlegen

1. Aktivieren Sie **Sonstige Hardware** und legen Sie ein neues Objekt an.
2. Geben Sie einen **Namen** ein.
3. Wählen Sie unter **Hersteller** „Qognify Video Analytics“.
4. Wählen Sie unter **Typ** „LPR VCA“.
5. Geben Sie den **Host** (IP-Adresse oder Name) des Moduls an.
6. Wählen Sie das installierte **LPR-Modul**, um den LPR VCA-Analysekanal zu spezifizieren, um die Bilddaten zu analysieren (siehe „[LPR-Modul konfigurieren](#)“ auf [Seite 446](#)).
7. Klicken Sie auf **OK**. Das neue LPR VCA-Modul ist im ausgewählten Unternehmenselement zur weiteren Konfiguration verfügbar.

Allgemeine LPR VCA-Einstellungen

General	
General	
<input checked="" type="checkbox"/> Activated	
Name:	LPR VCA
LPR module:	Analytics Interface Module 10 SCHRI-HP
Camera:	AXIS M3046-V 1.8MM
Video classification:	Analytics

Abb. 164: Allgemeine LPR VCA-Einstellungen

1. Aktivieren oder deaktivieren Sie das Modul.
2. Passen Sie gegebenenfalls den **Namen** an.
3. Wählen Sie das geeignete **LPR-Modul** aus.
4. Wählen Sie die geeignete **Kamera** aus.
5. Wählen Sie die geeignete **Videoklassifikation** aus. Die Videoklassifikation bestimmt, welches Videoprofil im Überwachungsmodus für die verschiedenen Modi (Normal, Ausgewählt, Alarm) verwendet wird. Bei MPEG-4-, H.264- oder H.265-Streaming muss die Bildrate für die Erkennung der Bildrate für die Standardaufzeichnung der ausgewählten Kamera entsprechen, bei Motion JPEG kann ein beliebiger Wert eingetragen werden.
6. Wählen Sie die Authentifikationsmethode aus und geben Sie ggf. Benutzernamen und Passwort ein.
7. Um je nach Kamerahersteller einen externen LPR-Dienst zu verwenden, aktivieren Sie **Verwende externen Dienst** und geben Sie den **Host (IP-Adresse oder Name)** und die **Port**-Nummer des Diensts an.

Abhängig vom externen Dienst biete die externe Software möglicherweise zusätzliche Parameter, die konfiguriert werden können.

8. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Fahrspurkonfiguration - Allgemein

Einige Drittanbieter-LPR-Module können mehrere Fahrspuren mit einem Kanal unterstützen (z. B. Megapixelkameras, die mehrere Spuren gleichzeitig überwachen). Daher unterstützen LPR VCA-Plugins die Zuweisung mehrerer Fahrspuren an denselben Drittanbieter-LPR-Kanal.

Lane 1

Activated

General

Create new list

Name: Lane 1

3rd party ID:

Role: Not assigned

Delete LPR events after (number of days): 28

Offset (ms): 0

LPR archive

Assigned layer: No assignment

Assigned cameras:

- AXIS
- Cam1
- Vivotek
- Samsung

Abb. 165: Fahrspurkonfiguration - Allgemein

1. Aktivieren Sie die Fahrspur und passen Sie gegebenenfalls den **Namen** an.

Für jede aktivierte Fahrspur wird eine Lizenz benötigt.

2. Klicken Sie auf **Neue Liste anlegen**, um eine oder mehrere Kennzeichenlisten anzulegen (siehe „[Fahrspurkonfiguration - Listen](#)“ auf der nächsten Seite).
3. Wählen Sie die gewünschte **Rolle** aus. Im LPR-Modus können Sie dadurch z. B. die Suche auf alle Einfahrten begrenzen und müssen nicht jede Einfahrt-Fahrspur manuell auswählen.
4. Legen Sie fest, nach **wie vielen Tagen** aufgetretene LPR-Ereignisse (erkannte Kennzeichen, Änderungen an den Stammdaten usw.) gelöscht werden sollen.
5. Legen Sie den **Offset** fest, um das Offset des Kamerasignals auszugleichen.
6. Weisen Sie im Archivmodus eine Ansicht zu, in der das LPR-Bild angezeigt werden soll.
7. Wählen Sie die LPR-Kamera aus.

Es können maximal zwei Kameras zugewiesen werden

8. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Solange das Konfigurationsfenster geöffnet ist, werden die vom Plugin vorgenommenen Änderungen nicht angezeigt. Um die Änderungen anzuzeigen, muss die Konfiguration des Moduls/der Fahrspur geschlossen und erneut geöffnet werden.

Fahrspurkonfiguration - Listen

Mithilfe von Listen können die Kennzeichen von Fahrzeugen bequem klassifiziert werden, z. B. in „Mitarbeiter“ und „Lieferanten“ oder „ungültige Kennzeichen“. Beispielsweise kann ein Alarm ausgelöst werden, wenn ein Kennzeichen aus der Liste „ungültige Kennzeichen“ erkannt wird.

The screenshot shows a configuration window titled 'Service'. At the top, there is a checkbox labeled 'Activated' which is checked. Below this, there is a 'Name:' label followed by a text input field containing the word 'Service'. Underneath, there is a 'License plate groups:' label followed by a list of items. The first item is 'Service' with an unchecked checkbox. At the bottom right of the window, there is a button labeled 'Delete list'.

Abb. 166: Fahrspurkonfiguration - Listen

1. Aktivieren Sie die Liste und passen Sie gegebenenfalls den **Namen** an.
2. Wählen Sie die **Kennzeichengruppen** aus, die ausgewertet werden sollen. Im dazugehörigen Alarmszenario kann damit festgelegt werden, dass z. B. bei einem Kennzeichen aus Liste 1 ein Alarm ausgelöst wird, bei einem Kennzeichen aus Liste 2 wird automatisch eine Schranke geöffnet.
3. Klicken Sie auf **Liste löschen**, um die ausgewählte Liste zu löschen.
4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Qognify Analytics

Das klassische Qognify Analytics ist obsolet und wird seit Qognify VMS R9 nicht mehr verteilt! Es ist nur für Migrationszwecke verfügbar. Die Funktion wird durch Qognify Analytics Server ersetzt (Details finden Sie unter [„Qognify Analytics Server“ auf Seite 335](#)).

Um eine intelligente Videoanalyse durchführen zu können, muss der Qognify-Server die Kamerabilder zum Qognify Analytics-Modul senden. Basierend auf der Analyse können Alarme ausgelöst werden.

Um ein Qognify Analytics-Modul zu konfigurieren, muss es zunächst im Qognify VA Administrationstool angelegt werden (siehe [„Qognify VMS VA Administrationstool“ auf Seite 513](#) und [„Neue Hardware anlegen“ auf Seite 296](#)). Alternativ wird es mit einer benutzerdefinierten Installation des Analytics-Modul installiert (siehe [„Server-Komponenten“ auf Seite 43](#)).

Übersicht der Qognify Analytics-Pakete

Es stehen innerhalb der Qognify-Lösung verschiedene Qognify Analytics-Pakete zur Verfügung:

- Qognify Analytics Basic
- Qognify Analytics Premium
- Qognify Analytics Enterprise

	Qognify Analytics Basic	Qognify Analytics Premium	Qognify Analytics Enterprise
Area of Interest	X	X	X
Objektklassifizierung	X	X	X
Tripwire (auch nicht-linear)	X	X	X
Multisegment-Tripwire	X		X
Dringt ein		X	X
Verlässt		X	X
Erscheint		X	X
Verschwindet		X	X
Zurückgelassen			X
Weggenommen			X

Qognify Analytics-Modul hinzufügen

1. Aktivieren Sie **Sonstige Hardware** und legen Sie ein neues Objekt an.
2. Geben Sie einen **Namen** ein.
3. Wählen Sie unter **Hersteller** „Qognify Video Analytics“.
4. Wählen Sie unter **Typ** entweder „Qognify Analytics Basic“, „Qognify Analytics Premium“ oder „Qognify Analytics Enterprise“ aus.
5. Wählen Sie das **Videoanalyse-Modul** aus, um festzulegen, welcher Videoanalyse-Kanal die Auswertung der Bilddaten durchführen soll.
6. Klicken Sie auf **OK**.

Allgemein

1. Aktivieren Sie das Modul und passen Sie gegebenenfalls den Namen an.
2. Wählen Sie das Videoanalyse-Modul aus, um festzulegen, welcher Videoanalyse-Kanal die Auswertung der Bilddaten durchführen soll.
3. Wählen Sie die Kamera für die Lieferung des analytischen Video-Streams aus.

Auf der ausgewählten Kamera darf kein Privacy-Masking verwendet werden. Qognify Analytics-Geräte können nicht kopiert werden. Falls die Kamera nach der Konfiguration verdreht wird, beendet das Videoanalyse-Modul unter Umständen die Erkennung.

4. Wählen Sie die **Videoklassifikation** aus, um festzulegen, welches Profil für die Bildübertragung zum Videoanalyse-Kanal verwendet werden soll. Diese Einstellung gilt nur für Multistreaming. Qognify empfiehlt, für die Videoanalyse einen zusätzlichen Stream von der Kamera zu verwenden. In der Regel ist eine CIF-Auflösung für die Analyse ausreichend (Kompression: 20%). Wählen Sie größere Auflösungen nur nach Rücksprache.
5. Legen Sie die **Bildrate für die Analyse** fest, um anzugeben, wie viele Bilder pro Sekunde an den Videoanalyse-Kanal übertragen werden. Qognify empfiehlt eine Bildrate von 12 Bildern pro Sekunde (fps).

6. Der **Kanalzustand** zeigt Ihnen den aktuellen Zustand des Qognify Analytics-Kanals an. Folgende Zustände sind möglich:
 - **Bekannte Szene (Good View)**: Der Qognify Analytics-Kanal läuft. Die Videodaten werden analysiert.
 - **Kein Signal (Bad Signal)**: Der Qognify Analytics-Kanal läuft. Die Videodaten werden nicht analysiert. (Mögliche Ursachen: Die Bildqualität ist zu schlecht, der Kontrast ist z. B. zu niedrig oder das Bild ist zu dunkel.) In diesem Zustand kann ein Alarmszenario gestartet werden. Als Auslöseereignis für das Alarmszenario wählen Sie die Option „Ausfall der Videoanalyse durch zu wenig Licht oder blockierte Optik“.
 - **Ungültige Szene (Invalid View)**: Unbekannter Fehler. Die Videodaten werden nicht analysiert.
 - **Unbekannte Szene (Unknown View)**: Die aktuelle Szene entspricht nicht der angelernten Szene (die Kamera wurde z. B. verdreht). Die Videodaten werden nicht analysiert. In diesem Zustand kann ein Alarmszenario gestartet werden. Als Auslöseereignis für das Alarmszenario wählen Sie die Option „Ausfall der Videoanalyse durch Verdrehung der Kamera“.
 - **Bekannte Szene suchen (Searching for View)**: Der Qognify Analytics-Kanal befindet sich in der Anlernphase. Wenn der Qognify Analytics-Kanal aktiviert ist, ändert sich der Zustand in „Bekannte Szene“, „Unbekannte Szene“ oder „Unbekannt“.
 - **Unbekannt (Unknown)**: Keine Verbindung zum Qognify Analytics-Kanal.
7. Wählen Sie die gewünschte **Verwendung** aus.
 - **Innen**. Alle Objekte in einem Raum oder Gebäude werden überwacht
 - **Innen und nur Personen**. Nur Personen in einem Raum oder Gebäude werden überwacht
 - **Außen**: Alle Objekte in Außenbereichen werden überwacht.
 - **Außen, aber keine Personen**: Alle Objekte ausgenommen Personen in Außenbereichen werden überwacht.
 - **Beliebig**. Alle der oben genannten Punkte treffen zu
8. Wählen Sie aus, ob die Analyse **Personen** oder **Fahrzeuge** erkennen soll.
9. Klicken Sie auf **Person** bzw. **Fahrzeug**, um im Kamerabild einen Bereich anzulegen, auf den die Kamera kalibriert werden soll.
10. Klicken Sie zur räumlichen Zuordnung des Fahrzeugs auf **Reifen** und definieren Sie die Position der Reifen.

11. Definieren Sie in dem angelegten Bereich die Position der Körperstellen (Kopf/Fuß) bzw. des oberen Fahrzeugpunkts (z. B. Dach).

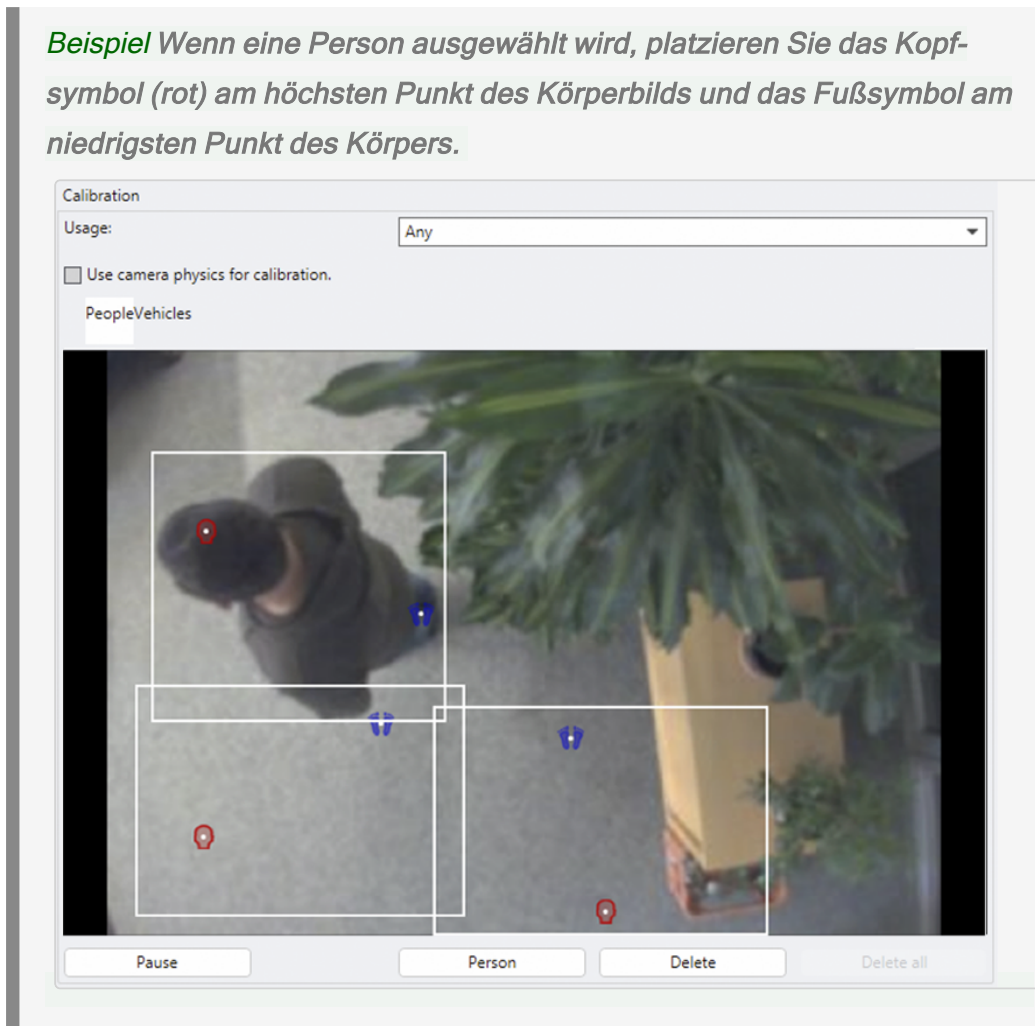


Abb. 167: Allgemein

12. Wenn ein Fahrzeug ausgewählt wird, platzieren Sie das Kreuzsymbol am höchsten Punkt (Dach) und wählen Sie mindestens ein Rad aus.

Es müssen mindestens drei Personen oder Fahrzeuge definiert werden.

13. Um einen angelegten Bereich zu löschen, markieren Sie den Bereich und klicken Sie auf **Löschen**.
14. Um alle Bereiche zu löschen, klicken Sie auf **Alle löschen**.
15. Aktivieren Sie **Neue Blickwinkel automatisch anlernen**, um die neue Position der Kamera automatisch als neue Szene zu hinterlegen. Optional können Sie auch beim Verdrehen der Kamera ein Alarmszenario starten.

16. Aktivieren Sie **Neue Blickwinkel erzwingen**, um zu verhindern, dass die Videodaten nicht analysiert werden können, weil die aktuelle Szene nicht der angelernten entspricht. Im Unterschied zu der Option Neue Blickwinkel automatisch anlernen können Sie mit der Aktivierung der Option Neue Blickwinkel erzwingen kein Alarmszenario starten.
17. Aktivieren Sie **Einzelbilder bei Alarm exportieren**, um die Bilder als JPEG separat zu speichern, auf denen eine Bewegung oder Änderung erkannt wird.
18. Legen Sie den Zeitraum fest, nach dem die exportierten Bilder gelöscht werden. Wenn Sie als Zeitraum „0“ eingeben, werden die Bilder nicht gelöscht.
19. Geben Sie optional die Generischen Parameter an, die für die Analyse der Bilder berücksichtigt werden.

Informationen zur Verwendung generischer Parameter finden Sie im Dokument „Technical_Guides_Qognify_Qognify VMS_7.4_DE.pdf“ oder wenden Sie sich an den Support (siehe „Support“ auf Seite 13).

20. Klicken Sie auf **Neue Regel hinzufügen** und geben Sie der Regel einen eindeutigen **Namen**.
21. Wählen Sie den Regel-Typ aus. Es stehen folgende Regeln zur Verfügung:
 - „**Tripwire**“ unten: Sobald der Tripwire in eine oder beide Richtungen überschritten wird, kann ein Alarm ausgelöst werden.
 - „**Area of Interest (AOI)**“ auf der nächsten Seite: Beliebige Bereiche im Kamerabild, die einen Alarm auslösen können.
 - „**Szenenwechsel**“ auf Seite 334: Es werden sämtliche Veränderungen des Sichtfeldes der Kamera erkannt, wenn sich das Kamerabild signifikant ändert.

Eine Regel ist nach der Erstellung nicht automatisch aktiviert. Aktivieren Sie die Regel während der Konfiguration der Regel (siehe unten). Für jede Regel können Sie zusätzliche Startereignisse angeben.

Tripwire

1. Aktivieren Sie das Modul und passen Sie gegebenenfalls den **Namen** an.
2. Aktivieren Sie die **Zielobjekt-Klassifizierung**, um die erkannten Objekttypen zuzuordnen. Es können mehrere Objekte ausgewählt werden.
3. Klicken Sie auf **Tripwire**, um einen Stolperdraht anzulegen, und zeichnen Sie virtuelle Stolperdrähte in das Kamerabild.

4. Klicken Sie auf **MultiSegment TW**, um MultiSegment Tripwires anzulegen. MultiSegment Tripwires können abgewinkelt angelegt werden.
5. Zeichnen Sie die virtuelle Stolperdrähte in das Kamerabild.
6. Sie erzeugen die Ecken des Stolperdrahts, indem Sie in das Kamerabild klicken und weiterzeichnen.
7. Sollten Sie einen MultiSegment Tripwire angelegt haben, schließen Sie ihn durch Doppelklick.
8. Wählen Sie die **Parameter** für die Richtungen aus, aus denen das Objekt erkannt werden soll.
9. Wählen Sie den **Filter für Minimalgröße** und den **Filter für Maximalgröße** aus, um die Größe des Objekts festzulegen, das erkannt werden soll.
10. Aktivieren Sie die Filter, mit dem das Objekt angezeigt werden soll. Die farbliche Hervorhebung erleichtert bei der Konfiguration die Erkennung von Zielobjektgrößen im Vordergrund bzw. Hintergrund.
11. Wählen Sie die zusätzlichen Filter aus:
 - **Salience**: Sich bewegende Objekte ignoriert, z. B. Spiegelungen, fallende Blätter oder Wasserbewegungen.
 - **Maximale Größenänderung (%)**: Sich schnell ändernde Objekte werden gefiltert, z. B. Schatten.

Beispiel Ein Schatten hat im ersten Bild eine Größe von angenommenen 100 %, die Größenänderung ist auf 50 % eingestellt.

Wenn der Schatten größer wird, wird er ignoriert, bis die Größenänderung 150 % übersteigt.

Wenn der Schatten kleiner wird, wird er solange ignoriert, bis die Größenänderung 50 % unterschreitet.

12. Klicken Sie auf **Diese Regel löschen**, um die aktuell angezeigte Regel zu löschen.

Area of Interest (AOI)

1. Aktivieren Sie das Modul und passen Sie gegebenenfalls den **Namen** an.
2. Aktivieren Sie die **Zielobjekt-Klassifizierung**, um die erkannten Objekttypen zuzuordnen. Es können mehrere Objekte ausgewählt werden.

3. Wählen Sie die Triggertypen, um festzulegen, bei welchem Objektverhalten das Ereignis ausgelöst werden soll.
 - **Verlässt**: Objekt verlässt den Auswertungsbereich (auch teilweise) und ist danach noch im Bild zu sehen.
 - **Dringt ein**: Objekt betritt den Auswertungsbereich (auch teilweise) und war vorher schon im Bild zu sehen.
 - **Verschwundet**: Objekt verlässt den Auswertungsbereich und ist danach nicht mehr im Bild zu sehen.
 - **Erscheint**: Objekt ist im Auswertungsbereich und war vorher nicht im Bild zu sehen.
4. Klicken Sie auf **AOI** und legen Sie den Bildbereich fest.
5. Schließen Sie den Bereich nach dem Einzeichnen durch Doppelklick.
6. Wählen Sie **Zusätzliche Parameter** für die Objekterkennung aus.
7. Geben Sie für **Herumlungern ab (s)** und **Zurückgelassen seit (s)** einen Zeitraum an, nach dem ein Signal geschickt wird, um einen Alarm auszulösen.
 - **Lungert herum**: Objekt ist längere Zeit im Auswertungsbereich (länger als X Sekunden).
 - **Zurückgelassen**: Objekt wird im Bereich länger als X Sekunden im Auswertungsbereich zurückgelassen (auch teilweise).
8. Wählen Sie die **Ebene**, um festzulegen, auf welcher Ebene sich das Objekt befindet. Dies stellt den Differenzhintergrund für die Objekterkennung dar.
9. **Bodenebene**: Die Erkennung soll auf einer horizontalen Fläche stattfinden, z. B. bei einem langen Flur. Die Bodenebene kann dabei als Teppich in dem Flur angesehen werden, den das Objekt betritt.
10. **Bildebene**: Es soll jede Bewegung erkannt werden. Eine Erkennung auf Bildebene kann am besten mit einer traditionellen Bewegungserkennung verglichen werden. Bei der Erkennung auf Bildebene findet allerdings zusätzlich eine Objektklassifizierung statt.
11. Wählen Sie in der **Ansicht** aus, ob die Erkennung in einem **Bildausschnitt** oder auf dem **ganzen Bild** ausgeführt werden soll. Die Erkennung im ganzen Bild sollte verwendet werden, wenn alle unspezifischen Bewegungen erkannt werden sollen (Person betritt oder verlässt den Kamerabereich). Da alle Bewegungen erkannt werden, ist es jedoch auch möglich, mehrere unerwünschte Alarme zu erhalten. Wenn die Erkennung auf dem ganzen Bild ausgeführt werden soll, können einige Objektverhalten nicht verwendet werden und sind daher ausgegraut.

12. Wählen Sie den **Filter für Minimalgröße** und den **Filter für Maximalgröße** aus, um die Größe des Objekts festzulegen, das erkannt werden soll.
13. Aktivieren Sie die Filter, mit denen der Bereich angezeigt werden soll. Die farbliche Hervorhebung erleichtert bei der Konfiguration die Erkennung von Zielobjektgrößen im Vordergrund bzw. Hintergrund.
14. Wählen Sie die zusätzlichen Filter aus:
 - **Saliency**: Sich bewegende Objekte werden ignoriert, z. B. Spiegelungen, fallende Blätter oder Wasserbewegungen.
 - **Maximale Größenänderung (%)**: Sich schnell ändernde Objekte werden gefiltert, z. B. Schatten.

Beispiel Ein Schatten hat im ersten Bild eine Größe von angenommenen 100 %, die Größenänderung ist auf 50 % eingestellt. Wenn der Schatten größer wird, wird er ignoriert, bis die Größenänderung 150 % übersteigt. Wenn der Schatten kleiner wird, wird er solange ignoriert, bis die Größenänderung 50 % unterschreitet.

15. Klicken Sie auf **Diese Regel löschen**, um die aktuell angezeigte Regel zu löschen.
16. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
17. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Szenenwechsel

1. Aktivieren Sie das Modul und passen Sie gegebenenfalls den **Namen** an.
2. Wählen Sie den **Szenenwechsel** aus, der ein Ereignis auslösen soll. Es werden sämtliche Veränderungen des Sichtfeldes der Kamera erkannt, wenn sich das Kamerabild signifikant ändert.
 - **Beliebige Änderung**: Kombination aller vorhandenen Möglichkeiten der Auswahl.
 - **Licht an**: Wechsel von dunkel auf hell
 - **Licht aus**: Wechsel von hell auf dunkel
 - **Licht an oder aus**: Wechsel von hell auf dunkel oder dunkel auf hell
 - **Unbekannter Vorgang**: Nicht zuordenbare Veränderung
 - **Kamerabewegung**: Kamera wird verdreht

3. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
4. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Qognify Analytics Server

Der Qognify Analytics Server bietet zwei allgemeine Varianten der Videoanalyse:

- **3D Analytics**
- **2D intelligente Bewegungserkennung**

3D Analytics

Die 3D-Videoanalyse-Funktionen des Qognify Analytics Server eignen sich zur Erkennung des Eindringens von Personen oder Fahrzeugen in so genannte sterile Zonen. Eine sterile Zone ist ein Bereich, in dem sich keine Personen oder Fahrzeuge befinden (z. B. der Bereich entlang einer Umzäunung oder ein Lagerraum während der Nacht). Der Qognify Analytics Server kann implementiert werden als (Beispiele):

- Perimeterschutz von Industriegeländen oder kritischen Infrastrukturen
- Zonenschutz von sensiblen Einrichtungen, Lagerstätten und Recyclinganlagen oder privaten Außenbereichen
- Außenhautschutz von Geschäften, Lagergebäuden, Firmengebäuden oder Privathäusern

Qognify Analytics Server kann unterscheiden zwischen

- Personen
- Fahrzeugen
- Personen und Fahrzeugen

2D intelligente Bewegungserkennung

In manchen Fällen deckt Qognify Analytics 3D nicht alle Videoanalyse-Anforderungen ab, z. B.:

- Kalibrierung ist nicht möglich (z. B. Testperson darf nicht vor der Kamera gehen).

- Kameraposition ist zu niedrig oder um die Längsachse gedreht.
- Die Kamera befindet sich in einem Innenraum - 3D Analytics funktioniert in Innenbereichen nicht besonders gut, da in den meisten Situationen zu viele Gegenstände vorhanden sind, die die Sicht behindern (Person ist nicht von Kopf bis Fuß sichtbar), oder die Person im Blickfeld zu viel Platz einnimmt.
- Der Blickwinkel ist unzureichend (d. h., die Kamera zeigt direkt auf eine Wand oder Fassade).

Architektur

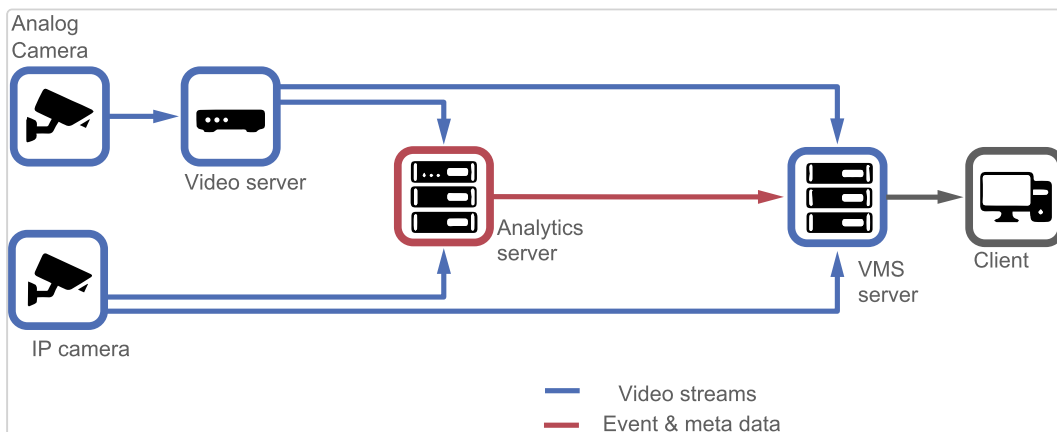


Abb. 168: Architektur von Qognify Analytics

Hinweise

- Um eine Qognify Analytics Server-Funktion hinzuzufügen und zu konfigurieren, muss das betreffende Modul zunächst im Qognify VA Administrationstool angelegt werden (siehe „[Qognify VMS VA Administrationstool](#)“ auf Seite 513). Alternativ muss es in einer benutzerdefinierten Installation installiert werden (siehe „[Angepasste Installation](#)“ auf Seite 41).
- Die Qognify Analytics-Hardware muss hinzugefügt werden (siehe „[Analytics Server-Modul hinzufügen](#)“ auf der gegenüberliegenden Seite).
- Kameraseitiges Privacy Masking kann nicht verwendet werden.
- Qognify Analytics-Geräte können nicht kopiert werden.

- Falls die Kamera nach der Konfiguration verdreht wird, beendet das Qognify Analytics Server-Modul unter Umständen die Erkennung.

Analytics Server-Modul hinzufügen

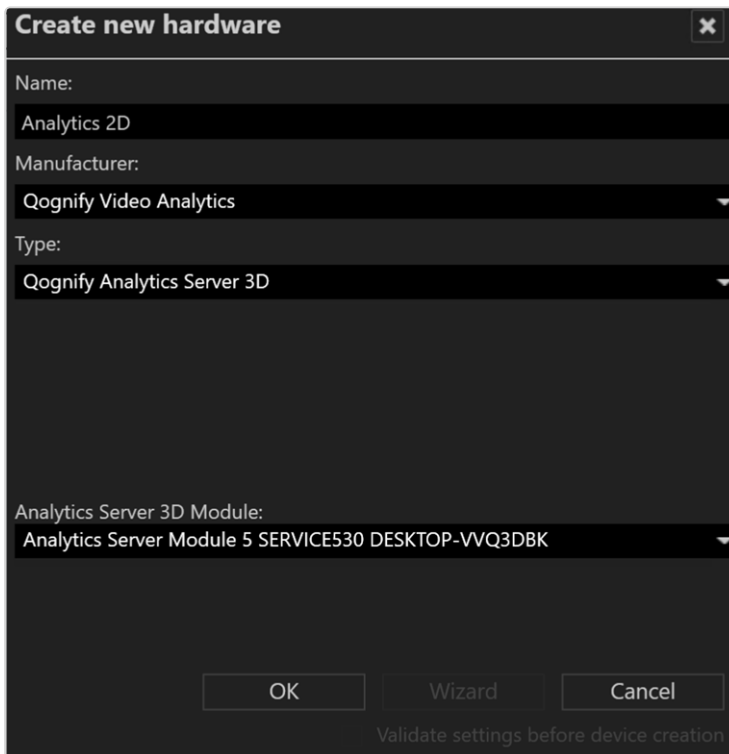


Abb. 169: Analytics Server-Modul hinzufügen

1. Aktivieren Sie **Sonstige Hardware** und legen Sie ein neues Objekt an.
2. Geben Sie einen **Namen** für das Objekt ein.
3. Wählen Sie unter **Hersteller** „Qognify Video Analytics“.
4. Wählen Sie unter **Typ** „Qognify Video Analytics Server 3D“.
5. Wählen Sie das gewünschte „Analytics Server-Modul“ für **Analytics Server 3D-Modul** aus (siehe „[Analytics Server-Modul hinzufügen](#)“ auf Seite 516).
6. Klicken Sie auf **OK**.

Informationen zur Modulkonfiguration finden Sie unter „[Qognify Analytics Server-Modul konfigurieren](#)“ auf der nächsten Seite.

Qognify Analytics Server-Modul konfigurieren

Allgemein

1. Wählen Sie das Qognify Analytics Server-Modul in der Übersicht aus.

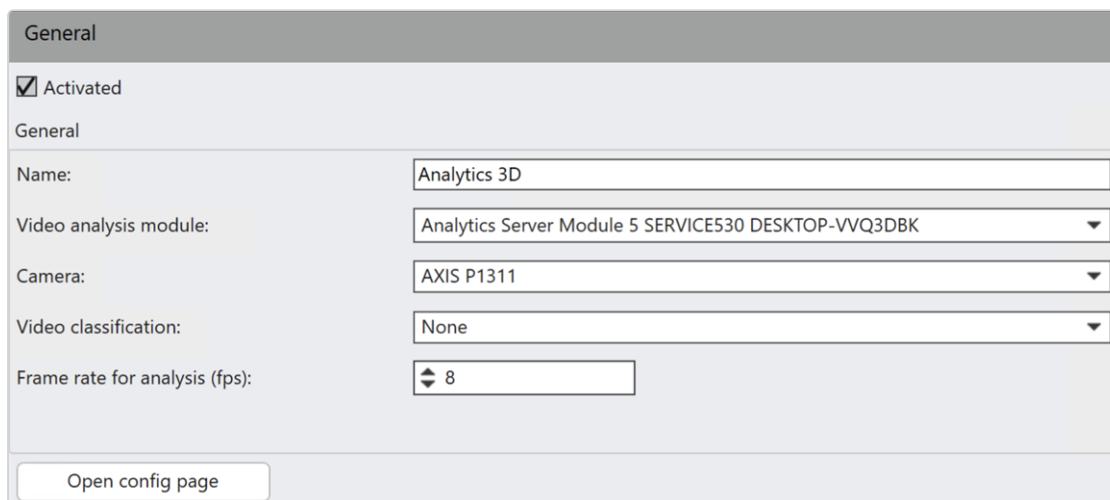


Abb. 170: Qognify Analytics Server-Modul konfigurieren

2. Aktivieren Sie das Modul und passen Sie gegebenenfalls den **Namen** an.
3. Wählen Sie das **Videoanalyse-Modul** aus, um festzulegen, welcher Videoanalyse-Kanal zur Auswertung der Bilddaten verwendet wird.
4. Wählen Sie die **Kamera** für die Bereitstellung des Videostreams aus.
5. Wählen Sie die **Videoklassifikation** aus, um festzulegen, welches Profil für die Bildübertragung zum Videoanalyse-Kanal verwendet wird. Diese Einstellung gilt nur für Multistreaming (siehe „[Videostreams](#)“ auf Seite 263).

Es wird empfohlen, für die Videoanalyse einen zusätzlichen Stream von der Kamera zu verwenden. In der Regel ist eine 4CIF-Auflösung für die Analyse ausreichend. Wählen Sie größere Auflösungen nur nach Rücksprache mit dem Qognify-Support (siehe „[Support](#)“ auf Seite 13).

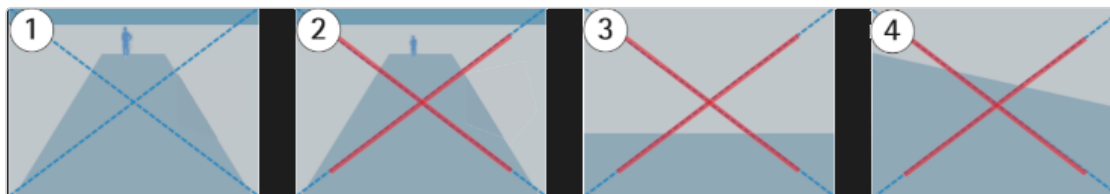


Abb. 171: Einrichtung der Szene für die Analyse

Damit die Analyse ordnungsgemäß funktioniert, müssen die folgenden Anforderungen erfüllt sein.

Die Szene sollte allgemein Abbildung 1 entsprechen:

- Die Kamera ist in einer Mindesthöhe von 2 m (Innenbereich) oder 2,5 m (Außenbereich) montiert, ausreichend geneigt und nicht um die Längsachse gedreht.
 - Der Boden in der Szene ist überwiegend flach.
 - Die Lichtverhältnisse in der Szene sind ausreichend, um menschliche Aktivität zu erkennen.
 - Der Erkennungsbereich ist eine sterile Zone (für gewöhnlich frei von bewegten Objekten).
 - Die Größe der Person beträgt über 10 % der Bildhöhe und über 7 %, wenn es sich um eine Wärmekamera handelt (ein negatives Beispiel, bei dem die Person zu klein ist, ist in Abbildung 2 dargestellt).
 - Die Mitte des Bilds liegt unter der Horizontlinie (ein negatives Beispiel, bei dem die Horizontlinie über der Bildmitte liegt, ist in Abbildung 3 dargestellt).
 - Die Kamera ist nicht oder nur geringfügig um die Längsachse gedreht (ein negatives Beispiel mit einem zu großen Rollwinkel der Kamera ist in Abbildung 4 dargestellt).
6. Legen Sie die **Bildrate für die Analyse (fps)** fest, um anzugeben, wie viele Bilder pro Sekunde an den Videoanalyse-Kanal übertragen werden.

Es wird eine Bildrate von 8 Bildern pro Sekunde (fps) empfohlen.

7. Klicken Sie auf **Konfigurationsseite öffnen**, um den Qognify Analytics-Server zu konfigurieren und Analytics-Regeln zu definieren. Wenn die Konfigurationsseite für das Modul zum ersten Mal geöffnet wird, wählen Sie den Typ der durchzuführenden Analyse aus. Folgende Typen sind verfügbar (siehe „[Qognify Analytics Server](#)“ auf Seite 335):
- 2D intelligente Bewegungserkennung
 - 3D Analytics

Vergewissern Sie sich, dass das Analytics-Setup-Tool installiert ist (siehe „[Komponenten für die angepasste Installation](#)“ auf Seite 42). Ausführliche Informationen zur Konfiguration finden Sie im entsprechenden Handbuch, das über das Hilfemenü des Setup-Tools aufgerufen werden kann.

Advantech

In diesem Abschnitt wird die Konfiguration folgender Module beschrieben:

- ADAM 6050/6050W
- ADAM 6052
- ADAM 6060/6060W/6066

Die ADAM Remote-I/O-Module sind vielseitige und zuverlässige Rechnerschnittstellen für die universelle Anwendung bei der Prozesssteuerung und -automatisierung. Die Module werden durch einen Mikroprozessor gesteuert und bieten eine einfache und zuverlässige Kommunikation sowie analoge und digitale I/O per Ethernet oder RS-485.

Allgemein

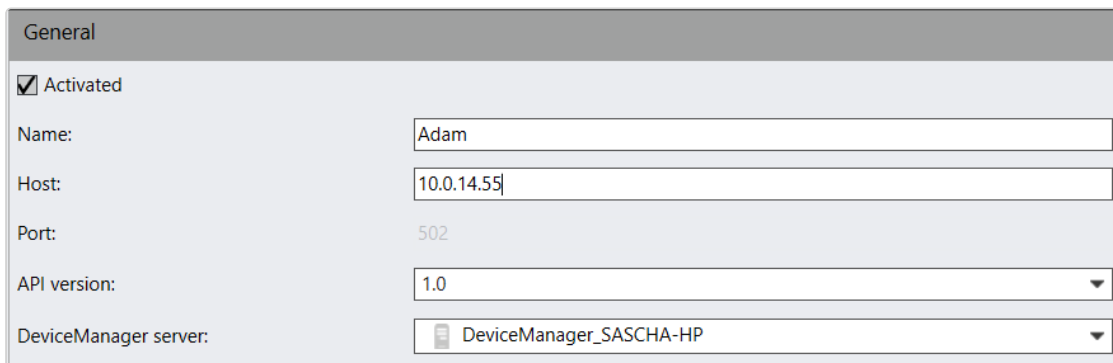
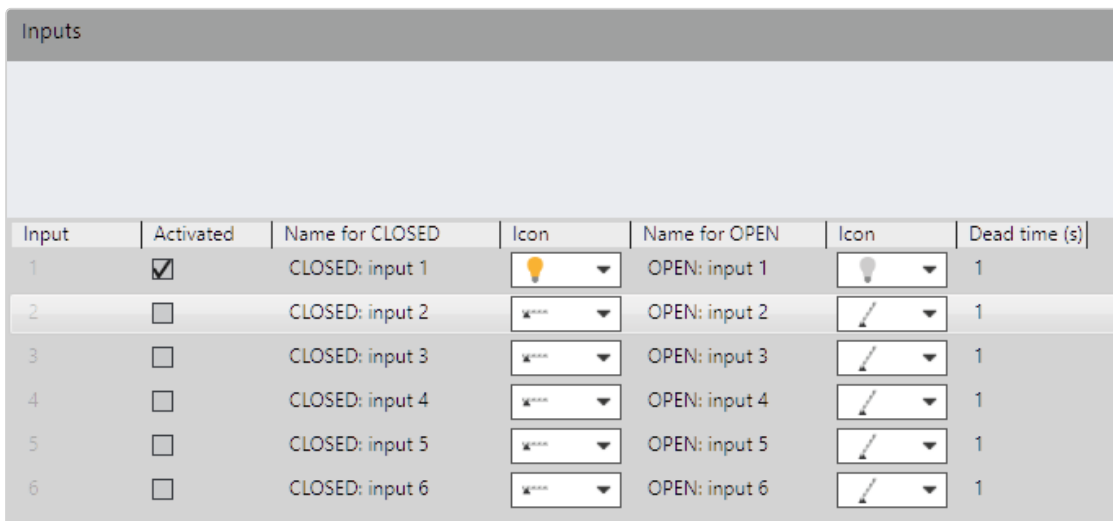


Abb. 172: Advantech Adam-Modul - Allgemein

1. Aktivieren oder deaktivieren Sie das Modul.
2. Passen Sie gegebenenfalls den Namen an.
3. Passen Sie gegebenenfalls die IP-Adresse oder den Namen des **Hosts** an.
4. Wählen Sie gegebenenfalls die geeignete **API-Version**.
5. Ändern Sie den Server zur Verwaltung des **Device Manager-Servers**.

Eingänge



Input	Activated	Name for CLOSED	Icon	Name for OPEN	Icon	Dead time (s)
1	<input checked="" type="checkbox"/>	CLOSED: input 1	💡	OPEN: input 1	💡	1
2	<input type="checkbox"/>	CLOSED: input 2	✖	OPEN: input 2	✖	1
3	<input type="checkbox"/>	CLOSED: input 3	✖	OPEN: input 3	✖	1
4	<input type="checkbox"/>	CLOSED: input 4	✖	OPEN: input 4	✖	1
5	<input type="checkbox"/>	CLOSED: input 5	✖	OPEN: input 5	✖	1
6	<input type="checkbox"/>	CLOSED: input 6	✖	OPEN: input 6	✖	1

Abb. 173: Advantech Adam - Eingänge

Die Anzahl der Eingänge hängt vom Gerätetyp ab.

1. Aktivieren Sie den gewünschten Eingang und passen Sie den **Namen für GESCHLOSSEN** an.
2. Wählen Sie das passende **Symbol** aus, um den aktuellen Status des Eingangs grafisch darzustellen. Das Symbol, das im Lageplan angezeigt wird, legen Sie im gleichnamigen Feld fest.
3. Passen Sie den **Namen für OFFEN** an.
4. Wählen Sie das passende Symbol aus, um den aktuellen Status des Eingangs grafisch darzustellen. Das Symbol, das im Lageplan angezeigt wird, legen Sie im gleichnamigen Feld fest.
5. Geben Sie das Intervall für die **Totzeit** (in Sekunden) an, nach dem wieder ein Signal ausgewertet wird.

Ausgänge

Outputs				
Output	Activated	Name for CLOSE	Name for OPEN	Hold time (s)
1	<input checked="" type="checkbox"/>	CLOSE: output 1	OPEN: output 1	4
2	<input type="checkbox"/>	CLOSE: output 2	OPEN: output 2	0
3	<input type="checkbox"/>	CLOSE: output 3	OPEN: output 3	0
4	<input type="checkbox"/>	CLOSE: output 4	OPEN: output 4	0

Abb. 174: Advantech Adam-Modul - Ausgänge

Die Anzahl der Ausgänge hängt vom Gerätetyp ab.

1. Aktivieren Sie den gewünschten Ausgang und passen Sie den **Namen für SCHLIESSEN** an.
2. Passen Sie den **Namen für OFFEN** an.
3. Geben Sie die **Haltedauer (s)** für den Zeitraum an, in dem der Ausgang geöffnet oder geschlossen wird (0 = unendlich).
4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
5. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

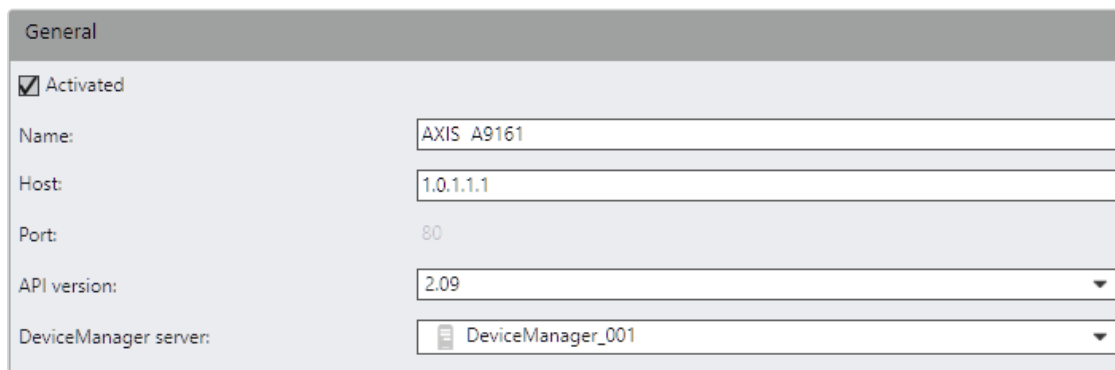
AXIS

In diesem Abschnitt wird die Konfiguration folgender Module beschrieben:

- A9161
- A9188

Die Axis Netzwerk-E/A-Relaismodule verfügen über konfigurierbare E/As mit überwachten Eingängen und einem Relais. Die Module reagieren auf Eingänge, wie Signale von PIR-Bewegungsmelder oder Schalter, und lösen Aktionen aus. Ihre offene Plattform ermöglicht eine hohe Integration mit AXIS A1001 Network Door Controller, Netzwerkkameras und andere Anlagensysteme. Sie funktionieren auch als eigenständige Module. Durch die Versorgung von E/A-Geräten mit Strom können sie die Funktionalität von Axis-Produkten erweitern, wenn zusätzliche E/As oder Relais benötigt werden.

Allgemein



General	
<input checked="" type="checkbox"/> Activated	
Name:	AXIS A9161
Host:	1.0.1.1.1
Port:	80
API version:	2.09
DeviceManager server:	DeviceManager_001

Abb. 175: AXIS - Allgemein

1. Aktivieren oder deaktivieren Sie das Modul.
2. Passen Sie gegebenenfalls den Namen an.
3. Passen Sie gegebenenfalls die IP-Adresse oder den Namen des **Hosts** an.
4. Wählen Sie gegebenenfalls die geeignete **API-Version**.
5. Ändern Sie den Server zur Verwaltung des **Device Manager-Servers**.

Eingänge













Input	Activated	Name for CLOSED	Icon	Name for OPEN	Icon	Dead time (s)
1	<input checked="" type="checkbox"/>	CLOSED: input 1		OPEN: input 1		1
2	<input type="checkbox"/>	CLOSED: input 2		OPEN: input 2		1
3	<input type="checkbox"/>	CLOSED: input 3		OPEN: input 3		1
4	<input type="checkbox"/>	CLOSED: input 4		OPEN: input 4		1
5	<input type="checkbox"/>	CLOSED: input 5		OPEN: input 5		1
6	<input type="checkbox"/>	CLOSED: input 6		OPEN: input 6		1

Abb. 176: AXIS - Eingänge

Die Anzahl der Eingänge hängt vom Gerätetyp ab.

1. Aktivieren Sie den gewünschten Eingang und passen Sie den **Namen für GESCHLOSSEN** an.
2. Wählen Sie das passende **Symbol** aus, um den aktuellen Status des Eingangs grafisch darzustellen. Das Symbol, das im Lageplan angezeigt wird, legen Sie im gleichnamigen Feld fest.
3. Passen Sie den **Namen für OFFEN** an.
4. Wählen Sie das passende Symbol aus, um den aktuellen Status des Eingangs grafisch darzustellen. Das Symbol, das im Lageplan angezeigt wird, legen Sie im gleichnamigen Feld fest.
5. Geben Sie das Intervall für die **Totzeit** (in Sekunden) an, nach dem wieder ein Signal ausgewertet wird.

Ausgänge

Outputs				
Output	Activated	Name for CLOSE	Name for OPEN	Hold time (s)
1	<input checked="" type="checkbox"/>	CLOSE: output 1	OPEN: output 1	0
2	<input type="checkbox"/>	CLOSE: output 2	OPEN: output 2	0
3	<input type="checkbox"/>	CLOSE: output 3	OPEN: output 3	0
4	<input type="checkbox"/>	CLOSE: output 4	OPEN: output 4	0
5	<input type="checkbox"/>	CLOSE: output 5	OPEN: output 5	0
6	<input type="checkbox"/>	CLOSE: output 6	OPEN: output 6	0
7	<input type="checkbox"/>	CLOSE: output 7	OPEN: output 7	0

Abb. 177: AXIS - Ausgänge

Die Anzahl der Ausgänge hängt vom Gerätetyp ab.

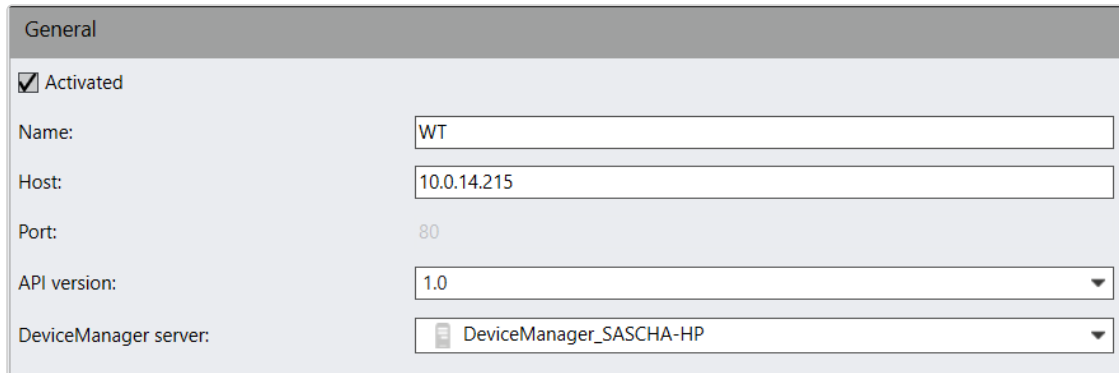
1. Aktivieren Sie den gewünschten Ausgang und passen Sie den **Namen für SCHLIESSEN** an.
2. Passen Sie den **Namen für OFFEN** an.
3. Geben Sie die **Haltedauer (s)** für den Zeitraum an, in dem der Ausgang geöffnet oder geschlossen wird (0 = unendlich).
4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
5. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

W&T

In diesem Abschnitt wird die Konfiguration des Web-IO 12x Digital Input, 12x Digital Output beschrieben.

Mit dem Web-IO Digital können Sie Schaltsignale über TCP/IP-Ethernet steuern, erfassen und überwachen. Für die Meldung von Änderungen an den Ein- und Ausgängen stehen zahlreiche Web- und Netzwerkdienste zur Verfügung. Für die Fernsteuerung über das Internet wird in der Regel nur ein Browser oder ein Smartphone benötigt.

Allgemein



General

Activated

Name:

Host:

Port:

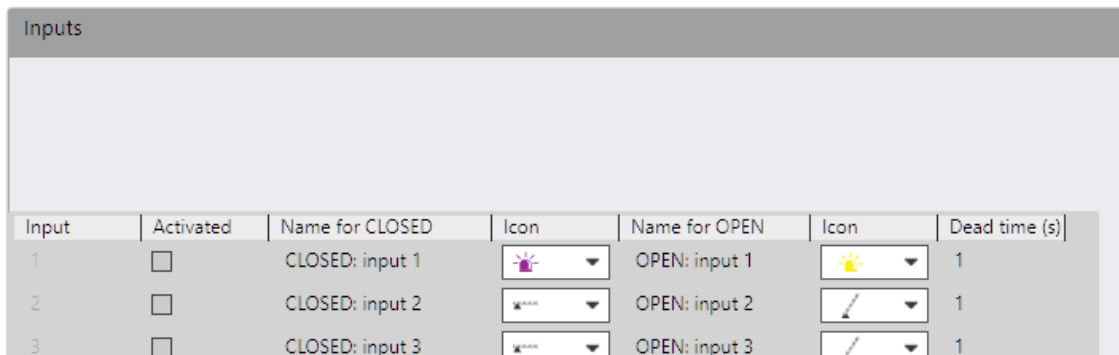
API version:

DeviceManager server:

Abb. 178: W&T - Allgemein

1. Aktivieren oder deaktivieren Sie das Modul.
2. Passen Sie gegebenenfalls den Namen an.
3. Passen Sie gegebenenfalls die IP-Adresse oder den Namen des **Hosts** an.
4. Wählen Sie gegebenenfalls die geeignete **API-Version**.
5. Ändern Sie den **Device Manager-Server**.

Eingänge









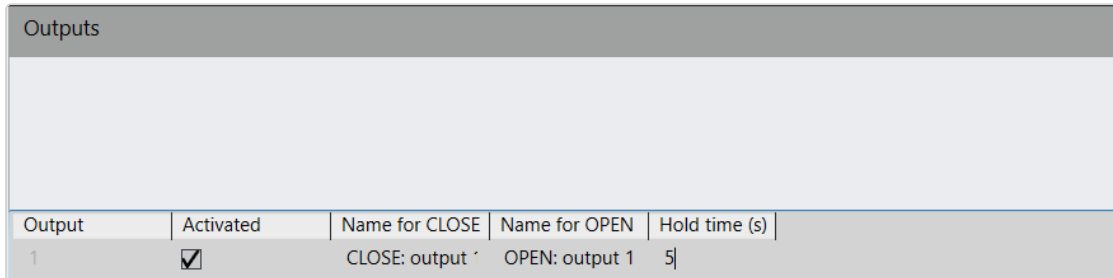
Input	Activated	Name for CLOSED	Icon	Name for OPEN	Icon	Dead time (s)
1	<input type="checkbox"/>	CLOSED: input 1		OPEN: input 1		1
2	<input type="checkbox"/>	CLOSED: input 2		OPEN: input 2		1
3	<input type="checkbox"/>	CLOSED: input 3		OPEN: input 3		1

Abb. 179: W&T - Eingänge

1. Aktivieren Sie den gewünschten Eingang und passen Sie den **Namen für GESCHLOSSEN** an.
2. Wählen Sie das passende **Symbol** aus, um den aktuellen Status des Eingangs grafisch darzustellen. Das Symbol, das im Lageplan angezeigt wird, legen Sie im gleichnamigen Feld fest.
3. Passen Sie den **Namen für OFFEN** an.
4. Wählen Sie das passende **Symbol** aus, um den aktuellen Status des Eingangs grafisch darzustellen. Das Symbol, das im Lageplan angezeigt wird, legen Sie im gleichnamigen Feld fest.

5. Geben Sie das Intervall für die **Totzeit** (in Sekunden) an, nach dem wieder ein Signal ausgewertet wird.

Ausgänge



Output	Activated	Name for CLOSE	Name for OPEN	Hold time (s)
1	<input checked="" type="checkbox"/>	CLOSE: output 1	OPEN: output 1	5

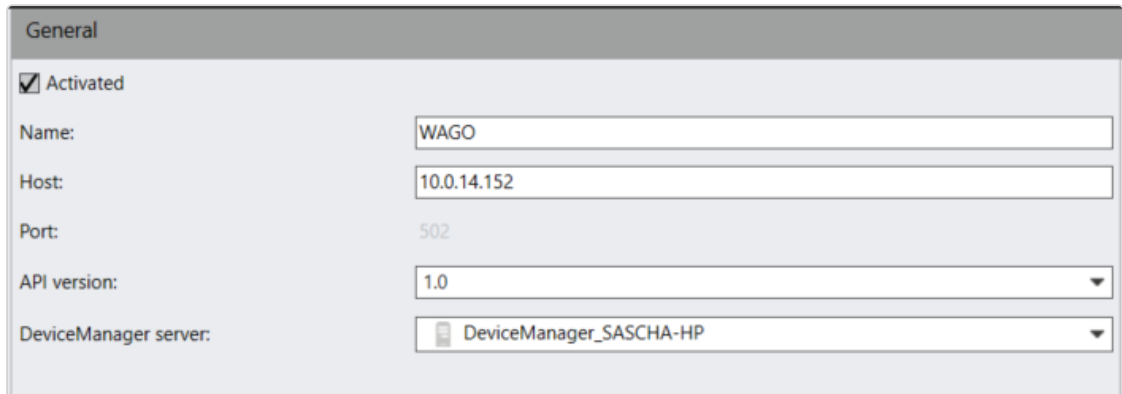
Abb. 180: W&T - Ausgänge

1. Aktivieren Sie den gewünschten Ausgang und passen Sie den **Namen für SCHLIESSEN** an.
2. Passen Sie den **Namen für OFFEN** an.
3. Geben Sie die **Haltedauer (s)** für den Zeitraum an, in dem der Ausgang geöffnet oder geschlossen wird (0 = unendlich).
4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
5. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Wago

In diesem wird die Konfiguration des Wago System 750 I/O-Moduls beschrieben. Feldbus-Koppler, Feldbus-Controller und I/O-Module des modularen WAGO I/O-SYSTEM 750 empfangen digitale und analoge Signale von Sensoren und übertragen diese an Aktoren oder übergeordnete Steuersysteme.

Allgemein



General

Activated

Name:

Host:

Port: 502

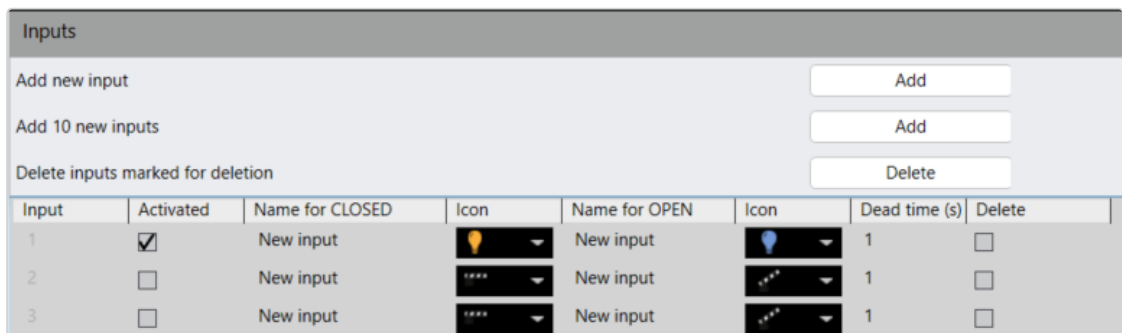
API version:

DeviceManager server:

Abb. 181: Wago - Allgemein

1. Aktivieren oder deaktivieren Sie das Modul.
2. Passen Sie gegebenenfalls den Namen an.
3. Passen Sie gegebenenfalls die IP-Adresse oder den Namen des **Hosts** an.
4. Wählen Sie gegebenenfalls die geeignete **API-Version**.
5. Wählen Sie den **Device Manager-Server** für die Kommunikation mit dem Modul aus.

Eingänge



Inputs

Add new input

Add 10 new inputs

Delete inputs marked for deletion







Input	Activated	Name for CLOSED	Icon	Name for OPEN	Icon	Dead time (s)	Delete
1	<input checked="" type="checkbox"/>	New input		New input		1	<input type="checkbox"/>
2	<input type="checkbox"/>	New input		New input		1	<input type="checkbox"/>
3	<input type="checkbox"/>	New input		New input		1	<input type="checkbox"/>

Abb. 182: Wago - Eingänge

1. Klicken Sie auf **Neuen Eingang hinzufügen** bzw. **10 neue Eingänge hinzufügen**, um einen bzw. zehn neue Eingänge anzulegen.
2. Aktivieren Sie den gewünschten Eingang und passen Sie den **Namen für GESCHLOSSEN** an.
3. Wählen Sie das passende **Symbol** aus, um den aktuellen Status des Eingangs grafisch darzustellen. Das Symbol, das im Lageplan angezeigt wird, legen Sie im gleichnamigen Feld fest.
4. Passen Sie den **Namen für OFFEN** an.

5. Wählen Sie das passende **Symbol** aus, um den aktuellen Status des Eingangs grafisch darzustellen. Das Symbol, das im Lageplan angezeigt wird, legen Sie im gleichnamigen Feld fest.
6. Geben Sie das Intervall für die **Totzeit** (in Sekunden) an, nach dem wieder ein Signal ausgewertet wird.
7. Um Einträge zu löschen, markieren Sie die zu löschenden Einträge und klicken Sie auf **Als „Löschen“ markierte Eingänge löschen**.

Ausgänge



Output	Activated	Name for CLOSE	Name for OPEN	Hold time (s)	Delete
1	<input checked="" type="checkbox"/>	New output	New output	0	<input type="checkbox"/>
2	<input type="checkbox"/>	New output	New output	0	<input type="checkbox"/>
3	<input type="checkbox"/>	New output	New output	0	<input type="checkbox"/>
4	<input type="checkbox"/>	New output	New output	0	<input type="checkbox"/>

Abb. 183: Wago - Ausgänge

1. Klicken Sie auf **Neuen Ausgang hinzufügen** bzw. **10 neue Ausgänge hinzufügen**, um einen bzw. zehn neue Ausgänge anzulegen.
2. Aktivieren Sie den gewünschten Ausgang und passen Sie den **Namen für SCHLIESSEN** an.
3. Passen Sie den **Namen für OFFEN** an.
4. Geben Sie die **Haltedauer (s)** für den Zeitraum an, in dem der Ausgang geöffnet oder geschlossen wird (0 = unendlich).
5. Um Einträge zu löschen, markieren Sie die zu löschenden Einträge und klicken Sie auf **Als „Löschen“ markierte Ausgänge löschen**.
6. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
7. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Event Interfaces

Mit der Funktion Qognify Event Interface in der Verwaltungssteuerung können Sie Sicherheitssysteme von Drittanbietern konfigurieren und verwalten, die auf einer Qognify VMS generischen Basis integriert werden können, wie z. B. Einbrecheralarme, Brandmeldezentralen, Zugangskontrollen usw. Diese Geräte können teilweise mit Hilfe der Qognify-Software verwaltet und angesteuert werden, als auch mit Hilfe der von den entsprechenden Drittherstellern bereitgestellten Software.

Nachdem die Event Interfaces oder generischen Zutrittskontrollen konfiguriert wurden, können sie mit Alarmszenarien verbunden werden (siehe „[Alarmer](#)“ auf Seite 386) und die Elemente können Lageplänen hinzugefügt werden (siehe „[Lagepläne](#) und „[Erweiterte Lagepläne](#)“ auf Seite 407).

Für die Event Interfaces sind bestimmte Plugin-Dateien erforderlich, die in die Qognify-VA-Plugin-Verzeichnisse kopiert werden müssen („C:\Programme\Qognify\VersatileApplications64\AccessControlPlugins“ oder „C:\Programme\Qognify\VersatileApplications64\EventPlugins“). Weitere Informationen finden Sie in den technischen Anleitungen oder fragen Sie den Qognify-Support nach der Verwendung von ereignisbasierten Plug-Ins von Drittanbietern.

Um eine Ereignisschnittstelle oder ein generisches Zugriffskontrollmodul zu konfigurieren, muss es im Qognify VA Administrationstool angelegt werden (siehe „[Qognify VMS VA Administrationstool](#)“ auf Seite 513).

Für die generische Qognify-Zutrittskontrolle muss mindestens eines der folgenden Zutrittskontrollmodule installiert werden:

- Continental CardAccess3000Paxton Net2
- Lenel

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Event Interfaces** in der Steuerleiste.

Nicht verfügbare Elemente in den Interfaces werden nicht gelöscht, sondern ausgeblendet. So kann ohne erneute Konfiguration jederzeit auf sie zugegriffen werden.

Event Interface anlegen

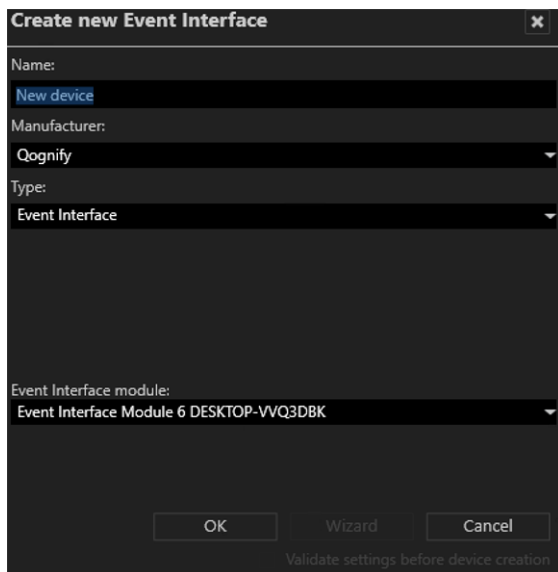


Abb. 184: Event Interface anlegen

1. Legen Sie eine neue **Event Interface** an.
2. Geben Sie den **Namen** für die neue Event Interface ein.
3. Wählen Sie den **Hersteller** aus.
4. Wählen Sie den **Typ** der Event Interface aus.
5. Wählen Sie das installierte **Event Interface-Modul** aus.
6. Klicken Sie auf **OK**. Die neue Event Interface ist im ausgewählten Steuerelement Unternehmen verfügbar.

Generische Zutrittskontrolle erstellen

1. Erstellen Sie ein neues **Event Interface**-Element.

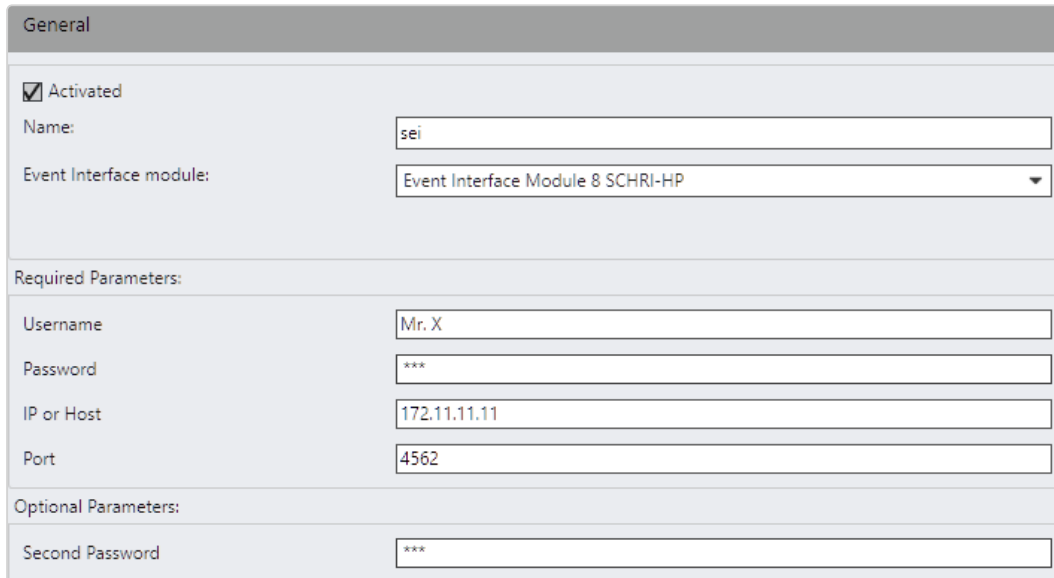


Abb. 185: Generische Zutrittskontrolle erstellen

2. Geben Sie den **Namen** für die neue generische Zutrittskontrolle ein.
3. Wählen Sie den **Hersteller** aus.
4. Wählen Sie unter **Typ** „Generische Zutrittskontrolle“.
5. Geben Sie den **Host** (IP-Adresse oder Name) des Moduls an.
6. Wählen Sie das installierte **Zutrittskontrollmodul** (siehe „[Generisches Zutrittskontrollmodul hinzufügen](#)“ auf Seite 524).
7. Wählen Sie **OK**. Die neue Zutrittskontrolle ist im ausgewählten Unternehmenselement verfügbar.

