MAKE THE
WORLD SEE

# Milestone Systems

## XProtect® VMS 2023 R3

Bedienungsanleitung für Administratoren

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

# Inhalt

# Copyright, Marken und Verzichtserklärung



**Marken**

XProtect ist eine eingetragene Marke von Milestone Systems A/S.

Microsoft und Windows sind eingetragene Marken der Microsoft Corporation. App Store ist eine Dienstleistungsmarke von Apple Inc. Android ist eine Handelsmarke von Google Inc.

Alle anderen in diesem Dokument genannten Marken sind Marken ihrer jeweiligen Eigentümer.

**Haftungsausschluss**

Dieses Dokument dient ausschließlich zur allgemeinen Information und es wurde mit Sorgfalt erstellt.

Der Empfänger ist für jegliche durch die Nutzung dieser Informationen entstehenden Risiken verantwortlich, und kein Teil dieser Informationen darf als Garantie ausgelegt werden.

Milestone Systems A/S behält sich das Recht vor, ohne vorherige Ankündigung Änderungen vorzunehmen.

Alle Personen- und Unternehmensnamen in den Beispielen dieses Dokuments sind fiktiv. Jede Ähnlichkeit mit tatsächlichen Firmen oder Personen, ob lebend oder verstorben, ist rein zufällig und nicht beabsichtigt.

Das Produkt kann Software anderer Hersteller verwenden, für die bestimmte Bedingungen gelten können. In diesem Fall finden Sie weitere Informationen in der Datei `3rd_party_software_terms_and_conditions.txt`, die sich im Installationsordner Ihres Milestone Systems befindet.

# Übersicht

## Was ist neu?

### In Management Client 2023R3

XProtect Management Client

Azure Active Directory kann jetzt für die Authentifizierung verwendet werden. Während der Installation können Sie zwischen **Windows-Authentifizierung** und **Azure Active Directory integriert** für integrierte Sicherheit auswählen.

Weitere Informationen zur Installation von XProtect mit integrierter Sicherheit von Azure finden Sie in Systeminstallation - Benutzerdefiniert auf Seite 168.

XProtect Management Client

Eine Option (Serverzertifikat nicht vertrauen) ist jetzt für die Windows-Authentifizierung und für das integrierte Azure Active Directory verfügbar. Für das integrierte Azure Active Directory ist diese Option obligatorisch. Die Option (Serverzertifikat nicht vertrauen) sorgt dafür, dass die Serverzertifikate vor der Installation verifiziert und validiert werden.

XProtect Management Client:

Eine neue Benutzerberechtigung **Alarmeinstellungen bearbeiten** wurde für Alarme eingeführt, die Administratoren das Bearbeiten von Alarmdefinitionen, Alarmzuständen, Alarmkategorien, Alarmtönen sowie die Alarm- und Ereignisspeicherung ermöglicht. Die entsprechenden Bearbeitungsberechtigungen für Alarmdefinitionen wurden von der vorhandenen Benutzerberechtigung **Verwalten** entfernt und Administratoren benötigen die beiden Benutzerberechtigungen (**Alarmeinstellungen verwalten** und **Verwalten**) zur Verwaltung von Alarmeinstellungen.

Die neue Benutzerberechtigung **Alarmeinstellungen verwalten** wird nicht für vorhandene Benutzer übernommen und muss Benutzern, die Zugriff auf Administratorebene zur Konfiguration von Alarmen nach der Installation oder Upgrades benötigen, manuell zugewiesen werden.

Informationen zur benutzerdefinierten Installation finden Sie unter Rollen (Sicherheitsknoten) auf Seite 553

**In Management Client 2023 R2**

XProtect Management Client:

Adaptives Streaming kann jetzt für die Nutzung im Wiedergabemodus konfiguriert werden. Diese Methode wird als adaptive Wiedergabe bezeichnet. Weitere Informationen finden Sie unter Adaptive Wiedergabe (erklärt) auf Seite 249.

XProtect Management Client:

Wenn Sie die XProtect-Komponenten installieren, können Sie jetzt im Rahmen einer benutzerdefinierten Installation die Nutzung einer vorgefertigten Datenbank auswählen. Informationen zur benutzerdefinierten Installation finden Sie unter Systeminstallation - Benutzerdefiniert auf Seite 168

XProtect Management Client:

Neue Benutzerberechtigungen für die Video-Einschränkung wurden eingeführt. Diese ermöglichen den Administratoren die Konfiguration und Zuweisung von Berechtigungen zum Erstellen, Ansehen, Bearbeiten und Löschen für Benutzer. Weitere Informationen finden Sie unter Rollen (Sicherheitsknoten) auf Seite 553

**In Management Client 2023 R1**

XProtect Incident Manager:

- Zur Einhaltung der DSGVO oder anderer geltender Gesetze bezüglich personenbezogener Daten können Administratoren von XProtect Management Client nun eine Speicherzeit für Vorfallprojekte festlegen.

**In Management Client 2022 R3**

XProtect Incident Manager:

- Die XProtect Incident Manager Erweiterung ist jetzt auch kompatibel mit XProtect Expert, XProtect Professional+, und XProtect Express+ Version 2022 R3 oder höher.
- XProtect Incident Manager kann jetzt mehr als 10.000 Vorfallprojekte anzeigen.

**In Management Client 2022 R2**

XProtect Incident Manager:

- Die erste Version dieser Erweiterung.
- Die XProtect Incident Manager Erweiterung ist mit der XProtect Corporate Version 2022 R2 und neueren Versionen sowie mit XProtect Smart Client Version 2022 R2 und neueren Versionen kompatibel.

XProtect LPR:

- Die Nummernschild-Stile, die Teil der Ländermodule sind, sind jetzt an einer Stelle aufgeführt.
- Um die Verwaltung der Nummernschild-Stile zu vereinfachen, können Sie sie je nach Ihren Anforderungen an die Nummernschilderkennung in Aliasnamen gruppieren.
- Übereinstimmungslisten unterstützen jetzt auch Aliasnamen.

**In Management Client 2022 R1**

Verschlüsselung des Event Servers:

- Sie können die zweiseitige Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, verschlüsseln, , einschließlich des LPR Server.

  Weitere Informationen finden Sie unter Aktivieren Sie die Verschlüsselung auf dem Ereignisserver auf Seite 328.

Anmeldung über einen externen IDP:

- Sie können sich nun über einen externen IDP am Milestone XProtect VMS anmelden. Die Anmeldung über eine externe IDP ist eine Alternative zur Anmeldung als Active Directory- oder Basisbenutzer. Bei der Anmeldung über einen externen IDP-können Sie die Einrichtungsanforderungen eines Basisbenutzers umgehen und sind dennoch berechtigt, auf die Komponenten und Geräte in XProtect zuzugreifen.

  Weitere Informationen finden Sie unter Externer IDP (Erklärung).

Hardware-Daten aktualisieren

- Sie können jetzt die aktuelle Firmware-Version für das Hardwaregerät sehen, das vom System im Management Client erkannt wird.

  Weitere Informationen finden Sie unter Aktualisieren Sie Ihre Hardware-Daten auf Seite 375.

XProtect Management Server Failover

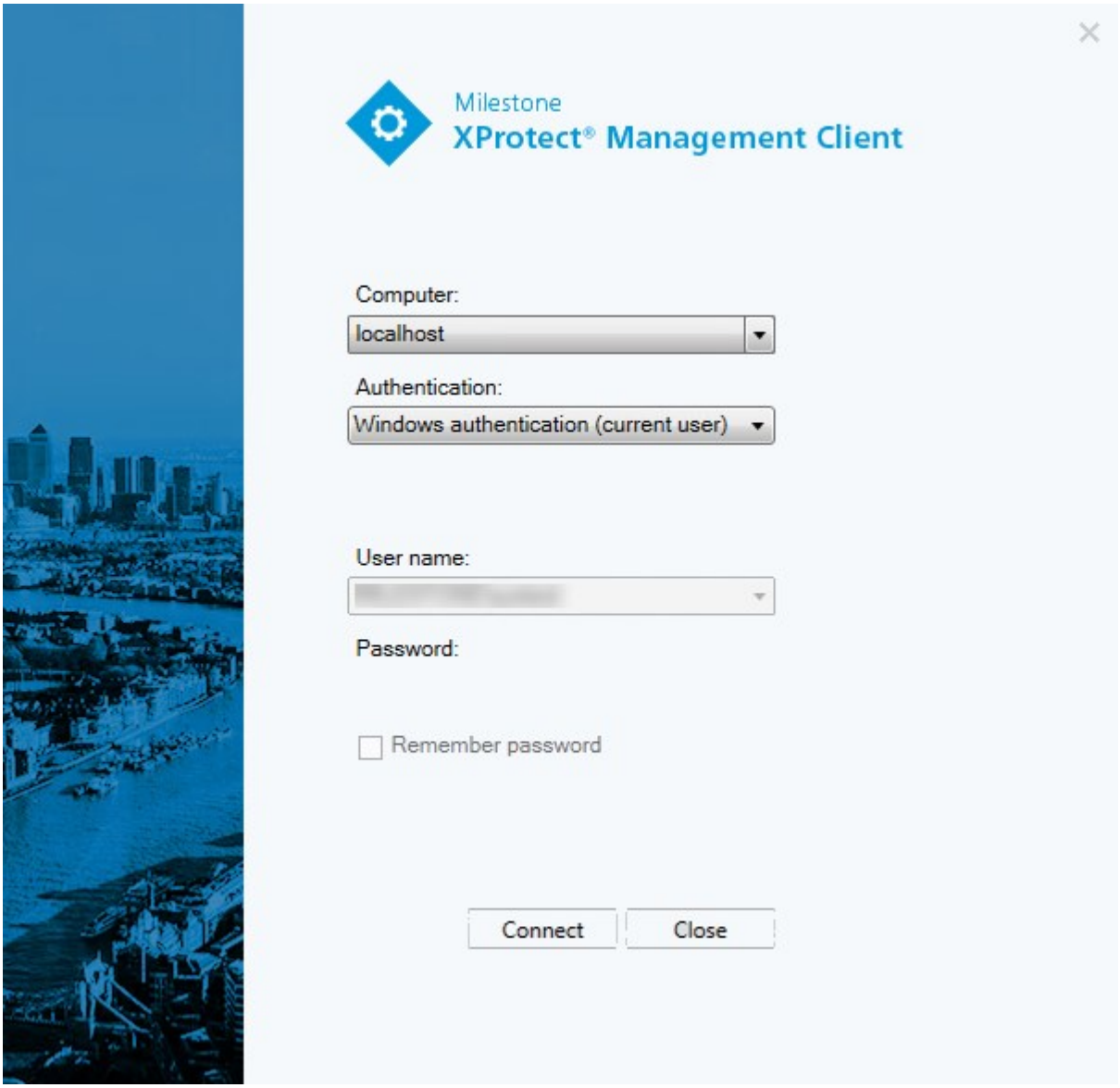
- Sie können nun eine hohe Verfügbarkeit Ihres Systems erreichen, indem Sie einen ausfallsicheren Management Server zwischen zwei redundanten Computern konfigurieren. Wenn der Computer, auf dem der Management Server läuft, ausfällt, übernimmt der zweite Computer. Die Replizierung der Daten in Echtzeit sorgt dafür, dass die Datenbanken des Management Servers, des Log-Servers und des Event Servers auf beiden Computern identisch sind.

  Weitere Informationen finden Sie unter XProtect Management Server Failover auf Seite 39.

## Anmeldung (Erklärung)

Wenn Sie den Management Client starten, müssen Sie zuerst Ihre Anmeldeinformationen eingeben, um eine Verbindung zu einem System herstellen zu können.

Mit installiertem XProtect Corporate 2016 oder XProtect Expert 2016 oder einer neueren Version können Sie sich nach der Installation eines Patches an Systemen anmelden, auf denen eine ältere Version des Produkts läuft. Die unterstützen Versionen sind XProtect Corporate 2013 und XProtect Expert 2013 oder neuer.




## Anmeldungsautorisierung (Erklärung)

Das System erlaubt Administratoren, Benutzer so einzurichten, dass sie sich nur dann bei einem System anmelden können, wenn ein zweiter Benutzer mit ausreichenden Rechten ihre Anmeldung autorisiert. In diesem Fall fragen der XProtect Smart Client oder der Management Client während der Anmeldung nach der zweiten Autorisierung.

Benutzer, die mit der integrierten Rolle **Administratoren** verknüpft sind, verfügen stets über eine Berechtigung zur Autorisierung und werden nicht um eine zweite Anmeldung gebeten, es sei denn, der Benutzer ist mit einer weiteren Rolle verknüpft, die eine zweite Anmeldung voraussetzt.

Benutzer, die sich über einen externen IDP anmelden, können nicht so eingerichtet werden, dass sie von einem zweiten Benutzer autorisiert werden müssen.

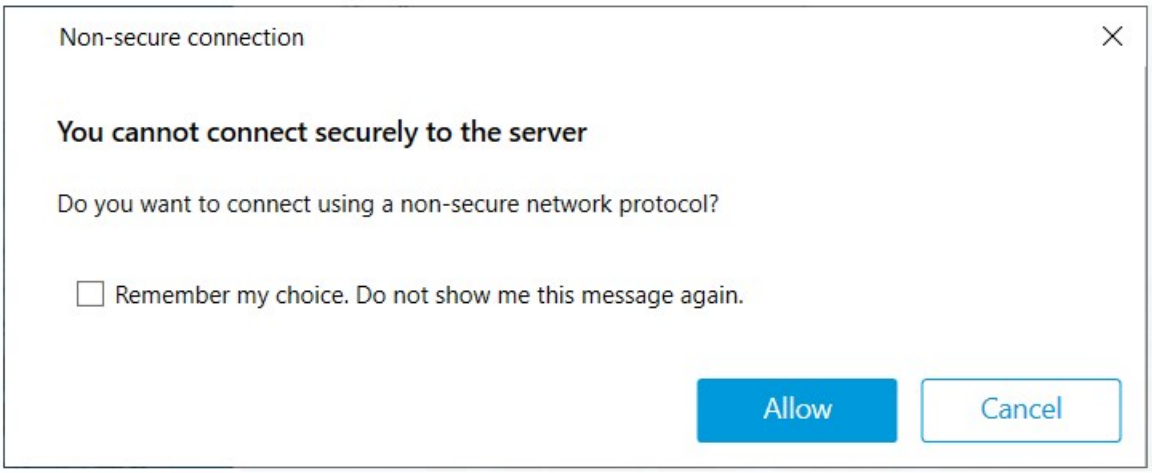
So verknüpfen Sie eine Anmeldungsautorisierung mit einer Rolle:

- Stellen Sie die **Anmeldungautorisierung**, die für die ausgewählte Rolle erforderlich ist, auf der Registerkarte **Info** (siehe Einstellungen für Rollen) unter **Rollen** so ein, dass der Benutzer bei der Anmeldung um zusätzliche Autorisierung gebeten wird.
- Stellen Sie **Benutzer autorisierten** für die ausgewählte Rolle auf der Registerkarte **Gesamtsicherheit** (siehe Einstellungen für Rollen) unter **Rollen** so ein, dass der Benutzer die Anmeldung anderer Benutzer autorisierten kann

Für einen Benutzer lassen sich beide Optionen auswählen. Das bedeutet, dass der Benutzer bei der Anmeldung nach einer zusätzlichen Autorisierung gefragt wird, er jedoch auch Anmeldungen anderer Benutzer autorisieren kann (außer seiner eigenen).

## Anmeldung über eine unsichere Verbindung

Wenn Sie sich am Management Client anmelden, werden Sie evtl. gefragt, ob Sie sich über ein unsicheres Netzwerkprotokoll anmelden möchten.




- Klicken Sie auf **Zulassen**, um die Benachrichtigung zu ignorieren und sich anzumelden. Um diese Benachrichtigung in Zukunft nicht mehr angezeigt zu bekommen, wählen Sie entweder **Meine Auswahl speichern. Diese Meldung nicht mehr anzeigen,** oder klicken Sie auf **Extras** > **Optionen** und wählen Sie dann **Nicht sichere Verbindung zum Server zulassen (Neustart des Management Client erforderlich)**.

Informationen zur sicheren Kommunikation finden Sie unter Sichere Kommunikation (Erklärung) auf Seite 155.

## Ändern Ihres Basisnutzer-Passwortes

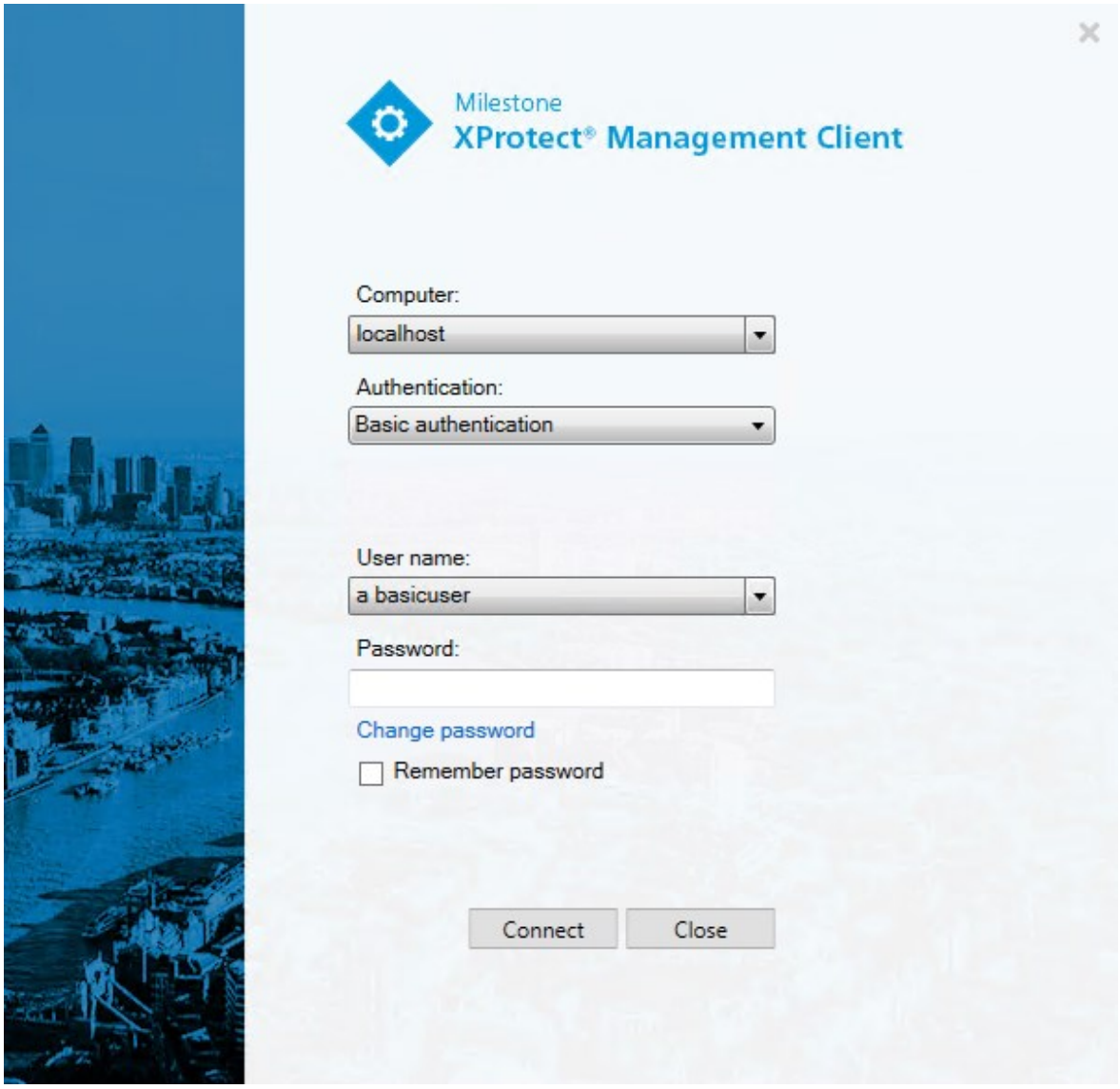
Wenn Sie sich als **Basisnutzer** anmelden, können Sie Ihr Passwort ändern. Wenn Sie eine andere Authentifizierungsmethode wählen, kann nur Ihr Systemadministrator Ihr Passwort ändern. Wenn Sie Ihr Passwort ändern, erhöht dies oft die Sicherheit Ihres XProtect VMS-Systems.

**Voraussetzungen**

Die Version Ihres XProtect VMS-Systems muss 2021 R1 oder später sein.

Schritte:

1. Starten Sie Management Client. Das Anmeldefenster wird geöffnet.
2. Geben Sie Ihre Anmeldeinformationen ein. Wählen Sie aus der Liste **Authentifizierung** **Basisauthentifizierung** aus. Ein Link mit dem Text **Passwort ändern** erscheint.




3. Klicken Sie auf das Link. Ein Browserfenster wird geöffnet.
4. Folgen Sie den Anweisungen und speichern Sie Ihre Änderungen.
5. Sie können sich nun mit Ihrem neuen Passwort bei Management Client anmelden.

## Produktübersicht

Die XProtect VMS-Produkte sind Videomanagementsoftware für Installationen jeder Art und Größe. Ganz gleich, ob Sie Ihr Geschäft vor Vandalismus schützen oder eine Hochsicherheitsinstallation mit mehreren Standorten verwalten möchten – XProtect macht es möglich. Die Lösungen bieten eine zentralisierte

Verwaltung aller Geräte, Server und Benutzer und stellen ein äußerst flexibles Regelsystem bereit, das von Zeitplänen und Ereignissen gesteuert wird.

Ihr System umfasst folgende Hauptkomponenten:

- Den **Management-Server** – das Zentrum Ihrer Installation, das aus mehreren Servern besteht
- Einen oder mehrere **Aufzeichnungsserver**
- Eine oder mehrere Installationen von **XProtect Management Client**
- **XProtect Download Manager**
- Eine oder mehrere Installationen von **XProtect® Smart Client**
- Eine oder mehrere Verwendungen von **XProtect Web Client** und/oder Installationen des **XProtect Mobile** Clients, falls erforderlich

Das System umfasst zudem die vollintegrierte Matrix-Funktionalität für die dezentrale Anzeige von Videos einer beliebigen Kamera in Ihrem Überwachungssystem auf einem Computer, auf dem XProtect Smart Client installiert ist.

Sie können Ihr System in einer verteilten Einrichtung auf virtualisierten Servern oder auf mehreren physischen Servern installieren. Siehe auch Einrichtung eines verteilten Systems auf Seite 94.

Darüber hinaus bietet das System die Möglichkeit, beim Exportieren von Videobeweisbildern vom XProtect® Smart Client – Player die Standalone-Lösung XProtect Smart Client mit einzubeziehen. XProtect Smart Client – Player ermöglicht es den Empfängern von Videobeweisbildern (z. B. Polizeibeamte, interne oder externe Ermittler usw.), die exportierten Aufzeichnungen zu durchsuchen und wiederzugeben, ohne Software auf ihrem Computer zu installieren.

Wenn Sie die umfassendsten Produkte installiert haben (siehe Produktvergleich auf Seite 120), kann Ihr System mit unbegrenzt vielen Kameras, Servern und Benutzern umgehen, und dies wenn nötig über mehrere Standorte hinweg. Das System unterstützt sowohl IPv4 als auch IPv6.

# Systemkomponenten

## Management-Server (Erklärung)

Der Management-Server ist die zentrale Komponente des VMS-Systems. Er speichert die Konfiguration des Überwachungssystems in einer SQL Server-Datenbank, entweder auf einem SQL Server auf dem Computer des Management-Servers selbst oder auf einem eigenen SQL Server im Netzwerk. Außerdem verwaltet es die Benutzerauthentifizierung, die Benutzerberechtigungen, das Regelsystem uvm. Zur Verbesserung der Systemleistung können Sie mehrere Management-Server als Milestone Federated Architecture™ ausführen. Der Management-Server wird als Dienst ausgeführt und wird üblicherweise auf einem eigenen Server installiert.

Benutzer stellen für die anfängliche Authentifizierung eine Verbindung zum Management-Server und anschließend – für Zugriff auf Videoaufzeichnungen usw. – eine transparente Verbindung zu den Aufzeichnungsservern her.

## SQL Server Installationen und Datenbanken (Erklärung)

Der Management-Server, der Event-Server und der Log-Server speichern z.B. die Systemkonfiguration, Alarme Ereignisse und Protokollmeldungen in SQL Server-Datenbanken auf einer oder mehreren SQL Server-Installationen. Der Management Server und der Event Server nutzen dieselbe SQL Server-Datenbank, während der Log Server , XProtect Incident Manager, und die Identity Provider jeweils ihre eigene SQL Server Datenbank haben. Weitere Informationen zum Identity Provider finden Sie im Identity Provider (Erklärung) auf Seite 68. Weitere Informationen über die XProtect Incident Manager Datenbank und die Protokollierung finden Sie im separaten Administratorhandbuch für XProtect Incident Manager.

Der Systeminstaller enthält Microsoft SQL Server Express, eine kostenlose Ausgabe von SQL Server.

Für sehr große Systeme, oder für Systeme mit vielen Transaktionen zu und von den SQL Server-Datenbanken, empfiehlt Milestone Ihnen, die Microsoft® SQL Server® Standard oder Microsoft® SQL Server® Enterprise-Ausgabe von SQL Server auf einem eigenen Computer im Netzwerk und auf einem bestimmten Festplattenlaufwerk zu verwenden, das für keine anderen Zwecke verwendet wird. Die Installation von SQL Server auf einem eigenen Laufwerk verbessert die Leistung des gesamten Systems.

## Aufzeichnungsserver (Erklärung)

Der Aufzeichnungsserver ist für die Kommunikation mit den Netzwerkkameras und Videoencodern, die Aufzeichnung der abgerufenen Audio- und Videoinhalte sowie die Bereitstellung von Client-Zugriff auf Live- basierte und aufgezeichnete Audio- und Videoinhalte verantwortlich. Außerdem sorgt der Aufzeichnungsserver für die Kommunikation mit anderen Milestone-Produkten mittels der Milestone Interconnect-Technologie.

**Gerätetreiber**

- Netzwerkkameras und Videoencodern kommunizieren über einen Gerätetreiber, der speziell für einzelne Geräte oder eine Serie ähnlicher Geräte des gleichen Herstellers entwickelt wurde.
- Ab der Ausgabe 2018 R1 sind die Gerätetreiber in zwei Gerätepacks aufgeteilt: das reguläre Gerätepaket mit neueren Treibern und ein Stamm-Gerätepaket mit älteren Treibern
- Das reguläre Gerätepaket wird automatisch installiert, wenn Sie den Aufzeichnungsserver installieren. Später können Sie die Treiber aktualisieren, indem Sie eine neuere Version des Gerätepakets herunterladen und installieren
- Das Stammgerätepaket kann nur installiert werden, wenn ein reguläres Gerätepaket im System installiert ist. Die Treiber aus dem Stammgerätepaket werden automatisch installiert, wenn eine vorige Version bereits auf Ihrem System installiert ist. Sie steht auf der Software-Download-Seite (https://www.milestonesys.com/downloads/) zum manuellen Herunterladen und Installieren zur Verfügung.

**Mediendatenbank**

- Die abgerufenen Audio- und Videodaten werden vom Recording-Server in der maßgeschneiderten Hochleistungs-Mediendatenbank gespeichert, die für das Aufzeichnen und Speichern von Audio- und Videodaten optimiert ist.

- Die Mediendatenbank unterstützt verschiedene einzigartige Funktionen wie abgestufte mehrstufige Archivierung, Videoausdünnung, Verschlüsselung und das Hinzufügen einer digitalen Signatur zu den Aufzeichnungen.

Das System verwendet Aufzeichnungsserver zum aufnehmen von Videofeeds und für die Kommunikation mit Kameras und anderen Geräten. Ein Überwachungssystem besteht typischerweise aus mehreren Aufzeichnungsservern.

Aufzeichnungsserver sind Computer, auf denen Sie die Software Recording Server installiert und sie so konfiguriert haben, dass sie mit dem Management-Server kommuniziert. Aufzeichnungsserver werden im Bereich **Übersicht** angezeigt, wenn Sie den **Server**-Ordner ausklappen und dann **Aufzeichnungsserver** auswählen.