Event Interfaces konfigurieren

Allgemein



General	
<input checked="" type="checkbox"/> Activated	
Name:	sei
Event Interface module:	Event Interface Module 8 SCHRI-HP
Required Parameters:	
Username	Mr. X
Password	***
IP or Host	172.11.11.11
Port	4562
Optional Parameters:	
Second Password	***

Abb. 186: Event Interface-Einstellungen - Allgemein

1. Wählen Sie die Event Interface in der **Event Interface**-Übersicht aus.
2. **Aktivieren** Sie die Event Interface.
3. Bearbeiten Sie den **Namen**.
4. Wählen Sie das **Event Interface-Modul** aus.
5. Geben Sie die erforderlichen und optionalen Parameter an, die vom Plugin benötigt werden:
 - **Benutzername** und **Passwort** für das Zutrittskontrollmodul
 - **Port-Nummer** und die **IP-Adresse** des Moduls
 - **Zweites Passwort** für den Zugriff auf das Modul
6. Wählen Sie **OK**.

Elemente

Abhängig vom Plugin stellt die Event Interface verschiedene Objekte bereit, wie die Zustände der Bereiche eines Alarmsystems oder die Ereignisse von einem Drittanbieter-Videoanalyse-System. Die verfügbaren Objekte können in Alarmen (siehe „[Alarme](#)“ auf Seite 386) oder Lageplänen (siehe „[Lagepläne](#) und „[Erweiterte Lagepläne](#)““ auf Seite 407) verwendet werden.

Name	Type	Icon	Apply icon to	Enabled	Error
Area #010000	Area		Area	<input checked="" type="checkbox"/>	
Area state 1	State		State	<input type="checkbox"/>	
Area state 2	State		State	<input type="checkbox"/>	
Zone #010100	Zone		Zone	<input checked="" type="checkbox"/>	
Zone state 1	State		State	<input type="checkbox"/>	
Zone state 2	State		State	<input type="checkbox"/>	
Door #010101	Door		Door	<input checked="" type="checkbox"/>	
Offline	State		State	<input type="checkbox"/>	
Opened	State		State	<input type="checkbox"/>	
Opened too long	State		State	<input type="checkbox"/>	

Abb. 187: Event Interface-Elemente

Elemente suchen

1. Geben Sie im Feld **Suche** eine Zeichenfolge ein. Die zutreffenden Elemente werden aufgelistet und die Zeichenfolge wird im Elementnamen hervorgehoben.

Symbol wechseln

1. Klicken Sie auf das angezeigte Symbol.
2. Wählen Sie ein anderes aus. Wenn Sie ein Symbol verwenden möchten, das mehrere Zustände unterstützt, lesen Sie Abschnitt [„Symbole für mehrere Zustände anlegen“](#) auf Seite 356.
3. Klicken Sie auf die Schaltfläche „Für Element übernehmen“.

Element aktivieren oder deaktivieren

1. Klicken Sie auf das Kontrollkästchen **Aktiviert**. Der Zustand ändert sich entsprechend.

Regeln

Um verschiedene Ereigniszustände zu gruppieren, können die einzelnen Ereignisse oder Zustände in einer sogenannten „Regel“ zusammengefasst werden. Dies vereinfacht die Verwaltung von mehreren Ereignissen oder Zuständen. Die Regel wird ausgelöst, wenn ein Ereignis oder ein Zustand in ihr geändert oder ausgelöst wird.

Die Regeln können zu einem Alarmszenario hinzugefügt werden (siehe „[Start](#)“ auf [Seite 393](#)).

Name	Type	Selected
emergency	State	<input type="checkbox"/>
Tampered	State	<input type="checkbox"/>
Alarmed	State	<input checked="" type="checkbox"/>
Doorbell rings	Event	<input checked="" type="checkbox"/>
Someone knocks	Event	<input type="checkbox"/>
Door #020102	Door	
Zone #020200	Zone	

Rule name	Selected
TestRule	<input type="checkbox"/>

Abb. 188: Event Interface-Einstellungen - Regeln

Eine Regel erstellen

1. Wählen Sie Ereignisse oder Zustände aus der Ereignisliste aus. Suchen Sie bei Bedarf nach dem Ereignis oder verringern Sie die Anzahl der angezeigten Elemente, indem Sie die Liste einklappen.
2. Benennen Sie die Regel und wählen Sie **Regel erstellen**. Die neue Regel wird in der Regelliste angezeigt.
3. Wiederholen Sie dies für mehrere Regeln.

Regeln dürfen nicht identisch benannt werden.

Löschen einer Regel

1. Wählen Sie eine Regel in der Regelliste aus oder suchen Sie nach der Regel.

2. Wählen Sie **Löschen**.
3. Um alle Regeln in der Liste zu löschen, wählen Sie **Alle löschen**.

Nicht verfügbare Elemente

In diesem Tab werden die Elemente angezeigt, die derzeit deaktiviert, d. h. ausgeblendet sind, und ohne Konfiguration aktiviert werden können. Die nicht verfügbaren Elemente werden im Steuerelement angezeigt und sind mit einem roten Kreuz markiert.

Name	Type	Icon	Apply icon to	Enabled	Error
Area #010000	Area		Area	<input checked="" type="checkbox"/>	
Area state 1	State		State	<input type="checkbox"/>	
Area state 2	State		State	<input type="checkbox"/>	
Zone #010100	Zone		Zone	<input checked="" type="checkbox"/>	
Zone state 1	State		State	<input type="checkbox"/>	
Zone state 2	State		State	<input type="checkbox"/>	
Door #010101	Door		Door	<input checked="" type="checkbox"/>	
Offline	State		State	<input type="checkbox"/>	
Opened	State		State	<input type="checkbox"/>	
Opened too long	State		State	<input type="checkbox"/>	

Abb. 189: Event Interface - nicht verfügbare Elemente

Element aktivieren

1. Wählen Sie das Element aus oder geben Sie den Namen des Elements in das Suchfeld oberhalb der Liste ein.
2. Öffnen Sie das Element, indem Sie darauf doppelklicken.
3. Wählen Sie **Aktiviert** aus (siehe „Allgemein“ auf Seite 352).

Element löschen

1. Wählen Sie das Element aus und klicken Sie auf **Löschen**.
2. Bestätigen Sie den Löschvorgang mit **Ja**. Das Element wird endgültig gelöscht.

Symbole für mehrere Zustände anlegen

Event Interfaces in Qognify VMS unterstützen Symbole, die bis zu vier verschiedene Zustände eines einzelnen Ereignisses anzeigen können. Die Symbolzustände werden als transparente Einblendungen über den ursprünglichen Symbolen auf einem Lageplan dargestellt. So können für das Symbol eines einzelnen Ereignisses verschiedene Zustände wie geschlossen/offen angezeigt werden.

Die Symbole werden in Qognify VMS nicht bereitgestellt, sondern müssen angelegt werden. Dabei sind folgende Anforderungen zu beachten:

- Der Hintergrund ist transparent, sodass er das ursprüngliche Symbol darunter nicht verdeckt.
- Das Symbol hat eine feste Größe von 64 x 64 px.
- Das Bildformat ist PNG.
- Jeder Zustand bedeckt nur ein Viertel des ursprünglichen Symbols.
- Jeder Zustand ist auf den entsprechenden Quadranten beschränkt, z. B. wird der Alarmzustand nur in Quadrant 1 angezeigt und der Rest des Symbols ist transparent.



Event Interfaces löschen

1. Wählen Sie die Event Interface (oder generische Zutrittskontrolle) in der **Event Interface-Übersicht** aus.
2. Klicken Sie auf **Objekt löschen**.

Benutzer

Mit der Funktion **Benutzer** im Steuerelement **Administration** können Sie neue Benutzerprofile anlegen und löschen. Darüber hinaus können Sie die Anbindung an eine vorhandene Active Directory®-Benutzerverwaltung konfigurieren. Abhängig davon, ob sich ein Benutzer mit seinem Benutzernamen oder als Gruppe angemeldet hat, erhält er die entsprechenden Berechtigungen und Profile zugewiesen.

Eine allgemeine Beschreibung der administrativen Rechte und Benutzerrechte finden Sie unter „[Administrative Rechte und Benutzerrechte](#)“ auf Seite 24.

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements **Benutzer** angezeigt.
2. Wählen Sie **Benutzer** im Steuerelement Administration.

Benutzer anlegen

1. Wählen Sie im Steuerelement **Benutzer** die Option **Objekt neu anlegen** aus.
Zwei Optionen stehen zur Verfügung:
 - Basisbenutzer erstellen: Erstellt einen neuen Benutzer mit Benutzerrechten, die in Qognify VMS konfiguriert werden.
 - Active Directory-Benutzer erstellen: Wenn ein Active Directory-(AD-)Server installiert ist, werden der Benutzer und seine Gruppenzugehörigkeit mit dem Konto des Benutzers in Qognify VMS verknüpft.

Basisbenutzer erstellen

1. Wählen Sie **Basisbenutzer erstellen**.
2. Geben Sie den **Namen** und das **Passwort** des neuen Benutzers ein.
3. Bestätigen Sie den Namen mit **OK**. Der neue Benutzer wird im Steuerelement angezeigt.

Active Directory-Benutzer erstellen

1. Wählen Sie den **Objekttyp** „Benutzer“ aus.
2. Öffnen Sie den **Suchpfad** zum AD-Server.

3. Geben Sie den Benutzernamen ein. Das entsprechende Benutzerkonto wird angezeigt.
4. Um anhand des Namens nach dem Benutzer zu suchen, wählen Sie **Namen prüfen**.
5. Klicken Sie auf **OK**.

Benutzer konfigurieren

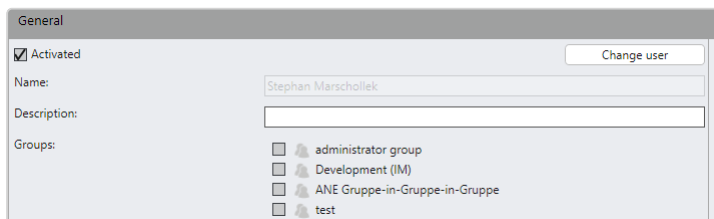
1. Wählen Sie den Benutzer im Steuerelement **Benutzer** aus.

AD-Benutzer synchronisieren

Die Namen von Active Directory-Benutzern müssen mit dem AD-Server synchronisiert werden, da die Namen in Qognify VMS nicht bearbeitet werden können.

1. Wählen Sie im Steuerelement Benutzer **Neu laden**  aus.

Allgemein



General

Activated Change user

Name:

Description:

Groups:

- administrator group
- Development (IM)
- ANE Gruppe-in-Gruppe-in-Gruppe
- test

Abb. 190: Benutzer - Allgemein

1. **Aktivierung** des Benutzers.

Der Administrator kann nicht deaktiviert werden.

2. Wenn Sie den Namen des Active Directory-Benutzers ändern möchten, wählen Sie **Gruppe ändern** aus und ändern Sie den Benutzernamen im Dialog.
3. Geben Sie eine **Beschreibung** des Benutzer-Accounts ein. Dies kann beispielsweise der Name des Benutzers sein.

4. Aktivieren Sie die **Gruppen**, zu denen der Benutzer-Account gehören soll (siehe „[Gruppen](#)“ auf Seite 367). Die Zugehörigkeit zu einer Gruppe ist optional.

Passwort

Passwort

User must use a secure password

User may change own password

User must change password regularly

Validity: Days

Last changed: 9/22/2016 10:49:36 AM

Change user password

New user password:

Enter new user password again:

User needs two passwords

New second user password:

Enter the new second user password again:

Abb. 191: Benutzer - Passwort

1. Aktivieren Sie **Benutzer muss ein sicheres Passwort verwenden**. Falls das Passwort nicht den Sicherheitsanforderungen (siehe unten) genügt, erhalten Sie eine entsprechende Meldung.
2. Aktivieren Sie **Benutzer darf eigenes Passwort ändern**, um dem Benutzer selbst die Änderung seines Passworts zu erlauben.
3. Aktivieren Sie **Benutzer muss Passwort regelmäßig ändern** und geben Sie die **Gültigkeitsdauer** des Passworts an. Vor Ablauf der Frist wird der Benutzer gebeten, sein Passwort zu ändern, um sich weiterhin anmelden zu dürfen.

4. Aktivieren Sie **Benutzerpasswort ändern** und geben Sie ein neues Benutzerpasswort ein.

Benutzerpasswörter von AD-Konten können in Qognify VMS nicht geändert werden.

Falls Sie die Option „Benutzer muss ein sicheres Passwort verwenden“ aktiviert haben, wählen Sie ein Passwort, das mindestens acht Zeichen, davon mindestens eine Ziffer, einen Groß- und einen Kleinbuchstaben, enthält.

5. Geben Sie das eingegebene Benutzerpasswort erneut ein.
6. Um ein zweites Passwort nach dem „Vier-Augen-Prinzip“ anzulegen, aktivieren Sie **Benutzer braucht zwei Passwörter** und geben Sie ein weiteres Passwort an, das denselben Sicherheitsregeln genügen muss.
7. Geben Sie das zweite Passwort erneut ein.

Wenn Sie das Administratorpasswort vergessen und der Administratorgruppe keine Benutzer zugewiesen haben (siehe „[Gruppen](#)“ auf Seite 367), ist es nicht mehr möglich, auf den Zugangs-konfigurationsmodus zuzugreifen.

Rechte-Optionen

Rights options

Consider, that also group restrictions will be applied if applicable.

Limit archive access

Days: Hours: Minutes:

Extend on non-operating days

Restrict operating hours

Allow current day

Use secure password for exports

A comment is required to change to archive mode

Show recording button

Abb. 192: Benutzer - Rechte-Optionen

1. Aktivieren Sie **Archivzugriff beschränken** und geben Sie die Dauer der Zugriffszeit (in Minuten) an, um für den Benutzer den fortlaufenden Zugriff auf das Archiv zu beschränken.

2. Bestimmen Sie die Anzahl an Tagen, Stunden und Minuten, wie lange der Benutzer Zugriff auf das Aufzeichnungsarchiv hat.

Folgende Elemente sind nicht Teil der aktuellen Lizenz, falls sie nicht sichtbar sind. Staatliche Feiertage und arbeitsfreie Tage werden bei der Aufbewahrungsdauer und dem Archivzugriff nicht berücksichtigt.

Wenn ein Benutzer Teil einer Gruppe ist, werden auch diese Einstellungen berücksichtigt. Wenn sich die Einstellungen zwischen Benutzern und Gruppen widersprechen (z. B. 2 Tage Archiv-Zugriff für den Benutzer und 3 Tage für die Gruppe), wird die höchste Einschränkung angewendet (d. h., der Benutzer sieht nur 2 Tage vom Archiv-Material).

- Aktivieren Sie **Auf nicht-operative Tage ausweiten**, um Tage wie Feiertage oder arbeitsfreie Tage in das erweiterte Aufzeichnungs- und Zugriffsmanagement einzuschließen.
- Aktivieren Sie **Betriebsstunden beschränken**, um das Archiv für den konfigurierten Bereich während der Betriebsstunden auszublenden.
- Wählen Sie **Aktuellen Tag zulassen** als Ausnahmebedingung, damit der Benutzer das Archiv während der Betriebszeiten des aktuellen Tages ansehen kann.

Zudem kann die erweiterte Aufzeichnungs- und Zugriffsverwaltung („Betriebstage“) basierend auf dem Benutzer eingeschränkt werden (siehe „Gruppenrechte verwalten“ auf Seite 372).

3. Aktivieren Sie **Sicheres Passwort für Exporte verwenden**. Wenn ein Benutzer berechtigt ist, Aufzeichnungen zu exportieren, muss er ein sicheres Passwort angeben.
4. Aktivieren Sie **Für Wechsel in Archivmodus ist ein Kommentar erforderlich**.
5. Aktivieren Sie **Aufnahmetaste anzeigen**, um die Schaltfläche REC in der Kameraansicht anzuzeigen.

Benutzerrechte verwalten

Benutzerrechte und administrative Rechte werden nur positiv vererbt, das heißt, wenn einem Benutzer eine bestimmte Berechtigung als Benutzerrecht, jedoch nicht als administratives Recht zugewiesen wird, besitzt er trotzdem beide Rechte.

Beispiel

Benutzer A wurde unter „Benutzer / Benutzerrechte verwalten“ das Recht zum Löschen von Aufzeichnungen zugewiesen, dieses Recht wurde ihm jedoch nicht unter „Gruppen / Benutzerrechte verwalten“ zugewiesen. Der Benutzer kann weiterhin Aufnahmen löschen - auch wenn er einer Gruppe angehört, die nicht über die entsprechenden Rechte verfügt.

Wenn Benutzer A hingegen zu einer Gruppe gehört, die berechtigt ist, einen Button zu definieren, dem Benutzer selbst dieses Recht jedoch nicht zugewiesen wurde, besitzt er dennoch das Gruppenrecht.

Auf diese Weise können Benutzer Mitglieder einer Gruppe sein und trotzdem über benutzerspezifische Rechte verfügen, ohne Konflikte zu verursachen.

Benutzerrechte können bei Zugehörigkeit zu einer Gruppe auch über deren Gruppenrechte verwaltet werden (siehe „[Administrative Rechte und Benutzerrechte](#)“ auf Seite 24). Die Zugehörigkeit des Benutzers zu bestimmten Gruppen ist erkennbar an den Farbfeldern (für die Konfiguration der Farbgebung von Gruppen, siehe „[Gruppen](#)“ auf Seite 367).

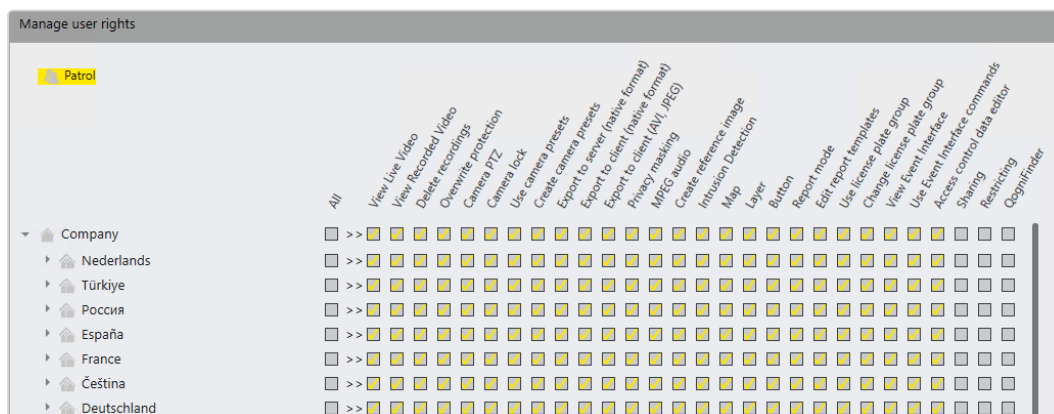


Abb. 193: Benutzer - Benutzerrechte verwalten

1. Aktivieren oder deaktivieren Sie die Rechte für den gewählten Benutzer, um auf den installierten Geräten und Objekten bestimmte Aktionen durchzuführen.
2. Öffnen Sie optional den Unternehmensbaum und definieren Sie die Benutzerrechte speziell für jeden Zweig.

Abhängig vom Gerät bzw. Objekt stehen folgende Rechte zur Verfügung, die einzeln oder als Ganzes aktiviert oder deaktiviert werden können.

- **Alle:** Aktiviert oder deaktiviert alle Benutzerrechte für das entsprechende Gerät oder Objekt.
- **Live-Video anzeigen:** Der Benutzer darf eine Kamera und deren Live-Bilder im Überwachungsmodus sehen.

-
- **Videoaufzeichnung anzeigen:** Der Benutzer darf Kameras im Archivmodus verwenden.
 - **Aufzeichnungen löschen:** Der Benutzer darf Aufzeichnungen im Archivmodus löschen.
 - **Überschreibschutz:** Der Benutzer darf Aufzeichnungen im Archivmodus mit Überschreibschutz versehen bzw. darf einen vorhandenen Überschreibschutz entfernen.
 - **Kamera-PTZ:** Der Benutzer darf die PTZ-Kamera, einschließlich des Digitalzooms, verwenden, mit Ausnahme von Preset-Kamerapositionen.
 - **Kamerasperre:** Der Benutzer darf die Position der PTZ-Kamera sperren.
 - **Kamera-Presets verwenden:** Der Benutzer darf die vordefinierten Kamerapositionen verwenden.
 - **Kamera-Presets anlegen:** Der Benutzer darf Kamera-Preset-Positionen anlegen bzw. vordefinierte Positionen löschen.
 - **Export zum Server (natives Format):** Der Benutzer kann Bilddaten im Qognify-spezifischen Format auf dem Server speichern.
 - **Export zum Client (natives Format):** Der Benutzer kann Bilddaten im Qognify-spezifischen Format auf dem Client speichern.
 - **Export zum Client (AVI, JPEG):** Der Benutzer kann Bilddaten als eine AVI- oder JPEG-Datei auf dem Server speichern.
 - **Privacy-Masking:** Der Benutzer darf das Privacy-Masking deaktivieren.
 - **MPEG-Audio:** Der Benutzer darf die Audioübertragung verwenden.
 - **Referenzbild erstellen:** Der Benutzer kann den manuellen Referenzbildvergleich im Menü „Extras“ verwenden.
 - **Einbruchmeldeanlage:** Der Benutzer kann Einbruchmeldebefehle verwenden, z. B. auf Lageplänen.
 - **Lageplan:** Der Benutzer darf den entsprechenden Lageplan verwenden.
 - **Ansicht:** Der Benutzer darf festgelegte Ansichten anzeigen lassen.
 - **Button:** Der Benutzer darf Buttons verwenden.
 - **Ereignisauswertung:** Der Benutzer darf die Ereignisauswertung einsehen.
 - **Berichtsvorlagen bearbeiten:** Der Benutzer kann im Modus „Ereignisauswertung“ Berichtsabfragen erstellen und bearbeiten und sie als Vorlagen speichern.

- **Kennzeichengruppe verwenden:** Der Benutzer kann Kennzeichengruppen nur verwenden, wenn der LPR-Stammdateneditor automatisch geöffnet wird, wenn ein unbekanntes Kennzeichen erkannt wird.
- **Kennzeichengruppe ändern:** Der Benutzer kann den LPR-Stammdateneditor über das Menü „Ansicht“ öffnen und Kennzeichen vollständig bearbeiten.
- **Event Interface anzeigen:** Der Benutzer kann die Event Interface-Elemente anzeigen.
- **Event Interface-Befehle verwenden:** Der Benutzer kann den Zustand eines Event Interface-Elements, z. B. auf Lageplänen, ändern.
- **Editor für Zutrittskontrolldaten:** Der Benutzer kann den Editor für Zutrittskontrolldaten im Menü „Ansicht“ verwenden.
- **Freigabe:** Der Benutzer darf eine Kamera für andere Benutzer und jede verbundene Active Directory-Gruppe freigeben. *Um eine Kamera freizugeben, benötigt der Benutzer keine Administratorrechte.*

Die Freigabeerlaubnis umfasst auch das Recht, vorübergehende Einschränkungen der Kameras einzustellen (siehe „Einschränkungsmanager“ auf Seite 111).

- **Einschränkung:** Der Benutzer kann die Einschränkungseinstellungen für Kameras bearbeiten.
- **QogniFinder:** Der Benutzer kann unter Verwenden des QogniFinder im Archivmodus nach Objekten suchen.

Administrative Rechte verwalten

Nur Benutzer mit administrativen Rechten können das System im Konfigurationsmodus bearbeiten.

Beispiel

Ein Benutzer kann als Systemadministrator für die Filiale „Hamburg“ festgelegt werden, ohne Zugriff auf die Filiale „München“ zu haben (siehe [„Beziehung zwischen der Hauptfiliale und ihren Unterfilialen“ auf Seite 218](#)).

Die Rechte von Benutzern und Gruppen werden auch serverseitig geprüft, das heißt, selbst wenn ein gehackter Client (ohne Prüfung der Rechte) verwendet wird, ist es dennoch nicht möglich, Benutzer, Gruppen oder deren Profile zu konfigurieren.

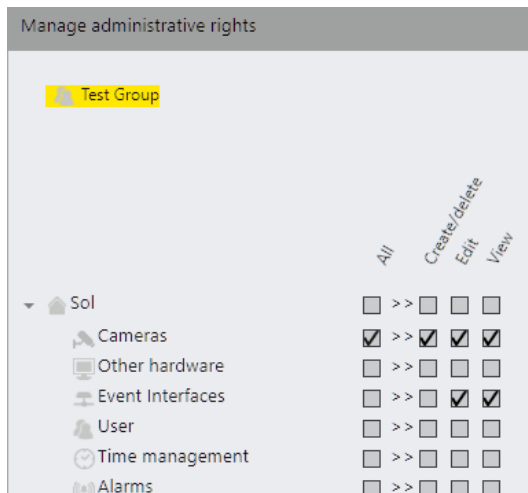


Abb. 194: Benutzer - Administrative Rechte verwalten

1. Aktivieren oder deaktivieren Sie für den gewählten Benutzer die Berechtigungen, um Änderungen durchzuführen oder Einstellungen vorzunehmen. Es stehen drei Arten administrativer Rechte zur Verfügung:
 - **Anlegen/Löschen:** Der Benutzer darf die gewählten Objekte vollumfänglich verwalten und beispielsweise Kameras anlegen, konfigurieren und löschen.
 - **Bearbeiten:** Der Benutzer darf die Einstellungen der gewählten Objekte anpassen, die Objekte selbst jedoch nicht anlegen oder löschen.
 - **Betrachten:** Der Benutzer darf die gewählten Objekte sehen und bedienen, darf jedoch keine Einstellungen vornehmen bzw. Objekte anlegen und löschen. Dies gilt nicht für Ansichten, die im Überwachungsmodus erstellt wurden („temporäre Ansichten“).
2. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
3. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Sonstiges

Um auf eine Kamera mit einer statischen IP-Adresse und einem statischen Port zugreifen zu können, muss der Benutzer über die erforderlichen Rechte verfügen.



Misc

Enable static URL access

Password:

Abb. 195: Benutzer - Sonstiges

1. Wählen Sie **Statischen URL-Zugang aktivieren** (IP-Adresse und Portnummer) für diesen Benutzer.
2. Geben Sie das Passwort an.
3. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
4. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Benutzer löschen

1. Wählen Sie den Benutzer in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Benutzer duplizieren

1. Wählen Sie den Benutzer in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den **Namen** für den duplizierten Benutzer ein.
3. Bestätigen Sie den Namen mit **OK**. Der neue Benutzer wird in der Übersicht angezeigt.

Gruppen

Mit der Funktion **Gruppen** im Steuerelement Administration können Sie die angelegten Benutzer zu Gruppen hinzufügen und die Berechtigungen der Gruppen verwalten. Abhängig davon, ob sich ein Benutzer mit einem Benutzerprofil oder einem Gruppenprofil angemeldet ist, erhält er die entsprechenden Berechtigungen und Profile zugewiesen.

Eine allgemeine Beschreibung der administrativen Rechte und Benutzerrechte finden Sie unter [„Administrative Rechte und Benutzerrechte“ auf Seite 24](#).

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Gruppen** im Steuerelement Administration.

Neue Gruppe anlegen

1. Wählen Sie im Steuerelement **Gruppen** die Option **Objekt neu anlegen** aus.
Zwei Optionen stehen zur Verfügung:
 - Basisgruppe erstellen: Erstellt einen neuen Benutzer mit Benutzerrechten, die in Qognify VMS konfiguriert werden.
 - Active Directory-Gruppe erstellen: Wenn ein Active Directory-(AD-)Server installiert ist, werden der Benutzer und seine Gruppenzugehörigkeit mit dem Konto des Benutzers in Qognify VMS verknüpft.

Basisgruppe erstellen

1. Wählen Sie **Basisgruppe erstellen**.
2. Geben Sie den **Namen** für die neue Gruppe ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Gruppe wird in der Übersicht angezeigt.

Active Directory®-Gruppe erstellen

1. Wählen Sie den **Objekttyp** „Gruppen“ aus.
2. Öffnen Sie den **Suchpfad** zum AD-Server.
3. Geben Sie den Gruppennamen ein. Die entsprechende Gruppe wird angezeigt.
4. Um anhand des Namens nach dem Benutzer zu suchen, wählen Sie **Namen prüfen**.
5. Klicken Sie auf **OK**.

Gruppe konfigurieren

1. Wählen Sie die Gruppe in der Übersicht aus.

Active Directory-Gruppen, die in AD angelegt werden, behalten die Rechte bei, die sie von der übergeordneten Gruppe übernommen haben. Ein Benutzer, der in Qognify VMS nicht vorhanden ist, darf sich anmelden, sofern er Mitglied einer in Qognify VMS angelegten übergeordneten Gruppe ist.

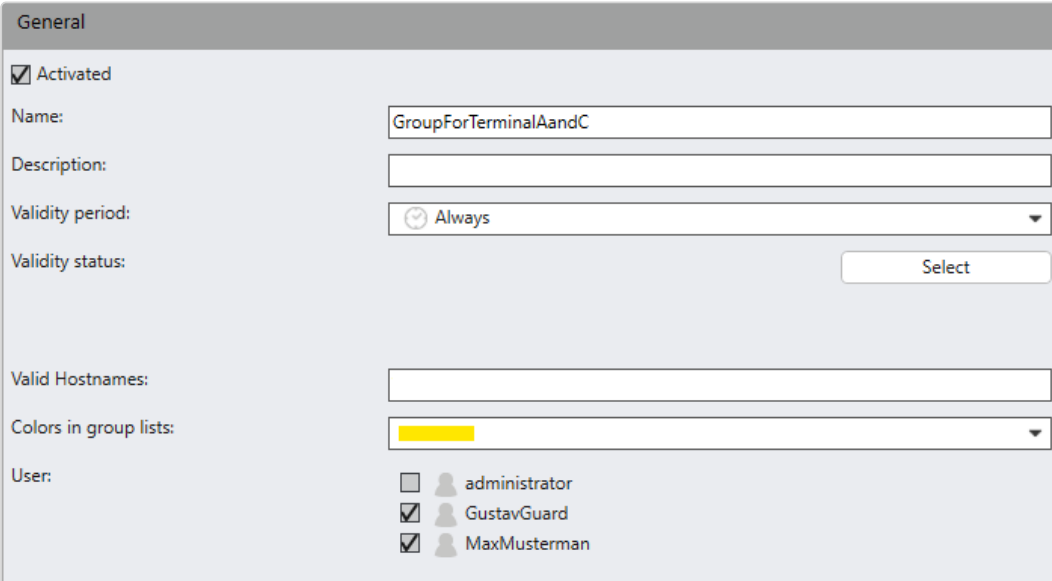
Die Rechteverwaltung für eine Gruppierung erfolgt außerhalb von Qognify VMS.

AD-Gruppen synchronisieren

Die Namen und Rechte von Active Directory-Gruppen müssen mit dem AD-Server synchronisiert werden, da die Namen in Qognify VMS nicht bearbeitet werden können.

1. Wählen Sie im Steuerelement Gruppen **Neu laden** .

Allgemein



General

Activated

Name:

Description:

Validity period:

Validity status:

Valid Hostnames:

Colors in group lists:

User:

administrator

GustavGuard

MaxMusterman

Abb. 196: Gruppen - Allgemein

1. **Aktivieren** Sie die Gruppe.
2. Wenn Sie den Namen der Active Directory-Gruppe ändern möchten, wählen Sie **Gruppe ändern** aus und ändern Sie den Gruppennamen im Dialog.
3. Geben Sie eine **Beschreibung** der Gruppe ein.
4. Wählen Sie einen **Gültigkeitszeitraum** für die Gruppe aus, innerhalb dessen Gruppenmitglieder abhängig von ihren Benutzerrechten auf das System zugreifen können. Die möglichen Zeiträume werden in der „[Zeitverwaltung](#)“ auf [Seite 381](#) festgelegt.

Eine allgemeine Beschreibung der administrativen Rechte und Benutzerrechte finden Sie unter „[Administrative Rechte und Benutzerrechte](#)“ auf [Seite 24](#).

5. Legen Sie den **Gültigkeitszustand** fest, um die Gruppe zu aktivieren bzw. zu deaktivieren. Alle Benutzer dieser Gruppe können dadurch vom Zugriff auf bestimmte Kameras ausgeschlossen werden.
6. Wenn die Gruppe auf einen oder mehrere Bereiche (Hosts) innerhalb einer Multi-Host-Konfiguration beschränkt ist, geben Sie die **gültigen Hostnamen** getrennt durch Kommas ein (siehe „[Einschränkung der Verwendung mehrerer Hosts](#)“ unten).
7. Teilen Sie der Gruppe eine **Farbgebung in Gruppen-Listen** zu. Die Verwendung unterschiedlicher Farben für verschiedene Gruppen erleichtert die Verwaltung der Benutzerrechte, da auf jeden Benutzer die Rechte und Farben der Gruppe, zu der er gehört, vererbt werden.
8. Aktivieren Sie die **Benutzer**, die der Gruppe zugeordnet werden sollen.

Einschränkung der Verwendung mehrerer Hosts

Der Benutzer kann beim Zugriff auf Kameras eingeschränkt werden, um zu verhindern, dass er auf Kameras Zugriff hat, die nicht zu seinem eigentlichen Arbeitsbereich gehören (z. B. Wachmann in Gebäude A, aber nicht in Gebäude B). Während die Funktion den Zugriff auf Kameras (und Entitäten) unabhängig von dem Host, mit dem er verbunden ist, einschränkt, kann dieser Zugriff weiter eingeschränkt werden, indem nur die Bereiche (d. h. Hosts) definiert werden, bei denen der Benutzer derzeit angemeldet ist.

Dadurch sieht der Benutzer nicht nur die durch seine Funktion zugewiesenen Kameras, sondern auch nur die mit seinem aktuellen Host verbundenen Kameras.

Rechte-Optionen

Rights options

Consider that also user restrictions will be applied if applicable.

Limit archive access

Days: Hours: Minutes:

Extend on non-operating days

Restrict operating hours

Allow current day

Activate Active Directory support

Use secure password for exports

A comment is required to change to archive mode

Show recording button

Abb. 197: Gruppen - Rechte-Optionen

1. Aktivieren Sie **Archivzugriff beschränken** und geben Sie die Dauer der Zugriffszeit (in Minuten) an, um für die Gruppenmitglieder den fortlaufenden Zugriff auf das Archiv zu beschränken.
2. Bestimmen Sie die Anzahl an Tagen, Stunden und Minuten, wie lange Gruppenmitglieder Zugriff auf das Aufzeichnungsarchiv haben.

Folgende Elemente sind nicht Teil der aktuellen Lizenz, falls sie nicht sichtbar sind. Staatliche Feiertage und arbeitsfreie Tage werden bei der Aufbewahrungsdauer und dem Archivzugriff nicht berücksichtigt.

Wenn ein Benutzer Teil einer Gruppe ist, werden auch diese Einstellungen berücksichtigt. Wenn sich die Einstellungen zwischen Benutzern und Gruppen widersprechen (z. B. 2 Tage Archiv-Zugriff für den Benutzer und 3 Tage für die Gruppe), wird die höchste Einschränkung angewendet (d. h., der Benutzer sieht nur 2 Tage vom Archiv-Material).

- Aktivieren Sie **Auf nicht-operative Tage ausweiten**, um Tage wie Feiertage oder arbeitsfreie Tage in das erweiterte Aufzeichnungs- und Zugriffsmanagement einzuschließen.
- Aktivieren Sie **Betriebsstunden beschränken**, um das Archiv für den konfigurierten Bereich während der Betriebsstunden auszublenden.
- Wählen Sie **Aktuellen Tag zulassen** als Ausnahmebedingung, damit der Benutzer das Archiv während der Betriebszeiten des aktuellen Tages ansehen kann.

Zudem kann die erweiterte Aufzeichnungs- und Zugriffsverwaltung („Betriebstage“) basierend auf dem Benutzer eingeschränkt werden (siehe „Benutzerrechte verwalten“ auf Seite 361).

3. Aktivieren Sie **Active Directory Unterstützung aktivieren**, um Berechtigungseinstellungen eines angeschlossenen Active Directory-Servers zu übernehmen.
4. Aktivieren Sie **Sicheres Passwort für Exporte verwenden**. Wenn ein Benutzer berechtigt ist, Aufzeichnungen zu exportieren, muss er ein sicheres Passwort angeben.

- Aktivieren Sie **Für Wechsel in Archivmodus ist ein Kommentar erforderlich**, damit der Benutzer beim Wechseln in den Archivmodus einen Kommentar eingeben muss. Dadurch wird verhindert, dass unbemerkt in den Archivmodus gewechselt wird.

Gruppenrechte verwalten

Die Rechte von Benutzern und Gruppen werden auch serverseitig geprüft, das heißt, selbst wenn ein gehackter Client (ohne Prüfung der Rechte) verwendet wird, ist es dennoch nicht möglich, Benutzer, Gruppen oder deren Profile zu konfigurieren.

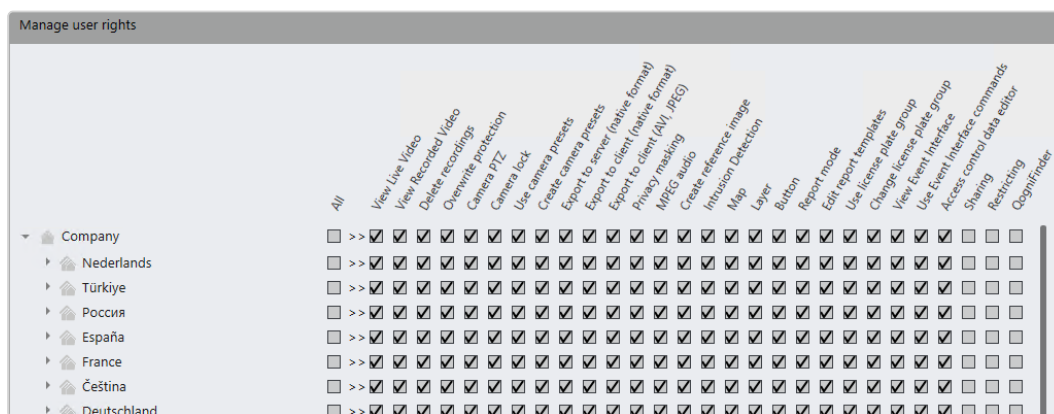


Abb. 198: Gruppen - Gruppenrechte verwalten

- Aktivieren oder deaktivieren Sie für die gewählte Gruppe die Berechtigungen, auf den installierten Geräten und Objekten bestimmte Aktionen durchzuführen, siehe „[Benutzerrechte verwalten](#)“ auf Seite 361).

Abhängig vom Gerät bzw. Objekt stehen folgende Rechte zur Verfügung, die einzeln oder als Ganzes aktiviert oder deaktiviert werden können.

- **Alle:** Aktiviert oder deaktiviert alle Benutzerrechte für das entsprechende Gerät oder Objekt.
- **Live-Video anzeigen:** Der Benutzer darf eine Kamera und deren Live-Bilder im Überwachungsmodus sehen.
- **Videoaufzeichnung anzeigen:** Der Benutzer darf Kameras im Archivmodus verwenden.
- **Aufzeichnungen löschen:** Der Benutzer darf Aufzeichnungen im Archivmodus löschen.

- **Überschreibschutz:** Der Benutzer darf Aufzeichnungen im Archivmodus mit Überschreibschutz versehen bzw. darf einen vorhandenen Überschreibschutz entfernen.
- **Kamera-PTZ:** Der Benutzer darf die PTZ-Kamera, einschließlich des Digitalzooms, verwenden, mit Ausnahme von Preset-Kamerapositionen.
- **Kamerasperre:** Der Benutzer darf die Position der PTZ-Kamera sperren.
- **Kamera-Presets verwenden:** Der Benutzer darf die vordefinierten Kamerapositionen verwenden.
- **Kamera-Presets anlegen:** Der Benutzer darf Kamera-Preset-Positionen anlegen bzw. vordefinierte Positionen löschen.
- **Export zum Server (natives Format):** Der Benutzer kann Bilddaten im Qognify-spezifischen Format auf dem Server speichern.
- **Export zum Client (natives Format):** Der Benutzer kann Bilddaten im Qognify-spezifischen Format auf dem Client speichern.
- **Export zum Client (AVI, JPEG):** Der Benutzer kann Bilddaten als eine AVI- oder JPEG-Datei auf dem Server speichern.
- **Privacy-Masking:** Der Benutzer darf das Privacy-Masking deaktivieren.
- **MPEG-Audio:** Der Benutzer darf die Audioübertragung verwenden.
- **Referenzbild erstellen:** Der Benutzer kann den manuellen Referenzbildvergleich im Menü „Extras“ verwenden.
- **Einbruchmeldeanlage:** Der Benutzer kann Einbruchmeldebefehle verwenden, z. B. auf Lageplänen.
- **Lageplan:** Der Benutzer darf den entsprechenden Lageplan verwenden.
- **Ansicht:** Der Benutzer darf festgelegte Ansichten anzeigen lassen.
- **Button:** Der Benutzer darf Buttons verwenden.
- **Ereignisauswertung:** Der Benutzer darf die Ereignisauswertung einsehen.
- **Berichtvorlagen bearbeiten:** Der Benutzer kann im Modus „Ereignisauswertung“ Berichtsabfragen erstellen und bearbeiten und sie als Vorlagen speichern.
- **Kennzeichengruppe verwenden:** Der Benutzer kann Kennzeichengruppen nur verwenden, wenn der LPR-Stammdateneditor automatisch geöffnet wird, wenn ein unbekanntes Kennzeichen erkannt wird.

- **Kennzeichengruppe ändern:** Der Benutzer kann den LPR-Stammdateneditor über das Menü „Ansicht“ öffnen und Kennzeichen vollständig bearbeiten.
- **Event Interface anzeigen:** Der Benutzer kann die Event Interface-Elemente anzeigen.
- **Event Interface-Befehle verwenden:** Der Benutzer kann den Zustand eines Event Interface-Elements, z. B. auf Lageplänen, ändern.
- **Editor für Zutrittskontrolldaten:** Der Benutzer kann den Editor für Zutrittskontrolldaten im Menü „Ansicht“ verwenden.
- **Freigabe:** Der Benutzer darf eine Kamera für andere Benutzer und jede verbundene Active Directory-Gruppe freigeben. *Um eine Kamera freizugeben, benötigt der Benutzer keine Administratorrechte.*

Die Freigabeerlaubnis umfasst auch das Recht, vorübergehende Einschränkungen der Kameras einzustellen (siehe „Einschränkungsmanager“ auf Seite 111).

- **Einschränkung:** Der Benutzer kann die Einschränkungseinstellungen für Kameras bearbeiten.
- **QogniFinder:** Der Benutzer kann unter Verwenden des QogniFinder im Archivmodus nach Objekten suchen.

Administrative Rechte verwalten

1. Wählen Sie die entsprechenden Berechtigungen für die ausgewählte Gruppe in den Administrationseinstellungen aus (siehe „Administrative Rechte verwalten“ auf Seite 365).
 - **Anlegen/Löschen:** Die Gruppe darf die gewählten Objekte voll umfänglich verwalten und beispielsweise Kameras anlegen und löschen.
 - **Bearbeiten:** Die Gruppe darf die Einstellungen der gewählten Objekte anpassen, die Objekte selbst jedoch nicht anlegen oder löschen.
 - **Betrachten:** Die Gruppe darf die gewählten Objekte sehen und bedienen, darf jedoch keine Einstellungen vornehmen bzw. Objekte anlegen und löschen.

2. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
3. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Gruppe löschen

1. Wählen Sie die Gruppe in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Gruppe duplizieren

1. Wählen Sie die Gruppe in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für die duplizierte Gruppe ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Gruppe wird in der Übersicht angezeigt.

Profile

Mit der Funktion **Profile** im Steuerelement Administration können Sie einem Benutzer-Account oder einer Gruppe allgemeine Einstellungen zuweisen, die für die Bedienung und Schnittstelleneinstellungen des Clients gelten. Für jeden Benutzer und jede Benutzergruppe wird automatisch ein Profil angelegt. Die Profile für den Administrator und die Administratorgruppe können nicht gelöscht werden. Das Profil der Administratorgruppe ist standardmäßig deaktiviert.

Die Rechte von Benutzern und Gruppen werden auch serverseitig geprüft, das heißt, selbst wenn ein gehackter Client (ohne Prüfung der Rechte) verwendet wird, ist es dennoch nicht möglich, Benutzer, Gruppen oder deren Profile zu konfigurieren.

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Profile** im Steuerelement Administration.

Allgemein

General

Activated

Confirm termination of the client

Confirm termination of the client with user password

Always use default password for video exports

Lock user interface

Log off user when inactive

Inactivity timeout (min):

PTZ priority: 1=highest ... 1000=lowest

Timeout (s) for PTZ priority actions:

Timeout (s) for PTZ lock actions:

Layers: Schreibtisch

Patrols:

Abb. 199: Profile - Allgemein

1. Aktivieren oder deaktivieren Sie das gewählte Profil.
2. Aktivieren Sie **Beenden des Clients bestätigen**, um beim Beenden des Clients eine Bestätigung anzuzeigen.
3. Optional können Sie **Beenden des Clients mit Benutzerpasswort bestätigen** aktivieren, um beim Beenden des Clients eine Bestätigung anzuzeigen, die der Benutzer mit seinem Passwort bestätigen muss.
4. Wählen Sie **Immer Standardpasswort für Videoexporte nutzen**, um den Benutzer von der Verwendung eines spezifischen Passworts beim Export abzuhalten. Die Option für die Eingabe eines spezifischen Passworts ist bei Video-Export deaktiviert (siehe „Export von nativen Daten zum Client“ auf Seite 117).
5. Wählen Sie **Benutzeroberfläche sperren**, wenn der Benutzer daran gehindert werden soll, die Benutzeroberfläche zu verändern (z. B. das Fenster Qognify VMS zu verschieben oder in der Größe zu verändern).
6. Optional können Sie **Benutzer bei Inaktivität abmelden** aktivieren und das **Timeout** (Zeitintervall in Minuten) angeben, nach dem der Benutzer automatisch vom System abgemeldet wird, sofern er keine Aktionen durchführt.

7. Setzen Sie den Zähler **PTZ-Priorität** auf einen Wert zwischen 1 und 1000 (je niedriger die Zahl, desto höher die Priorität) und geben Sie das **Timeout für PTZ-Prioritätsaktionen** in Sekunden an. Wenn der Benutzer keine PTZ-Steuerungen aktiviert, wird nach der Zeitüberschreitung (Timeout) die Kamerasteuerung wieder freigegeben.

Bei Übernahme der Steuerung der Kamera kann ein Benutzer (oder ein Alarm oder eine Serversequenz) mit einer höheren PTZ-Priorität einen anderen Benutzer (bzw. einen anderen Alarm oder eine andere Serversequenz) übersteuern.

8. Geben Sie das **Timeout für PTZ-Sperraktionen** in Sekunden an. Wenn der Benutzer eine PTZ-Kamera im Überwachungsmodus sperrt und die Kamera nicht manuell wieder freigibt, wird die Kamera automatisch nach dem angegebenen Timeout freigegeben.
9. Aktivieren Sie die **Ansichten**, die dem Benutzer oder der Gruppe angezeigt werden können (siehe „[Ansichten](#)“ auf Seite 404). Diese Ansichten werden beim Start des Clients mit dem betreffenden Profil sofort im Überwachungsmodus angezeigt und können nicht geschlossen werden.
10. Aktivieren Sie die **Wächterrundgänge**, die der Benutzer oder die Gruppe aktivieren kann, wenn der Client mit dem betreffenden Profil gestartet wird (siehe „[Wächterrundgänge](#)“ auf Seite 422).

Bildeinstellungen

Mit den Bildeinstellungen wird die Qualität der im Überwachungsmodus angezeigten Videobilder in Abhängigkeit vom Benutzerprofil festgelegt.

Image settings			
Single image (Motion JPEG, MxPEG)			
	Frame rates (fps):	Display mode:	
Normal:	<input type="text" value="2"/>	<input type="text" value="Top speed"/>	
Selected:	<input type="text" value="25"/>	<input type="text" value="Best quality"/>	
Alarm:	<input type="text" value="25"/>	<input type="text" value="Best quality"/>	
Streaming (MPEG-4, H.264)			
	Frame rates (fps):		
Normal:	<input type="text" value="Full"/>		
Selected:	<input type="text" value="Full"/>		
Alarm:	<input type="text" value="Full"/>		
Video classifications (for multistreaming)			
	Small	Medium	Large
Normal:	<input type="text" value="Analytics"/>	<input type="text" value="Analytics"/>	<input type="text" value="Analytics"/>
Selected:	<input type="text" value="HD quality"/>	<input type="text" value="HD quality"/>	<input type="text" value="HD quality"/>
Alarm:	<input type="text" value="HD quality"/>	<input type="text" value="HD quality"/>	<input type="text" value="HD quality"/>

Abb. 200: Profile - Bildeinstellungen

Einzelbild (Motion JPEG, MxPEG)

Mit den Einzelbildeinstellungen legen Sie fest, wie viele Bilder der Client pro Kamera in der Sekunde darstellen soll, wenn die Kamera Motion JPEG-Bilder liefert.

Diese Einstellungen betreffen nur die Darstellung im Client, wenn bei der Kamerakonfiguration als Streaming-Modus „Motion JPEG“ aktiviert ist. Sie haben keine Auswirkungen auf die Aufzeichnungen.

1. Geben Sie die Bildraten des angezeigten **normalen** und **ausgewählten** Videobilds sowie des **Alarm**-Videobilds an.
2. Wählen Sie den **Darstellungsmodus**, der die Kompressionsrate des Videobilds bestimmt.

Streaming (MPEG-4, H.264)

Mit „Streaming (MPEG-4, H.264)“ legen Sie die Bildrate (fps) für das MPEG-4-, H.264- oder H.265-Streaming fest. Sie können zwischen einer maximalen und einer reduzierten Bildrate wählen.

- **Maximal:** Bei der maximalen Bildrate wird der gesamte Bildstrom übertragen. Dies kann zu einer starken Belastung des Client-PCs führen, wenn mehr als vier Kameras gleichzeitig angezeigt werden und/oder die Rechnerhardware zu leistungsschwach ausgelegt ist.
 - **Reduziert:** Bei der reduzierten Bildrate werden nur die I-Frames (Vollbilder) übertragen, was zu einer erheblich geringeren CPU-Last des Clients führt. Die Standardeinstellung für I-Frames ist ein I-Frame pro Sekunde. Das bedeutet, bei reduzierter Bildrate wird nur ein Bild pro Sekunde im Überwachungsmodus angezeigt. Die Anzahl der I-Frames pro Sekunde muss in der Kamerakonfiguration geändert werden (siehe „[Kamera konfigurieren](#)“ auf Seite 242).
1. Geben Sie die Bildraten des angezeigten **normalen** und **ausgewählten** Videobilds sowie des **Alarm**-Videobilds an.

Videoklassifikation (für Multistreaming)

Mit der Videoklassifikation können Sie die Bildrate für drei Kamerabildgrößen festlegen. Wenn in einer Ansicht viele Kameras angezeigt werden, kann die Auflösung der einzelnen Kameras durch Auswahl einer anderen Einstellung für jede Bildanzeigegröße verringert werden:

- Klein: für Bildanzeigegrößen bis 320 px
- Mittel: für Bildanzeigegrößen zwischen 320 px und 640 px
- Groß: für Bildanzeigegrößen über 640 px

Durch Verringern der Auflösung wird die Systemleistung verbessert. Entsprechend kann auch die Streaming-Rate an die verfügbare Bandbreite angepasst werden (z. B. HD (High Definition), Web, Mobile).

1. Geben Sie die Bildraten und die Streaming-Rate des angezeigten **normalen** und **ausgewählten** Videobilds sowie des **Alarm**-Videobilds an. Wird keine Rate ausgewählt, wird das Streaming automatisch angepasst.

Videowand-Modulmapping

	Window	Video wall module
<input type="checkbox"/>	0	DA(0/0)
<input type="checkbox"/>	1	DA(1/0)
<input type="checkbox"/>	2	DA(2/0)

Abb. 201: Profile - Videowand-Modulmapping

Mit dem Videowand-Modulmapping legen Sie fest, ob und in welchem Videowand-Modul ein auftretender Alarm oder ein Wächterrundgang für das ausgewählte Profil angezeigt wird.

Vor dem Mapping von Videowand-Modulen muss eine Videowand (siehe „[eyevis Wand](#)“ auf Seite 300) oder ein Qognify Display Agent (siehe [SeeTec Display Agent \(Videowand\)](#)) festgelegt werden (siehe „[Videowände](#)“ auf Seite 430).

1. Wählen Sie das **Standard-Modulmapping** aus oder wählen Sie aus, welches Ansichtsfenster auf welchem Videowand-Modul angezeigt werden soll. Dieses Standard-Modulmapping wird verwendet, wenn Sie kein Videowand-Modulmapping für das aufzurufende Qognify-Fenster definiert haben. Das Standard-Modulmapping wird im Steuerelement Videowände konfiguriert (siehe „[Videowände](#)“ auf Seite 430).
2. Sollte die Anzahl der Modulzuordnungen nicht ausreichen, erweitern Sie die Liste, indem Sie auf das Symbol **Hinzufügen** klicken.
3. Wählen Sie in **Zusätzliche Modulmappings** aus, welches Fenster in welchem Videowand-Modul angezeigt werden soll.

***Beispiel** Das Hauptfenster wird im Videowand-Modul als 0/0 angezeigt. Im Alarmszenario wird festgelegt, dass die Alarmkamera im Hauptfenster angezeigt werden soll. Mit Hilfe des Videowand-Modulmapping wird das Bild der Alarmkamera auf der Videowand im Modul 0/0 angezeigt.*

4. Aktivieren Sie die Module, die Sie entfernen möchten, und klicken Sie auf **Löschen**.
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.

6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Zeitverwaltung

Mit der **Zeitverwaltung** im Steuerelement Administration können Sie Zeitschablonen ähnlich einem Stundenplan anlegen, um die Standardbildaufzeichnung einzelner oder mehrerer Kameras sowie die Gültigkeit in Alarmszenarien und Benutzergruppen zeitlich zu koordinieren.

Zudem kann die erweiterte Aufzeichnungs- und Zugriffsverwaltung („Betriebstage“) basierend auf dem Benutzer eingeschränkt werden (siehe „[Benutzerrechte verwalten](#)“ auf Seite 361).

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Zeitverwaltung** im Steuerelement Administration.

Konfiguration der erweiterten Aufzeichnungs- und Zugriffsverwaltung („Betriebstage“)

Folgende Elemente sind nicht Teil der aktuellen Lizenz, falls sie nicht sichtbar sind. Staatliche Feiertage und arbeitsfreie Tage werden bei der Aufbewahrungsdauer und dem Archivzugriff nicht berücksichtigt.

General

Operating days extend retention time

Operating days:
 Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Expand all Collapse all

Name ♀	Include days from calendar ♀	Exclude days from calendar ♀	
Company			
Company calendar	<input type="checkbox"/>	<input type="checkbox"/>	
extra operating days	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
holidays in germany	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Operating Hours

	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								

Abb. 202: Betriebstage

Jeder Kalendertag kann als Betriebstag markiert werden.

1. Wählen Sie „Betriebstage - Aufbewahrungsdauer verlängern“, um nur Betriebstage für die Aufbewahrungsdauer zu berücksichtigen. Die arbeitsfreien Tage werden bei der Aufbewahrungsdauer nicht berücksichtigt. Die Auswahl im Kalender ändert die Berechnung entsprechend. Wenn beispielsweise Montag bis Freitag als Betriebstage markiert sind und die Aufbewahrungsdauer auf einer Kamera auf 5 Tage eingestellt ist.

Beispiel: Heute ist Samstag 00:01 Uhr. Die Aufbewahrungsdauer beträgt 5 Tage (Mo-Fr sind 5 Tage und jeweils Betriebstage => 5 Tage).

2. Wählen Sie die Betriebstage aus.
3. Wählen Sie aus, welche Tage ein- oder ausgeschlossen werden sollen
 - Markieren Sie auch die Tage, die von den regulären Betriebszeiten ausgeschlossen sind, wie beispielsweise ein Sonntag, an dem geöffnet ist.
 - Schließen Sie Tage wie Firmenschließungen oder staatliche Feiertage aus, die auf einen Betriebstag fallen.
4. Klicken und ziehen Sie die Maus über den Kalender, um die **Öffnungszeiten** zu markieren.

Neue Zeitverwaltungsschablone anlegen

Name: MUC

	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	
Monday	[Blue shaded]																								
Tuesday	[Blue shaded]																								
Wednesday	[Blue shaded]																								
Thursday	[Blue shaded]																								
Friday	[Blue shaded]																								
Saturday	[Blue shaded]																								
Sunday	[Blue shaded]																								
Public holiday	[Blue shaded]																								

Company calendars

CH

Company calendar

FR

Abb. 203: Zeitverwaltungsschablone

1. Legen Sie eine neue Zeitverwaltungsschablone an.
2. Geben Sie den Namen für die neue Zeitverwaltungsschablone ein.
3. Bestätigen Sie den Namen mit **OK**. Ein Kalender zur Definition der Zeit-schablone wird angezeigt.
4. Markieren Sie in der Kalenderdarstellung die Zeiträume, in denen Aktionen stattfinden sollen, durch Überstreichen mit dem Mauszeiger und gedrückter Maustaste.
5. Um Teile der ausgewählten Zeitabschnitte zu entfernen, streichen Sie mit dem Mauszeiger und gedrückter Maustaste erneut über den betreffenden Zeitraum.

Zeitverwaltungsschablone konfigurieren

1. Wählen Sie die Zeitverwaltungsschablone in der Übersicht aus.
2. Wenn die Zeitverwaltung nur auf eine Filiale angewendet werden soll, wählen Sie ein Filialzeitmuster aus. Alternativ können Sie das zentrale Zeitverwaltungsmuster auswählen, das auf alle Filialen angewendet wird.
3. Markieren Sie in der Kalenderdarstellung die Zeiträume, in denen Aktionen stattfinden sollen, durch Überstreichen mit dem Mauszeiger und gedrückter Maustaste.
4. Wählen Sie die Kalender aus, auf die der Zeitplan angewendet werden soll. Die Kalender werden in den Betriebskalendern definiert (siehe „[Betriebskalender](#)“ auf der gegenüberliegenden Seite).
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Zeitverwaltungsschablone löschen

1. Wählen Sie die Zeitverwaltungsschablone in der Übersicht aus.
2. Klicken Sie auf das Symbol **Objekt löschen**.

Zeitverwaltungsschablone duplizieren

1. Wählen Sie die Zeitverwaltungsschablone in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für die duplizierte Zeitverwaltungsschablone ein.
3. Bestätigen Sie den Namen mit **OK**. In der Übersicht wird ein Kalender zur Definition der Zeitverwaltungsschablone angezeigt.
4. Bearbeiten Sie den Kalender (siehe „[Neue Zeitverwaltungsschablone anlegen](#)“ auf der vorherigen Seite).

Betriebskalender

Jede Filiale eines Unternehmens kann über mehrere Kalender verfügen. Daher weisen das Unternehmen sowie die einzelnen Filialen eine Kategorie namens „Betriebskalender“ auf. Die Benutzerrechte werden im Bereich mit den Benutzerrechten verwaltet (siehe „[Administrative Rechte verwalten](#)“ auf Seite 365).

In jedem Kalender legen Sie die Tage fest, die in Zeitschablonen gesondert von normalen Wochentagen behandelt werden (z. B. Feiertage oder arbeitsfreie Tage). Zeitschablonen werden in der Zeitverwaltung erstellt (siehe „[Zeitverwaltung](#)“ auf Seite 381). Sie ermöglichen eine präzise Spezifikation von Aufzeichnungszeiträumen oder Zeiten, in denen Alarmszenarien gestartet werden.

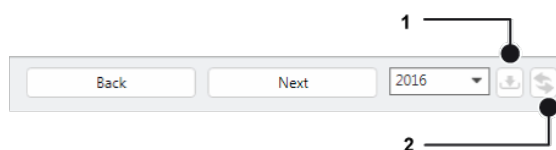


Abb. 204: Betriebskalender konfigurieren

1. Wählen Sie das Jahr aus, in dem Sie eine Kalenderschablone anlegen möchten. Es werden sechs Monate angezeigt.
2. Klicken Sie auf **Vorwärts**, um die folgenden sechs Monate anzuzeigen, oder klicken Sie auf **Zurück**, um die zurückliegenden sechs Monate anzuzeigen.
3. Um zum aktuellen Datum zu navigieren, klicken Sie auf **Zum aktuellen Datum springen** (2).

Betriebskalender bearbeiten

Kalender konfigurieren

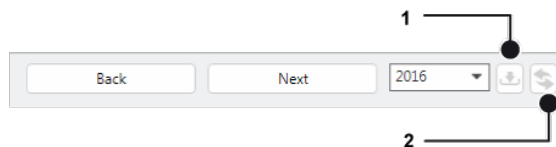


Abb. 205: Kalender konfigurieren

1. Wählen Sie den Kalender in der Übersicht aus.
2. Klicken Sie auf **Objekt bearbeiten** und geben Sie den neuen Namen des Kalenders ein.

3. Klicken Sie auf **Import** (1), um die gesetzlichen Feiertage in den Betriebskalender einzutragen. Die Schablonen für den Feiertageimport finden Sie im Qognify-Installationsverzeichnis im Verzeichnis „\Client\calendar“ als Textdateien.
4. Wählen Sie gegebenenfalls die gewünschten Bundesländer aus.
5. Aktivieren Sie **Vorhandene Feiertage ersetzen**, um alle bereits eingetragenen Feiertage manuell zu ersetzen, und bestätigen Sie mit **OK**. Die importierten Daten werden blau unterlegt angezeigt.
6. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
7. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.
8. Konfigurieren Sie die Zeitpläne für die Kalendertage (siehe [„Zeitverwaltung“ auf Seite 381](#)).

Kalender löschen

1. Wählen Sie den Kalender in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen** .

Kalender duplizieren

1. Wählen Sie den Kalender in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den **Namen** für den duplizierten Kalender ein.
3. Bestätigen Sie den Namen mit **OK**. Der neue Kalender wird in der Übersicht angezeigt.

Alarmer

Mit Qognify VMS können Sie komplexe Alarmroutinen individuell definieren. Alle Ereignisse, die einen Alarm starten können (z. B. Bewegungsmeldung, Ereignisse aus der Videoanalyse, Kennzeichenmeldung (LPR), I/O-Kontakt, Network I/O, Button), können eine Vielzahl verschiedener Aktionen auslösen. Dazu zählen Alarmaufzeichnung und Visualisierung, Senden von Triggern an Drittsysteme über physische I/O-Kontakte oder Network I/Os, Senden von Videosequenzen per E-Mail und FTP sowie das

Starten externer Programme. Daher kann für jede Alarmsituation ein angepasster Workflow eingerichtet werden.

Mit der Funktion **Alarmer** im Steuerelement Administration können Sie Alarmszenarien konfigurieren und verwalten.

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Alarmer** im Steuerelement Administration.

Alarmszenario anlegen

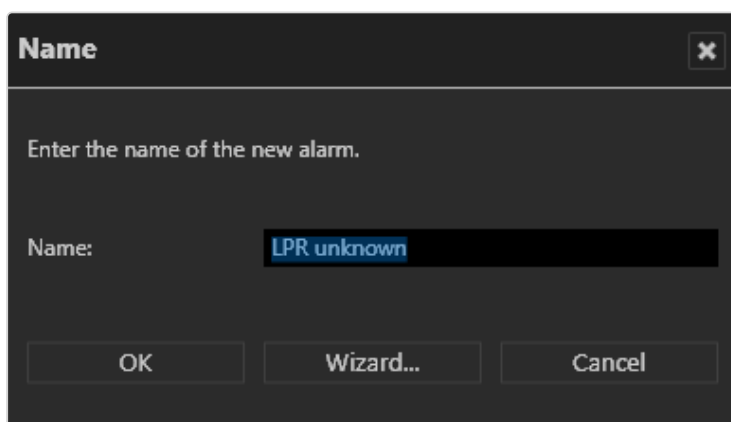


Abb. 206: Alarmszenario anlegen

1. Wählen Sie im Steuerelement Alarm die Option **Objekt neu anlegen** aus.
2. Geben Sie den Namen für das Alarmszenario ein.
3. Falls Sie das Alarmszenario mit Hilfe des Konfigurationsassistenten einstellen möchten, wählen Sie **Assistent** (siehe [„Alarmszenario mit dem Assistenten anlegen“ unten](#)) oder bestätigen Sie den Namen mit **OK**. Das neue Alarmszenario wird in der Übersicht angezeigt.
4. Informationen zur Konfiguration ohne den Assistenten finden Sie unter [„Alarm konfigurieren“ auf Seite 391](#).

Alarmszenario mit dem Assistenten anlegen

Die Alarmer basieren auf dem detaillierten Rechtekonzept von Cognify VMS und können individuellen Benutzern oder Benutzergruppen zugewiesen werden. Die Einstellungen entsprechen den Schritten im Steuerelement „Alarm“ (siehe [„Alarmszenario anlegen“ oben](#)).