Abwärtskompatibilität mit Aufzeichnungsservern älterer Versionen als diese Version des Management-Servers sind eingeschränkt. Sie können mit älteren Versionen immer noch auf Aufzeichnungen der Aufzeichnungsserver zugreifen, allerdings muss für eine Änderung der Konfiguration die Version mit der des Management-Servers übereinstimmen. Milestone empfiehlt, dass Sie die Versionen aller Aufzeichnungsserver in Ihrem System mit denen Ihres Management-Servers abgleichen.

Der Aufzeichnungsserver unterstützt die Verschlüsselung der Datenstreams zu den Clients und Diensten:

- Verschlüsselung zu Clients und Servern aktivieren auf Seite 330
- Verschlüsselungsstatus an Clients anzeigen auf Seite 313

Der Aufzeichnungsserver unterstützt außerdem die Verschlüsselung der Verbindung mit dem Management Server:

- Die Verschlüsselung zum und vom Managementserver aktivieren auf Seite 324

Sie haben mehrere Optionen bei der Verwaltung Ihres Aufzeichnungsservers:

- Hardware hinzufügen auf Seite 229
- Hardware verschieben auf Seite 368
- Löschen sämtlicher Hardware auf einem Aufzeichnungsserver auf Seite 388
- Deinstallieren eines Aufzeichnungsservers auf Seite 388

Wenn der Recording Server-Dienst ausgeführt wird, ist es äußerst wichtig, dass weder der Windows Explorer noch andere Programme auf Mediendatenbank-Ordner oder -Dateien zugreifen, die Ihrer Systemkonfiguration zugewiesen sind. Wenn sie es dennoch tun, ist es wahrscheinlich, dass der Aufzeichnungsserver wichtige Mediendaten nicht umbenennen oder verschieben kann. Dies könnte den Aufzeichnungsserver stoppen. Um einen gestoppten Aufzeichnungsserver neu zu starten, halten Sie den Recording Server-Dienst an, schließen Sie das Programm, das auf die Mediendaten oder Ordner zugreift und starten Sie den Recording Server-Dienst neu.

## Mobilserver (Erklärung)

Der mobile Server sorgt dafür, dass XProtect Mobile-Client und XProtect Web Client-Benutzer Zugriff auf das System erhalten.

Der mobile Server dient nicht nur als System-Gateway für die beiden Clients, sondern kann auch Video transcodieren, da der ursprüngliche Videostream einer Kamera für die Bandbreite, die Client-Benutzern zur Verfügung steht, oft zu groß ist.

Wenn Sie eine **Verteilte** oder **Benutzerdefinierte** Installation vornehmen, empfiehlt Milestone die Installation des mobilen Servers auf einem eigenen Server.

## Event Server (Erklärung)

Der Event Server kümmert sich um verschiedene Aufgaben im Hinblick auf Ereignisse, Alarme und Karten , und vielleicht auch um Drittintegrationen über den MIP SDK.

**Ereignisse**

- Alle Systemereignisse werden auf einem Event-Server konsolidiert, sodass Partner Integrationen zur Nutzung von Systemereignissen an einem Ort und über eine Schnittstelle vornehmen können
- Zudem ermöglicht der Event-Server Dritten über die Schnittstellen für generische Ereignisse oder Analyseereignisse das Senden von Ereignissen an das System

**Alarme**

- Der Event-Server hostet die Alarmfunktion, Alarmlogik und den Alarmstatus und verwaltet die Alarmdatenbank. Die Alarmdatenbank wird in derselben SQL Server-Datenbank gespeichert, der auch vom Management-Server verwendet wird

**Meldungen**

- Die Kommunikation mit Meldungen wird vom Event Server gehandhabt und erlaubt Plug-ins das Senden von Meldungen in Echtzeit zwischen Umgebungen, zum Beispiel XProtect Smart Client, Management Client, Event Server und eigenständigen Diensten.

**Karten**

- Zudem hostet der Event-Server jene Karten, die im XProtect Smart Client konfiguriert und verwendet werden

**MIP SDK**

- Abschließend können auf dem Event-Server Plug-ins von Dritten installiert werden und Zugriff auf Systemereignisse erhalten

## Log-Server (Erklärung)

Der Log-Server speichert alle Protokollnachrichten für das gesamte System in einer SQL Server-Datenbank. Diese Datenbank für Protokollmeldungen kann auf demselben SQL Server vorhanden sein wie die Datenbank für die Management-Server Systemkonfiguration oder auf separaten SQL Server. Der Log-Server ist typischerweise auf dem selben Server installiert wie der Management-Server, kann jedoch auch auf einem separaten Server installiert sein, um die Leistung des Management- oder Log-Servers zu erhöhen.

## API Gateway (Erklärung)

Die MIP VMS API bietet eine einheitliche RESTful-API an, die auf Industriestandardprotokollen wie OpenAPI basiert, um auf XProtect VMS-Funktionen zuzugreifen, Integrationsprojekte zu vereinfachen und als Grundlage für die Kommunikation mit der Cloud zu dienen.

Der XProtect VMS API Gateway unterstützt diese Integrationsoptionen durch die Milestone Integration Platform VMS API (MIP VMS API).

Der API Gateway wird vor Ort installiert und soll als Front-End und gemeinsamer Einstiegspunkt für RESTful-API- und WebSocket Messaging API-Dienste auf allen aktuellen VMS-Serverkomponenten (Management-Server, Event Server, Aufzeichnungsserver, Log-Server usw.) dienen. Ein API Gateway-Dienst kann auf demselben Host installiert werden wie der Management-Server, oder separat, und es können mehrere davon installiert werden (jeder auf seinem eigenen Host).

Die RESTful-API wird zum Teil von jeder bestimmten VMS-Serverkomponente implementiert, und die API Gateway kann diese Anfragen und Antworten einfach durchreichen, während bei anderen Anfragen die API Gateway die Anfragen und Antworten entsprechend umwandelt.

Derzeit steht die Konfigurations-API, die vom Management-Server gehostet wird, als RESTful-API zur Verfügung. Die RESTful Events API, Websockets Messaging API und RESTful Alarms API sind gehostet vom Event Server ebenfalls verfügbar.

Weitere Informationen finden Sie im API Gateway Administratorhandbuch und in der Milestone Integration Platform VMS API Referenzdokumentation.

# Failover

## XProtect Management Server Failover

Wenn ein eigenständiger Computer, auf dem der Dienst Management Server oder SQL Server ausgeführt werden, einen Hardwarefehler aufweist, hat dies keine Auswirkungen auf die Aufzeichnungen oder den Aufzeichnungsserver. Solche Hardwareausfälle können jedoch zu Ausfallzeiten für Anwender und Administratoren führen, die nicht bei den Clients angemeldet sind.

XProtect Management Server Failover bietet hohe Verfügbarkeit und Notfallwiederherstellung für den Management-Server. Wenn der Management-Server auf einem Computer nicht mehr erreichbar ist, übernimmt der andere Computer den Betrieb der Systemkomponenten.

Sie können die sichere Echtzeitreplikation der SQL Server Datenbanken nutzen, um sicherzustellen, dass es im Fall von Hardware-Ausfällen nicht zu Datenverlust kommt.

XProtect Management Server Failover kann Ihnen dabei helfen, Systemausfallzeiten zu minimieren. Sie profitieren von einem Failover Cluster, wenn:

- Ein Server ausfällt – Sie können den Management Server-Dienst und SQL Server von einem anderen Computer aus ausführen, während Sie die Probleme beheben.
- Sie System-Updates und Sicherheits-Patches implementieren müssen – Die Anwendung von Sicherheits-Patches auf einem eigenständigen Management-Server kann zeitaufwändig sein und zu längeren Ausfallzeiten führen. Mit einer Failover Cluster können Sie System-Updates und Sicherheits-Patches mit minimalen Ausfallzeiten anwenden.
- Wenn Sie eine ungestörte Verbindung benötigen – Benutzer erhalten ständigen Zugriff auf Live- und Wiedergabevideos sowie auf die Konfiguration des Systems.

Wenn Sie XProtect Management Server Failover zwischen zwei Computern konfigurieren. Damit die Ausfallsicherung funktioniert, müssen Sie die Software auf jedem Computer installieren:

- XProtect Management Server
- XProtect Event Server-Dienst
- XProtect Log Server-Dienst
- Microsoft SQL Server (empfohlen)

## Failover-Management-Server (Erklärung)

Failover-Unterstützung auf dem Management-Server wird durch das Installieren des Management-Servers in einem Microsoft Windows Cluster erreicht. Der Cluster sorgt dafür, dass ein anderer Server die Management-Server-Funktion übernimmt, falls der erste Server ausfällt.

## Der ausfallsichere Aufzeichnugnsserver (Erklärung)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Ein Failover-Aufzeichnungsserver ist ein zusätzlicher Aufzeichnungsserver, der die Arbeit des eigentlichen Aufzeichnungsservers übernimmt, falls dieser nicht mehr verfügbar ist. Sie können einen Failover-Aufzeichnungsserver in zwei Modi konfigurieren, als **Cold-Standby-Server** oder als **Hot-Standby-Server**.

Sie installieren ausfallsichere Aufzeichnungsserver wie Standard-Aufzeichnungsserver (siehe Installation eines Failover-Aufzeichnungsservers Download Manager auf Seite 181). Sobald Sie Failover-Aufzeichnungsserver installiert haben, werden diese im Management Client angezeigt. Milestone empfiehlt die Installation aller Failover-Aufzeichnungsserver auf separaten Computern. Achten Sie darauf, dass sie Failover-Aufzeichnungsserver mit der korrekten IP-Adresse/dem korrekten Hostnamen des Management-Servers konfigurieren. Die Benutzerberechtigungen für das Benutzerkonto, unter dem der Failover-Server-Dienst ausgeführt wird, werden bei der Installation gegeben. Dies sind:

- Start-/Stopp- Berechtigungen zu starten oder stoppen des ausfallsicheren Aufzeichnungsservers
- Lesende und schreibende Zutrittsberechtigung zum Lesen und Schreiben in der Datei RecorderConfig.xml

Wird für die Verschlüsselung ein Zertifikat ausgewählt, so muss der Administrator dem Benutzer auf dem ausgewählten Zertifikate-Privatschlüssel des Failover-Servers die Lesezugriffsberechtigung geben.

Wenn der Failover-Aufzeichnungsserver von einem Aufzeichnungsserver übernimmt, der eine Verschlüsselung verwendet, so empfiehlt Milestone, dass Sie den Failover-Aufzeichnungsserver ebenfalls dafür vorbereiten, dass er eine Verschlüsselung verwendet. Weitere Informationen finden Sie unter Sichere Kommunikation (Erklärung) auf Seite 155 und Installation eines Failover-Aufzeichnungsservers Download Manager auf Seite 181.

Sie können bestimmen, welche Art von Failover-Unterstützung Sie auf Geräteebene möchten. Für jedes Gerät auf einem Aufzeichnungsserver können Sie vollständige, teilweise oder keine Failover-Unterstützung auswählen. So können Sie Ihren Failover-Ressourcen Prioritäten zuweisen und Failover beispielsweise nur für Video- und nicht für Audiokanäle einrichten oder Failover nur auf wichtigen Kameras haben.

Während ihr System im Failover-Modus ist, können Sie keine Hardware ersetzen oder umziehen, den Aufzeichnungsserver aktualisieren oder Gerätekonfigurationen ändern, wie zum Beispiel Speicherungseinstellungen oder Einstellungen für Videostreams.

### Cold-Standby-Failover-Aufzeichnungsserver

Bei einem Cold-Standby-Failover-Aufzeichnungsserver gruppieren Sie mehrere Failover-Aufzeichnungsserver in einer Failover-Gruppe. Die gesamte Failover-Gruppe dient dem Zweck, mehrere vorab ausgewählte Aufzeichnungsserver abzulösen, wenn einer von ihnen nicht mehr verfügbar sein sollte. Sie können so viele Gruppen erstellen, wie Sie wollen (siehe Gruppieren von Failover-Aufzeichnungsservern für Cold-Standby auf Seite 227).

Gruppen haben einen klaren Vorteil: Wenn Sie später bestimmen, welche Failover-Aufzeichnungsserver einen Aufzeichnungsserver ablösen sollen, wählen Sie einfach eine Gruppe von Failover-Aufzeichnungsservern aus. Falls die ausgewählte Gruppe aus mehr als einem Failover-Aufzeichnungsserver besteht, haben Sie zur Sicherheit mehr als einen Failover-Aufzeichnungsserver zur Ablösung in Bereitschaft, falls ein Aufzeichnungsserver nicht mehr verfügbar sein sollte. Sie können eine sekundäre Failover-Server-Gruppe bestimmen, welche die Aufgaben der primären Gruppe übernimmt, sollten alle Aufzeichnungsserver der primären Gruppe ausgelastet sein. Ein Failover-Aufzeichnungsserver kann nicht Teil mehrerer Gruppen sein.

Failover-Aufzeichnungsserver in einer Failover-Gruppe sind in einer Sequenz angeordnet. Die Sequenz bestimmt die Reihenfolge, in der die Failover-Aufzeichnungsserver einen Aufzeichnungsserver ablösen. Standardmäßig entspricht die Sequenz der Reihenfolge, in der Sie die Failover-Aufzeichnungsserver in die Failover-Gruppe aufgenommen haben: Der zuerst aufgenommene Server ist der erste in der Sequenz. Bei Bedarf können Sie dies ändern.

### Hot-Standby-Failover-Aufzeichnungsserver

Bei einem Hot-Standby-Failover-Aufzeichnungsserver bestimmen Sie einen Failover-Aufzeichnungsserver, der nur **einen** Aufzeichnungsserver ablöst. So kann das System diesen Failover-Aufzeichnungsserver im „Standby"-Modus behalten, sodass er mit der korrekten/aktuellen Konfiguration des ihm zugewiesenen Aufzeichnungsservers synchronisiert wird und viel schneller zur Ablösung bereit ist als ein Cold-Standby-Failover-Aufzeichnungsserver. Wie bereits erwähnt, weisen Sie Hot-Standby-Server nur einem Aufzeichnungsserver zu und können sie nicht gruppieren. Sie können Failover-Server, die bereits Teil einer Failover-Gruppe sind, nicht zu Hot-Standby-Aufzeichnungsservern machen.

**Validierung ausfallsicherer Aufzeichnungsserver**

Um zusammengeführte Videodaten vom ausfallsicheren Server auf dem Aufzeichnungsserver zu validlieren müssen Sie dafür sorgen, dass der Aufzeichnungsserver nicht erreichbar ist, indem Sie entweder den Aufzeichnungsserverdienst anhalten oder den Computer abschalten, auf dem der Aufzeichnungsserver installiert ist.

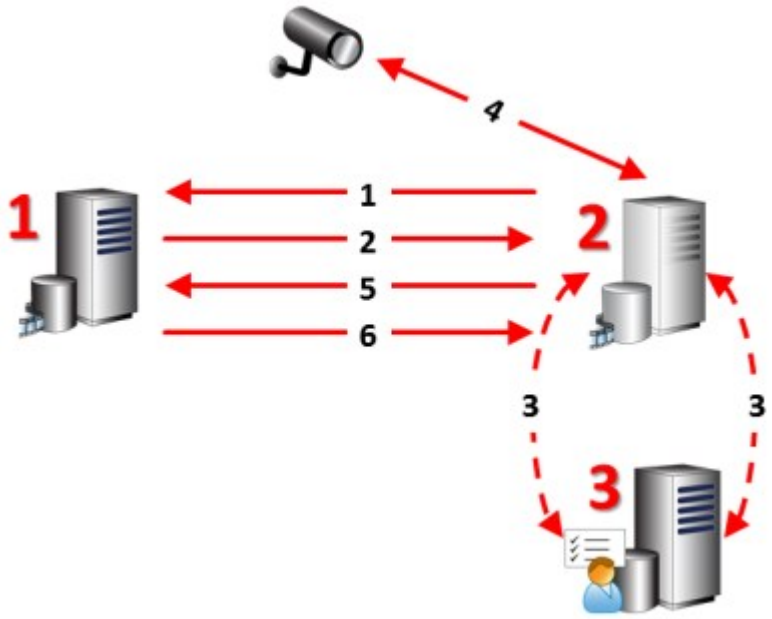
> Eine manuelle Unterbrechung des Netzwerks, die Sie dadurch verursachen können, dass Sie das Netzwerkkabel abziehen oder das Netzwerk mit einem Prüfwerkzeug blockieren, ist keine gültige Methode.

### Die Funktionalität der Failover-Aufzeichnungsserver (Erklärung)

- Ein Failover-Aufzeichnungsserver überprüft den Status relevanter Aufzeichnungsserver alle 0,5 Sekunden. Falls ein Aufzeichnungsserver 2 Sekunden lang nicht reagiert, wird er als nicht verfügbar eingestuft und der Failover-Aufzeichnungsserver übernimmt
- Ein Cold-Standby-Failover-Aufzeichnungsserver übernimmt die Aufzeichnung für den nicht mehr verfügbaren Server nach fünf Sekunden sowie dem Zeitraum, in dem der Recording Server-Dienst des Failover-Aufzeichnungsservers startet und in dem die Verbindung zu den Kameras aufgebaut wird. Ein Hot-Standby-Failover-Aufzeichnungsserver hingegen übernimmt schneller, da der Recording Server-Dienst bereits über die korrekte Konfiguration verfügt und nur die Kameras starten muss, um Feeds zu liefern. Während des Systemstarts können Sie weder Aufzeichnungen speichern noch Live-Video von betroffenen Kameras sehen
- Sobald ein Aufzeichnungsserver wieder verfügbar ist, übernimmt er automatisch für den Failover-Aufzeichnungsserver. Vom Failover-Aufzeichnungsserver gespeicherte Aufzeichnungen werden automatisch in den Datenbanken des Standard-Aufzeichnungsservers zusammengeführt. Die Dauer dieses Vorgangs hängt von der Aufzeichnungsmenge, Netzwerkkapazität und weiteren Faktoren ab. Während der Zusammenführung können Sie keine Aufzeichnungen aus dem Zeitraum der Übernahme durch den Failover-Aufzeichnungsserver einsehen
- Wenn ein Failover-Aufzeichnungsserver beim Zusammenführen während der Einrichtung eines Cold-Standby-Failover-Aufzeichnungsservers die Aufgabe eines anderen Aufzeichnungsservers übernehmen muss, verschiebt er den Zusammenführungsprozess mit Aufzeichnungsserver A und übernimmt die Aufgabe von Aufzeichnungsserver B. Wenn Aufzeichnungsserver B wieder verfügbar ist, nimmt der Failover-Aufzeichnungsserver den Zusammenführungsprozess wieder auf, so dass sowohl Aufzeichnungsserver A als auch Aufzeichnungsserver B gleichzeitig Aufnahmen zusammenzuführen können.
- In einer Hot-Standby-Konfiguration kann ein Hot-Standby-Server nicht für einen zusätzlichen Aufzeichnungsserver übernehmen, da er nur Hot Standby für einen einzigen Aufzeichnungsserver sein kann. Fällt dieser Aufzeichnungsserver jedoch wieder aus, übernimmt der Hot-Standby-Server abermals und behält die zuvor gemachten Aufzeichnungen. Der Aufzeichnungsserver behält Aufzeichnungen, bis sie wieder im primären Recorder zusammengeführt werden oder dem Failover-Aufzeichnungsserver kein Festplattenspeicher mehr zur Verfügung steht

- Eine Failover-Lösung bietet keine vollständige Redundanz. Sie ist nur eine zuverlässige Methode, um Ausfallzeiten zu minimieren. Wenn ein Aufzeichnungsserver wieder verfügbar ist, stellt der Failover Server-Dienst sicher, dass der Aufzeichnungsserver wieder Aufzeichnungen speichern kann. Erst dann ist der eigentliche Aufzeichnungsserver wieder für die Speicherung von Aufzeichnungen zuständig. Daher ist ein Aufzeichnungsverlust in diesem Teil des Prozesses sehr unwahrscheinlich
- Für Clientbenutzer ist die Ablösung durch den Failover-Aufzeichnungsserver fast unmerklich. Eine kurze Pause tritt auf, die meistens nur ein paar Sekunden dauert, wenn der Failover-Aufzeichnungsserver übernimmt. Während dieser Pause können Benutzer nicht auf Videoaufnahmen des betroffenen Aufzeichnungsservers zugreifen. Clientbenutzer können wieder Live-Video ansehen, sobald der Failover-Aufzeichnungsserver übernommen hat. Da neue Aufzeichnungen auf dem Failover-Aufzeichnungsserver gespeichert werden, können Sie Aufzeichnungen aus der Zeit abspielen, nachdem der Failover-Aufzeichnungsserver übernommen hat. Clients können keine älteren, nur auf dem betroffenen Aufzeichnungsserver gespeicherten Aufzeichnungen abspielen, bis dieser Aufzeichnungsserver wieder funktioniert und für den Failover-Aufzeichnungsserver übernommen hat. Sie haben keinen Zugriff auf archivierte Aufzeichnungen. Wenn der Aufzeichnungsserver wieder funktioniert, findet eine Zusammenführung statt, bei der die Failover-Aufzeichnungen wieder mit der Datenbank des Aufzeichnungsservers zusammengeführt werden. Während dieses Vorgangs können Sie keine Aufzeichnungen aus dem Zeitraum abspielen, in dem der Failover-Aufzeichnungsserver übernommen hat
- In einer Cold-Standby-Konfiguration ist es nicht notwendig, einen Failover-Aufzeichnungsserver als Backup für einen anderen Failover-Aufzeichnungsserver einzurichten. Dies liegt daran, dass Sie Failover-Gruppen und keine bestimmten Failover-Aufzeichnungsserver für die Ablösung bestimmter Aufzeichnungsservers zuweisen. Eine Failover-Gruppe muss mindestens einen Failover-Aufzeichnungsserver enthalten, doch Sie können so viele wie notwendig hinzufügen. Falls eine Failover-Gruppe mehr als einen Failover-Aufzeichnungsserver enthält, steht mehr als ein Failover-Aufzeichnungsserver zur Ablösung bereit.
- In einer Hot-Standby-Konfiguration können Sie keine Failover-Aufzeichnungsserver oder Hot-Standby-Server als Failover für einen Hot-Standby-Server einrichten

Failover-Schritte (Erklärung)




| Beschreibung |
| --- |
| Beteiligte Server (Zahlen in rot):<br>1. Recording Server<br>2. Failover Recording Server<br>3. Management Server |
| Failover-Schritte für **Cold-Standby**:<br>1. Um zu prüfen, ob er läuft oder nicht, steht ein Failover-Server in ständiger TCP-Verbindung mit einem Aufzeichnungsserver.<br>2. Diese Verbindung wird unterbrochen.<br>3. Der Failover-Aufzeichnungsserver erfragt die aktuelle Konfiguration des Aufzeichnungsservers vom Management-Server. Der Management-Server sendet die angefragte Konfiguration, der Failover-Aufzeichnungsserver erhält sie, startet und beginnt dann anstelle des Aufzeichnungsservers aufzuzeichnen.<br>4. Der Failover-Aufzeichnungsserver und die relevante(n) Kamera(s) tauschen Videodaten aus. |

| Beschreibung |
| --- |
| 5. Der Failover-Aufzeichnungsserver versucht kontinuierlich, die Verbindung mit dem Aufzeichnungsserver wiederherzustellen.<br>6. Wenn die Verbindung zum Aufzeichnungsserver wiederhergestellt ist, fährt der Failover-Aufzeichnungsserver herunter, und der Aufzeichnungsserver holt ggf. die während seiner Ausfallzeit aufgezeichneten Videodaten und die Videodaten werden in der Datenbank des Aufzeichnungsservers wieder zusammengeführt. |
| Failover-Schritte für **Hot-Standby**:<br>1. Um zu prüfen, ob er läuft oder nicht, steht ein Hot-Standby-Server in ständiger TCP-Verbindung mit dem zugewiesenen Aufzeichnungsserver.<br>2. Diese Verbindung wird unterbrochen.<br>3. Der Hot-Standby-Server kennt die aktuelle Konfiguration des zugewiesenen Aufzeichnungsservers bereits und beginnt an seiner Stelle aufzuzeichnen.<br>4. Der Hot-Standby-Server und die relevante(n) Kamera(s) tauschen Videodaten aus.<br>5. Der Hot-Standby-Server versucht kontinuierlich, die Verbindung mit dem Aufzeichnungsserver wiederherzustellen.<br>6. Wenn die Verbindung zum Aufzeichnungsserver wiederhergestellt wurde, kehrt der Hot-Standby-Server in den Hot-Standby-Modus zurück und der Aufzeichnungsserver erhält (ggf.) Videodaten, die während der Ausfallzeit aufgenommen wurden. Diese werden in seiner Datenbank zusammengeführt. |

## Failover-Aufzeichnugnsserver-Dienst (Erklärung)

Ein Failover-Aufzeichnungsserver verfügt über zwei installierte Dienste:

- Ein Failover Server-Dienst, der die Abläufe für die Übernahme vom Aufzeichnungsserver übernimmt. Dieser Dienst ist immer aktiv und überprüft konstant den Status relevanter Aufzeichnungsserver
- Ein Failover Recording Server-Dienst, durch den der Failover-Aufzeichnungsserver als Aufzeichnungsserver agieren kann.

  In einer Cold-Standby-Konstellation wird dieser nur bei Bedarf gestartet, wenn also der Cold-Standby-Failover-Aufzeichnungsserver den Aufzeichnungsserver ablöst. Das Starten dieses Dienstes dauert in der Regel ein paar Sekunden, kann aber länger dauern, je nach lokalen Sicherheitseinstellungen usw. In einer Hot-Standby-Einrichtung. Dieser Dienst läuft immer, sodass der Hot-Standby-Server schneller übernimmt als der Cold-Standby-Failover-Aufzeichnungsserver.

# Clients

## Management Client (Erklärung)

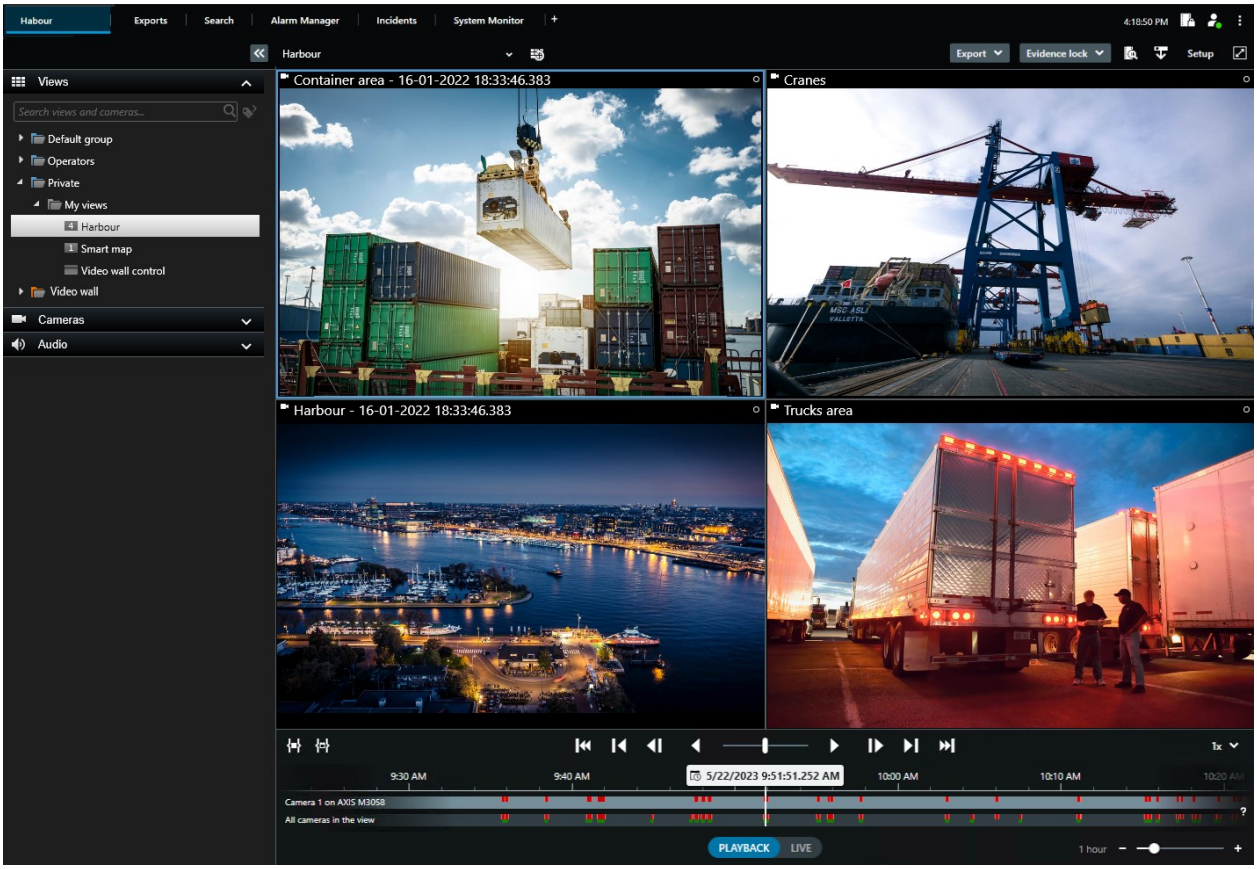
Die Management Client ist ein umfassender Administrations-Client für die Konfiguration und die tagtägliche Verwaltung des Systems. In mehreren Sprachen verfügbar.