Ereignisse

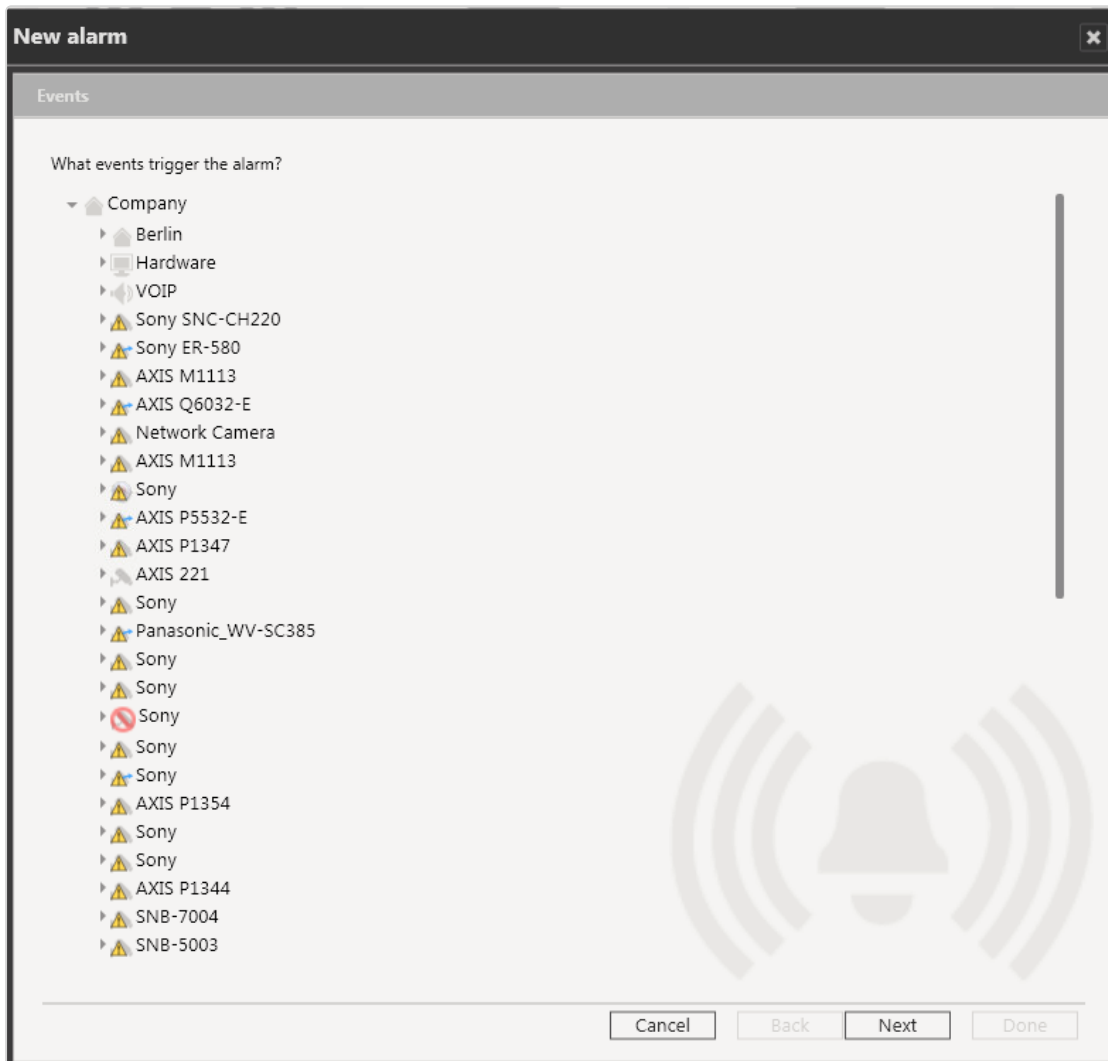
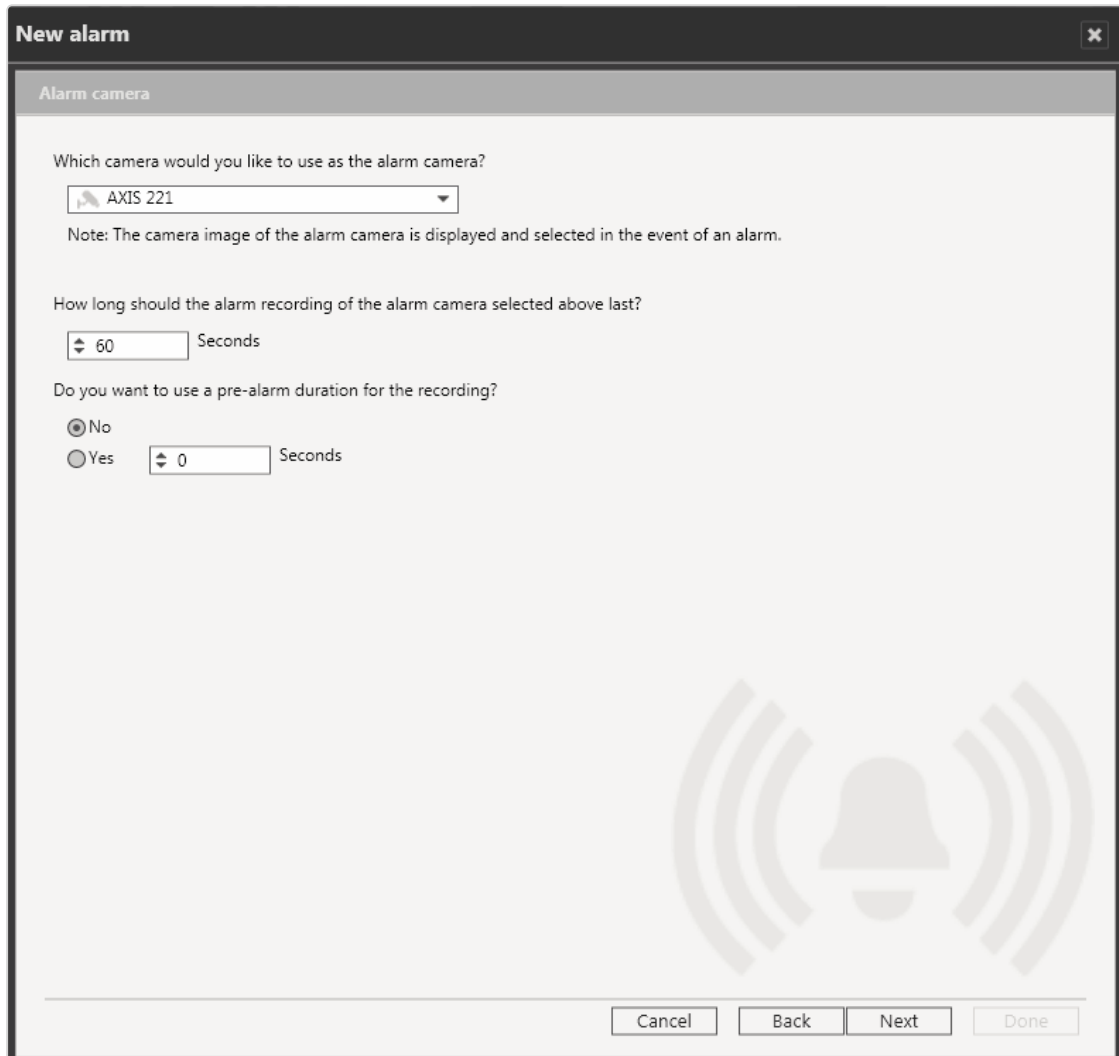


Abb. 207: Alarmer - Ereignisse

1. Aktivieren Sie die Objekte, die ein Alarmereignis auslösen.
2. Klicken Sie auf **Weiter**.

Alarmkamera



The screenshot shows a 'New alarm' configuration window with the following elements:

- Title:** New alarm
- Section:** Alarm camera
- Question:** Which camera would you like to use as the alarm camera?
- Input:** A dropdown menu showing 'AXIS 221'.
- Note:** Note: The camera image of the alarm camera is displayed and selected in the event of an alarm.
- Question:** How long should the alarm recording of the alarm camera selected above last?
- Input:** A spinner box set to '60' followed by the text 'Seconds'.
- Question:** Do you want to use a pre-alarm duration for the recording?
- Options:** Radio buttons for 'No' (selected) and 'Yes'.
- Input:** A spinner box set to '0' followed by the text 'Seconds'.
- Buttons:** Cancel, Back, Next, Done.
- Background:** A faint watermark of a bell icon with sound waves.

Abb. 208: Alarme - Alarmkamera

1. Wählen Sie die Kamera aus, die als Alarmkamera angezeigt werden soll und legen Sie die Dauer der Alarmaufzeichnung fest (in Sekunden).
2. Wählen Sie, ob Sie eine Voralarmdauer hinzufügen möchten, und geben Sie die Dauer in Sekunden an.
3. Klicken Sie auf **Weiter**.

Beteiligte Benutzer

The screenshot shows a window titled "New alarm" with a close button (X) in the top right corner. Below the title bar is a section header "Users involved". The main content area contains the following text and controls:

Which users should be notified in the event of an alarm?

- Select all
- administrator
- User
- administrator group
- Patrol

Are the selected users to be notified by means of a message window in the event of an alarm?

No
 Yes

At the bottom right of the window, there are four buttons: "Cancel", "Back", "Next", and "Done". A large, faint bell icon with sound waves is visible in the background of the window.

Abb. 209: Alarmer - Beteiligte Benutzer

1. Legen Sie fest, welcher Benutzer durch ein Alarmereignis benachrichtigt werden soll. Die Benutzer müssen zuvor im Steuerelement Benutzer angelegt worden sein (siehe „Benutzer“ auf Seite 357).
2. Legen Sie fest, ob die Benutzer bei einem Alarmereignis durch eine Alarmbenachrichtigung (siehe „Alarmermeldungen“ auf Seite 170) informiert werden sollen.
3. Falls die Benutzer durch ein Meldungsfenster benachrichtigt werden sollen, geben Sie eine kurze Nachricht an.
4. Klicken Sie auf **Weiter**.

Zusammenfassung

Summary	
Title	New alarm
Events	0
Alarm camera	AXIS 221
Duration of alarm recording	60
Pre-alarm duration	0
Users involved	4
Message window	No
Additional text for the message window	

Cancel Back Next Done

Abb. 210: Alarme - Zusammenfassung

1. Überprüfen Sie die Einstellungen.
2. Um Änderungen vorzunehmen, wählen Sie **Zurück** und passen Sie die Einstellungen an.
3. Um die Einstellungen zu übernehmen, wählen Sie **Fertig**.

Alarm konfigurieren

1. Wählen Sie den Alarm in der Alarmübersicht aus.

Allgemein

General

Activated

Name:

Description:

Priority:

 Low (10) (8) High (1)

 This alarm does not need to be confirmed by the user.

Validity:

Color in alarm list: Default

Settings:

 Only remove alarm when it is ended and confirmed

 Automatically start new alarm on clients

Settings for low-priority alarms:

 Terminate alarm on clients when terminated on server

 Start new alarm on clients if another low-priority alarm is active

 Do not close layers automatically at end of alarm

PTZ priority: 1=highest ... 1000=lowest

Timeout (s) for PTZ priority actions:

The alarm scenario is initiated as a test alarm. If you have made any changes to the configuration, choose "Apply" to save the changes before you click the button.

Abb. 211: Alarmer - Allgemein

1. Aktivieren oder deaktivieren Sie das Alarmszenario.
2. Passen Sie gegebenenfalls den **Namen** des Alarms an.
3. Geben Sie eine **Beschreibung** ein.
4. Weisen Sie dem Alarm mit dem Schieberegler eine **Priorität** zu. Die Bedeutung der jeweiligen Prioritätsstufe wird angezeigt. Ein Alarm mit niedriger Priorität kann nach dem Alarmende sofort beendet werden. Alle dynamisch geöffneten Elemente (Ansichten, Kameras und Meldungsfenster) werden wieder geschlossen und die vorherige Ansicht wird wiederhergestellt. Alarmer mit mittlerer/hocher Priorität werden erst nach ihrer Bestätigung beendet. Dies ist in den Einstellungen für niedrigprioritäre Alarmer konfigurierbar (s. u.).
5. Wählen Sie den **Gültigkeitszeitraum** für den Alarm aus. Der Alarm ist nur innerhalb des angegebenen Gültigkeitszeitraums aktiv. Die möglichen Zeiträume werden in der Zeitverwaltung festgelegt (siehe „Zeitverwaltung“ auf Seite 381).
6. Wählen Sie die **Farbgebung in der Alarmliste** aus. Die Alarmer werden in der Alarmliste im Überwachungsmodus und im Archivmodus in der ausgewählten Farbe angezeigt.

7. Aktivieren Sie **Alarm erst entfernen, wenn er beendet und bestätigt ist**, um den Alarm erst dann aus der Liste zu entfernen, wenn sein Status auf „bestätigt“ gesetzt und der Alarm beendet wurde (siehe „[Alarmliste und Systemmeldungen](#)“ auf Seite 170).
8. Deaktivieren Sie **Neuen Alarm auf Client automatisch starten**, um zu verhindern, dass durch den Alarm Ereignisse gestartet werden. Wenn die Option deaktiviert ist, muss der Benutzer die zugeordneten Alarmereignisse manuell starten.
9. Aktivieren Sie die **Einstellungen für die niedrigprioräre Alarme**.
10. **Alarm auf Clients beenden, wenn er serverseitig beendet wird**: Der Alarm wird auf allen beteiligten Clients beendet und aus der Alarmliste entfernt.
11. **Neuen Alarm auf Clients starten, wenn anderer niedrigpriorärer Alarm aktiv ist**: Ein niedrigpriorärer Alarm verdrängt einen anderen aktiven niedrigpriorären Alarm. Das heißt, der aktuelle Alarm wird zurückgestellt und der neue Alarm wird angezeigt.
12. **Ansichten bei Alarmende nicht automatisch schließen**: Verhindert, dass die Ansicht beim Alarmende automatisch geschlossen wird. Außerdem bleiben dadurch die Alarmkameras fokussiert auf die Alarmkachel, selbst wenn der Alarm deaktiviert wird.
13. Setzen Sie den Zähler **PTZ-Priorität** auf einen Wert zwischen 1 und 1000 (je höher die Zahl, desto niedriger die Priorität) und geben Sie das Timeout für PTZ-Prioritätsaktionen in Sekunden an. Wenn der Alarm keine PTZ-Steuerungen aktiviert, wird die Kamerasteuerung nach der Zeitüberschreitung (Timeout) wieder freigegeben.

Bei Übernahme der Steuerung der Kamera kann ein Benutzer (oder ein Alarm oder eine Serversequenz) mit einer höheren PTZ-Priorität einen anderen Benutzer (bzw. einen anderen Alarm oder eine andere Serversequenz) übersteuern.

Start

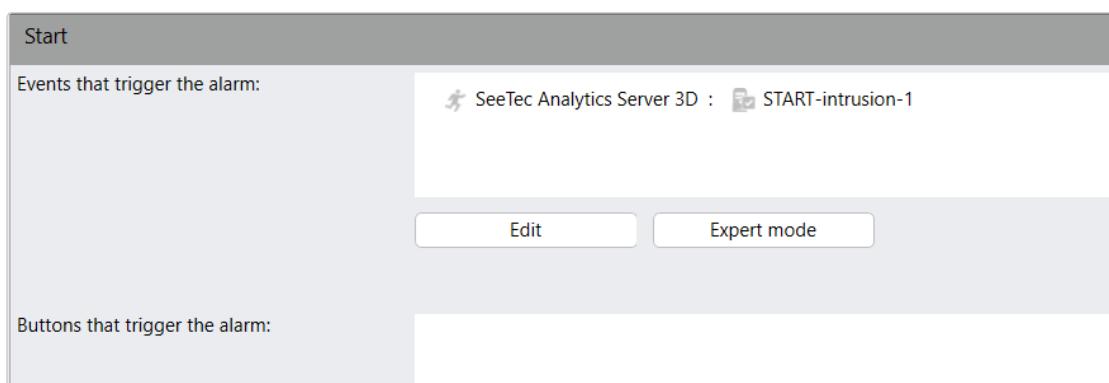
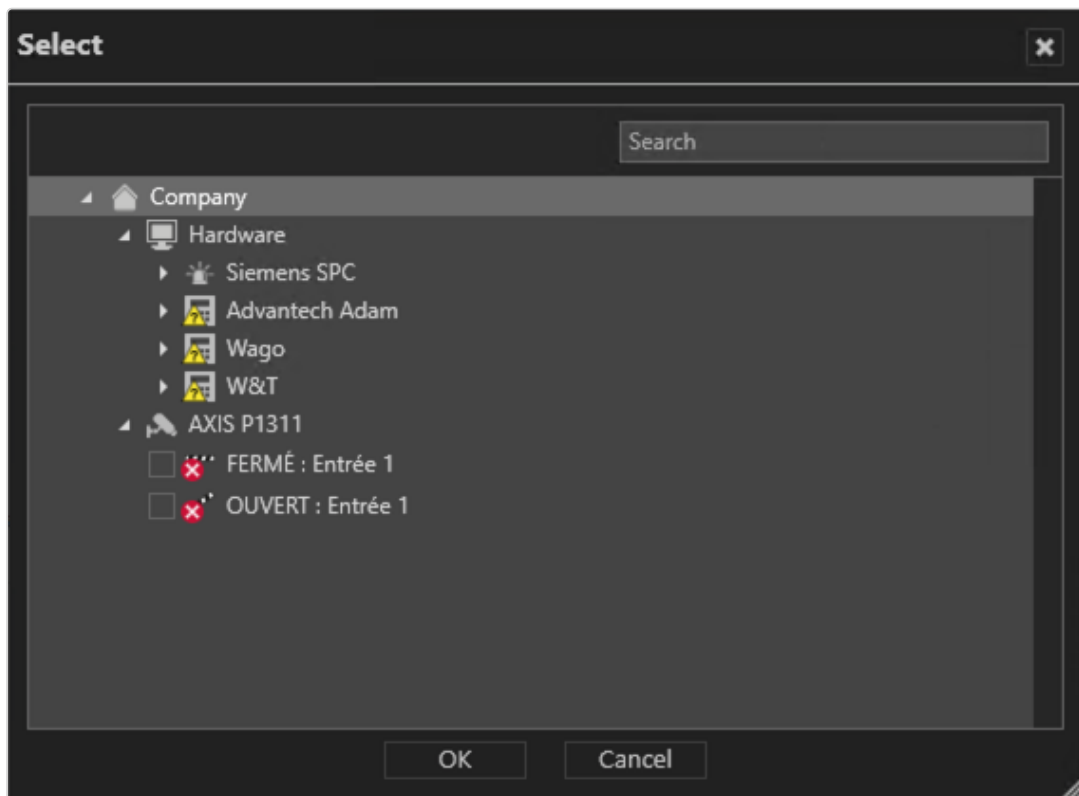


Abb. 212: Alarme - Start

Abhängig vom verwendeten Kameramodell oder von der sonstigen Hardware können folgende Ereignisse als Auslöser für ein Alarmszenario verwendet werden:

- Manipulation: Der Kamerablickwinkel wird verändert oder das Objektiv der Kamera wird verdeckt.
- Verlust des Videosignals: Die Verbindung zwischen analoger Kamera und Video-server ist unterbrochen.
- Bewegungserkennung: In einem definierten Bereich des Kamerabilds sind signifikante Bewegungen erkannt worden.
- Digital I/O: Ein eintreffendes digitales Signal löst einen Alarm aus.
- VoIP-Ereignisse wie Starten oder Stoppen einer VoIP-Sitzung
- Auslöser von externen Schnittstellen wie Zutrittskontrollsystemen oder Alarmsystemen

1. Klicken Sie zur Auswahl der **Ereignisse, die den Alarm auslösen** auf **Bearbeiten**. Die Hardware und das Ereignis werden angezeigt. Sie können mehrere Objekte auswählen.



Diese Auslöser müssen Sie vor der Konfiguration des Alarmszenarios erstellen oder aktivieren. Eine Ausnahme hierbei sind Buttons, die Sie nachträglich im Steuerelement Buttons definieren können (siehe „Buttons“ auf Seite 416). Ein Starterereignis kann z. B. das Eingehen eines TCP-Signals von einer Kamera sein, wenn diese eine Bewegung erkennt. Dies wird über den Qognify Network I/O realisiert.

2. Klicken Sie auf **Expertenmodus**, um die Einstellungen zu präzisieren.

Expertenmodus

Der Expertenmodus ermöglicht Ihnen, komplexe Alarmszenarios zu erstellen. Der Alarm wird erst durch verschiedene Bedingungen ausgelöst, die logisch miteinander verknüpft sind (UND-/ODER-Bedingungen).

Start

The alarm is not triggered unless the following conditions are met at the inputs

AXIS 221 : OPEN: input 1

Edit

and if within the following period (s)

0

At least one event from each of the following groups occurs

Hamburg 01 : Voice over IP start

Edit

and

AXIS P1357 Analytics 3d : OPEN: input 1
AXIS P1357 Analytics 3d : Tampering

Edit

and

Edit

Buttons that trigger the alarm:

Abb. 213: Alarmer - Expertenmodus

1. Klicken Sie auf **Bearbeiten** und wählen Sie die Bedingungen an den (digitalen) Eingängen aus, die erfüllt sein müssen, um einen Alarm auszulösen.
2. Bestimmen Sie den **Zeitraum** (in Sekunden), an dem mindestens eines der folgenden Ereignisse aus jeder Gruppe auftritt.

- Um die Ereignisse zu der Bedingung hinzuzufügen, klicken Sie auf **Bearbeiten** und wählen Sie die entsprechenden Objekte aus.

Ende

End

Maximum server alarm duration (s):

Events that terminate the alarm:

Adam : CLOSED: input 3

Edit

Buttons that terminate the alarm:

Abb. 214: Alarmer - Ende

- Geben Sie die **Maximale Server-Alarmdauer** (in Sekunden) an, um festzulegen, wie lange der Alarm aufgezeichnet werden soll.
- Klicken Sie zur Auswahl der **Ereignisse, die den Alarm vorzeitig beenden** auf **Bearbeiten**. Die Hardware und die Ereignisse werden angezeigt.

Visualisierung

Im Bereich Visualisierung können Sie festlegen, wie Alarmer auf dem Client dargestellt werden.

Visualization					
Cameras and layers	Alarm camera	Alarm view	Window mode	Window	Digital preset
AXIS 221	<input type="checkbox"/>	<input type="checkbox"/>	None	0	
AXIS P1311 Multi	<input type="checkbox"/>	<input type="checkbox"/>	None	0	
AXIS P1357 Analytics 3d	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Normal	1	
kam M	<input type="checkbox"/>	<input type="checkbox"/>	None	0	
Motion Detection Cam 1	<input type="checkbox"/>	<input type="checkbox"/>	None	0	
P1357 analytics personen	<input type="checkbox"/>	<input type="checkbox"/>	None	0	
<input type="checkbox"/> 1			None	0	
<input type="checkbox"/> 1+3			None	0	
<input type="checkbox"/> New layer			None	0	
<input type="checkbox"/> ud			None	0	

Abb. 215: Alarmer - Visualisierung

Es gibt drei Arten der Darstellung, die Sie auch kombinieren können:

- **Alarmkamera:** Die Alarmkamera wird in den jeweiligen Fenstern im Überwachungsmodus mit einem roten Rahmen gekennzeichnet.
- **Alarmansichten:** Die Alarmaufzeichnungen der gewählten Kamera werden im gewählten Fenster in vier Kacheln in einer 2x2-Ansicht angezeigt: Voralarm, Nachalarm, Alarmbild (Standbild) und Live-Bild.
- **Ansichten:** Ansichten können mehrere Kameras beinhalten, die in Kacheln angeordnet sind. Sie können auch Lagepläne enthalten (siehe „[Ansichten](#)“ auf [Seite 404](#)).

Ein Alarm mit niedriger Priorität wird nach dem Alarmende sofort beendet, d. h., alle dynamisch geöffneten Elemente (Ansichten, Kameras und Meldungsfenster) werden wieder geschlossen und die vorherige Ansicht wird wiederhergestellt. Alarme mit mittlerer/hocher Priorität werden erst nach ihrer Bestätigung beendet.

1. Aktivieren Sie die **Kameras und Ansichten**, die auf den jeweiligen Fenstern im Überwachungsmodus angezeigt werden sollen. Der Fenstermodus wird automatisch auf die **Normalansicht** gestellt.
2. Legen Sie fest, ob die Kameras als Alarmkamera und/oder in der Alarmansicht angezeigt werden sollen.
3. Wählen Sie den **Fenstermodus** zwischen **normalem** Modus und **Vollbildmodus** aus.
4. Wählen Sie die Option **Fenster** aus, um die Kamera bzw. Ansicht im Hauptfenster oder in einem Nebenfenster anzeigen zu lassen.

Diese Option ist nur verfügbar, wenn der Fenstermodus nicht auf „Keiner“ festgelegt ist.

5. Wählen Sie die Option **Digitales Preset** aus, um ein digitales Preset anzuzeigen (siehe „[Kamerapositionen/Digitale Presets](#)“ auf [Seite 271](#)).

Diese Option ist nur verfügbar, wenn der Fenstermodus nicht auf „Keiner“ festgelegt ist.

Kameras und Ansichten sowie Alarmkameras können nicht im selben Fenster angezeigt werden.

Beteiligte Personen

Persons involved

Profiles:

- administrator
- Max
- administrator group
- Nightwatch

Message window:

Play signal tone: When the alarm is activated

Use custom alarm sound:

Loop sound:

Run external program: Select

Additional parameters:

Abb. 216: Alarmer - Beteiligte Personen

Die Alarmer werden nur für die gewählten Profile angezeigt.

Für die Funktion „Alarm-Watchdog“ (siehe „[Der Alarm-WatchDog](#)“ auf [Seite 573](#)) müssen die in den Systemeinstellungen festgelegten Benutzer aktiviert werden.

1. Wählen Sie für **Profile** die Benutzer oder Gruppen, die den Alarm sehen dürfen.

Die Visualisierung des Alarms ist auch vom Benutzerprofil bzw. von den Gruppenprofilen abhängig (siehe „[Profile](#)“ auf [Seite 375](#)).

2. Geben Sie für Alarmer mit mittlerer oder hoher Priorität im Meldungsfenster einen Text ein. Dieser Text wird im **Meldungsfenster** angezeigt.

3. Aktivieren Sie **Signalgeräusch abspielen** und wählen Sie aus, ob das Signalgeräusch bei der Aktivierung des Alarms durch das Alarmszenario oder beim manuellen Auslösen des Alarms durch den Benutzer abgespielt werden soll.

Das Alarmgeräusch befindet sich im Dateisystem im „<Installationsverzeichnis>/Client/Sound“ oder „<Installationsverzeichnis>/Client64/Sound“ und kann gegen andere *.wav-Dateien ausgetauscht werden.

4. Optional können Sie einen benutzerdefinierten Alarmton wählen (siehe „[Ton- und Symboldateien mit benutzerdefinierten Medien verwalten](#)“ auf Seite 482).
5. Optional können Sie den Ton als Endlosschleife abspielen lassen.
6. Aktivieren Sie **Externes Programm ausführen**, wenn gleichzeitig mit dem Alarm ein Programm gestartet werden soll, und wählen Sie, welches Dokument von dem Programm geöffnet werden soll. Das ausgewählte Programm muss auf dem jeweiligen Client-PC installiert sein.
7. Geben Sie **Zusätzliche Parameter** ein, die für das Programm erforderlich sind. Damit kann beispielsweise ein Dokument mit Hilfe des gewählten Programms geöffnet werden.

Server

The screenshot shows a configuration window titled 'Server'. It contains the following elements:

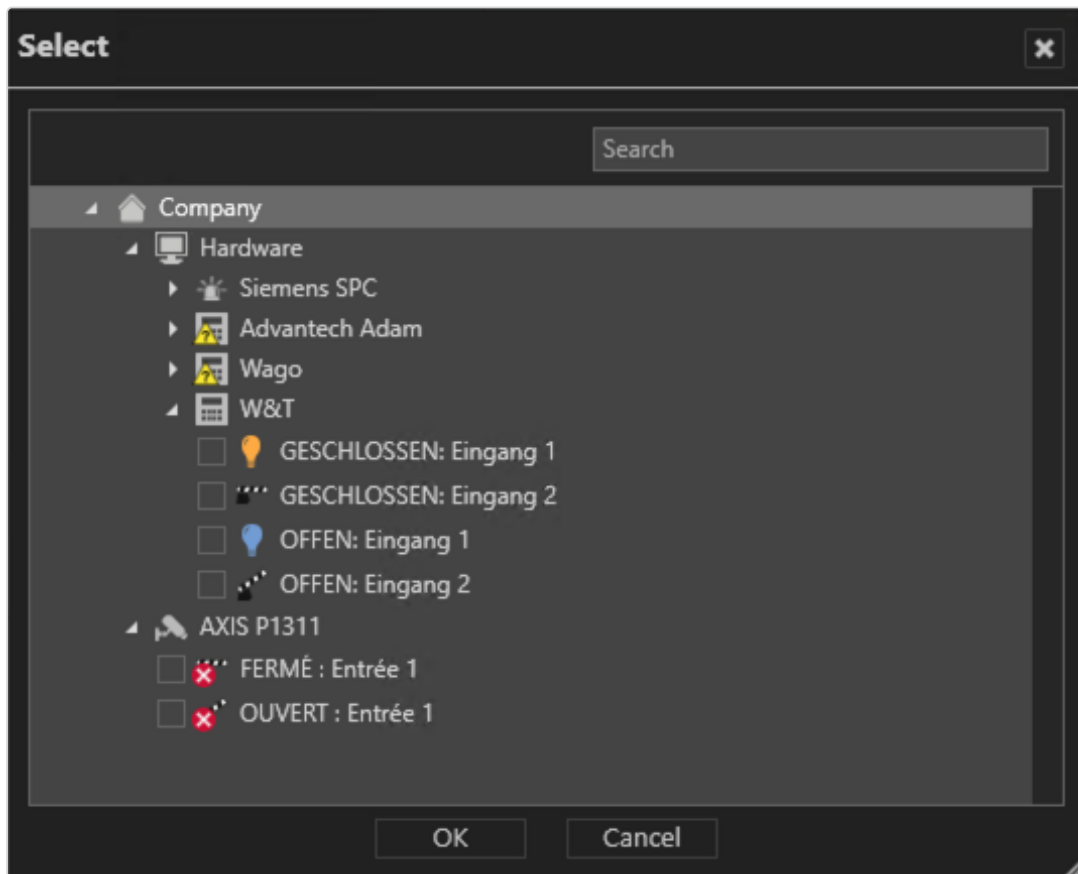
- Pre-alarm duration for camera recordings (s):** A numeric input field with a value of 10 and a spinner control.
- Use separate frame rate (fps) for camera recordings:** A checkbox that is currently unchecked, followed by an empty numeric input field.
- Actions at start of alarm:** A list of actions, each with a camera icon and a document icon:
 - AXIS P1357 Analytics 3d : Start alarm recording
 - P1357 analytics personen : Start alarm recording
- Actions at end of alarm:** An empty list area.
- Edit button:** A button located at the bottom right of the actions list.

Abb. 217: Alarmer - Server

1. Geben Sie die **Voralarmdauer für Kameraaufzeichnungen** (in Sekunden) an (maximal 3600 s), um bei einer Alarmaufzeichnung einen Zeitraum vor der Alarmauslösung aufzuzeichnen.

Wenn die Standardaufzeichnung deaktiviert ist, wird die maximale Aufzeichnungsdauer durch die Voralarm-Pufferzeit begrenzt (siehe Konfiguration der „**MultimediaDatabase**“ auf Seite 505).

2. Aktivieren Sie **Eigene Bildrate (fps) für Kameraaufzeichnungen verwenden** und geben Sie die gewünschte Bildrate ein. Eine Änderung der Bildrate ist nur bei M-JPEG möglich.
3. Wählen Sie **Bearbeiten** und aktivieren Sie die **Aktionen bei Alarmstart**. Die gewählten Aktionen werden angezeigt.



4. Wählen Sie **OK**.
5. Wählen Sie **Bearbeiten** und aktivieren Sie die **Aktionen bei Alarmende**. Die gewählten Aktionen werden angezeigt.

Folgende Alarmaktionen sind verfügbar:

■ Hardware

- Ausgänge an I/O-Modulen von Network I/Os von Adam, Axis, W&T, Wago oder Qognify usw. können geöffnet oder geschlossen werden.

Die Ausgänge müssen an den betreffenden Modulen aktiviert werden.

- Die Kennzeichenerkennung kann an LPR-Modulen gestartet werden.

■ Servergesteuerte Sequenzen können gestartet oder unterbrochen werden (siehe „Sequenzen“ auf Seite 426).

■ Server Der Videodaten-Export kann von Device Managern gestartet werden (siehe „Video-Backup“ auf Seite 442).

■ Systemverwaltung

- Eine SNMP-Aktion kann für einen konfigurierten SNMP-Server ausgelöst werden (siehe „SNMP-Server konfigurieren“ auf Seite 477).
- Eine Alarm-Watchdog-Aktion kann ausgelöst werden, um den Alarm im Alarm-Watchdog anzuzeigen (siehe „Der Alarm-WatchDog“ auf Seite 573).
- Eine Benachrichtigung kann an die EBÜS-Anbindung gesendet werden.

■ Kameras

- Alarmaufzeichnungen können gestartet oder gestoppt werden.
- Preset-Positionen können ausgelöst werden.
- Ausgänge können geöffnet oder geschlossen werden.

E-Mail und FTP

Email and FTP

Subject: Alarm at Front door

Message:

Notify the following recipients when the alarm starts:

Send to: alarmnotification@some.dd

Notify the following recipients at end of alarm:

Send to: alarmnotification@some.dd

Attach data from the following cameras to the emails at end of alarm:

AXIS P1357 Analytics 3d
 P1357 analytics personen

Data format: Video

Transmit data from the following cameras to the FTP server at the end of the alarm:

AXIS P1357 Analytics 3d
 P1357 analytics personen

Data format: Single-image sequence

Abb. 218: Alarmer - E-Mail und FTP

Der SMTP-Server für E-Mails und die E-Mail-Adressen müssen im Steuerelement System angelegt worden sein, damit das System die Nachrichten weiterleiten kann (siehe „SMTP-Server konfigurieren“ auf Seite 476).

Im Fall eines Alarms kann zusätzlich zur Alarmmeldung auch eine standardisierte E-Mail gesendet bzw. ein Datenexport auf einen FTP-Server festgelegt werden.

1. Geben Sie den **Betreff** und den Text der **Nachricht** der E-Mail ein.
2. Aktivieren Sie die **Empfänger**, die bei Alarmstart bzw. Alarmende die E-Mail erhalten sollen. Die E-Mail-Adressen können Sie im Bereich „Alarm-Adressen und System-Adressen“ in den Einstellungen zum System angeben (siehe „Alarm-Adressen und System-Adressen“ auf Seite 477).

3. Aktivieren Sie **Bei Alarmende Daten von folgenden Kameras an die E-Mails anhängen**, um festzulegen, welche Kameradaten an die E-Mails angehängt werden sollen, und wählen Sie das **Datenformat** aus. Zwei Datenformattypen sind möglich:

- Video: Die Dateien werden unverschlüsselt im *.avi-Format gesendet (siehe [„Video-Backup/-Export“ auf Seite 274](#)).
- Einzelbildsequenz: Die Dateien werden als Bildsequenz (JPEG) gesendet.

Beachten Sie, dass die E-Mail-Anhänge die zulässige Größe der E-Mail überschreiten können.

4. Aktivieren Sie die Kameras, deren Daten bei größeren Datenmengen auf einem FTP-Server abgelegt werden, und legen Sie das **Datenformat** fest. Der FTP-Server wird im Qognify VA Administrationstool (siehe [„Qognify VMS VA Administrationstool“ auf Seite 513](#)) festgelegt.

Wenn Probleme beim FTP-Versand bei Alarmende auftreten, z. B. der FTP-Server nicht erreichbar ist, wird einmal pro Minute versucht, die Daten erneut auf dem FTP-Server zu speichern. Nach einer Stunde wird der Versuch abgebrochen und die Daten werden verworfen.

5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Alarm löschen

1. Wählen Sie den Alarm in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Alarm duplizieren

1. Wählen Sie den Alarm in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für den duplizierten Alarm ein.

3. Falls Sie den neuen Alarm mithilfe des Konfigurationsassistenten einstellen möchten, wählen Sie **Assistent** im Dialogfenster (siehe „[Alarmszenario mit dem Assistenten anlegen](#)“ auf Seite 387).
4. Bestätigen Sie den Namen mit **OK**. Der neue Alarm wird in der Übersicht angezeigt.

Ansichten

Mit der Funktion **Ansichten** im Steuerelement Administration können Sie die Arbeitsfläche im Überwachungsmodus Ihren Bedürfnissen anpassen, indem Sie die Arbeitsfläche in mehrere „Kacheln“ aufteilen. Der Benutzer erhält damit festgelegte Anordnungen und Inhalte der Arbeitsfläche. Diese Ansichten können einem Benutzer- oder Gruppenprofil zugeordnet werden und stehen nach dem Programmstart zur Verfügung.

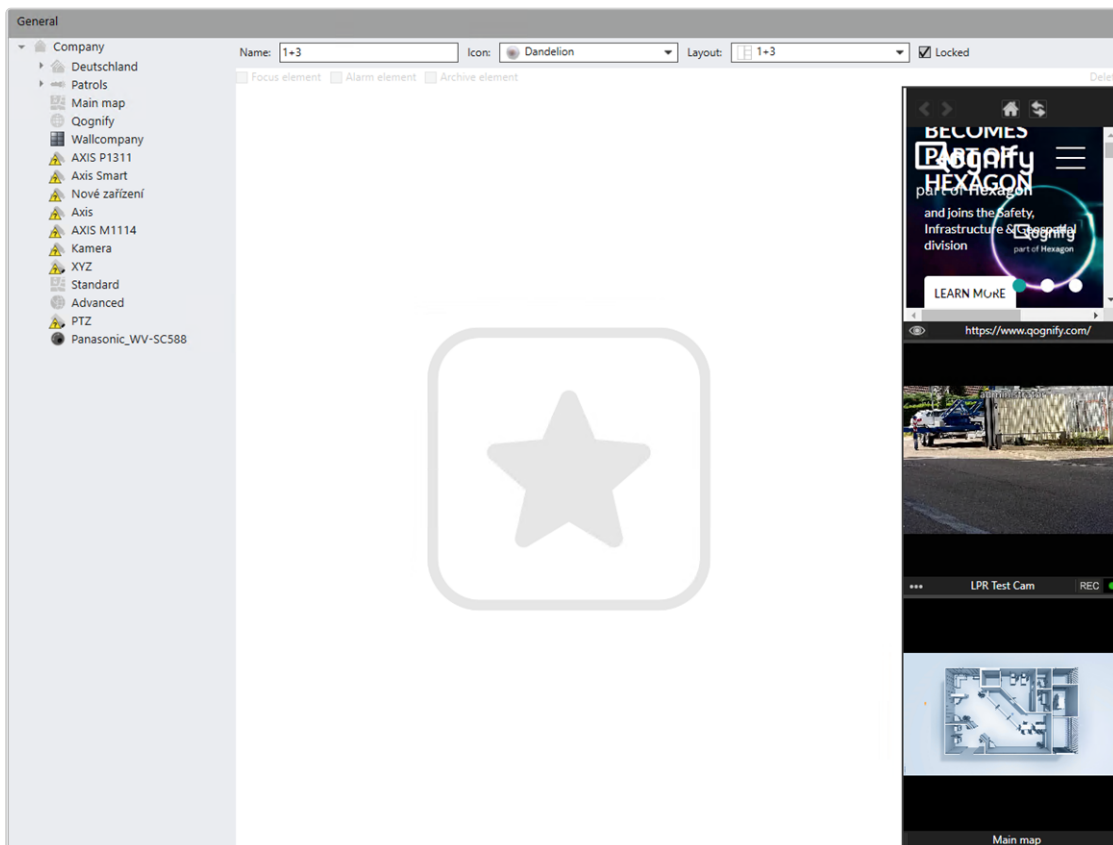



Abb. 219: Ansichten

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Ansichten** im Steuerelement Administration.

Neue Ansicht anlegen

1. Wählen Sie in der Ansichten-Steuerleiste die Option **Objekt neu anlegen**  aus.
2. Geben Sie den **Namen** der neuen Ansicht ein.
3. Wählen Sie den **Typ** des Layouts aus.
4. Um die Anzahl der Kacheln selbst festzulegen, wählen Sie im Aufklappmenü **Benutzerdefiniert**.
5. Bestätigen Sie die Einstellung mit **OK**. Die neue Ansicht wird in der Übersicht angezeigt.
6. Falls Sie **Benutzerdefiniert** gewählt haben, passen Sie die Anzahl der Reihen und Spalten der Ansicht an. Es stehen maximal 100 Felder zur Verfügung (64 x 1 oder 9 x 7).
7. Ziehen Sie den Mauszeiger über eine beliebige Anzahl nebeneinander liegender Kacheln und klicken Sie auf **Verbinden**, um die ausgewählten Kacheln zu einer Kachel zusammenzufassen.
8. Klicken Sie auf eine zusammengefasste Kachel und klicken Sie auf **Trennen**, um die ursprüngliche Anzahl an Kacheln wiederherzustellen.
9. Bestätigen Sie die Einstellung mit **OK**. Die neue Ansicht wird in der Übersicht angezeigt.

Ansicht konfigurieren

1. Wählen Sie die Ansicht in der Übersicht aus.
2. Ändern Sie gegebenenfalls den **Namen** der Ansicht an.
3. Wählen Sie im Aufklappmenü ein **Symbol** für die Ansicht aus. Das ausgewählte Symbol wird in der Übersicht im Überwachungsmodus angezeigt.
4. Wählen Sie im Aufklappmenü ein **Layout** aus. Das gewählte Layout wird angezeigt.
5. Um eine Ebene zu entsperren, deaktivieren Sie die Option **Gesperrt**. Dadurch wird die aktuelle Ebene entsperrt und Sie können das Layout ändern. Um Änderungen zu verhindern, ist die Ebene standardmäßig gesperrt.

6. Ziehen Sie die gewünschten Kameras, Wächterrundgänge oder Webseiten entsprechend der gewählten Anordnung in das Ansichtsfenster.


Alle Elemente des ausgewählten Rundgangs, mit Ausnahme der Kameraoperationen, werden in der Ansicht ignoriert.

7. Klicken Sie auf eine Kachel mit einer Kamera und aktivieren Sie die Option **Fokuskachel**. Sie können in jeder Ansicht eine Kachel als Fokuskachel markieren. Wenn Sie in einer Ansicht mit Fokuskachel auf eine Kamera doppelklicken, wird das Kamerabild in der Fokuskachel angezeigt. Wenn Sie in einer Ansicht ohne Fokuskachel zweimal auf eine Kamera klicken, wird das Kamerabild in einer eigenen Ansicht angezeigt.
8. Klicken Sie auf eine Kachel mit einer Kamera und aktivieren Sie die Option **Alarmelement**. Wenn die Ansicht bei Aktivierung eines Alarms sichtbar ist, werden die Alarmkameras in sequenzieller Reihenfolge auf die Alarmkacheln umgeschaltet.
 - Unter „Alarm konfigurieren“ wird beschrieben, wie Alarmkameras mit der Option „Ansichten bei Alarmende nicht automatisch schließen“ auf die Alarmkachel fokussiert gehalten werden, selbst wenn der Alarm deaktiviert wird (siehe „[Alarm konfigurieren](#)“ auf Seite 391.)

Wenn die Anzahl der Alarmkameras in einem Alarm die Anzahl der sichtbaren Alarmkacheln übersteigt, werden die restlichen Alarmkameras ignoriert.

9. Klicken Sie auf eine Kachel mit einer Kamera und aktivieren Sie die Option **Archivelement**. Wenn Sie eine Ebene mit einem Archivelement öffnen, zeigt die Kamera Videomaterial der letzten 30 Sekunden an und eine aktive Archiv-Zeitleiste wird angezeigt. Wenn ein Alarm konfiguriert und aktiv ist, zeigt die Kamera die letzten 30 Sekunden vor dem Alarm an.
10. Um eine Kamera aus der Ansicht zu entfernen, markieren Sie die Kamera und klicken Sie auf **Löschen**.
11. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
12. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Ansicht löschen

1. Wählen Sie die Ansicht in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**  .

Ansicht duplizieren

1. Wählen Sie die Ansicht in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für die duplizierte Ansicht ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Ansicht wird in der Übersicht angezeigt.

Lagepläne und „Erweiterte Lagepläne“

Mit der Funktion **Lagepläne** im Steuerelement Administration können Sie die grafischen Übersichtskarten des überwachten Geländes bzw. Gebäudes einschließlich des Anbringungsorts der Überwachungs-Hardware konfigurieren und verwalten.

Sie können auf einem Lageplan interaktive Symbole, Kameras, Buttons, digitale Eingänge, Ansichten, Webseiten, Alarmer und andere Lagepläne platzieren. Die geografischen Koordinaten einer Kamera werden dazu verwendet, das Objekt auf einem Lageplan zu platzieren (siehe [„Geografische Koordinaten“ auf Seite 250](#)).

Die Symbole sind interaktiv, die Buttons können beispielsweise angeklickt werden, die Kameras können blinken, wenn sie als Alarmkameras definiert sind (siehe [„Visualisierung“ auf Seite 396](#)), Alarmer blinken, wenn sie aktiv sind, und Eingänge zeigen verschiedene Symbole zur Darstellung ihres aktuellen Zustands an (siehe [„Eingänge“ auf Seite 340](#)).

Erweiterte Lagepläne

Die Lageplan-Funktion unterstützt außerdem die Nutzung von Mapping-Diensten wie ESRI (Environmental Systems Research Institute), um alle Mapping-Daten bereitzustellen, ohne mehrere statische Lagepläne als Hintergründe anzulegen.

Für die Nutzung der Funktion „Erweiterte Lagepläne“ wird möglicherweise eine zusätzliche Lizenz des Mapping-Diensteanbieters benötigt, die in der Softwarelizenz nicht enthalten ist.

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Lagepläne** im Steuerelement Administration.

Neuen Lageplan anlegen

1. Klicken Sie auf **Objekt neu anlegen**.
2. Wählen Sie eine der folgenden Optionen:
 - Standardlageplan
 - Erweiterter Lageplan
3. Geben Sie den Namen für den neuen Lageplan ein.
4. Bestätigen Sie den Namen mit **OK**. Der neue Lageplan wird in der Übersicht angezeigt.

Konfiguration eines Standardlageplans

1. Wählen Sie den Standardlageplan in der Übersicht aus.

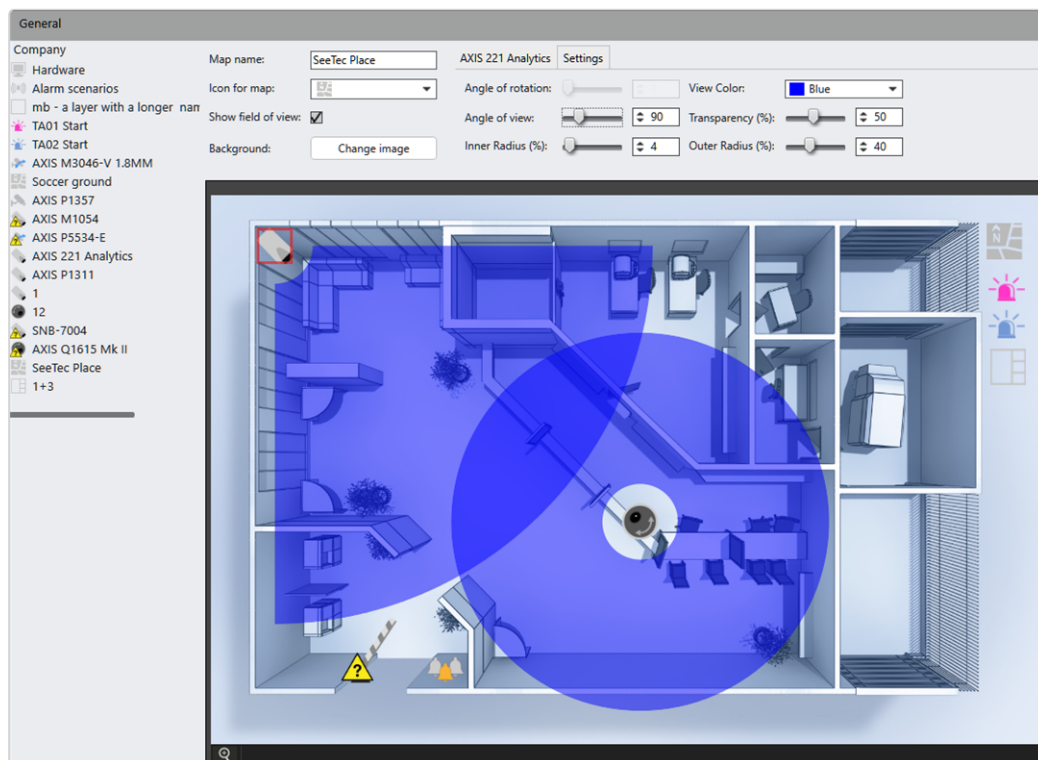


Abb. 220: Standardlageplan - Übersicht

2. Vergrößern bzw. verkleinern Sie den Lageplan durch Drehen des Mausekkrads.
3. Verschieben Sie den Lageplan mit den Scrollfeldern an eine bestimmte Position. Optional können Sie die Position des Lageplans mit gedrücktem Mausekkrad verschieben.
4. Ziehen Sie die verfügbaren Elemente vom Baum **Unternehmen**, wie Kameras, Eingänge, Buttons, Alarne usw., die für das gewünschte Areal erforderlich sind, aus der Liste auf den Hintergrund des Lageplans.

Allgemeine Einstellungen

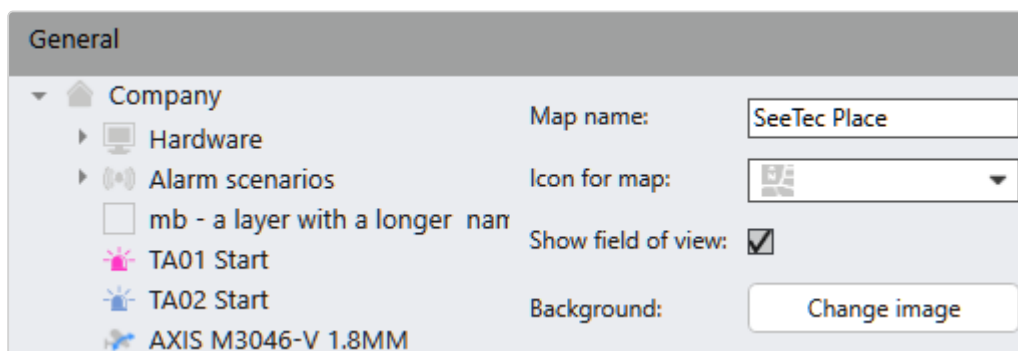


Abb. 221: Lagepläne - Allgemein

1. Ändern Sie bei Bedarf den Namen im Feld **Name Lageplan**.
2. Wählen Sie ein benutzerdefiniertes **Symbol für Lageplan** aus, sofern verfügbar (siehe „[Ton- und Symboldateien mit benutzerdefinierten Medien verwalten](#)“ auf Seite 482).
3. Aktivieren Sie **Blickfeld anzeigen**, um ein grafisches Blickfeld für auf dem Lageplan platzierte Kameras anzuzeigen bzw. auszublenden.
4. Klicken Sie auf **Bild ändern** und wählen Sie das gewünschte Hintergrundbild (z. B. Gebäudegrundriss) aus. Die folgenden Dateiformate sind möglich:
 - Bilder, wie z. B. JPG, GIF, PNG, BMP
 - Vektorgrafiken (auflösungsunabhängig): PDF

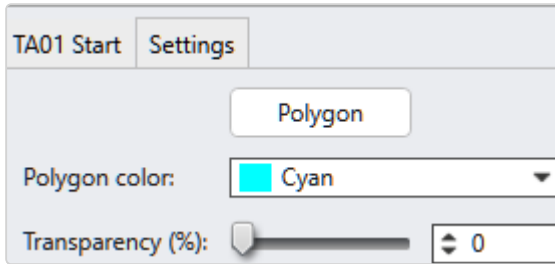
Wenn beim Ablegen eines neuen Symbols ein Symbol auf dem Lageplan markiert ist, werden für das neue Symbol die gleichen Einstellungen wie für das markierte Symbol übernommen.

Wenn beim Ablegen eines neuen Symbols kein Symbol auf dem Lageplan markiert ist, werden für das neue Symbol die Standardeinstellungen übernommen.

Kamerasymbol-Einstellungen

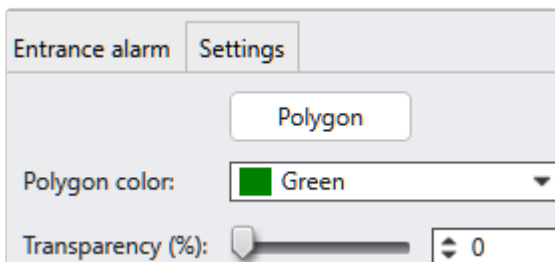
1. Klicken Sie auf dem Lageplan auf das Kamerasymbol, das Sie konfigurieren möchten. Wenn Sie mehrere Elemente auswählen möchten, halten Sie gleichzeitig die STRG-Taste gedrückt. Abhängig von der Auswahl können die folgenden kameraspezifischen Optionen geändert werden:
 - **Drehwinkel:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um den Drehwinkel des Symbols zu ändern. Diese Funktion ist verfügbar, wenn die Option „Winkel sperren“ in den allgemeinen Symboleinstellungen nicht aktiviert ist (siehe [Allgemeine Symboleinstellungen](#)).
 - **Blickwinkel:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Größe der Einblendung des Blickwinkels der Kamera zu ändern.
 - **Innenradius:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Visualisierung des toten Winkels der Kamera zu ändern.
 - **Anzeigefarbe:** Wählen Sie eine Farbe für die Einblendung des Blickwinkels der Kamera aus.
 - **Transparenz:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Transparenz der Einblendung des Blickwinkels der Kamera zu ändern.
 - **Außenradius:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um den Außenradius der Einblendung des Blickwinkels der Kamera zu ändern.

Buttonsymbol-Einstellungen



1. Klicken Sie auf dem Lageplan auf das Buttonsymbol, das Sie konfigurieren möchten. Wenn Sie mehrere Elemente auswählen möchten, halten Sie gleichzeitig die STRG-Taste gedrückt. Abhängig von der Auswahl können die folgenden Button-spezifischen Optionen geändert werden:
 - **Polygon:** Klicken Sie darauf, um die Funktion zu aktivieren. Zeichnen Sie dann den aktiven Bereich des Buttons ein, indem Sie auf die Eckpunkte des Polygons auf dem Lageplan klicken.
 - **Polygonfarbe:** Wählen Sie eine Farbe für die Einblendung des Polygons aus.
 - **Transparenz:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Transparenz der Einblendung des Polygons zu ändern.

Alarmsymbol-Einstellungen



1. Klicken Sie auf dem Lageplan auf das Alarmsymbol, das Sie konfigurieren möchten. Wenn Sie mehrere Elemente auswählen möchten, halten Sie gleichzeitig die STRG-Taste gedrückt. Abhängig von der Auswahl können die folgenden Button-spezifischen Optionen geändert werden:

- **Polygon:** Klicken Sie darauf, um die Funktion zu aktivieren. Zeichnen Sie dann den aktiven Bereich des Alarms ein, indem Sie auf die Eckpunkte des Polygons auf dem Lageplan klicken.
- **Polygonfarbe:** Wählen Sie eine Farbe für die Einblendung des Polygons aus.
- **Transparenz:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Transparenz der Einblendung des Polygons zu ändern.

Konfiguration eines erweiterten Lageplans

1. Wählen Sie den erweiterten Lageplan in der Übersicht aus.

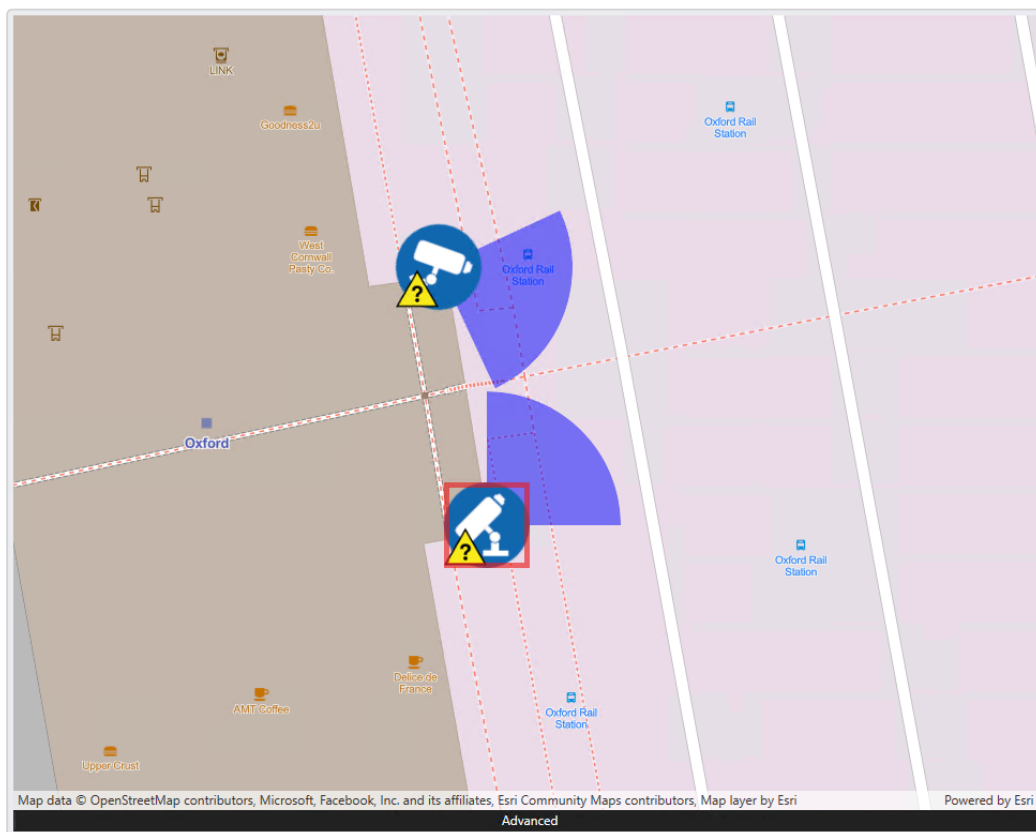


Abb. 222: Erweiterter Lageplan - Übersicht

2. Geben Sie die Geo-Koordinaten ein oder zoomen Sie in den Lageplan, indem Sie das Mausrad am gewünschten Standort drehen. Beim Zoomen passen sich die Koordinaten entsprechend an.

3. Verschieben Sie den Lageplan mit den Scrollfeldern an eine bestimmte Position. Optional können Sie die Position des Lageplans mit gedrücktem Mausrad verschieben.
4. Ziehen Sie die verfügbaren Elemente vom Baum **Unternehmen**, wie Kameras, Eingänge, Buttons, Alarmer usw., die für das gewünschte Areal erforderlich sind, aus der Liste auf den Hintergrund des Lageplans.

Allgemeine Einstellungen

Field	Value
Map name	Advanced
Icon for map	[Globe Icon]
URL	
X coordinate	-141345.03339348
Y coordinate	6755670.13008406
Scale	305
Show field of view	<input checked="" type="checkbox"/>

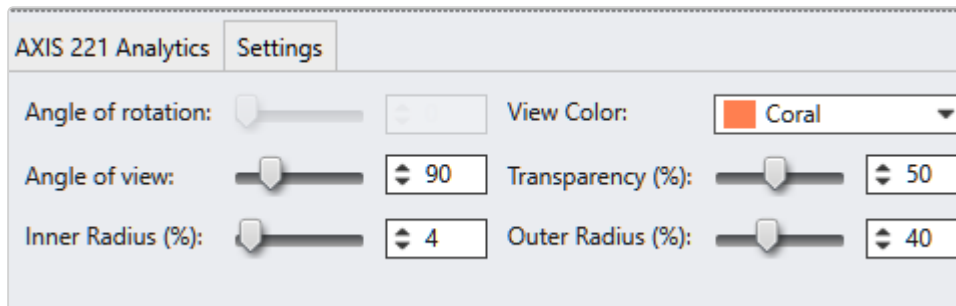
Abb. 223: Lagepläne - Allgemein

1. Ändern Sie bei Bedarf den Namen im Feld **Name Lageplan**.
2. Wählen Sie ein benutzerdefiniertes **Symbol für Lageplan** aus, sofern verfügbar (siehe „[Ton- und Symboldateien mit benutzerdefinierten Medien verwalten](#)“ auf Seite 482).
3. Anpassung der Geo-Koordinaten.
4. Anpassung des Skalierungsfaktors.. Je höher die Zahl, umso höher „über dem Boden“ ist die Aussicht.
5. Aktivieren Sie **Blickfeld anzeigen**, um ein grafisches Blickfeld für auf dem Lageplan platzierte Kameras anzuzeigen bzw. auszublenden.

Wenn beim Ablegen eines neuen Symbols ein Symbol auf dem Lageplan markiert ist, werden für das neue Symbol die gleichen Einstellungen wie für das markierte Symbol übernommen.

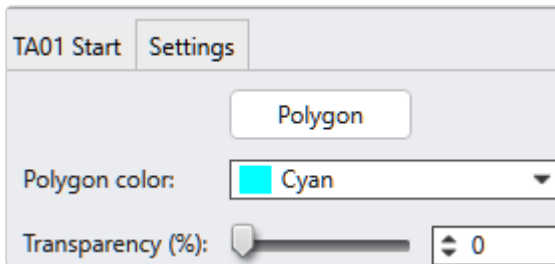
Wenn beim Ablegen eines neuen Symbols kein Symbol auf dem Lageplan markiert ist, werden für das neue Symbol die Standardeinstellungen übernommen.

Kamerasymbol-Einstellungen



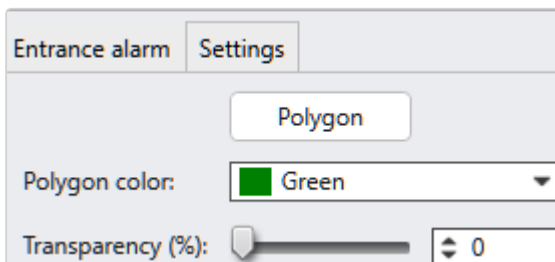
1. Klicken Sie auf dem Lageplan auf das Kamerasymbol, das Sie konfigurieren möchten. Wenn Sie mehrere Elemente auswählen möchten, halten Sie gleichzeitig die STRG-Taste gedrückt. Abhängig von der Auswahl können die folgenden kameraspezifischen Optionen geändert werden:
 - **Drehwinkel:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um den Drehwinkel des Symbols zu ändern. Diese Funktion ist verfügbar, wenn die Option „Winkel sperren“ in den allgemeinen Symboleinstellungen nicht aktiviert ist (siehe [Allgemeine Symboleinstellungen](#)).
 - **Blickwinkel:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Größe der Einblendung des Blickwinkels der Kamera zu ändern.
 - **Innenradius:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Visualisierung des toten Winkels der Kamera zu ändern.
 - **Anzeigefarbe:** Wählen Sie eine Farbe für die Einblendung des Blickwinkels der Kamera aus.
 - **Transparenz:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Transparenz der Einblendung des Blickwinkels der Kamera zu ändern.
 - **Außenradius:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um den Außenradius der Einblendung des Blickwinkels der Kamera zu ändern.

Buttonsymbol-Einstellungen



1. Klicken Sie auf dem Lageplan auf das Buttonsymbol, das Sie konfigurieren möchten. Wenn Sie mehrere Elemente auswählen möchten, halten Sie gleichzeitig die STRG-Taste gedrückt. Abhängig von der Auswahl können die folgenden Button-spezifischen Optionen geändert werden:
 - **Polygon:** Klicken Sie darauf, um die Funktion zu aktivieren. Zeichnen Sie dann den aktiven Bereich des Buttons ein, indem Sie auf die Eckpunkte des Polygons auf dem Lageplan klicken.
 - **Polygonfarbe:** Wählen Sie eine Farbe für die Einblendung des Polygons aus.
 - **Transparenz:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Transparenz der Einblendung des Polygons zu ändern.

Alarmsymbol-Einstellungen



1. Klicken Sie auf dem Lageplan auf das Alarmsymbol, das Sie konfigurieren möchten. Wenn Sie mehrere Elemente auswählen möchten, halten Sie gleichzeitig die STRG-Taste gedrückt. Abhängig von der Auswahl können die folgenden Button-spezifischen Optionen geändert werden:

- **Polygon:** Klicken Sie darauf, um die Funktion zu aktivieren. Zeichnen Sie dann den aktiven Bereich des Alarms ein, indem Sie auf die Eckpunkte des Polygons auf dem Lageplan klicken.
- **Polygonfarbe:** Wählen Sie eine Farbe für die Einblendung des Polygons aus.
- **Transparenz:** Verschieben Sie den Regler oder geben Sie einen Wert ein, um die Transparenz der Einblendung des Polygons zu ändern.

Lageplan löschen

1. Wählen Sie den Lageplan in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Lageplan duplizieren

1. Wählen Sie den Lageplan in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für den duplizierten Lageplan ein.
3. Bestätigen Sie den Namen mit **OK**. Der neue Lageplan wird in der Übersicht angezeigt.

Buttons

Mit der Funktion **Buttons** im Steuerelement Administration können Sie festgelegte Abläufe (Aktionen) wie beispielsweise Kameraaufzeichnungen oder Alarmszenarien starten.

Um die konfigurierten Buttons im Überwachungsmodus aufzurufen, muss in der Steuerleiste die Funktion Buttons aufgerufen werden (siehe „Buttons“ auf Seite 164).

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.

2. Wählen Sie **Buttons** im Steuerelement Administration.

Neuen Button anlegen

1. Legen Sie einen neuen Button an.
2. Geben Sie den **Namen** für den neuen Button ein.
3. Bestätigen Sie den Namen mit **OK**. Der neue Button wird in der Übersicht angezeigt.

Button konfigurieren

1. Wählen Sie den Button in der Übersicht aus.

Allgemein

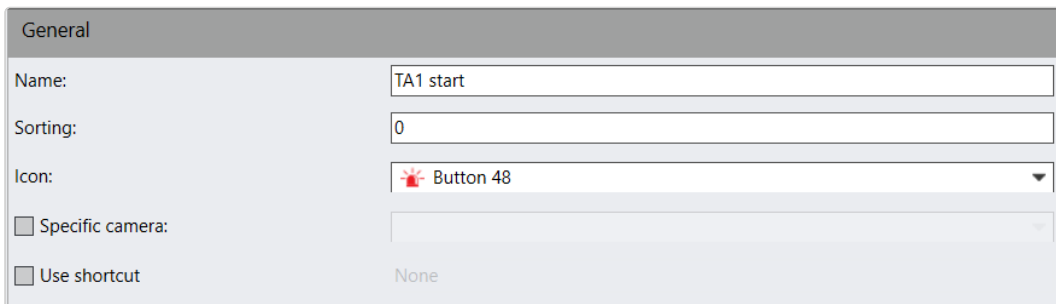


Abb. 224: Buttons - Allgemein

1. Passen Sie gegebenenfalls den **Namen** an.
2. Legen Sie die **Sortierung** der Buttons in der Steuerung im Überwachungsmodus fest (siehe „Buttons“ auf Seite 164). Die Buttons werden automatisch aufsteigend sortiert, d. h., je höher die Nummer eines Buttons, desto weiter unten in der Liste des Tabs wird der Button angezeigt.
3. Wählen Sie ein **Symbol** aus, um die Wiedererkennung zu vereinfachen.
4. Aktivieren Sie die Aktion für eine **bestimmte Kamera** und wählen Sie die Kamera aus. In diesem Fall wird der Button nur angezeigt, wenn die festgelegte Kamera im Überwachungsmodus ausgewählt ist.

5. Aktivieren Sie **Tastenkürzel verwenden** und drücken Sie die gewünschte Tastenkombination auf der Tastatur, um den Button mit einer Tastenkombination auszulösen. Die Tastenkombination wird angezeigt.