Wird üblicherweise auf der Administrator-Workstation des Überwachungssystems o. ä. installiert.

## XProtect Smart Client (Erklärung)

XProtect Smart Client ist eine Desktop-Anwendung, mit der Sie ihre -Überwachungskameras verwalten können. Sie bietet die intuitive Kontrolle über Sicherheitsinstallationen, indem sie dem Benutzer Zugriff auf Live-Video und Videoaufzeichnungen, die sofortige Kontrolle über Kameras und angeschlossene Sicherheitsgeräte, sowie die Möglichkeit gibt, erweiterte Suchen nach Aufzeichnungen und Metadaten vorzunehmen.

Der in verschiedenen Sprachen verfügbare XProtect Smart Client bietet eine anpassbare Benutzeroberfläche, die sich für die Aufgaben einzelner Benutzer optimieren und an besondere Fähigkeiten und Berechtigungsstufen anpassen lässt.



Die Benutzeroberfläche erlaubt es Ihnen, Ihre Anzeige für ganz bestimmte Arbeitsumgebungen zu gestalten, indem Sie ein helles oder ein dunkles Thema auswählen. Außerdem bietet es arbeitsoptimierte Registerkarten und eine Haupt-Zeitlinie für eine einfache Überwachung.

Mithilfe des MIP SDK kann der Benutzer verschiedene Arten von Sicherheits- und Geschäftssystemen sowie Videoanalysenanwendungen integrieren, die Sie über XProtect Smart Client verwalten können.

XProtect Smart Client muss auf den Computern des Betreibers installiert sein. Überwachungssystemadministratoren verwalten den Zugriff zum Überwachungssystem über die Management Client. Von Clients angezeigte Aufzeichnungen stellt Ihr XProtect System über dessen Image Server-Dienst bereit. Der Dienst wird auf dem Server des Überwachungssystems im Hintergrund ausgeführt. Es wird keine separate Hardware benötigt.

## XProtect Mobile Client (Erklärung)

Der XProtect Mobile-Client ist eine mobile Überwachungslösung, die nahtlos mit dem Rest Ihres XProtect-Systems integriert ist. Er läuft auf Ihrem Android-Tablet oder Smartphone oder auf Ihrem Apple®-Tablet, Smartphone oder tragbaren Musikplayer und gibt Ihnen den Zugriff auf Kameras, Ansichten und weitere Funktionen, die im Management Client eingerichtet sind.

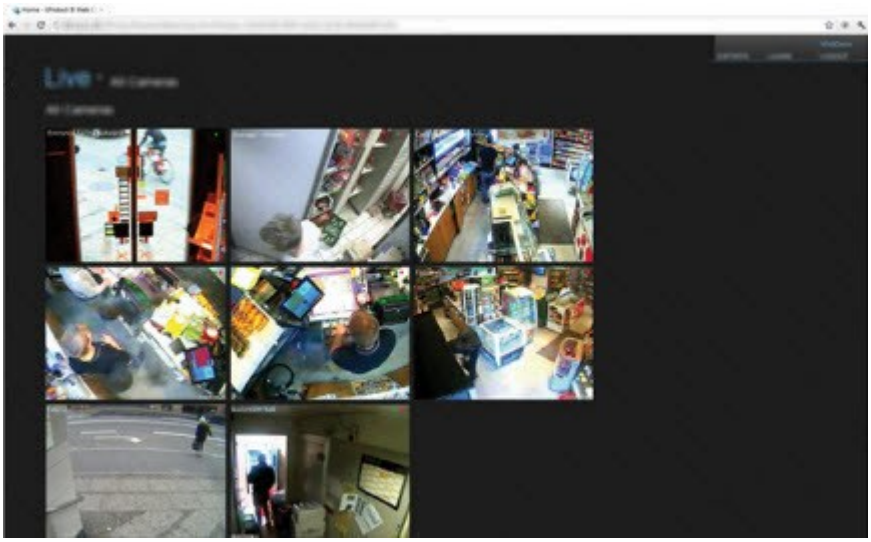
Nutzen Sie den XProtect Mobile-Client, um von einer oder mehreren Kameras Live-Videos oder Videoaufzeichnungen anzuzeigen und wiederzugeben, PTZ-Kameras (Pan/Tilt/Zoom) zu steuern, Ausgaben und Ereignisse auszulösen sowie mit der Video Push-Funktion Videodaten von Ihrem Gerät an das XProtect-System zu senden.

Wenn Sie den XProtect Mobile-Client für Ihr System verwenden möchten, müssen Sie über einen XProtect Mobile-Server verfügen, um eine Verbindung zwischen dem XProtect Mobile-Client und Ihrem System herstellen zu können. Wenn der XProtect Mobile Server einmal eingerichtet ist, laden Sie den XProtect Mobile Client gratis von Google Play oder App Store herunter, um mit der Nutzung von XProtect Mobile zu beginnen.

Sie benötigen eine Gerätelizenz für jedes Gerät, das in der Lage sein soll, Videoaufzeichnungen an Ihr XProtect System zu senden.

### XProtect Web Client (Erklärung)

XProtect Web Client ist eine webbasierte Client-Anwendung für die Anzeige, Wiedergabe und Freigabe von Videoinhalten. Sie bietet unmittelbaren Zugriff auf die am häufigsten verwendeten Überwachungsfunktionen inkl. Anzeige von Live-Videos, Wiedergabe aufgezeichneter Videoinhalte und Exportieren von Beweisen. Der Zugriff auf die Funktionen hängt von den Berechtigungen des jeweiligen Benutzers ab, die in Management Client eingerichtet werden.




Für den Zugriff auf XProtect Web Client müssen Sie über einen XProtect Mobile-Server verfügen, der die Verbindung zwischen XProtect Web Client und Ihrem System herstellt. XProtect Web Client selbst erfordert keine Installation und funktioniert mit den meisten Internetbrowsern. Sobald Sie den XProtect Mobile-Server eingerichtet haben, können Sie Ihr XProtect-System von jedem beliebigen Computer oder Tablet mit Internetzugang aus überwachen (vorausgesetzt, Sie kennen die richtige externe/Internetadresse, den Benutzernamen und das Passwort).

## XProtect Erweiterungen

### XProtect Access (Erklärung)

Milestone hat verschiedene Erweiterungen entwickelt. Erweiterungen sind Produkte, welche den Umfang der XProtect VMS-Produkte um zusätzliche Spezialfunktonen erweitern. Ihre XProtect-Lizenzdatei steuert den Zugang zu Erweiterungen.

Zur Nutzung von XProtect Access müssen Sie eine Basislizenz erworben haben, die Ihnen den Zugriff auf diese Funktion innerhalb Ihres XProtect-Systems erlaubt. Zudem benötigen Sie für jede Tür, die Sie kontrollieren möchten, eine Zutrittskontrolltür-Lizenz.

Sie können XProtect Access zusammen mit Zutrittskontrollsystemen anderer Anbieter verwenden, sofern diese über ein anbieterspezifisches Plug-in für XProtect Access verfügen.

Die Funktion der Zutrittskontrollintegration führt neue Funktionalität ein, die eine einfache Integration der Zutrittskontrollsysteme von Kunden mit XProtect ermöglichen. Sie erhalten:

- Eine allgemeine Bedienoberfläche für Anwender für mehrere Zutrittskontrollsysteme in XProtect Smart Client
- Schnellere und bessere Integration der Zutrittskontrollsysteme
- Mehr Funktionalität für den Anwender (siehe unten)

In XProtect Smart Client erhält der Anwender:

- Live-Überwachung von Ereignissen an Zutrittspunkten
- Anwendergestützter Zutritt für Zutrittsanforderung
- Karten-Integration
- Alarmdefinitionen für Ereignisse bezogen auf die Zutrittskontrolle
- Untersuchung von Ereignissen am Zutrittspunkt
- Zentralisierte Übersicht und Kontrolle von Türstatus
- Kartenhalter-Informationen und -Verwaltung

Das **Auditprotokoll** protokolliert die Befehle, die jeder Benutzer im Zutrittskontrollsystem von XProtect Smart Client ausführt.

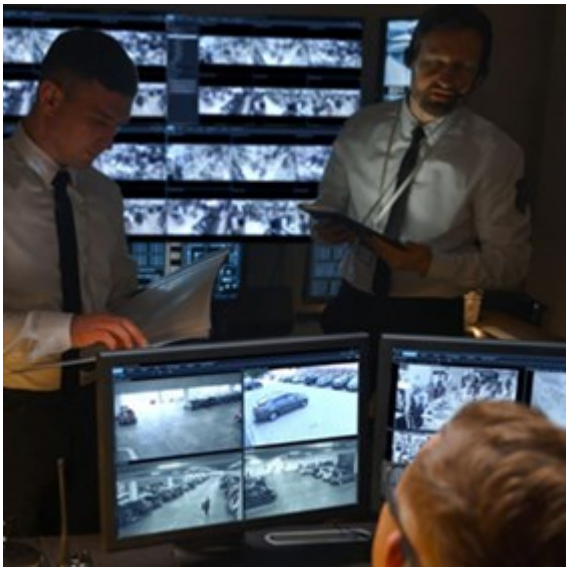
Neben einer Basislizenz für XProtect Access brauchen Sie ein anbieterspezifisches Integrations-Plug-in, das auf dem Event Server installiert ist, bevor Sie mit einer Integration beginnen können .

## XProtect Incident Manager

Milestone hat verschiedene Erweiterungen entwickelt. Erweiterungen sind Produkte, welche den Umfang der XProtect VMS-Produkte um zusätzliche Spezialfunktonen erweitern. Ihre XProtect-Lizenzdatei steuert den Zugang zu Erweiterungen.

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

XProtect Incident Manager ist eine Erweiterung, mit der Organisationen Vorfälle dokumentieren und sie mit Sequenzbeweisen (Video und ggf. Audio) aus dem XProtect VMS kombinieren können.



Die Benutzer von XProtect Incident Manager können alle Informationen zu einem Vorfall in Vorfallprojekten speichern. In den Vorfallprojekten können sie den Status und die Aktivitäten zu jedem Vorfall verfolgen. Auf diese Weise können die Benutzer Vorfälle effektiv verwalten und aussagekräftige Beweise zu Vorfällen sowohl intern mit Kollegen als auch extern mit Behörden austauschen.

XProtect Incident Manager hilft Organisationen dabei, eine Übersicht über die Vorfälle in den überwachten Bereichen zu erhalten und diese zu verstehen. Mit dieser Kenntnis können Organisationen Maßnahmen ergreifen, um ähnliche Vorfälle in der Zukunft möglichst auszuschließen.

In XProtect Management Client können die XProtect VMS-Administratoren einer Organisation die in XProtect Incident Manager verfügbaren Vorfalleigenschaften den Bedürfnissen der Organisation entsprechend festlegen. Die Anwender von XProtect Smart Client starten, speichern und verwalten Vorfallprojekte und fügen verschiedene Informationen zu den Vorfallprojekten hin. Dies sind u.a. Freitext, von den Administratoren definierte Vorfalleigenschaften und Sequenzen aus dem XProtect VMS. Die XProtect VMS sorgt für eine vollständige Rückverfolgbarkeit, indem sie protokolliert, wenn Administratoren Vorfalleigenschaften festlegen und bearbeiten und wenn Anwender Vorfallprojekte erstellen und aktualisieren.

## XProtect LPR (Erklärung)

Milestone hat verschiedene Erweiterungen entwickelt. Erweiterungen sind Produkte, welche den Umfang der XProtect VMS-Produkte um zusätzliche Spezialfunktonen erweitern. Ihre XProtect-Lizenzdatei steuert den Zugang zu Erweiterungen.

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

XProtect LPR bietet videobasierte Inhaltsanalyse (VCA) sowie die Erkennung von Nummernschildern und interagiert mit Ihrem Überwachungssystem und Ihrem XProtect Smart Client.

Zur Erkennung der Zeichen auf einem Nummernschild verwendet XProtect LPR eine optische Zeichenerkennung auf Bildern, unterstützt durch spezielle Kameraeinstellungen.

Sie können LPR (Nummernschilderkennung) mit anderen Überwachungsfunktionen wie Aufzeichnung und ereignisbasierter Aktivierung von Ausgängen kombinieren.

Beispiele für Ereignisse in XProtect LPR:

- Auslösen von Aufzeichnungen des Überwachungssystems in besonderer Qualität
- Aktivieren von Alarmen
- Abgleich mit Positiv-/Negativlisten
- Öffnen von Toren
- Einschalten der Beleuchtung
- Verschieben eines Videos mit Vorfällen auf die Computerbildschirme von bestimmtem Sicherheitspersonal
- Senden von SMS-Nachrichten

Bei einem Ereignis können Sie Alarme im XProtect Smart Client aktivieren.

## XProtect Smart Wall (Erklärung)

Siehe auch das XProtect Smart Wall Handbuch.

Milestone hat verschiedene Erweiterungen entwickelt. Erweiterungen sind Produkte, welche den Umfang der XProtect VMS-Produkte um zusätzliche Spezialfunktonen erweitern. Ihre XProtect-Lizenzdatei steuert den Zugang zu Erweiterungen.

XProtect Smart Wallist eine zusätzliche Erweiterung, mit der Organisationen Videowände erstellen können, die auf ihre speziellen Sicherheitsanforderungen zugeschnitten sind. XProtect Smart Wall gibt einen Überblick über alle Videodaten im XProtect VMS[1]-System und unterstützt eine beliebige Anzahl oder Kombination von Monitoren.

[1]Abkürzung für "Video Management Software".

XProtect Smart Wall gestattet es Anwendern, statiche Videowände anzuzeigen, die von ihrem Systemadministrator mit einem festgelegten Satz Kameras und Bildschirmlayout definiert wurde. In dem Sinne, dass Anwender kontrollieren können, was angezeigt wird, ist die Videowand ist allerdings auch anwenderbetrieben. Hierzu gehören:

- Schieben von Kameras und anderen Inhalten auf die Videowand, beispielsweise Bilder, Text, Alarme und Smart Maps
- Ganze Ansichten an die Bildschirme sendet
- Anwendung alternativer Voreinstellung[1] im Rahmen bestimmter Ereignisse

Zu guter Letzt können Änderungen an der Anzeige durch Regeln gesteuert werden, die Voreinstellungen automatisch aufgrund von spezifischen Ereignissen oder Zeitplänen ändern.

## XProtect Transact (Erklärung)

Milestone hat verschiedene Erweiterungen entwickelt. Erweiterungen sind Produkte, welche den Umfang der XProtect VMS-Produkte um zusätzliche Spezialfunktonen erweitern. Ihre XProtect-Lizenzdatei steuert den Zugang zu Erweiterungen.

---

[1]Ein vorgegebenes Layout für einen oder mehrere Smart Wall-Monitore in XProtect Smart Client. Voreinstellungen legen fest, welche Kameras angezeigt werden und wie der Inhalt auf jedem Bildschirm auf der Videowand angeordnet ist.

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

XProtect Transact ist eine Erweiterung für die IP-Videoüberwachungslösungen von Milestone.

XProtect Transact dient zur Überwachung laufender Transaktionen und zur Untersuchung vergangener Transaktionen. Die Transaktionen sind zur Überwachung der Transaktionen mit dem digitalen Überwachungsvideo verknüpft, um beispielsweise Beweismittel gegen einen Straftäter bereitzustellen oder einen Betrugsfall nachzuweisen. Dabei besteht zwischen den Transaktionsleitungen und den Videobildern eine 1-zu-1-Beziehung.

Die Transaktionsdaten stammen möglicherweise von verschiedenen Transaktionsquellen, in der Regel Point-of-Sale-Systeme (PoS) oder Geldautomaten.

## Milestone Open Network Bridge (Erklärung)

Milestone hat verschiedene Erweiterungen entwickelt. Erweiterungen sind Produkte, welche den Umfang der XProtect VMS-Produkte um zusätzliche Spezialfunktonen erweitern. Ihre XProtect-Lizenzdatei steuert den Zugang zu Erweiterungen.

Milestone Open Network Bridge ist eine offene, ONVIF-konforme Schnittstelle für den standardisierten Videoaustausch zwischen XProtect VMS-Systemen und anderen Sicherheitssystemen auf IP-Basis. So können die Strafverfolgungsbehörden, Überwachungszentralen oder ähnliche Organisationen (die als ONVIF-Clients bezeichnet werden) auf Live-Videostreams und Videoaufzeichnungen vom XProtect VMS-System zu den zentralen Überwachungslösungen zugreifen. Die Videoströme werden als RTSP-Streams über das Internet gesendet.

Die wichtigsten Vorteile dabei sind:

- Ermöglicht eine echte Interoperabilität und Wahlfreiheit für groß angelegte, herstellerübergreifende Sicherheitsimplementierungen und eine nahtlose Videointegration zwischen privaten und öffentlichen Einrichtungen
- Gibt externen Zugriff auf Videostreams in H.264 und H.265 im XProtect VMS-System, und zwar sowohl auf Live-Videos als auch auf Playback
- Bietet standardisierte Schnittstellen, die eine einfache und problemlose Integration von XProtect VMS-Lösungen mit Alarmzentralen und Überwachungsstationen ermöglichen

Dieses Dokument bietet folgendes:

- Informationen über den ONVIF-Standard und Links zu Referenzmaterial
- Anleitungen zur Installation und Konfiguration der Milestone Open Network Bridge in Ihrem XProtect VMS-Produkt.
- Beispiele zur Aktivierung verschiedener Typen von ONVIF-Clients zum Streamen von aufgezeichnetem und Live-Video von XProtect VMS-Produkten.

## XProtect DLNA Server (Erklärung)

Dieses Produkt wird von Milestone nicht mehr unterstützt.

Milestone hat verschiedene Erweiterungen entwickelt. Erweiterungen sind Produkte, welche den Umfang der XProtect VMS-Produkte um zusätzliche Spezialfunktonen erweitern. Ihre XProtect-Lizenzdatei steuert den Zugang zu Erweiterungen.

DLNA (Digital Living Network Alliance) ist ein Standard zur Verbindung von Multimediageräten. Elektronikhersteller lassen ihre Produkte DLNA-zertifizieren, damit die Interoperabilität zwischen verschiedenen Anbietern und Geräten gewährleistet ist. Dies ermöglicht ihnen den Vertrieb von Videoinhalten.

Öffentliche Bildschirme und TVs verfügen oftmals über eine DLNA-Zertifizierung und sind mit einem Netzwerk verbunden. Sie können das Netzwerk nach Medien scannen, sich zum Gerät verbinden und einen Medienstream zu ihrem integrierten Media-Player anfordern. XProtect DLNA Server kann von gewissen DLNA-zertifizierten Geräten gefunden werden und Live-Videostreams von ausgewählten Kameras an DLNA-zertifizierte Geräte mit einem Media-Player liefern.

Die DLNA-Geräte verfügen über eine Live-Videoverzögerung von 1-10 Sekunden. Dies wird durch verschiedene Puffergrößen in den Geräten verursacht.

XProtect DLNA Server muss mit dem selben Netzwerk wie das XProtect-System verbunden werden und das DLNA-Gerät muss mit dem selben Netzwerk wie XProtect DLNA Server verbunden werden.

# Geräte

## Hardware (Erklärung)

Hardware steht entweder für:

- Die physische Einheit, die mit dem Aufzeichnungsserver des Überwachungssystems direkt über IP verbunden ist, beispielsweise eine Kamera, ein Videoencoder, ein I/O-Modul
- Ein Aufzeichnungsserver an einem Remote-System in einer Milestone Interconnect-Einrichtung

Sie haben mehrere Optionen, um zu den Aufzeichnungsservern in Ihrem System Hardware hinzuzufügen.

Wenn Ihre Hardware sich hinter einem NAT-fähigen Router oder einer Firewall befindet, müssen Sie möglicherweise eine andere Portnummer bestimmen und den Router/die Firewall so konfigurieren, dass die von der Hardware genutzten Port- und IP-Adressen zugewiesen werden.

Der Assistent zum **Hardware hinzufügen** hilft Ihnen dabei, in Ihrem Netzwerk Hardware wie etwa Kameras und Videoencoder zu finden und diese den Aufzeichnungsservern in Ihrem System hinzuzufügen. Mit dem Assistenten können Sie auch Remote-Server für Milestone Interconnect-Einrichtungen hinzufügen. Fügen Sie jeweils nur bei **einem Aufzeichnungsserver** zur selben Zeit Hardware hinzu.

### Hardwarevorkonfiguration (Erklärung)

Manche Hersteller fordern, dass auf Hardware im Auslieferungszustand Benutzerdaten eingerichtet werden, bevor die Hardware erstmals zu einem VMS-System hinzugefügt wird. Dies wird als Hardwarevorkonfiguration bezeichnet und erfolgt mithilfe des Assistenten **Hardwaregeräte vorkonfigurieren**, der geöffnet wird, wenn der Assistent Hardware hinzufügen auf Seite 229 solche Hardware erkennt.

Einige wichtige Informationen zum Assistenten **Hardwaregeräte vorkonfigurieren**:

- Hardware, für die Benutzerdaten erforderlich sind, bevor sie zu einem VMS-System hinzugefügt wird, kann nicht unter Verwendung der typischen Standard-Benutzerdaten hinzugefügt werden und muss über den Assistenten konfiguriert werden, oder indem die Hardware direkt angeschlossen wird
- Benutzerdaten (Benutzername oder Passwort) können Sie nur auf Felder anwenden, die als **nicht festgelegt** gekennzeichnet sind
- Sobald der Hardware-**Status** auf **konfiguriert** lautet, können Sie die Benutzerdaten (Benutzername oder Passwort) nicht mehr ändern
- Die Vorkonfiguration gilt für Hardware im Auslieferungszustand und muss nur einmal erfolgen. Sobald die Hardware vorkonfiguriert wurde, kann sie wie jede andere Hardware verwaltet werden in Management Client
- Sobald Sie den Assistenten **Hardwaregeräte vorkonfigurieren** schließen, erscheint in dem Assistenten Hardware hinzufügen auf Seite 229 die vorkonfigurierte Hardware, und diese kann nun zu Ihrem System hinzugefügt werden

> ⚠ Es wird sehr empfohlen, die vorkonfigurierte Hardware zu Ihrem System hinzufügen, indem Sie den Assistenten schließen, erscheint in dem Assistenten Hardware hinzufügen auf Seite 229 ausführen, nachdem Sie den Assistenten **Hardwaregeräte vor Konfigurieren** geschlossen haben. Management Client speichert die vorkonfigurierten Benutzerdaten nicht ab, wenn Sie die Hardware nicht zu Ihrem System hinzufügen.

## Geräte (Erklärung)

Hardware verfügt über eine Anzahl Geräte, die Sie einzeln verwalten können, wie zum Beispiel:

- Eine physische Kamera verfügt über Geräte, die den Kamerateil repräsentieren (Objektive), sowie Mikrofone, Lautsprecher, Metadaten, Eingang und Ausgang, ob angefügt oder eingebaut
- Ein Videoencoder ist mit mehreren analogen Kameras verbunden, die in einer Geräteliste auftauchen, welche den Kamerateil repräsentieren (Objektive), sowie Mikrofone, Lautsprecher, Metadaten, Eingang und Ausgang, ob angefügt oder eingebaut
- Ein I/O-Modul verfügt über Geräte, die die Eingangs- und Ausgangskanäle für beispielsweise Lampen repräsentieren
- Ein zugehöriges Audio-Modul verfügt über Geräte, die Mikrofone und Lautsprecher-Ein- und -Ausgänge repräsentieren
- In einer Milestone Interconnect-Einrichtung erscheint das System in einer einzigen Liste als Hardware mit allen Geräten aus der Remote-Systeminstallation-Liste

Das System fügt der Hardware zugehörige Geräte automatisch hinzu, wenn Sie die Hardware hinzufügen.

Informationen über unterstütze Hardware finden Sie auf der Seite mit der unterstützten Hardware auf der Website Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

In den folgenden Abschnitten wird jeder Gerätetyp beschrieben, den Sie hinzufügen können.

### Kameras

Kamerageräte senden Videostreams an das System, das die Clientbenutzer verwenden können, um Live-Video anzuzeigen oder damit das System für spätere Wiedergaben durch die Clientbenutzer aufzeichnen kann. Die Rollen bestimmen die Berechtigung der Benutzer, Videos anzusehen.

### Mikrofone

An viele Geräte lassen sich externe Mikrofone anfügen. Einige Geräte verfügen über eingebaute Mikrofone.

Mikrofongeräte senden Audiostreams an das System, das die Clientbenutzer verwenden können, um Live-Audio anzuhören oder damit das System für spätere Wiedergaben durch die Clientbenutzer aufzeichnen kann. Sie können das System so einrichten, dass es für jedes Mikrofon bestimmte Ereignisse empfängt, die entsprechende Maßnahmen auslösen.

Die Rollen bestimmen die Berechtigung der Benutzer zum Abhören von Mikrofonen. Sie können Mikrofone nicht vom Management Client abhören.

### Lautsprecher

An viele Geräte lassen sich externe Lautsprecher anfügen. Einige Geräte verfügen über eingebaute Lautsprecher.

Das System versendet einen Audiostream an die Lautsprecher, wenn ein Benutzer im XProtect Smart Client die Sprechtaste drückt. Sie können diese Funktion auch von XProtect Web Client und XProtect® Mobile verwenden. Lautsprecheraudio wird nur aufgenommen, wenn ein Benutzer spricht. Die Rollen bestimmen die Berechtigung der Benutzer, über Lautsprecher zu sprechen. Sie können vom Management Client nicht über Lautsprecher sprechen.

Wenn zwei Benutzer gleichzeitig sprechen wollen, bestimmen die Rollen die Erlaubnis der Benutzer, über Lautsprecher zu sprechen. Sie können als Teil der Rollendefinierung Prioritäten für Sprecher festlegen, die von sehr hoch bis sehr niedrig reichen. Wenn zwei Benutzer zum selben Zeitpunkt sprechen möchten, erhält der Benutzer mit der Rolle, welche die höchste Priorität hat, die Gelegenheit zu sprechen. Wenn zwei Benutzer mit derselben Rolle gleichzeitig sprechen möchten, wird nach dem Windhundprinzip verfahren.

### Metadaten

Metadatengeräte versenden Datenstreams an das System, das die Client-Benutzer verwenden können, um Daten zu Daten anzuzeigen, zum Beispiel Daten, die das Videobild, den Inhalt, Objekte im Bild oder den Ort beschreiben, an dem das Bild aufgezeichnet wurde. Metadaten können an Kameras, Mikrofone oder Lautsprecher angehängt werden.