Die Standard-Tastenkombinationen können nicht überschrieben werden. Änderungen durch den Administrator werden ignoriert.

Aktion

The screenshot shows the 'Action' configuration window. The 'Call URL' option is selected, and the 'Test' button is visible. The 'Perform action' option is also visible, along with the 'Start alarm scenario' option which is currently selected and shows 'TA1' in the dropdown menu. The 'Terminate alarm scenario', 'Start patrol', and 'Run program' options are also present with their respective dropdown menus and 'Select' buttons.

Abb. 225: Buttons - Aktion

1. Wählen Sie die Option **URL aufrufen** und geben Sie die Internet- oder Intranetadresse ein. Mit dieser Adresse können beispielsweise Kamera-Scripts gestartet werden. Dazu wird keine Internet-/Intranet-Adresse angezeigt (zur Einbettung von Webseiten in die Ansicht, siehe [„Webseiten“ auf Seite 420](#)).
2. Wählen Sie **Testen**, um die Funktion der angegebenen URL zu prüfen.
3. Aktivieren Sie gegebenenfalls die Option **Beim Aufrufen der URL Autorisierung anwenden** und geben Sie den erforderlichen **Benutzernamen** und das **Passwort** ein, um Zugriff auf die URL zu erhalten.
4. Wählen Sie die Option **Aktion ausführen** und wählen Sie die entsprechende Aktion aus.

5. Falls eine zweite Aktion durchgeführt werden soll, aktivieren Sie **Weitere Aktion beim Loslassen ausführen** und wählen Sie die Aktion aus. Im Überwachungsmodus wird die Aktion ausgeführt, sobald Sie die Taste loslassen.
6. Wählen Sie die Option **Alarmszenario starten** und wählen Sie das Alarmszenario aus (siehe „[Alarmer](#)“ auf Seite 386).
7. Wählen Sie die Option **Alarmszenario beenden** und wählen Sie das Alarmszenario aus (siehe „[Alarmer](#)“ auf Seite 386).
8. Wählen Sie die Option **Wächterrundgang starten** und wählen Sie den Wächterrundgang aus (siehe „[Wächterrundgänge](#)“ auf Seite 422).
9. Wählen Sie die Option **Programm ausführen** und klicken Sie auf **Auswählen**, um ein Programm auszuwählen, das gestartet werden soll.

Der Dateipfad des ausgewählten Programms muss auf dem entsprechenden Client-PC aufgerufen werden können.

10. Geben Sie die für das Programm gegebenenfalls erforderlichen Parameter ein. Damit kann beispielsweise ein Dokument mit Hilfe des gewählten Programms geöffnet werden.
11. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
12. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Button löschen

1. Wählen Sie die Aktion in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Button duplizieren

1. Wählen Sie die Aktion in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für die duplizierte Aktion ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Aktion wird in der Übersicht angezeigt.

Webseiten

Mit der Funktion **Webseiten** im Steuerelement Administration können beliebige Webseiten in die Ansicht eingebettet werden, z. B. Webcams oder Intranetseiten.

Mit der Funktion „Webseiten“ werden einfach aufgebaute Webseiten angezeigt. Komplexe oder passwortgeschützte Webseiten, z. B. Konfigurationsoberflächen von Kameras, weisen möglicherweise Funktionsprobleme auf oder können gar nicht angezeigt werden.

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Webseiten** im Steuerelement Administration.

Neue Webseite anlegen

1. Legen Sie eine neue Webseite an.
2. Geben Sie den **Namen** für die neue Webseite ein.
3. Wählen Sie für die Webseite ein benutzerdefiniertes Symbol aus, sofern verfügbar (siehe „[Ton- und Symboldateien mit benutzerdefinierten Medien verwalten](#)“ auf Seite 482).
4. Bestätigen Sie den Namen mit **OK**. Die neue Webseite wird in der Übersicht angezeigt.

Webseite konfigurieren

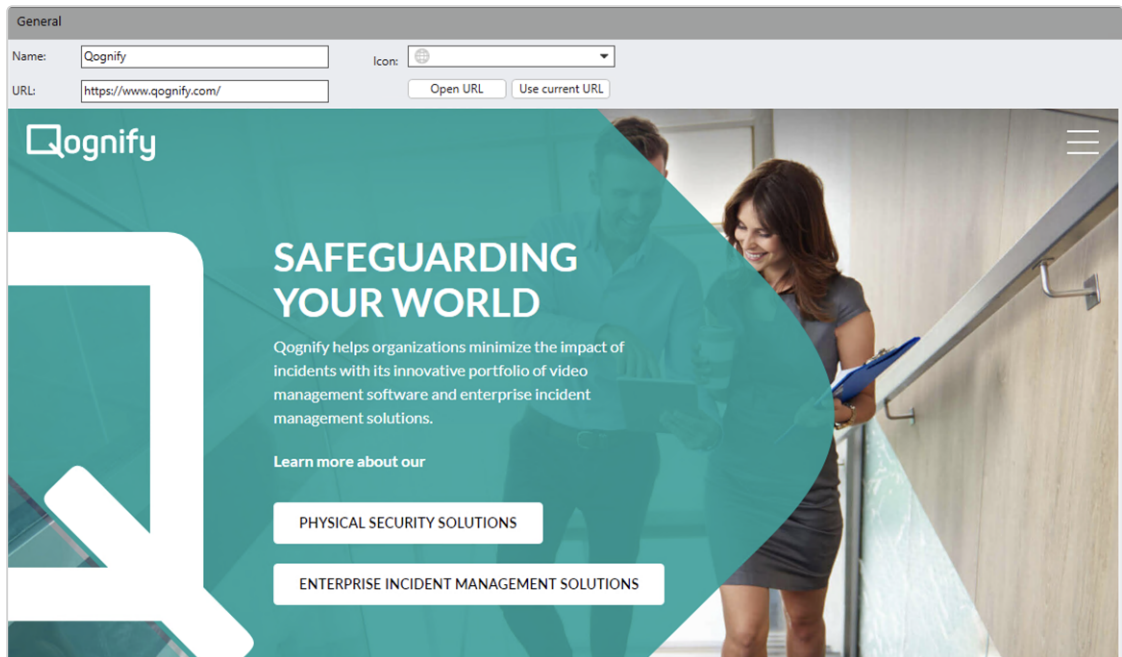


Abb. 226: Webseite konfigurieren - Allgemein

1. Wählen Sie die Webseite in der Übersicht aus.
2. Passen Sie gegebenenfalls den **Namen** der Webseite an und geben Sie die **URL** (Internet- bzw. Intranetadresse) ein.
3. Sofern verfügbar, ändern Sie das Symbol für die Webseite (siehe „[Ton- und Symboldateien mit benutzerdefinierten Medien verwalten](#)“ auf Seite 482).
4. Wählen Sie **URL öffnen**, um zu prüfen, dass man auf die Webseite zugreifen kann.
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Webseite löschen

1. Wählen Sie die Webseite in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Webseite duplizieren

1. Wählen Sie die Webseite in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für die duplizierte Webseite ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Webseite wird in der Übersicht angezeigt.

Wächterrundgänge

Mit der Funktion **Wächterrundgänge** im Steuerelement **Administration** können Sie mehrere Kameras, eingestellte Positionen, Lagepläne und Ansichten nacheinander für eine frei definierbare Zeit konfigurieren. Zusätzlich ist es möglich, innerhalb eines Rundgangs digitale Ausgänge zu öffnen oder zu schließen und Kontrollpunkte anzulegen.

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Wächterrundgänge** im Steuerelement Administration.

Neuen Wächterrundgang erstellen

1. Legen Sie einen neuen Wächterrundgang an.
2. Geben Sie den **Namen** für den neuen Wächterrundgang ein.
3. Bestätigen Sie den Namen mit **OK**. Der neue Wächterrundgang wird in der Übersicht angezeigt.

Um den neuen Wächterrundgang im Überwachungsmodus aktivieren zu können, muss er einem Benutzerprofil zugeordnet werden. Wechseln Sie in das Steuerelement **Profil** und aktivieren Sie den Wächterrundgang für das gewünschte Benutzerprofil (siehe [Profil konfigurieren](#)).

Wächterrundgang konfigurieren

- Wächterrundgänge können nur auf Clients ausgelöst werden, die sich im Überwachungsmodus befinden.

- Bei Auslösung mehrerer Wächterrundgänge wird der zuletzt ausgelöste Rundgang gestartet. Alle zuvor gestarteten Wächterrundgänge werden gestoppt.
- Während eines Alarms können keine Wächterrundgänge gestartet werden. Der Wächterrundgang wird gestartet, sobald der Alarm beendet ist.

Allgemein

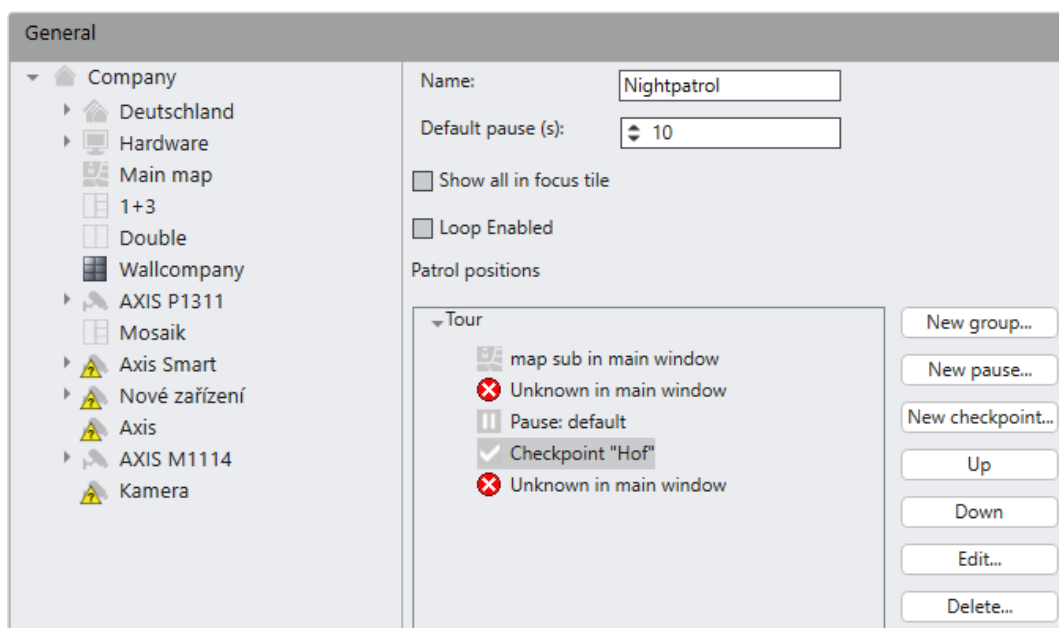


Abb. 227: Wächterrundgänge - Allgemein

1. Wählen Sie den Wächterrundgang in der Übersicht aus.
2. Passen Sie gegebenenfalls den **Namen** des Wächterrundgangs an.
3. Wählen Sie die **Standard-Pause** (in Sekunden), um die Dauer einzustellen, mit der eine Ansicht angezeigt werden soll.
4. Aktivieren Sie **Alle in Fokuskachel anzeigen**, um alle Entitäten (Kameras, Lagepläne usw.) des Wächterrundgangs in einer einzigen Kachel statt auf dem gesamten Bildschirm oder in ganzen Ansichten anzuzeigen. Die Entitäten „rotieren“ in der Kachel wie in einer Art Karussell.
5. Wählen Sie **Neue Gruppe**, um die Objekte des Rundgangs zusammenzufassen.
6. Geben Sie den Namen der Gruppe an und wählen Sie **OK**.
7. Ziehen Sie die Objekte aus der linken Spalte in die Positionen Wächterrundgang oder die Gruppe.

8. Um eine bestimmte Position einer Kamera in die Liste aufzunehmen, ziehen Sie zunächst die Kamera in die Gruppe, dann die dazugehörige Preset-Position.
9. Wählen Sie eine Kamera und dann **Bearbeiten**.
10. Wenn **Alle in Fokuskachel anzeigen** deaktiviert ist, aktivieren Sie die Fokuskachel für jedes Element separat.
11. Wählen Sie das Fenster aus, in dem die Kamera angezeigt werden soll, und klicken Sie auf **OK**.
12. Fügen Sie gegebenenfalls eine **Neue Pause** ein und passen Sie die Dauer der Pause an.
13. Fügen Sie einen **Neuen Kontrollpunkt** ein und geben Sie einen Namen ein. Wenn ein Kontrollpunkt erreicht wird, wird ein Hinweisfenster eingeblendet. Der Benutzer hat dann die Auswahl, ob er den Rundgang fortführen oder beenden möchte. Das Erreichen eines Kontrollpunkts wird in der Ereignisauswertung gespeichert.
14. Um die Reihenfolge der eingefügten Objekte zu ändern, markieren Sie das Objekt in Positionen Wächterrundgang und bewegen Sie das Objekt in der Liste **Auf** oder **Ab**, indem Sie auf die entsprechende Schaltfläche klicken.

Damit ein Wächterrundgang im Überwachungsmodus gestartet werden kann, muss dieser zuerst im Steuerelement Profile einem Benutzer oder einer Gruppe zugeordnet werden (siehe „Profile“ auf Seite 375).

15. Wählen Sie das Objekt in „Positionen Wächterrundgang“ und anschließend **Bearbeiten**, um die Einstellungen des Objekts anzupassen. Damit können Sie festlegen, in welchem Fenster das Kamerabild angezeigt werden soll.
16. Wählen Sie das Objekt in „Positionen Wächterrundgang“ und anschließend **Löschen**, um das Objekt zu löschen.

Start

1. Wählen Sie den Wächterrundgang in der Übersicht aus.
2. Wählen Sie **Start** aus.
3. Klicken Sie auf **Bearbeiten** und wählen Sie aus der Liste ein Element aus, das den Ereignisstart festlegt. Sie können auch nach dem Element suchen.
4. Wählen Sie **OK**. Das Startereignis wird in der Ereignisliste angezeigt.

5. Um ein weiteres Ereignis hinzuzufügen, klicken Sie auf **Bearbeiten** und aktivieren Sie ein anderes Starterereignis.
6. Um das Ereignis zu entfernen, wählen Sie das Element aus und dann **Bearbeiten** und deaktivieren Sie das Element in der Liste.
7. Wählen Sie **OK**. Das Starterereignis wird aus der Liste entfernt.

Beenden

1. Wählen Sie den Wächterrundgang in der Übersicht aus.
2. Wählen Sie **Ende** aus.
3. Klicken Sie auf **Bearbeiten** und wählen Sie aus der Liste ein Element aus, das den Ereignisstopp festlegt. Sie können auch nach dem Element suchen.
4. Wählen Sie **OK**. Das Stoppereignis wird in der Ereignisliste angezeigt.
5. Um ein weiteres Ereignis hinzuzufügen, klicken Sie auf **Bearbeiten** und aktivieren Sie ein anderes Stoppereignis.
6. Um das Ereignis zu entfernen, wählen Sie das Element aus und dann **Bearbeiten** und deaktivieren Sie das Element in der Liste.
7. Wählen Sie **OK**. Das Ereignis wird aus der Liste entfernt.

Beteiligte Personen

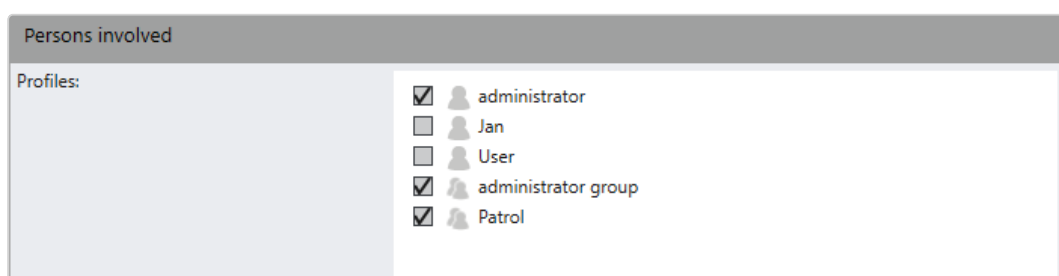


Abb. 228: Profile in Wächterrundgängen konfigurieren

1. Wählen Sie den Wächterrundgang in der Übersicht aus.
2. Wählen Sie **Beteiligte Personen** aus. Die verfügbaren Profile, die in den Profileinstellungen definiert wurden ([Profil konfigurieren](#)), werden angezeigt.
3. Wählen Sie die Profile aus, die mit dem Wächterrundgang verknüpft sind.
4. Speichern Sie **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Wächterrundgang löschen

1. Wählen Sie den Wächterrundgang in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Wächterrundgang duplizieren

1. Wählen Sie den Wächterrundgang in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für den duplizierten Wächterrundgang ein.
3. Bestätigen Sie den Namen mit **OK**. Der neue Wächterrundgang wird in der Übersicht angezeigt.

Sequenzen

Mit der Funktion **Sequenzen** im Steuerelement **Administration** können Sie serverseitige Sequenzen anlegen, in denen konfigurierbare Aktionen ausgelöst werden.

Allgemeine Hinweise zu Sequenzen

- Einer Sequenz können mehrere Zeitpunkte und/oder Zeiträume hinzugefügt werden.
- Mehrere Sequenzen können parallel ausgeführt werden.
- Ein Zeitplan ist nicht nötig, wenn die Sequenz durch ein Alarmszenario gestartet werden soll.
- Wenn eine Sequenz durch ein Alarmszenario gestartet wird, werden schon laufende Sequenzen fortgesetzt.
- Wird eine Sequenz durch ein Alarmszenario gestartet, wird die Sequenz komplett abgearbeitet, auch wenn das Alarmszenario früher gestoppt wird.
- Wenn eine laufende Sequenz durch ein Alarmszenario gestoppt wird, wird die Sequenz nur für die konfigurierte Totzeit unterbrochen.
- Eine Aufzeichnung kann nur im Zusammenhang mit einem Alarm gestartet werden, nicht durch die Sequenz direkt.

- Sequenzen haben keinen exklusiven Zugriff auf die Kamerapositionen: Wenn eine PTZ-Kamera während einer laufenden Sequenz gesteuert wird, dann werden die Preset-Positionen mit einer Totzeit von einer Minute nicht von der Sequenz angefahren.
 - Durch ein Alarmszenario kann eine Preset-Position ebenfalls angefahren werden, auch wenn kurz zuvor die Sequenz eine andere Preset-Position der gleichen Kamera angefahren hat. Das Gleiche gilt auch für eine weitere Sequenz.
1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
 2. Wählen Sie **Sequenzen** im Steuerelement Administration.

Neue Sequenz erstellen

1. Legen Sie eine neue Sequenz an.
2. Geben Sie den **Namen** für die neue Sequenz ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Sequenz wird in der Übersicht angezeigt.

Sequenz konfigurieren

1. Wählen Sie die Sequenz in der Übersicht aus.

Allgemein

Days	Start	End	Loop	Interval	Edit/delete
Mon Tue Wed Thu Fri	5:43 PM	6:43 PM	No	5	<input type="checkbox"/>

Abb. 229: Sequenzen - Allgemein

1. Aktivieren Sie die Sequenz und passen Sie gegebenenfalls den **Namen** an.
2. Setzen Sie den Zähler **PTZ-Priorität** auf einen Wert zwischen 1 und 1000 (je höher die Zahl, desto niedriger die Priorität) und geben Sie das **Timeout für PTZ-Prioritätsaktionen** in Sekunden an. Wenn die Sequenz keine PTZ-Steuerungen aktiviert, wird die Kamerasteuerung nach der Zeitüberschreitung (Timeout) wieder freigegeben.

Bei Übernahme der Steuerung der Kamera kann ein Benutzer (oder ein Alarm oder eine Serversequenz) mit einer höheren PTZ-Priorität einen anderen Benutzer (bzw. einen anderen Alarm oder eine andere Serversequenz) übersteuern.

3. Fügen Sie mit Hilfe der Schaltflächen **Zeitpunkte** und **Zeiträume** hinzu.
 - **Zeitpunkt:** Die Sequenz an jedem ausgewählten Tag zum gewählten Zeitpunkt einmal gestartet.
 - **Zeitraum:** Die Sequenz wird an jedem ausgewählten Tag innerhalb des Zeitraums abhängig von der Dauer der Sequenz gegebenenfalls mehrmals gestartet.
4. Markieren Sie einen oder mehrere Einträge und wählen Sie **Markierte Einträge bearbeiten**, um die Einträge nacheinander anzupassen.

5. Markieren Sie einen oder mehrere Einträge und wählen Sie **Markierte Einträge löschen**, um die Einträge zu entfernen.

Aktionen

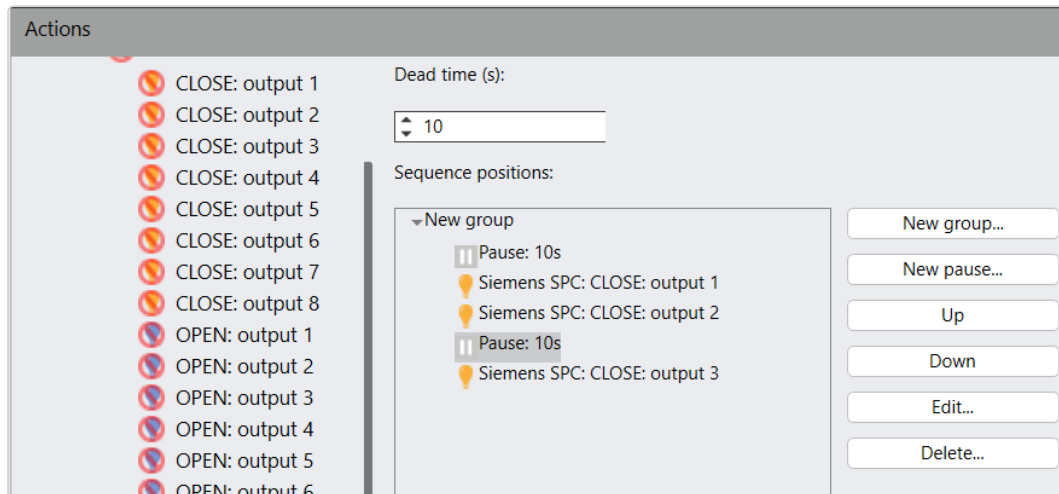


Abb. 230: Sequenzen - Aktionen

1. Legen Sie eine **Neue Gruppe** an und geben Sie einen Namen ein.
2. Geben Sie die **Totzeit** (in Sekunden) an, um eine Zeitspanne zu definieren, in der die Sequenz durch einen Alarmtrigger unterbrochen wird.
3. Ziehen Sie eine oder mehrere Kamerapositionen oder Aktionen in die Gruppe.
4. Markieren Sie eine Gruppe und passen Sie mit Hilfe von **Neue Pause** die jeweilige Pause (in Sekunden) an, um festzulegen, wie lange die Kamera bzw. die Ansicht oder der Lageplan angezeigt wird.
5. Markieren Sie eine Gruppe oder einen Eintrag und verschieben Sie die Reihenfolge mit Hilfe von **Auf** bzw. **Ab**.
6. Markieren Sie eine Gruppe oder eine Pause und wählen Sie **Bearbeiten**, um den Namen der Gruppe oder die Dauer der Pause anzupassen.
7. Markieren Sie eine Gruppe oder einen Eintrag und wählen Sie **Löschen**, um die Gruppe oder den Eintrag zu entfernen.
8. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
9. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Sequenz löschen

1. Wählen Sie die Sequenz in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Sequenz duplizieren

1. Wählen Sie die Sequenz in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für die duplizierte Sequenz ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Sequenz wird in der Übersicht angezeigt.

Videowände

Mit der Funktion **Videowände** im Steuerelement Administration konfigurieren Sie den Qognify Dispatcher zur Steuerung eines Display Agent (siehe „[Display Agent](#)“ auf [Seite 93](#)). Wenn im Benutzerprofil definiert, können Sie damit Kamerabilder, Ansichten, Lagepläne, Alarmszenarien und Webseiten auf Videowänden im Dispatcher-Modus anzeigen.

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Videowände** im Steuerelement Administration.

Neue Videowand erstellen

1. Legen Sie eine neue Videowand an.
2. Geben Sie den **Namen** für die neue Videowand ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Videowand wird in der Übersicht angezeigt.

Videowand konfigurieren

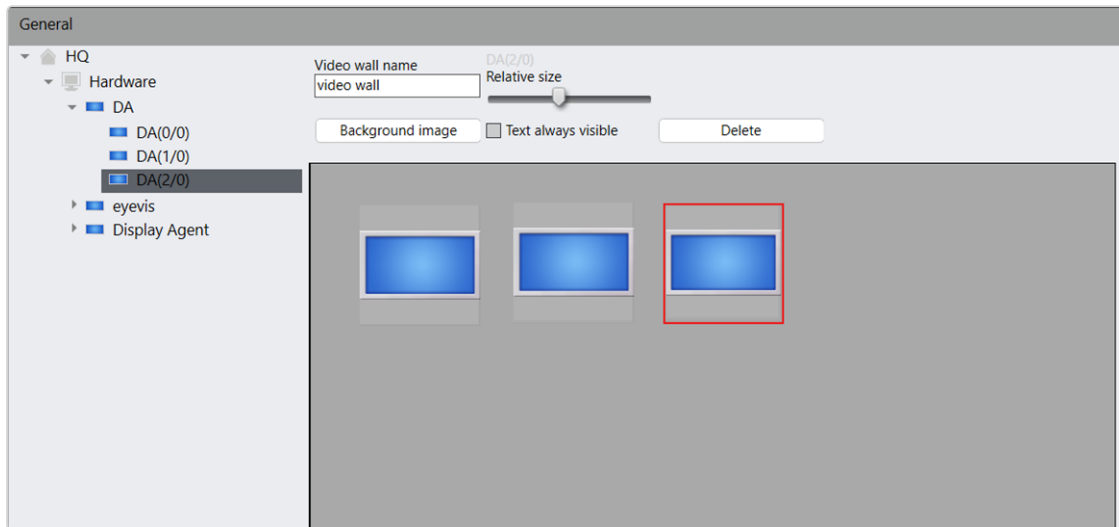


Abb. 231: Videowände - Allgemein

1. Wählen Sie die Videowand in der Übersicht aus.
2. Passen Sie gegebenenfalls den **Namen** der Videowand an.
3. Wählen Sie das Hintergrundbild aus, das in der Videowand angezeigt werden soll.
4. Ziehen Sie die Monitore, die als Display Agent definiert werden müssen, auf die Videowand und passen Sie die Anordnung der Monitore an (siehe „[Sonstige Hardware](#)“ auf Seite 296).
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Im Benutzerprofil sind weitere Einstellungen erforderlich (siehe „[Videowand-Modulmapping](#)“ auf Seite 380).

Videowand löschen

1. Wählen Sie die Videowand in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Videowand duplizieren

1. Wählen Sie die Videowand in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für die duplizierte Videowand ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Videowand wird in der Übersicht angezeigt.

Kennzeichengruppen

In den **Kennzeichengruppen** können Kennzeichengruppen für die Kennzeichenerkennung (LPR) konfiguriert und verwaltet werden. Abhängig von der Konfiguration des LPR-Prozesses können Kennzeichen automatisch oder manuell in Gruppen angeordnet werden. Wenn beispielsweise ein Kennzeichen aus der Gruppe „Lieferanten“ erkannt wird, wird automatisch eine Schranke geöffnet. Informationen zum manuellen Hinzufügen von Kennzeichen zu einer Gruppe finden Sie unter [„LPR-Stammdateneditor“ auf Seite 94](#).

Um die Nutzung des LPR-Modus einzuschränken (und möglichen Missbrauch zu verhindern), muss mindestens eine LPR-Gruppe mit den entsprechenden Rechten konfiguriert werden (siehe auch [„LPR-Modus“ auf Seite 487](#)).

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
2. Wählen Sie **Kennzeichengruppe** im Steuerelement Administration.

Neue Kennzeichengruppe anlegen

1. Legen Sie eine neue Kennzeichengruppe an.
2. Geben Sie den **Namen** für die neue Kennzeichengruppe ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Kennzeichengruppe wird in der Übersicht angezeigt.

Kennzeichengruppe konfigurieren

General

General

Activated

Name: Suppliers

Display: XX YY 123

Font color: Turquoise

Background color: Crimson

Export

Activate XML export

Abb. 232: Kennzeichengruppen - Allgemein

1. Wählen Sie die Kennzeichengruppe in der Übersicht aus.
2. **Aktivieren** Sie die Kennzeichengruppe.
3. Ändern Sie gegebenenfalls den **Namen** der Kennzeichengruppe.
4. Passen Sie die **Textfarbe** und die **Hintergrundfarbe** in der Darstellung des Kennzeichens an.
5. Aktivieren Sie den **XML-Export**, um die Kennzeichendaten als XML-Datei zu exportieren, sobald ein Kennzeichen aus dieser Gruppe von einem LPR-Ereignis erkannt wird. Die XML-Daten werden in dem Verzeichnis abgelegt, das Sie bei der Konfiguration des LPR-Moduls angegeben haben (siehe „[LPR-Modul konfigurieren](#)“ auf Seite 446).
6. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
7. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Kennzeichengruppe löschen

1. Wählen Sie die Kennzeichengruppe in der Übersicht aus.
2. Klicken Sie auf **Objekt löschen**.

Kennzeichengruppe duplizieren

1. Wählen Sie die Kennzeichengruppe in der Übersicht aus.
2. Klicken Sie auf **Objekt duplizieren** und geben Sie den Namen für die duplizierte Kennzeichengruppe ein.
3. Bestätigen Sie den Namen mit **OK**. Die neue Kennzeichengruppe wird in der Übersicht angezeigt.

Server

Mit der Funktion **Server** im Steuerelement Administration können Sie die Serverdienste konfigurieren.

Folgende Dienste stehen nach einer Standardinstallation zur Verfügung:

- Core Service Main
- Device Manager
- Globale OCR-Einstellungen
- 2 Bewegungserkennungsmodule
- Modul „Generischer DVR“

Die folgenden Module können über eine benutzerdefinierte Installation (siehe [„Angepasste Installation“ auf Seite 41](#)) oder mit dem VA Administrationstool (siehe [„Qognify VMS VA Administrationstool“ auf Seite 513](#)) erstellt werden:

- Licence Plate Recognition (Kennzeichenerkennung, LPR)
- TranscodingEngine
- Analytics Server-Modul
- Gateway Service
- Analytics Interface
- Serverbasierte Bewegungserkennung
- Generischer DVR
- Generische Zutrittskontrolle
- Event Interface

Informationen zu weiteren Einstellungen finden Sie unter [„Qognify VMS VA Administrationstool“ auf Seite 513](#).

1. Wählen Sie den Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.

2. Wählen Sie **Server** im Steuerelement Administration.

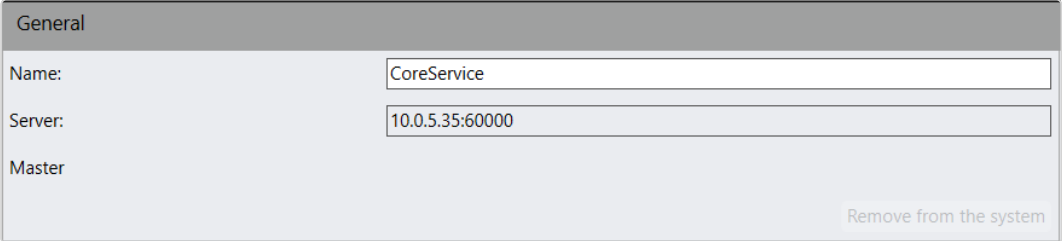
Konfigurieren des Hauptdienstes

Die Hauptaufgaben des Core Service sind:

- Verwaltung der Systemkonfiguration
- Einstellungen der Kameras, Lagepläne usw.
- Verwaltung aller systeminternen Ereignisse
- Weiterleitung an alle Dienste und Clients
- Verwaltung von Alarmszenarien
- Benutzerverwaltung

In einer verteilten Installation mit mehreren Core Servern kann die Hauptfiliale den Core Service Main (CSM) und einen CoreService Sub (CSS) enthalten (siehe „[Kerndienste und Filialen](#)“ auf Seite 22).

Allgemein



General	
Name:	CoreService
Server:	10.0.5.35:60000
Master	
Remove from the system	

Abb. 233: Kerndienst - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Passen Sie gegebenenfalls den **Namen** des **Servers** an.

Die Netzwerkadresse und die Portnummer des Core-Servers können mit dem Administrationstool geändert werden.

3. Klicken Sie auf **Aus dem System entfernen**, um den Core Server aus der Systemkonfiguration zu entfernen. Ein Core Service Sub (CSS) kann nur aus dem System entfernt werden, wenn der Server nicht mit dem Core Service Main (CSM) verbunden ist.

Wenden Sie sich vor dem Löschen stets zuerst an den Qognify-Support.

4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
5. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Device Manager (DM) konfigurieren

Die Hauptaufgaben des Device Manager sind:

- Verwaltung sämtlicher verbundener Hardware wie Kameras, Videosever, I/O-Module
- Verteilung der Bilddaten, z. B. an die Clients, MultimediaDatabase
- Kommunikation mit anderen Diensten
- Ereignishandling

Allgemein

General	
Name:	<input type="text" value="DeviceManager_Obi-Wan"/>
Server:	<input type="text" value="172.16.12.4:60008"/>
Server for failover image recording	<input type="text" value="DeviceManager_PWERN-HP"/>
Mirroring	<input checked="" type="checkbox"/> active
Time of the data-aging search:	<input type="text" value="02:00"/>
Permanently save the following events:	<input type="checkbox"/> Accesses to video sources (surveillance mode)
Automatically delete events older than:	<input type="text" value="2 month(s)"/>
Display statistics	<input type="button" value="Apply"/>
Remove from the system	<input type="button" value="Apply"/>
Enable thresholds	<input checked="" type="checkbox"/>
Maximum packet loss (%)	<input type="text" value="25,00"/>
Standard recording	
Frame rate delta (fps)	<input type="text" value="1,0"/>
Maximum frames dropped	<input type="text" value="2"/>
Alarm recording	
Frame rate delta (fps)	<input type="text" value="2,0"/>
Maximum frames dropped	<input type="text" value="50"/>
Enable MDB Statistics Notifications	<input type="text" value="Never"/>

Abb. 234: Device Manager - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Passen Sie gegebenenfalls den **Namen** des Bilddatenservers an.
3. Wählen Sie den **Server für FailOver-Bildaufzeichnung**. Im Falle eines Ausfalls des Bilddatenservers werden alle angeschlossenen Geräte auf den FailOver-Server umgeschaltet.

Bei einem FailOver-Aufzeichnungssystem muss der Device Manager abgesetzt installiert werden (siehe „[Installation eines abgesetzten Servers](#)“ auf Seite 38), da der FailOver-Server über ausreichend Kapazitäten zur Übernahme der Geräte verfügen muss (siehe „[Systemvoraussetzungen](#)“ auf Seite 31).

4. **Spiegeln** aktivieren: Mit dieser Option wird die redundante Aufzeichnung aller angeschlossenen Kameras aktiviert.

Diese Option ist nur mit einer Infinity X-Lizenz verfügbar.

Wenn diese Option aktiviert wird:

- Der produktive DM hat die primäre Rolle inne und überträgt die Daten gleichzeitig an beide MDS, sofern konfiguriert.
 - Wenn der produktive oder redundante Server ausfällt, werden die Aufzeichnungen auf dem noch funktionierenden Server fortgesetzt.
 - Wenn der produktive DM ausfällt, findet das reguläre FailOver-Szenario statt und der Basisdienst schaltet die Steuerung der Kamera auf den FailOver-Server um. In diesem Fall (sofern nicht über Kreuz konfiguriert) erfolgt die Aufzeichnung nur auf dem FailOver-Server. Sobald wieder zurückgeschaltet wurde, erfolgt wieder eine redundante Aufzeichnung.
 - Bei Durchführung eines serverseitigen Exports exportiert jeder der beiden Server seine jeweiligen Teile der Aufzeichnungen.
 - Auf beiden Servern wird der Schreibschutz von Aufzeichnungen angewendet.
 - Auf beiden Servern werden Aufzeichnungen gelöscht.
 - Auf beiden Servern wird ein Edge-Speicher-Import durchgeführt.
5. Legen Sie den **Zeitpunkt des Data Aging Suchlaufs** fest.
6. Aktivieren Sie **Zugriffe auf Videoquellen**, um diese Ereignisse zu speichern.
7. Wählen Sie den Zeitraum aus, nach dem die Ereignisse automatisch gelöscht werden.

Aufgrund gesetzlicher Vorschriften dürfen bei Installationen in Frankreich diverse Ereignisse nicht gelöscht werden.

8. Aktivieren Sie **Statistik anzeigen**, um Statistiken über das Streaming- und Aufzeichnungsverhalten für den ausgewählten Device Manager anzuzeigen. Um detailliertere Statistiken zu erhalten, können im Bereich „Schwellenwerte“ unten Schwellenwerte für eine bessere Visualisierung kritischer Streaming-Verhaltensweisen definiert werden.

9. Klicken Sie auf **Aus dem System entfernen**, um den Device Manager aus der Systemkonfiguration zu entfernen.

Kontaktieren Sie vor Entfernen des Device Manager aus dem System unbedingt den Qognify-Support.

Schwellenwerte

Um zu prüfen, ob der Device Manager gemäß den Spezifikationen arbeitet, können für bestimmte Parameter Schwellenwerte festgelegt werden. Wenn einer der Werte außerhalb der Spezifikationen liegt, wird die Kamera in der Device Manager-Statistik als „beschränkt“ gekennzeichnet und die entsprechenden Werte werden mit einem farbigen Hintergrund hervorgehoben.

Die Device Manager-Statistik muss für die Schwellenwertanalyse nicht geöffnet sein, da dieser Vorgang im Hintergrund abläuft.

1. Aktivieren Sie **Schwellenwerte aktivieren**.
2. Legen Sie Schwellenwerte für die folgenden Werte fest:
 - **Max. Paketverlust (%)**
 - **Bildrate Delta (fps)**: Die Abweichung zwischen der konfigurierten Bildrate und der aufgezeichneten Bildrate.
 - **Max. Anz. ausgelassener Bilder**: Die maximale Anzahl an Bildern, die von der MultimediaDatabase (MDB) ausgelassen werden.
3. Wählen Sie einen Zeitbereich für **MDB-Statistik-Benachrichtigungen aktivieren** aus. Wird als Zeitbereich beispielsweise 1 Stunde gewählt, wird stündlich geprüft, ob bestimmte Werte aus der MDB-Statistik im Durchschnitt über oder unter einem der angegebenen Schwellenwerte liegt. Systembenutzer können dann benachrichtigt werden. Dazu muss in der Ereignisverwaltung die Option **Schwellenwerte wurden überschritten** aktiviert sein.

Device Manager-Statistik

In der Device Manager-Statistik werden statistische Informationen über den Device Manager angezeigt, z. B. ob die Aufzeichnung gemäß den Parametern erfolgt, die konfiguriert wurden, um eine fehlende (oder unzureichende)

Videodokumentation zu vermeiden.

Die Statistik kann folgende Werte über die angeschlossenen Kameras anzeigen.

- Kamera ID
- Kameraname
- Kamerahersteller
- Modell
- Kamera-Firmware
- Kamera-IP
- Paketverlustquote
- Status der Aufzeichnung
- Sequenzen
- Für jede Standard- und Alarmaufzeichnung:
 - Anz. an Bildern
 - Anz. der ausgelassenen Bilder
 - Erstes Bild
 - Letztes Bild
 - Alter des ersten Zeitstempels im Aufzeichnungsbereich
 - Gefüllter Anteil in Prozent im Aufzeichnungsbereich
 - Größe (GB)
 - Breite
 - Höhe
 - Erwartete Höhe
 - Codec
 - Erwarteter Codec
 - Video-Bildrate (fps)
 - Video-Bitrate (kbps)

Die Granularität ist standardmäßig auf eine Stunde eingestellt, d. h., es werden nur Daten der jeweils letzten Stunde berücksichtigt.

The screenshot shows the 'DeviceManager info' window for 'DeviceManager_001'. It displays a table of zones, a list of cameras with their status and recording statistics, and a summary table at the bottom.

Path	Status	Writable	Assigned disk space (GB)	Used disk space (GB)	Used disk space (%)
C:\Users\sascha.christmann\Desktop\zone01	Ready for operation	Yes	211.55	7.60	4 %

Camera ID	Camera	Model	Camera IP	Packet loss ratio	Status of recording	Sequences	Standard recording Amount of frames	Standard recording Amount of dropped frames	Standard recording Max. time period	Standard recording Actual time period	Standard recording First image	Standard recording Last image
4611967493405105575	AXIS P1357	P1357(-E)	10.0.7.73	0	Limited	5	0	0	1d 1h 0m	0d 0h 58m	8/7/2017 2:15:26 PM	8/8/2017
4611967493405105576	AXIS P1311	P1311	10.0.8.234	0	Limited	4	33233	0	1d 1h 0m	0d 0h 59m	8/7/2017 2:15:08 PM	8/8/2017
4611967493405105612	AXIS M1114	M1114(-E)	10.0.101.31	0.001	Limited	3	35946	0	1d 1h 0m	0d 0h 59m	8/7/2017 2:19:05 PM	8/8/2017

Packet loss ratio	Sequences	Standard recording Amount of frames	Standard recording Amount of dropped frames	Standard recording Max. time period	Standard recording First image	Standard recording Last image	Standard recording Size (GB)	Alarm recording Amount of frames	Alarm recording Amount of dropped frames	Alarm recording Max. time period
0	12	69179	0	1d 1h 0m	8/7/2017 2:15:08 PM	8/8/2017 9:34:50 AM	7.5825	183	0	1d 1h 0m

Abb. 235: Device Manager-Statistik

Folgende Optionen stehen zur Verfügung:

- **DeviceManager-Server:** Der Device Manager kann schnell geändert werden.
- **Zonen:** Zeigt eine Übersicht der Zonen an, die mit dem ausgewählten Device Manager konfiguriert sind.
- **Kameras:** Zeigt detaillierte Informationen über die angeschlossenen Kameras an.
- Durch Auswahl von **Optionen** können Einzelheiten angegeben werden. Alle Spalten können angezeigt oder ausgeblendet werden.
- Die **Spalten** der Statistik können manuell durch Ziehen der Spaltentitel nach links oder rechts sortiert werden.
- Die Werte der Statistik können durch Klicken auf den entsprechenden Spaltentitel neu geordnet werden.
- **Zeitraum:** Wählen Sie den Zeitraum aus, auf dem die Statistik basieren soll. Der Standardwert ist 1 Stunde.
- **Zusammenfassung:** Zeigt die Zusammenfassungswerte aller an den ausgewählten Device Manager angeschlossenen Kameras an.
- **CSV exportieren:** Die angezeigte Statistik kann als CSV-Datei exportiert werden.
- **Neu laden:** Lädt die Statistik neu, um die aktuellsten Werte anzuzeigen.
- **Schließen:** Schließt das Statistik-Fenster.

Optionen



Options

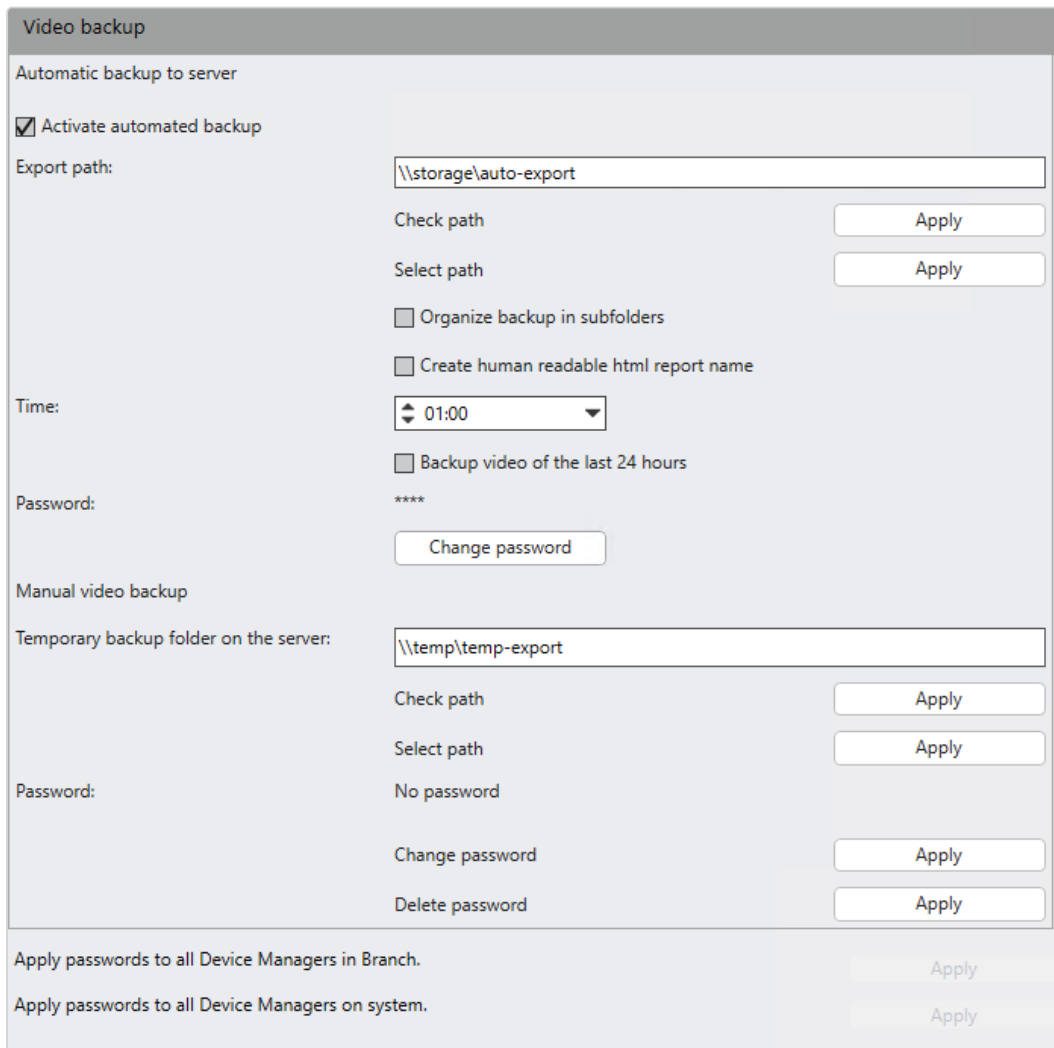
Port for SIP messages:

Abb. 236: Device Manager - Optionen

1. Passen Sie gegebenenfalls den **Port für SIP-Nachrichten** an (siehe „[VoIP und SIP](#)“ auf Seite 78).

Video-Backup

In diesem Bereich können die Einstellungen des Device Manager für den automatischen und manuellen Videodaten-Export konfiguriert werden.



Video backup

Automatic backup to server

Activate automated backup

Export path:

Check path

Select path

Organize backup in subfolders

Create human readable html report name

Time:

Backup video of the last 24 hours

Password: ****

Manual video backup

Temporary backup folder on the server:

Check path

Select path

Password: No password

Apply passwords to all Device Managers in Branch.

Apply passwords to all Device Managers on system.

Abb. 237: Device Manager - Video-Backup

Automatischer Backup auf den Server

Der automatische Video-Backup auf den Server hängt von den Kameraeinstellungen ab. Dort muss der kameraspezifische Export aktiviert werden (siehe „[Video-Backup/-Export](#)“ auf Seite 274).

1. Aktivieren Sie den automatischen Export.
2. Legen Sie den **Exportpfad** für die automatische Speicherung der Bilddaten an oder klicken Sie auf **Pfad auswählen**, um das Verzeichnis direkt im Windows Explorer auszuwählen (der Pfad kann nur ausgewählt werden, wenn der Qognify VMS-Client auf demselben Windows-System ausgeführt wird wie der Device Manager).

Der Device Manager-Server muss auf den Exportpfad zugreifen können.

3. Klicken Sie auf **Pfad prüfen**, um die Verfügbarkeit des angegebenen Pfads zu kontrollieren.
4. Aktivieren Sie **Videoexport in Unterordnern organisieren**, wenn die exportierten Aufzeichnungen in Ordnern gespeichert werden sollen, die nach den Kameranamen benannt sind. Anderenfalls werden die exportierten Aufzeichnungen nicht in Ordnern organisiert.
5. Aktivieren Sie **Visuell lesbaren HTML-Berichtnamen anlegen**. Anderenfalls wird als Dateiname des Berichts der Zeitstempel des Computers verwendet.
6. Legen Sie die **Uhrzeit** fest, zu der der Export beginnen soll.
7. Aktivieren Sie **Bilddaten der letzten 24 Stunden exportieren**, um die Bilddaten der letzten 24 Stunden vor dem festgelegten Exportzeitpunkt zu exportieren. Sollte diese Option nicht aktiviert sein, werden die Bilddaten des vergangenen Tages (0h bis 24h) exportiert.
8. Geben Sie ein **Passwort** an, mit dem die Bilddaten verschlüsselt werden.
9. Um das Passwort auf die gesamte Bilddatenverschlüsselung in einer Filiale anzuwenden, wählen Sie die entsprechende Option **Anwenden** aus.

10. Um das Passwort auf die gesamte Bilddatenverschlüsselung in einem Unternehmen anzuwenden, wählen Sie die entsprechende Option **Anwenden** aus.

Manueller Bilddatenexport

Für den manuellen Bilddatenexport zum Client wird ein temporäres Verzeichnis auf dem Server benötigt (siehe „[Video-Backup/-Export](#)“ auf [Seite 274](#)). Dort werden die Exportdaten zwischengespeichert, bevor sie zum Client gesendet werden.

1. Legen Sie das **Temporäre Exportverzeichnis auf dem Server** für die manuelle Speicherung der Bilddaten an oder klicken Sie auf **Pfad auswählen**, um das Verzeichnis direkt im Windows Explorer auszuwählen.

Der Device Manager-Server muss auf den temporären Exportpfad zugreifen können.

2. Wählen Sie **Pfad prüfen**, um sicherzustellen, dass die Qognify-Serverdienste in das Verzeichnis schreiben und daraus lesen können.

Stellen Sie sicher, dass ausreichend Speicherplatz für große Exportdateien auf der Partition zur Verfügung steht, auf der das temporäre Verzeichnis angelegt wird.

3. Geben Sie ein **Passwort** an, mit dem die Bilddaten verschlüsselt werden sollen. Dieses Passwort wird für den Export der Bilddaten benötigt (siehe „[Mehrfachexport von Bilddaten](#)“ auf [Seite 114](#)).
4. Mit **Passwort löschen** entfernen Sie das hinterlegte Passwort.
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Globale OCR-Einstellungen konfigurieren

Der Server, auf dem der LPR-Dienst ausgeführt werden soll, wird angezeigt.

General

Unknown license plates

Enable automatic master data entry

Display for unknown license plates: XX YY 123

Font color: ■ Red

Background color: ■ AliceBlue

Activate XML export for unknown license plates

License plates that are no longer valid

Enable automatic master data entry

User-defined master data fields

Title	Required field	Search field
Company	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>

Abb. 238: Globale OCR-Einstellungen - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Wählen Sie **Automatische Stammdateneingabe aktivieren** bei unbekanntem Kennzeichen. Dadurch wird der LPR-Stammdateneditor angezeigt, sobald ein unbekanntes Kennzeichen von der Kamera erkannt wird.

Für den Stammdaten-Editor muss der Benutzer die Berechtigung haben, mindestens eine Kennzeichengruppe zu bearbeiten (d. h. es muss mindestens eine Kennzeichengruppe vorhanden sein), und die Berechtigung „Live sehen“ für die Kamera, die das Kennzeichen erkannt hat.

3. Passen Sie für unbekannte Kennzeichen die **Textfarbe** und die **Hintergrundfarbe** in der Darstellung des Kennzeichens an. Bekannte Kennzeichen können im Steuerelement Kennzeichengruppen angepasst werden (siehe „[Kennzeichengruppen](#)“ auf Seite 432).
4. Aktivieren Sie den **XML-Export**, um die Kennzeichendaten als XML-Datei zu exportieren.
5. Aktivieren Sie **Automatische Stammdateneingabe aktivieren** für nicht mehr gültige Kennzeichen, z. B. aufgrund eines abgelaufenen Tickets.

6. Definieren Sie bis zu 10 **Benutzerdefinierte Stammdatenfelder**. Diese Felder werden beim Hinzufügen oder Ändern eines Kennzeichens angezeigt.
7. Aktivieren Sie **Pflichtfeld**, um anzugeben, dass das Feld ausgefüllt werden muss.
8. Aktivieren Sie **Suchfeld**, um anzugeben, dass in diesem Feld im LPR-Stammdateneditor nach den Daten gesucht werden kann.
9. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
10. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

LPR-Modul konfigurieren

Um ein LPR-Modul zu konfigurieren, muss es zunächst im Qognify VA Administrationstool angelegt werden (siehe „[Qognify VMS VA Administrationstool](#)“ auf Seite 513).

The screenshot shows the 'General' configuration window for the LPR Module. The window is divided into two main sections: 'General' and 'Settings'.
In the 'General' section:
- 'Name' is set to 'LPR Module SCHRI-HP'.
- 'Server' status is 'This service is not currently running on any computer.'
- 'Failover module' is set to 'Do not use failover'.
In the 'Settings' section:
- 'Detect spaces' is checked, with a value of '1'.
- 'timeout' is set to a dropdown menu.
Below these are sections for XML export and SQL export.
- 'XML export path' is an empty text field.
- 'Embed images in XML file' is an unchecked checkbox.
- 'SQL export' section includes fields for 'URL', 'Database', 'Table', 'User name', and 'Password', all of which are empty.
At the bottom, there is a 'Character set' section with a 'Selected character set' dropdown menu.
Buttons at the bottom include 'Remove from system', 'Expert mode', 'Cancel', 'Apply', and 'Save'.

Abb. 239: LPR-Modul - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Passen Sie gegebenenfalls den **Namen** des Moduls an.
3. Wählen Sie das **FailOver-Modul**, um bei Ausfall des Servers auf einen anderen Server ausweichen zu können.
4. Aktivieren Sie **Leerzeichen erkennen**, um die Leerzeichen in den Kennzeichen einzubeziehen.
 - Legen Sie den Wert auf „1“ fest, um maximal ein einziges Leerzeichen zwischen den erkannten Zeichen des Kennzeichens zu verarbeiten.
 - Legen Sie den Wert auf „2“ fest, um die Erkennung der neuen deutschen E-Kennzeichen (XX XXX E) für Elektrofahrzeuge zu aktivieren.

Für die Erkennung der deutschen E-Kennzeichen ist ein ARH-Don-
gle mit der neuen LPR-Modul-Version 9 (cmanpr-7.3.9.97:latin) erforder-
lich.

5. Geben Sie den **XML-Exportpfad** an, in das die exportierten XML-Daten abgelegt werden sollen. Der Exportpfad muss auf dem LPR-Modul-Server verfügbar sein. Jedes erkannte Kennzeichen wird als separate XML-Datei gespeichert, inklusive Kennzeichen, Kennzeichengruppe, Zeit und Fahrspurname.
6. Aktivieren Sie **Bilder in XML-Datei einbetten**, um ein Bild als JPEG in Base64 des erkannten Kennzeichens in der XML-Datei zu speichern.
7. Legen Sie optional den Exportpfad für den SQL-Export fest. Geben Sie dazu die entsprechenden Informationen an (**URL, Datenbank, Tabelle** sowie **Benutzername** und **Passwort** für den Zugriff auf die Datenbank). Der Export enthält das Kennzeichen, die Länderkennung, das Datum und die Uhrzeit. In der SQL-Tabelle müssen drei Spalten erstellt werden:
 - „NumberPlate“ (char), ca. 20 Zeichen
 - „LastSeen“ (varchar) oder (string), Größe 20 Zeichen
 - „Country“ (char) mit mind. 30 Zeichen. Die Größe hängt von den erkannten Länderkennungen ab. Die meisten Länderkennungen bestehen aus nur drei Buchstaben, z. B. GER, FRA. Es gibt jedoch auch längere Länderkennungen, wie GER_Oldtimer_old.

Es wird nur Microsoft SQL-Database unterstützt.

Beispiel

Kfz-Kennzeichen, LastSeen, Land

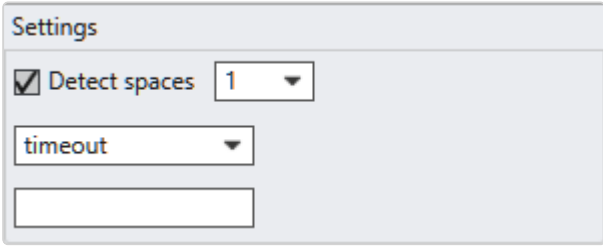
KA LH 0001, 10.02.2011 16:27:25, GER

8. Falls mehrere Zeichensätze installiert worden sind, wählen Sie aus, welcher Zeichensatz für die Erkennung des Kennzeichens verwendet werden soll.
 - Der Zeichensatz cmanpr-7.2.7:99: default hat keine integrierte Länderkennung.
 - Der Zeichensatz cmanpr-7.2.7:99: latin erkennt auch das jeweilige Land, benötigt aber einen etwas längeren Zeitraum für die Erkennung.
 - Zeichensätze für außereuropäische Kennzeichen erhalten Sie auf Anfrage.
9. Klicken Sie auf **Aus System entfernen**, um das LPR-Modul vollständig aus dem Qognify VMS-System zu löschen.
10. Klicken Sie auf **Expertenmodus**, um spezielle Parameter zur Erhöhung der Bildqualität für den LPR-Prozess zu ändern (siehe [„Expertenmodus des LPR-Moduls“ auf der gegenüberliegenden Seite](#)).

11. Fügen Sie nach der Konfiguration mindestens eine LPR-Gruppe hinzu, um einen Missbrauch der Kennzeichenerkennung zu verhindern (siehe „[Kennzeichengruppen](#)“ auf Seite 432).

Expertenmodus des LPR-Moduls

Bevor Sie im Expertenmodus Werte ändern, halten Sie Rücksprache mit dem Qognify-Supportteam und fragen Sie nach dem Referenzhandbuch für das CMANPR-Softwaremodul.



The screenshot shows a 'Settings' window with the following elements:

- A checked checkbox labeled 'Detect spaces' followed by a dropdown menu showing the value '1'.
- A dropdown menu labeled 'timeout'.
- An empty text input field below the 'timeout' dropdown.

Abb. 240: LPR-Module - Expertenmodus

Im Expertenmodus des LPR-Moduls können die folgenden Werte bearbeitet werden, um die Qualität der erkannten Kennzeichen zu verbessern:

- timeout
- contrast_min
- size
- nchar_min
- nchar_max
- size_min
- size_max
- slope
- slope_min
- slope_max
- slant
- slant_min
- slant_max
- xtoyres
- colortype
- unicode_in_text

Qognify Analytics Server 3D-Modul konfigurieren

Um ein Analytics Server-Modul zu konfigurieren, muss es zunächst im Qognify VA Administrationstool angelegt werden (siehe [„Analytics Server-Modul hinzufügen“ auf Seite 516](#)).

General	
Name:	Analytics Server Module 5
Server:	10.0.5.35:60611
Failover module	Do not use failover
<input type="button" value="Restart module"/>	

Abb. 241: Qognify Analytics Server 3D-Modul - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Ändern Sie gegebenenfalls den **Namen** des Moduls.
3. Wählen Sie das **FailOver-Modul**, um bei Ausfall des aktuellen Analytics Servers auf einen anderen Analytics Server ausweichen zu können.
4. Starten Sie das Modul bei Bedarf neu.

Ein Neustart des Moduls ist nach einer Änderung der Konfiguration nicht notwendig. Ein Neustart von Modulen wird nur empfohlen, wenn diese nicht ordnungsgemäß funktionieren.

5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Die Einstellungen werden unter [„Qognify Analytics Server“ auf Seite 335](#) beschrieben.

Analytics Interface-Modul konfigurieren

Um ein Analytics Interface-Modul zu konfigurieren, muss es zunächst im Qognify VA Administrationstool angelegt werden (siehe [„Analytics Interface-Modul hinzufügen“ auf Seite 521](#)).

General	
General	
Name:	Analytics Interface Module 10 SCHRI-HP
Server:	192.168.56.1:60621
Failover module	Do not use failover
Details	
Manufacturer:	SeeTec AG
Type:	Lpr Test Plugin
API version:	6.13.0
Authentication	
<input checked="" type="checkbox"/> Use authentication	
User name:	Miller
Password:	***
External service	
<input checked="" type="checkbox"/> Use external service	
Host (IP address or name):	LPR Server
Port:	8445
<input type="button" value="Restart module"/>	

Abb. 242: Analytics Interface-Modul - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Ändern Sie gegebenenfalls den **Namen** des Moduls.
3. Wählen Sie das **FailOver-Modul**, um bei Ausfall des aktuellen Analytics Servers auf einen anderen Analytics Server ausweichen zu können.
4. Wenn erforderlich, geben Sie den **Benutzernamen** und das Passwort für den Zugriff auf das Modul ein.
5. Wenn konfiguriert, geben Sie den **Host-Namen** oder die **IP-Adresse** des externen LPR-Diensts ein.
6. Starten Sie das Modul bei Bedarf neu.

Ein Neustart des Moduls ist nach einer Änderung der Konfiguration nicht notwendig. Ein Neustart von Modulen wird nur empfohlen, wenn diese nicht ordnungsgemäß funktionieren.

7. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
8. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Gateway-Service-(SGS-)Modul konfigurieren

Um ein Gateway-Service-Modul zu konfigurieren, muss es zunächst im Qognify VA Administrationstool angelegt werden (siehe „[Gateway-Service-Modul \(SGS\) hinzufügen](#)“ auf Seite 519).

The screenshot shows a configuration dialog box for the Gateway-Service-Modul (SGS) in the Qognify VA Administration tool. The dialog is titled "General" and is divided into two sections: "General" and "Network".

General Section:

- Activated
- Name: SGS Module 3 DISEN-HP
- Server: Unknown

Network Section:

- SOAP/REST IP address: 192.168.1.134
This address is also used for video streaming and must be accessible for the MobileClient; use your external IP if the Gateway Service is to provide video streams outside your network (Internet)
- SOAP/REST port: 41000
- RTSP port: 9100
- NodeJS port (streaming port for Webclient): 8081
- Activate one port solution for Webclient

At the bottom right of the dialog, there is a button labeled "Remove from the system". At the bottom center, there are three buttons: "Cancel", "Apply", and "Save".

Abb. 243: Qognify-Gateway-Service-Modul - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Ändern Sie gegebenenfalls den **Namen** des Moduls.
3. Ändern Sie gegebenenfalls die **SOAP-/REST-IP-Adresse**. Diese Adresse wird auch zum Video-Streaming verwendet und muss für den Mobile Client erreichbar sein. Verwenden Sie Ihre externe IP, wenn der GatewayService Videoströme außerhalb des Netzwerks (Internet) bereitstellen soll.
 - Geben Sie für den Zugriff auf das Netzwerk über das Intranet (interner Zugriff) die lokale IP des Servers an.
 - Geben Sie für den Zugriff auf das Netzwerk über das Internet (externer Zugriff) die öffentliche IP des Routers oder der Firewall an. Darüber hinaus muss am Router oder in der Firewall die transparente Port-Weiterleitung aktiviert werden.

4. Ändern Sie gegebenenfalls den **SOAP-/REST-Port**.
5. Ändern Sie gegebenenfalls den **RTSP-Port**.
6. Ändern Sie gegebenenfalls den **NodeJS-Port** (Streaming-Port für Web Client).
7. Sie können **1-Port-Lösung für WebClient aktivieren**, wenn alle Videos über Port 443 gestreamt werden sollen.

Diese Option ist nicht rückwärtskompatibel. Wenn Sie ein Upgrade auf Qognify VMS 7.4 von einer älteren Version vorgenommen haben, bei der Sie die 1-Port-Lösung in der Konfigurationsdatei manuell aktiviert haben, müssen sie auch hier im Konfigurationsmodus aktivieren, um den WebClient zu zwingen, wieder die 1-Port-Lösung zu verwenden.

8. Sie können **DisplayAgent-TCP-Port aktivieren**, um einfache Textkommandos über eine TCP-Verbindung (nur IPv4) zu versenden (Informationen zur Entitäten-Nummerierung finden Sie unter „[Entitäten-Nummerierung konfigurieren](#)“ auf Seite 479).

Das Aktivieren dieser Funktion stellt ein potenzielles Sicherheitsrisiko dar. Es erfolgt keine Authentifizierung, Autorisierung oder Verschlüsselung. Wenn diese Funktion aktiviert wird, stellen Sie sicher, dass kein unbefugter Zugriff möglich ist.

9. Starten Sie das Modul bei Bedarf neu.

Ein Neustart des Moduls ist nach einer Änderung der Konfiguration nicht notwendig. Ein Neustart von Modulen wird nur empfohlen, wenn diese nicht ordnungsgemäß funktionieren.

10. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
11. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Nachdem die Konfiguration gespeichert wurde, wird ein Hinweis über eine mögliche Verringerung der Leistung beim Video-Streaming angezeigt.

Transcoding-Modul konfigurieren

Das Transcoding-Modul wird zur Optimierung der Videobilder benötigt, die im Web Client (siehe „[Qognify VMS Web Client](#)“ auf Seite 545 und Mobile Client (siehe „[Der Qognify VMS Mobile Client](#)“ auf Seite 551) angezeigt werden sollen.

General

General:

Name:

Server:

Failover module:

Channels:

Maximum number of channels:

Lowest RTSP port for channels:

Highest RTSP port for channels:

Assigned DeviceManager server:

[Remove from the system](#)

Abb. 244: Transcoding-Modul - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Passen Sie gegebenenfalls den **Namen** des Moduls an.
3. Wählen Sie das **FailOver-Modul**, um bei Ausfall des aktuellen Transcoding-Moduls auf ein anderes Transcoding-Modul ausweichen zu können.
4. Geben Sie die **Maximale Anzahl von Kanälen** an (Standardanzahl: 20). Für jedes vom Web Client oder Mobile Client angeforderte Bild wird ein Kanal benötigt.

Um die Netzwerklast und die Last auf dem Transcoding-Modul zu verringern, wird empfohlen, die Anzahl an Kanälen pro Transcoding-Modul zu beschränken.

5. Geben Sie die Nummer des **Niedrigsten RTSP-Ports** und des **Höchsten RTSP-Ports** für Kanäle an. Die Anzahl der Ports muss mindestens der Anzahl der Kanäle entsprechen. Der Standard-Portbereich umfasst 40 Ports (Port 555 bis Port 595).
6. Aktivieren Sie den **Zugeordneten Device Manager-Server**, von dem das Transcoding-Modul die zu transcodierenden Videobilder empfängt.
7. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
8. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

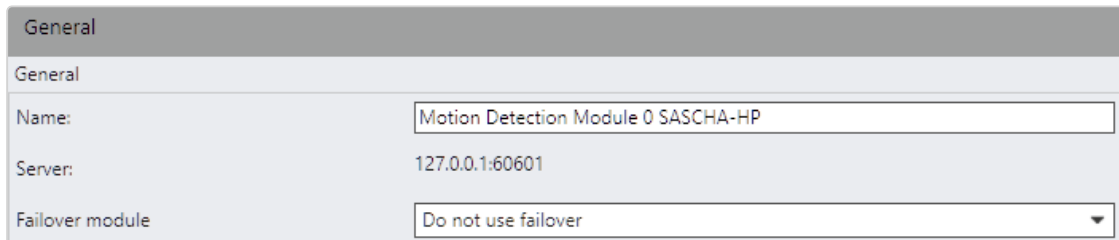
Bewegungserkennungsmodul konfigurieren

Standardmäßig sind zwei Bewegungserkennungsmodule verfügbar.

Voraussetzung

Um ein Bewegungserkennungsmodul zu konfigurieren, muss es zunächst im Qognify VA Administrationstool angelegt werden (siehe [„Analytics Server-Modul hinzufügen“ auf Seite 516](#)).

Konfiguration



General	
Name:	Motion Detection Module 0 SASCHA-HP
Server:	127.0.0.1:60601
Failover module	Do not use failover

Abb. 245: Bewegungserkennungsmodul - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Ändern Sie gegebenenfalls den **Namen** des Moduls.
3. Wählen Sie das **FailOver-Modul**, um bei Ausfall des aktuellen Moduls auf ein anderes Bewegungserkennungsmodul ausweichen zu können.
4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
5. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Informationen zu weiteren Einstellungen finden Sie unter [„Bewegungserkennung“ auf Seite 277](#).

Konfiguration des QMM-Server-Moduls

Voraussetzungen

- Ein QognifyMetadataManager (QMM)-Server muss installiert werden (siehe [„Installation und Upgrade“ auf Seite 556](#)).
- Die IP-Adresse des VMS Core-Service muss angewandt werden, so dass Qognify VMS Core registriert wird.

Konfiguration

General

General

Name: QMMServer SENEATEST

Server: 169.254.0.2:60044

License

Licensed channels: 999

Activated channels: 2

Query

Abb. 246: Konfiguration des QMM-Server-Moduls

1. Wählen Sie das Modul in der Server-Funktion.
2. Ändern Sie gegebenenfalls den **Namen** des Moduls.
3. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Modul „Generischer DVR“ konfigurieren

Überprüfen Sie, dass das Modul im VA Administrationstool hinzugefügt und ordnungsgemäß vorkonfiguriert wurde.

General

General

Activated

Name

Generic DVR Module SASCHA-HP

Server

127.0.0.1:60607

DVR plugins

Selected plugin:

BettiniDVR (1.0)

Maximum devices

50

Used devices

0

Remove from the system

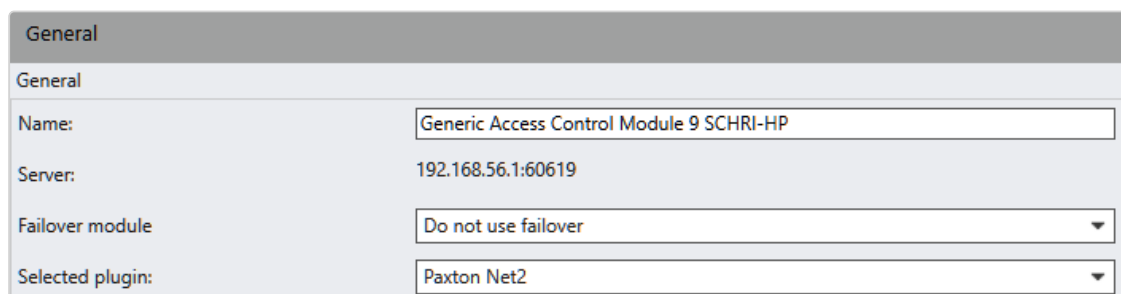
Abb. 247: Modul „Generischer DVR“ - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Ändern Sie gegebenenfalls den **Namen** des Moduls.
3. Wählen Sie ein **DVR-Plugin**.

4. Geben Sie die **maximale Anzahl an Geräten** an.
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Generisches Zutrittskontrollmodul konfigurieren

Um ein generisches Zutrittskontrollmodul zu konfigurieren, muss es zunächst im Qognify VA Administrationstool angelegt werden (siehe „[Qognify VMS VA Administrationstool](#)“ auf Seite 513).



General	
Name:	Generic Access Control Module 9 SCHRI-HP
Server:	192.168.56.1:60619
Failover module	Do not use failover
Selected plugin:	Paxton Net2

Abb. 248: Generisches Zutrittskontrollmodul - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Ändern Sie gegebenenfalls den **Namen** des Moduls.
3. Wählen Sie ein **FailOver-Modul** aus (Qognify VMS Infinity X-Lizenz erforderlich).
4. Wählen Sie bei **Ausgewähltes Plugin** ein Plugin aus.
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Informationen zu weiteren Einstellungen finden Sie unter „[Event Interfaces](#)“ auf Seite 349.

Qognify Event Interface-(QEI-)Modul konfigurieren

Um ein Event Interface-Modul zu konfigurieren, muss es zunächst im Qognify VA Administrationstool angelegt werden (siehe „[Qognify VMS VA Administrationstool](#)“ auf Seite 513).

General	
General	
Name:	Event Interface Module 8 SCHRI-HP
Server:	192.168.56.1:60617
Failover module	Do not use failover
Plugin Details	
Manufacturer:	SeeTec
Type:	Plugin Sample
Version:	1.3
Remove from system	

Abb. 249: Event Interface-Modul - Allgemein

1. Wählen Sie das Modul in der Server-Funktion.
2. Ändern Sie gegebenenfalls den **Namen** des Moduls.
3. Wählen Sie ein **FailOver-Modul** aus (Qognify VMS Infinity X-Lizenz erforderlich).
4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
5. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Informationen zu weiteren Einstellungen finden Sie unter [„Event Interfaces“](#) auf [Seite 349](#).

Konfigurieren eines Body-Worn Camera Connector Moduls

Um ein Body-Worn Camera Connector Modul zu konfigurieren, müssen Sie es zuerst im Qognify VA-Administrationstool erstellen (siehe [„Hinzufügen eines Body-Worn Camera Connector Moduls“](#) auf [Seite 529](#)).

Wenn Sie das AXIS Body Worn-System von einem anderen VMS aus verschieben, um Qognify VMS sicherzustellen, dass bestehende Benutzer vom System-Controller exportiert werden, bevor das System zurückgesetzt und die Verbindungsdatei hochgeladen wird. Sie können die Benutzer importieren, nachdem das am Körper getragene System eingerichtet wurde.

1. Zurücksetzen des System Controllers auf die Werkseinstellungen.

Der System Controller muss auf die Werkseinstellung zurückgesetzt werden, bevor die von Qognify VMS erstellte Verbindungsdatei importiert werden kann. Wenn Sie das Ziel für den Inhalt ändern möchten, an das der System Controller das Video weiterleitet, müssen Sie den System Controller auf die Werkseinstellungen zurücksetzen.

General

Name:

Server:

IP Address:

Upload Path:

Video channel prefix:

Current certificate:

Select certificate

Certificate password:

Create connection file Remove from the system

Abb. 250: Body-Worn Camera Connector Modul

1. Wählen Sie das Modul in der Server-Funktion.
2. Ändern Sie gegebenenfalls den **Namen** des Moduls.
3. Geben Sie den Server und die IP-Adresse des Rechners an, auf dem das VA-Modul läuft.
4. Geben Sie den Pfad zum temporären Upload-Ordner ein, in dem die Videodateien der am Körper getragenen Kamera gespeichert werden (siehe [„Konfigurieren des Anschlusses der am Körper getragenen Kamera“](#) auf Seite 240).
5. Geben Sie das Präfix des anzuzeigenden Videokanals an. Dies hilft bei der Unterscheidung von am Körper getragenen Kamerakanälen gegenüber regulären IP-Kamerakanälen.
6. Wählen Sie ein P12-Zertifikat (für die Erstellung eines selbst-signierten P12-Zertifikats, siehe [„Selbst-signiertes P12-Zertifikat erstellen“](#) auf der nächsten Seite). Ein Webserver wird auf der angegebenen IP-Adresse und dem Port gestartet.

Der verwendete Port muss von der Firewall für eingehende Pakete zugelassen sein.

7. Geben Sie das Passwort des Zertifikats ein.
8. Wählen Sie **Verbindungsdatei erstellen**. Eine JSON-Datei wird in dem bereits festgelegten Ordner gespeichert.

Diese Datei muss manuell in den AXIS Body-Worn Camera System Controller im werkseitigen Standardzustand oder nach einem vollständigen Reset importiert werden.

9. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Selbst-signiertes P12-Zertifikat erstellen

Konfigurationsdatei für die Zertifikaterstellung definieren

1. Erstellen Sie eine neue .txt-Datei, indem Sie die App „Editor“ öffnen und folgenden Inhalt in die .txt-Datei einfügen.

```
1 [req]
2 default_bits = 2048
3 distinguished_name = req_distinguished_name
4 req_extensions = req_ext
5 x509_extensions = v3_req
6 prompt = no
7
8 [req_distinguished_name]
9 countryName = XX
10 stateOrProvinceName = N/A
11 localityName = N/A
12 organizationName = Self-signed certificate
13 commonName = VMS AxisBodyWornCamera Connector
14
15 [req_ext]
16 subjectAltName = @alt_names
17
18 [v3_req]
19 subjectAltName = @alt_names
20
21 [alt_names]
22 IP.1 = xxx.xxx.xxx.xxx
```

2. Ändern Sie die IP-Adresse in der Datei „certificate.conf“ auf die IP-Adresse des VA-Moduls, das mit dem Axis W800 System Controller kommunizieren wird. **Nur die konfigurierte IP-Adresse ist berechtigt, mit dem W800 System Controller zu kommunizieren.**

Vergewissern Sie sich, dass Sie die IP-Adresse des Computers dort einfügen, wo das AXIS Body Worn Camera VA-Modul ausgeführt wird.

3. Speichern Sie die Datei als „certificate.conf“.

Zertifikat-Erstellung

1. OpenSSL-Win64 oder OpenSSL-Win32 herunterladen und installieren (z. B.: <https://www.heise.de/download/product/win32-openssl-47316>).
2. Installieren Sie OpenSSL-Win64 und führen Sie „win64openssl-3_0_9.exe“ aus.
3. Wählen Sie für die Installation die Option „Windows system directory“.
4. Öffnen Sie OpenSSL als Befehlskonsole „Win64 OpenSSL Command Prompt“.

5. Führen Sie OpenSSL-Win64 mit folgenden Parametern über eine Befehlszeile aus (passen Sie den Parameter <full path> und die Gültigkeitsdauer auf Ihre Bedürfnisse an):

```
openssl req -x509 -newkey rsa:2048 -keyout <full path>\cert.key -out <full path>\cert.crt -days 365 -nodes -config <full path>\certificate.conf
```

Beispiel: `openssl req -x509 -newkey rsa:2048 -keyout C:\temp\cert.key -out C:\temp\cert.crt -days 365 -nodes -config C:\temp\certificate.conf`

Es werden zwei Dateien erstellt (cert.key und cert.crt).

Zertifikat-Konvertierung in das P12-Format

1. Öffnen Sie OpenSSL als Befehlskonsole „Win64 OpenSSL Command Prompt“.

- Führen Sie OpenSSL-Win64 mit folgenden Parametern über eine Befehlszeile aus und passen Sie die Parameter an <full path>:

```
openssl pkcs12 -inkey <full path>\cert.key -in <full path>\cert.crt -export -out <full path>\QVMS_certificate.p12
```

Beispiel: `openssl pkcs12 -inkey C:\temp\cert.key -in C:\temp\cert.crt -export -out C:\temp\FieldTest365.p12`

- Legen Sie ein Passwort für das Zertifikat fest. Das Passwort müssen Sie zu einem späteren Zeitpunkt beim Import des P12-Zertifikats in das VA-Modul eingeben.

```
Administrator: Win64 OpenSSL Command Prompt - openssl pkcs12 -inkey C:\temp\cert.key -in C:\temp\cert.crt -export -out C:\temp\FieldTest365.p12
Win64 OpenSSL Command Prompt
OpenSSL 3.0.9 30 May 2023 (Library: OpenSSL 3.0.9 30 May 2023)
built on: Wed May 31 00:24:47 2023 UTC
platform: VC-WIN64A
options: bn(64,64)
compiler: cl /Z7 /Fdssl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71 -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0xffffa32034f8bffff:0x8d19e27eb

C:\Users\Administrator>openssl pkcs12 -inkey C:\temp\cert.key -in C:\temp\cert.crt -export -out C:\temp\FieldTest365.p12
Enter Export Password:
Verifying - Enter Export Password: _
```

Im angegebenen Ordner wird eine Zertifizierungsdatei „QVMS_certificate.p12“ erstellt.

System

Mit der Funktion **System** im Steuerelement **Administration** können Sie u. a. systemweite Einstellungen zum Netzwerk, zu automatischen Backups sowie zu Kommunikationseinstellungen und zur Ereignisverwaltung konfigurieren und verwalten.

Die Systemverwaltung ist für alle Standorte gültig.

- Wählen Sie den Haupt-Standort im Steuerelement **Unternehmen** aus. Der gewählte Standort wird in der Titelleiste des Steuerelements Administration angezeigt.
- Wählen Sie **System** im Steuerelement Administration.

Videoklassifikation konfigurieren

Allgemein

Name	Delete
HD quality	<input type="button" value="Rename"/>
Standard quality	<input type="button" value="Rename"/>
Mobile	<input type="button" value="Rename"/>
Web	<input type="button" value="Rename"/>
Analytics	<input type="button" value="Rename"/>

Abb. 251: Videoklassifikation - Allgemein

1. Deaktivieren Sie **Zweiten Strom standardmäßig konfigurieren**. Neue Kameras werden dann mit nur einem konfigurierten Stream eingebunden. Ein zusätzlicher Stream muss manuell konfiguriert werden (siehe [Neuen Videostream erstellen](#)).
2. Um eine neue Videoklassifikation hinzuzufügen, wählen Sie **Hinzufügen** und geben Sie den **Namen** der Videoklassifikation an.
3. Bestätigen Sie mit **OK**. Die neue Videoklassifikation wird in der Liste angezeigt.
4. Um zur Löschung gekennzeichnete Videoklassifikationen zu löschen, wählen Sie die Video-Klassifikationen, die Sie löschen möchten, und klicken Sie **Löschen**.

Die Standard-Videoklassifikationen („HD Qualität“, „Standard Qualität“, „Mobile“, „Web“ und „Analytics“) können nicht gelöscht, sondern nur umbenannt werden.

5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Bandbreitenoptimierung

Abhängig von der Lizenz kann im Archivmodus ein bandbreitenoptimierter Videostream ausgewählt werden (siehe „Archiv Player“ auf Seite 178).

Für die Bereitstellung eines bandbreitenoptimierten Streams aus den archivierten Aufzeichnungen ist ein Transcoding-Kanal erforderlich (siehe „Transcodierungs-Engine-Modul hinzufügen“ auf Seite 518).

Bei Verwendung eines Multi Installation Login muss die Funktion bei allen verbundenen Installationen aktiviert werden, anderenfalls wird die bandbreitenoptimierte Wiedergabe nicht aktiviert (siehe „Installationsmanager“ auf Seite 88).

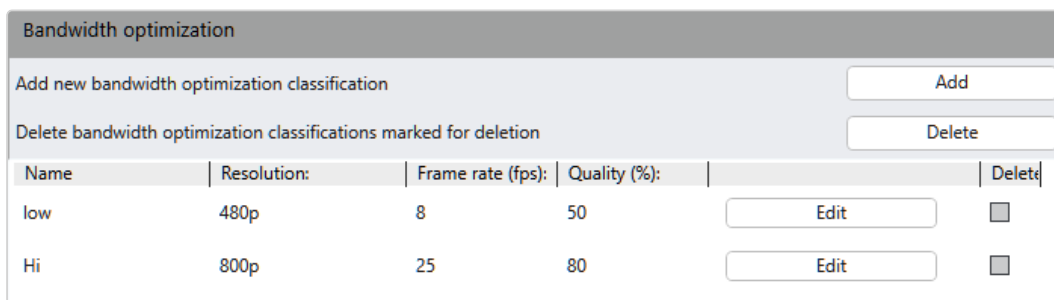


Abb. 252: Videoklassifikation - Bandbreitenoptimierung

Bandbreitenoptimierte Videoklassifikation hinzufügen

1. Wählen Sie **Hinzufügen**. Das Fenster für die Konfiguration der Videoklassifikation wird eingeblendet.



2. Geben Sie den **Namen** für die Videoklassifikation an.
3. Geben Sie die **Auflösung**, **Bildrate (fps)** und **Qualität (%)** an.
4. Bestätigen Sie mit **OK**. Die neue Videoklassifikation wird in der Liste angezeigt.

Bandbreitenoptimierte Videoklassifikation bearbeiten

1. Wählen Sie die betreffende Videoklassifikation aus und wählen Sie **Bearbeiten**. Das Fenster für die Konfiguration der Videoklassifikation wird eingeblendet.
2. Bearbeiten Sie die gewünschten Einstellungen.
3. Bestätigen Sie mit **OK**.

Bandbreitenoptimierte Videoklassifikation löschen

1. Wählen Sie die betreffende Videoklassifikation aus und wählen Sie **Löschen**.

Konfigurieren der Alarm-Klassifizierungen

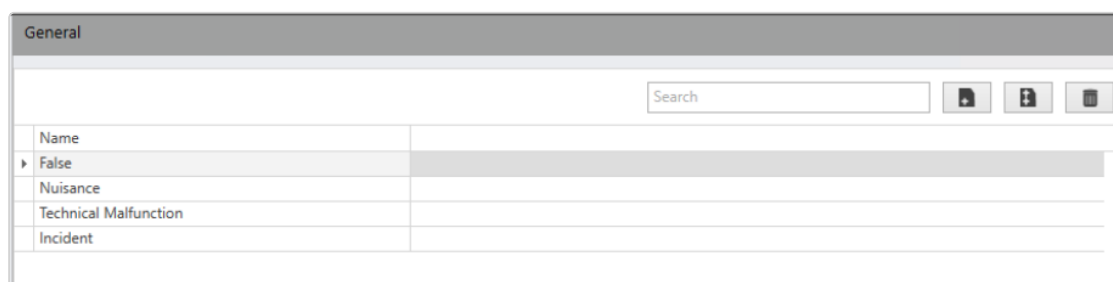





Abb. 253: Alarm-Klassifizierungen

Die Alarmkategorien werden in der Funktion **System** über die Alarmklassifizierungen definiert. Standardmäßig sind vier Klassifizierungen vorgesehen: „Falsch“, „Störung“, „Technische Störung“, „Vorfall“.

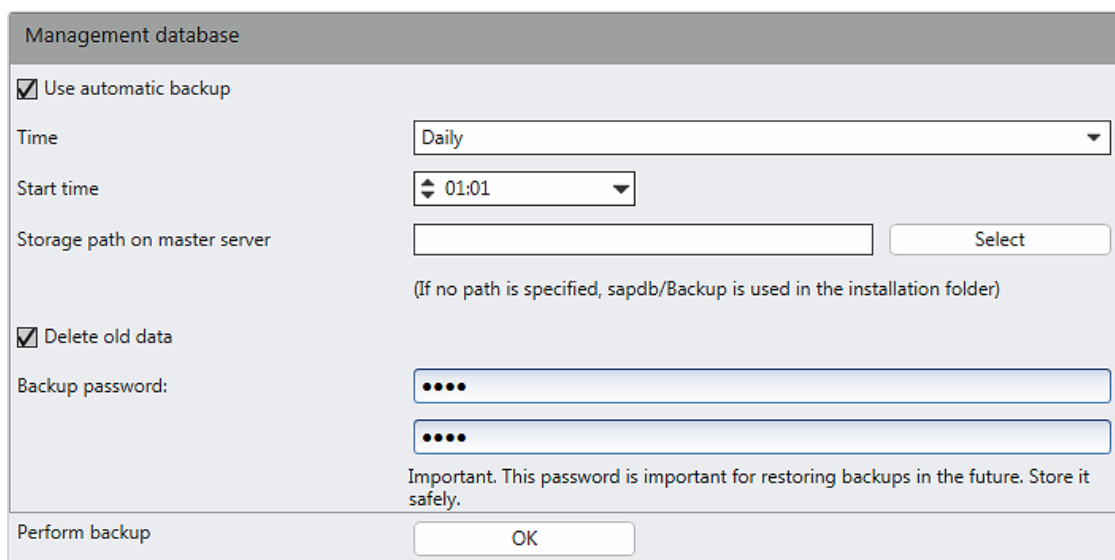
1. Wählen Sie Alarm-Klassifizierungen.
2. Doppelklicken Sie auf einen bestehenden Eintrag und ändern Sie den Namen, falls erforderlich.
3. Wählen Sie **Hinzufügen** , um einen einzelnen Artikel hinzuzufügen und seinen Namen zu bearbeiten.
4. Wählen Sie **Mehrere hinzufügen** , um der Liste zehn neue Einträge hinzuzufügen und deren Namen zu bearbeiten.
5. Markieren Sie einen bestehenden Eintrag in der Liste und wählen Sie **Löschen** , um die Klassifizierung aus der Liste zu entfernen.

Die Klassifizierung wird auch aus den entsprechend klassifizierten Alarmen entfernt.

6. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Backup konfigurieren

Die Standardeinstellung für die automatische Datensicherung der Verwaltungsdatenbank lautet täglich um 01:00 Uhr morgens. Für die Wiederherstellung einer Datensicherung wird das Administrationstool benötigt (siehe „[Qognify Administrationstool](#)“ auf Seite 501).



The screenshot shows a dialog box titled "Management database" with the following settings:

- Use automatic backup
- Time: Daily (dropdown menu)
- Start time: 01:01 (dropdown menu)
- Storage path on master server: [empty text box] [Select button]
- (If no path is specified, sapdb/Backup is used in the installation folder)
- Delete old data
- Backup password: [password input box]
- [password input box]
- Important. This password is important for restoring backups in the future. Store it safely.
- Perform backup: [OK button]

Abb. 254: Backup konfigurieren

1. Aktivieren Sie **Automatisches Backup verwenden**, um eine automatische zeitgesteuerte Datensicherung zu veranlassen.
2. Wählen Sie den **Zeitpunkt** und die **Startzeit** des Backups aus.
3. Passen Sie gegebenenfalls den **Speicherpfad** der Datensicherung an oder klicken Sie auf **Auswählen**, um das Verzeichnis direkt im Windows Explorer auszuwählen.

Der Export-Ordner kann nur ausgewählt werden, wenn der Client auf dem Core-Service-Hauptserver installiert ist. Anderenfalls muss der Speicherpfad des Exportverzeichnisses auf dem Server manuell eingegeben werden.

4. Aktivieren Sie **Alte Daten löschen**, um vor der Datensicherung bereits vorhandene Backups zu entfernen. Diese Einstellung gilt nur für die automatische Datensicherung. Es liegen maximal 8 Backups vor.

Das Backup-Verzeichnis sollte in regelmäßigen Abständen auf ein Bandlaufwerk oder andere Backup-Medien gesichert werden, damit die darin enthaltenen Datensicherungen auch nach einem Festplattendefekt noch zur Verfügung stehen.

5. Geben Sie das **Backup-Passwort** an. Die Datensicherungen werden mit AES-256 verschlüsselt, um sie vor Missbrauch zu schützen.

Das Backup-Passwort darf nicht leer sein.

6. Klicken Sie auf **Backup ausführen**, um die Datensicherung unmittelbar durchzuführen. Das Backup wird gestartet. Die Backup-Datei entspricht folgender Namensgebung: „Qognify_M_20yyymmdd.hhmm.zip“, wobei „yy“ das Jahrzehnt und „mm“ den Monat bezeichnen.

Beispiel „Qognify_M_20130725.1145.zip“ für eine manuelle Sicherung, die am 25. Juli 2013 um 11:45 Uhr durchgeführt wurde.

„Qognify_A_20130725.1145.zip“ für eine automatische Sicherung, die am 25. Juli 2013 um 11:45 Uhr durchgeführt wurde.

7. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
8. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Ereignisverwaltung konfigurieren

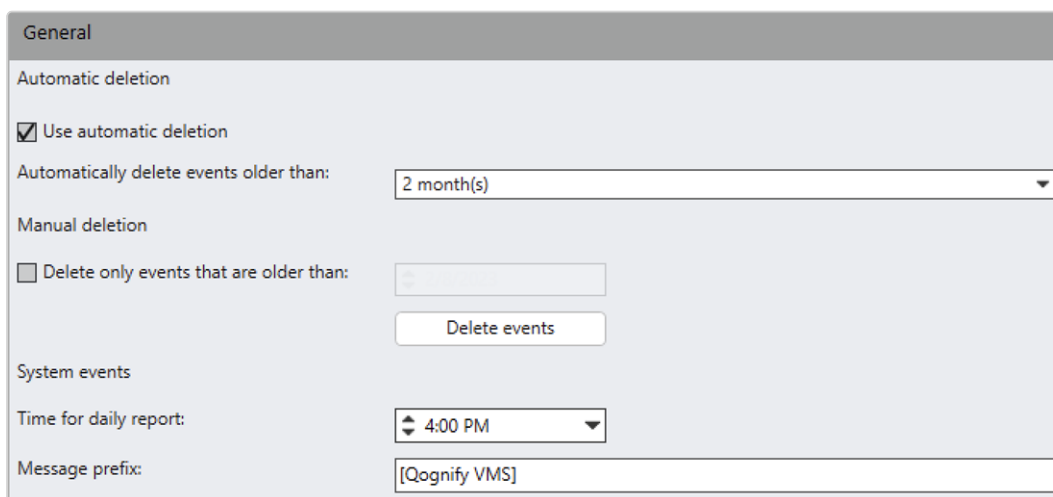
Während des Betriebs treten verschiedene Systemereignisse auf, die in der Systemdatenbank verwaltet werden. In der Ereignisverwaltung werden die Ereignisdatenbank sowie die Benachrichtigungseinstellungen für E-Mail und SNMP verwaltet.

Ereignisse werden in die Kategorien Fehler, Warnung und Info unterteilt.

Der Zugriff auf Videoquellen im Überwachungsmodus wird im entsprechenden Device Manager gespeichert (siehe „[Device Manager \(DM\) konfigurieren](#)“ auf Seite 436).

Aufgrund gesetzlicher Vorschriften in Frankreich werden bei Installationen in Frankreich diverse Ereignisse nie gelöscht. Stellen Sie sicher, dass die Verwaltungsdatenbank (MaxDB) ausreichend Speicher zu Verfügung hat. Die Kapazität der Verwaltungsdatenbank wird mit dem Qognify Administrationstool konfiguriert.

Allgemein



General

Automatic deletion

Use automatic deletion

Automatically delete events older than: 2 month(s)

Manual deletion

Delete only events that are older than:

Delete events

System events

Time for daily report: 4:00 PM

Message prefix: [Qognify VMS]

Abb. 255: Ereignisverwaltung - Allgemein

Automatische Bereinigung

1. Aktivieren Sie **Automatische Bereinigung verwenden** und wählen Sie den Zeitraum, nach dem die Ereignisdatenbank gelöscht werden soll (Standard: aktiv, Zeitraum: 2 Monate).
2. Aktivieren Sie für die manuelle Bereinigung **Nur Ereignisse löschen, die älter sind als** und legen Sie den Zeitraum fest.

3. Klicken Sie auf **Ereignisse löschen**, um die Ereignisse des gewählten Zeitraums aus der Datenbank zu entfernen.




Systemereignisse

Die Software kann per E-Mail einen täglichen Bericht zum Systemstatus senden. Zu diesem Zweck müssen ein SMTP-Server (siehe „[SMTP-Server konfigurieren](#)“ auf Seite 476) sowie E-Mail-Adressen (siehe „[E-Mail-Verwaltung konfigurieren](#)“ auf Seite 477) konfiguriert werden.

1. Legen Sie die **Uhrzeit für den täglichen Bericht** der Systemereignisse fest. Die E-Mail mit dem Bericht der aufgetretenen Ereignisse der letzten 24 Stunden wird an alle E-Mail-Adressen gesendet, die in der E-Mail-Verwaltung als Systemadressen eingetragen sind.
2. Fügen Sie bei Bedarf ein **Nachrichtenpräfix** hinzu, das an die Nachricht angehängt wird, um diese zu identifizieren.

Benachrichtigungen

Ereignisse werden nach ihrer Häufigkeit gruppiert und anhand der folgenden Kriterien klassifiziert:

- Fehler  : Fehler sind schwerwiegende Ereignisse, die die Funktion der Software beeinträchtigen. Administrative Maßnahmen sind erforderlich (siehe „[Fehler](#)“ auf der nächsten Seite).
- Warnungen  : Warnungen sind systemrelevante Ereignisse, die die Funktion des gesamten Systems oder von Teilen des Systems beeinträchtigen können. In der Regel sind schnelle administrative Maßnahmen erforderlich (siehe „[Warnungen](#)“ auf Seite 472).
- Info  : Infos sind systemrelevante Ereignisse, die sich nicht auf die Funktion des gesamten Systems oder von Teilen des Systems auswirken. In der Regel sind keine administrativen Maßnahmen erforderlich (siehe „[Info](#)“ auf Seite 474).

Die einzelnen Benachrichtigungen können bearbeitet werden (siehe „[Benachrichtigungen bearbeiten](#)“ auf Seite 475).

Fehler

Folgende Fehler lösen eine Benachrichtigung aus:

- **Fehler beim Ändern der Lizenzdatei:** Die Lizenzdatei im Verzeichnis „conf“ kann nicht geändert werden. Mögliche Gründe sind eine ungültige Lizenzdatei oder geänderte Benutzerrechte.
- **Flatfile-Protokollierung: Alarmdatei kann nicht geschrieben werden:** Die Flatfile-Protokollierung kann in der Konfiguration des Cre Service Main eingerichtet werden. Mögliche Gründe für Fehler sind geänderte Benutzerrechte für das Freigabevolumen oder unzureichender Speicherplatz.
- **Flatfile-Protokollierung: Zusammenfassungsdatei kann nicht geschrieben werden:** Die Flatfile-Protokollierung kann in der Konfiguration des Cre Service Main eingerichtet werden. Mögliche Gründe für Fehler sind geänderte Benutzerrechte für das Freigabevolumen oder unzureichender Speicherplatz.
- **Prüfung der Diensteüberwachung fehlgeschlagen:** Der Benutzer wird benachrichtigt, wenn ein Dienst, z. B. der Device Manager, der MDS oder der Video Analytics-Dienst, aufgrund von Netzwerkproblemen ausfällt.
- **Diensteüberwachung nicht verfügbar:** Das Modul zur Überwachung der Dienste kann nicht geladen werden und keine Meldung zu ausgefallenen Diensten ausgeben.
- **Die Konfigurations- und Ereignisdatenbank ist voll:** Das Datenvolumen der MaxDB beträgt nach einer Standardinstallation 4 GB. Die Größe kann mit dem Administrationstool angepasst werden (siehe [„Qognify Administrationstool“ auf Seite 501](#)).
- **Zone der MultimediaDatabase konnte nicht eingebunden werden:** Ohne Zone können keine Videodaten aufgezeichnet werden. Mögliche Gründe sind ein falscher Serverpfad oder fehlende Berechtigungen. Die Zoneneinstellungen müssen überprüft werden (siehe [„Verwaltungsdatenbank \(MaxDB\)“ auf Seite 503](#)).

- **MultimediaDatabase konnte nicht gestartet werden:** Der MDS kann nicht gestartet werden. Ein möglicher Grund kann mangelnder Speicherplatz sein (Zone ist voll).
- **MultimediaDatabase-Statistik ist nicht verfügbar:** Die Statistik kann nicht erstellt werden. Wenden Sie sich an den Qognify-Support.
- **Zone der MultimediaDatabase ist voll:** Die Speicherbelegung hat 95 % erreicht. Der Edge-Speicher löscht die ältesten Aufzeichnungen (siehe [„Bildspeicherung“ auf Seite 252](#)).
- **Ein Dienst meldet einen Speicherüberlauf:** Dies betrifft die Dienste VMS_Core, VMS_DM und VMS_MDS. Wenden Sie sich an den Qognify-Support.
- **Ein Dienst wurde unerwartet beendet:** Wenden Sie sich an den Qognify-Support.
- **LPR-Dongle nicht gefunden:** Die Kennzeichenerkennung funktioniert nicht, da der LPR-Dongle fehlt (siehe [„LPR-Modus“ auf Seite 487](#)).
- **Ausfall der Bildanalyse bei zu wenig Licht:** Dieser Fehler betrifft die Videoanalyse (siehe [„Qognify Video Analytics“ auf Seite 315](#)). Wenn im Bild nicht genug Details erkannt werden können, schlägt die Bildanalyse fehl.
- **Ausfall der Bildanalyse bei Verdrehung:** Dieser Fehler betrifft die Videoanalyse (siehe [„Qognify Analytics“ auf Seite 327](#)). Wenn das Bild aufgrund einer Kameramanipulation verdreht ist, kann das Bild nicht analysiert werden.
- **Keine zusätzlichen Threads verfügbar:** Die Systemressourcen sind voll. Wenden Sie sich an den Qognify-Support.
- **VA-Kommunikation mit Drittanbieter-System unterbrochen:** Die Netzwerkverbindung des VA-Moduls wurde wahrscheinlich unterbrochen. Überprüfen Sie das Drittanbieter-System, die Netzwerkeinstellung oder die VA-Konfiguration (siehe [„Qognify VMS VA Administrationstool“ auf Seite 513](#)).

- **VA-Dienst hat Videosignal verloren:** Der VA-Dienst benötigt einen zuverlässigen Videostream, z. B. für die Bewegungserkennung. Mögliche Gründe sind der Verlust der Netzwerkverbindungen oder Kameraprobleme.
- **AV-Export fehlgeschlagen:** Der AV-Export funktioniert nicht. Ein möglicher Grund kann eine Einstellung in der AV-Konfiguration sein (siehe [„Qognify VMS VA Administrationstool“ auf Seite 513](#)).
- **Bildstrom kann nicht aufgebaut werden:** Der Device Manager kann keinen Bildstrom von der Kamera aufbauen. Mögliche Gründe können Netzwerk- oder Kameraprobleme sein.
- **Gerät kann nicht gestartet werden:** Eine Kamera oder ein anderes Hardwaregerät ist nicht verfügbar. Ein möglicher Grund kann ein Hardwaredefekt sein.
- **Die Initialisierung des Dienstes VMS_DM ist fehlgeschlagen:** Der DM-Dienst kann nicht gestartet werden. Weitere Informationen finden Sie im Logfile oder wenden Sie sich an den Qognify-Support (siehe [„Support“ auf Seite 13](#)).
- **Benutzer deaktiviert:** Der Benutzer wird nach einer voreingestellten Anzahl von fehlgeschlagenen Anmeldeversuchen deaktiviert (siehe [„Benutzer-Sicherheitseinstellungen konfigurieren“ auf Seite 484](#)).

Warnungen

Folgende Warnungen lösen eine Benachrichtigung aus:

- **Zyklisches Backup der Konfigurations- und Ereignisdatenbank ist fehlgeschlagen:** Das zyklische Backup der Systemdatenbanken ist fehlgeschlagen (siehe [„Backup konfigurieren“ auf Seite 466](#)).
- **Sub Core nicht erreichbar:** Wenn mehrere Core Service Server installiert sind, kann der Core Service Sub nicht erreicht werden (siehe [„Kerndienste und Filialen“ auf Seite 22](#)).

- **Die Konfigurations- und Ereignisdatenbank ist fast voll:** Das Datenvolumen der MaxDB beträgt nach einer Standardinstallation 4 GB. Die Größe kann mit dem Administrationstool angepasst werden (siehe [„Qognify Administrationstool“ auf Seite 501](#)).
- **Automatischer MDB-Video-Backup unterbrochen:** Der automatische Videodaten-Backup wurde unterbrochen (siehe [„Video-Backup/-Export“ auf Seite 274](#) und [„Video-Backup“ auf Seite 442](#)).
- **Das letzte Archivbild ist älter als der konfigurierte Wert:** Ein Konfigurationsfehler ist aufgetreten (siehe [„MultimediaDatabase“ auf Seite 252](#)).
- **Schwellenwerte der DM-Statistik wurden überschritten:** Wenn bestimmte Schwellenwerte der Device Manager-Statistik überschritten wurden, kann eine Benachrichtigung gesendet werden (siehe [„Allgemein“ auf Seite 437](#)).
- **Zone fast voll:** Es verbleiben nur noch 15 % des verfügbaren Video-Speicherplatzes. Sobald die Speicherbelegung 95 % erreicht, löscht das Ringspeicher-System die ältesten Aufzeichnungen (siehe [„Bildspeicherung“ auf Seite 252](#)).
- **Systemzeit geändert:** Die Änderung der Systemzeit wirkt sich auf die Zeitstempel des Archivs oder das Client-Verhalten aus, wenn diese nicht mit dem CoreService-Server synchron sind.
- **AV-Export älter als zwei Stunden:** Die Konfiguration an der Kamera muss angepasst (siehe [„Video-Backup/-Export“ auf Seite 274](#)) und in den Alarmeinstellungen aktiviert werden (siehe [„E-Mail und FTP“ auf Seite 402](#)).
- **AV-Export älter als vier Stunden:** Die Konfiguration an der Kamera muss angepasst (siehe [„Video-Backup/-Export“ auf Seite 274](#)) und in den Alarmeinstellungen aktiviert werden (siehe [„E-Mail und FTP“ auf Seite 402](#)).
- **Edge-Speicher-Import wurde unterbrochen:** Eine Benachrichtigung wird ausgelöst, wenn ein Edge-Speicher-Import fehlgeschlagen ist (siehe [„Allgemein“ auf Seite 437](#)).

- **Verlust des Videosignals am Encoder erkannt:** Diese Funktion muss in der Kamerakonfiguration aktiviert werden (siehe „[Manipulationserkennung](#)“ auf Seite 282). Darüber hinaus kann dieses Ereignis als Alarmauslöser verwendet werden (siehe „[Alarm konfigurieren](#)“ auf Seite 391).
- **Dienste wurden gestoppt:** Überprüfen Sie die Qognify-Dienste neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511).
- **Manipulationsalarm:** Diese Funktion muss in der Kamerakonfiguration aktiviert werden (siehe „[Manipulationserkennung](#)“ auf Seite 282). Darüber hinaus kann dieses Ereignis als Alarmauslöser verwendet werden (siehe „[Alarm konfigurieren](#)“ auf Seite 391).

Info

Folgende Informationen lösen eine Benachrichtigung aus:

- **Lizenzdatei erfolgreich geändert:** Beim CoreService-Server wurde eine Lizenzdatei erfolgreich registriert.
- **Automatischer MDB-Video-Backup abgeschlossen:** Der automatische Videodaten-Export ist abgeschlossen (siehe „[Video-Backup/-Export](#)“ auf Seite 274 und „[Video-Backup](#)“ auf Seite 442).
- **Automatischer MDB-Video-Backup gestartet:** Der automatische Videodaten-Export wurde gestartet (siehe „[Video-Backup/-Export](#)“ auf Seite 274 und „[Video-Backup](#)“ auf Seite 442).
- **Wiederherstellung ausgefallener Bildanalyse:** In manchen Fällen kann eine unterbrochene Kalibrierung der Videoanalyse nicht wiederhergestellt werden.
- **VA-Videosignal wiederhergestellt:** Ein verloren gegangenes Videosignal konnte wiederhergestellt werden.
- **Edge-Speicher-Import war erfolgreich:** Der Edge-Speicher-Import wurde erfolgreich abgeschlossen.
- **Dienste wurden neu gestartet:** Wenn ein Dienst angehalten wird, z. B. aufgrund eines Updates, wird er automatisch neu gestartet.

Benachrichtigungen bearbeiten

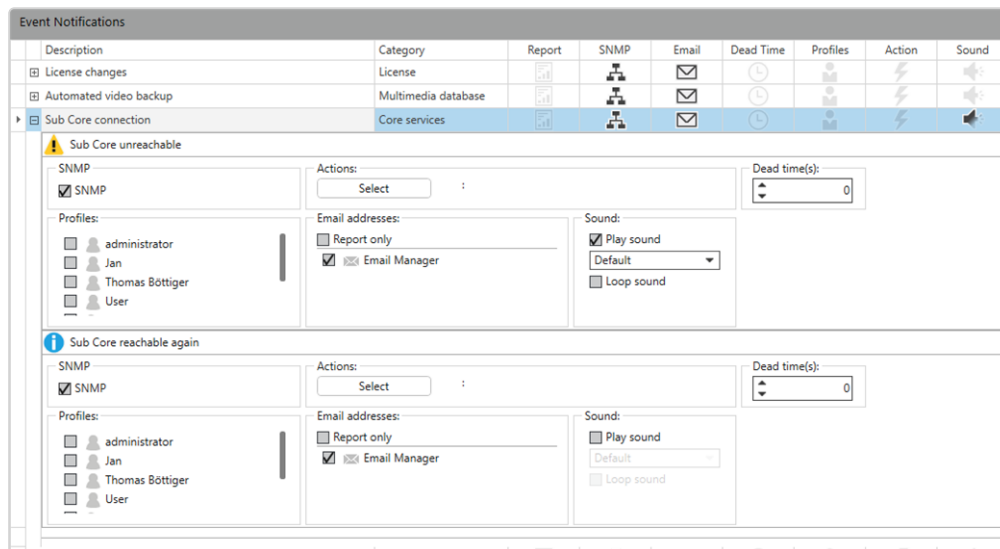


Abb. 256: Benachrichtigungen bearbeiten

1. Markieren Sie das Ereignis in der Liste, und wählen Sie:
 - ob das Ereignis nur im täglichen Bericht der Systemereignisse angezeigt werden soll, der per E-Mail gesendet wird (siehe „SMTP-Server konfigurieren“ auf der nächsten Seite und „E-Mail-Verwaltung konfigurieren“ auf Seite 477).
 - ob eine SNMP-Trap an einen Verwaltungshost gesendet wird, wenn das Ereignis auftritt (siehe auch „SNMP-Server konfigurieren“ auf Seite 477).
2. Um ein Ereignis oder mehrere Ereignisse zu bearbeiten, markieren Sie es in der Spalte **Bearbeiten** und klicken Sie auf **Markierte Objekte bearbeiten**.
3. Legen Sie fest, ob eine **Aktion** durchgeführt werden soll:
 - an welche Empfänger eine E-Mail verschickt werden soll,
 - bei welchen **Profilen** eine Meldung im Überwachungsmodus angezeigt werden soll.
 - ob ein Ton abgespielt wird, wenn das Ereignis eintritt, welcher Ton abgespielt werden soll und ob er wiederholt wird. Informationen zu benutzerdefinierten Sounds „Ton- und Symboldateien mit benutzerdefinierten Medien verwalten“ auf Seite 482.

4. Klicken Sie auf **Zur Übersicht zurückkehren**, um zur Liste der Ereignisse zurück zu navigieren.
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

SMTP-Server konfigurieren

Damit die Qognify-Dienste ein Fehlverhalten oder den Ausfall einer Kamera melden können, benötigt die Software die Daten eines erreichbaren SMTP-Servers.

1. Aktivieren Sie den SMTP-Server.
2. Geben Sie die Netzwerkadresse des SMTP-Servers und die SMTP-Portnummer an.
3. Geben Sie den **Benutzernamen** und das **Passwort** für den Benutzer-Account ein.
4. Wählen Sie gegebenenfalls die Verschlüsselungsmethode, mit der die E-Mails übertragen werden sollen. Folgende Verschlüsselungsmethoden stehen zur Verfügung: SSL und TSL.
5. Tragen Sie die **Absenderadresse** ein.
6. Klicken Sie auf **Test-E-Mail senden**, um die angegebenen Einstellungen zu überprüfen.
7. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
8. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Internetdienste wie Google blockieren Anmeldeversuche möglicherweise. In diesem Fall müssen Sie Ihr Google-Konto so konfigurieren, dass der Zugriff auf Ihr Konto für weniger sichere Apps erlaubt wird.

E-Mail-Verwaltung konfigurieren

Die E-Mail-Listen verwenden Sie für den Versand der Systemmeldungen (siehe „[Ereignisverwaltung konfigurieren](#)“ auf Seite 468). Diese E-Mail-Adressen werden auch für den Versand des Berichts verwendet (siehe „[SNMP-Server konfigurieren](#)“ unten).

1. Klicken Sie auf **Neue E-Mail-Liste hinzufügen** und geben Sie den Namen für die neue Liste an.
2. Bestätigen Sie mit **OK**. Die neue Liste wird angezeigt.
3. Um die Liste zu entfernen, aktivieren Sie die Liste und klicken Sie auf **Als „Löschen“ markierte Liste löschen**. Alle aktivierten Listen (außer Alarm-Adressen und System-Adressen) werden gelöscht.

Alarm-Adressen und System-Adressen

Die Listen der Alarm-Adressen und der System-Adressen sind bereits angelegt. Die Systemmeldungen werden standardmäßig an alle unter System-Adressen hinterlegten E-Mail-Adressen gesendet.

1. Wählen Sie die gewünschte Liste aus.
2. Klicken Sie auf **Neue E-Mail-Adresse hinzufügen** und geben Sie die neue E-Mail-Adresse ein.
3. Bestätigen Sie mit **OK**. Die neue E-Mail wird in der Liste angezeigt.
4. Um die E-Mail-Adresse zu ändern, klicken Sie auf **Umbenennen**.
5. Um die E-Mail-Adresse zu entfernen, aktivieren Sie die E-Mail und klicken Sie auf **Als „Löschen“ markierte E-Mail-Adressen löschen**. Alle aktivierten E-Mail-Adressen werden gelöscht.

SNMP-Server konfigurieren

Es können SNMP v1-, v2- und v3-Traps versendet werden.

1. Aktivieren Sie den SNMP-Server, um Systemfehler über SNMP-Nachrichten zu melden.
2. Tragen Sie den **ManagementHost** ein.
3. Geben Sie den **ManagementHostTrapListenPort**, den **LocalTrapSendPort** und den **CommunityString** gemäß den Einstellungen an, die Sie für Ihren SNMP-Server benötigen.

Falls in der Systemsteuerung > Software > Windows-Komponenten hinzufügen/entfernen > Verwaltungs- und Überwachungsprogramme die Komponente SNMP (Simple Network Management Protocol) installiert ist, muss ein anderer Port für LocalTrapSendPort eingetragen werden, da über den Port 161 nicht gesendet werden kann. In der Voreinstellung ist der Port 161 eingetragen, dieser funktioniert dann nicht.

MIB (Management Information Base)

Zur Überwachung des aktuellen Status von Qognify VMS in einer Drittanbieter-Überwachungslösung wird zusammen mit dem Core Service im Installationsverzeichnis „/tools/MIB“ die MIB-Datei (Management Information Base) „vms.mib“ installiert. Sobald die MIB-Datei in die PRTG-Software eingelesen wurde, sind die Beschreibungen für SNMP v1- und SNMP v2-Traps verfügbar.

PRTG ist eine Netzwerküberwachungssoftware, die auf einem Windows-Gerät innerhalb des Netzwerks ausgeführt werden kann. Sie sammelt Statistiken von verschiedenen Hosts wie Routern, Servern, Switches und anderen wichtigen Geräten oder Anwendungen.

SNMP v1/v2

1. Aktivieren Sie **SNMP v1** oder **SNMP v2**. SNMP v2 bietet zusätzlich einfache Sicherheits-Features, SNMP v1 hingegen nicht.
2. Geben Sie den **CommunityString** an, sodass korrekte Antworten vom Host möglich sind.

SNMP v3

SNMP v3 ist die derzeit sicherste Protokollversion.

1. Aktivieren Sie **SNMP v3**.
2. Geben Sie den **Sicherheitsnamen**, den **Authentifizierungstyp**, das **Authentifizierungspasswort**, den **Verschlüsselungstyp** und das **Verschlüsselungspasswort** ein.
3. Um die Einstellungen zu testen, klicken Sie auf **SNMP-Testnachricht** senden, um die angegebenen Einstellungen zu überprüfen.
4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
5. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

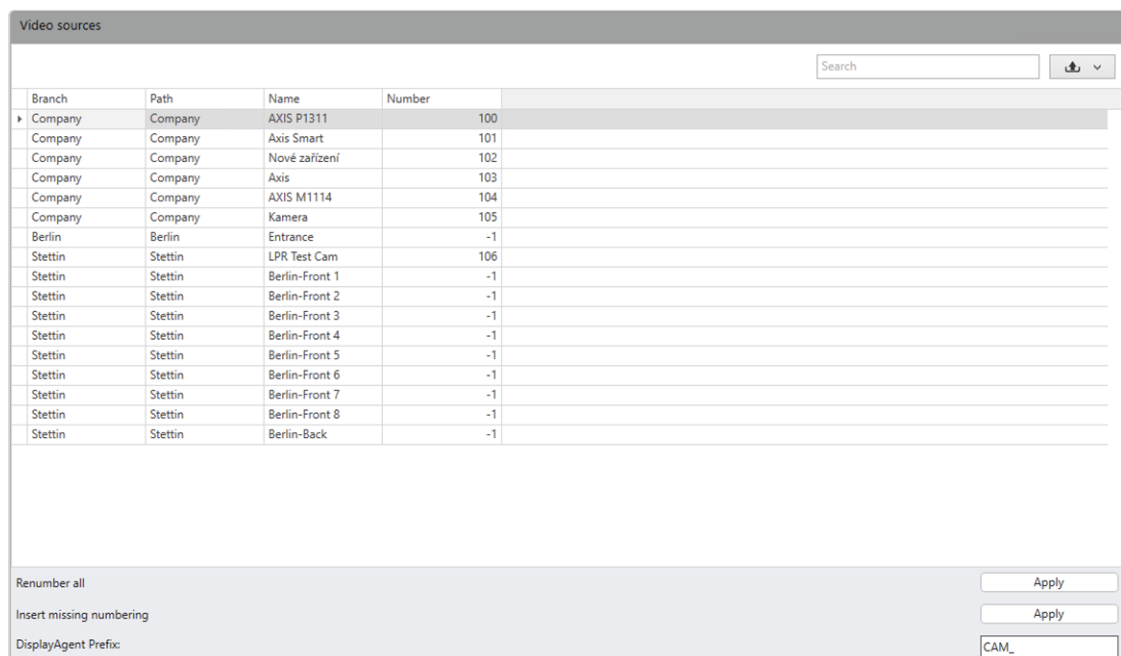
NAT-Liste konfigurieren

Um auf die Qognify-Software per NAT über das Internet ohne VPN-Tunnel zugreifen zu können, muss auf Ihrem Router bzw. in Ihrer Firewall die Port-Weiterleitung (Forwarding) aktiviert werden. Standardmäßig werden für NAT die Ports 60000-60008 benötigt.

Diese Ports müssen auf allen abgesetzten Servern offen sein.

1. Klicken Sie auf **Neuen NAT-Eintrag hinzufügen**.
2. Geben Sie die interne und die öffentliche Adresse an.
3. Um einen Eintrag zu entfernen, wählen Sie die Liste aus, aktivieren Sie **Löschen** am Ende jeder Zeile und klicken Sie auf **Als „Löschen“ markierte NAT-Einträge löschen**.
4. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
5. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Entitäten-Nummerierung konfigurieren



Branch	Path	Name	Number
Company	Company	AXIS P1311	100
Company	Company	Axis Smart	101
Company	Company	Nové zařízení	102
Company	Company	Axis	103
Company	Company	AXIS M1114	104
Company	Company	Kamera	105
Berlin	Berlin	Entrance	-1
Stettin	Stettin	LPR Test Cam	106
Stettin	Stettin	Berlin-Front 1	-1
Stettin	Stettin	Berlin-Front 2	-1
Stettin	Stettin	Berlin-Front 3	-1
Stettin	Stettin	Berlin-Front 4	-1
Stettin	Stettin	Berlin-Front 5	-1
Stettin	Stettin	Berlin-Front 6	-1
Stettin	Stettin	Berlin-Front 7	-1
Stettin	Stettin	Berlin-Front 8	-1
Stettin	Stettin	Berlin-Back	-1

Abb. 257: Entitäten Nummerierung

Die ID Entitäten-Nummerierung wird **nicht** vom System vergeben. Wenn Entitäten-Nummerierungen verwendet werden, müssen diese manuell konfiguriert werden. Die Nummer dient als Referenz für das SDK oder die Tastenzuordnung der Tastatur mit vir-

tuellen Sequenzen (siehe „[Eingabegeräte](#)“ auf Seite 79). Diese kann auch nachträglich angepasst werden.

Die maximale Entitäten-Nummerierung ist 99.999.999.

1. Passen Sie gegebenenfalls die Entitäten-Nummer der Geräte an, indem Sie die neue ID direkt in das Textfeld eingeben oder mit den Pfeiltasten schrittweise nach oben oder unten zählen.

Ändern Sie die Entitäten-Nummerierung nur bei Bedarf während der Konfiguration der Software von Drittherstellern.


2. Wählen Sie **Alles erneut nummerieren**, um jedem Gerät eine eindeutige Entitäten-Nummer durch Auswahl einer Startnummer zuzuweisen. Nach Angabe der Startnummer Qognify VMS werden die Nummern automatisch in Schritten von „1“ erhöht.

Nur sichtbare Einträge werden neu nummeriert.

3. Wählen Sie **Fehlende Nummerierung einführen**, um Geräten ohne Entitäten-Nummer eine eindeutige Entitäten-Nummer zuzuweisen. Qognify VMS verwendet automatisch die höchste Zahl in der Liste und ein Inkrement von „1“.
4. Legen Sie das **DisplayAgent-Präfix** fest. Es sind vier konfigurierbare Präfixe für Kameras, Ansichten, Fenster und Kacheln verfügbar (siehe „[Mit dem DisplayAgent-Präfix arbeiten](#)“ auf der gegenüberliegenden Seite). Zulässige Kombinationen:
 - Kamera auf Fenster
 - Kamera auf Kachel
 - Ansicht auf Fenster
 - Wächterrundgang-Sequenzen (siehe „[Kameras sequenziell wechseln](#)“ auf der gegenüberliegenden Seite)
5. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
6. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Exportieren der Entitäten-Nummerierung

Die Liste der Entitäten-Nummerierungen kann als PDF-Datei oder als kommagetrenntes Dokument exportiert werden, das mit jedem Tabellenkalkulationsprogramm importiert werden kann.

1. Wählen Sie **Exportieren** ()
2. Wählen Sie das Exportdateiformat (PDF oder CSV).
3. Wählen Sie den Ordner und klicken Sie auf **Speichern**.

Kameras sequenziell wechseln

Die Kamerasequenz kann so eingestellt werden, dass sie in einer Kachel nacheinander angezeigt werden, z. B. für Wächterrundgänge. Die Kamerasequenz wird in einer Endlosschleife durchlaufen, bis in derselben Kachel etwas anderes angezeigt wird.

Es ist möglich, in verschiedenen Kacheln im selben Display Agent unterschiedliche Kamerasequenzen gleichzeitig laufen zu lassen.

1. Wählen Sie **Wächterrundgänge** aus.
2. Ändern Sie die Entitäten-Nummer des Wächterrundgangs, um eine Sequenz zu definieren.
3. Legen Sie das **DisplayAgent-Präfix** fest.

Mit dem DisplayAgent-Präfix arbeiten

Wenn das DisplayAgent-Präfix aktiviert ist, kann der Absender für jeden Befehl eine neue Verbindung öffnen oder unterschiedliche Befehle durch einen Zeilenenumbruch (CR, LF oder CRLF) trennen. Der Parser sucht nach den Präfixen und einer direkt darauffolgenden Zahl. Alle anderen Zeichen werden ignoriert.

Der einfachste Befehl hat das Format CAM_1 WINDOW_1, es können jedoch auch Befehle wie DUMMY_HEADER CAM_1 SOME_TEXTWINDOW_1 gesendet werden.¹

Alarm-WatchDog konfigurieren

Der Alarm-Watchdog überwacht die Alarme mehrerer installierter Qognify-Systeme gleichzeitig. Wenn in einem der überwachten Systeme ein Alarm auftritt, kann der Benutzer eine Verbindung zum System herstellen und den Alarm anzeigen. Um die entsprechende Alarmübertragung zu aktivieren, legen Sie die Alarm-Watchdog-Option in

¹Beide Nachrichten werden als „Kamera 1 auf Fenster 1 anzeigen“ interpretiert.

den Servereinstellungen des betreffenden Alarmszenarios fest (siehe „[Alarmer](#)“ auf [Seite 386](#)).

Jedes System kann nur mit einem Alarm-Watchdog verbunden werden.

1. Um den Alarm-Watchdog zu konfigurieren, wählen Sie **Alarm-Watchdog** in der System-Steuerleiste aus.
2. Aktivieren Sie den Alarm-Watchdog und geben Sie die IP-Adresse und Portnummer (Standard: 12000) des Clients an, auf dem der Alarm-Watchdog installiert ist. Informationen zum Abrufen der korrekten IP-Adresse finden Sie im Abschnitt zur Alarm-Watchdog-Konfiguration (siehe „[Alarm-WatchDog konfigurieren](#)“ auf [Seite 573](#)).
3. Geben Sie die IP-Adresse und die Portnummer des VMS-Servers an. Alle zu überwachenden Clients müssen mit diesem Server verbunden werden.
4. Legen Sie den **Benutzernamen** und das **Passwort** des Benutzers fest, der sich im Fall eines Alarms am Server anmeldet.
5. Legen Sie das Benutzerprofil fest (Standard: Benutzername).
6. Geben Sie eine Beschreibung für den Server ein.
7. Aktivieren Sie **NAT**, wenn der Client den Server nur über NAT (Network Address Translation) erreichen kann, z. B. über einen Router.
8. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten.
9. **Speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Ton- und Symboldateien mit benutzerdefinierten Medien verwalten

Mit der Funktion „Benutzerdefinierte Medien“ können Sie Ihre eigenen Ton- und Symboldateien verwalten. Benutzerdefinierte Symbole und Töne werden in der Verwaltungsdatenbank gespeichert. Die Ton- und Symboldateien können auf gewünschte Elemente angewendet werden, z. B. benutzerdefinierte Symbole für Kameras.

Bilddateien hochladen und löschen

Um höchste Qualität sicherzustellen, wird empfohlen, Bilddateien mit geringer Komplexität (bei Anzeige als Symbole) und 512 x 512 Pixel (bei Verwendung für Lagepläne und größere Formate) zu verwenden.

1. Klicken Sie auf **Hinzufügen**, um eine benutzerdefinierte Bilddatei aus dem Dateisystem hinzuzufügen. Folgende Bildformate werden unterstützt: PNG, JPG, GIF.
2. Klicken Sie auf **Speichern**, um die Bilder in den Server hochzuladen. Für eine bessere Leistung werden Sie im lokalen Cache gespeichert. Nachdem die Bilder erfolgreich hochgeladen wurden, wird das Dateisymbol angezeigt.
3. Klicken Sie auf **Bearbeiten**, um die Datei umzubenennen.
4. Wenn Sie das Bild löschen möchten, klicken Sie auf **Löschen**. Nach dem Neustart des Clients werden alle zugewiesenen Elemente mit ihren Standardsymbolen angezeigt.

Tondateien hochladen und löschen

1. Klicken Sie auf **Hinzufügen**, um eine benutzerdefinierte Tondatei aus dem Dateisystem hinzuzufügen. Folgende Tonformate werden unterstützt: MP3, WAV.
2. Klicken Sie auf **Speichern**, um die Tondateien in den Server hochzuladen. Für eine bessere Leistung werden Sie im lokalen Cache gespeichert.
3. Klicken Sie auf **Bearbeiten**, um die Datei umzubenennen oder den ausgewählten Ton abzuspielen.
4. Wenn Sie die Tondatei löschen möchten, klicken Sie auf **Löschen**. Nach dem Neustart des Clients werden alle zugewiesenen Elemente auf ihre Standardtöne zurückgesetzt.

Benutzerdefinierte Medien zuweisen

1. Um die benutzerdefinierten Dateien Elementen zuzuweisen, rufen Sie im Konfigurationsmodus folgende Einstellungen auf:
 - Kamera - Allgemein: Wenn das benutzerdefinierte Symbol einer Kamera zugewiesen wird, wird es für diese Kamera im gesamten System angezeigt.
 - Hardware-Einstellungen
 - Lagepläne
 - Videowand
 - Ansichten

Benutzer-Sicherheitseinstellungen konfigurieren

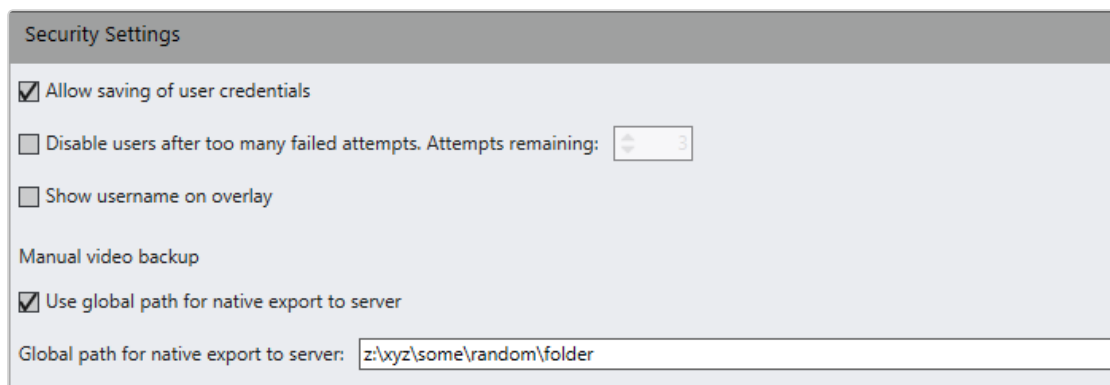


Abb. 258: Sicherheitseinstellungen

Zur Einhaltung der DSGVO-Bestimmungen gemäß EU-Recht kann die automatische Speicherung von Benutzer-Anmeldedaten deaktiviert werden. Sie ist standardmäßig für alle Benutzer aktiviert und kann nur pro Installation aktiviert oder deaktiviert werden. Darüber hinaus kann die Anzahl der Anmeldeversuche begrenzt werden.

1. Wählen Sie **Sicherheitseinstellungen** in der System-Steuerleiste.
2. Deaktivieren Sie die Speicherung der Benutzer-Anmeldedaten. Wenn diese deaktiviert ist, müssen die Benutzer-Anmeldedaten bei der Anmeldung eingegeben werden.
3. Aktivieren Sie **Benutzername bei Überlagerung anzeigen**, um den aktuellen Benutzer der Kamera im oberen Teil des Bildes als Überlagerung anzuzeigen.

Diese Funktion erhöht die CPU-Auslastung um 10 % und kann Auswirkungen auf die Reaktionsfähigkeit haben.

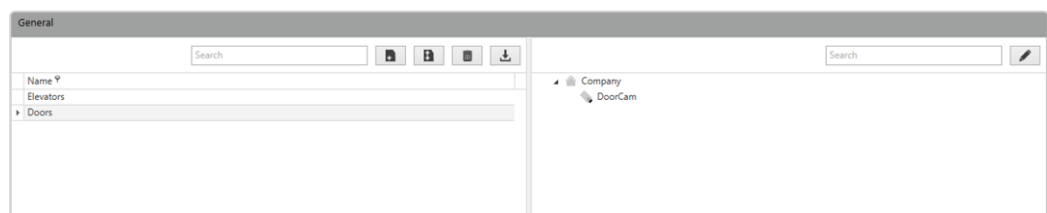
4. Aktivieren Sie die Einstellung für die Anzahl der fehlgeschlagenen Anmeldeversuche und legen Sie die Anzahl auf einen angemessenen Wert fest (Standard ist drei Versuche). Wenn der Benutzer die Anzahl der zulässigen Anmeldeversuche überschreitet, kann eine Benachrichtigung ausgelöst werden (siehe „[Benachrichtigungen](#)“ auf Seite 469).
5. Um zu verhindern, dass Benutzer ihre Dateien in auf dem Server absichtlich ausgewählte Standorte exportieren, aktivieren Sie **Globalen Pfad für nativen Export zum Server benutzen** und legen Sie den Pfad fest, auf dem alle nativen Exporte platziert werden. Wenn aktiviert, ist die Standortoption in den Exporteinstellungen deaktiviert (siehe „[Exportieren nativer Bilddaten auf den Server](#)“ auf Seite 119).
6. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.




Erstellen von Entitätsetiketten


Etiketten können jeder beliebigen Entität, wie z. B. Kameras zugeordnet werden und können Ihnen mit vorkonfigurierten Filtern bei der Ergebnissuche helfen. Etiketten können für die Suche im Überwachungsmodus, im Archivmodus und im LPR-Modus verwendet werden. Die Etiketten fungieren als Filter, die als Boolesche ODER-Parameter kombiniert werden, sodass bei einer Mehrfachsuche von Etiketten die Ergebnisse angezeigt werden, die auf alle Etiketten zutreffen. Jedoch wird bei der Suche der Boolesche UND-Parameter verwendet.

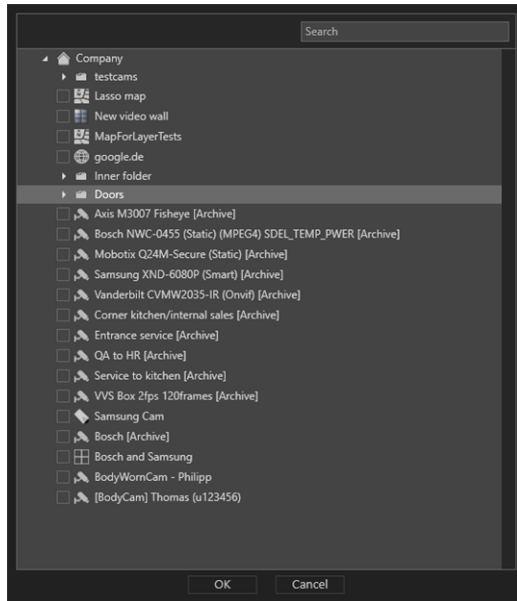
Dem Benutzer werden nur Etiketten angezeigt, die den jeweiligen Benutzerrechten entsprechen.

1. Wählen Sie **Entitätsetiketten** in der System-Steuerleiste.



2. Wählen Sie **Hinzufügen**  oder **Mehrere hinzufügen** , um der Liste eine oder mehrere Etiketten hinzuzufügen und diese zu benennen.
3. Um vordefinierte Etiketten hinzuzufügen, wählen Sie **Importieren**  und navigieren Sie zu der Textdatei, die die Etiketten enthält (siehe [„Etikettendatei wird vorbereitet“ auf der nächsten Seite](#)). Nach dem Importieren wird die Liste mit den Etiketten aus der Datei eingetragen.

4. Wählen Sie ein Etikett auf der linken Seite aus und klicken Sie danach auf **Bearbeiten** .



5. Weisen Sie dem ausgewählten Etikett ein oder mehrere Entitäten zu und klicken Sie danach auf **OK**. Die zugeordneten Entitäten werden nun rechts neben dem jeweiligen Etikett angezeigt.
6. **Übernehmen** Sie die eingestellten Werte, falls Sie weitere Einstellungen vornehmen möchten, oder **speichern** Sie die eingestellten Werte, um die Werte zu übernehmen und die Eingabe zu beenden.

Etikettendatei wird vorbereitet

Etiketten können in einer einfachen Textdatei (z. B. mit dem Editor) vorbereitet werden, indem Namen für Etiketten durch Zeilenumbrüche getrennt hinzugefügt werden.