Metadaten können erzeugt werden von:

- Das Gerät, das selbst die Daten liefert, z. B. eine Kamera, die Videoaufzeichnungen liefert
- Einem Drittsystem oder Integration über einen generischen Metadatentreiber

Die durch das Gerät erzeugten Metadaten werden automatisch mit einem oder mehreren Geräten derselben Hardware verknüpft.

Rollen bestimmen die Berechtigung der Benutzer, Metadaten einzusehen.

### Eingänge

An viele Geräte lassen sich externe Einheiten an Eingangsports anfügen. Eingabegeräte sind normalerweise externe Sensoren. Solche externen Sensoren können beispielsweise genutzt werden, um zu registrieren, ob Türen, Fenster oder Tore geöffnet werden. Eingaben über diese externen Eingabegeräte werden vom System als Ereignisse angesehen.

Sie können diese Ereignisse in Regeln verwenden. Beispielsweise können Sie eine Regel erstellen, in der bestimmt wird, dass eine Kamera die Aufzeichnung startet, wenn eine Eingabe aktiviert wird, und 30 Sekunden nach Deaktivierung der Eingabe die Aufnahme beendet.

### Ausgaben

An viele Geräte lassen sich externe Einheiten an Ausgangsports anfügen. Hierdurch können Sie Lampen, Sirenen etc. über das System aktivieren/deaktivieren.

Sie können Ausgabe bei der Erstellung von Regeln nutzen. Sie können Regeln erstellen, die Ausgaben automatisch aktivieren oder deaktivieren, und Regeln, die Aktionen auslösen, wenn der Status einer Ausgabe verändert wird.

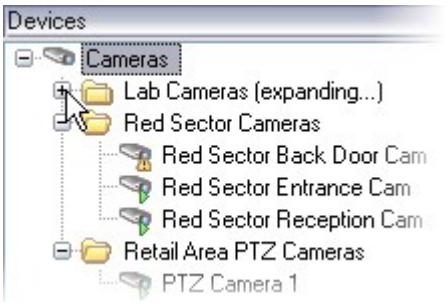
## Gerätegruppen (Erklärung)

Das Zusammenfügen von Geräten in Gerätegruppen ist Teil des **Hardware hinzufügen**-Assistenten. Sie können allerdings die Gruppen jederzeit verändern oder bei Bedarf neue Gruppen hinzufügen.

Ein Zusammenfügen verschiedener Gerätetypen (Kameras, Mikrofone, Lautsprecher, Metadaten, Eingänge und Ausgänge) in Gruppen kann für Ihr System von Vorteil sein:

- Gerätegruppen bieten eine intuitive Übersicht der Geräte in Ihrem System
- Geräte können zu mehreren Gruppen gehören
- Sie können Untergruppen und Untergruppen innerhalb von Untergruppen erstellen
- Sie können allgemeine Eigenschaften für alle Geräte in einer Gerätegruppe gleichzeitig festlegen
- Geräteeigenschaften, die mittels der Gruppe festgelegt werden, gelten für die einzelnen Geräte und nicht für die Gruppe
- Bezüglich Rollen können Sie allgemeine Sicherheitseinstellungen für alle Geräte in einer Gerätegruppe gleichzeitig festlegen
- Sie können eine Regel für alle Geräte in einer Gerätegruppe gleichzeitig festlegen

Sie können so viele Gerätegruppen erstellen, wie Sie benötigen, jedoch nicht verschiedene Gerätetypen (z. B. Kameras und Lautsprecher) in einer Gerätegruppe vermischen.




Erstellen Sie Gerätegruppen mit **weniger** als 400 Geräten, um alle Eigenschaften anzeigen und bearbeiten zu können.

Wenn Sie eine Gerätegruppe löschen, entfernen Sie nur die Gerätegruppe selbst. Wenn Sie ein Gerät, beispielsweise eine Kamera, aus Ihrem System entfernen möchten, sollten Sie dies auf der Ebene des Aufzeichnungsservers tun.

Die folgenden Beispiele zeigen Kameras, die zu Gerätegruppen zusammengefasst wurden. Das gleiche Prinzip gilt aber für alle Geräte

Eine Gerätegruppe hinzufügen

Bestimmen, welche Geräte die Gruppe beinhalten soll

Bestimmen Sie die allgemeinen Eigenschaften für alle Geräte in einer Gerätegruppe

# Medienspeicherung

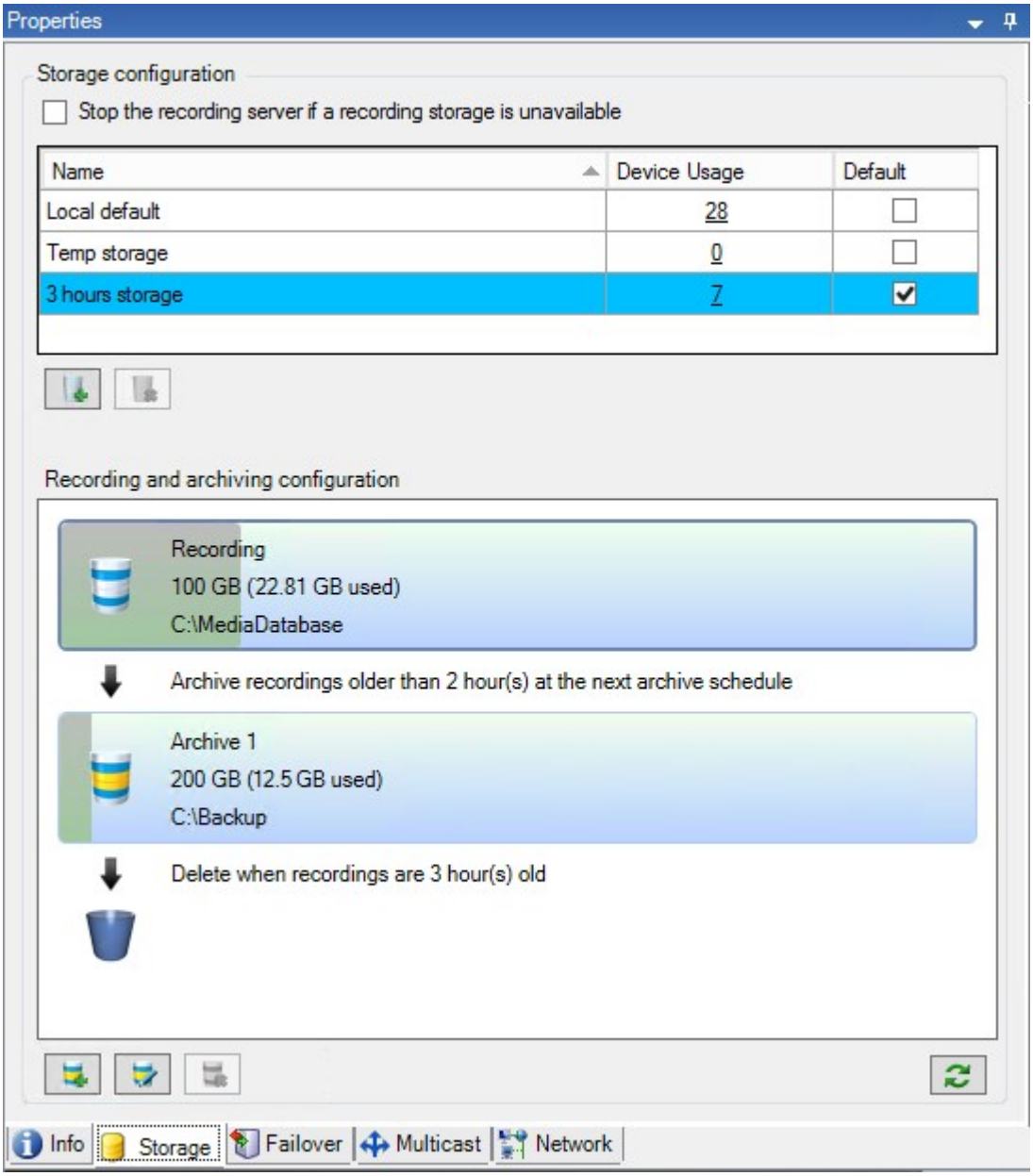
## Lagerung und Archivierung (Erklärung)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Auf der Registerkarte **Speicher** können Sie Aufzeichnungen für einen ausgewählten Aufzeichnungsserver einrichten, verwalten und anzeigen.

Zur Aufzeichnung von Speicher und Archiven zeigt die horizontale Leiste die aktuelle Menge an Speicherplatz an. Sie können das Verhalten des Aufzeichnungsservers für den Fall angeben, dass Aufzeichnungsspeicher nicht mehr verfügbar sind. Dies ist vor allem wichtig, wenn Ihr System Failover-Server beinhaltet.

Bei Verwendung von **Beweissicherung** zeigt eine vertikale rote Linie an, welcher Speicherplatz für Aufnahmen mit Beweissicherung verwendet wird.




Wenn eine Kamera Video- oder Audiodaten aufzeichnet, werden alle ausgewählten Aufzeichnungen standardmäßig in dem für das Gerät definierten Speicher gespeichert. Jeder Speicher besteht aus einem Aufzeichnungsspeicher, der Aufzeichnungen in der **Aufzeichnungs**-Datenbank speichert. Ein Speicher hat keine Standardarchive; Sie können jedoch Archive erstellen.

Um zu vermeiden, dass die Aufzeichnungsdatenbank vollläuft, können Sie weitere Speichergeräte erstellen (siehe Einen neuen Speicher hinzufügen auf Seite 213). Sie können auf jedem Speichergerät auch Archive erstellen und einen Archivierungsprozess zum Speichern von Daten auslösen (siehe Erstellen eines Archivs in einem Speicher auf Seite 213).

Bei der Archivierung handelt es sich um die automatische Übertragung von Aufzeichnungen beispielsweise von der Aufzeichnungsdatenbank einer Kamera an einen anderen Speicherort. Das bedeutet, dass die Menge der Aufzeichnungen, die Sie speichern können, nicht auf die Größe der Aufzeichnungsdatenbank beschränkt ist. Bei der Archivierung können Sie Ihre Aufzeichnungen auch auf anderen Medien sichern.

Speicherung und Archivierung lassen sich auf jedem Aufzeichnungsserver konfigurieren.

Solange Sie archivierte Aufzeichnungen lokal oder in aufrufbaren Netzwerklaufwerken speichern, können Sie XProtect Smart Client zu ihrer Ansicht verwenden.

Wenn ein Laufwerk ausfällt und der Aufzeichnungsspeicher nicht länger verfügbar ist, wechselt der horizontale Balken auf Rot. Es ist zwar noch möglich, Live-Video in XProtect Smart Client anzuzeigen, aber die Aufzeichnung und Archivierung wird gestoppt, bis das Festplattenlaufwerk wiederhergestellt wird. Wenn Ihr System mit ausfallsicheren Aufzeichnungsservern konfiguriert wurde, können Sie festlegen, dass der Aufzeichnungsserver nicht mehr ausgeführt werden soll, damit die ausfallsicheren Server übernehmen Geben Sie an, wie das System sich verhalten soll, wenn kein Speicherplatz für Aufzeichnungen verfügbar ist auf Seite 211.

Im Folgenden werden hauptsächlich Kameras und Video erwähnt, das Gleiche gilt jedoch auch für Lautsprecher, Mikrofone, Audio und Ton.

Milestone empfiehlt die Verwendung einer dedizierten Festplatte für die Aufzeichnung-Speicher und -Archive, um eine beeinträchtigte Leistung der Festplatte zu vermeiden. Bei der Formatierung der Festplatte muss die Einstellung **Größe der Zuweisungseinheiten** von 4 auf 64 Kilobyte geändert werden. Dadurch lässt sich die Aufzeichnungsleistung der Festplatte maßgeblich verbessern. Mehr Informationen und Hilfestellungen zur Größe der Zuweisungseinheiten finden Sie auf der Microsoft-Website (https://support.microsoft.com/en-us/topic/default-cluster-size-for-ntfs-fat-and-exfat-9772e6f1-e31a-00d7-e18f-73169155af95).

Wenn weniger als 5 GB Speicherplatz frei sind, werden immer die ältesten Daten in einer Datenbank automatisch archiviert (oder gelöscht, wenn kein nächstes Archiv festgelegt ist). Wenn weniger als 1 GB frei ist, werden die Daten gelöscht. Eine Datenbank erfordert 250 MB an freiem Speicherplatz. Wenn Sie diese Grenze erreichen, weil die Daten nicht schnell genug gelöscht werden, kann der Versuch, in die Datenbank zu schreiben, fehlschlagen. In diesem Fall werden keine weiteren Daten in die Datenbank geschrieben, bis Sie genügend Speicherplatz freigegeben haben. Die tatsächliche Maximalgröße Ihrer Datenbank ist die Anzahl der angegebenen Gigabyte minus 5 GB.

Für FIPS 140-2-konforme Systeme mit Exporten und archivierten Mediendatenbanken von XProtect VMS Versionen vor 2017 R1, die mit nicht FIPS-konformen Ziffern verschlüsselt sind, ist es erforderlich, die Daten an einem Ort zu archivieren, von wo aus weiterhin auf sie zugegriffen werden kann, wenn FIPS aktiviert wurde. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

**Anbinden von Geräten an einen Speicher**

Sobald Sie die Speicher- und Archivierungseinstellungen für einen Aufzeichnungsserver konfiguriert haben, können Sie die Speicherung und Archivierung für einzelne Kameras oder eine Kameragruppe aktivieren. Sie können dies über die einzelnen Geräte oder über die Gerätegruppe ausführen. Siehe Anbinden eines Geräts oder eine Gruppe von Geräten an einen Speicher auf Seite 213.

**Effektive Archivierung**

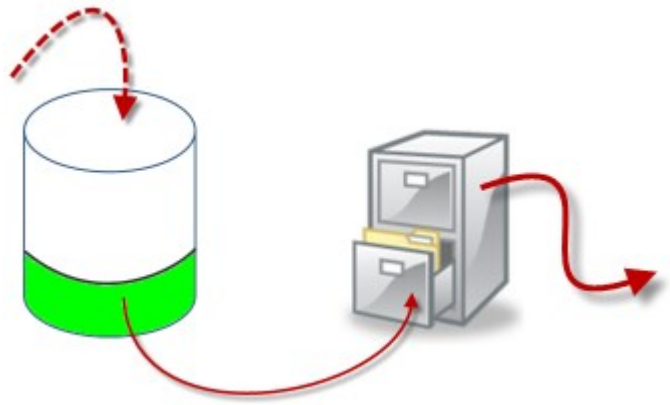
Wenn Sie die Archivierung für eine Kamera oder eine Kameragruppe aktivieren, wird der Inhalt des Aufnahmespeichers in von Ihnen festgelegten Abständen automatisch in das erste Archiv verschoben.

Je nach Anforderungen können Sie für jeden Ihrer Speicher ein oder mehrere Archive konfigurieren. Archive lassen sich entweder lokal auf dem Computer des Aufzeichnungsservers selbst oder an einem anderen Speicherort platzieren, den das System aufrufen kann (z. B. in einem Netzwerklaufwerk).

Indem Sie Ihre Archivierung effektiv einrichten, können Sie den Speicherbedarf optimieren. Oft möchte man, dass archivierte Aufnahmen möglichst wenig Platz beanspruchen, besonders langfristig, wo man vielleicht sogar an der Bildqualität sparen kann. Auf der Registerkarte **Speicher** eines Aufzeichnungsservers nehmen Sie effektive Archivierungen vor, indem Sie verschiedene voneinander abhängige Einstellungen anpassen:

- Aufzeichnung der Speichererhaltung
- Aufzeichnung der Speichergröße
- Speicherzeit von Archiven
- Größe von Archiven
- Archiv-Zeitplan
- Verschlüsselung
- Bilder pro Sekunde (FPS).

Mit den Größenfeldern lässt sich die Größe des Aufzeichnungsspeichers, veranschaulicht durch den Zylinder, und seiner Archive festlegen:



Durch Einstellung der Speicherzeit und Größe für die Aufzeichnungsspeicher (veranschaulicht durch den weißen Bereich im Zylinder) können Sie festlegen, wie alt Aufzeichnungen sein müssen, bevor sie archiviert werden. In unserem dargestellten Beispiel archivieren Sie die Aufzeichnungen, wenn sie alt genug sind, um archiviert zu werden.

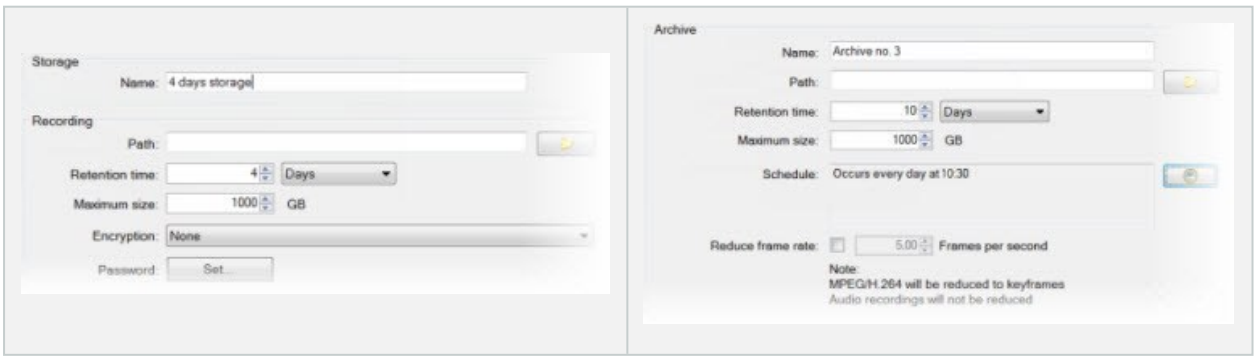
Die Einstellung der Speicherzeit und Größe für Archive bestimmt darüber, wie lange die Aufzeichnungen im Archiv verbleiben. Aufzeichnungen bleiben für die angegebene Zeit bzw. solange im Archiv, bis das Archiv das festgelegte Größenlimit erreicht hat. Wenn diese Einstellungen erfüllt sind, beginnt das System damit, alte Aufzeichnungen im Archiv zu überschreiben.

Der Archiv-Zeitplan bestimmt darüber, wie oft und zu welchen Zeiten Archivierungen vorgenommen werden.

Die Bilder pro Sekunde bestimmen über die Größe der Daten in den Datenbanken.

Für eine effektive Archivierung Ihrer Aufzeichnungen müssen Sie alle der Parameter passend zueinander konfigurieren. Das bedeutet, dass die Speicherzeit des nächsten Archivs stets länger sein muss als die Speicherzeit des aktuellen Archivs bzw. der aktuellen Aufzeichnungsdatenbank. Der Grund dafür ist, dass die Zahl der Speichertage, die für ein Archiv angegeben sind, alle Speicherzeiten beinhaltet, die früher im Prozess angegeben wurden. Außerdem muss die Archivierung in kürzeren Abständen erfolgen als die Speicherzeit; ansonsten drohen Datenverluste. Wenn Sie eine Speicherzeit von 24 Stunden eingerichtet haben, werden alle Daten gelöscht, die älter als 24 Stunden sind. Wenn Sie Ihre Daten stets sicher ins nächste Archiv verschieben wollen, müssen Sie die Archivierung häufiger als einmal alle 24 Stunden ausführen.

**Beispiel**: Diese Speicher (Abbildung links) weisen eine Speicherzeit von 4 Tagen, das folgende Archiv (Abbildung rechts) eine Speicherzeit von 10 Tagen auf. Die Archivierung wurde so konfiguriert, dass sie jeden Tag um 10:30 Uhr stattfindet, sodass Archivierungen häufiger vorgenommen werden als die Speicherzeit lang ist.



Außerdem können Sie die Archivierung mithilfe von Regeln und Ereignissen steuern.

## Archivstruktur (Erklärung)

Bei der Archivierung von Aufzeichnungen speichern Sie diese in einer bestimmten Struktur des Archivs, die verschiedene Unterverzeichnisse umfasst.

> Bei der gesamten regulären Nutzung Ihres Systems ist die Struktur mit Unterverzeichnissen für die Benutzer des Systems vollkommen transparent, wenn sie sämtliche Aufzeichnungen mit dem XProtect Smart Client durchsuchen. Dabei ist es egal, ob die Aufzeichnungen archiviert sind oder nicht. Wenn Sie Ihre archivierten Aufzeichnungen effektiv sichern möchten, ist es wichtig, dass Sie die Struktur mit Unterverzeichnissen gut kennen.

In jedem der Archivverzeichnisse des Aufzeichnungsservers erstellt das System automatisch separate Unterverzeichnisse. Diese Unterverzeichnisse werden nach dem Namen des Geräts und der Archivdatenbank benannt.

Da Sie Aufzeichnungen aus verschiedenen Kameras im gleichen Archiv speichern können und die Archivierung für die einzelnen Kameras wahrscheinlich in regelmäßigen Abständen vorgenommen wird, werden automatisch Unterverzeichnisse hinzugefügt.

Diese Unterverzeichnisse stehen für je eine Stunde Aufzeichnungen. Dank dieser stundenweisen Aufteilung werden nur relativ kleine Teile von Daten in einem Archiv verschoben, wenn Sie die zulässige Maximalgröße des Archivs erreichen.

Die Unterverzeichnisse werden nach dem Gerät benannt, gefolgt von einem Hinweis darauf, woher die Aufzeichnungen stammen (lokaler Speicher oder SMTP), **plus** Datum und Uhrzeit des aktuellsten Datensatzes in der Datenbank, der im Unterverzeichnis enthalten ist.

**Namensstruktur**

```
...[Storage Path]\[Storage name]\[device-name] - plus date and time of most
recent recording]\
```

Wenn vom lokalen Speicher:

```
...[Storage Path]\[Storage name]\[device-name] (Edge) - plus date and time of
most recent recording]\
```

Falls via SMTP:

```
...[Storage Path]\[Storage name]\[device-name] (SMTP) - plus date and time of
most recent recording]\
```

**Praktisches Beispiel**

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

**Unterverzeichnisse**

Außerdem werden automatisch weitere Unterverzeichnisse hinzugefügt. Zahl und Art der Unterverzeichnisse hängen von der Art der jeweiligen Aufzeichnungen ab. So werden zum Beispiel separate Unterverzeichnisse hinzugefügt, wenn Aufzeichnungen technisch in Sequenzen aufgeteilt werden. Dies kommt häufig vor, wenn Sie zur Auslösung von Aufzeichnungen eine Bewegungserkennung nutzen.

- **Medien**: Dieser Ordner enthält die tatsächlichen Medien, bei denen es sich um entweder Video- oder Audioinhalte handelt (nicht aber beides)
- **MotionLevel**: Dieser Ordner enthält Raster mit Bewegungsraten, die aus den Videodaten mit unserem Bewegungserkennungsalgorithmus erstellt wurden. Auf Grundlage dieser Daten kann die Smart Search-Funktion in XProtect Smart Client extrem schnelle Suchen durchführen.
- **Bewegung**: In diesem Ordner werden Bewegungssequenzen gespeichert. Eine Bewegungssequenz ist ein zeitlicher Abschnitt, in dem eine Bewegung in den Videodaten erkannt wurde. Diese Informationen werden zum Beispiel in der Zeitachse in XProtect Smart Client verwendet
- **Aufzeichnung**: In diesem Ordner werden Aufzeichnungssequenzen gespeichert. Eine Aufzeichnungssequenz ist ein Zeitintervall, für das es kohärente Aufzeichnungen mit Mediendaten gibt. Diese Informationen werden zum Beispiel zum Zeichnen der Zeitachse in XProtect Smart Client verwendet
- **Signatur**: Dieser Ordner enthält die für die Mediendaten (im Medienordner) erstellten Signaturen. Mit diesen Informationen können Sie sicherstellen, dass die Mediendaten seit ihrer Aufzeichnung nicht manipuliert wurden.

Falls Sie Ihre Archive sichern möchten, können Sie Sicherungen gezielt vornehmen, wenn Sie die Grundlagen der Struktur mit Unterverzeichnissen gut kennen.

**Sicherungsbeispiele**

Wenn Sie den Inhalt eines gesamten Archivs sichern möchten, sichern Sie das entsprechende Archivverzeichnis mit all seinen Inhalten. Zum Beispiel alles unterhalb von:

```
...F:\OurArchive\
```

Um die Aufzeichnungen einer bestimmten Kamera aus einem bestimmten Zeitraum zu sichern, sichern Sie ausschließlich die entsprechenden Unterverzeichnisse. Zum Beispiel alles unterhalb von:

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

## Puffern und abspeichern von Aufzeichnungen (Erklärung)

Voralarm-Puffern ist die Möglichkeit, Audio und Video aufzuzeichnen bevor das eigentliche auslösende Ereignis auftritt. Dies ist besonders nützlich, wenn Sie Audio oder Video aufnehmen möchten, das zu einem Ereignis führt, welches die Aufzeichnung auslöst (z. B. das Öffnen einer Tür).

Voralarm-Puffern ist möglich, da das System kontinuierlich Audio- und Video-Streams von den verbundenen Geräten empfängt und diese temporär über den festgelegten Voralarm-Zeitraum speichert.

- Bei Auslösung einer Aufzeichnungsregel werden temporäre Aufzeichnungen zu permanenten während der eingestellten Voralarmaufzeichnungszeit
- Wenn keine Aufzeichnungsregel ausgelöst wird, werden die temporären Aufzeichnungen im Voralarm-Puffer automatisch nach der eingestellten Voralarm-Pufferzeit gelöscht

### Speicherort für vorübergehend gepufferte Aufzeichnungen

Sie können den Speicherort der temporären Voralarm-Puffer-Aufzeichnungen auswählen:

- Im Speicher ist der Voralarm-Zeitraum auf 15 Sekunden begrenzt.
- Auf der Festplatte (in der Mediendatenbank) können Sie alle Werte auswählen.

Speichern im Speicher statt auf der Festplatte verbessert die Systemleistung, ist jedoch nur für kürzere Vorpufferzeiten möglich.

Sollten Aufzeichnungen im Speicher aufbewahrt werden, müssen Sie einige der temporären Aufzeichnungen zu permanenten machen, wodurch die übrigen temporären Aufzeichnungen unwiederbringlich gelöscht werden. Wenn Sie die übrigen Aufzeichnungen behalten möchten, speichern Sie diese auf der Festplatte.

# Authentifizierung

## Active Directory (Erklärung)

Active Directory ist ein verteilter Verzeichnisdienst, der von Microsoft für Windows-Domänennetzwerke implementiert wird. Dieser Dienst ist in den meisten Windows Server-Betriebssystemen enthalten. Er identifiziert die Ressourcen in einem Netzwerk, sodass Benutzer oder Anwendungen darauf zugreifen können.

Wenn der Dienst installiert ist, können Sie Windows-Benutzer aus Active Directory hinzufügen. Außerdem haben Sie die Möglichkeit, Basisnutzer ohne Active Directory hinzuzufügen. Im Zusammenhang mit Basisnutzer gelten bestimmte Systemeinschränkungen.

## Benutzer (Erklärung)

Der Begriff **Benutzer** bezeichnet primär Benutzer, die sich über die Clients mit dem Überwachungssystem verbinden. Sie können solche Benutzer auf zwei verschiedene Weisen konfigurieren:

- Als **Basisnutzer**, Authentifizierung durch Benutzername und Passwort
- Als **Windows-Benutzer**, Authentifizierung auf Basis ihrer Windows-Anmeldung

### Windows-Benutzer

Sie können Windows-Benutzer mithilfe von Active Directory hinzufügen. Active Directory (AD) ist ein Verzeichnisdienst, der von Microsoft für Windows-Domänennetzwerke implementiert wird. Dieser Dienst ist in den meisten Windows Server-Betriebssystemen enthalten. Er identifiziert die Ressourcen in einem Netzwerk, sodass Benutzer oder Anwendungen darauf zugreifen können. Active Directory verwendet die Konzepte von Benutzern und Gruppen.