1. Erstellen Sie eine neue Datei im Editor.
2. Geben Sie einen Etikettennamen ein und drücken Sie die Eingabetaste.
3. Fügen Sie so viele Etiketten wie nötig hinzu, jede in einem neuen Absatz.
4. Speichern Sie das Dokument als *.txt-Datei.

LPR-Modus

Die automatische Kennzeichenerkennung (LPR) im Videobild und der Abgleich mit einer Kennzeichen-Datenbank ermöglicht u. a. Zufahrtskontrolle und Schrankensteuerung, Park- und Ladeflächenverwaltung sowie das Auslösen von Alarmen. Der LPR-Modus dient zur Auswertung der LPR-Ereignisse und zur Darstellung der Informationen, die zum Ereignis gehören (inklusive Stammdaten, falls vorhanden). Darüber hinaus können Statistiken erfasst werden.

Für die LPR-Funktion wird ein Lizenzschlüssel benötigt.

Benutzerrechte im LPR-Modus

- Die für die Verwendung des LPR-Modus erforderlichen Benutzerrechte und Berechtigungen werden durch die LPR-Benutzergruppen definiert. Nur Gruppen mit der Berechtigung „Ansicht“ oder „Ändern“ dürfen den LPR-Modus verwenden.
- Wenn keine LPR-Gruppen vorhanden sind, kann jeder Benutzer den LPR-Modus benutzen und sehen.

Um die Nutzung des LPR-Modus einzuschränken (und möglichen Missbrauch zu verhindern), muss mindestens eine LPR-Gruppe mit den entsprechenden Rechten konfiguriert werden (siehe „[Kennzeichengruppen](#)“ auf [Seite 432](#)).

LPR-Stammdaten bearbeiten

LPR-Stammdaten sind alle Informationen, die einem bestimmten Kennzeichen zugeordnet sind (beispielsweise Gruppe, Gültigkeit). Die Stammdaten werden mit dem LPR-Stammdateneditor angelegt und verwaltet (siehe „[LPR-Stammdateneditor](#)“ auf [Seite 94](#)).

Details der Kennzeichenerkennung anzeigen

Bei der Erkennung eines Kennzeichens werden die zum Kennzeichen gehörenden Stammdaten und Alarmmeldungen angezeigt.

1. Klicken Sie auf einen Spaltentitel, um anhand der Kategorie der Spalte (Alarm, Ansicht/Kamera, Start, Stopp) aufsteigend oder absteigend zu sortieren.
2. Wählen Sie die gewünschte Ansicht oder Kamera (bzw. Aufzeichnungsbeginn oder -ende) aus. Das gewählte Objekt wird im Player angezeigt.

Player

Die Bedienung des Players im LPR-Modus entspricht der des Players im Archivmodus (siehe „[Archivmodus](#)“ auf [Seite 177](#)).

Kennzeichen abfragen

Im Steuerelement Administration können die gespeicherten Ereignisse zu einem Kennzeichen oder Containercode im Stammdatensatz in der LPR-Datenbank gesucht werden.

Abb. 259: Kennzeichen im LPR-Modus abfragen

1. Klicken Sie auf einen Spaltentitel, um die Kennzeichen anhand der Kategorie der Spalte (Zeitpunkt, Kennzeichen, Gruppe) aufsteigend oder absteigend zu sortieren.
2. Klicken Sie auf **Abfrage starten**, um alle gespeicherten Ereignisse zu dem gewählten Kennzeichen abzurufen.
3. Grenzen Sie den Suchfilter ein, indem Sie den **Abfragemodus** auswählen und gegebenenfalls Informationen zum **Kennzeichen** bzw. **Container**, zur **Gruppe**, **Fahrspur** und zum **Zeitraum** angeben.
4. Falls nur die Statistiken durchsucht werden sollen, aktivieren Sie **Nur Statistiken abfragen** und wählen Sie den Typ der Statistiken aus.
5. Klicken Sie auf **Abfrage starten**, um die Datenbank beispielsweise nach Kennzeichen, Gruppe, Land oder Fahrspur zu durchsuchen.
6. Die Suchergebnisse werden im Fenster **Details der Kennzeichenerkennung** angezeigt.
7. Klicken Sie auf das gefundene Ereignis. Der Player springt automatisch zum gewählten Zeitpunkt.

AdminTools

Die Qognify AdminTools beinhalten eine Suite von Administrationstools für die Verwaltung der Server, Clients und Zusatzmodule wie des UpdateService und des Alarm-Watchdog (siehe „[Der Alarm-WatchDog](#)“ auf Seite 573).

- **VA Administrationstool:** Das VA Administrationstool dient zur Konfiguration der Einstellungen für den Core-Server und zur Installation der Erweiterung „Versatile Application“. Die Erweiterungsparameter werden dann über den Client konfiguriert (siehe „[Qognify VMS VA Administrationstool](#)“ auf Seite 513).
- **Administrationstool:** Mit dem Administrationstool konfigurieren Sie die Bild-datenbank und die Verwaltungsdatenbank der Server (siehe „[Qognify Administrationstool](#)“ auf Seite 501).
- **ServiceManager:** Der ServiceManager ermöglicht das Starten und Stoppen der Dienste (siehe „[Qognify ServiceManager](#)“ auf Seite 511).
- **UpdateService Konfigurationstool:** Das UpdateService Konfigurationstool verwaltet die Konfiguration des UpdateService auf dem CoreServiceMain (CSM) und der UpdateAgents auf den Clients (siehe „[UpdateService Konfigurationstool](#)“ auf der nächsten Seite).

UpdateService Konfigurationstool

Das UpdateService Konfigurationstool verwaltet die Konfiguration des UpdateService und der verbundenen UpdateAgents (d. h. abgesetzter Server, Module und Clients). Das Konfigurationstool wird automatisch zusammen mit dem UpdateService installiert (siehe „[UpdateAgent konfigurieren und aktualisieren](#)“ auf Seite 47).

Der UpdateService sucht direkt nach der Installation nach verfügbaren Updates und Patches und lädt diese herunter, um sie anschließend zu verteilen (siehe „[Serverkonfiguration bearbeiten](#)“ auf Seite 499).

Das UpdateService Konfigurationstool unterstützt folgende Funktionen:

- Anzeigen aller verbundenen UpdateAgents, ihrer Hardwarespezifikationen, ihrer installierten Features sowie der angewendeten Patches jedes UpdateAgent
- Anzeigen der Statusinformationen aller UpdateAgents in einer Gruppe
- Anlegen von Gruppen von zu konfigurierenden UpdateAgents
- Umbenennen und Löschen von Gruppen und alten UpdateAgents in der Konfiguration
- Importieren und Exportieren von Downloadpaketen und Patchdateien für den UpdateService (keine Verzeichnisse erforderlich)
- Exportieren von Patches und Updates und Importieren dieser Patches und Updates mithilfe eines kleinen Tools in die UpdateAgents
- Konfigurieren, wie Updates/Patches abgerufen und wie sie für die UpdateAgents bereitgestellt werden
- Suchen nach Updates und Patches auf dem Server

Mit dem UpdateService kann die Software ohne installierten Qognify VMS-Client aktualisiert werden, da er die Konfigurations- und Logdaten in einem separaten Ordner ablegt.

1. Starten Sie das UpdateService Konfigurationstool im Installationsverzeichnis von Qognify VMS. Bestätigen Sie bei Bedarf die Administrationsrechte des Systems. Der Tab „Information“ wird angezeigt.

Informationen zu Rollbacks

Möglicherweise ist es erforderlich, das System auf ein zuvor installiertes Update zurückzusetzen (Rollback), um einen möglichst reibungslosen Systembetrieb sicherzustellen. Bei einem Update-Fehler werden alle Schritte auf das Backup rückgängig gemacht, das vor dem Update erstellt wurde.

UpdateService konfigurieren

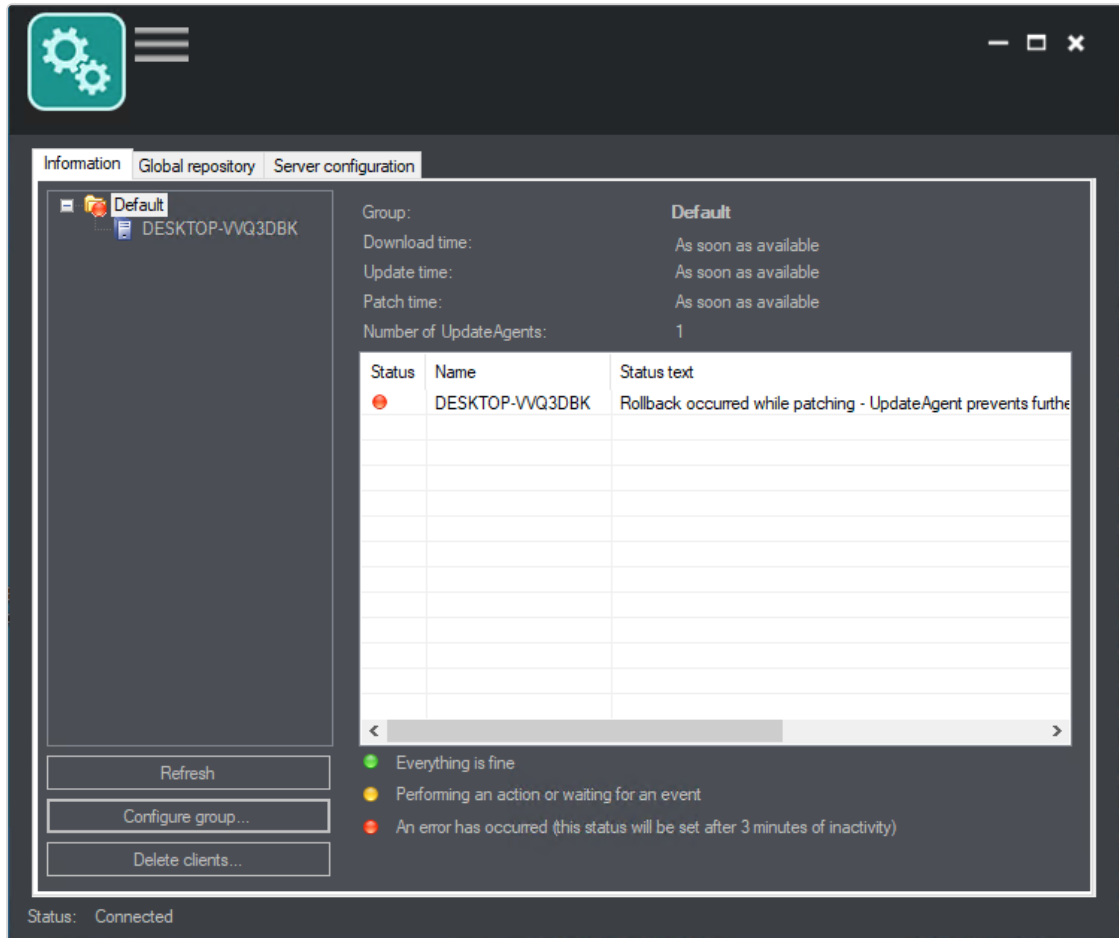


Abb. 260: UpdateService konfigurieren

In der Spalte „Gruppen“ werden alle vom UpdateService verwalteten Gruppen alphabetisch aufgelistet. Die Standardgruppe enthält alle UpdateAgents (Clients), die keiner Gruppe zugeordnet sind.

Außerdem werden der Update-Status und der Status der Verbindung zum Server angezeigt.

Clients in der Standardgruppe werden automatisch aktualisiert. Clients, die keine Updates oder Patches erhalten sollen, müssen sich in einer separaten Gruppe befinden (siehe „Gruppe konfigurieren“ auf Seite 495).

1. Durch Klicken auf einen Gruppenordner wird ein Statusüberblick über alle Clients in der Gruppe angezeigt. Ein farbiger Punkt auf dem Ordnersymbol zeigt den schlechtesten Status jedes Elements in der Gruppe an und ein weiterer farbiger Punkt zeigt den aktuellen Status eines jeden Clients an:
 - **Rot:** Auf dem Client ist ein Fehler aufgetreten oder der UpdateAgent des Clients ist seit mehr als drei Minuten offline.
 - **Gelb:** Der UpdateAgent ist derzeit ausgelastet (Ausführen von Patches, Herunterladen von Daten usw.) oder wartet auf die Auslösung eines Ereignisses durch den UpdateService (z. B. manuelle Verteilung von Patches).
 - **Grün:** Der UpdateAgent des Clients ist auf dem aktuellen Stand.
2. Klicken Sie auf den Clientnamen, um die installierten Komponenten (z. B. die Systemsoftware, die Softwareversion, den Status und die installierten Patches) anzeigen zu lassen.
3. Klicken Sie auf **Liste aktualisieren**, um den Status zu aktualisieren.
4. Klicken Sie auf **Gruppen konfigurieren**, um eine Gruppe anzulegen, umzubenennen oder zu löschen und die Update- und Patcheinstellungen der Gruppe festzulegen (siehe „[Gruppe konfigurieren](#)“ auf der gegenüberliegenden Seite).
5. Klicken Sie auf **Clients löschen**, um Clients zu entfernen, die mit dem UpdateService nicht mehr verbunden sind. Die Clients werden nicht automatisch gelöscht.

Update- bzw. Patchprozess manuell starten

Wenn eine Gruppe für manuelle Updates oder Patches konfiguriert ist, wird im Statusbereich der Gruppe die Option **Patch/Update auf den UpdateAgents starten** angezeigt.

1. Um das Update zu starten, klicken Sie auf **Patch/Update auf den UpdateAgents starten**. Es dauert bis zu 60 Sekunden, bis der Updateprozess gestartet wird.

Vorgehensweise nach einem Rollback

1. Sehen Sie im Log nach, was das Problem war.
2. Beheben Sie das Problem.
3. Beenden Sie die Dienste.

4. Löschen Sie auf dem UpdateServer die Update-Dateien im Update-Verzeichnis und passen Sie upd64.xml /upd.xml an, indem Sie die MD5-Summen und das Versions-Tag löschen.
5. Löschen Sie auf dem UpdateAgent die bereits heruntergeladenen Update-Dateien sowie die Rollback-Datei im Update-Verzeichnis.
6. Passen Sie upd64.xml /upd.xml an, indem Sie die MD5-Summen und das Versions-Tag löschen.
7. Starten Sie die Dienste neu.

Gruppe konfigurieren

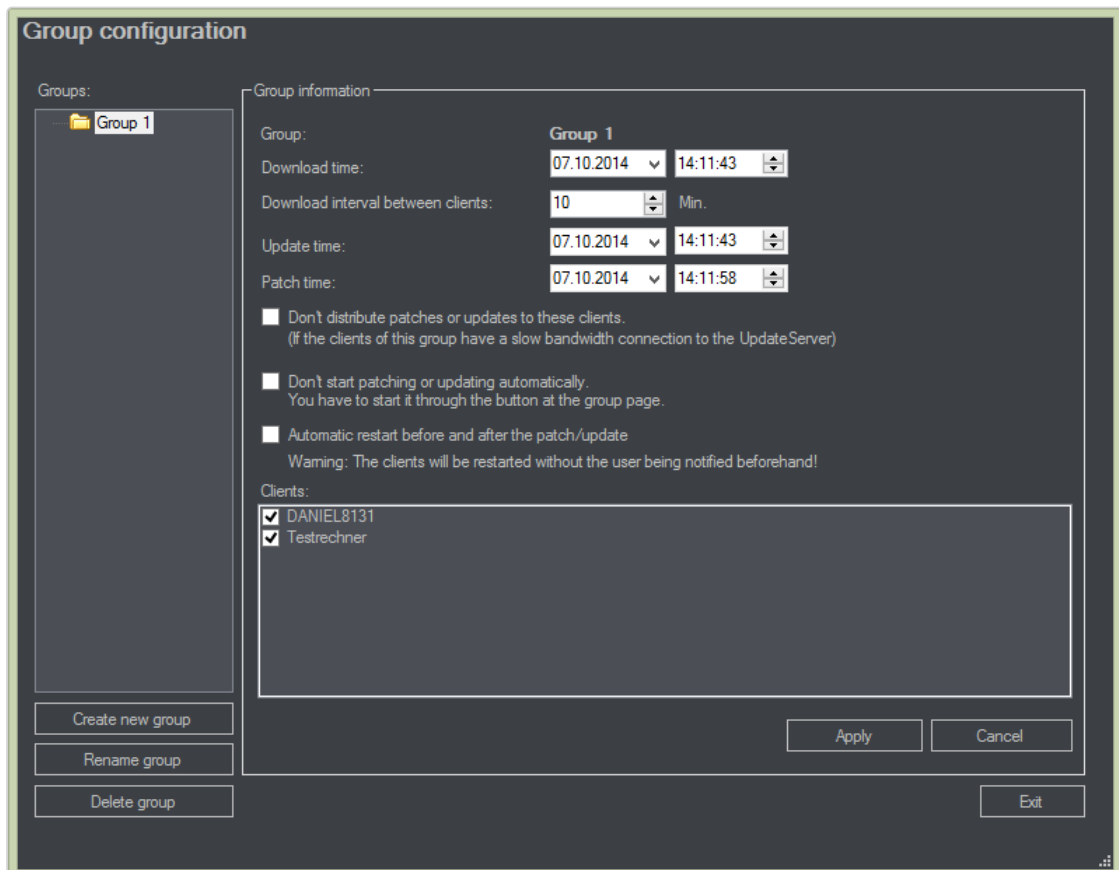


Abb. 261: Gruppe konfigurieren

Über die Gruppenkonfiguration kann Folgendes konfiguriert werden:

- Datum und Uhrzeit des Downloads des Updatepakets oder der Patchdateien.

Wenn der Zeitpunkt in der Vergangenheit liegt, werden Downloads und Patches sofort gestartet.

- Download-Abstand zwischen jedem UpdateAgent in Minuten (z. B. startet der erste UpdateAgent den Download um 10:00 Uhr, der zweite UpdateAgent startet den Download um 10:10 Uhr, der dritte um 10:20 Uhr usw.)
- Datum und Uhrzeit des Updates und des Patch
- Update- und Patchverhalten der UpdateAgents in der aktuellen Gruppe

1. Geben Sie die gewünschten Update- und Patcheinstellungen für die Gruppe an.
2. Um eine automatische Verteilung bei geringer Bandbreite zu unterdrücken, wählen Sie **Patches oder Updates nicht an diese Clients verteilen**. Wenn diese Option aktiviert ist, müssen die Patches manuell verteilt werden.
3. Wenn Sie keine automatische Installation von Patches und Updates wünschen, wählen Sie **Patches oder Updates nicht automatisch ausführen**. Wenn diese Option ausgewählt wird, müssen Patches und Updates manuell ausgeführt werden.
4. Um die Windows-Systeme auf den UpdateAgents vor und nach Anwendung des Patch herunterzufahren, wählen Sie **Automatischer Neustart vor und nach dem Patch/Update**. Die Clients werden automatisch neu gestartet.
5. Deselektieren Sie bei Bedarf Clients in der Gruppenliste. Die Gruppeneinstellungen werden nur für die ausgewählten Clients übernommen.

Gruppe anlegen

1. Klicken Sie auf **Neue Gruppe erstellen**.
2. Geben Sie einen **Namen** für die neue Gruppe ein und klicken Sie auf **OK**. Die neue Gruppe wird in der Spalte „Gruppen“ aufgelistet.

Gruppe umbenennen

1. Klicken Sie auf **Gruppe umbenennen**.
2. Ändern Sie den Namen der Gruppe und bestätigen Sie mit **OK**. Alle zugeordneten UpdateAgents bleiben in der Gruppe und übernehmen die Einstellungen der Gruppe.

Gruppe löschen

1. Wählen Sie in der Spalte „Gruppen“ eine Gruppe aus.
2. Klicken Sie auf **Gruppe löschen**. Alle Clients in der Gruppe werden in die Standardgruppe verschoben und aus den Updateeinstellungen ausgenommen. UpdateAgents in der Standardgruppe erhalten Updates und Patches, sobald diese verfügbar sind.

Die Standardgruppe kann nicht gelöscht werden.

Globale Datenquelle

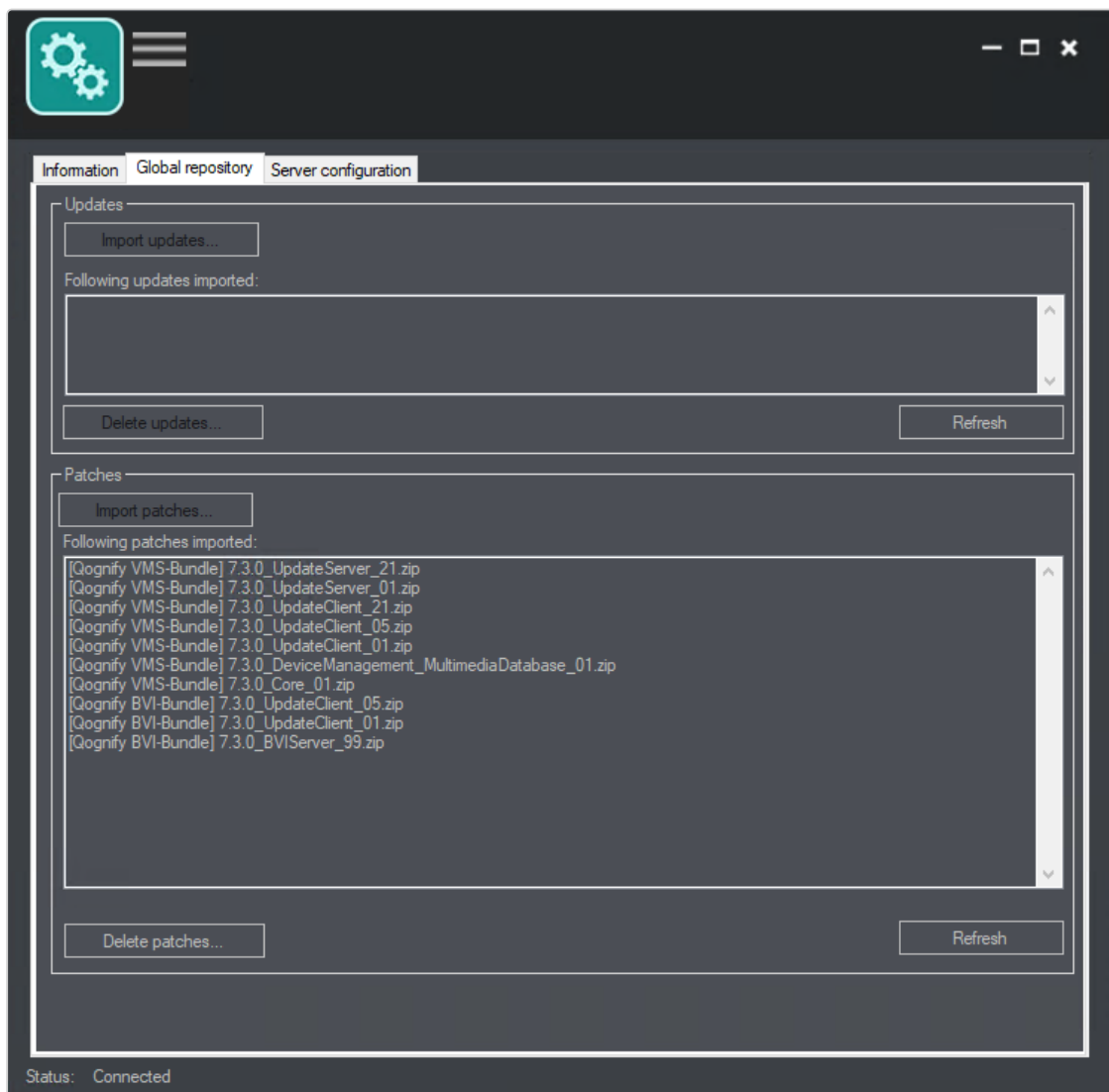


Abb. 262: Globale Datenquelle

In diesem Tab werden die verfügbaren Updates und Patches angezeigt. Wenn der UpdateService im Tab „Serverkonfiguration“ für die manuelle Verteilung konfiguriert wurde, können alle Updates und Patches vom Server importiert und in ein Verzeichnis auf dem Server oder auf einen angeschlossenen Datenträger exportiert werden (siehe [„Serverkonfiguration bearbeiten“ auf der gegenüberliegenden Seite](#)).

- Updates können immer nur einer nach dem anderen importiert werden.
- Patches können jeweils mehrere gleichzeitig importiert werden.

1. Wählen Sie **Updates importieren**, um die verfügbaren Updates von einem Verzeichnis herunterzuladen, der im lokalen Netzwerk verfügbar ist.
2. Um auf dem Server nach Updates zu suchen, die noch nicht angezeigt werden, klicken Sie auf **Aktualisieren**.
3. Um die Updates und die Anwendung „Qognify.UpdatePatchImport.exe“ in ein Verzeichnis zu kopieren, das auf einen Datenträger wie einen USB-Stick kopiert werden kann, klicken Sie auf **Export**. Die Updates und Patches der „Qognify.UpdatePatchImport.exe“ können auf jedem Client separat installiert werden (siehe [„Updates und Patches auf den UpdateAgent importieren“ auf Seite 501](#)).
4. Um die verfügbaren Patches von einem Verzeichnis im lokalen Netzwerk herunterzuladen, klicken Sie auf **Patches importieren**. Die verfügbaren Patches werden angezeigt.
5. Um die Patches und die Anwendung „Qognify.UpdatePatchImport.exe“ in ein Verzeichnis zu kopieren, das auf einen Datenträger wie einen USB-Stick kopiert werden kann, klicken Sie auf **Export**. Die Updates und Patches der „Qognify.UpdatePatchImport.exe“ können auf jedem Client separat installiert werden (siehe [„Updates und Patches auf den UpdateAgent importieren“ auf Seite 501](#)).
6. Um auf dem Server nach Patches zu suchen, die noch nicht angezeigt werden, klicken Sie auf **Aktualisieren**.

Entfernung von Patches / Updates von der Liste

1. Wenn die Patches nicht benötigt werden, wählen Sie die Patches von der Liste. Durch Drücken der Shift-Taste werden mehrere Objekte gleichzeitig ausgewählt.
2. Wählen Sie **Patches löschen**, bevor Sie sie exportieren. Nur die aufgelisteten Patches werden verteilt.

Serverkonfiguration bearbeiten



Abb. 263: Serverkonfiguration bearbeiten

Im Tab „Serverkonfiguration“ werden die grundlegenden Einstellungen für die Kommunikation zwischen dem UpdateServer und den Clients verwaltet. Standardmäßig verbindet sich der UpdateService mit dem Server, der die Updates bereitstellt, lädt die Updates und Patches herunter und verteilt sie an die UpdateAgents. Wenn jedoch eine manuelle Verteilung oder ein anderer Server für Downloads bevorzugt wird, kann die automatische Einstellung geändert werden.

1. Wählen Sie eine Option aus dem Menü aus:
 - **Updates/Patches automatisch aus dem Internet herunterladen und installieren.** Dies ist die empfohlene Einstellung für automatische Updates und die automatische Verteilung von Patches.
 - **Updates/Patches von einem angegebenen Remote-Speicherort automatisch herunterladen und installieren.** Die Updates und Patches werden von einem FTP-Server, der konfiguriert werden muss, heruntergeladen und auf den UpdateAgents automatisch installiert (siehe „[FTP-Server konfigurieren](#)“ unten).
 - **Nicht nach Updates im Internet oder einem Remote-Speicherort suchen.** Diese Option wird nicht empfohlen, da keine Updates oder Patches automatisch heruntergeladen bzw. verteilt werden. Die Updates und Patches müssen manuell heruntergeladen und exportiert werden (siehe „[Globale Datenquelle](#)“ auf Seite 497).
2. Aktivieren Sie **Vollständige Upgrade-Pakete ebenfalls herunterladen** aus, um alle Downloads herunterzuladen und zudem Pakete einschließlich Versionsupgrades zu verteilen, sofern die erforderliche Berechtigung (neuer Lizenzschlüssel für die nächste Hauptversion) zur Verfügung steht. Alle UpdateAgents werden entsprechend Ihren Gruppeneinstellungen auf die neue Version aktualisiert. (Standardmäßig lädt der UpdateService nur Patches mit Fehlerbehebungen herunter.)
3. Bestimmen Sie die Tageszeit, zu der Updates und Patches heruntergeladen und installiert werden.
4. Um manuell nach verfügbaren Downloads zu suchen, klicken Sie auf **Jetzt nach Updates/Patches suchen**. Es werden die derzeit aktiven Downloads angezeigt.
5. Klicken Sie auf **UpdateServer neu starten**, um den UpdateServer mit den übernommenen Einstellungen neu zu starten.
6. Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.

FTP-Server konfigurieren

1. Wenn Sie die Option **Updates/Patches von einem angegebenen Remote-Speicherort automatisch herunterladen und installieren** ausgewählt haben, geben Sie die IP-Adresse und die **Portnummer** des **FTP-Servers** an.
2. Geben Sie den **Benutzernamen** und das **Passwort** für den FTP-Server an.

3. Um eine sichere Verbindung herzustellen, aktivieren Sie **FTP über SSL verwenden**, sofern der Server SFTP unterstützt. (Erfragen Sie die korrekten Einstellungen beim Netzwerkadministrator.)

Updates und Patches auf den UpdateAgent importieren

1. Nachdem die Patches oder Updates erfolgreich exportiert wurden (siehe „[Globale Datenquelle](#)“ auf Seite 497), kopieren Sie das Verzeichnis auf einen USB-Stick und schließen Sie diesen an den Computer an, auf dem der UpdateAgent ausgeführt wird.
2. Starten Sie die Anwendung „Qognify.UpdatePatchImport.exe“ und klicken Sie auf **Ja**.
3. Klicken Sie auf **OK** und starten Sie den Update- bzw. Patchprozess. Der UpdateAgent wird für den Update-/Patchprozess gestoppt. Nach Abschluss des Prozesses wird der UpdateAgent automatisch neu gestartet.

Qognify Administrationstool

Mit dem Qognify Administrationstool konfigurieren Sie die Verwaltungsdatenbank (MaxDB) und die Bilddatenbank (MDB) der Server.

Falsche Einstellungen im Administrationstool können zu einem nicht funktionierenden System führen.

1. Starten Sie das Administrationstool im Installationsverzeichnis von Qognify VMS.

Alle Einstellungen im Administrationstool werden erst nach einem Neustart der Dienste bzw. des kompletten Rechners gültig (zum Starten der Dienste siehe „[Qognify ServiceManager](#)“ auf Seite 511)

Allgemeine Einstellungen

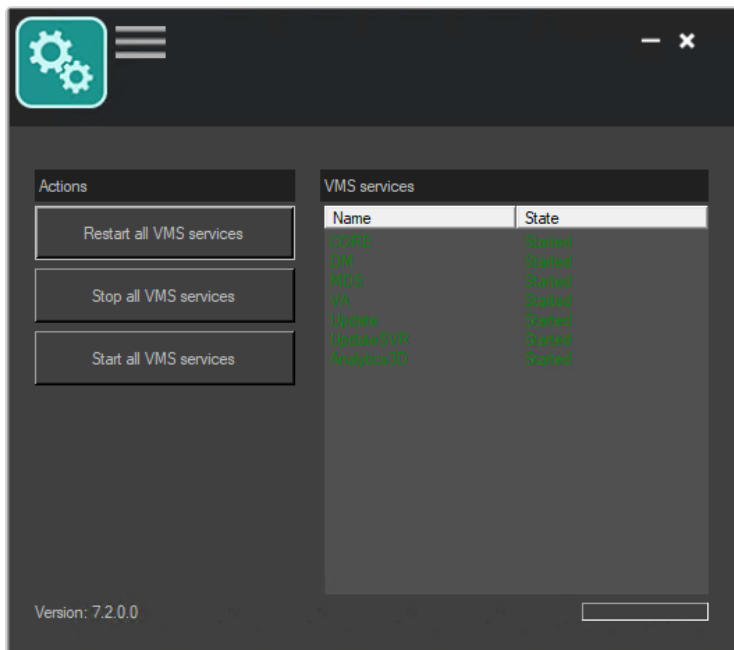


Abb. 264: Allgemeine Einstellungen

1. Passen Sie den **Server** und **Port** des Basisdienst-Servers an, falls die Administration auf einem abgesetzten Server gestartet wurde. Falls die Administration auf dem Hauptserver gestartet wurde, lassen Sie diese Einstellungen unverändert (Standard: Server: localhost, Port: 60000).
2. Geben Sie im Bereich „IP-Adresse/Hostname für Serverkommunikation“ die IP-Adresse des **Servers** und den **Hostnamen** an, mit denen sich die Dienste verbinden sollen.
3. Geben Sie das **Netzwerkpasswort** an.
4. Wählen Sie **Einstellungen** () und wählen Sie **Speichern** vom Menü **Datei**, um die Änderungen zu speichern.
5. Starten Sie die Dienste neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511).

Verwaltungsdatenbank (MaxDB)

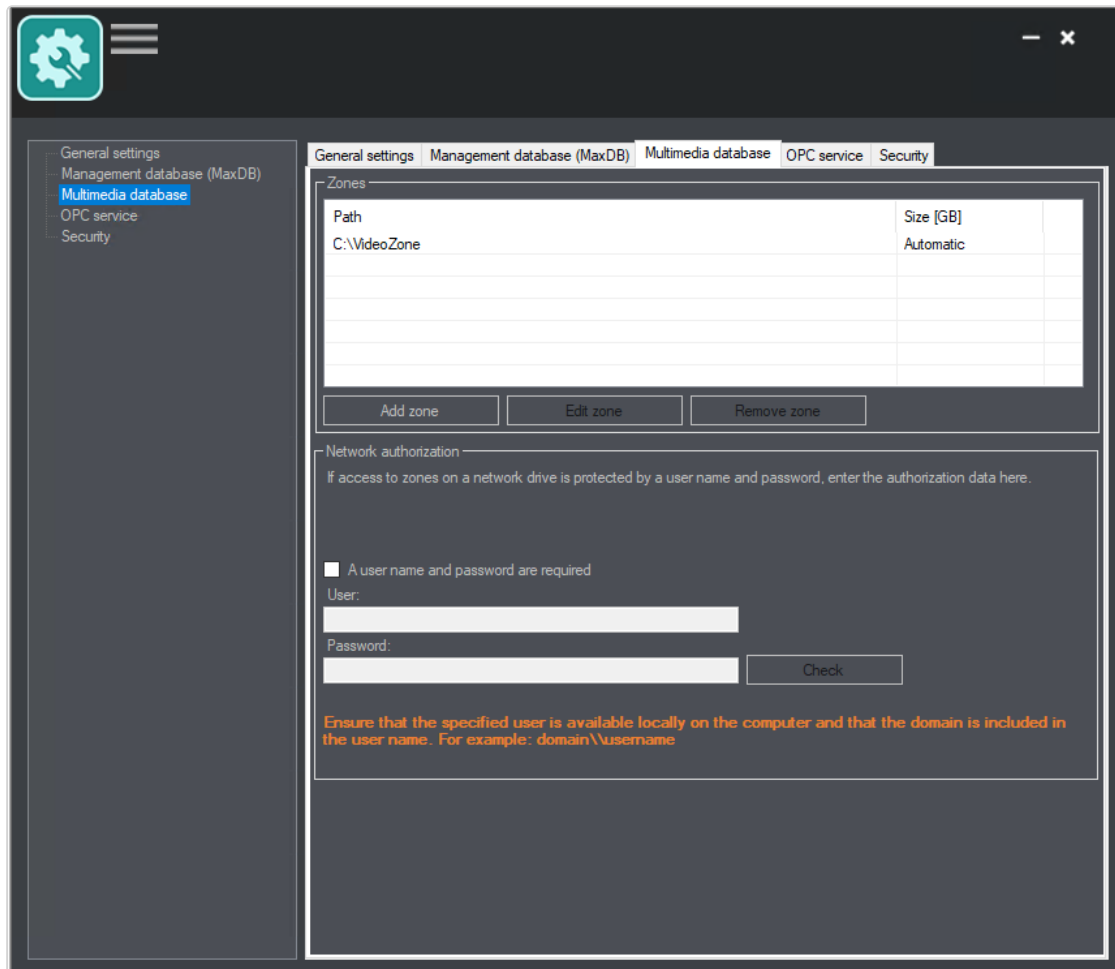


Abb. 265: Verwaltungsdatenbank (MaxDB)

Sichern und wiederherstellen

Für ein sicheres Backup (mit AES-256 verschlüsselt) im Dateiformat 7z ist ein Passwort erforderlich. Das Passwort wird auch zur Wiederherstellung von Backups im Dateiformat 7z benötigt (siehe „[Backup konfigurieren](#)“ auf Seite 466).

1. Um ein Backup der Verwaltungsdatenbank zu erstellen, klicken Sie auf **Sichern**. Die Sicherung der Datenbank wird im Verzeichnis „\Qognify\sapd-b\backup“ abgelegt.
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Fügen Sie bei Bedarf ein (anderes) **zweites Passwort** hinzu.

4. Klicken Sie auf **OK**. Die Verwaltungsdatenbank wird gesichert. Abhängig von der Größe der Datenbank kann dies einige Zeit dauern.

Unterbrechen Sie den Prozess nicht.


5. Um eine Datensicherung wiederherzustellen, klicken Sie auf **Wiederherstellen** und geben Sie das Passwort ein.

Speicher (und Volume) erweitern

Muss der Verwaltungsdatenbank (MaxDB) mehr Speicherplatz zur Verfügung gestellt werden, weil z. B. die Ereignisdaten längere Zeit vorgehalten werden sollen, kann der MaxDB ein weiteres Volume hinzugefügt werden. Die Größe der MaxDB beträgt standardmäßig 4 GB.

Die MaxDB kann um maximal vier Volumes erweitert werden.

Diese Erweiterung hat keinen Einfluss auf die aktuelle MultimediaDatabase (MaxDB).

1. Geben Sie die **Größe [MB]** des zusätzlichen Speicherplatzes für die Erweiterung der MaxDB an (minimal: 512 MB, maximal: 8000 MB).
2. Klicken Sie auf **Neues Volume hinzufügen**. Der zusätzliche Speicherplatz steht sofort unter DISK000X im MaxDB-Installationsverzeichnis zur Verfügung.
3. Klicken Sie auf **Aktualisieren** (), um eine Abschätzung zu erhalten, wie lange (in Tagen) der Platz der MaxDB bei der aktuellen Alarmrate ausreichen wird. Eine verlässliche Aussage kann nur dann getroffen werden, wenn das System unter Normallast bezüglich des Alarmvorkommens läuft.

Cache

Falls viele Ereignisse auftreten und deshalb hohe Ladezeiten entstehen, kann der Cache der MaxDB vergrößert werden.

Dieser Wert sollte jedoch sinnvoll gewählt werden. Die Vergrößerung des Caches ist nicht sinnvoll, wenn nicht tatsächlich genügend freier Hauptspeicher auf diesem PC zur Verfügung steht.

Die aktuelle Cachegröße des für die MaxDB reservierten Hauptspeichers wird angezeigt. Die aktuelle Größe der MaxDB wird unter „Aktuelle Auslastung der Verwaltungsdatenbank“ angezeigt.

Die Cachegröße der MaxDB ist ein äußerst systemkritischer Parameter, der nur in begründeten Fällen geändert werden sollte. Der optimale Durchsatz wird erzielt, wenn die ganze Datenbank im Cache vorgehalten wird.

1. Geben Sie als die gewünschte **Größe** einen Wert in MB an und klicken Sie auf **Cachegröße anpassen**.

MultimediaDatabase

Der Tab „MultimediaDatabase“ ermöglicht das Einpflegen und Bearbeiten von Zonen der MultimediaDatabase. Bei diesen Zonen handelt es sich um Pfade, in die die MultimediaDatabase ihre Bilddaten speichert. Dabei können sowohl lokale Laufwerke als auch Netzlaufwerke angesprochen werden. Die angegebene Zonengröße wird nicht sofort reserviert, die Belegung erfolgt erst bei Bedarf.

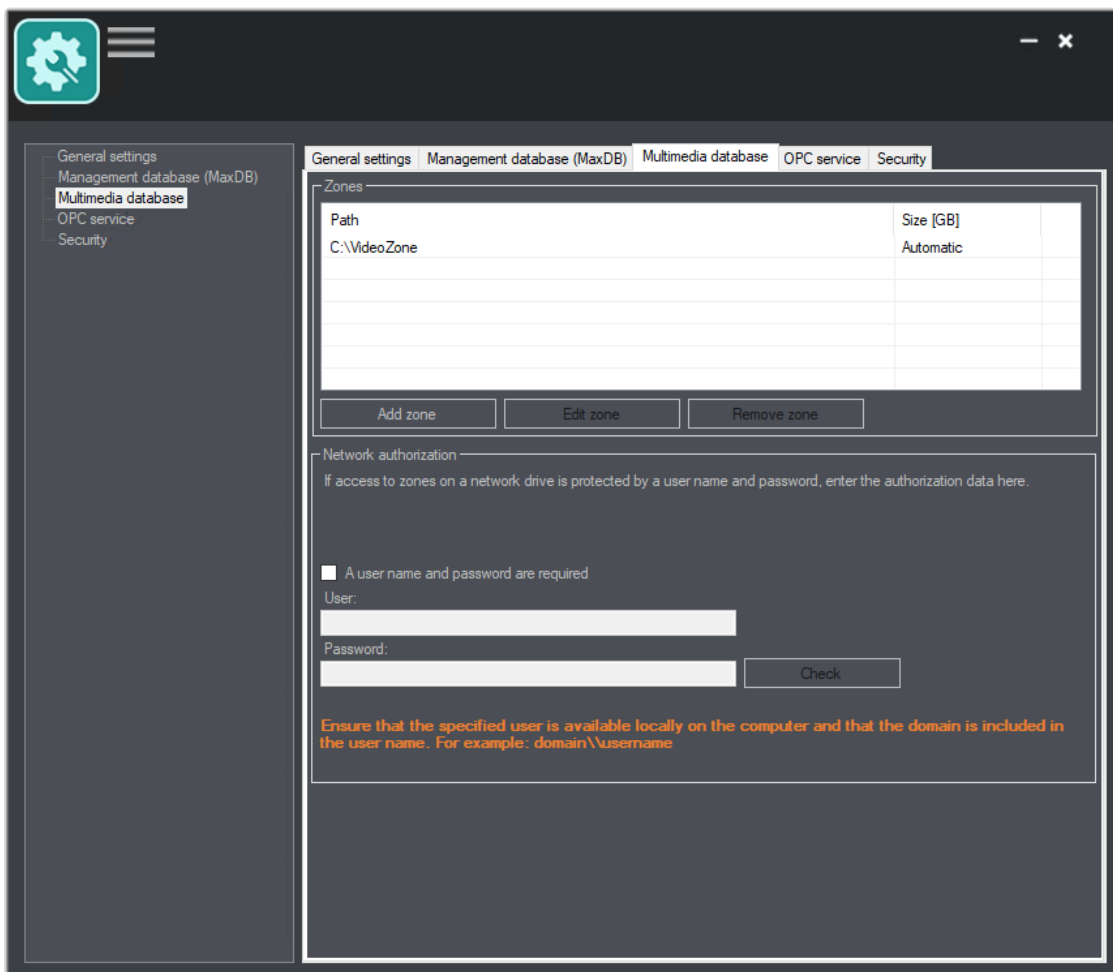


Abb. 266: MultimediaDatabase

Informationen zu Zonen

Zonen legen die maximale Speichertiefe der MultimediaDatabase und somit der Software fest. Standardmäßig werden von der Software keinerlei Begrenzungen bezüglich der Zone der MultimediaDatabase festgelegt. Bei einer Neuinstallation wird die Standardzone im folgenden Verzeichnis angelegt: „Qognify VMS-Installationsverzeichnis\re\md\mds\data“.

Es wird jedoch empfohlen, diese durch eine Zone auf einer dedizierten Partition zu ersetzen.

Reicht das Volumen der vorhandenen Zone nicht aus, kann eine weitere Zone hinzugefügt werden. Es sollten maximal zehn Zonen angelegt werden. Eine größere Anzahl wirkt sich negativ auf die Leistung der MultimediaDatabase aus. Außerdem sollten eher wenige große Zonen als mehrere kleine Zonen angelegt werden.

Falls den angeschlossenen Kameras mehr Speicherplatz zugewiesen wird, als über die eingepflegten Zonen hinweg oder auf der Festplatte zur Verfügung steht, stellt die Datenbank die Aufzeichnung ein.

Verwenden Sie keine externe Festplatte, die über USB oder FireWire angeschlossen ist, als Zone der MultimediaDatabase, da die Leistungsfähigkeit dadurch sehr stark leidet. Aus Performancegründen sollten Sie die MultimediaDatabase z. B. auf eine weitere Festplatte oder ein RAID-System auslagern.

Hinzufügen einer Zone

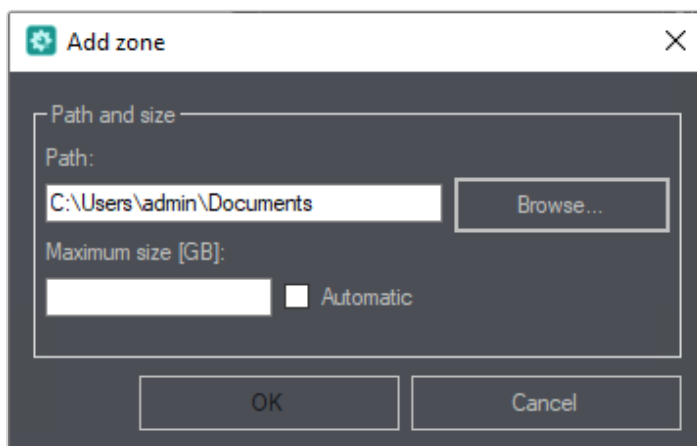


Abb. 267: Zone hinzufügen

1. Legen Sie als Zone auf einer dedizierten Partition ein Verzeichnis an, um darin die Bilddaten zu speichern. Die Clustergröße sollte 64 KB betragen.
2. Klicken Sie auf **Zone hinzufügen**.
3. Geben Sie den **Pfad** des Zonenverzeichnisses ein oder klicken Sie auf **Durchsuchen** und navigieren Sie zum Verzeichnis.

4. Geben Sie die maximale Größe (in GB) an.
5. Aktivieren Sie **Automatisch**, um den gesamten physischen Raum in der Partition zu verwenden.

Es wird empfohlen, „Automatisch“ zu aktivieren, damit die MultimediaDatabase den verfügbaren Speicherplatz effizient verwalten kann. Wenn eine feste maximale Größe definiert werden muss, achten Sie darauf, dass nicht mehr als 95 % des physikalischen Platzes einer Partition ausgelastet werden, da darüber hinaus mit Leistungseinbußen durch das Betriebssystem zu rechnen ist.

6. Bestätigen Sie mit **OK**.

Hinzufügen einer Zone auf dem Netzlaufwerk

1. Legen Sie auf einem Server im Netzwerk ein Verzeichnis an, um darin die Bilddaten zu speichern.
2. Klicken Sie auf **Zone hinzufügen**.
3. Geben Sie den **UNC-Pfad** und die **Maximale Größe** (in GB) an, beispielsweise „\\192.168.2.20\Pfad\zur\Freigabe“.
4. Aktivieren Sie **Unbegrenzt**, um den kompletten physikalischen Platz der Partition zu verwenden.
5. Aktivieren Sie im Bereich „Netzwerkautorisierung“ **Benutzername und Passwort werden benötigt**, um die Autorisierungsdaten des Netzlaufwerks, d. h. die Anmeldeinformationen am Server, anzugeben.
6. Geben Sie den **Benutzernamen** und das **Passwort** ein. Beachten Sie, dass der Benutzer auch lokal auf dem Rechner verfügbar sein muss und die Domäne mit angegeben werden muss, z. B.: DOMÄNE\vorname.nachname
7. Klicken Sie auf **Prüfen**, um die Verfügbarkeit und Autorisierung am Netzlaufwerk zu prüfen.

Bearbeiten einer Zone

1. Wählen Sie im Feld Zonen die gewünschte MultimediaDatabase aus.
2. Klicken Sie auf **Zone bearbeiten**, um den Pfad und/oder die Größe zu ändern. Wir empfehlen, den physikalischen Platz einer Partition zu maximal 95 % auszulasten, da darüber hinaus mit Leistungseinbußen durch das Betriebssystem zu rechnen ist.
3. Bestätigen Sie mit **OK**.

Entfernen einer Zone

1. Wählen Sie im Feld Zonen die gewünschte MultimediaDatabase aus.
2. Klicken Sie auf **Zone entfernen**.

**Die Bilddaten der gelöschten Zone sind nicht mehr in verfügbar
Qognify VMS, werden aber nicht automatisch gelöscht.**

OPC-Dienst

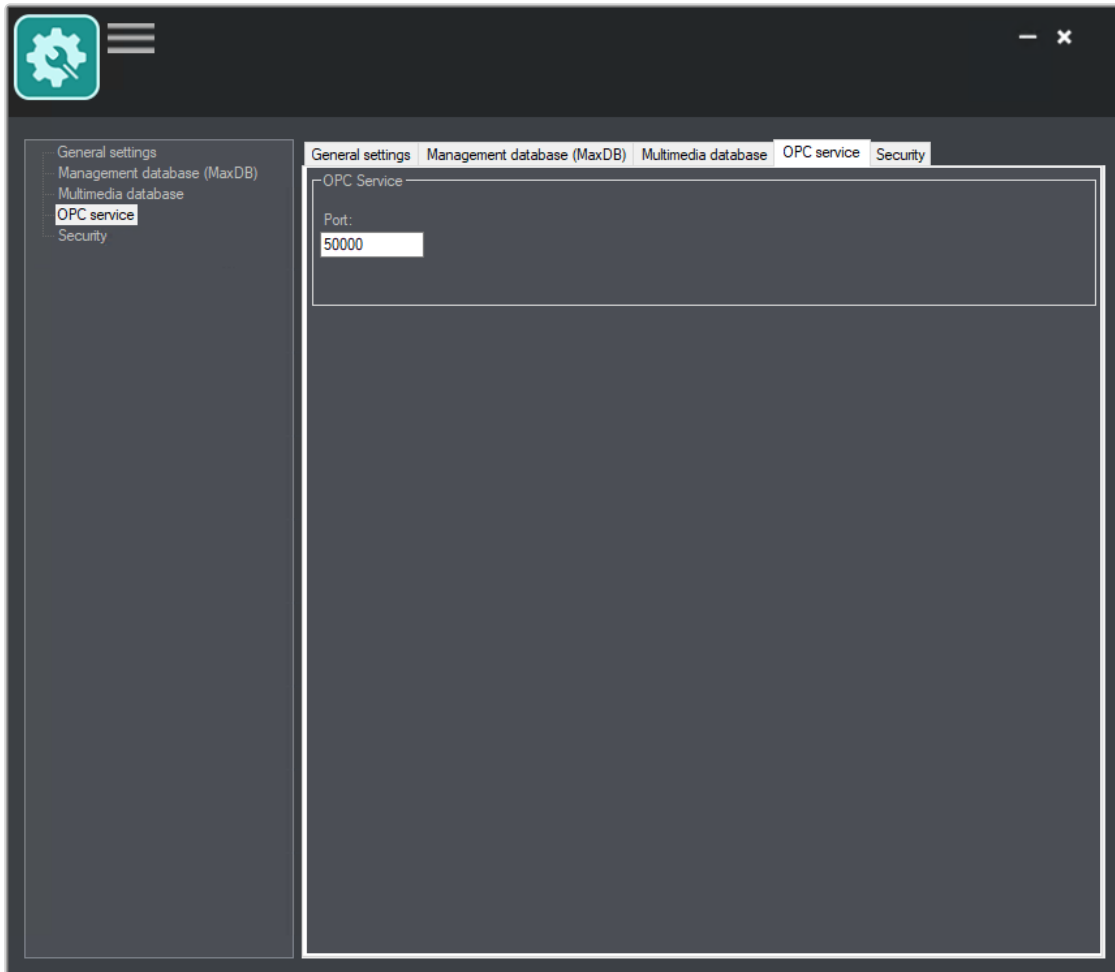


Abb. 268: OPC-Dienst

Der OPC-Dienst definiert die Portnummer für die Kommunikation zwischen Qognify VMS und dem Softwaredienst.

Der OPC-Dienst ist optional. Die Einstellung ist nur verfügbar, wenn der UpdateAgent aktiviert ist.

1. Geben Sie die Portnummer ein.

Sicherheit

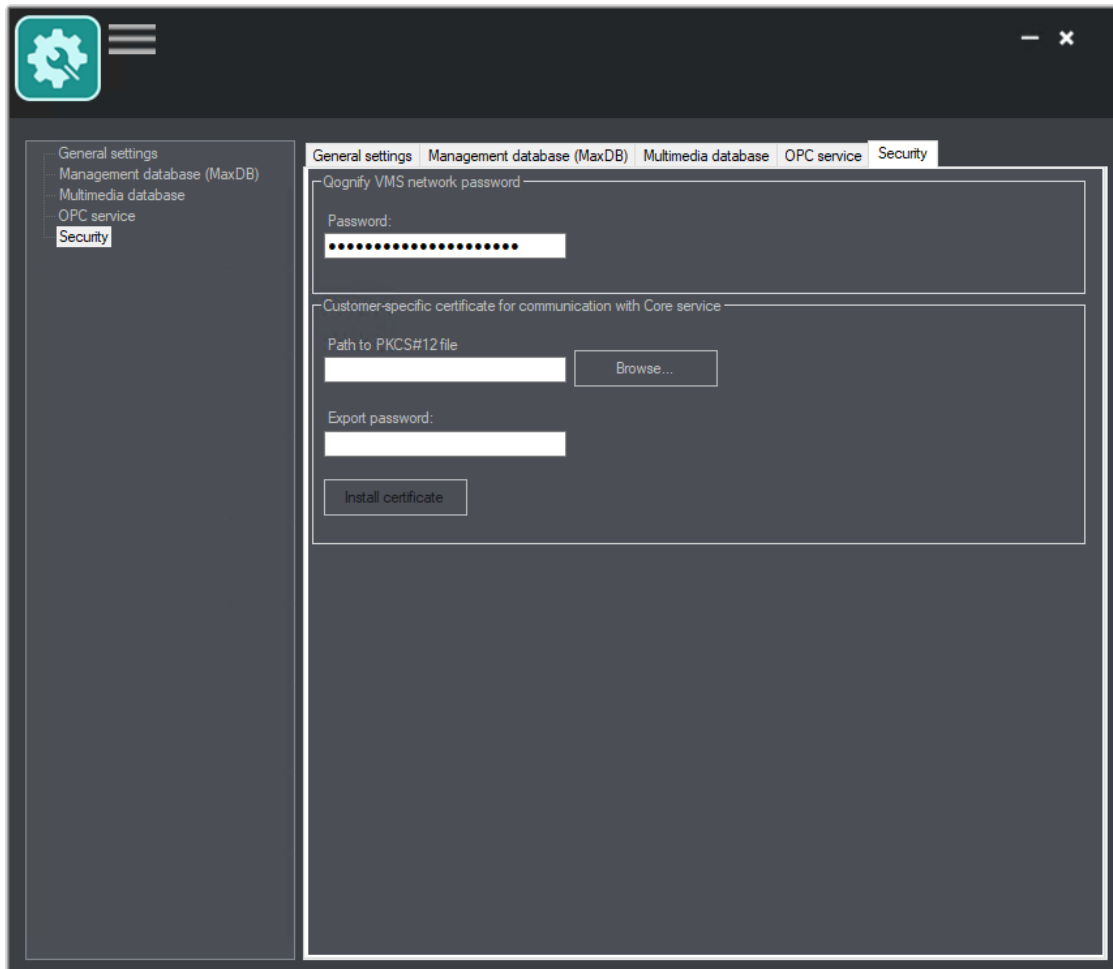


Abb. 269: Sicherheit

Die Sicherheitseinstellungen unterstützen die Festlegung eines Netzwerkpassworts und eines kundenspezifischen Zertifikats für die Kommunikation zwischen Qognify VMS und dem Server.

Um das Netzwerkpasswort zu verwenden, muss das Passwort auf dem Computer mit dem Kerndienst ersetzt werden.

1. Geben Sie ein Netzwerkpasswort an. Das Passwort wird für die Kommunikation zwischen den Diensten von Qognify VMS verwendet. **Halten Sie sich aus Sicherheitsgründen an die erforderlichen Sicherheitsstandards des Unternehmens.**
2. Erstellen oder laden Sie eine PKCS#12-verschlüsselte Zertifikatsdatei herunter.
3. Wählen Sie „Durchsuchen“ und navigieren Sie zu der Datei.
4. Geben Sie das „Qognify VMS Netzwerkpasswort“ ein und wählen Sie **Zertifikat installieren**.

5. Starten Sie den Kerndienst neu (siehe [„Dienste starten und stoppen“](#) auf der [nächsten Seite](#)).
6. Wiederholen Sie die Zertifikatsinstallation für jeden Kerndienst, der das gleiche Zertifikat verwendet.
7. Installieren Sie das entsprechende öffentliche Schlüsselzertifikat auf jedem Computer, der mit den Kerndiensten verbunden ist, in das folgende Verzeichnis:
 - %SeeTecINSTALL%\conf\
8. Benennen Sie die Datei in „cayugaCore.crt“ um.

Qognify ServiceManager

Der ServiceManager ermöglicht das Starten und Stoppen der Dienste. Folgende Funktionen sind im ServiceManager verfügbar:

- Alle Dienste neu starten
- Alle Dienste beenden
- Alle Dienste starten

Der ServiceManager wird bei der Installation eines Serverdienstes automatisch installiert.

Wenn der ServiceManager bei der Anmeldung automatisch gestartet werden soll, fügen Sie „-autostart“ als Kommandozeilenparameter hinzu (siehe [„Kommandozeilenparameter“](#) auf Seite 533).

1. Starten Sie den ServiceManager im Installationsverzeichnis oder im Windows-Startmenü.

Displaysprache umstellen

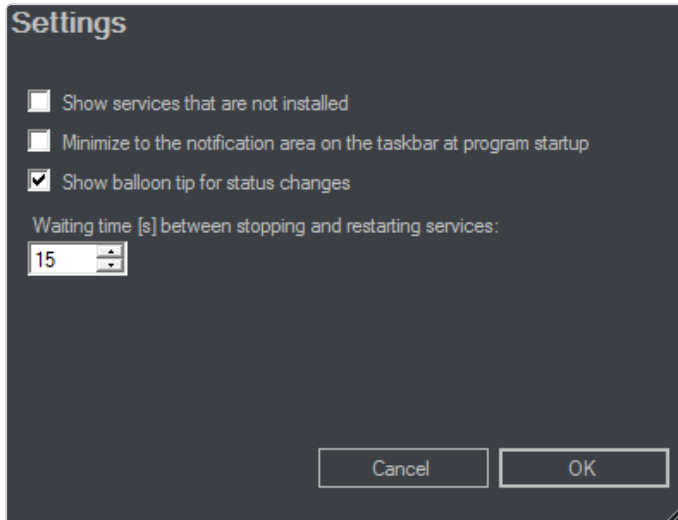
1. Beenden Sie den ServiceManager.
2. Starten Sie die Eingabeaufforderung als Administrator und geben Sie "VMS_ServiceManager.exe -l:<Code_für_die_Displaysprache>" ein.

Beispiel Für Englisch: "VMS_ServiceManager.exe -l:en-us" oder für Französisch: "VMS_ServiceManager.exe -l:fr-fr"

3. Starten Sie den ServiceManager.

Einstellungen bearbeiten

1. Wählen Sie **Einstellungen** (☰).



2. Aktivieren Sie **Nicht installierte Dienste anzeigen**, um auch alle möglichen Dienste in der Liste zu zeigen. Standardmäßig werden nicht installierte Dienste nicht angezeigt.
3. Aktivieren Sie **Bei Programmstart direkt in den Infobereich der Taskleiste minimieren**, um schnelleren Zugriff auf den ServiceManager zu erhalten.
4. Aktivieren Sie **Sprechblasentext bei Zustandsänderungen anzeigen**, um bei Änderungen an den Diensten eine sofortige Benachrichtigung auf dem Bildschirm zu erhalten.
5. Definieren Sie die **Wartezeit zwischen dem Beenden und Neustarten der Dienste** (Standard 15 Sekunden). Erhöhen Sie das Intervall, sodass die Dienste bei großen Installationen korrekt gestartet und beendet werden können.
6. Bestätigen Sie mit **OK**.

Dienste starten und stoppen

Der Zustand der jeweiligen Dienste wird angezeigt und farblich unterschieden:

- Grün = Dienst ist gestartet
- Rot = Dienst ist gestoppt
- Gelb = Dienst wird gestartet oder gestoppt
- Schwarz = Dienst ist nicht installiert

1. Klicken Sie auf **Alle Dienste neu starten**, um unabhängig vom Zustand der Dienste alle Dienste zu beenden und neu zu starten.
2. Klicken Sie auf **Alle Dienste beenden**, um unabhängig vom Zustand der Dienste alle Dienste zu beenden.
3. Klicken Sie auf **Alle Dienste starten**, um unabhängig vom Zustand der Dienste alle Dienste zu starten.

Optional können Sie auch bestimmte Dienste starten, stoppen oder neu starten, indem Sie mit der rechten Maustaste auf den gewünschten Dienst klicken.

Qognify VMS VA Administrationstool

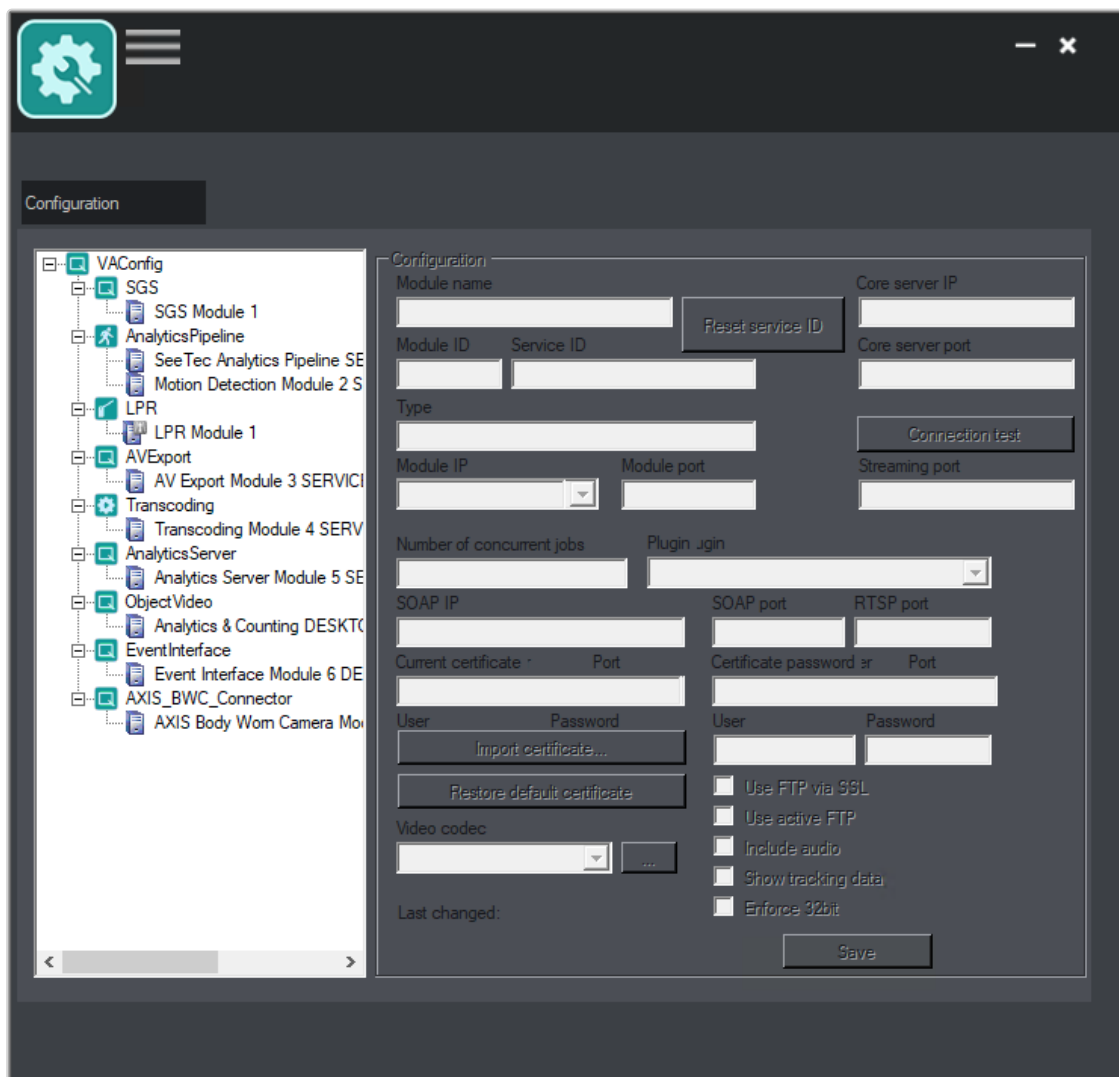


Abb. 270: Das Qognify VMS VA Administrationstool

Mit dem Qognify VMS VA Administrationstool können die folgenden Module (Dienste) verwaltet werden:

- **Kennzeichenerkennung (LPR)**, siehe „LPR-Modul hinzufügen“ auf der gegenüberliegenden Seite
- **Analytics Server**, siehe „Analytics Server-Modul hinzufügen“ auf Seite 516
- **Transcodierungs-Engine**, siehe „Transcodierungs-Engine-Modul hinzufügen“ auf Seite 518
- **Gateway Service**, siehe „Gateway-Service-Modul (SGS) hinzufügen“ auf Seite 519
- **Analytics Interface**, siehe „Analytics Interface-Modul hinzufügen“ auf Seite 521
- **Serverbasierte Bewegungserkennung**, siehe „Modul zur serverbasierten Bewegungserkennung hinzufügen“ auf Seite 522
- **Generische Zutrittskontrolle**, siehe „Generisches Zutrittskontrollmodul hinzufügen“ auf Seite 524
- **Ereignisschnittstelle**, siehe „Qognify Event Interface-Modul hinzufügen“ auf Seite 527
- **AV-Export-Modul**, siehe „AV-Export-Modul konfigurieren“ auf Seite 525

Das Qognify VMS VA Administrationstool wird über das Windows®-Startmenü oder über das Qognify VMS-Installationsverzeichnis gestartet.

Displaysprache umstellen

1. Beenden Sie das Qognify VA Administrationstool.
2. Starten Sie die Eingabeaufforderung als Administrator und geben Sie „VMS_VA_ConfigurationTool.exe -l:<Code_für_die_Displaysprache>“ ein.

Beispiel Für Englisch: „VMS_VA_ConfigurationTool.exe -l:en-gb“ oder „VMS_VA_ConfigurationTool.exe -l:en-us“
bzw für Französisch: „VMS_VA_ConfigurationTool.exe -l:fr-fr“

3. Starten Sie das Qognify VA Administrationstool.

Neue Konfigurationsdatei erstellen

1. Klicken Sie auf **Einstellungen** (1) und wählen Sie **Neue Konfigurationsdatei erstellen** im Menü **Datei**.

LPR-Modul hinzufügen

Das Qognify LPR-Modul ist eine Schnittstelle für die Anbindung an eine LPR-Engine von ARH.

Sie können nur jeweils ein LPR-Modul pro Server bedienen. Sie können jedoch mehrere LPR-Module auf mehreren Servern installieren, wenn nur ein Server aktiviert ist.

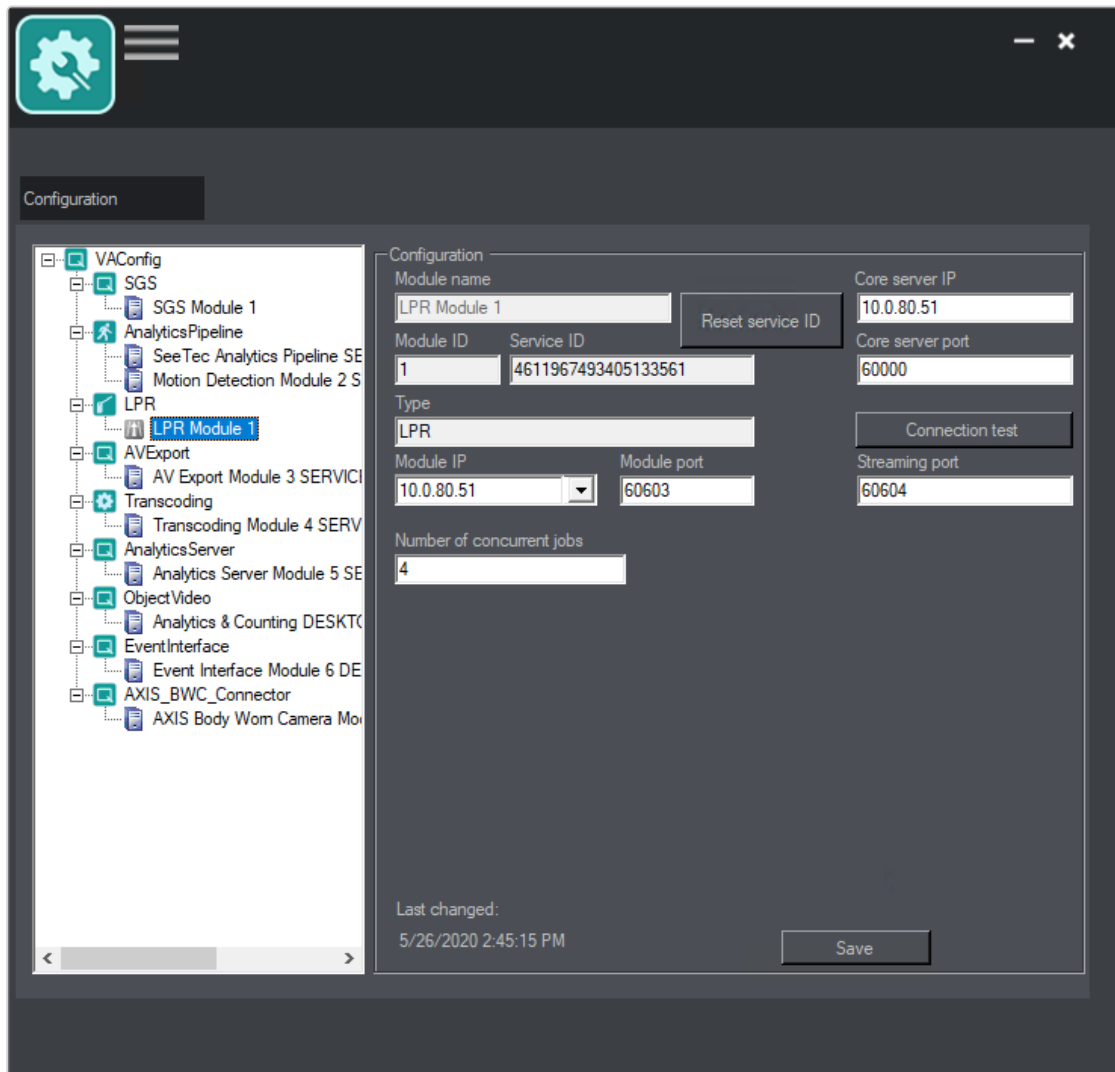


Abb. 271: LPR-Modul hinzufügen

1. Klicken Sie oben im Modulbaum mit der rechten Maustaste auf **VACONFIG**.
2. Wählen Sie **Ein neues Modul auswählen**.
3. Wählen Sie **Kennzeichenerkennung** aus. Ein neuer Eintrag wird erstellt.
4. Passen Sie den **Modulnamen** an.
5. Geben Sie die **IP-Adresse** des Core-Servers an.

Verwenden Sie nicht localhost oder 127.0.0.1 als Eintrag, da andere Dienste über diese IP-Adressen kommunizieren müssen.

Die Service-ID ändert sich nach der ersten Verbindung zum Qognify-Server.

Setzen Sie die Service-ID nur nach Rücksprache mit dem Qognify-Support zurück.

6. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen. Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.
7. Wählen Sie die **Modul-IP** aus.
8. Geben Sie den **Modul-Port** an, den das LPR-Modul verwendet.
9. Legen Sie die **Anzahl gleichzeitiger Jobs** fest, die übertragen werden sollen. Diese Anzahl sollte höher sein als die Anzahl der zu überwachenden Fahrspuren.

Beispiel In jeder Fahrspur wartet möglicherweise mehr als ein Fahrzeug. Daher können pro Fahrspur mehrere gleichzeitige Jobs vorhanden sein. Die Jobs werden dann auf eine „Warteliste“ gesetzt, in der die Warteschlange nacheinander abgearbeitet wird. Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Qognify-Support (siehe „Support“ auf Seite 13).

Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Support.

10. Klicken Sie auf **Speichern**.
11. Starten Sie die Dienste mit dem ServiceManager neu (siehe „Qognify ServiceManager“ auf Seite 511) oder fügen Sie weitere Module hinzu.

Im Konfigurationsmodus sind weitere Konfigurationsschritte erforderlich (siehe „LPR-Modul konfigurieren“ auf Seite 446).

Analytics Server-Modul hinzufügen

Das Qognify Analytics Server-Modul wird für **3D Analytics** und **2D intelligente Bewegungserkennung** benötigt. Weitere Details finden Sie unter „Qognify Analytics Server“ auf Seite 335.

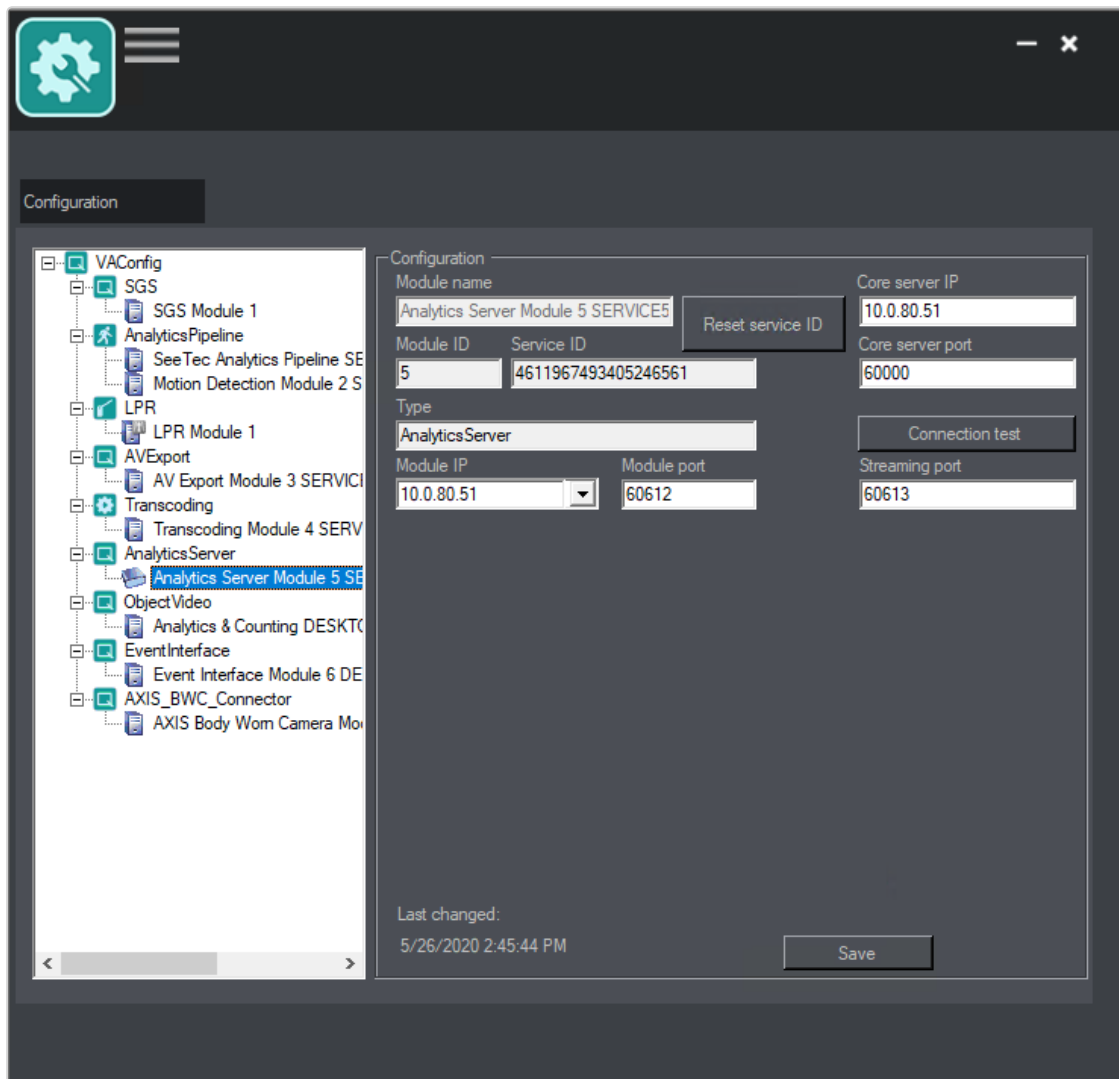


Abb. 272: Analytics Server-Modul hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die Konfigurationsdatei in der linken Spalte und wählen Sie **Analytics Server** aus dem Kontextmenü **Neues Modul hinzufügen**. Im Menübaum in der Konfigurationsdatei wird ein neuer Eintrag angelegt (siehe „[Transcoding-Modul konfigurieren](#)“ auf Seite 453).
2. Passen Sie den **Modulnamen** an.
3. Geben Sie die **IP-Adresse** des Core-Servers an.

Verwenden Sie nicht „localhost“ oder „127.0.0.1“, da andere Dienste über diese IP-Adressen kommunizieren müssen. Die Service-ID ändert sich nach der ersten Verbindung zum Qognify-Server. Setzen Sie die Service-ID nur nach Rücksprache mit dem Qognify-Support zurück (siehe „[Support](#)“ auf Seite 13).

4. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen.

Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.

5. Wählen Sie die Modul-IP aus.
6. Geben Sie den **Modul-Port** an, den das Analytics Server-Modul verwendet.
7. Klicken Sie auf **Speichern**.
8. Fügen Sie weitere Module hinzu oder starten Sie die Dienste neu (siehe [„Qognify ServiceManager“ auf Seite 511](#)).

Transcodierungs-Engine-Modul hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die Konfigurationsdatei in der linken Spalte und wählen Sie **Transcodierungs-Engine** aus dem Kontextmenü **Neues Modul hinzufügen**. Im Menübaum unter der Konfigurationsdatei wird ein neues Element angelegt (siehe [„Transcoding-Modul konfigurieren“ auf Seite 453](#)).
2. Passen Sie den **Modulnamen** an.
3. Geben Sie die **IP-Adresse** des Core-Servers an.

Verwenden Sie nicht localhost oder 127.0.0.1 als Eintrag, da andere Dienste über diese IP-Adressen kommunizieren müssen.

Die Service-ID ändert sich nach der ersten Verbindung zum Qognify-Server.

Setzen Sie die Service-ID nur nach Rücksprache mit dem Qognify-Support zurück (siehe [„Support“ auf Seite 13](#)).

4. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen. Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.
5. Wählen Sie die **Modul-IP** aus.
6. Geben Sie den **Modul-Port** an, den das Transcoding-Modul verwendet.
7. Wählen Sie **32bit erzwingen**, falls die Geräte nicht unter 64 Bit lauffähig sind. Diese Einstellung betrifft nur Geräte, die noch nicht für 64 Bit freigegeben wurden.

Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Qognify-Support (siehe [„Support“ auf Seite 13](#)).

8. Klicken Sie auf **Speichern**.
9. Starten Sie die Dienste neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511) oder fügen Sie weitere Module hinzu.

Gateway-Service-Modul (SGS) hinzufügen

Das Qognify-Gateway-Service-Modul ist eine netzwerkbasierte Schnittstelle, die für Dienste wie Qognify WebClient oder Mobile Client oder SDK bestimmte Funktionen zur Verfügung stellt.

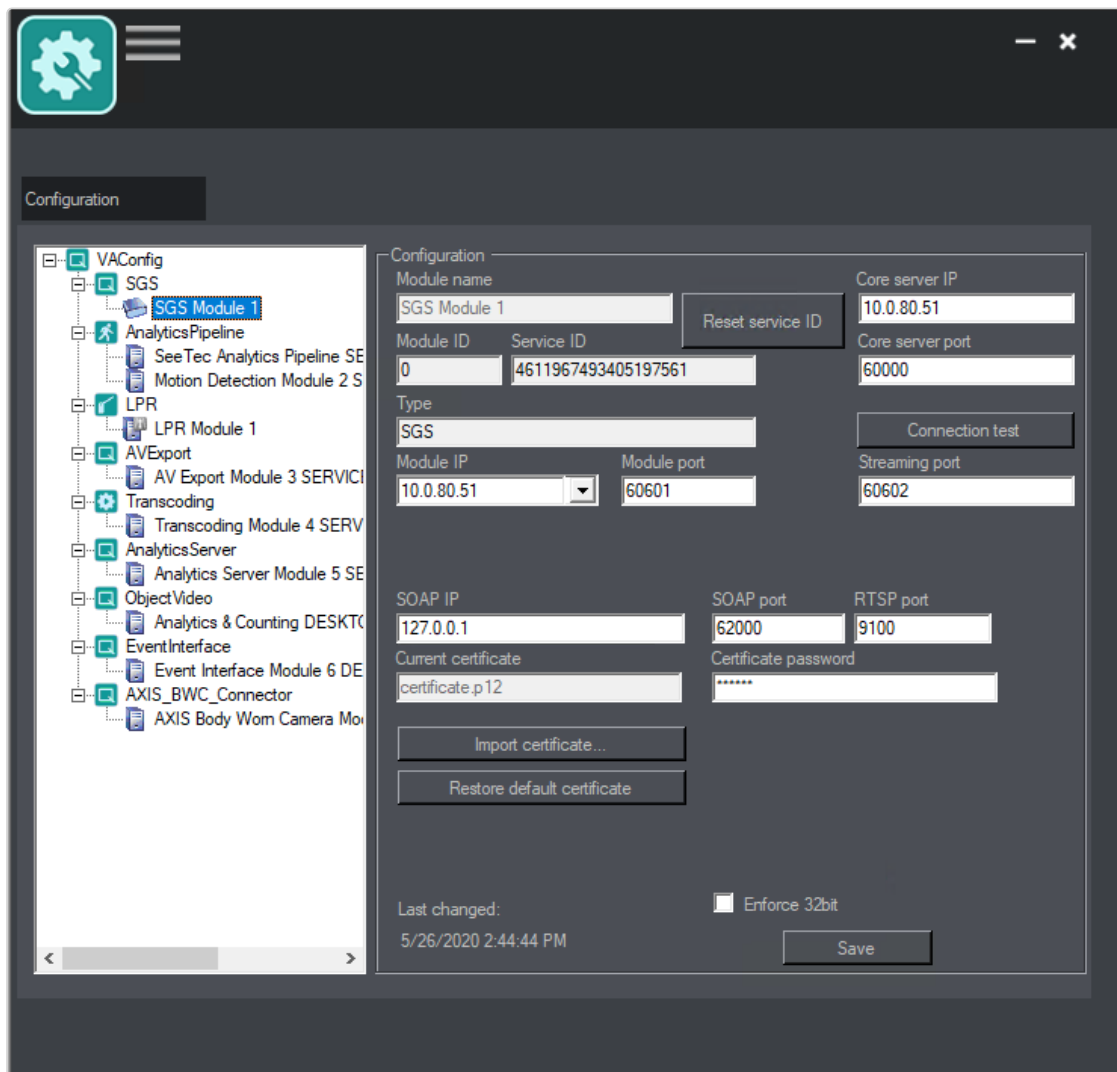


Abb. 273: Gateway-Service-Modul hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die linke Spalte und wählen Sie **Gateway-Service** aus dem Kontextmenü **Neues Modul hinzufügen**. Im Menübaum unter der Konfigurationsdatei wird ein neuer Eintrag angelegt (siehe „[Server](#)“ auf Seite 434).

2. Passen Sie den **Modulnamen** an.
3. Geben Sie die **IP-Adresse** des Core-Servers an.

Verwenden Sie nicht localhost oder 127.0.0.1 als Eintrag, da andere Dienste über diese IP-Adressen kommunizieren müssen.

Die Service-ID ändert sich nach der ersten Verbindung zum Qognify-Server.

Setzen Sie die Service-ID nur nach Rücksprache mit dem Qognify-Support zurück.

4. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen. Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.
5. Wählen Sie die **Modul-IP** aus.
6. Geben Sie den **Modul-Port** an, den das SGS-Modul verwendet.
7. Geben Sie die **SOAP-IP** und den **SOAP-Port** an.
8. Geben Sie für den Zugriff auf das Netzwerk über das Intranet (interner Zugriff) die lokale IP des Servers an.
9. Geben Sie für den Zugriff auf das Netzwerk über das Internet (externer Zugriff) die öffentliche IP des Routers oder der Firewall an. Darüber hinaus muss am Router oder in der Firewall die transparente Port-Weiterleitung aktiviert werden.
10. Optional können Sie Ihr eigenes Zertifikat importieren. Bei dem Zertifikat muss es sich um ein PKCS#12-(X.509-)Zertifikat handeln, das den privaten Schlüssel enthält.
11. Wählen Sie **32bit erzwingen**, falls die Geräte nicht unter 64 Bit lauffähig sind. Diese Einstellung betrifft nur Geräte, die noch nicht für 64 Bit freigegeben wurden.

Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Qognify-Support.

12. Klicken Sie auf **Speichern**.
13. Starten Sie die Dienste neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511) oder fügen Sie weitere Module hinzu.

Im Konfigurationsmodus sind weitere Konfigurationsschritte erforderlich (siehe „[Gateway-Service-\(SGS-\)Modul konfigurieren](#)“ auf Seite 452.

Analytics Interface-Modul hinzufügen

Über das standardisierte Qognify Analytics Interface (SAI) können server- oder kame-rabasierte Analyseanwendungen anderer Hersteller in die Qognify VMS-Umgebung integriert werden.

SAI-Plugins sind von mehreren Herstellern erhältlich, z. B. Axis, Forlan, NumberOk usw.

Die erhältlichen SAI-Plugins werden auf der Qognify-Partnerseite aufgelistet und können dort heruntergeladen werden.

Beachten Sie, dass Drittanbieter-Plugins (nicht zertifiziert) zuerst von Qognify geprüft und zertifiziert werden müssen. Nicht zertifizierte Plugins werden nach 12 Stunden automatisch deaktiviert.

The screenshot shows the configuration window for adding an Analytics Interface module. The fields are as follows:

Field	Value
Module name	Analytics Interface Module 10 SCHRI
Core server IP	SCHRI-HP
Module ID	10
Service ID	4611967494090007561
Core server port	60000
Type	VcaApi
Module IP	192.168.56.1
Module port	60621
Streaming port	60622
VCA plugin	SeeTec AG Lpr Test Plugin (x64)

Additional elements: A 'Reset service ID' button is located next to the Service ID field. A 'Connection test' button is located below the Type field. At the bottom, there is a 'Last changed' timestamp (12/09/2018 15:32:46), an 'Enforce 32bit' checkbox (unchecked), and a 'Save*' button.

Abb. 274: Analytics Interface-Modul hinzufügen

1. Kopieren Sie die DLL-Dateien des VCA-Plugins in das Qognify-Plugin-Verzeichnis (C:\Programme\Qognify\VersatileApplications64\VcaPlugin\).
2. Starten Sie die VA-Dienste mit dem ServiceManager neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511).

3. Klicken Sie oben im Modulbaum mit der rechten Maustaste auf **VAConfig**. Das Menü **Neues Modul hinzufügen** wird angezeigt.
4. Klicken Sie auf **Analytics-Schnittstelle**. Ein neuer Eintrag wird erstellt.
5. Passen Sie den **Modulnamen** an.
6. Geben Sie die **IP-Adresse** des Core-Servers an.

Verwenden Sie nicht localhost oder 127.0.0.1 als Eintrag, da andere Dienste über diese IP-Adressen kommunizieren müssen.

Die Service-ID ändert sich nach der ersten Verbindung zum Qognify-Core-Server.

Setzen Sie die Service-ID nur nach Rücksprache mit dem Qognify-Support zurück.

7. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen. Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.
8. Wählen Sie die **Modul-IP** aus.
9. Geben Sie den **Modul-Port** an, den das VCA-Modul verwendet.
10. Geben Sie den **Streaming-Port** an, den das VCA-Modul verwendet.
11. Wählen Sie das **VCA-Plugin** aus. Das Qognify bereitgestellte Plugin muss zuvor im Plugin-Verzeichnis (C:\Programme\Qognify\plug-ins) installiert worden sein.
12. Wählen Sie **32bit erzwingen**, falls die Geräte nicht unter 64 Bit lauffähig sind. Diese Einstellung betrifft nur Geräte, die noch nicht für 64 Bit freigegeben wurden.

Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Qognify-Support.

13. Klicken Sie auf **Speichern**.
14. Starten Sie die Dienste neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511) oder fügen Sie weitere Module hinzu.

Um einen SAI-Kanal für eine CogVis Forlan-Kamera zu entfernen, muss der Kanal auf dem System des Herstellers entfernt werden.

Modul zur serverbasierten Bewegungserkennung hinzufügen

Standardmäßig sind zwei Module zur serverbasierten Bewegungserkennung vor-konfiguriert. Sie werden für die serverseitigen Funktionen (siehe „[Serverseitige Funktionen](#)“ auf Seite 276) wie Bewegungserkennung, Referenzbildvergleich und

Manipulationserkennung benötigt. Weitere Konfiguration ist in den Servereinstellungen des Konfigurationsmodus verfügbar (siehe „[Server](#)“ auf Seite 434).

Configuration

Module name: Motion Detection Module 1

Module ID: 1

Service ID: 4611967493405104561

Core server IP: 172.16.80.7

Core server port: 60000

Type: AnalyticsPipeline

Module IP: 172.16.80.7

Module port: 60603

Streaming port: 60604

Buttons: Reset service ID, Connection test, Save

Enforce 32bit:

Last changed: 11/6/2014 11:18:14 AM

Abb. 275: Modul zur serverbasierten Bewegungserkennung hinzufügen

1. Klicken Sie mit der rechten Maustaste auf die Konfigurationsdatei in der linken Spalte und wählen Sie **Serverbasierte Bewegungserkennung** aus dem Kontextmenü **Neues Modul hinzufügen**. Im Menübaum unter der Konfigurationsdatei wird ein neuer Eintrag angelegt (siehe „[Server](#)“ auf Seite 434).
2. Passen Sie den **Modulnamen** an.
3. Geben Sie die **IP-Adresse** des Core-Servers an.

Verwenden Sie nicht localhost oder 127.0.0.1 als Eintrag, da andere Dienste über diese IP-Adressen kommunizieren müssen.

Die Service-ID ändert sich bei der ersten Verbindung zum Qognify-Server.

Setzen Sie die Service-ID nur nach Rücksprache mit dem Qognify-Support zurück.

4. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen. Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.
5. Wählen Sie die **Modul-IP** aus.
6. Geben Sie den **Modul-Port** an, den das Motion Detection-Modul verwendet.

- Wählen Sie **32bit erzwingen**, falls die Geräte nicht unter 64 Bit lauffähig sind. Diese Einstellung betrifft nur Geräte, die noch nicht für 64 Bit freigegeben wurden.

Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Qognify-Support.

- Klicken Sie auf **Speichern**.
- Starten Sie die Dienste neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511) oder fügen Sie weitere Module hinzu.

Generisches Zutrittskontrollmodul hinzufügen

Mit einem generischen Zutrittskontrollmodul wird das Qognify-System mit Zutrittskontrollgeräten von Drittanbietern verbunden.

The screenshot shows the configuration interface for a generic access control module. The window is titled "Configuration" and contains the following fields and controls:

- Module name:** Generic Access Control Module 9 SCI
- Core server IP:** SCHRI-HP
- Module ID:** 9
- Service ID:** 4611967494089992561
- Core server port:** 60000
- Type:** GenericAccessControlConfig
- Module IP:** 192.168.56.1
- Module port:** 60619
- Streaming port:** 60620
- Buttons:** "Reset service ID", "Connection test", and "Save".
- Enforce 32bit:** A checkbox that is currently unchecked.
- Last changed:** 12/09/2018 14:13:33

Abb. 276: Generisches Zutrittskontrollmodul

1. Klicken Sie mit der rechten Maustaste auf die Konfigurationsdatei in der linken Spalte und wählen Sie **Generische Zutrittskontrolle** aus dem Kontextmenü **Neues Modul hinzufügen**. Im Menübaum unter der Konfigurationsdatei wird ein neuer Eintrag angelegt (siehe „[Generisches Zutrittskontrollmodul konfigurieren](#)“ auf Seite 457).
2. Passen Sie den **Modulnamen** an.
3. Geben Sie die **IP-Adresse** des Core-Servers an.

Verwenden Sie nicht localhost oder 127.0.0.1 als Eintrag, da andere Dienste über diese IP-Adressen kommunizieren müssen.

Die Service-ID ändert sich nach der ersten Verbindung zum Server.

Setzen Sie die Service-ID nur nach Rücksprache mit dem Qognify-Support zurück.

4. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen. Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.
5. Wählen Sie die Modul-IP aus.
6. Geben Sie den **Modul-Port** an, den das Modul verwendet.
7. Wählen Sie **32bit erzwingen**, falls die Geräte nicht unter 64 Bit lauffähig sind. Diese Einstellung betrifft nur Geräte, die noch nicht für 64 Bit freigegeben wurden.

Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Qognify-Support.

8. Klicken Sie auf **Speichern**.
9. Starten Sie die Dienste neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511) oder fügen Sie weitere Module hinzu.

AV-Export-Modul konfigurieren

Das AV-Export-Modul wird standardmäßig installiert und kann nicht gelöscht werden. Es wird zur Transcodierung von Videoaufzeichnungen basierend auf einem Video-Codec und zur Übertragung der Ergebnisse auf einen FTP-Server oder SMTP-Server benötigt. In der Kamerakonfiguration (siehe „[Video-Backup/-Export](#)“ auf Seite 274) bzw. Alarmkonfiguration (siehe „[E-Mail und FTP](#)“ auf Seite 402) sind weitere Einstellungen erforderlich.

Abb. 277: AV-Export-Modul konfigurieren

1. Klicken Sie auf das **AV-Export-Modul**.
2. Geben Sie die **IP-Adresse** des Core-Servers an, wenn sich diese geändert hat.

Verwenden Sie nicht localhost oder 127.0.0.1 als Eintrag, da andere Dienste über diese IP-Adressen kommunizieren müssen.

Die Service-ID ändert sich bei der ersten Verbindung zum Qognify-Server.

Setzen Sie die Service-ID nur nach Rücksprache mit dem Qognify-Support zurück.

3. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen. Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.
4. Wählen Sie die **Modul-IP** aus.
5. Geben Sie den **Modul-Port** an, den das AV-Export-Modul verwendet.
6. Geben Sie den **Streaming-Port** an, den das AV-Export-Modul verwendet.

7. Geben Sie die IP-Adresse und den **Port** des **Primären FTP-Servers** und ggf. für den **Sekundären FTP-Server** an.
8. Geben Sie den **Benutzer** und das **Passwort** für den Zugriff auf die FTP-Server an.
9. Um eine sichere Verbindung mit den FTP-Servern herzustellen, aktivieren Sie **FTP über SSL verwenden**.
10. Aktivieren Sie **Aktives FTP verwenden**. Andernfalls wird passives FTP (Standard) verwendet.

Bei aktivem FTP (auch „aktiver Modus“) öffnet der Client einen zufälligen Port und teilt dem Server diesen Port und seine eigene IP-Adresse mit dem Befehl PORT oder EPRT mit.

Bei passivem FTP (auch „passiver Modus“ genannt) sendet der Client einen PASV- oder EPSV-Befehl und der Server öffnet einen Port und übermittelt ihn zusammen mit der IP-Adresse an den Client. Diese Methode wird angewendet, wenn der Server keine Verbindung zum Client herstellen kann.

11. Aktivieren Sie **Audio einschließen**, um in das exportierte Video Audioaufzeichnungen zu integrieren.
12. Aktivieren Sie **Trackingdaten anzeigen**, um im exportierten Video Trackingdaten aus Video Analytics darzustellen.
13. Wählen Sie **32bit erzwingen**, falls die Geräte nicht unter 64 Bit lauffähig sind. Diese Einstellung betrifft nur Geräte, die noch nicht für 64 Bit freigegeben wurden.

Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Qognify-Support.

14. Klicken Sie auf **Speichern**.
15. Starten Sie die Dienste neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511) oder fügen Sie weitere Module hinzu.

Qognify Event Interface-Modul hinzufügen

Die Qognify Event Interface (QEI) ist eine offene Schnittstelle für die Anbindung an Drittanbieter-Sicherheitssysteme, wie Einbruchalarm, Brandmeldezentrale, Zutrittskontrolle usw. Die Qognify Event Interface ist nicht auf bestimmte Hersteller oder Systeme beschränkt.

Entwickler von Drittanbietern können ein Plugin für die Schnittstelle bereitstellen. Bei weiteren Fragen wenden Sie sich an den Qognify-Support (siehe „[Support](#)“ auf Seite 13).

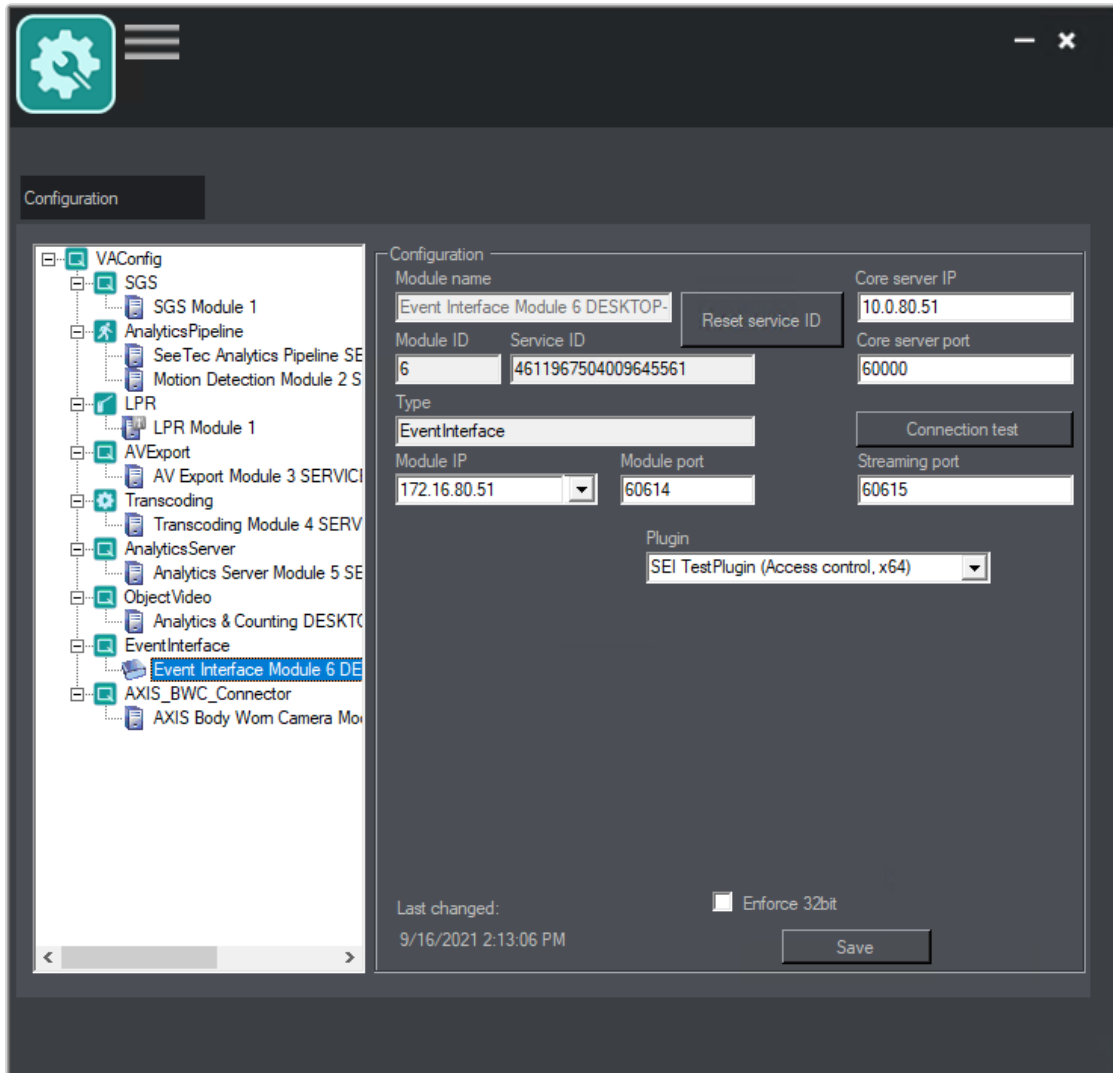


Abb. 278: Qognify Event Interface-Modul (QEI) hinzufügen

1. Kopieren Sie die DLL-Dateien des QEI-Plugins in das Qognify-Plugin-Verzeichnis (C:\Programme\Qognify\VersatileApplications64\EventPlugins\"Plugin-Name").
2. Starten Sie die VA-Dienste mit dem ServiceManager neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511).
3. Klicken Sie oben im Modulbaum mit der rechten Maustaste auf **VAConfig**. Das Menü **Neues Modul hinzufügen** wird angezeigt.
4. Klicken Sie auf **Event Interface**. Ein neuer Eintrag wird erstellt.
5. Passen Sie den **Modulnamen** an.
6. Geben Sie die **IP-Adresse** des Core-Servers an.

Verwenden Sie nicht localhost oder 127.0.0.1 als Eintrag, da andere Dienste über diese IP-Adressen kommunizieren müssen.

Die Service-ID ändert sich nach der ersten Verbindung zum Qognify-Core-Server.

Setzen Sie die Service-ID nur nach Rücksprache mit dem Support zurück.

7. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen. Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.
8. Wählen Sie die **Modul-IP** aus.
9. Geben Sie den **Modul-Port** an, den das Qognify Event Interface-Modul verwendet.
10. Geben Sie den **Streaming-Port** an, den das Qognify Event Interface-Modul verwendet.
11. Wählen Sie das **QEI-Plug-in**.
12. Wählen Sie **32bit erzwingen**, falls die Geräte nicht unter 64 Bit lauffähig sind. Diese Einstellung betrifft nur Geräte, die noch nicht für 64 Bit freigegeben wurden.

Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Support.

13. Klicken Sie auf **Speichern**.
14. Starten Sie die Dienste mit dem ServiceManager neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511) oder fügen Sie weitere Module hinzu.

Informationen zu weiteren Konfiguration finden Sie unter „[Event Interfaces](#)“ auf Seite 349.

Hinzufügen eines Body-Worn Camera Connector Moduls

Das Body-Worn Camera Connector Modul ist für die korrekte Informationsübertragung zwischen der Steuerung und Qognify VMS.

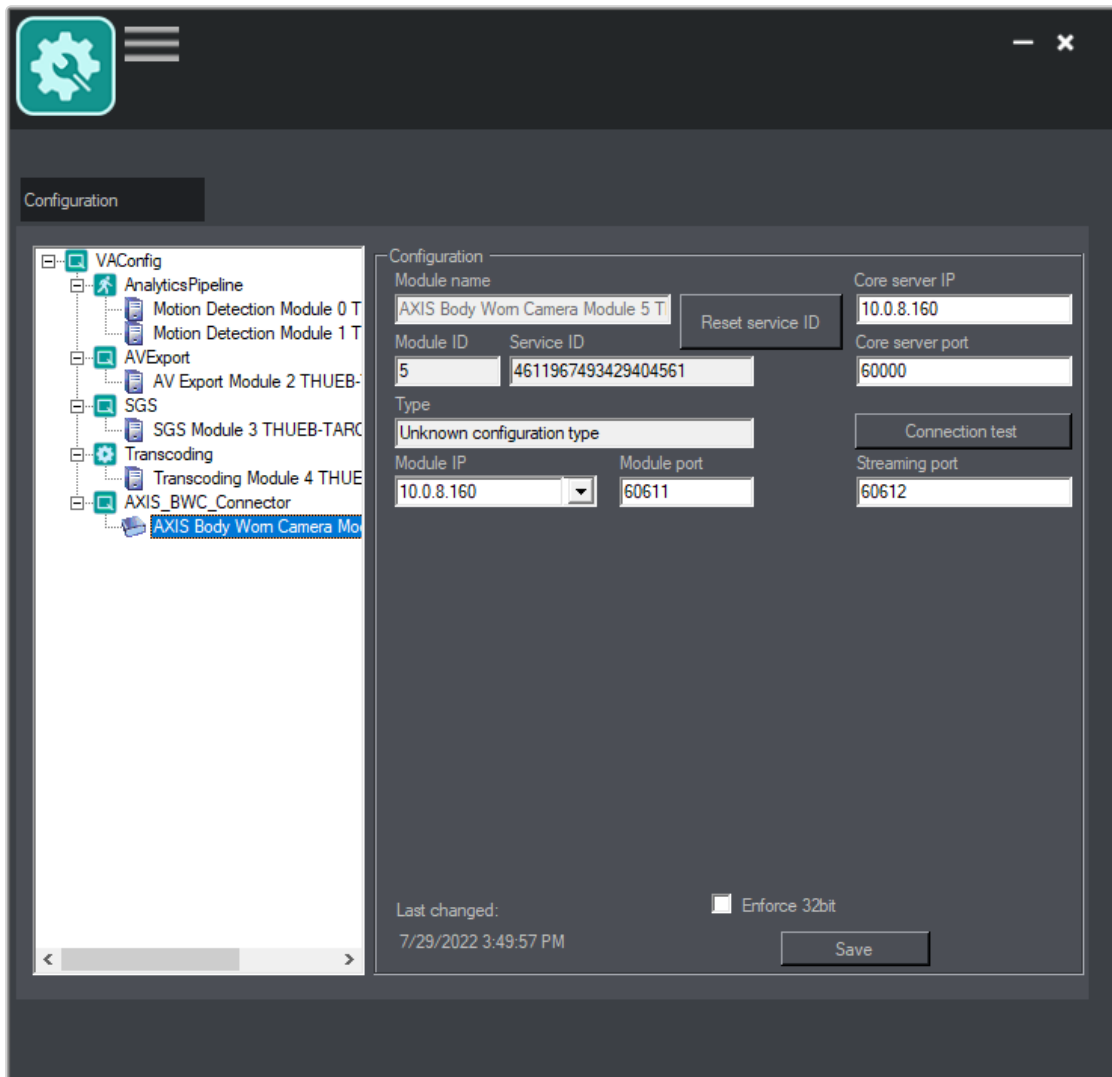


Abb. 279: Hinzufügen eines AXIS Body-Worn Camera Connector Moduls

1. Klicken Sie oben im Modulbaum mit der rechten Maustaste auf **VAConfig**.
2. Wählen Sie im Kontextmenü **Neues Modul hinzufügen**.
3. Wählen Sie im Kontextmenü **AXIS Body-Worn Camera Connector**. Ein neuer Eintrag wird erstellt.
4. Fall nötig, geben Sie die **IP-Adresse** des Hauptservers ein.

Verwenden Sie nicht localhost oder 127.0.0.1 als Eintrag, da andere Dienste über diese IP-Adressen kommunizieren müssen.

Die Service-ID ändert sich nach der ersten Verbindung zum Qognify-Core-Server.

Setzen Sie die Service-ID nur nach Rücksprache mit dem Support zurück.

5. Klicken Sie auf **Verbindungstest**, um die Verbindung zwischen dem Modul und dem Hauptserver zu überprüfen. Wenn keine Verbindung zum Modul hergestellt werden kann, überprüfen und konfigurieren Sie die Netzwerk- und Firewall-Einstellungen.

6. Wählen Sie die **Modul-IP** aus.
7. Geben Sie den **Module-Port** ein.
8. Geben Sie den **Streaming-Port** ein.
9. Wählen Sie **32bit erzwingen**, falls die Geräte nicht unter 64 Bit lauffähig sind.
Diese Einstellung betrifft nur Geräte, die noch nicht für 64 Bit freigegeben wurden.

Ändern Sie den 32-Bit-Modus nur nach Rücksprache mit dem Support.

10. Klicken Sie auf **Speichern**.
11. Starten Sie die Dienste mit dem ServiceManager neu (siehe „[Qognify ServiceManager](#)“ auf Seite 511) oder fügen Sie weitere Module hinzu.

Weitere Informationen zur Konfiguration der am Körper getragenen Kameras finden Sie unter „[Die am Körper getragene AXIS-Kamerasteuerung](#)“ auf Seite 239.

Konfigurationseinstellungen exportieren

Die konfigurierten Einstellungen in Qognify VMS, wie die Kameraeinstellungen, die Benutzer- und Gruppeneinstellungen und die Alarmeinstellungen, können als XLSX-Datei exportiert werden.

1. Navigieren Sie zum Verzeichnis „tools/Configuration export“ im Installationsverzeichnis von Qognify VMS.
2. Führen Sie „VMS_ConfigurationExport.exe“ aus.

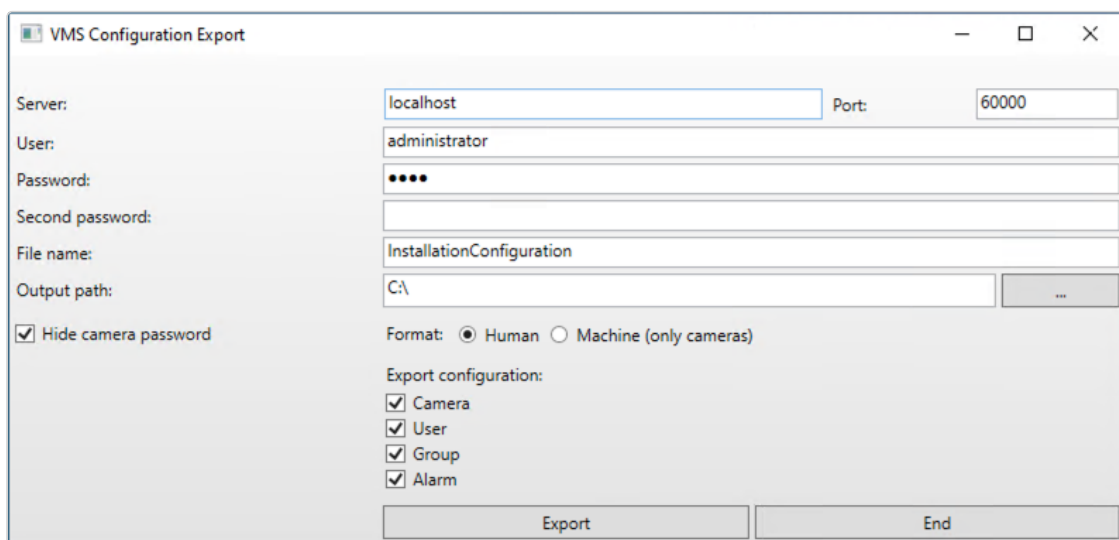


Abb. 280: Konfigurationseinstellungen exportieren

3. Legen Sie die IP des **Servers** fest, auf dem Qognify VMS gehostet wird. Bei einer lokalen Installation geben Sie alternativ „localhost“ ein.
4. Geben Sie die **Port**-Nummer an (Standardport: 60000).
5. Geben Sie den Namen des **Benutzers** und das **Passwort** für den Administrator ein, der in den Qognify VMS-Einstellungen konfiguriert ist (siehe „Anmeldung“ auf Seite 57).
6. Geben Sie bei Bedarf das zweite Passwort an.
7. Geben Sie den **Dateinamen** für die exportierten Daten ein und wählen Sie den Dateipfad zum Ausgabeverzeichnis aus.
8. Wenn die Kamerapasswörter in der Ausgabedatei nicht angezeigt werden sollen, aktivieren Sie **Kamerapasswort ausblenden**.
9. Wenn die Ausgabedatei in einem für Bediener lesbaren Format ausgegeben werden soll, aktivieren Sie **Visuell lesbar** und wählen Sie die Einstellungen aus, die im Export enthalten sein sollen.
10. Wenn die Ausgabedatei nur für den Computer lesbar sein soll, aktivieren Sie **Maschine**.

Nur die Kameraeinstellungen werden exportiert.

11. Aktivieren Sie die Einstellungen, die exportiert werden sollen.
12. Klicken Sie auf **Exportieren**. Der Exportfortschritt wird angezeigt.
13. Beenden Sie die Anwendung, wenn der Export abgeschlossen ist.
14. Öffnen Sie die exportierte Datei mit einer geeigneten Tabellenkalkulationsanwendung.

Kommandozeilenparameter

Übersicht

Kommandozeilenparameter	Anwendung	Bedeutung
alarmid:<AlarmEventID>	Alarm-Watchdog	Alarmereignis mit der angegebenen ID öffnen
camerano:<CameraID>	<ul style="list-style-type: none">▪ Qognify VMS nativer Client▪ Qognify Viewer	Kamera mit der angegebenen ID öffnen
config:<directory>		Pfad für die Client-Konfiguration festlegen
host:<IP/hostname>		IP-Adresse oder Name des Qognify-Servers
-l:<language> (nur ServiceManager und VA Administrationstool)		Sprache ändern: Mit diesem Kommandozeilenparameter ist es

Kommandozeilenparameter	Anwendung	Bedeutung
lang:<Sprache>		möglich, den Client in einer anderen Sprache zu starten. Folgende Sprachen werden unterstützt: en-us (Englisch), de-de (Deutsch), fr-fr (Französisch), ru-ru (Russisch), tr-tr (Türkisch), nl-nl (Niederländisch), sv-sv (Swedish), da-da (Dänisch), no-no (Norwegisch), it-it (Italienisch), es-es (Spanisch), pl-pl (Polnisch), pt-pt (Portugiesisch), cs-cs (Tschechisch), gr-gr (Griechisch), ja-JP (Japanisch), ro-RO (Rumänisch), th-TH (Thai)
log:<directory>		Pfad für das Client-Log festlegen
nat:<true/false>		Anmeldung über NAT ja (true)/nein (false)
nolayers		Client ohne Ansichten starten
nosecondinstancecheck		Unterdrückt die Warnung beim Start des Clients, wenn bereits eine andere Client-Instanz ausgeführt wird.
noserverip		Wenn festgelegt, werden die Beschriftung und das Textfeld des Anmeldebildschirms ausgeblendet. Das Menüelement „Installation wechseln“ ist hiervon nicht betroffen.
nosip		Client mit deaktiviertem SIP-Protokoll starten
pass:<password>		Passwort

Kommandozeilenparameter	Anwendung	Bedeutung
pass2:<password>		Zweites Passwort (falls benötigt)
port:<port>		Port für die Anmeldung, Standard: 60000
profile:<profile>		Profil (Benutzer- oder Gruppenprofil)
user:<user name>		Benutzername
viewer	Qognify VMS-Client	Der Qognify VMS-Client wird direkt im Offline-Modus (Archivmodus) gestartet. Kann zusammen mit dem Befehl „lang“ zur Spracheinstellung verwendet werden.

Vorgehensweise

1. Klicken Sie im Verzeichnis „Startmenü > Programme“ auf die Anwendungsverknüpfung.
2. Klicken Sie mit der rechten Maustaste auf das Anwendungs-Icon und wählen Sie **Eigenschaften**.
3. Navigieren Sie zum Tab **Verknüpfung** und fügen Sie die gewünschten Parameter an den Text im Feld **Ziel** an.

4. Fügen Sie die gewünschten Kommandozeilenparameter an die Eigenschaften des Clients an. Die Kommandozeilenparameter werden in der Form `<key>:<value>` übergeben.

***Beispiel** Um den Qognify-Client in englischer Sprache am Server mit der IP-Adresse 192.168.0.10 zu starten, klicken Sie die Verknüpfung mit der rechten Maustaste an und hängen Sie am Ende der Zeile den Kommandozeilenparameter „lang:en-us“ an.*

Die Zeile wird dann wie folgt angezeigt (für einen Standard-Installationspfad):

```
"C:\Program Files\Qognify\Qognify VMS\Ver-  
satileApplications64\VMS_VA_ConfigurationTool.exe" -  
l:de-DE
```

Beachten Sie, dass nach den Doppelpunkten keine Leerzeichen stehen dürfen.

5. Bestätigen Sie mit **OK** und starten Sie das Programm. Der Client wird mit den eingegebenen Parametern gestartet.

Tastenkürzel

Um Funktionsaufrufe zu beschleunigen, stehen einem Benutzer im Client folgende Tastenkürzel zur Verfügung.

In der Client-Konfiguration sind weitere Tastenkürzel verfügbar und konfigurierbar (siehe „[Tastenkombinationen](#)“ auf Seite 84).

Tastenkürzel	Bedeutung
Strg+1	Wechsel in den Überwachungsmodus
Strg+2	Wechsel in den Archivmodus
Strg+3	Wechsel zur Ereignisauswertung
Strg+4	Wechsel in den Konfigurationsmodus (nur als Administrator möglich)
Strg+5	Wechsel in den LPR-Modus
STRG-Y	Statistik im Videobild im Überwachungs- und Archivmodus anzeigen
F10	Vollbildmodus ein- oder ausschalten

Tastenkürzel	Bedeutung
F1	Qognify-Benutzerhandbuch einblenden
F2	Alle Fenster auf primäres Display verschieben (nur, wenn mehrere Displays angeschlossen sind)
ESC	Alle Steuerelemente ausblenden
+/-	Bei aktivem Digitalzoom wird mit + und - hinein- bzw. herausgezoomt.

Anywhere Viewer

Der Anywhere Viewer ermöglicht Ihnen, auf exportierte Bilddaten zuzugreifen, die im Bildformat von Qognify vorliegen, ohne eine Verbindung zur Datenbank.

Der Viewer zeigt aufgezeichnete Daten nur im Archivmodus an. Alle anderen Modi sind nicht verfügbar, das sie den Zugriff auf die Datenbank erfordern.

- Der Viewer wird im Rahmen der Installation des Qognify VMS-Client grundsätzlich mit installiert. Sie können ihn auch in einer benutzerdefinierten Installation getrennt installieren (siehe „[Angepasste Installation](#)“ auf Seite 41).
- Der Viewer wird bei einem Videodaten-Export in das Exportverzeichnis exportiert.
- Das Handbuch für den Viewer wird während der Installation im Handbuchverzeichnis abgelegt.

Wenn Sie mit dem Viewer Dateien anzeigen, die auf die lokale Festplatte des Client exportiert wurden, müssen Sie alle lokalen Installationen des Qognify VMS-Client beenden, um Konflikte zu vermeiden.

1. Beenden Sie Qognify VMS, wenn es als normaler Client mit Verbindung zu einer Datenbank ausgeführt wird.
2. Starten Sie den Viewer im Exportverzeichnis.

Sprache der Benutzeroberfläche umstellen

Wenn auf der lokalen Festplatte kein Qognify VMS-Client installiert ist, kann die Sprache nur mit Kommandozeilenparametern geändert werden.

1. Beenden Sie den Qognify Viewer und starten Sie den Qognify VMS-Client.
2. Ändern Sie die Sprache der Benutzeroberfläche über das Menü **Datei** in der Funktionsleiste des Qognify VMS-Client (siehe „[Sprache ändern](#)“ auf Seite 85).
3. Beenden Sie den Qognify VMS-Client und starten Sie entweder den Qognify VMS-Client im Viewer-Modus oder den Qognify Viewer.

Aufzeichnung importieren und abspielen

Aufzeichnung in den Viewer importieren

1. Starten Sie den Qognify Viewer (siehe „[Anmeldung](#)“ auf Seite 57). Die Übersicht mit den verfügbaren Aufzeichnungen wird angezeigt.
2. Um zusätzliche exportierte Kamerasequenzen hinzuzufügen, wählen Sie in der Übersicht **Exportierte Kameras hinzufügen** aus.
3. Optional können Sie zum Exportverzeichnis der Aufzeichnung navigieren und den Qognify Viewer im Verzeichnis starten.
4. Navigieren Sie zu dem Verzeichnis, in dem sich die Dateien befinden.

5. Klicken Sie auf **OK**, um die ausgewählten Daten in den Viewer zu importieren.

Wenn Sie ein Verzeichnis öffnen, das mehrere exportierte Kamerasequenzen enthält (selbst in Unterverzeichnissen), werden alle Dateien importiert.

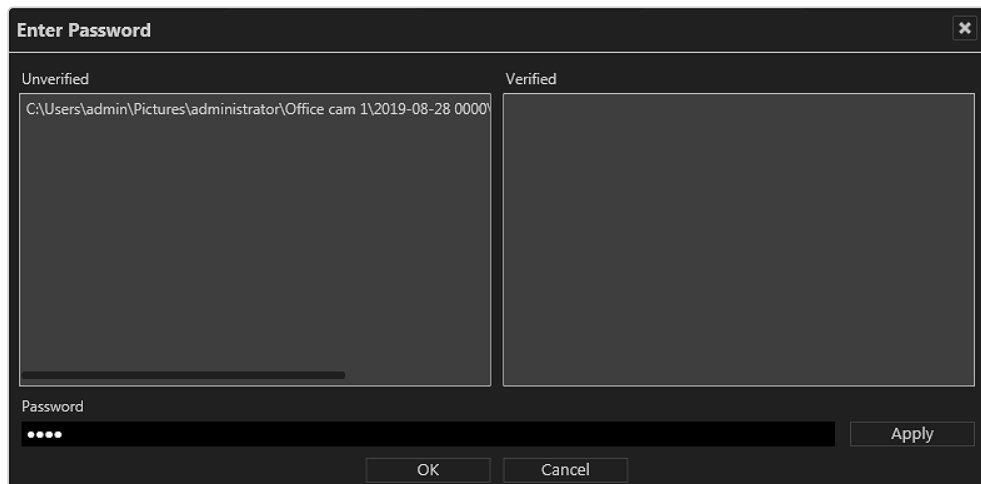


Abb. 281: Auswahl der Datei für den Import in den Viewer im Offline-Modus

6. Geben Sie das beim Export angegebene **Passwort** ein.
 7. **Übernehmen** Sie das Passwort und klicken Sie auf **OK**. Alle exportierten Videosequenzen, die mit dem Passwort übereinstimmen, werden in den Abschnitt „Verifiziert“ rechts verschoben. Sie können weitere Passwörter für zusätzliche Videosequenzen eingeben und anwenden.
 8. Geben Sie das beim Export angegebene **Passwort** ein.
 9. **Übernehmen** Sie das Passwort und klicken Sie auf **OK**. Alle exportierten Videosequenzen, die mit dem Passwort übereinstimmen, werden in den Abschnitt „Verifiziert“ rechts verschoben. Sie können weitere Passwörter für zusätzliche Videosequenzen eingeben und anwenden.
- Das Einlesen der Daten in den Qognify Viewer kann einige Zeit dauern.**
10. Klicken Sie auf die exportierte Kamera, den Sie anzeigen möchten. Alternativ können Sie auch die gewünschte Kamera per Drag & Drop in die bereits belegte Kachel ziehen. Wenn Sie mehrere Sequenzen von derselben Kamera importiert haben, werden diese im Baum als eine Kamera angezeigt. Wenn Sie diese Kamera öffnen, befinden sich alle Sequenzen dieser Kamera im selben Zeitstrahl.

Aufzeichnung abspielen

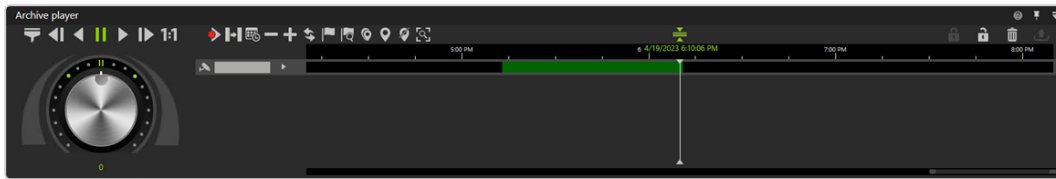


















Abb. 282: Die Steuerelemente des Qognify Viewer







Der Viewer ermöglicht die beschränkte Steuerung des Abspielvorgangs von einer oder mehreren exportierten Aufzeichnungen in einem Zeitstrahl. Im Viewer-Modus bzw. im Viewer können Ansichten verwendet werden, um mehrere Kameras gleichzeitig in einem Raster anzuzeigen. Mehrere Zeitstrahlen werden wie im normalen Qognify VMS-Client angezeigt.


Der Viewer besitzt die folgenden Funktionen:

- **Optionen zur Bandbreitenoptimierung** (): Abhängig von der Lizenz und der Konfiguration kann ein optimierter Videostream ausgewählt werden, um die Client- und Netzwerkauslastung zu reduzieren (siehe „[Bandbreitenoptimierung](#)“ auf Seite 464).
- **Einzelschritt rückwärts** (): Springt zum vorangegangenen Videoframe der Aufzeichnung.
- **Rückwärts abspielen** (3): Spielt den archivierten Videostream in umgekehrter zeitlicher Reihenfolge ab.
- **Pause** (): Unterbricht den Abspielvorgang.
- **Vorwärts abspielen** (): Spielt die Videoaufzeichnung in der zeitlich korrekten Reihenfolge ab.
- **Einzelschritt vorwärts** (): Springt zum nächsten Videoframe der Aufzeichnung.
- **Echtzeit** (): Spielt das Ereignis in Echtzeit ab.
- **Nächste Alarmaufzeichnung** (): Springt zur nächsten Alarmaufzeichnung der ausgewählten Kamera.
- **Pause überspringen** (): Überspringt die Pause zwischen zwei Aufzeichnungen im Abspielmodus.
- **Kalender** (): Öffnet ein Kalenderfenster, um zu einem bestimmten Kalenderzeitpunkt (Datum und Uhrzeit) zu navigieren.

- Aus der Zeitleiste **herauszoomen** () oder **hineinzoomen** (): Vergrößert oder verkleinert die Darstellung der Zeitleiste. Durch einen Klick in die Zeitleiste und anschließendem Drehen des Mausekzes können Sie ebenfalls innerhalb des Aufzeichnungszeitraums zoomen.
- **Zeitleiste aktualisieren** (): Aktualisiert die Zeitleiste der Kamera. Um eine manuelle Synchronisierung mit Edge-Speicherung vorzunehmen (siehe „[Vollständiger Import](#)“ auf Seite 258), klicken Sie bei gedrückter STRG-Taste auf das Symbol.
- **Bookmark hinzufügen** (): Fügt ein Bookmark zum aktuellen Bild hinzu.
- **Bookmark-Übersicht** (): Zeigt die Übersicht aller Bookmarks an (siehe „[Mit Bookmarks arbeiten](#)“ auf Seite 193).
- **Multiselektionsmodus** (): Setzt eine Markierung über mehrere Zeitströme.
- **Marker setzen** (): Setzt die Start- und Endmarkierung für einen ausgewählten Bereich auf der Zeitleiste (siehe „[Bereich bearbeiten](#)“ auf Seite 181).

Bookmarks werden im Viewer-Modus/ Qognify Viewer nicht unterstützt.

- **Markierung löschen** (): Löschen Sie die ausgewählte Markierung.
- **QogniFinder** (): Startet die forensische Suche, wenn die entsprechenden Nutzungsrechte vorhanden sind (siehe „[Verwenden des QogniFinder](#)“ auf Seite 183).
- **Synchronisierter Modus** (): Alle sichtbaren Kameras werden standardmäßig auf die Zeit der ausgewählten Kamera synchronisiert. Wenn der synchronisierte Modus deaktiviert ist, kann jede Kamera einen anderen Zeitpunkt anzeigen.
- **Schreibschutz** ( / ): Setzt den Schreibschutz für den markierten Bereich auf der Zeitleiste. Siehe „[Schreibschutz](#)“ auf Seite 189.
- **Bereich löschen** (): Löscht den markierten Bereich aus der Zeitleiste.

- **Bereich exportieren** (): Startet den AVI-Export bzw. den Qognify-Videodaten-Export (siehe „Aufzeichnungen exportieren“ auf Seite 186).

Der Export in das Qognify-Dateiformat wird nicht unterstützt.

- **Jog Dial**: Spielt die Sequenz vorwärts und rückwärts ab. Je weiter das Jog Dial nach rechts oder links gedreht wird, desto schneller wird vorwärts oder rückwärts abgespielt. Die Abspielgeschwindigkeit wird unter dem Jog Wheel angezeigt.
- **Zeitleiste / Zeitstrahl**: Siehe „Zeitleiste / Zeitstrahl“ auf Seite 180.

Aufzeichnung exportieren

Informationen zum Exportieren der Aufnahmen finden Sie unter „Der Export Designer“ auf Seite 105.

Qognify VMS Web Client

Über den Qognify VMS Web Client wird das Qognify-System mit einer webbasierten Oberfläche in einem Browser dargestellt. Die Bildqualität des an den Web Client übertragenen Videostreams entspricht den Einstellungen eines Standardstreams. Die maximale Bildrate beträgt 12 fps. Die maximale Auflösung wird unter Umständen durch die Größe der Kachel, in der das Videobild dargestellt wird, begrenzt.

Im Überwachungsmodus bietet die Weboberfläche Grundfunktionen des Clients, wie z. B.:

- Zugreifen auf Kameras
- Zugreifen auf vordefinierte Ansichten
- Zugreifen auf Lagepläne
- Zugreifen auf Webseiten (d. h. „https://...“)
- Empfangen und Bestätigen von Alarmen
- Steuern der PTZ-Kameras und Aktivieren der PTZ-Preset-Positionen
- Anzeigen von Buttons und Auslösen von deren Aktionen
- Anzeigen des gleichen Entitätenbaums wie in Windows®

Im Archivmodus bietet der Web Client folgende Funktionen:

- Vor-/Rücklauf in Einzelbildschritten im Archiv
- Vorlauf des Archivs in Echtzeit (ohne Geschwindigkeitsauswahl und Rücklauf)

Konfigurationsmodus und Ereignisauswertung sind nicht verfügbar.

Web Client-Dienste auf dem Qognify-Server installieren

1. Führen Sie eine angepasste Installation des Qognify-Systems durch (siehe [„Angepasste Installation“ auf Seite 41](#)) und fügen Sie zusätzlich das Web Client-Feature hinzu.
2. Wechseln Sie zum nativen Qognify-Client und öffnen Sie das Menü „Server“ im Konfigurationsmodus.
3. Wählen Sie **Server - Transcoding-Modul** im Konfigurationsmodus und konfigurieren Sie die erforderlichen Einstellungen (siehe [„Transcoding-Modul konfigurieren“ auf Seite 453](#)).
4. Wählen Sie **Server - Gateway Service** im Konfigurationsmodus und konfigurieren Sie die erforderlichen Einstellungen (siehe [„Gateway-Service-\(SGS-S-\)Modul konfigurieren“ auf Seite 452](#)).

Wenn Sie die korrekte IP des Core-Servers ausgewählt haben (Informationen zum Abrufen der IP-Adresse finden Sie unter [„Konfigurieren des Hauptdienstes“ auf Seite 435](#)), sollte der Gateway-Service vom Installationsprogramm automatisch konfiguriert werden.

Mit Qognify Web Client verbinden

1. Öffnen Sie einen aktuellen Browser und geben Sie in der URL-Zeile die IP-Adresse des Clients ein: „https://<Ihre-Client-IP>“. Das Web Client-Webseite wird angezeigt.

Achten Sie darauf, dass die URL mit "https" beginnt.

2. Wenn Sie gebeten werden, einigen Sicherheitsausnahmen zu vertrauen, bestätigen Sie die Anforderung.
3. Geben Sie im Anmeldebildschirm den **Benutzernamen** und das **Passwort** ein.
4. Klicken Sie auf **Anmeldung**.

Anmerkungen, Einschränkungen und bekannte Probleme

- Die Auflösung und Qualität der Streams auf den Mobile Client kann im Benutzerprofil konfiguriert werden (siehe „[Bildeinstellungen](#)“ auf Seite 377):
 - Für Einzelbild (Motion JPEG, MxPEG): **Normale** Qualität
 - Für konfigurierte Videoklassifikationen: **Normale** oder **mittlere** Qualität
- Die Uploadgeschwindigkeit muss mindestens 2 MB/s betragen (für 2 bis 3 simultane Kameraansichten). Je höher die Anzahl der Verbindungen und Kameraansichten, desto mehr Bandbreite wird benötigt.
- Die folgenden Ports müssen bei Verwendung einer Firewall transparent weitergeleitet werden:
 - Port 62000 (SGS)
 - Port 9100 (RTSP-Proxy)
 - Port 443 (Webserver)
 - Port 8081 (Node.js, liefert die Bilder)
- Grandeye IPC Fisheye-Kameras werden derzeit nicht unterstützt und es ist kein Live-Stream möglich.
- Es wird empfohlen, eine aktuelle Browserversion zu verwenden.
- Die Uploadgeschwindigkeit muss mindestens 2 MB/s betragen (für 2 bis 3 simultane Kameraansichten). Je höher die Anzahl der Verbindungen und Kameraansichten, desto mehr Bandbreite wird benötigt.
- Die folgenden Ports müssen bei Verwendung einer Firewall transparent weitergeleitet werden:
 - Port 62000 (SGS)
 - Port 9100 (RTSP-Proxy)
 - Port 443 (Webserver)
 - Port 8081 (Node.js, liefert die Bilder)
- Im Qognify-System konfigurierte Benutzerprofile werden nicht unterstützt. Zugeordnete Startansichten für das Benutzerprofil werden im Web Client nicht automatisch angezeigt. Die Benutzer- und Gruppenrechte sind hiervon nicht betroffen.

- Neu hinzugefügte oder gelöschte Kameras werden erst nach erneutem Laden des Web Clients im Browser angezeigt. Es gibt keine Einschränkung bezüglich der Anzahl an gleichzeitig angezeigten Kameras, beachten Sie jedoch, dass der Webbrowser alle Bilder darstellen muss UND dass die Bilder über den TranscodingService geliefert werden müssen, der nur die konfigurierte Anzahl an Kanälen bedient. Die Bilddarstellung ist auch von der Hardware abhängig.
- Grandeye IPC Fisheye-Kameras werden derzeit nicht unterstützt und es ist kein Live-Stream möglich.
- MOBOTIX (MxPEG)-Kameras erzeugen ein gespiegeltes Bild, wenn ein Einzelbild exportiert wird.
- Wenn eine Ansicht eine unsichere (Nicht-HTTPS) Webseite enthält oder eine vordefinierte unsichere (Nicht-HTTPS) Webseite im Web Client angezeigt wird, stellt der Browser die Webseite möglicherweise nicht dar, da sie vom Browser oder den Systemeinstellungen automatisch als „unsicher“ blockiert wird. Abhängig vom Browser können diese Kontrollen dauerhaft oder für die aktuelle Sitzung deaktiviert werden.
- Objekte wie Kameras, Ansichten, Lagepläne usw. müssen in den Ansichtsbereich gezogen werden (sie werden nicht durch Klicken wie im nativen Qognify VMS-Client angezeigt).