Benutzer sind Active Directory-Objekte, Einzelpersonen werden durch ein Benutzerkonto dargestellt. Beispiel:


Gruppen sind Active Directory-Objekte mit mehreren Benutzern. In diesem Beispiel hat die Management-Gruppe drei Benutzer:


Gruppen können eine beliebige Anzahl an Benutzern beinhalten. Wenn Sie dem System eine Gruppe hinzufügen, fügen Sie alle Gruppenmitglieder auf einmal hinzu. Sobald Sie die Gruppe dem System hinzugefügt haben, werden alle Änderungen, die an der Gruppe in Active Directory vorgenommen wurden (z. B. neue Mitglieder, die Sie hinzufügen oder alte Mitglieder, die Sie später entfernen) sofort auf das System übertragen. Ein Benutzer kann Mitglied mehrerer Gruppen zugleich sein.

Wenn Sie Active Directory verwenden, um bestehende Benutzer- und Gruppeninformationen dem System hinzuzufügen, hat dies einige Vorteile:

- Benutzer und Gruppen werden zentral in Active Directory angelegt, deshalb müssen Sie Benutzerkonten nicht von Grund auf neu erstellen
- Sie brauchen die Benutzerauthentifizierung nicht auf dem System zu konfigurieren, da Active Directory die Authentifizierung regelt

Bevor Sie Benutzer und Gruppen über den Active Directory-Dienst hinzufügen können, muss in Ihrem Netzwerk ein Server vorhanden sein, auf dem Active Directory installiert ist.

### Basisnutzer

Wenn ihr System keinen Zugriff auf Active Directory hat, erstellen Sie einen Basisbenutzer. Informationen dazu, wie ein Basisbenutzer erstellt wird, finden Sie unter Erstellen von Basisnutzer auf Seite 311.

## Identity Provider (Erklärung)

Identity Provider app pool (IDP) ist eine Systemeinheit, die für Basisbenutzer Angaben zur Identität erstellt, pflegt und verwaltet.

Identity Provider bietet auch Authentifizierungs- und Registrierungsdienste für abhängige Anwendungen oder Dienste, in diesem Fall: Aufzeichnungsserver, Management Server, Data Collector und Berichtsserver.

Wenn Sie sich bei XProtect Clients und Diensten als Basisbenutzer anmelden, geht Ihre Anfrage an die Identity Provider. Nach der Authentifizierung kann der Benutzer den Management Server anrufen.

Identity Provider läuft im IIS als Teil des Management Servers, unter Verwendung desselben SQL Server mit einer separaten Datenbank und ist für die Erstellung und Bearbeitung von OAuth-Kommunikationstokens zuständig, die Dienste bei der Kommunikation (Surveillance_IDP) verwenden.

Identity Provider Protokolle finden Sie unter: `\\ProgramData\Milestone\IDP\Logs`.

## Externer IDP (Erklärung)

IDP ist ein Akronym für Identity Provider. Ein externer IDP ist eine externe Anwendung und ein Dienst, in dem Sie Angaben zur Identität der Benutzer speichern und verwalten und Dienste zur Benutzerauthentifizierung für andere Systeme bereitstellen können. Sie können einen externen IDP mit dem XProtect VMS verknüpfen.

XProtect VMS unterstützt externe IDPs, die mit OpenID Connect kompatibel sind (OIDC).

### Ansprüche (Erklärung)

Ansprüche sind das Bindeglied zwischen dem externen IDP und dem XProtect VMS.

Ein Anspruch ist eine Aussage, die eine Entität wie ein Nutzer oder eine Anwendung über sich selbst macht. Im XProtect VMS kann ein Anspruch mit einer Rolle verknüpft werden, die die XProtect Berechtigungen der Benutzer bestimmt.

Der Anspruch ist ein Schlüsselwert, der aus Namen des Anspruchs und seinem Wert besteht. Der Name des Anspruchs könnte z.B. ein Standardname sein, der den Inhalt des Anspruchswertes beschreibt, und der Anspruchswert könnte der Name einer Gruppe sein. Beispiel für Ansprüche von einem externen IDP. Beispiel für Ansprüche von einem externen IDP.

### Lassen Sie die Benutzer sich von einem externen IDP am XProtect VMS anmelden

- Legen Sie vom externen IDP die Benutzer an. Außerdem müssen Sie die XProtect und die Interaktion zwischen XProtect und dem externen IDP identifizieren. Schließlich erstellen Sie die Ansprüche, um die Benutzer als externe IDP-Benutzer in der XProtect VMS zu identifizieren.
- Erstellen Sie in der XProtect VMS eine Konfiguration, die es dem Identity Provider ermöglicht, den externen IDP zu kontaktieren. Weitere Informationen zum Erstellen einer Konfiguration für einen externen IDP finden Sie unter Hinzufügen und Konfigurieren eines externen IDP.
- Richten Sie vom XProtect VMS aus die Authentifizierung der Benutzer ein, indem Sie die Benutzeransprüche aus dem externen IDP zu den XProtect Rollen zuordnen. Weitere Informationen zum Zuordnen von Ansprüchen zu Rollen finden Sie unter Ansprüche von einem externen IDP zu Rollen in XProtect zuordnen.

### Weiterleitung URIen

Die Weiterleitung URI gibt die Seite an, zu der der Benutzer nach einer erfolgreichen Authentifizierung weitergeleitet wird. In Ihrem externen IDP müssen Sie die Adresse des Management-Servers hinzufügen, gefolgt von dem **Rückrufpfad**, der in XProtect Management Client definiert wurde. Zum Beispiel https://management-server-computer.company.com/idp/signin-oidc

### Eindeutige Benutzernamen für Benutzer des externen IDP

Die Benutzernamen werden automatisch für Benutzer erstellt, die sich über einen externen IDP an Milestone XProtect anmelden.

Der externe IDP stellt eine Reihe von Ansprüchen bereit, um in XProtect automatisch einen Namen für den Benutzer zu erstellen, und in XProtect wird mit Hilfe eines Algorithmus ein Name aus dem externen IDP ausgewählt, der in der VMS-Datenbank eindeutig ist.

#### Beispiel für Ansprüche von einem externen IDP

Die Ansprüche bestehen aus einem Anspruchsnamen und einem Anspruchswert. Beispielsweise:

| Name der Forderung | Wert der Forderung |
|---|---|
| Name | Raz Van |
| E-Mail | 123@domain.com |
| amr | pwd |

| Name der Forderung | Wert der Forderung |
|---|---|
| idp | 00o2ghkgazGgi9BIE5d7 |
| preferred_ username | 321@domain.com |
| vmsRole | Bediener |
| locale | en-US |
| given_name | Raz |
| family_name | Lindberg |
| zoneinfo | America/Los_Angeles |
| email_verified | Wahr |

Verwendung der laufenden Nummer des Anspruchs zum Erstellen von Benutzernamen in XProtect

In XProtect wird die Suchpriorität beim Anlegen eines Benutzers im XProtect VMS durch die laufende Nummer der Ansprüche in der folgenden Tabelle gesteuert. Der erste verfügbare Anspruchsname wird im XProtect VMS verwendet:

| Name der Forderung | Laufende Nummer | Beschreibung |
|---|---|---|
| UserNameClaimType | 1 | Das Mapping wurde mit einem Anspruch konfiguriert, um den Benutzernamen festzulegen. Der Anspruch wird im Feld **Anspruch zum Anlegen des Benutzernamens** auf der Registerkarte **externer IDP** unter **Werkzeuge** > **Optionen** definiert. |
| preferred_username | 2 | Anspruch, der von dem externen IDP ausgehen kann. Ein Standardanspruch, der in der Regel dafür in Oidc verwendet wird (OpenID |

| Name der Forderung | Laufende Nummer | Beschreibung |
|---|---|---|
| | | Connect). |
| Name | 3 | |
| given_name family_ name | 4 | Vorname und Familienname in einer Kombination wie Bob Johnson. |
| E-Mail | 5 | |
| Erster verfügbarer Anspruch + #(erste verfügbare Nummer) | 6 | Z.B. Bob#1 |

Definition spezifischer Ansprüche zur Erstellung von Benutzernamen in XProtect

Die XProtect Administratoren können einen bestimmten Anspruch aus dem externen IDP definieren, der zur Erstellung eines Benutzernamens im XProtect VMS verwendet werden soll. Wenn ein Administrator einen Anspruch definiert, der für die Erstellung des Benutzernamens im XProtect VMS verwendet werden soll, muss der Name des Anspruchs genau so geschrieben werden, wie der Name des Anspruchs, der aus dem externen IDP stammt.

- Den für den Benutzernamen zu verwendenden Anspruch können Sie im Feld **Anspruch zum Erstellen des Benutzernamens** auf der Registerkarte **externer IDP** unter **Extras** > **Optionen** festlegen.

### Löschen externer IDP-Benutzer

In XProtect von einem externen IDP-Login erstellten Benutzer werden auf die gleiche Weise gelöscht wie ein normaler Benutzer, und der Benutzer kann jederzeit nach seiner Erstellung gelöscht werden.

Wenn ein Benutzer in XProtect gelöscht wird und sich der Benutzer erneut aus dem externen IDP anmeldet, wird in XProtect ein neuer Benutzer angelegt. Allerdings gehen die mit dem Benutzer in XProtect verbundenen Daten, z.B. private Ansichten und Rollen, verloren, und diese Informationen müssen für den Benutzer in XProtect neu erstellt werden.

Wenn ein externer IDP in der Management Client gelöscht wird, werden auch alle Benutzer gelöscht, die über den externen IDP mit dem VMS verbunden sind.

# Sicherheit

## Rollen und Berechtigungen einer Rolle (Erklärung)

Alle Benutzer in Milestone XProtect VMS gehören zu einer Rolle.

Rollen definieren die Berechtigungen der Benutzer, einschließlich der Geräte, auf die die Benutzer zugreifen können. Rollen definieren auch Sicherheits- und Zugriffsberechtigungen innerhalb des Videoverwaltungssystems.

Das System wird standardmäßig mit einer **Administratorenrolle** ausgeliefert, die vollen Zugriff auf alle Systemfunktionen bietet. In den meisten Fällen benötigen Sie jedoch mehr als eine Rolle in Ihrem System, um zwischen den Benutzern und dem Zugriff, den sie erhalten sollen, zu unterscheiden. Sie können so viele Rollen hinzufügen, wie Sie benötigen. Siehe Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen auf Seite 309.

So könnten Sie beispielsweise verschiedene Arten von Rollen für Benutzer von XProtect Smart Clienteinrichten, je nachdem, auf welche Geräte sie Zugriff haben sollen, oder ähnliche Arten von Einschränkungen, die eine Differenzierung zwischen Benutzern erfordern.

Um eine Unterscheidung zwischen den Benutzern zu schaffen, müssen Sie:

- Erstellen und richten Sie Rollen ein, die Sie benötigen, um die Geschäftsanforderungen Ihres Unternehmens zu erfüllen
- Fügen Sie Benutzer und Benutzergruppen hinzu, die Sie den Rollen zuordnen, denen sie angehören sollen
- Erstellen Sie Smart Client Profile und Management Client Profile, um festzulegen, was Benutzer in der XProtect Smart Client und Management Client Benutzeroberfläche sehen können.

  Rollen steuern nur Ihre Zugriffsberechtigungen und nicht, was die Benutzer in der Benutzeroberfläche von XProtect Smart Client oder Management Clientsehen können. Sie müssen kein spezielles Management Client Profil für Benutzer erstellen, die Management Clientniemals verwenden.

Um den XProtect Smart Client Benutzern oder Management Client Benutzern mit eingeschränktem Zugang zu den Management Client Funktionen ein optimales Benutzererlebnis zu bieten, sollten Sie sicherstellen, dass die von der Rolle bereitgestellten Berechtigungen und die vom Smart Client oder Management Client Profil bereitgestellten Elemente der Benutzeroberfläche konsistent sind.

> **!** Für den Zugriff auf Management Serverist es wichtig, dass alle Rollen die Sicherheitsberechtigung **Verbinden** aktiviert haben. Die Berechtigung befindet sich unter **Rolleneinstellungen** > **Management Server** > Registerkarte „Gesamtsicherheit“ (Rollen) auf Seite 556.

Um Rollen in Ihrem System zu erstellen, erweitern Sie **Sicherheit** > **Rollen**.

### Berechtigungen einer Rolle

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Wenn Sie eine Rolle in Ihrem System erstellen, können Sie dieser Rolle eine Reihe von Berechtigungen für die Systemkomponenten oder Funktionen zuweisen, auf die die betreffende Rolle zugreifen und sie nutzen kann.

So können Sie beispielsweise Rollen erstellen, die nur über die Berechtigung zum Zugriff auf Funktionen in XProtect Smart Client oder anderen Milestone Anzeige-Clients verfügen und nur bestimmte Kameras anzeigen dürfen. Wenn Sie solche Rollen einrichten, sollten diese keine Zugriffsrechte auf den Management Client haben, sondern sie sollten nur Zugriff auf einige oder alle Funktionen haben, die in XProtect Smart Client oder anderen Clients zu finden sind.

Um diesen Bedarf an Differenzierung zu decken, richten Sie dann eine Rolle ein, die über einige oder die meisten typischen Administratorrechte verfügt, z. B. die Berechtigung zum Hinzufügen und Entfernen von Kameras, Servern und ähnlichen Funktionen. Sie können Rollen erstellen, die einige oder die meisten Berechtigungen eines Systemadministrators haben. Das kann z. B. relevant sein, wenn Ihr Unternehmen zwischen Leuten unterscheiden will, die ein Subnetz des Systems verwalten dürfen und Leuten, die das gesamte System verwalten dürfen.

Rollen geben Ihnen die Möglichkeit, differenzierte Administratorberechtigungen für den Zugriff, die Bearbeitung oder Änderung einer Vielzahl von Systemfunktionen zu vergeben. Zum Beispiel die Berechtigung, die Einstellungen für Server oder Kameras in Ihrem System zu bearbeiten. Diese Berechtigungen weisen Sie auf der Registerkarte **Gesamtsicherheit** zu (siehe Registerkarte „Gesamtsicherheit“ (Rollen) auf Seite 556). Damit der differenzierte Systemadministrator Management Client starten kann, müssen Sie der Rolle Leseberechtigungen auf dem Management-Server gewähren.

> ⚠ Für den Zugriff auf Management Serverist es wichtig, dass alle Rollen die Sicherheitsberechtigung **Verbinden** aktiviert haben. Die Berechtigung befindet sich unter **Rolleneinstellungen** > **Management Server** > Registerkarte „Gesamtsicherheit“ (Rollen) auf Seite 556.

Sie können auch die gleichen Einschränkungen in der Benutzeroberfläche des Management Client s für jede Rolle vornehmen, indem Sie die Rolle mit einem Management Client-Profil verknüpfen, das die entsprechenden eingeschränkten Systemfunktionen von der Benutzeroberfläche hat. Weitere Informationen dazu finden Sie unter Management Client-Profile (Erklärung) auf Seite 76.

Um einer Rolle solche differenzierten Administratorrechte zu geben, muss die Person mit der vollen Standard-Administratorrolle die Rolle unter **Sicherheit** > **Rollen > Registerkarte Info > Neu hinzufügen** einrichten. Wenn Sie die neue Rolle erstellen, können Sie die Rolle mit Ihren eigenen Profilen verknüpfen, genauso wie beim Erstellen einer anderen Rolle im System oder bei der Verwendung der Standardprofile des Systems. Weitere Informationen finden Sie unter Hinzufügen und Verwalten einer Rolle auf Seite 308.

Wenn Sie die Profile festgelegt haben, die mit der Rolle verknüpft werden sollen, gehen Sie zur Registerkarte **Allgemeine Sicherheit**, um die Berechtigungen der Rolle festzulegen.

Die Berechtigungen, die Sie für eine Rolle festlegen können, sind für Ihre verschiedenen Produkte unterschiedlich. Sie können einer Rolle in XProtect Corporate nur alle verfügbaren Berechtigungen geben.

## Privatsphärenausblendung (Erklärung)

Privatsphärenausblendung (Erklärung)

Mit Privatsphärenausblendung können Sie festlegen, welche Bereiche des Videos von einer Kamera Sie mit Privatzonenmasken zu decken wünschen, wenn sie im Client gezeigt werden. Wenn eine Überwachungskamera beispielsweise eine Straße abdeckt, können Sie mit Privatzonenmasken bestimmte Bereiche eines Gebäudes (wie Fenster und Türen) verdecken, um die Privatsphäre der Bewohner zu schützen. In manchen Ländern ist dies eine gesetzliche Anforderung.

Sie können Privatzonenmasken als massiv oder unscharf bestimmen. Die Zonen decken Live-Videos, aufgezeichnete und exportierte Videos.

Verdeckte Bildbereiche werden auf Bereiche im Kamerabild angewendet und dort verriegelt, so dass der verdeckte Bereich den Schwenk- und Zoombewegungen nicht folgt, sondern immer derselbe Bereich des Kamerabildes abgedeckt wird. Auf manchen PTZ-Kameras können Sie an der Kamera selbst positionsbasierte Privatsphärenausblendung aktivieren.

Es gibt zwei Typen von Privatzonenmasken:

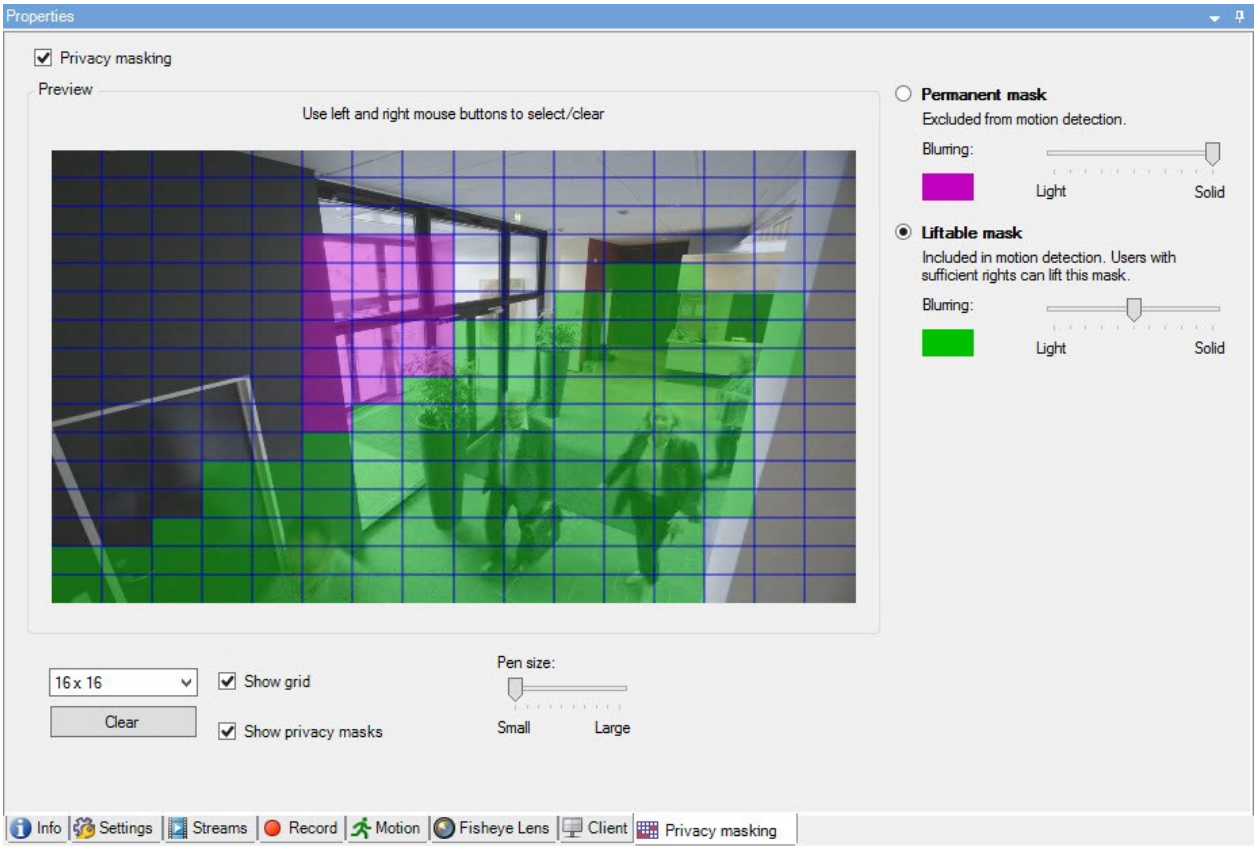
- **Permanente Privatzonenmaske**: Bereiche mit diesem Privatzonenmaskentyp sind in den Clients immer gedeckt. Sie können benutzt werden, um Bereiche des Videos abzudecken, die niemals Überwachung erfordern, wie öffentliche Bereiche oder Bereiche, in denen Überwachung nicht genehmigt ist. Bewegungserkennung ist ausgeschlossen von Bereichen mit permanenten Privatzonenmasken
- **Aufhebbare Privatzonenmaske**: Bereiche mit diesem Maskentyp können in XProtect Smart Client zeitweise aufgedeckt werden, von Benutzern mit der Ermächtigung zum Aufheben von Privatzonenmasken. Wenn der angemeldete XProtect Smart Client-Benutzer nicht über die Berechtigung verfügt, aus Datenschutzgründen verdeckte Bildbereiche aufzudecken, fordert das System, dass ein autorisierter Benutzer das Aufdecken genehmigt.
  Privatzonenmasken werden aufgehoben, bis sie abgelaufen sind oder der Benutzer sie erneut anwendet. Seien Sie sich bewusst, dass Privatzonenmasken auf Video von allen Kameras aufgehoben werden, auf die der Benutzer Zugriff hat

Wenn Sie ein Upgrade von einem 2017 R3-System oder älter vornehmen, in dem Privatzonenmasken angewendet sind, werden diese in aufhebbare Privatzonenmasken umgewandelt.

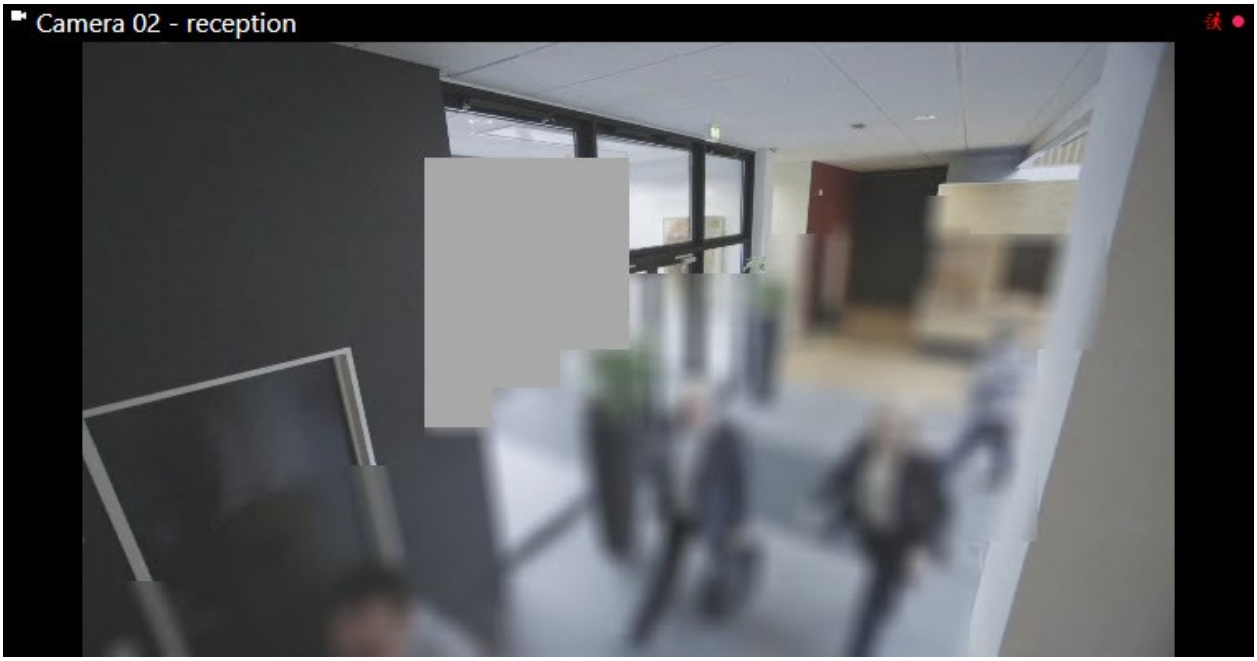
Wenn ein Benutzer Videoaufnahmen von einem Client exportiert oder abspielt, enthält das Video die zum Zeitpunkt der Aufnahme konfigurierten Privatzonenmasken, auch wenn Sie diese später geändert oder entfernt haben. Wenn der Datenschutz beim Exportieren aufgehoben wird, enthält das exportierte Video **nicht** die aufhebbaren Privatzonenmasken.

> Wenn Sie die Einstellungen der Privatsphärenausblendung oft ändern, beispielsweise einmal pro Woche, kann Ihr System potenziell überlastet werden.

Beispiel der Registerkarte **Privatsphärenausblendung** mit konfigurierten Privatzonenmasken:




Und so erscheinen sie in den Clients:




Sie können den Client über die Einstellungen der permanenten und aufhebbaren Privatzonenmasken informieren.

## Management Client-Profile (Erklärung)

Management Client Profile ermöglichen es Systemadministratoren, die Management Client-Benutzeroberfläche für andere Benutzer zu ändern. Ordnen Sie Management Client-Profile Rollen zu, damit die Benutzeroberfläche nur die Funktionen der jeweiligen Administratorrolle anzeigt.

Management Client-Profile regeln nur die visuelle Aufstellung von Systemfunktionen, nicht den tatsächlichen Zugriff dazu. Allgemein wird der Zugang zu Systemfunktionen über die Rolle gewährt, mit der der einzelne Benutzer verknüpft ist. Weitere Informationen dazu, wie der Zugriff auf Systemfunktionen für eine Rolle allgemein verwaltet wird, finden Sie unter Verwaltung der Sichtbarkeit von Funktionen für ein Management Client-Profil.

Sie können die Einstellungen für die Sichtbarkeit aller Management Client-Elemente ändern. Standardmäßig können über das Management Client-Profil alle Funktionen im Management Client angezeigt werden.

## Smart Client Profile (Erklärung)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Alle Benutzer in Milestone XProtect VMS gehören zu einer Rolle, mit der ein Smart Client Profil verbunden ist.

Rollen definieren die Berechtigungen der Benutzer, und die Smart Client Profile legen fest, was die Benutzer auf der XProtect Smart Client Benutzeroberfläche sehen können.

Alle Milestone XProtect VMS Installationen enthalten ein Standard-Smart Client-Profil, das mit einer Standardkonfiguration eingerichtet ist, um die meisten der im System Ihres Unternehmens verfügbaren Konfigurationen anzuzeigen. Einige Einstellungen sind standardmäßig immer deaktiviert.

In Fällen, in denen Sie mehrere verschiedene Rollen in einer Organisation haben, möchten Sie vielleicht Funktionen deaktivieren, auf die eine bestimmte Rolle in XProtect Smart Client keinen Zugriff hat/sollte.

Sie könnten zum Beispiel eine Rolle haben, deren tägliche Arbeit keine Videowiedergabe erfordert. Zu diesem Zweck können Sie ein neues Smart Client Profil für diese Rolle erstellen, in dem Sie den **Wiedergabemodus**deaktivieren. Wenn Sie diese Einstellung im Smart Client Profil deaktivieren, können XProtect Smart Client Benutzer mit einer Rolle, die dieses Smart Client Profil verwendet, den **Wiedergabemodus** in ihrer XProtect Smart Client Benutzeroberfläche nicht mehr sehen.

Es ist wichtig zu beachten, dass Smart Client Profile hauptsächlich steuern, was Benutzer in der XProtect Smart Client Benutzeroberfläche sehen können, und nicht die tatsächlichen Zugriffsberechtigungen der Rolle. Diese Zugriffsrechte, wie z. B. der Zugriff auf das Lesen, Ändern oder Löschen, werden in den Rolleneinstellungen gesteuert. So können XProtect Smart Client Benutzer über ihre Rolle Berechtigungen für Funktionen haben, die sie auf der Benutzeroberfläche nicht sehen können, weil sie im Smart Client Profil deaktiviert sind.

Um den XProtect Smart Client Benutzern ein optimales Erlebnis zu bieten, sollten Sie sicherstellen, dass die von der Rolle bereitgestellten Berechtigungen und die vom Smart Client Profil bereitgestellten Elemente der Benutzeroberfläche konsistent sind.

Um Smart Client Profile zu erstellen oder zu bearbeiten, erweitern Sie **Client** und wählen Sie **Smart Client Profile**.

Sie können außerdem etwas über die Beziehungen zwischen Smart Client Profilen, Rollen und Zeitprofilen herausfinden, sowie darüber, wie diese zusammen verwendet werden können (siehe Erstellen und Einrichten von Smart Client-Profilen, Rollen und Zeitprofilen auf Seite 283).

## Beweissicherung (Erklärung)

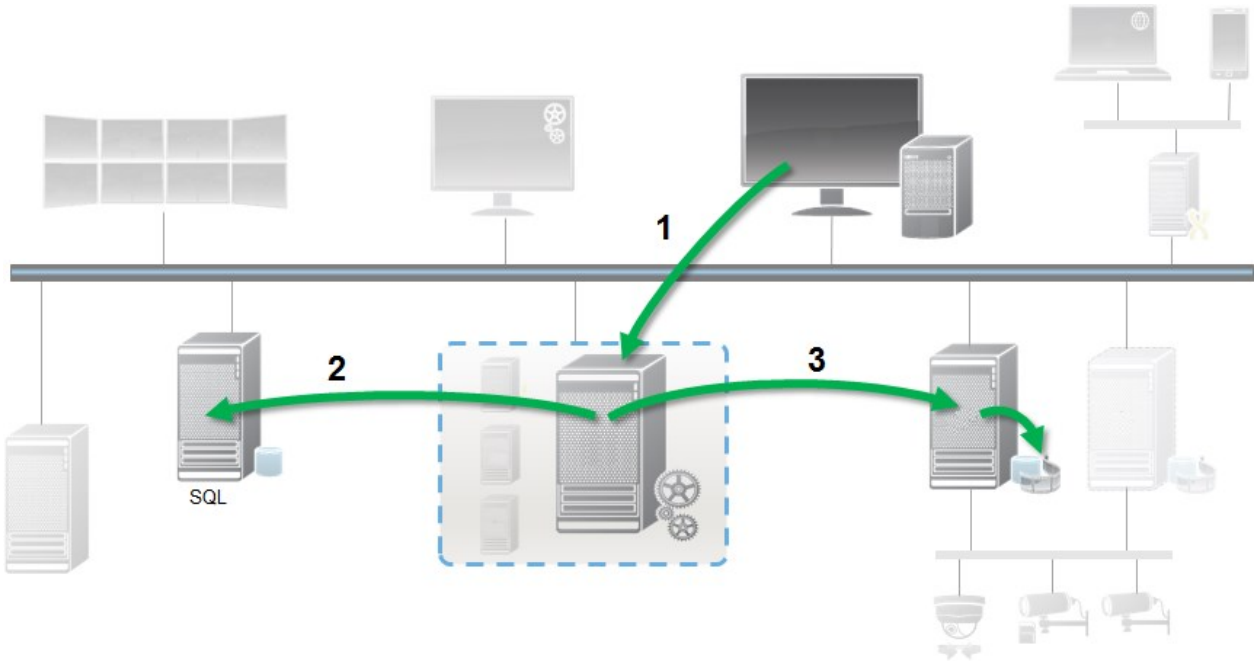
Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Ab XProtect VMS Version 2020 R2 ist es bei einem Upgrade des Management Servers von einer früheren Version erst wieder möglich, Beweissicherungen auf Aufzeichnungsservern zu erstellen oder zu ändern, die zur Version 2020 R1 oder früher gehören, wenn diese Aufzeichnungsserver aktualisiert wurden.
Das bedeutet auch, dass wenn die Hardware von einem Aufzeichnungsserver (von 2020 R1 oder früher) auf einen anderen Aufzeichnungsserver umgezogen ist und sich darauf noch Aufzeichnungen befinden, die Beweissicherung nicht erstellt oder geändert werden kann.

Mit der Funktionalität Beweissicherung können Client-Anwender Videosequenzen, einschließlich Audio und andere Daten vor dem Löschen schützen, falls erforderlich, z. B. bei einer laufenden Untersuchung oder einem laufenden Gerichtsverfahren. Weitere Informationen finden Sie im Benutzerhandbuch für XProtect Smart Client.

Sofern geschützt, können Daten nicht gelöscht werden, weder automatisch vom System nach der standardmäßigen Speicherzeit oder in anderen Situationen, noch manuell vom Client-Benutzer. Das System oder ein Benutzer kann die Daten erst löschen, wenn ein Benutzer mit ausreichenden Benutzerrechten die Beweismittel freigibt.

Flussdiagramm für Beweissicherung:




1. Ein XProtect Smart Client Benutzer erstellt eine Beweissicherung. Information wird an den Management-Server gesendet.
2. Der Management Server speichert die Informationen zur Beweissicherung in der SQL Server-

Datenbank.

3. Der Management-Server informiert den Aufzeichnungsserver darüber, die geschützten Aufzeichnungen in der Datenbank zu speichern und sicherzustellen.

Wenn der Anwender eine Beweissicherung erstellt, bleiben die geschützten Daten am Speicherort der Aufzeichnungen und werden dann an archivierende Festplatten zusammen mit den ungeschützten Daten verschoben. Allerdings gilt für die geschützten Daten:

- Folgen der Speicherzeit, die für die Beweissicherung festgelegt wurde. Potentiell unendlich
- Behält die ursprüngliche Qualität der Aufzeichnungen bei, auch wenn die Ausdünnung für ungeschützte Daten eingestellt wurde

Wenn ein Anwender Sicherungen erstellt, beträgt die minimale Größe einer Sequenz den Zeitraum, in dem die Datenbank die aufgezeichneten Dateien aufteilt; Standard-Einstellung sind einstündige Sequenzen. Sie können dies ändern, allerdings erfordert das eine Anpassung der Datei RecorderConfig.xml auf dem Aufzeichnungsserver. Wenn sich eine kleine Sequenz über zwei einstündige Zeiträume hinauszieht, sichert das System die Aufzeichnungen jeweils in beiden Zeiträumen.

Im Auditprotokoll im Management Client können Sie sehen, wenn ein Benutzer Beweissicherungen erstellt, bearbeitet oder gelöscht.

Sollte eine Festplatte nicht mehr genügend Speicherplatz haben, sind geschützte Daten nicht betroffen. Stattdessen werden die ältesten nicht geschützten Daten gelöscht. Wenn dem System keine ungeschützten Daten zum Löschen mehr zur Verfügung stehen, wird die Aufzeichnung angehalten. Sie können Regeln und Alarme erstellen, die bei Ereignissen mit vollem Speicherplatz auslösen und Sie so automatisch benachrichtigen.

Die Funktion der Beweissicherung beeinflusst nicht die Systemleistung, außer dass mehr Daten für einen längeren Zeitraum gespeichert werden und daher die Speicherkapazität beeinträchtigen könnte.

Wenn Sie mit Hardware (siehe Hardware verschieben auf Seite 368) auf einen anderen Aufzeichnungsserver umziehen:

- Durch Beweismittelsicherung geschützte Aufzeichnungen verbleiben auf dem alten Aufzeichnungsserver für die Speicherdauer, die festgelegt wurde, als die Beweismittelsicherung erstellt wurde
- Der XProtect Smart Client-Benutzer kann weiterhin Daten mit einer Beweissicherung in den Aufzeichnungen schützen, die auf einer Kamera gemacht wurden, bevor diese zu einem anderen Aufzeichnungsserver verschoben wurde. Selbst wenn Sie die Kamera mehrmals verschieben und die Aufzeichnungen auf mehreren Aufzeichnungsservern gespeichert werden

Standardmäßig ist allen Bedienern das Standard-Evidence-Lock-Profil zugewiesen, aber keine Benutzerzugriffsberechtigungen für die Funktion. Um die Zugriffsrechte einer Rolle für die Beweissicherung festzulegen, siehe die Registerkarte Gerät (Rollen) für Rolleneinstellungen. Zur Angabe des Beweissicherungsprofils als Rolle siehe die Registerkarte Info (Rollen) für die Einstellungen einer Rolle.

Im Management Client können Sie die Eigenschaften des Standard-Beweissicherungsprofils bearbeiten und weitere Beweissicherungsprofile erstellen und diese stattdessen den Rollen zuweisen.

# Regeln und Ereignisse

## Regeln (Erklärung)

Regeln bestimmen Aktionen, die unter bestimmten Bedingungen ausgeführt werden. Beispiel: Wenn eine Bewegung erkannt wird (Bedingung), startet eine Kamera die Aufzeichnung (Aktion).

Nachfolgend sind **Beispiele** für Anwendungen der Regeln aufgelistet:

- Starten und Anhalten der Aufzeichnung
- Nicht-standardmäßige Livebildrate einstellen
- Nicht-standardmäßige Aufzeichnungsbildrate einstellen
- Starten und Beenden des PTZ-Wachrundgangs
- Pausieren und Wiederaufnahme des PTZ-Wachrundgangs
- Bewegung der PTZ-Kameras zu bestimmten Positionen
- Status des Ausgangs als aktiviert/deaktiviert einstellen
- Senden von Benachrichtigungen per E-Mail
- Erstellen von Protokolleinträgen
- Ereignisse erstellen
- Übernehmen von neuen Geräteeinstellungen, beispielsweise eine andere Auflösung einer Kamera
- Videos in Matrix-Empfängern erscheinen lassen
- Starten und Anhalten von Plug-ins
- Starten und Beenden von Geräte-Feeds

Das Anhalten eines Geräts bedeutet, dass das Videosignal nicht mehr vom Gerät auf das System übertragen wird, wodurch Sie keine Videos live sehen und aufnehmen können. Im Gegensatz dazu kann ein Gerät, für das Sie den Feed angehalten haben, jedoch weiterhin mit dem Aufzeichnungsserver kommunizieren und Sie können den Feed vom Gerät über eine Regel automatisch starten – anders als wenn das Gerät manuell im Management Client deaktiviert wurde.

> ⚠ Für einige Regeln kann es erforderlich sein, dass bestimmte Funktionen für die entsprechenden Geräte aktiviert sind. Beispiel: Eine Regel, die bestimmt, dass eine Kamera aufzeichnet, funktioniert nicht wie beabsichtigt, wenn die Aufzeichnung für die entsprechende Kamera nicht aktiviert ist. Vor dem Erstellen einer Regel empfiehlt Milestone, dass Sie überprüfen, ob die entsprechenden Geräte die beabsichtigte Aktion durchführen können.

### Regelkomplexität

Die genaue Anzahl der Optionen hängt vom Typ der Regel ab, die Sie erstellen möchten, und von der Anzahl der Geräte, die auf Ihrem System verfügbar sind. Regeln bieten ein hohes Maß an Flexibilität: Sie können Ereignis- und Zeitbedingungen kombinieren, mehrere Aktionen in einer einzigen Regel angeben und sehr oft Regeln erstellen, die mehrere oder alle Geräte in Ihrem System abdecken.

Sie können Ihre Regeln so einfach oder komplex wie erforderlich gestalten. Sie können zum Beispiel sehr einfache zeitbasierte Regeln erstellen:

| Beispiel | Erläuterung |
|---|---|
| **Sehr einfache zeitbasierte Regel** | Montags zwischen 08:30 Uhr und 11:30 Uhr (Zeitbedingung) beginnen Kamera 1 und Kamera 2 die Aufzeichnung (Aktion), wenn der Zeitraum beginnt und beenden die Aufzeichnung (Aktion anhalten), wenn der Zeitraum endet. |
| **Sehr einfache ereignisbasierte Regel** | Wenn Bewegung auf Kamera 1 erkannt wird (Ereignisbedingung), beginnt Kamera 1 sofort die Aufzeichnung (Aktion) und beendet die Aufzeichnung dann nach 10 Sekunden (Aktion beenden).<br>Auch wenn eine ereignisbasierte Regel durch ein Ereignis auf einem Gerät aktiviert wird, können Sie bestimmen, dass Aktionen auf einem oder mehreren anderen Geräten erfolgen sollen. |
| **Regel mit mehreren Geräten** | Wenn Bewegung auf Kamera 1 erkannt wird (Ereignisbedingung), beginnt Kamera 2 sofort die Aufzeichnung (Aktion) und die Sirene, die mit Ausgang 3 verbunden ist, wird sofort aktiviert (Aktion). Nach 60 Sekunden soll Kamera 2 dann die Aufnahme anhalten (Aktion beenden) und die Sirene, die mit Ausgang 3 verbunden ist, wird deaktiviert (Aktion beenden). |
| **Regel, die Zeit, Ereignisse und Geräte kombiniert** | Wenn Bewegung auf Kamera 1 erkannt wird (Ereignisbedingung) und der Wochentag ein Samstag oder Sonntag ist (Zeitbedingung), beginnen Kamera 1 und Kamera 2 sofort die Aufzeichnung (Aktion) und es wird eine Benachrichtigung an die Sicherheitsleitung gesendet (Aktion). 5 Sekunden später, wenn keine Bewegung mehr auf Kamera 1 oder Kamera 2 erkannt wird, halten die beiden Kameras die Aufzeichnung an (Aktion beenden). |

Den Anforderungen und Bedürfnissen Ihres Unternehmens entsprechend, ist es in vielen Fällen besser viele einfache Regeln zu erstellen als einige wenige komplexe Regeln. Auch wenn dies bedeutet, dass Sie mehr Regeln in Ihrem System haben, können Sie dadurch auf einfache Weise einen Überblick über die

Auswirkungen Ihrer Regeln behalten. Wenn Sie Ihre Regeln einfach halten, haben Sie auch eine größere Flexibilität beim Deaktivieren/Aktivieren von einzelnen Regelbestandteilen. Mit einfachen Regeln können Sie bei Bedarf gesamte Regeln deaktivieren/aktivieren.

## Regeln und Ereignisse (Erklärung)

**Regeln** sind ein zentrales Element Ihres Systems. Regeln bestimmen äußerst wichtige Einstellungen, beispielsweise wann Kameras aufzeichnen sollten, wann PTZ-Kameras Wachrundgänge ausführen sollten, wann Benachrichtigungen verschickt werden sollten, etc.

Beispiel - Eine Regel, die festlegt, dass eine bestimmte Kamera die Aufzeichnung starten sollte, sobald sie eine Bewegung registriert:


**Ereignisse** sind zentrale Elemente bei der Anwendung des Assistenten **Regel verwalten**. In diesem Assistenten werden Ereignisse primär zur Auslösung von Aktionen verwendet. Sie können beispielsweise eine Regel erstellen, die festlegt, dass beim **Ereignis** Bewegungsregistrierung das Überwachungssystem die **Aktion** ausführen sollte, von einer bestimmten Kamera aus mit der Videoaufzeichnung zu beginnen.

Die folgenden Arten von Bedingungen können Regeln auslösen:

| Name | Beschreibung |
|---|---|
| **Ereignisse** | Wenn im Überwachungssystem Ereignisse auftreten, beispielsweise sobald Bewegungen registriert werden, oder das System Informationen von externen Sensoren empfängt. |
| **Zeitintervall** | Wenn Sie bestimmte Zeiträume eingeben, zum Beispiel:<br>`Thursday 16th August 2007 from 07.00 to 07.59`<br>oder `every Saturday and Sunday` |
| **Failover-Zeitintervall** | Zeiträume, in denen Failover aktiv oder inaktiv ist. |
| **Wiederholte** | Wenn Sie eine Aktion einrichten, die nach einem detaillierten, sich wiederholenden |

| Name | Beschreibung |
|---|---|
| **Zeit** | Zeitplan ausgeführt werden soll.<br>Beispielsweise:<br>• Jede Woche Dienstags, alle 1 Stunde(n) zwischen 15:00 und 15:30<br>• Am 15. alle 3 Monat(e) um 11:45 Uhr<br>• Jeden Tag alle 1 Stunde(n) zwischen 15:00 und 19:00 Uhr<br>Die Zeit basiert auf den örtlichen Zeiteinstellungen des Servers, auf dem Management Client installiert ist. |

Sie können mit folgenden Punkten unter **Regeln und Ereignisse** arbeiten:

- **Regeln**: Regeln sind ein zentrales Element des Systems. Das Verhalten Ihres Überwachungssystems wird maßgeblich durch Regeln bestimmt. Wenn Sie eine Regel erstellen, können Sie mit allen möglichen Ereignistypen arbeiten
- **Zeitprofile**: Zeitprofile sind im Management Client definierte Zeiträume. Sie verwenden sie beim Erstellen von Regeln im Management Client, z. B. um eine Regel zu erstellen, die festlegt, dass in einem bestimmten Zeitprofil eine bestimmte Aktion ausgeführt werden soll
- **Benachrichtigungsprofile**: Sie können Benachrichtigungsprofile zum Einstellen gebrauchsfertiger E-Mail-Benachrichtigungen verwenden, die automatisch von Regeln ausgelöst werden können, z. B. beim Eintreten eines bestimmten Ereignisses
- **Benutzerdefinierte Ereignisse**: Benutzerdefinierte Ereignisse sind maßgeschneiderte Ereignisse, die es Benutzern ermöglichen, Ereignisse im System manuell auszulösen oder auf Eingänge des Systems zu reagieren
- **Analyseereignisse**: Analyseereignisse sind Daten, die von externen Drittanbietern für Analysen von Videoinhalten (Video Content Analysis - VCA) erhalten werden. Sie können Analyseereignisse als Basis für Alarme verwenden
- **Generische Ereignisse**: Generische Ereignisse ermöglichen es Ihnen, Aktionen im XProtect Event-Server auszulösen, indem einfache Zeichenketten über das IP-Netzwerk an Ihr System gesendet werden

## Zeitprofile (Erklärung)

> Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

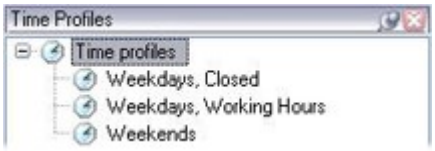
Zeitprofile sind vom Administrator definierte Zeiträume. Sie können Zeitprofile beim Erstellen von Regeln verwenden, z. B. eine Regel, die festlegt, dass in einem bestimmten Zeitraum eine bestimmte Aktion ausgeführt werden soll.

Zeitprofile sind zusammen mit Smart Client-Profilen auch Rollen zugeteilt. Standardmäßig sind alle Rollen dem Standardzeitprofil **Immer** zugeteilt. Das heißt Mitglieder von Rollen, denen dieses Standardzeitprofil zugeordnet ist, haben keine zeitlichen Beschränkungen für ihre Benutzerrechte im System. Sie können einer Rolle auch ein alternatives Zeitprofil zuteilen.

Zeitprofile sind äußerst flexibel: Sie können sie auf Basis eines oder mehrerer einzelner Zeiträume oder eines oder mehrerer wiederkehrender Zeiträume oder einer Kombination einzelner und wiederkehrender Zeiträume festlegen. Viele Benutzer sind evtl. mit den Konzepten einzelner und wiederkehrender Zeiträume aus Kalenderanwendungen vertraut, wie z.B. der in Microsoft® Outlook.

Zeitprofile gelten immer für die Ortszeit. Das bedeutet, dass wenn sich Ihre Aufzeichnungsserver in verschiedenen Zeitzonen befinden, alle Aktionen (zum Beispiel Kameraaufzeichnungen) hinsichtlich der Zeitprofile zur Ortszeit des jeweiligen Aufzeichnungsservers ausgeführt werden. Beispiel: Wenn Sie ein Zeitprofil haben, das den Zeitraum zwischen 08:30 und 09:30 Uhr abdeckt, werden alle damit verbundenen Aktionen auf einem Aufzeichnungsserver in New York zur Ortszeit zwischen 08:30 bis 09:30 Uhr ausgeführt. Die gleichen Aktionen werden auf einem Aufzeichnungsserver in Los Angeles erst einige Stunden später ausgeführt, nämlich zur dortigen Ortszeit zwischen 08:30 bis 09:30 Uhr.

Sie können Zeitprofile durch Erweitern von **Regeln und Ereignisse** > **Zeitprofile** erstellen und verwalten. Die Liste **Zeitprofile** wird geöffnet. Nur ein Beispiel:




Eine Alternative zu den Zeitprofilen finden Sie unter Tageslängen-Zeitprofil (Erklärung).

## Tageslängen-Zeitprofile (Erklärung)

Wenn Sie Kameras im Freien aufstellen, müssen Sie oftmals die Kameraauflösung verringern, schwarz/weiß aktivieren oder andere Einstellungen ändern, wenn es dunkel oder hell wird. Je weiter die Kameras nördlich oder südlich vom Äquator entfernt sind, desto stärker variieren die Sonnenaufgangs- und -untergangszeiten im Jahresverlauf. Deshalb ist es unmöglich, feste Standardzeitprofile für die Anpassung der Kameraeinstellungen entsprechend den Lichtverhältnissen zu verwenden.

In solchen Situationen können Sie stattdessen Tageslängen-Zeitprofile erstellen, um den Sonnenaufgang und -untergang für ein bestimmtes geografisches Gebiet zu definieren. Über die geographischen Koordinaten berechnet das System die Zeit des Sonnenauf- und Untergangs und bezieht sogar täglich die Sommerzeit mit ein. Dadurch folgt das Zeitprofil automatisch den jährlichen Veränderungen des Sonnenaufgangs und -untergangs im ausgewählten Gebiet, sodass das Profil nur dann aktiv ist, wenn es gebraucht wird. Alle Zeiten und Daten richten sich nach den Zeit- und Datumseinstellungen des Management-Servers. Sie können auch einen positiven oder negativen Offsetwert (in Minuten) für die Startzeit (Sonnenaufgang) und Endzeit (Sonnenuntergang) einstellen. Der Offsetwert für die Start- und Endzeit kann identisch oder unterschiedlich sein.

Sie können Tageslängenprofile beim Erstellen von Regeln und Rollen verwenden.

## Benachrichtigungsprofile (Erklärung)

Mit Benachrichtigungsprofilen können Sie vorgefertigte E-Mail-Benachrichtigungen einstellen. Benachrichtigungen können automatisch von Regeln ausgelöst werden können, z. B. wenn ein bestimmtes Ereignis eintritt.

Wenn Sie das Benachrichtigungsprofil erstellen, geben Sie einen Benachrichtigungstext ein und entscheiden, ob Sie Standbilder und AVI-Videoclips in die E-Mail-Benachrichtigungen aufnehmen wollen.

> Außerdem kann es erforderlich sein, mögliche E-Mailscanner zu deaktivieren, welche die Anwendung vom Versenden der E-Mailbenachrichtigungen abhalten.

### Anforderungen an die Erstellung von Benachrichtigungsprofilen

Bevor Sie ein Benachrichtigungsprofil erstellen können, müssen Sie die Einstellungen für den ausgehenden Mailserver für die E-Mailbenachrichtigungen festlegen.

Sie können die Kommunikation zum Mailserver sichern, wenn Sie die nötigen Sicherheitszertifikate auf dem Mailserver installieren.

Wenn Sie AVI-Videoclips in die E-Mailbenachrichtigungen einbinden können möchten, müssen Sie auch die Komprimierungseinstellungen dafür festlegen:

1. Gehen Sie zu **Werkzeuge** > **Optionen**. Dadurch öffnet sich das Fenster **Optionen**.
2. Konfigurieren Sie den Mail-Server auf der Registerkarte **Mail Server** (Registerkarte „Mailserver“ (Optionen) auf Seite 417) und die Kompressionseinstellungen auf der Registerkarte **AVI Generation** Registerkarte „AVI-Generierung“ (Optionen) auf Seite 418.

## Benutzerdefinierte Ereignisse (Erklärung)

Wenn das von Ihnen benötigte Ereignis nicht in der Liste **Ereignisübersicht** auftaucht, können Sie Ihre eigenen benutzerdefinierten Ereignisse erstellen. Benutzen Sie solche benutzerdefinierte Ereignisse, um andere Systeme in Ihr Überwachungssystem zu integrieren.

Durch benutzerdefinierte Ereignisse, ist es Ihnen möglich Daten eines Zutrittskontrollsystems von Dritten als Ereignisse in das System einzuspeisen. Die Ereignisse können später Aktionen auslösen. Auf diese Weise können Sie beispielsweise Video von relevanten Kameras aufzeichnen lassen, sobald jemand das Gebäude betritt.

Sie können also benutzerdefinierte Ereignisse für manuell ausgelöste Ereignisse verwenden, während Sie Live-Video in XProtect Smart Client ansehen oder sogar automatisch, wenn Sie diese in Regeln benutzen. Zum Beispiel: wenn benutzerdefiniertes Ereignis 37 geschieht, sollte PTZ-Kamera 224 aufhören zu überwachen und zur Preset Position 18 gehen.

Über Rollen definieren Sie, welche Benutzer die benutzerdefinierten Ereignisse auslösen können. Sie können bei Bedarf benutzerdefinierte Ereignisse auf zwei Arten und zur selben Zeit verwenden:

| Ereignisse | Beschreibung |
|---|---|
| **Für die Bereitstellung der Fähigkeit, manuell Ereignisse in XProtect Smart Client** auszulösen | In diesem Falle ermöglichen es benutzerdefinierte Ereignisse den Endbenutzern manuell Ereignisse auszulösen, während sie Live-Video in XProtect Smart Client ansehen. Wenn ein benutzerdefiniertes Ereignis auftritt, weil ein Benutzer von XProtect Smart Client es manuell auslöst, kann eine Regel dafür sorgen, dass eine oder mehr Aktionen im System stattfinden sollen. |
| **Für die Bereitstellung der Fähigkeit Ereignisse über API auszulösen** | In diesem Fall können Sie benutzerdefinierte Ereignisse außerhalb des Überwachungssystem auslösen. Das Verwenden von benutzerdefinierten Ereignissen auf diese Weise erfordert, dass ein eigenes API (Application Program Interface. Eine Reihe von Bausteinen für die Erstellung oder Anpassung von Softwareanwendungen) verwendet wird, wenn das benutzerdefinierte Ereignis ausgelöst wird. Eine Authentifizierung durch das Active Directory ist erforderlich, um ein benutzerdefiniertes Ereignis auf diese Art zu verwenden. Dies gewährleistet, dass auch wenn benutzerdefinierte Ereignisse außerhalb des Überwachungssystems ausgelöst werden können, dies nur durch autorisierte Benutzer geschehen kann.<br><br>Des weiteren können benutzerdefinierte Ereignisse über API mit Metadaten verbunden werden, die gewisse Geräte oder Gerätegruppen definieren. Dies ist besonders nützlich, wenn benutzerdefinierte Ereignisse genutzt werden, um Regeln auszulösen, denn Sie vermeiden es eine Regel für jedes Gerät zu haben, die im Grunde das gleiche ausführen. Beispiel: Ein Unternehmen verwendet eine Zutrittskontrolle bei 35 Eingängen, jedes mit einem Zutrittskontrollgerät. Wenn ein Zutrittskontrollgerät aktiviert wird, löst ein benutzerdefiniertes Ereignis im System aus. Dieses benutzerdefinierte Ereignis startet mittels einer Regel die Aufzeichnung einer Kamera, die mit diesem aktiviertem Zutrittskontrollgerät verbunden ist. In den Metadaten wird festgelegt, welche Kamera welcher Regel |

| Ereignisse | Beschreibung |
|---|---|
| | folgt. Auf diese Art und Weise muss das Unternehmen nicht 35 verschiedene benutzerdefinierte Ereignisse einrichten und mittels zugehöriger 35 Regeln auslösen. Ein einzelnes benutzerdefiniertes Ereignis und eine einzelne Regel sind ausreichend.<br><br>Wenn Sie benutzerdefinierte Ereignisse auf diese Art verwenden, stehen diese gegebenenfalls nicht immer für eine manuelle Auslösung in XProtect Smart Client zur Verfügung. Sie können Rollen nutzen, um die Sichtbarkeit von benutzerdefinierten Ereignissen in XProtect Smart Client festzulegen. |

## Analyseereignisse (Erklärung)

Analyseereignisse werden typischerweise zum Empfang von Daten von Video-Content-Analyse-Lösungen (CVA) von anderen Herstellern benutzt.