IIS härten

Am von IIS verwendeten Port 443 wurde eine Reihe von Problemen festgestellt, die sich durch Härten des IIS-Servers beheben lassen. Dazu muss die Konfiguration angepasst werden, z. B. mit „forbid SSL v3“.

TLS 1.0 und TLS 1.1 sollten möglichst weiterhin nicht verwendet werden.

SSL 3.0 gilt nicht mehr als ausreichend sicher, es sollte daher auf dem Server deaktiviert werden, falls nicht bereits geschehen.

Falls möglich, sollten auch die TLS-Versionen 1.0 und 1.1 für serverseitige Anwendungen deaktiviert werden.

1. Folgen Sie den unten stehenden Anweisungen, um die einzelnen Protokolle zu deaktivieren.
2. Starten Sie den Server neu, um die Änderungen zu übernehmen.

SSL 3.0

1. Gehen Sie zu
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server.
2. Erstellen Sie den Schlüssel, falls er noch nicht vorhanden ist.
3. Überprüfen Sie, ob der DWORD-Wert „Enabled“ vorhanden und auf 0 gesetzt ist.
4. Überprüfen Sie, ob der DWORD-Wert „DisabledByDefault“ (falls vorhanden) auf 1 gesetzt ist.
5. Außerdem wird empfohlen, SSLv3 für die Client-Authentifizierung zu deaktivieren, indem die obigen Schritte für den Schlüssel HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client wiederholt werden.

TLS 1.0

1. Gehen Sie zu
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server.
2. Erstellen Sie den Schlüssel, falls er noch nicht vorhanden ist.
3. Überprüfen Sie, ob der DWORD-Wert „Enabled“ vorhanden und auf 0 gesetzt ist.
4. Überprüfen Sie, ob der DWORD-Wert „DisabledByDefault“ (falls vorhanden) auf 1 gesetzt ist.

TLS 1.1

1. Gehen Sie zu
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server.
2. Erstellen Sie den Schlüssel, falls er noch nicht vorhanden ist.
3. Überprüfen Sie, ob der DWORD-Wert „Enabled“ vorhanden und auf 0 gesetzt ist.

4. Überprüfen Sie, ob der DWORD-Wert „DisabledByDefault“ (falls vorhanden) auf 1 gesetzt ist.

Der Qognify VMS Mobile Client

Die Mobile Client-App ist für iOS 7 oder höher und Android 2.3 oder höher verfügbar.

Im Überwachungsmodus bietet die mobile Oberfläche Grundfunktionen des Clients, wie z. B.:

- Zugreifen auf Kameras
- Zugreifen auf vordefinierte Ansichten
- Empfangen und Bestätigen von Alarmen
- Steuern der PTZ-Kameras und Aktivieren der PTZ-Preset-Positionen
- Anzeigen von Buttons und Auslösen von deren Aktionen
- Senden des ausgewählten Bilds per E-Mail

Im Archivmodus bietet der Mobile Client folgende Funktionen:

- Vor-/Rücklauf in Einzelbildschritten im Archiv
- Vorlauf des Archivs in Echtzeit (ohne Geschwindigkeitsauswahl und Rücklauf)
- Senden des ausgewählten Bilds per E-Mail

Konfigurationsmodus und Ereignisauswertung sind nicht verfügbar.

Mobile Client-Dienste auf dem Qognify-Server installieren

1. Führen Sie eine benutzerdefinierte Installation des Qognify-Systems durch (siehe „[Angepasste Installation](#)“ auf Seite 41) und fügen Sie zusätzlich das Mobile Client-Feature hinzu.
2. Wechseln Sie zum nativen Qognify-Client und öffnen Sie das Menü „Server“ im Konfigurationsmodus.
3. Wählen Sie **Server - Transcoding-Modul** im Konfigurationsmodus und konfigurieren Sie die erforderlichen Einstellungen (siehe „[Transcoding-Modul konfigurieren](#)“ auf Seite 453).
4. Wählen Sie **Server - Gateway Service** im Konfigurationsmodus und konfigurieren Sie die erforderlichen Einstellungen (siehe „[Gateway-Service-\(SGS-S-\)Modul konfigurieren](#)“ auf Seite 452).

Wenn Sie die korrekte IP des Core-Servers ausgewählt haben (Informationen zum Abrufen der IP-Adresse finden Sie unter „[Konfigurieren des Hauptdienstes](#)“ auf Seite 435), sollte der Gateway-Service vom Installationsprogramm automatisch konfiguriert werden.

Mobile Client auf einem Mobilgerät installieren

1. Überprüfen Sie vor dem Herunterladen, dass Ihr Gerät die erforderlichen Voraussetzungen erfüllt. Der Client ist in „Google Play“ für Android OS Version 2.3 oder höher und im iTunes App Store für iOS 7 oder höher erhältlich.
2. Laden Sie die Applikation im entsprechenden App Store herunter.

Qognify Mobile Client auf dem Mobilgerät konfigurieren

1. Starten Sie die App auf dem Mobilgerät.
2. Tippen Sie auf **Server hinzufügen** und geben Sie den **Benutzernamen** ein.
3. Geben Sie eine **Beschreibung** für den Server ein.
4. Geben Sie die SOAP-IP oder **URL** des Servers ein.
5. Geben Sie die **Portnummer** des Servers ein.
6. iOS-Geräte: Geben Sie bei Verbindung über ein 3G-Netzwerk die **FPS** (Bilder pro Sekunde) und die horizontale **Auflösung** an. Die Standardeinstellungen lauten: 3 fps und eine Auflösung von 200 px.
7. Wählen Sie den Servertyp aus (SeeTec 5 oder Qognify VMS).
8. Tippen Sie auf **Speichern**.

Anmerkungen, Einschränkungen und bekannte Probleme

- Auflösung und Qualität der Streams auf den Mobile Client:
 - Android-Tablet und -Smartphone: 480 x 320 px, 12 fps (WLAN & 3G)
 - iOS-iPad und -iPhone (niedrige Auflösung): Breite 480 px, 24 fps
 - iOS-iPad und -iPhone (hohe Auflösung): 703 x 512 px, 24 fps
- Die Uploadgeschwindigkeit muss mindestens 2 MB/s betragen (für 2 bis 3 simultane Kameraansichten). Je höher die Anzahl der Verbindungen und Kameraansichten, desto mehr Bandbreite wird benötigt.
- Die folgenden Ports müssen bei Verwendung einer Firewall transparent weitergeleitet werden:
 - Port 62000 (SGS)
 - Port 9100 (RTSP-Proxy)
 - Port 443 (Webserver)
 - Port 8081 (Node.js, liefert die Bilder)

Mit Qognify Mobile Client verbinden

1. Starten Sie die App auf dem Mobilgerät.
2. Wählen Sie einen vorkonfigurierten Server aus.
3. Geben Sie das Passwort an.
4. Tippen Sie auf **Anmeldung**.

Installation des Qognify Metadata Manager (QMM)

Einleitung

Der Qognify Metadata Manager (QMM) ist ein Modul, das Objektmetadaten von externen Videoanalysequellen übernimmt und speichert, um diese Metadaten für den QogniFinder bereitzustellen. QogniFinder ist eine Benutzeroberfläche im Qognify VMS-Client, die aufgezeichnetes Videomaterial nach bestimmten Objekttypen und weiteren Objektmerkmalen durchsuchen kann.

Objektmetadaten werden in Echtzeit generiert und gespeichert.

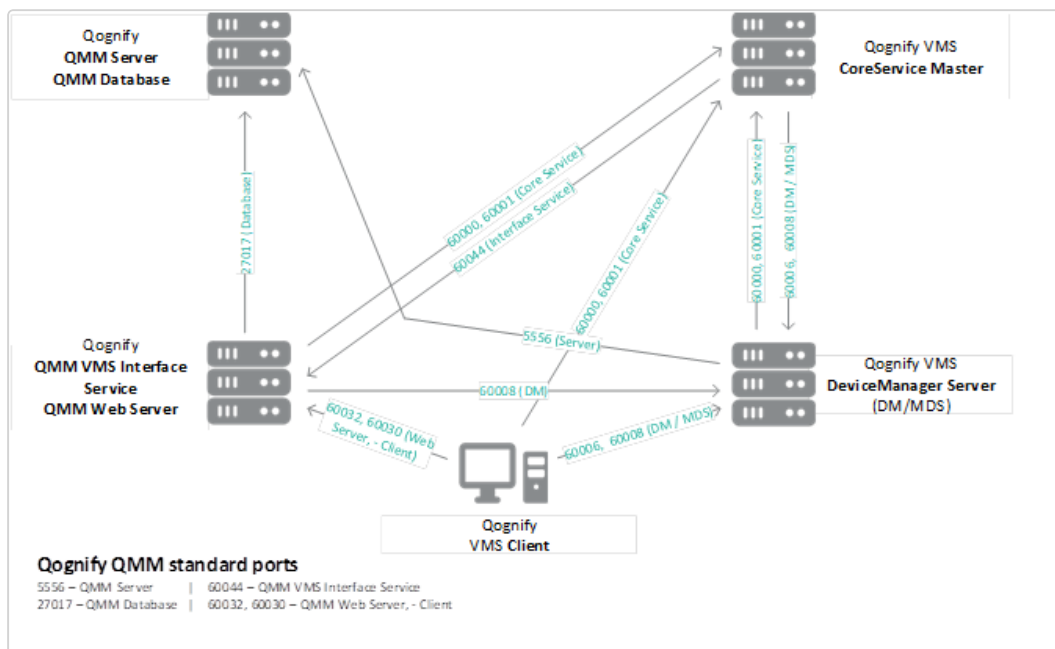
Voraussetzungen

Diese Anleitung beschreibt den Installationsvorgang des Qognify Metadata Manager.

Ein installiertes Qognify VMS ist erforderlich.

Bei der Installation werden .Net Framework and Microsoft Visual C++ Redistributable automatisch installiert, sobald der Installationsvorgang gestartet wird. Während der Installation kann ein Neustart des Betriebssystems erforderlich werden. Stellen Sie sicher, dass alle offenen Programme geschlossen werden, bevor Sie die Setup-Datei ausführen. Nach dem erneuten Start wird der Installationsvorgang automatisch fortgesetzt.

Architektur und verwendete Standard-Ports



Komponentenname	Beschreibung
QMM-Datenbank	MongoDB, die alle gesammelten Metadaten speichert
QMM-Server	Ein Service, der auf der gleichen Maschine wie die MongoDB läuft, der die Metadaten empfängt und sie in die Datenbank schreibt.
QMM VMS-Schnittstellenservice	Kommunikationsdienst zwischen QMM und Qognify VMS
QMM WebServer	IIS, das Metadaten aus der QMM-Datenbank anfordert und sie an den Qognify VMS Client liefert.

Installation und Upgrade	556
Kameraeinstellungen	570
Fehlerbehebung	572

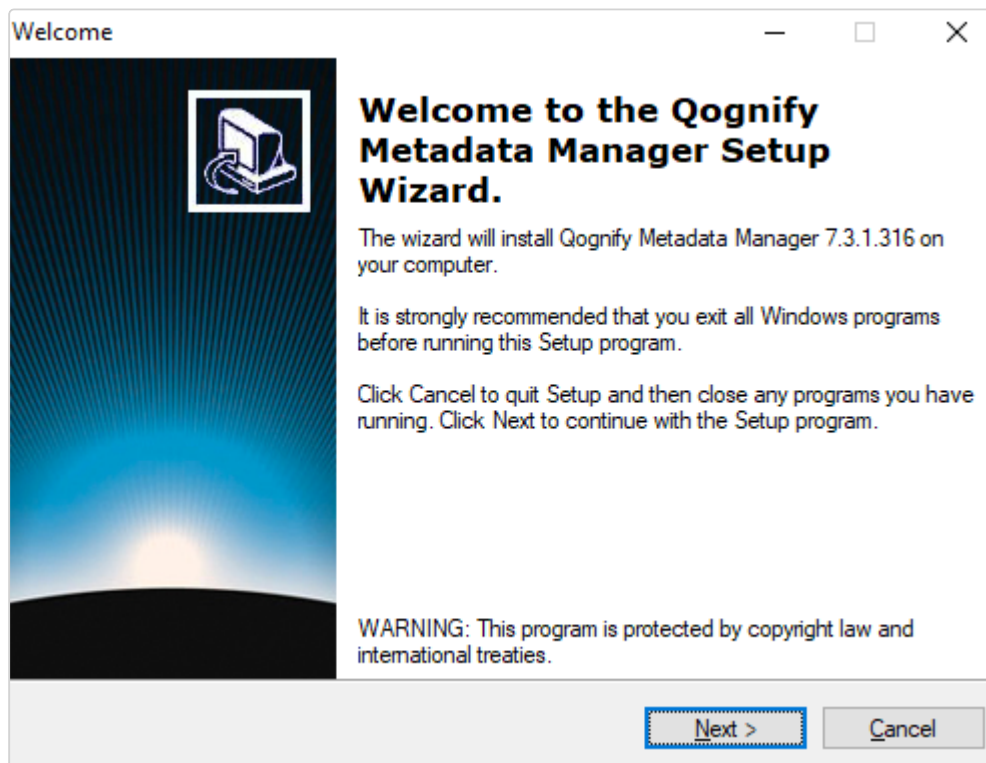
Installation und Upgrade

Der QMM-Installer wird als eine Zip-Datei bereitgestellt.

1. Dekomprimieren Sie das Installationsprogramm.
2. Führen Sie die Installationsdatei als Administrator aus und befolgen Sie den Installations-Assistenten. Sobald der Installationsvorgang beginnt, werden die folgenden Komponenten auf dem Server installiert:
 - .Net Framework 4.8
 - Microsoft Visual C++ Redistributable 2015-2019

Um die Installation fortzusetzen, ist der Neustart des Betriebssystems zwingend erforderlich.

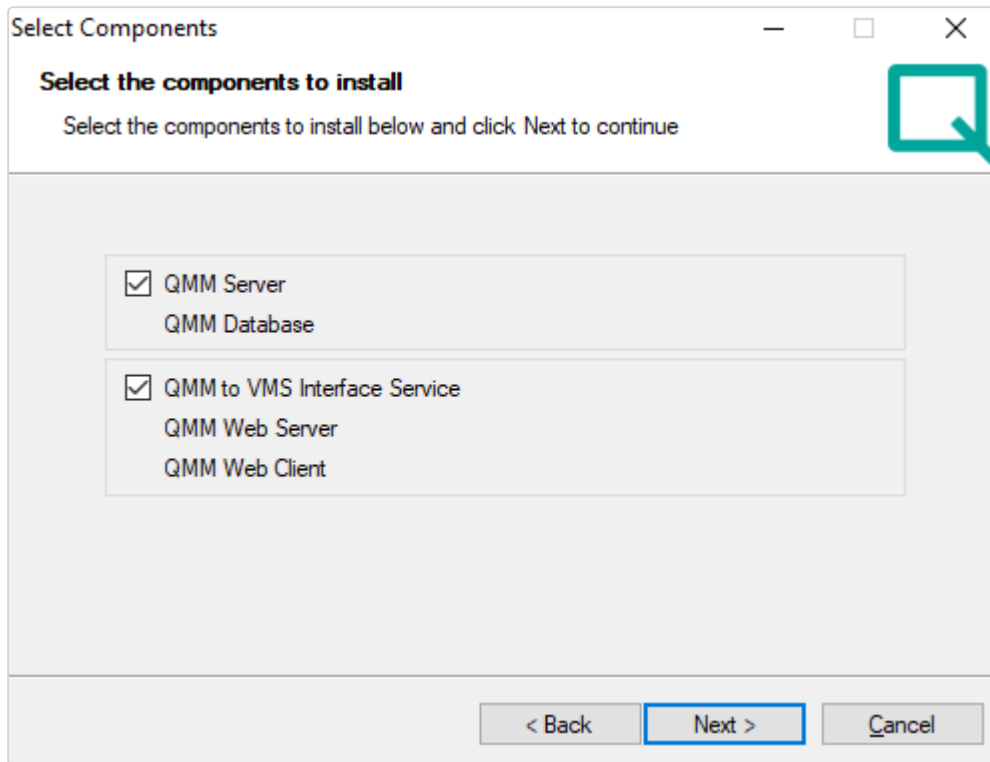
Nach dem Neustart wird die Installation unverzüglich starten und Sie werden den Begrüßungsbildschirm sehen.



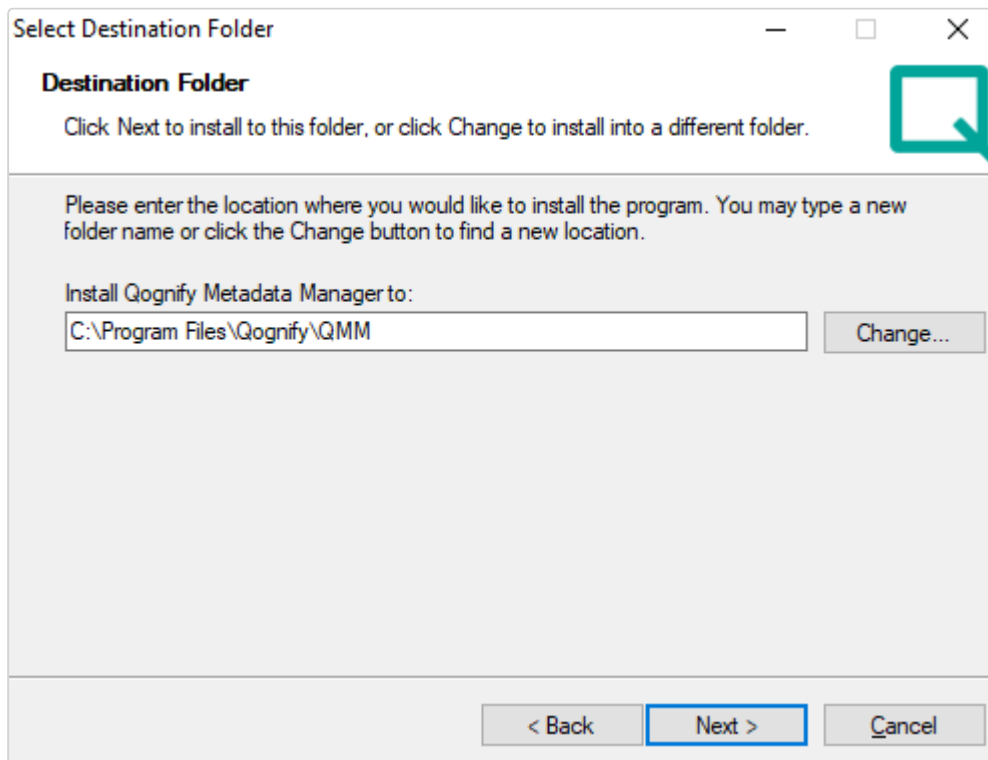
3. Die Endbenutzerlizenzvereinbarung lesen und akzeptieren.
4. Wählen Sie **Weiter**.

Wählen Sie im nächsten Abschnitt Komponenten, die Sie auf dem PC installieren möchten.

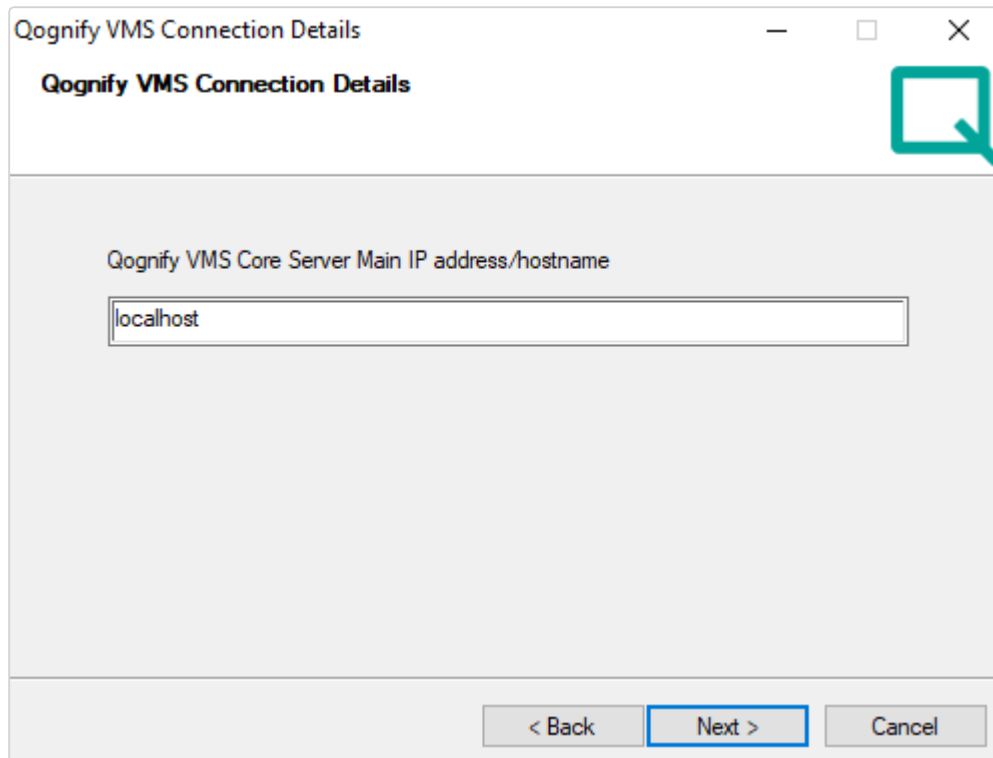
Option 1 (Standard): Alle Komponenten auswählen



1. Aktivieren Sie die Kontrollkästchen für alle Komponenten und wählen Sie **Weiter**.



2. Spezifizieren Sie auf der nächsten Seite das Installationsverzeichnis und wählen Sie **Weiter**.



Qognify VMS Connection Details

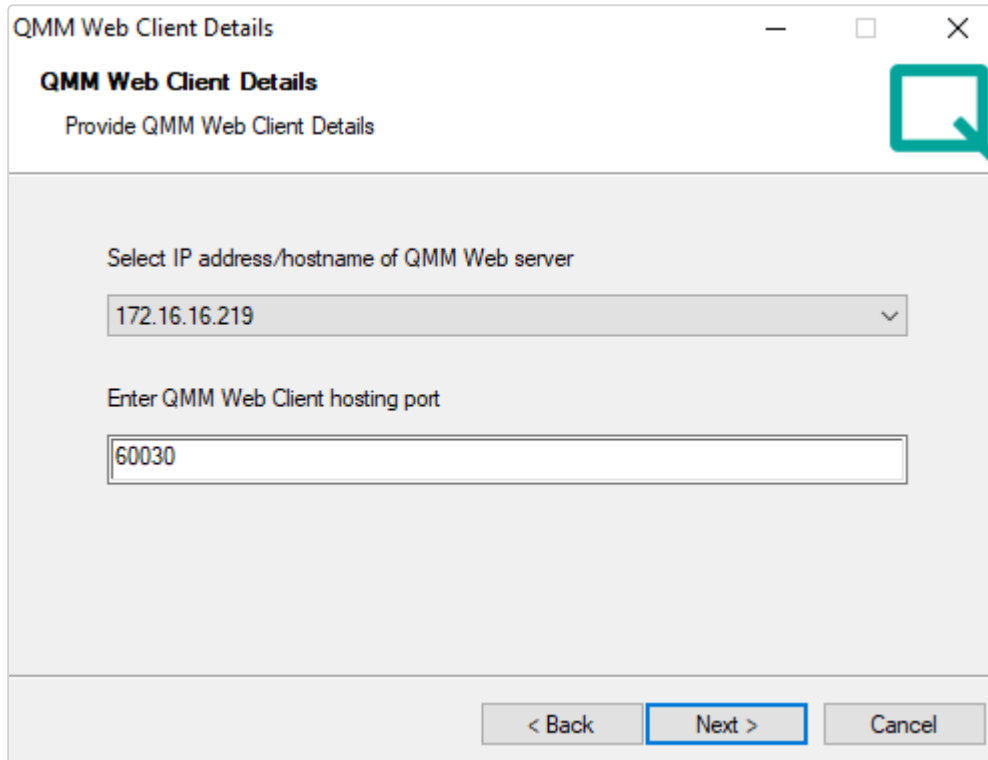
Qognify VMS Connection Details

Qognify VMS Core Server Main IP address/hostname

localhost

< Back Next > Cancel

3. Geben Sie die IP-Adresse oder den Host-Namen des Qognify VMS Core-Server-Main ein. Der Kommunikations-Port ist als Standard auf „60000“ gestellt und kann während des Installationsvorgangs nicht geändert werden.



QMM Web Client Details

QMM Web Client Details
Provide QMM Web Client Details

Select IP address/hostname of QMM Web server

172.16.16.219

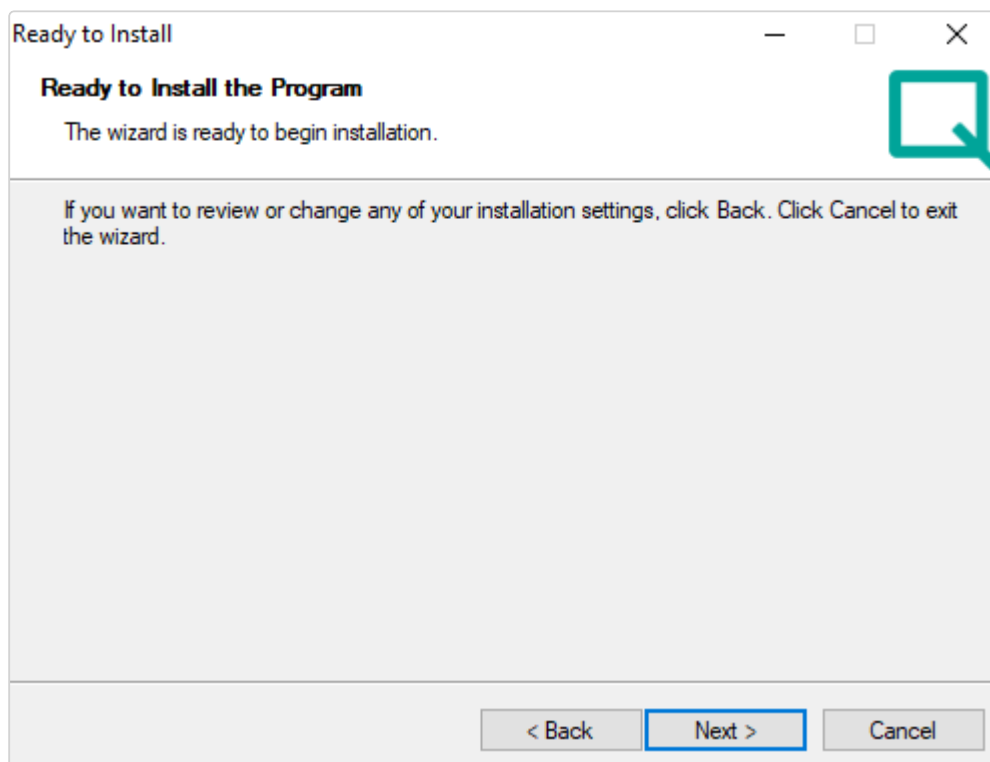
Enter QMM Web Client hosting port

60030

< Back Next > Cancel

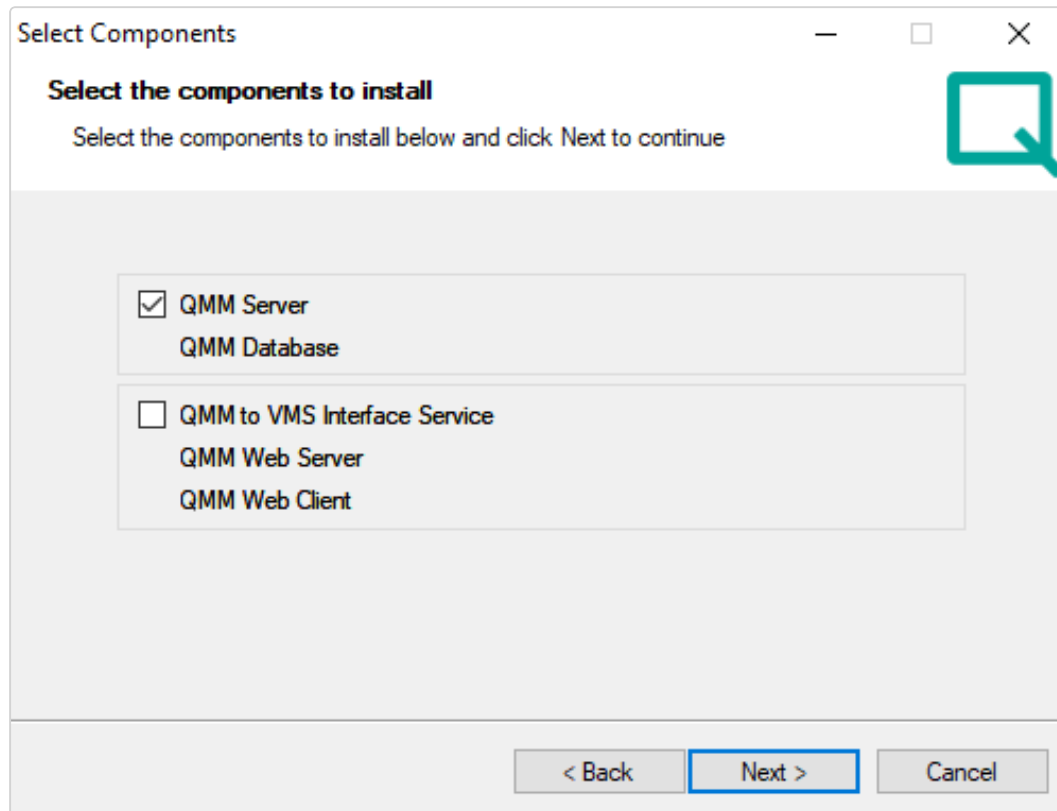
4. Wählen Sie die IP-Adresse oder den Host-Namen, auf der/dem der Web-Server zugänglich sein sollte. Spezifizieren Sie auch einen Port (Standard: 60030) für die Kommunikation.

Vergessen Sie nicht den Port in Ihren Firewall-Einstellungen zu öffnen, wenn die Installation abgeschlossen ist.



5. Wählen Sie **Weiter**, um die Installation zu starten.
6. Wählen Sie nach der Installation **Beenden**, um den Setup-Assistenten zu schließen.

Option 2: QMM-Server & QMM-Datenbank auswählen



Select Components

Select the components to install

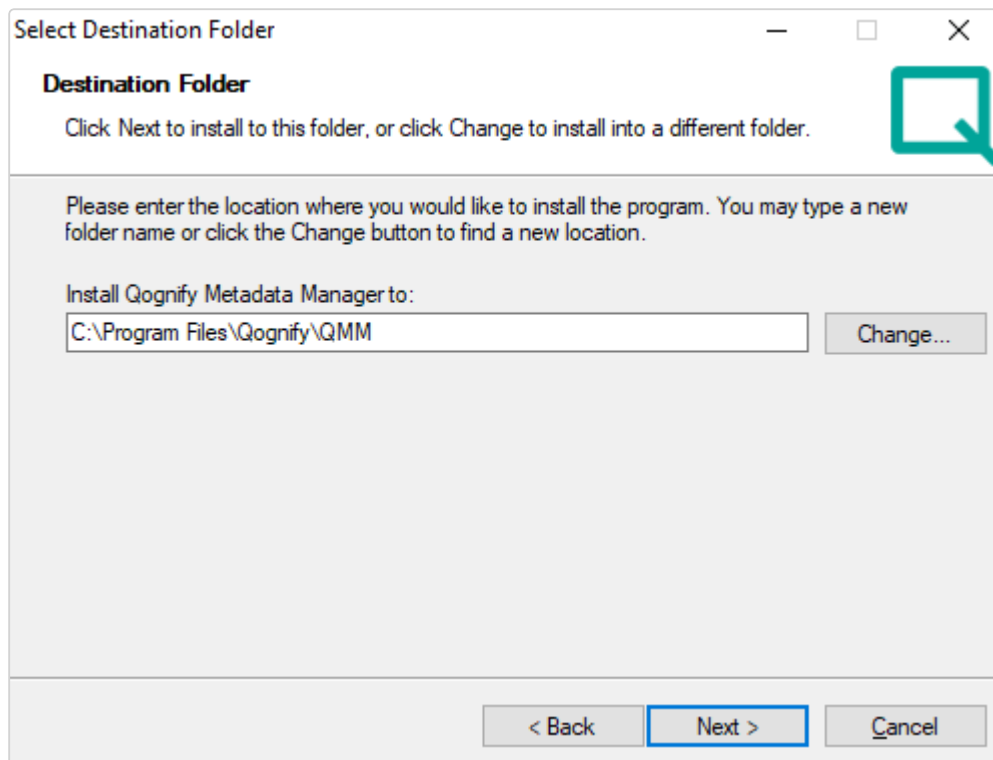
Select the components to install below and click Next to continue

QMM Server
QMM Database

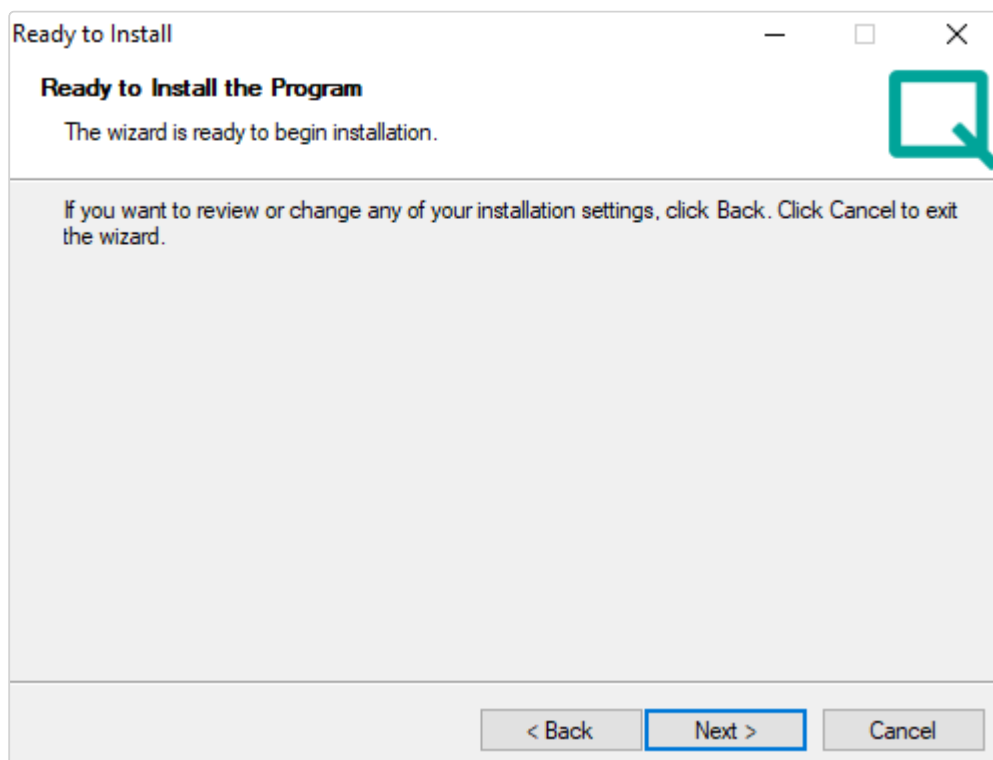
QMM to VMS Interface Service
QMM Web Server
QMM Web Client

< Back **Next >** Cancel

1. Aktivieren Sie den QMM-Server und die QMM-Datenbank und wählen Sie **Weiter**.



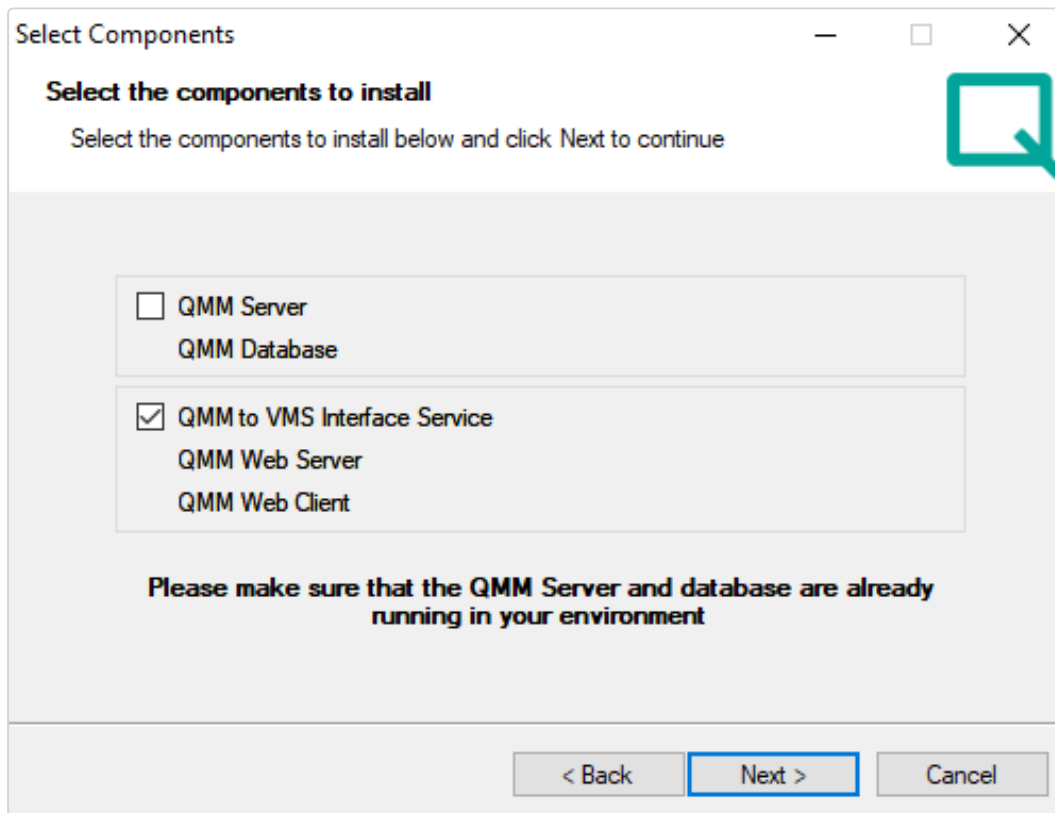
2. Spezifizieren Sie das Installationsverzeichnis und wählen Sie **Weiter**.



3. Wählen Sie **Weiter**, um die Installation zu starten.
4. Wählen Sie nach der Installation **Beenden**, um den Setup-Assistenten zu schließen.

Option 3: QMM-to-VMS Interface Service & QMM WebServer auswählen

Für diese Art der Installation benötigen Sie in Ihrer Umgebung einen vorhandenen QMM-Server und eine QMM-Datenbank.



Select Components

Select the components to install

Select the components to install below and click Next to continue

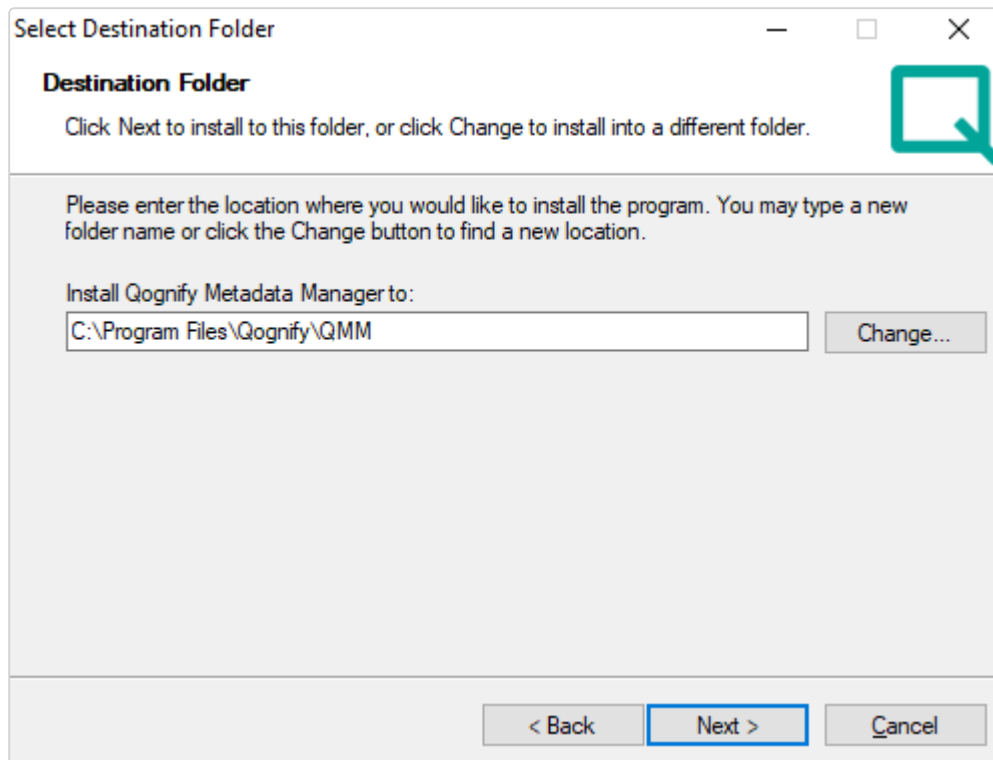
QMM Server
QMM Database

QMM to VMS Interface Service
QMM Web Server
QMM Web Client

Please make sure that the QMM Server and database are already running in your environment

< Back Next > Cancel

1. Aktivieren Sie den QMM-to-VMS Interface Service und wählen Sie **Weiter**.



Select Destination Folder

Destination Folder

Click Next to install to this folder, or click Change to install into a different folder.

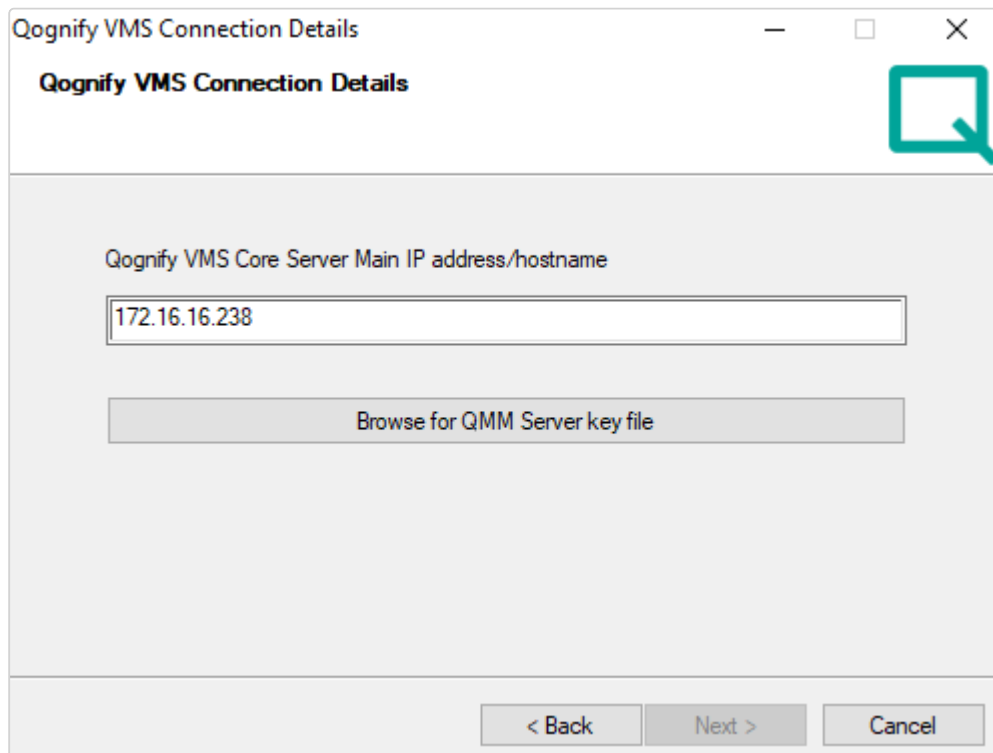
Please enter the location where you would like to install the program. You may type a new folder name or click the Change button to find a new location.

Install Qognify Metadata Manager to:

C:\Program Files\Qognify\QMM

< Back

2. Spezifizieren Sie das Installationsverzeichnis und wählen Sie **Weiter**.



Qognify VMS Connection Details

Qognify VMS Connection Details

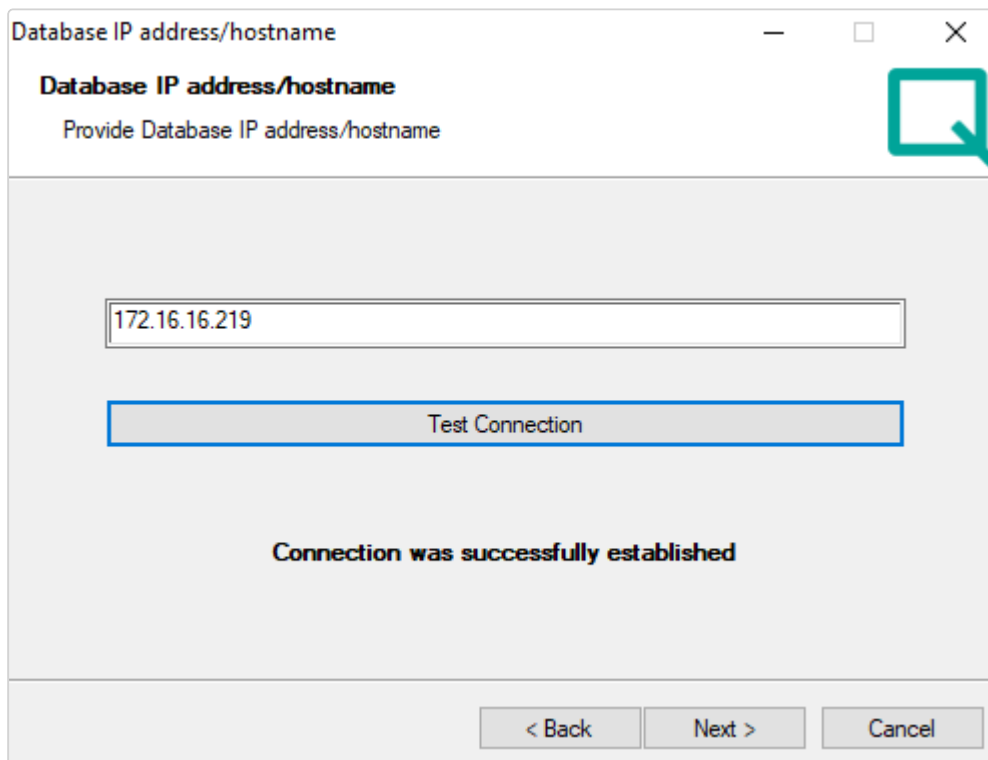
Qognify VMS Core Server Main IP address/hostname

172.16.16.238

< Back

565 / 574

3. Geben Sie die IP-Adresse für den öffentlichen QMM-Server-Schlüssel ein, der auf dem PC gespeichert wird, auf dem der QMM-Server und die QMM-Datenbank installiert sind. Sie können die Schlüsseldatei finden
4. Wählen Sie Nach QMM Server-Schlüsseldatei suchen und wählen Sie die Schlüsseldatei *QVAServerPublic.key* im Installationsverzeichnis aus: *%InstallDir%\Qognify\QMM\QMM Server*
5. Spezifizieren Sie die IP-Adresse oder den Host-Namen auf dem Qognify VMS Core Main Server und wählen Sie **Weiter**.



Database IP address/hostname

Database IP address/hostname
Provide Database IP address/hostname

172.16.16.219

Test Connection

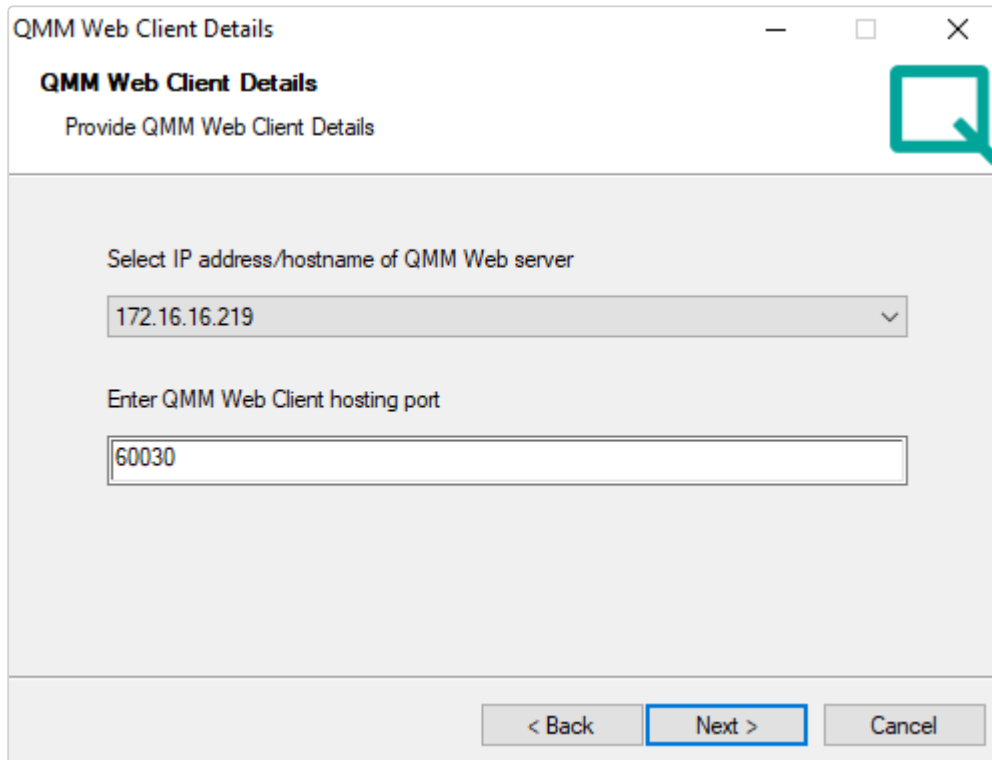
Connection was successfully established

< Back Next > Cancel

6. Stellen Sie IP-Adresse der QMM-Datenbank ein.

- Wählen Sie **Testverbindung** und warten Sie bis die Verbindung aufgebaut ist. Sobald die Verbindung erfolgreich hergestellt wurde, wählen Sie **Weiter**.

Stellen Sie sicher, dass die QMM-Datenbank läuft und aus der Ferne zugänglich ist.



- Wählen Sie die IP-Adresse oder den Host-Namen, auf der/dem der Web-Server zugänglich sein sollte
- Spezifizieren Sie einen Port (Standard: 60030) für die Kommunikation.

Vergessen Sie nicht den Port in Ihren Firewall-Einstellungen zu öffnen, wenn die Installation abgeschlossen ist.

- Wählen Sie **Weiter**, um die Installation zu starten.
- Wählen Sie nach der Installation **Beenden**, um den Setup-Assistenten zu schließen.

Upgrade und Deinstallation ausführen

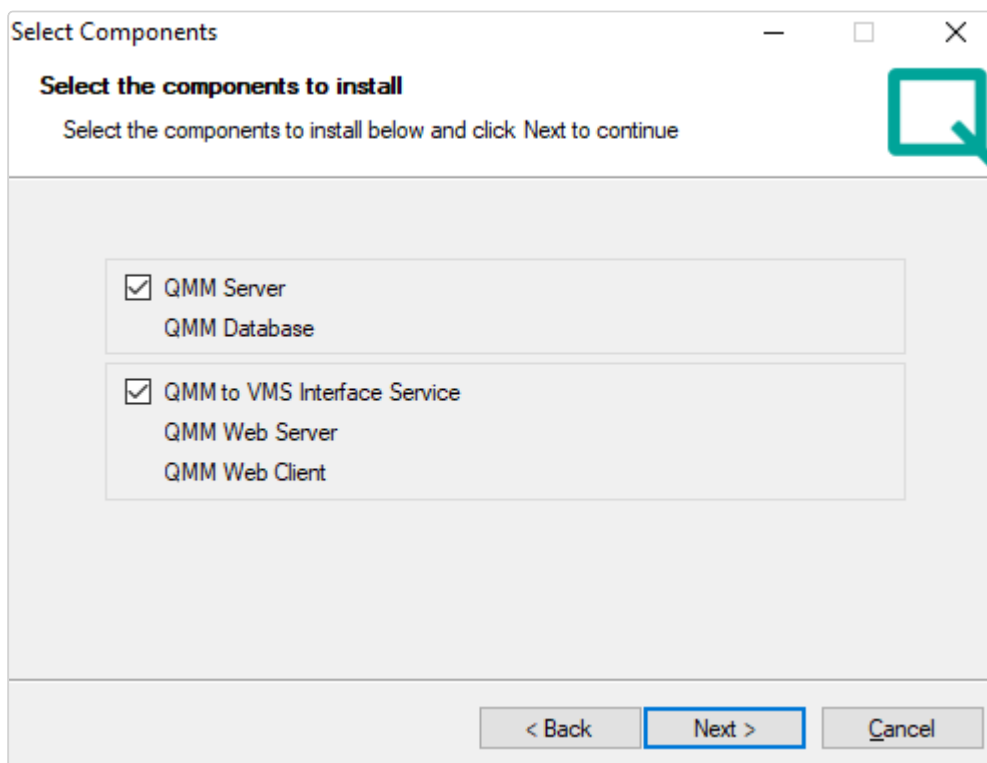
Upgrade ausführen

Die Software kann aktualisiert werden, ohne die vorherige Version zu deinstallieren.

Ein automatischer Neustart des Betriebssystems kann erforderlich sein. Stellen Sie sicher, dass Sie alle Anwendungen schließen, bevor Sie das Installationsprogramm ausführen.

Nach dem Neustart wird die Installation unverzüglich gestartet.

1. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.

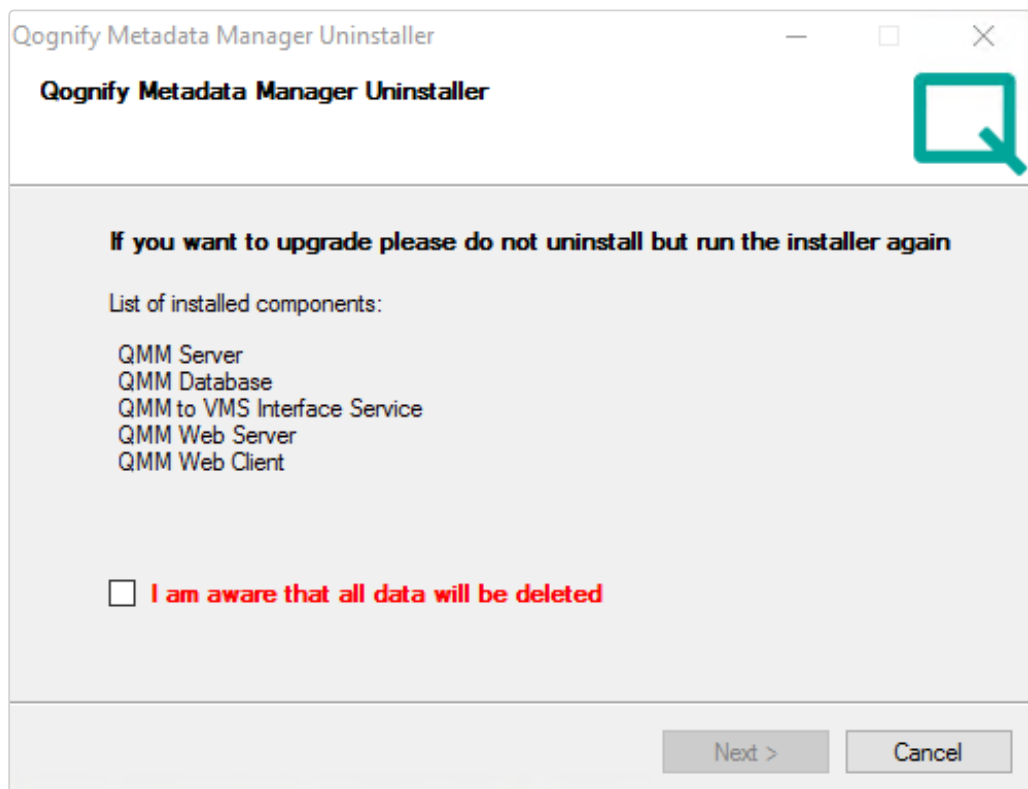


2. Wählen Sie die Komponenten, die Sie hochstufen möchten. Nur die zuvor installierten Komponenten werden ausgewählt.
3. Wählen Sie **Weiter**, um die Installation zu starten.
4. Wählen Sie nach der Installation **Beenden**, um den Setup-Assistenten zu schließen.

Deinstallieren

Beachten Sie, dass alle Komponenten und ihre Konfiguration bei der Deinstallation gelöscht sind. Alle gespeicherten Objektmetadaten werden gelöscht.

1. Um die Software vollständig zu deinstallieren, öffnen Sie **Systemsteuerung > Programme und Funktionen** und wählen Sie „Qognify Metadata Manager“.
2. Wählen Sie **Deinstallieren**. Der Deinstallationsprozess wird gestartet.



3. Um fortzufahren, aktivieren Sie das Kontrollkästchen und klicken auf **Weiter**.

Kameraeinstellungen

Um Metadaten von einer Kamera zu erhalten, müssen Sie das Gerät zuerst Ihrer Qognify VMS-Installation hinzufügen. Für mehr Informationen darüber, wie dem Qognify VMS-System eine neue Kamera-Entität hinzugefügt wird, siehe „Kameras“ auf Seite 231.

Um die von der Kamera erkannten Metadaten mit einem sehr genauen Zeitstempel zu erhalten, aktivieren Sie die Zeitsynchronisation und die Objekterkennung auf der Kamera-Seite.

Die Zeitsynchronisation ist für die Funktion des QogniFinder essentiell, da die Metadaten den korrekten Zeitstempel erfordern.


Unterstützte Geräte

Die folgende Kamera-Serie von Hanwha wird unterstützt:

- P-Serie AI - bietet Objekt-Klassifikation und weitere Attribute
- X-Serie AI - bietet nur eine Objekt-Klassifikation
- Multi-AI - bietet nur eine Objekt-Klassifikation

Zeitsynchronisation

Um den genauesten Zeitstempel für jedes Ereignis zu erhalten, müssen die Qognify VMS-Komponenten, Kameras, Betriebssysteme usw. mit dem gleichen Zeit-Server synchronisiert werden.

1. Öffnen Sie die Webschnittstelle der Kamera in Ihrem Browser und wählen Sie **Einstellungen** .

2. Wählen Sie **Basic** in der Konfiguration und dann **Datum & Zeit**.


The screenshot shows the WISENET configuration interface. On the left is a navigation menu with the following items: Basic (selected), Video profile, User, Date & Time, IP & Port, PTZ, Video & Audio, Network, Event, Analytics, Statistics, System, and Open platform. The main content area is titled 'Date & Time' and contains the following sections:

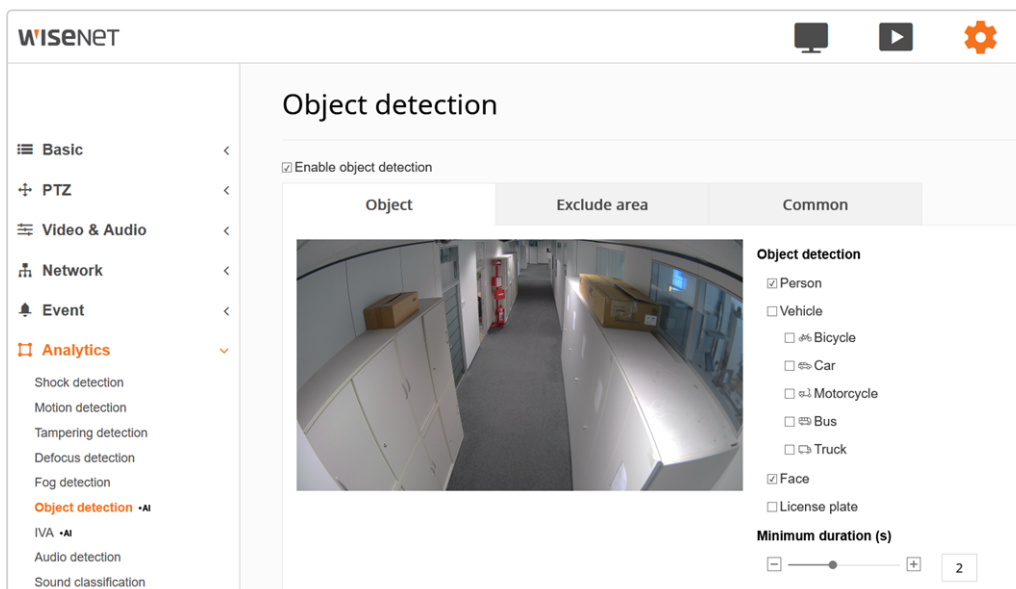
- Current system time**: A text field showing '2000-01-02 17:20:45'.
- Time zone**: A dropdown menu set to '(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna'.
- Daylight saving time**: A checked checkbox labeled 'Enable'. Below it are two text fields: 'Start time' with the value 'March.Last.Sun/02:00:00' and 'End time' with the value 'October.Last.Sun/03:00:00'.
- System time setup**: Two radio buttons, 'Manual' (selected) and 'Synchronize with NTP server'.
 - Under 'Manual', there is a 'Y - M - D' field with '2000 - 01 - 02' and an 'h : m : s' field with '17 : 20 : 05'.
 - Below that is a checkbox for 'Synchronize with PC viewer' which is unchecked, with a text field showing '2023-05-09 11:15:29'.
 - Under 'Synchronize with NTP server', there are five text fields labeled 'Address 1' through 'Address 5' with the following values: 'pool.ntp.org', 'asia.pool.ntp.org', 'europe.pool.ntp.org', 'north-america.pool.ntp.org', and 'time.nist.gov'.

At the bottom of each section, there are 'Apply' and 'Cancel' buttons.

3. Wählen Sie Ihre Zeitzone und aktivieren Sie die Option für **Sommerzeit**.
4. Aktivieren Sie im Abschnitt **Systemzeit-Setup** die Option **Mit dem NTP-Server synchronisieren**.
5. Definieren Sie die NTP-Server, die dazu verwendet werden sollten, die Kamerazeit zu synchronisieren. Metadaten und Archivmaterial werden durch den Zeitstempel synchronisiert.

Objekterkennung

1. Wählen Sie **Analytics** in den **Kameraeinstellungen** .
2. Wählen Sie **Objekterkennung**.



3. Wählen Sie **Objekterkennung aktivieren** und definieren Sie die betreffende Option auf der rechten Seite des Kamerabildes, die von der Kamera entdeckt werden sollten.

Die verfügbaren Optionen variieren je nach verwendetem Kameratyp.

Fehlerbehebung


Problem	Mögliche Ursache
In den Ergebnissen, die QogniFinder darstellt, wird kein Objekt angezeigt.	Überprüfen Sie die Systemzeit der Kamera und der Betriebssysteme, auf denen die Qognify VMS-Komponenten installiert sind. Um das genaueste Ergebnis zu erhalten, ist es wichtig, dass der gleiche Zeit-Server für die Zeitsynchronisation verwendet wird.

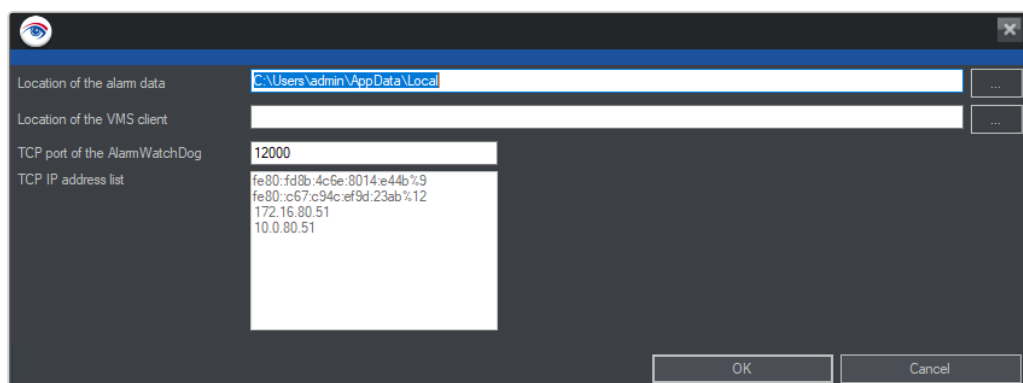
Der Alarm-WatchDog

Der Dienst Alarm-WatchDog zeigt alle Alarme auf allen mit dem Alarm-WatchDog-Server verbundenen Clients an, die als Alarm-WatchDog-Alarm definiert sind. Einrichtung und Konfiguration des Diensts werden unter „[Alarm-WatchDog konfigurieren](#)“ auf [Seite 481](#) beschrieben.

1. Starten Sie den Dienst **Alarm-WatchDog** über das Verzeichnis „Tools“ im Installationsverzeichnis.

Alarm-WatchDog konfigurieren

1. Öffnen Sie das Menü „Einstellungen“  .



2. Geben Sie den **Speicherort der Alarmdaten** an, indem Sie den Dateipfad zum Speicherverzeichnis festlegen.

Lese- und Schreibzugriff müssen aktiviert sein.

3. Geben Sie für **Speicherort (Pfad) des VMS-Clients** das Installationsverzeichnis des Clients an (z. B. C:\Programme\.).
4. Geben Sie für **TCP-Port des Alarm-WatchDog** die Portnummer an, die in der Serverkonfiguration des Alarm-WatchDog festgelegt wurde.
5. Die verfügbaren TCP-IP-Adressen des Clients werden angezeigt.
6. Wählen Sie in der **TCP-IP-Adressliste** eine IP-Adresse aus und kopieren Sie sie in die Zwischenablage.
7. Fügen Sie die IP-Adresse in den Alarm-WatchDog-Einstellungen im Menü „System“ ein (siehe „[Alarm-WatchDog konfigurieren](#)“ auf Seite 481).
8. Wählen Sie **OK**.

Alarm-WatchDog verwenden

1. Starten Sie den Dienst **Alarm-WatchDog** über das Verzeichnis „Tools“ im Installationsverzeichnis. Alle auftretenden Alarmer auf allen verbundenen Clients werden in der Liste angezeigt und zwar nach
 - Name des Alarmszenarios
 - Datum und Uhrzeit des Auftretens des Alarms
 - Name des Clients, auf dem der Alarm auftritt
 - Status des Alarms
2. Doppelklicken Sie auf den Alarm, um ihn zu öffnen. Der Client wird gestartet und eine Verbindung zum entsprechenden Server wird hergestellt.
3. Nachdem Sie auf den Alarm reagiert haben, schließen Sie den Client. Der Alarm wird im Alarm-WatchDog-Fenster als „beendet“ angezeigt.
4. Um alle beendeten Alarmer aus der Liste zu entfernen, klicken Sie auf **Beendete Alarmer entfernen**.