Die Verwendung von Analyseereignissen als Grundlage für Alarme ist ein Prozess mit drei Schritten:

- Erster Schritt: Aktivierung der Funktion der Analyseereignisse und Durchführung der zugehörigen Sicherheitseintellungen. Durch die Verwendung einer Liste zugelassener Adressen kann gesteuert werden, wer Ereignisdaten an das System senden kann und auf welchen Port der Server reagiert
- Zweiter Schritt: Erstellung des Analyseereignisses, wenn möglich mit einer Beschreibung und Test des Ereignisses
- Dritter Schritt: Verwendung des Analyseereignisses als Quelle für die Definition eines Alarms

Sie können Analyseereignisse in der Liste **Regeln und Ereignisse** im Bereich **Standort-Navigation** einstellen.

Zur Verwendung von auf VCA basierenden Ereignissen, ist ein VCA-Tool Dritter nötig, um das System mit Daten zu versorgen. Welches VCA-Tool Sie benutzen möchten liegt dabei ganz bei Ihnen, so lange die Daten aus dem Tool dem richtigen Format entsprechen. Dieses Format wird in der MIP SDK Dokumentation zu Analyseereignissen erläutert.

Detaillierte Informationen erhalten Sie von Ihrem Systemanbieter. VCA-Tools von Drittanbietern werden von unabhängigen Partnern entwickelt, die Lösungen auf Grundlage einer Open-Platform von Milestone anbieten. Diese Lösungen können Einfluss auf die Leistung des Systems haben.

## Generische Ereignisse (Erklärung)

Generische Ereignisse ermöglichen es Ihnen, Aktionen im XProtect Event-Server auszulösen, indem einfache Zeichenketten über das IP-Netzwerk an Ihr System gesendet werden.

Sie können jede Hardware oder Software verwenden, die Strings über TCP oder UDP versenden kann, um generische Ereignisse auszulösen. Ihr System kann erhaltene TCP- oder UDP-Datenpakete analysieren und automatisch generische Ereignisse auslösen, wenn bestimmte Bedingungen erfüllt sind. Auf diese Weise können Sie in Ihr System externe Quellen, z. B. Zutrittskontrollsysteme und Alarmsysteme integrieren. Das Ziel besteht darin, so vielen externen Quellen wie möglich zu erlauben, mit dem System zu interagieren.

Mit dem Konzept der Datenquellen vermeiden Sie Drittanbieter-Tools verwenden zu müssen, um den Standards Ihres Systems gerecht werden zu können. Mithilfe der Datenquellen können Sie mit einem bestimmten Teil Ihrer Hardware oder Software über einen bestimmten IP-Port kommunizieren und die Interpretation der Bytes, die an diesem Port ankommen, optimieren. Jeder generische Ereignistyp hängt mit einer Datenquelle zusammen und stellt eine Sprache dar, die für die Kommunikation mit einem bestimmten Teil der Hardware oder Software verwendet wird.

Die Arbeit mit Datenquellen erfordert allgemeine Kenntnisse über IP-Netzwerke und Fachkenntnisse über die jeweilige Hardware oder Software, die Sie als Interface verwenden möchten. Es gibt viele Parameter, die Sie verwenden können und keinen vorgefertigten Lösungsweg, nach dem Sie vorgehen müssen. Grundsätzlich gilt, dass Ihr System die Tools, aber nicht die Lösung liefert. Im Gegensatz zu benutzerdefinierten Ereignissen gibt es bei generischen Ereignissen keine Authentifizierung. Dadurch sind sie einfacher auszulösen, aber damit die Sicherheit nicht gefährdet wird, werden nur Ereignisse von lokalen Hosts akzeptiert. Sie können andere Client-IP-Adressen von der Registerkarte **generische Ereignisse** des Menüs **Optionen** zulassen.

## Webhooks (erklärt)

Webhooks sind HTTP Anfragen, die Webanwendungen ermöglichen, miteinander zu kommunizieren. Sie erleichtern die Übertragung von Echtzeitdaten von einer Anwendung auf eine andere, wenn ein vordefiniertes Ereignis auftritt, zum Beispiel das Senden von Ereignisdaten an einen vordefinierten Webhook-Endpunkt, wenn sich ein Benutzer am System anmeldet oder wenn eine Kamera einen Fehler meldet.

Ein Webhook-Endpunkt (Webhook URL) ist die vordefinierte Adresse, an die die Ereignisdaten gesendet werden sollen, ähnlich wie eine Einweg-Telefonnummer.

Sie können Webhooks verwenden, um Integrationen zu erstellen, die ausgewählte Ereignisse in XProtect abonnieren. Wenn ein Ereignis ausgelöst wird, wird ein HTTP POST an den Webhook-Endpunkt gesendet, den Sie für dieses Ereignis definiert haben. Der HTTP POST-Body enthält Ereignisdaten in JSON.

Webhooks fragen das System nicht nach Daten oder ausgelösten Ereignissen ab. Stattdessen sendet das System beim Eintreten eines Ereignisses Ereignisdaten an den Webhook-Endpunkt, wodurch Webhooks im Vergleich zu Abfrage-Lösungen weniger Ressourcen beanspruchen und schneller eingerichtet werden können.

Webhooks können so eingerichtet werden, dass sie mit oder ohne Verwendung von Codeskripten integriert werden können.

> ⚠ Sie sollten sich vergewissern, dass die von XProtect gesendeten Ereignisdaten den in Ihrem Land geltenden Rechtsvorschriften zum Schutz von Daten und Privatsphäre entsprechen.

Die Webhooks-Funktionalität ist ab XProtect 2023R1 standardmäßig installiert und einsatzbereit und zeigt die **Webhooks** Aktion auf der Registerkarte **Regeln** in Management Client.

# Alarme

## Alarme (Erklärung)

Diese Funktion ist nur verfügbar, wenn XProtect Event Server installiert ist.

Dieser Abschnitt beschreibt, wie Sie Alarme einstellen können, die, durch Ereignisse ausgelöst, im System erscheinen sollen.

Auf Basis der Funktionalität im Event-Server bietet die Alarmfunktion einen allgemeinen Überblick sowie Kontrolle und Skalierbarkeit für Alarme in einer beliebigen Anzahl von Installationen (einschließlich weiterer XProtect-Systeme) innerhalb Ihres Unternehmens. Sie können die Funktion so konfigurieren, dass Alarme auf Folgendem basieren können:

- **Interne systembezogene Ereignisse**

  Zum Beispiel Bewegung, Server antwortet/antwortet nicht, Archivierungsprobleme, zu wenig Speicherplatz usw.

- **Externe integrierte Ereignisse**

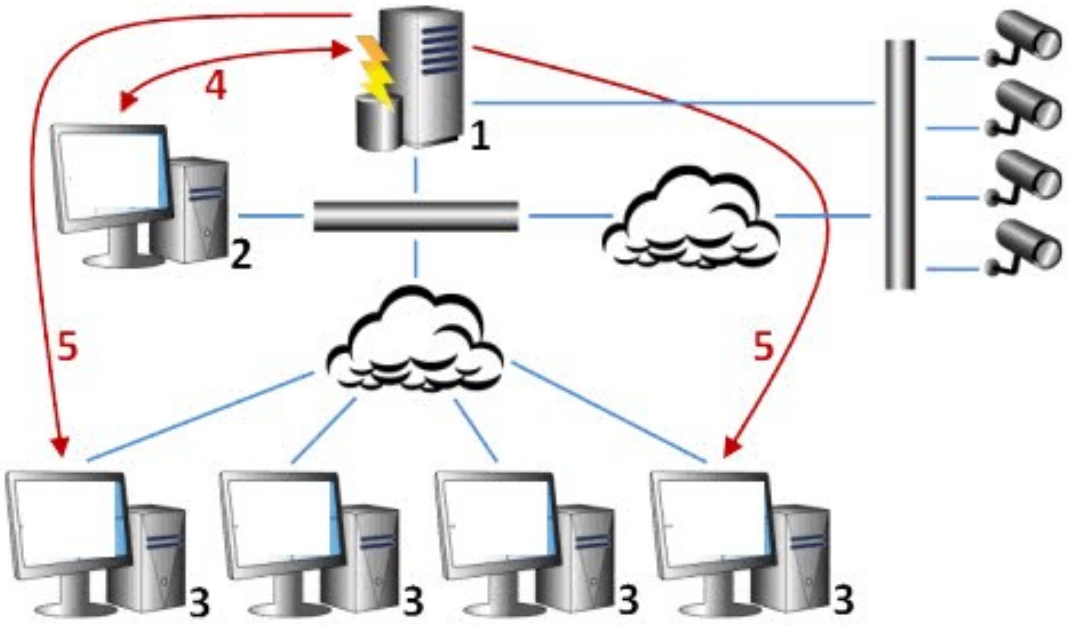
  Diese Gruppe besteht aus  verschiedenen Typen externer Ereignisse:

  - **Analyseereignisse**

    Dies betrifft in der Regel Daten, die von Video-Content-Analyse-Lösungen (CVA) anderer Hersteller bezogen wurden.

  - **MIP Plug-in-Ereignisse**

    Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins (z. B. für die Integration mit externen Zutrittskontrollsystemen) zu Ihrem System entwickeln.




Legende:

1. Überwachungssystem
2. Management Client
3. XProtect Smart Client
4. Alarmkonfiguration
5. Alarmdatenfluss

Sie bearbeiten und weisen Alarme in der Alarmliste in XProtect Smart Client zu. Sie können Alarme auch in die Smart-Map- und Karten-Funktion des XProtect Smart Client integrieren.

### Alarmkonfiguration

Die Alarmkonfiguration umfasst:

- Dynamische rollenbasierte Einrichtung der Alarmbearbeitung
- Zentraler technischer Überblick über alle Komponenten: Server, Kameras und externe Einheiten
- Konfiguration der zentralen Protokollierung aller eingehenden Alarme und Systeminformationen
- Handhabung von Plug-ins zur Unterstützung der benutzerdefinierten Integration anderer Systeme, z. B. externer Zutrittskontroll- oder VCA-basierter Systeme

In der Regel werden Alarme durch die Sichtbarkeit des Objekts kontrolliert, das den Alarm verursacht. Deshalb gibt es vier verschiedene Aspekte, die eine wichtige Rolle in Bezug auf Alarme spielen und bestimmen, wer sie in welchem Umfang kontrollieren/verwalten kann:

| Name | Beschreibung |
|---|---|
| **Sichtbarkeit Quelle/Gerät** | Wenn das Gerät, das einen Alarm verursacht, in einer Benutzerrolle nicht als sichtbar eingerichtet ist, kann der Benutzer den Alarm nicht in der Alarmliste in XProtect Smart Client sehen. |
| **Das Recht, benutzerdefinierte Ereignisse auszulösen** | Diese Berechtigung legt fest, ob die Rolle des Benutzers ausgewählte benutzerdefinierte Ereignisse in XProtect Smart Client auslösen kann. |
| **Externe Plug-ins** | Wenn in Ihrem System externe Plug-ins eingerichtet sind, können diese die Berechtigungen der Benutzer zum Umgang mit Alarmen steuern. |
| **Allgemeine Rollenrechte** | Legen fest, ob der Benutzer Alarme nur ansehen oder auch verwalten darf.<br>Was ein Benutzer von **Alarme** mit Alarmen tun kann, hängt von der Rolle des Benutzers und von den für diese Rolle konfigurierten Einstellungen ab. |

Auf der Registerkarte **Alarme und Ereignisse** in **Optionen** können Sie Einstellungen für Alarme, Ereignisse und Protokolle festlegen.

# Smart Map

## Smart Map (Erklärung)

In XProtect® Smart Client und in XProtect Mobile können Sie sich mit der Smart-Map-Funktion Geräte an mehreren Standorten weltweit geographisch korrekt anzeigen lassen und darauf zugreifen. Im Gegensatz zu den Karten, bei denen Sie eine unterschiedliche Karte für jeden Standort hatten, bietet Ihnen Smart Map ein großes Gesamtbild über eine einzige Ansicht.

Die folgende Konfiguration der Smart-Map-Funktion erfolgt in Management Client:

- Konfigurieren Sie die geographischen Hintergründe, die Sie für Ihre Smart Map auswählen können. Hierzu gehört die Integration Ihrer Smart Map in einen der folgenden Dienste:
  - Bing Maps
  - Google Maps
  - Milestone Map Service
  - OpenStreetMap
- Aktivieren Sie Bing Maps oder Google Maps in XProtect Management Client oder in XProtect Smart Client
- Aktivieren Sie die Bearbeitung von Smart Maps, einschl. Geräte, in XProtect Smart Client
- Positionieren Sie Ihre Geräte geographisch in XProtect Management Client
- Stellen Sie Ihre Smart Map ein, mit Milestone Federated Architecture

## Smart-Map-Integration mit Google Maps (Erklärung)

Zum einbetten von Google Maps in Ihre Smart Map benötigen Sie einen Maps-Static-API-Schlüssel von Google. Um den API-Schlüssel zu erhalten, müssen Sie zunächst ein Google-Cloud-Rechnungskonto erstellen. Die Berechnung erfolgt je nach dem Volumen der geladenen Karten pro Monat.

Sobald Sie den API-Schlüssel haben, müssen Sie ihn in XProtect Management Client eingeben. Siehe auch Aktivieren Sie Bing Maps oder Google Maps in Management Client auf Seite 347.

Wenn Sie sich hinter einer restriktiven Firewall befinden, ist es wichtig, den Zugriff auf die verwendeten Domänen zu ermöglichen. Möglicherweise müssen Sie ausgehenden Datenverkehr für Google Maps über maps.googleapis.com auf jedem Computer zulassen, auf dem Smart Client ausgeführt wird.

Für weitere Informationen, siehe:

- Google Maps-Platform - der Einstieg: https://cloud.google.com/maps-platform/
- Anleitung zur Rechnungsstellung auf der Google Maps Platform: https://developers.google.com/maps/billing/gmp-billing
- Anleitung für Entwickler für Maps Static API: https://developers.google.com/maps/documentation/maps-static/dev-guide

### Digitale Signatur zum Maps Static API-Schlüssel hinzufügen

Wenn Sie erwarten, dass die XProtect Smart Client Anwender pro Tag mehr als 25.000 Karten anfordern, benötigen Sie für Ihren Maps Static API-Schlüssel eine digitale Signatur. Mit der digitalen Signatur können die Server von Google überprüfen, ob eine Seite, die unter Verwendung Ihres API-Schlüssels Abfragen erzeugt, dazu autorisiert ist. Unabhängig von den Nutzungsanforderungen empfiehlt Google jedoch die Verwendung einer digitalen Signatur als zusätzliche Sicherheitsebene. Um eine digitale Signatur zu erhalten, müssen Sie ein URL Signing Secret abfragen. Weitere Informationen finden Sie unter https://developers.google.com/maps/documentation/maps-static/get-api-key#dig-sig-manual.

## Smart-Map-Integration mit Bing Maps (Erklärung)

Zum einbetten von Bing Maps in Ihre Smart Map benötigen Sie einen Basis- oder Enterprise-Schlüssel. Der Unterschied besteht darin, dass Basis-Schlüssel kostenlos sind, jedoch nur eine begrenzte Anzahl von Transaktionen erlauben, bevor die Transaktionen berechnet werden können oder der Zugriff auf den Kartendienst verweigert wird. Der Unternehmensschlüssel ist nicht kostenlos, gestattet jedoch eine unbegrenzte Anzahl an Transaktionen.

Weitere Informationen zu Bing Maps finden Sie unter https://www.microsoft.com/en-us/maps/licensing/.

Sobald Sie den API-Schlüssel haben, müssen Sie ihn in XProtect Management Client eingeben. Siehe Aktivieren Sie Bing Maps oder Google Maps in Management Client auf Seite 347.

> Wenn Sie sich hinter einer restriktiven Firewall befinden, ist es wichtig, den Zugriff auf die verwendeten Domänen zu ermöglichen. Möglicherweise müssen Sie auf jedem Rechner, auf dem Smart Client ausgeführt wird, ausgehenden Datenverkehr für Bing Maps über *.virtualearth.net zulassen.

## Zwischengespeicherte Smart Map Dateien (Erklärung)

> Wenn Sie Google Maps als geographischen Hintergrund verwenden, werden die Dateien nicht im Cache gespeichert.

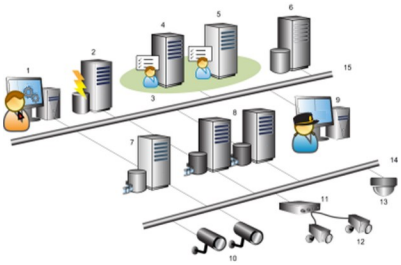
Die Dateien, die Sie für Ihren geografischen Hintergrund verwenden, werden von einem Kachelserver abgerufen. Die Speicherdauer für Dateien im Cache-Ordner ist abhängig von dem auf der Liste **Entfernte gecachte Smart-Map-Dateien** in dem Dialog **Einstellungen** in XProtect Smart Client ausgewählten Wert. Die Speichermöglichkeiten für die Dateien sind die folgenden:

- Unbegrenzt (**Nie**)
- 30 Tage lang, wenn die Datei nicht verwendet wird (**Wenn sie 30 Tage lang nicht verwendet wird**)
- Wenn der Anwender den XProtect Smart Client beendet (**Bei Beendigung**).

Beim Ändern der Adresse des Kachelservers wird automatisch ein neuer zwischengespeicherter Ordner erstellt. Die vorherigen Map-Dateien bleiben im jeweiligen zwischengespeicherten Ordner auf Ihrem lokalen Computer gespeichert.

# Architektur

## Einrichtung eines verteilten Systems



Beispiel für die Einrichtung eines verteilten Systems. Die Zahl der Kameras, Aufzeichnungsserver und verbundenen Clients kann beliebig hoch sein.

> Alle Computer in einer verteilten Einrichtung müssen entweder in einer Domäne oder in einer Workgroup sein.

Legende:

1. Management Client(s)
2. Ereignisserver
3. Microsoft Cluster
4. Managementserver
5. Failover-Management-Server
6. Server mit SQL Server
7. Failover-Aufzeichnungsserver
8. Aufzeichnungsserver
9. XProtect Smart Client(s)
10. IP-Videokameras
11. Videoencoder
12. Analogkameras

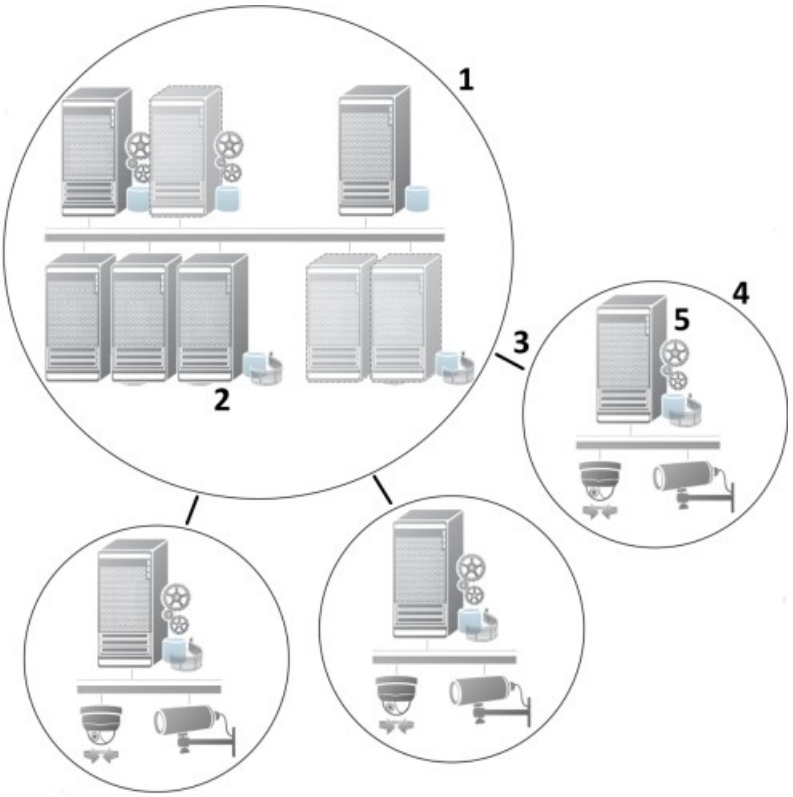
13. PTZ-IP-Kamera
14. Kameranetzwerk
15. Servernetzwerk

## Milestone Interconnect (Erklärung)

> Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Milestone Interconnect™ erlaubt Ihnen die Integration einer Anzahl kleiner, physisch fragmentierter und entfernter XProtect Installationen mit einer XProtect Corporate zentralen Seite. Sie können diese kleineren Standorte (Remote-Systeme) mobil mitführen, z. B. auf Booten, Bussen oder Zügen. Das bedeutet, dass solche Standorte nicht permanent mit einem Netzwerk verbunden sein müssen.

Die folgende Abbildung zeigt die Einrichtung von Milestone Interconnect in Ihrem System:



1. Milestone Interconnect Zentraler XProtect Corporate-Standort
2. Milestone Interconnect Treiber (verwalten die Verbindung zwischen den Aufzeichnungsservern des zentralen und des Remote-Systems; muss aus einer Liste von Treibern ausgewählt werden, wenn Remote-Systeme per **Hardware hinzufügen**-Assistenten hinzugefügt werden)
3. Milestone Interconnect Verbindung
4. Milestone Interconnect Remote-System (der gesamte Remote-System mit Systeminstallation, Benutzer, Kameras usw.)
5. Milestone Interconnect Remote-System (die tatsächliche technische Installation am Remote-Systeminstallation)

Mit dem Assistenten **Hardware hinzufügen** können Sie entfernte Standorte zu Ihrem zentralen Standort hinzufügen (siehe Einen Remote-Standort zum zentralen Milestone Interconnect-Standort hinzufügen auf Seite 339).

Jeder Remote-System läuft unabhängig und kann jegliche normalen Überwachungsaufgaben übernehmen. Je nach den Netzwerkverbindungen und den entsprechenden Benutzerrechten (siehe Benutzerrechte zuweisen auf Seite 340), Milestone Interconnect können Sie die Kameras der entfernten Standorte direkt live sehen und die Aufzeichnungen von den entfernten Standorten am zentralen Standort wiedergeben.

Der zentrale Standort kann nur solche Geräte sehen und auf diese zugreifen, auf die das bestimmte Benutzerkonto (beim Hinzufügen des Remote-Systems) Zugriff hat. Dies ermöglicht es lokalen Systemadministratoren zu steuern, welche Geräte dem zentralen Standort und dessen Benutzern zur Verfügung gestellt werden soll.

Am zentralen Standort können Sie den eigenen Status des Systems für die verbundenen Kameras sehen, allerdings nicht den direkten Status des Remote-Systems. Stattdessen können Sie zur Überwachung des entfernten Standortes über Ereignisse am entfernten Standort am zentralen Standort Alarm oder sonstige Meldungen auslösen (siehe Konfigurieren Sie Ihren zentralen Standort, so dass er auf Ereignisse von Remote-Systemen reagiert auf Seite 342).

Dies bietet Ihnen auch die Möglichkeit, Aufzeichnungen des Remote-Systems an den zentralen Standort zu senden, basierend entweder auf Ereignissen, Regeln/Planung, oder manuellen Anfragen von XProtect Smart Client-Benutzern.

Nur XProtect Corporate-Systeme können als zentrale Standorte fungieren. Alle anderen Produkte können Remote-Systeme sein, einschließlich XProtect Corporate. Welche Versionen und wie viele Kameras sowie die Art und Weise (oder überhaupt) des Umgangs mit Geräten und Ereignissen des Remote-Systems am zentralen Standort, unterscheidet sich von Einstellung zu Einstellung. Weitere Einzelheiten dazu, wie bestimmte XProtect Produkte in einer Milestone Interconnect Einrichtung miteinander interagieren, finden Sie auf der Milestone Interconnect Website (https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/).

### Auswahl von Milestone Interconnect oder Milestone Federated Architecture (Erklärung)

In einem physisch verteiltem System, in dem Benutzer am zentralen Standort Zugriff auf Video am Remote-System benötigen, können Sie zwischen Milestone Interconnect™ oder Milestone Federated Architecture™ wählen.

Milestone empfiehlt Milestone Federated Architecture, wenn:

- Die Netzwerkverbindung zwischen dem zentralen Standort und dem föderalen Standort instabil ist
- Das Netzwerk die selbe Domäne verwendet
- Es weniger größere Standorte gibt
- Die Bandbreite für die gewünschte Nutzung ausreicht

Milestone empfiehlt Milestone Interconnect, wenn:

- Die Netzwerkverbindung zwischen dem zentralen Standort und dem Remote-System instabil ist
- Sie oder Ihr Unternehmen ein anderes Produkt von XProtect am Remote-System verwenden möchten
- Das Netzwerk verschiedene Domains oder Arbeitsgruppen benutzt
- Es kleinere Standorte gibt

### Milestone Interconnect und Lizenzierung

Für die Ausführung von Milestone Interconnect benötigen Sie Milestone Interconnect Kameralizenzen an Ihrem zentralen Standort, um Video von Geräten an Remote-Systemen anzusehen. Die Anzahl der erforderlichen Milestone Interconnect Kameralizenzen ist abhängig von der Anzahl der Hardwaregeräte an den entfernten Standorten, von denen Sie Daten empfangen wollen. Beachten Sie, dass ausschließlich XProtect Corporate als zentraler Standort agieren kann.

Den Status Ihrer Milestone Interconnect Kameralizenzen finden Sie auf der Seite **Lizenzinformationen** am zentralen Standort.

### Milestone Interconnect-Einrichtungen (Erklärung)

Es gibt drei Wege Milestone Interconnect auszuführen. Wie Sie Ihre Einstellung ausführen hängt von Ihrer Netzwerkverbindung, Ihrer Wiedergabeart und ob Sie Fernaufzeichnungen abrufen und in welcher Weise ab.

Folgend sind die drei wahrscheinlichsten Einstellungen beschrieben:

#### Direkte Wiedergabe von Remote-Systemen (gute Netzwerkverbindungen)

Die direkteste Einstellung. Der zentrale Standort ist durchgehend mit seinen Remote-Systemen verbunden und Benutzer am zentralen Standort können Fernaufzeichnungen direkt von den Remote-Systemen Wiedergabe. Hierfür muss die Option **Aufzeichnungen von entfernten Systemen abspielen** verwendet werden (siehe Aktivieren der direkten Wiedergabe von der Kamera am Remote-System auf Seite 341).

**Regel- oder XProtect Smart Client-basierender Abruf ausgewählter Fernaufzeichnungssequenzen von Remote-Systemen (zeitweilig begrenzte Netzwerkverbindungen)**

Wird verwendet, wenn ausgewählte Aufzeichnungssequenzen (vom Remote-System) zentral gespeichert werden sollten, um die Unabhängigkeit der Remote-Systeme zu garantieren. Unabhängigkeit ist äußerst wichtig im Falle von Netzwerkfehlern oder -einschränkungen. Die Einstellungen zum Abrufen entfernter Aufzeichnungen können Sie auf der Registerkarte **Fernabruf** konfigurieren (siehe Registerkarte „Fernabfrage“ auf Seite 465).

Der Abruf von Fernaufzeichnungen kann bei Bedarf vom XProtect Smart Client gestartet werden oder durch eine Regel gesteuert werden. In einigen Szenarien sind Remote-Systeme die meiste Zeit online und in anderen offline. Dies hängt oft von der Branche ab. In einigen Branchen ist es üblich, dass der zentrale Standort permanent mit seinen Remote-Systemen in Kontakt steht (zum Beispiel die Hauptverwaltung eines Einzelhandels (zentraler Standort) und eine Anzahl von Läden (Remote-Systeme)). Bei anderen Branchen, wie in der Logistik und Transport, sind Remote-Systeme mobil (bspw. Busse, Züge, Schiffe usw.) und können nur sporadisch eine Netzwerkverbindung aufbauen. Sollte die Netzwerkverbindung während des Abrufs von Fernaufzeichnungen ausfallen, kann sie bei nächster Gelegenheit fortgesetzt werden.

Wenn das System den automatischen Abruf, oder eine Anforderung dessen von dem XProtect Smart Client außerhalb des in der Registerkarte **Fernabfrage** festgelegten Zeitintervalls erhält, wird es zwar angenommen, aber nicht gestartet, bis diese Zeit erreicht ist. Neue Abrufanfragen für Fernaufzeichnungen werden eingereiht und gestartet, sobald das eingestellte Zeitintervall erreicht ist. Sie können anstehende Abrufanfragen für Fernaufzeichnungen ansehen, unter **System-Dashboard** -> **Aktuelle Aufgaben**.

**Nach einem Verbindungsfehler werden fehlende Fernaufzeichnungen automatisch vom Remote-System abgefragt**

Verwendet Remote-Systeme, wie ein Aufzeichnungsserver den lokalen Speicher einer Kamera. Normalerweise sind Remote-Systeme mit ihrem zentralen Standort verbunden und beliefern ihn mit einem Live-Stream, den der zentrale Standort dann aufzeichnet. Sollte aus einem Grund das Netzwerk ausfallen, gehen dem zentralen Standort diese Aufzeichnungssequenzen verloren. Sobald das Netzwerk wieder hergestellt wurde, fragt der zentrale Standort automatisch die Fernaufzeichnungen des verpassten Zeitraums ab. Hierfür muss die Option **Fernaufzeichnungen automatisch abrufen wenn die Verbindung wiederhergestellt wird** verwendet werden (siehe Abruf von Fernaufzeichnungen von Kamera an Remote-System auf Seite 341), und zwar auf der Registerkarte **Aufzeichnen** für die jeweilige Kamera.

Sie können jeder der oben genannten Lösungen den individuellen Bedürfnissen Ihrer Organisation anpassen.

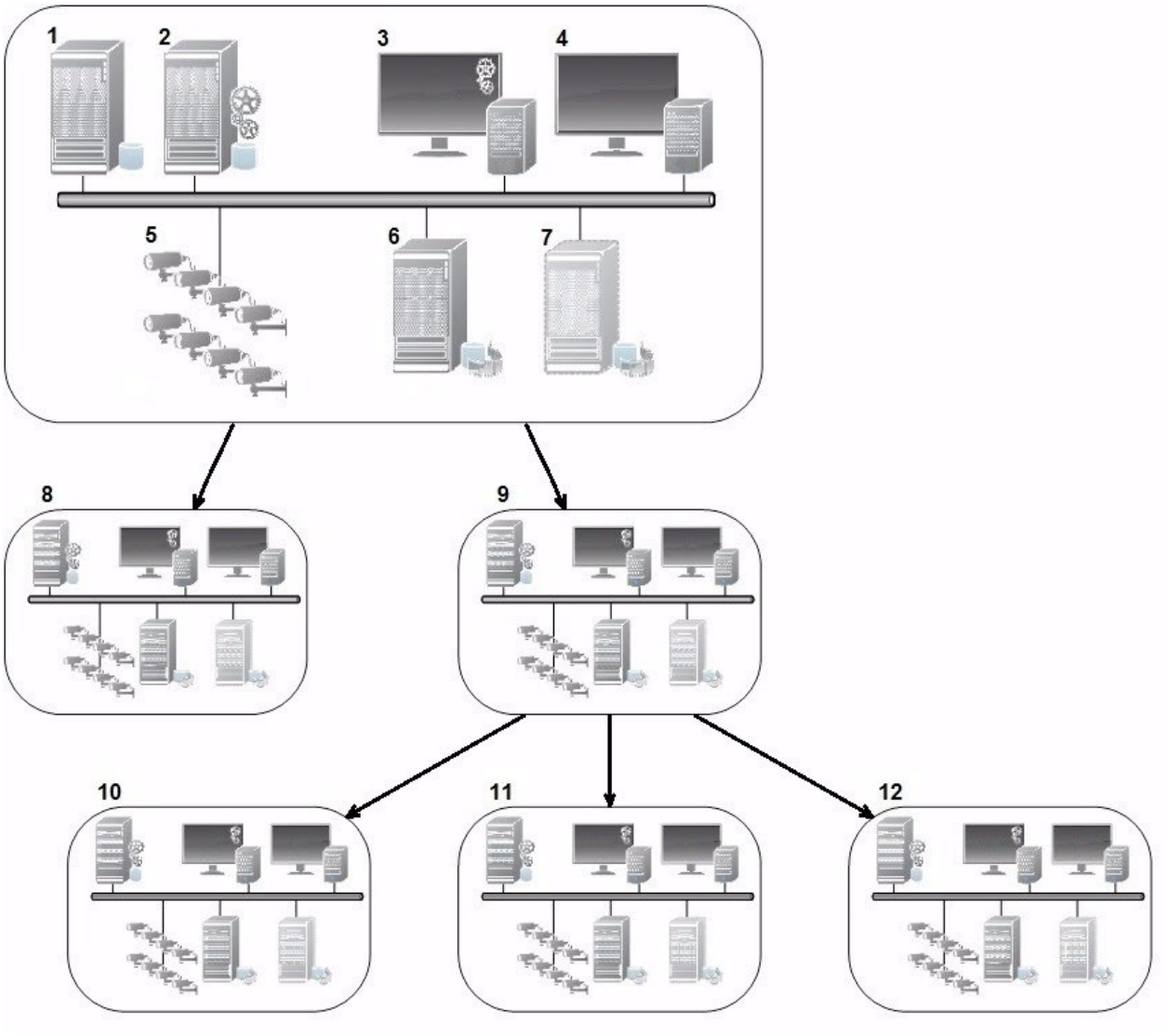
## Konfigurieren von Milestone Federated Architecture

XProtect Expert können nur als untergeordnete Standorte eingebunden werden.

Milestone Federated Architecture verbindet mehrere einzelne Standardsysteme zu einer Hierarchie von über- und untergeordneten föderalen Standorten. Client-Benutzer mit ausreichenden Berechtigungen haben nahtlosen Zugriff auf Video-, Audio- und andere Ressourcen an den einzelnen Standorten. Administratoren können alle Standorte ab Version 2018 R1 und neuer innerhalb der Verbundhierarchie zentral basierend auf den Administratorrechten für die einzelnen Standorte verwalten.

Benutzer mit Basisrechten werden in Milestone Federated Architecture-Systemen nicht unterstützt, daher müssen Sie über den Dienst Active Directory neue Benutzer als Windows-Benutzer hinzufügen.

Milestone Federated Architecture wird mit einem zentralen Standort (Top Site) und einer unbegrenzten Anzahl föderierter Standorte eingerichtet (siehe Einrichten Ihres Systems für föderale Standorte auf Seite 333). Wenn Sie sich an einem Standort anmelden, haben Sie Zugriff auf die Informationen aller untergeordneten Standorte und auch auf die Standorte, die wiederum diesen untergeordnet sind. Die Verknüpfung zwischen zwei Standorten wird hergestellt, wenn Sie die Verknüpfung von der Elternseite anfordern (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 335). Ein untergeordneter Standort kann nur mit einem einzigen übergeordneten Standort verbunden werden. Sollten Sie nicht der Administrator des untergeordneten Standorts sein, wenn Sie ihn zur Hierarchie der föderalen Standorte hinzufügen, muss die Anfrage vom Administrator des untergeordneten Standorts angenommen werden.




Die Bestandteile einer Milestone Federated Architecture-Konfiguration:

1. Server mit SQL Server
2. Managementserver
3. Management Client
4. XProtect Smart Client
5. Kameras
6. Aufzeichnungsserver
7. Failover-Aufzeichnungsserver
8. bis 12. Föderale Standorte

### Synchronisierung der Hierarchie

Ein übergeordneter Standort enthält eine sich aktualisierende Liste aller gegenwärtig untergeordneten Standorte, der Standorte die wiederum diesen untergeordnet sind und so weiter. Die Hierarchie der föderalen Standorte verfügt sowohl über eine planmäßige Synchronisierung zwischen den Standorten, als auch über eine Synchronisierung, die ausgelöst wird, wenn ein Standort durch einen System-Administrator hinzugefügt oder entfernt wird. Die Synchronisierung der Hierarchie durch das System läuft von Ebene zu Ebene ab, wobei jede Ebene die Kommunikation weiterleitet und zurücksendet, bis Sie den Server erreicht, der die Informationen anfordert. Das System versendet jedes Mal weniger als 1 MB. Je nach Anzahl der Ebenen kann es einige Zeit dauern, bis die Änderungen an einer Hierarchie in Management Client sichtbar werden. Sie können den Zeitplan für die Synchronisierungen nicht selbst festlegen.

### Datenverkehr

Das System sendet Kommunikations- oder Konfigurationsdaten, wenn sich ein Benutzer oder Administrator ein Live-Video oder eine Videoaufzeichnung ansieht oder einen Standort konfiguriert. Die Datenmenge hängt davon ab, was und wie viel angesehen oder konfiguriert wird.

### Milestone Federated Architecture mit sonstigen Produkten und Systemanforderungen

- Das Öffnen der Management Client in einer Milestone Federated Architecture wird bei drei größeren Releases unterstützt, einschließlich der aktuell vorgestellten. In einer Milestone Federated Architecture Einrichtung größeren Umfangs benötigen Sie eine separate Management Client, die zur Serverversion passt.
- Wenn der zentrale Standort XProtect Smart Wall verwendet, können Sie auch die Funktionen von XProtect Smart Wall in der Hierarchie der föderalen Standorte verwenden.
- Wenn der zentrale Standort XProtect Access verwendet und sich ein XProtect Smart Client-Benutzer an einem Standort der föderalen Standorthierarchie anmeldet, erscheinen Benachrichtigungen für Zugriffsanforderungen von den föderalen Standorten auch in XProtect Smart Client
- Sie können XProtect Expert 2013-Systeme oder neuere zur Hierarchie der föderalen Standorte als untergeordnete Standorte hinzufügen, nicht als übergeordnete Standorte.
- Die Milestone Federated Architecture benötigt keine zusätzlichen Lizenzen
- Weitere Informationen zu Anwendungsfällen und deren Vorteilen finden Sie im Whitepaper zu Milestone Federated Architecture.

### Anlegen einer Hierarchie der föderalen Standorte

Management Client empfiehlt Ihnen, aufzuzeichnen, wie Sie Ihre Standorte miteinander verbinden wollen, bevor Sie in Milestone die Hierarchie aufbauen.

Sie installieren und konfigurieren jeden Standort in einer Verbundhierarchie wie ein normales, eigenständiges System mit Standard-Systemkomponenten, Einstellungen, Regeln, Zeitplänen, Administratoren, Benutzern und Benutzerberechtigungen. Wenn Sie die Standorte bereits installiert und konfiguriert haben und sie nur noch in eine Hierarchie der föderalen Standorte kombinieren müssen, sind Ihre Systeme zum Einrichten bereit.

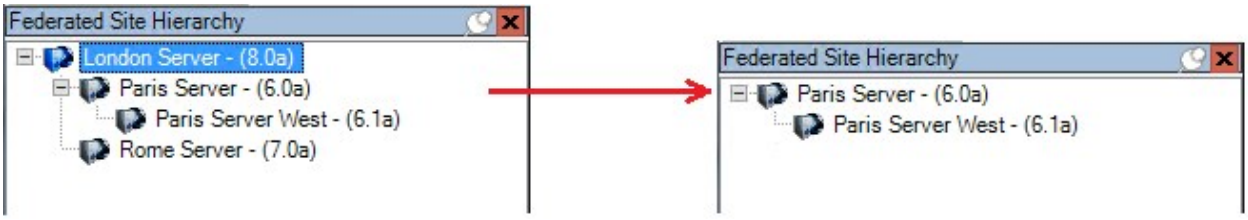
Soweit die einzelnen Standorte installiert sind, müssen Sie sie so einrichten, dass sie als föderierte Standorte laufen (siehe Einrichten Ihres Systems für föderale Standorte auf Seite 333).

Um die Hierarchie zu starten, melden Sie sich am Standort an, der als zentraler Standort dienen soll, und fügen Sie (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 335) den ersten föderalen Standort hinzu. Sobald die Verbindung besteht, erstellen die beiden Standorte automatisch eine Hierarchie der föderalen Standorte im Fenster **Hierarchie der föderalen Standorte** in Management Client. Hier können Sie weitere Standorte hinzufügen und damit die föderale Hierarchie ausbauen.

Sobald Sie eine Hierarchie der föderalen Standorte erstellt haben, können sich Benutzer und Administratoren an einem Standort anmelden und auf diesen sowie alle zugehörigen föderalen Standorte zugreifen. Der Zugang zu Verbundstandorten hängt von den Benutzerberechtigungen ab.

Sie können der föderalen Hierarchie eine unbeschränkte Anzahl an Standorten hinzufügen. Außerdem kann ein Standort auf einer älteren Produktversion mit einer neueren Version verbunden sein und umgekehrt. Die Versionsnummern erscheinen automatisch und können nicht gelöscht werden. Der Standort, an dem Sie angemeldet sind, befindet sich immer ganz oben im Fenster **Hierarchie der föderalen Standorte** und wird als Heimstandort bezeichnet.

Weiter unten finden Sie ein Beispiel für einen föderalen Standort im Management Client. Auf der linken Seite hat sich der Benutzer auf dem obersten Standort angemeldet. Auf der rechten Seite hat sich der Benutzer bei einer der untergeordneten Standpunkte, dem Pariser Server, angemeldet, der dann der Home-Standort ist.




### Statussymbole in der Milestone Federated Architecture

Die Symbole repräsentieren den Status eines Standorts:

| Beschreibung | Symbol |
|---|---|
| Der oberste Standort in der ganzen Hierarchie ist betriebsbereit. | |

| Beschreibung | Symbol |
|---|---|
| Der oberste Standort in der ganzen Hierarchie ist betriebsbereit, aber es liegt mindestens ein Problem vor. Wird oben auf dem Symbol des obersten Standorts angezeigt. |  |
| Der Standort ist betriebsbereit. |  |
| Der Standort wartet darauf, in die Hierarchie aufgenommen zu werden. |  |
| Der Standort hängt an, ist jedoch noch nicht betriebsbereit. |  |

## Vom System verwendete Ports

Alle XProtect-Komponenten sowie die von Ihnen benötigten Ports sind weiter unten aufgeführt. Damit die Firewall nur ungewünschten Traffic blockiert, müssen Sie die vom System genutzten Ports bestimmen. Sie sollten nur diese Ports freigeben. Die Liste enthält auch die verwendeten Ports der lokalen Prozesse.

Sie sind in zwei Gruppen unterteilt:

- **Serverkomponenten** (Dienste) bieten ihre Dienste über bestimmte Ports an, weshalb sie auf Clientanfragen auf diesen Ports reagieren. Daher müssen diese Ports in der Windows Firewall für eingehende und ausgehende Verbindungen geöffnet werden
- **Clientkomponenten** (Clients) initiieren Verbindungen zu bestimmten Ports in Serverkomponenten. Daher müssen diese Ports für ausgehende Verbindungen geöffnet werden. Ausgehende Verbindungen sind normalerweise standardmäßig in der Windows Firewall geöffnet

Sollte nichts weiteres angegeben sein, müssen Ports für Serverkomponenten für eingehende Verbindungen geöffnet werden und Ports für Clientkomponenten für ausgehende Verbindungen.

Denken Sie jedoch daran, dass Serverkomponenten als Clients für andere Serverkomponenten dienen können. Diese sind in diesem Dokument nicht ausdrücklich aufgeführt.

Die Portnummern sind Standardzahlen, können aber geändert werden. Kontaktieren Sie den Milestone-Support, wenn Sie diejenigen Ports ändern möchten, die nicht über den Management Client konfigurierbar sind.

**Serverkomponenten (eingehende Verbindungen)**

Jeder der folgenden Abschnitte führt die Ports auf, welche für einen bestimmten Dienst geöffnet werden müssen. Damit Sie erfahren, welche Ports auf einem bestimmten Computer geöffnet werden müssen, sollten Sie alle Dienste auf diesem Computer ausführen.

**Management Server-Dienst und zugehörige Prozesse**

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **80** | HTTP | IIS | Alle Server und XProtect Smart Client und Management Client | Der Zweck von Port 80 und Port 443 ist der gleiche. Welchen Port die VMS verwendet, hängt jedoch davon ab, ob Sie Zertifikate zur Sicherung der Kommunikation verwendet haben.<br>• Wenn Sie die Kommunikation nicht mit Zertifikaten gesichert haben, verwendet die VMS den Port 80.<br>• Wenn Sie die Kommunikation mit Zertifikaten gesichert haben, verwendet die VMS den Port 443, außer für die Kommunikation vom Event Server zum Management-Server. Die Kommunikation zwischen dem Event Server und dem Management-Server erfolgt über Windows Secured Framework (WCF) und Windows Authentifizierung auf Port 80. |
| **443** | HTTPS | IIS | | |
| **6473** | TCP | Management Server- | Management Server | Zeigt Status und verwaltet |

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| | | Dienst | Manager Taskleistensymbol, nur lokale Verbindungen. | den Dienst. |
| **8080** | TCP | Managementserver | Nur lokale Verbindung. | Kommunikation zwischen internen Prozessen auf dem Server. |
| **9000** | HTTP | Managementserver | Recording Server-Dienste | Webdienst für die interne Kommunikation zwischen Servern. |
| **12345** | TCP | Management Server-Dienst | XProtect Smart Client | Kommunikation zwischen dem System und Matrix-Empfängern.<br>Sie können die Portnummer im Management Client ändern. |
| **12974** | TCP | Management Server-Dienst | Windows SNMP-Dienst | Kommunikation mit dem SNMP-Erweiterungsagenten.<br>Verwenden Sie den Port nicht für anderen Zwecke, selbst wenn Ihr System SNMP nicht anwendet.<br>In XProtect-Systemen von 2014 und älter, lautete die Portnummer 6475.<br>In XProtect-Systemen der Version 2019 R2 und älter lautete die Portnummer 7475. |

**SQL Server-Dienst**

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **1433** | TCP | SQL Server | Management Server-Dienst | Speichern und Abrufen von Konfigurationen über die Identity Provider. |
| **1433** | TCP | SQL Server | Event Server-Dienst | Speichern und Abrufen von Ereignissen über die Identity Provider. |
| **1433** | TCP | SQL Server | Log Server-Dienst | Speichern und Abrufen von Protokolleinträgen über die Identity Provider. |

#### Data Collector-Dienst

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **7609** | HTTP | IIS | Auf dem Computer des Management-Servers: Data Collector Dienste auf allen anderen Servern.<br>Auf anderen Computern: Data Collector-Dienst auf dem Management-Server. | Systemmonitor. |

#### Event Server-Dienst

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **1234** | TCP/UDP | Event Server-Dienst | Jeder Server, der generische Ereignisse an Ihr XProtect-System sendet. | Mithören generischer Ereignissen von externen Systemen oder Geräte.<br>Nur wenn die relevante Datenquelle aktiviert ist. |

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| 1235 | TCP | Event Server-Dienst | Jeder Server, der generische Ereignisse an Ihr XProtect-System sendet. | Mithören generischer Ereignissen von externen Systemen oder Geräte.<br>Nur wenn die relevante Datenquelle aktiviert ist. |
| 9090 | TCP | Event Server-Dienst | Jeder Server oder Gerät, das Analyseereignisse an Ihr XProtect-System senden. | Mithören von Analyseereignissen von externen Systemen oder Geräte.<br>Nur relevant, wenn die Analyseereignisfunktion aktiviert ist. |
| 22331 | TCP | Event Server-Dienst | XProtect Smart Client und die Management Client | Konfiguration, Ereignisse, Alarme und Kartendaten. |
| 22332 | WS/WSS<br>HTTP/HTTPS* | Event Server-Dienst | API Gateway und die Management Client | Ereignis-/Statusabonnement, Events Rest API, Websockets Messaging API und Alarms REST API. |
| 22333 | TCP | Event Server-Dienst | MIP Plug-ins und Anwendungen. | MIP-Messaging. |

* Ein 403-Fehler wird zurückgegeben, wenn auf ein HTTP Zugriff auf einen HTTPS-only-Endpunkt erfolgt.

**Recording Server-Dienst**

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| 25 | SMTP | Recording | Kameras, Encoder und | Mithören von |

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| | | Server-Dienst | I/O-Geräte. | Ereignismeldungen von Geräten.<br>Der Port ist standardmäßig abgeschaltet.<br>(Nicht mehr genutzt) Wenn Sie diese Option aktivieren, wird für unverschlüsselte Verbindungen ein Port geöffnet. Dies wird nicht empfohlen. |
| **5210** | TCP | Recording Server-Dienst | Failover-Aufzeichnungsserver. | Zusammenführen von Datenbanken, nachdem ein Failover-Aufzeichnungsserver ausgeführt wurde. |
| **5432** | TCP | Recording Server-Dienst | Kameras, Encoder und I/O-Geräte. | Mithören von Ereignismeldungen von Geräten.<br>Der Port ist standardmäßig abgeschaltet. |
| **7563** | TCP | Recording Server-Dienst | XProtect Smart Client, Management Client | Abrufen von Video- und Audiostreams, PTZ-Befehlen. |
| **8966** | TCP | Recording Server-Dienst | Recording Server Manager Taskleistensymbol, nur lokale Verbindungen. | Zeigt Status und verwaltet den Dienst. |
| **9001** | HTTP | Recording Server-Dienst | Managementserver | Webdienst für die interne Kommunikation zwischen Servern.<br>Wenn mehrere Aufzeichnungsserverinstanzen verwendet werden, benötigt jede einzelne Instanz ihren |

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| | | | | eigenen Port. Zusätzliche Ports werden 9002, 9003 usw. sein. |
| **11000** | TCP | Recording Server-Dienst | Failover-Aufzeichnungsserver | Abfrage des Status der Aufzeichnungsserver. |
| **12975** | TCP | Recording Server-Dienst | Windows SNMP-Dienst | Kommunikation mit dem SNMP-Erweiterungsagenten.<br>Verwenden Sie den Port nicht für anderen Zwecke, selbst wenn Ihr System SNMP nicht anwendet.<br>In XProtect-Systemen von 2014 und älter, lautete die Portnummer 6474.<br>In XProtect-Systemen der Version 2019 R2 und älter lautete die Portnummer 7474. |
| **65101** | UDP | Recording Server-Dienst | Nur lokale Verbindung | Mithören von Ereignis-Mitteilungen der Treiber. |

Abgesehen von den eingehenden Verbindungen zu den Recording Server oben aufgeführten Diensten stellt der Recording Server Dienst ausgehende Verbindungen her zu:

- Kameras
- NVRs
- Untereinander fernverbundene Standorte (Milestone Interconnect ICP)

**Failover Server-Dienst und Failover Recording Server-Dienst**

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **25** | SMTP | Failover Recording Server-Dienst | Kameras, Encoder und I/O-Geräte. | Mithören von Ereignismeldungen von Geräten.<br>Der Port ist standardmäßig abgeschaltet.<br>(Nicht mehr genutzt) Wenn Sie diese Option aktivieren, wird für unverschlüsselte Verbindungen ein Port geöffnet. Dies wird nicht empfohlen. |
| **5210** | TCP | Failover Recording Server-Dienst | Failover-Aufzeichnungsserver | Zusammenführen von Datenbanken, nachdem ein Failover-Aufzeichnungsserver ausgeführt wurde. |
| **5432** | TCP | Failover Recording Server-Dienst | Kameras, Encoder und I/O-Geräte. | Mithören von Ereignismeldungen von Geräten.<br>Der Port ist standardmäßig abgeschaltet. |
| **7474** | TCP | Failover Recording Server-Dienst | Windows SNMP-Dienst | Kommunikation mit dem SNMP-Erweiterungsagenten.<br>Verwenden Sie den Port nicht für anderen Zwecke, selbst wenn Ihr System SNMP nicht anwendet. |
| **7563** | TCP | Failover Recording Server Dienst | XProtect Smart Client | Abrufen von Video- und Audiostreams, PTZ-Befehlen. |
| **8844** | UDP | Failover | Kommunikation | Kommunikation zwischen |

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| | | Recording Server Dienst | zwischen Failover Recording Server-Diensten. | den Servern. |
| **8966** | TCP | Failover Recording Server-Dienst | Failover Recording Server Manager Taskleistensymbol, nur lokale Verbindungen. | Zeigt Status und verwaltet den Dienst. |
| **8967** | TCP | Failover Server-Dienst | Failover Server Manager Taskleistensymbol, nur lokale Verbindungen. | Zeigt Status und verwaltet den Dienst. |
| **8990** | HTTP | Failover Server-Dienst | Management Server-Dienst | Überwachung des Status des Failover Server-Dienstes. |
| **9001** | HTTP | Failover Server-Dienst | Managementserver | Webdienst für die interne Kommunikation zwischen Servern. |

Abgesehen von den eingehenden Verbindungen zu den oben aufgeführten Diensten des Failover Servers / Failover Recording Servers, stellt der Dienst des Failover Servers / Failover Recording Servers ausgehende Verbindungen zu den regelmäßigen Aufnahmegeräten, Kameras sowie für Video Push her.

**Log Server-Dienst**

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **22337** | HTTP | Log Server-Dienst | Alle XProtect-Komponenten außer Management Client und der Recording-Server. | Sie können auf den Log-Server schreiben, von ihm lesen und ihn konfigurieren. |

### Mobile Server-Dienst

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **8000** | TCP | Mobile Server-Dienst | Mobile Server Manager Taskleistensymbol, nur lokale Verbindungen. | SysTray Anwendung. |
| **8081** | HTTP | Mobile Server-Dienst | Mobile Clients, Web Clients und Management Client. | Senden von Datenstreams; Video und Audio. |
| **8082** | HTTPS | Mobile Server-Dienst | Mobile Clients, Web Clients. | Senden von Datenstreams; Video und Audio. |
| **40001 - 40099** | HTTP | Mobile Server-Dienst | Aufzeichnungsserverdienst | Mobile Server Push-Video.<br>Dieser Portbereich ist standardmäßig abgeschaltet. |

### LPR Server-Dienst

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **22334** | TCP | LPR Server Dienst | Ereignisserver | Abruf erkannter Nummernschilder und Server-Status.<br>Für eine Verbindung muss der Event-Server das LPR Plug-in installiert haben. |
| **22334** | TCP | LPR Server-Dienst | LPR Server Manager Taskleistensymbol, nur lokale Verbindungen. | SysTray Anwendung |

### Milestone Open Network Bridge-Dienst

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **580** | TCP | Milestone Open Network Bridge-Dienst | ONVIF Clients | Authentifizierung und Anfrage für die Videostreamkonfiguration. |
| **554** | RTSP | RTSP-Dienst | ONVIF Clients | Streamen von angefordertem Video an ONVIF-Clients. |

### XProtect DLNA Server-Dienst

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **9100** | HTTP | DLNA Server Dienst | DLNA-Gerät | Geräteerkennung und Bereitstellung der Konfiguration von DLNA-Kanälen. Anfrage für Videostreams. |
| **9200** | HTTP | DLNA Server Dienst | DLNA-Gerät | Streamen von angeforderten Video an DLNA-Geräte. |

### XProtect Screen Recorder-Dienst

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **52111** | TCP | XProtect Screen Recorder | Recording Server-Dienst | Stellt Video von einem Bildschirm bereit. Es erscheint und handelt in der gleichen Art wie eine Kamera auf dem Aufzeichnungsserver.<br>Sie können die Portnummer im Management Client ändern. |

#### XProtect Incident Manager -Dienst

| Portnummer | Protokoll | Prozess | Verbindungen von... | Zweck |
|---|---|---|---|---|
| **80** | HTTP | IIS | XProtect Smart Client und die Management Client | Der Zweck von Port 80 und Port 443 ist der gleiche. Welchen Port die VMS verwendet, hängt jedoch davon ab, ob Sie Zertifikate zur Sicherung der Kommunikation verwendet haben.<br>• Wenn Sie die Kommunikation nicht mit Zertifikaten gesichert haben, verwendet die VMS den Port 80.<br>• Wenn Sie die Kommunikation mit Zertifikaten gesichert haben, verwendet die VMS den Port 443. |
| **443** | HTTPS | IIS | | |

### Serverkomponenten (ausgehende Verbindungen)

#### Management Server-Dienst

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **443** | HTTPS | Der Lizenzserver, der den Lizenzverwaltungsdienst hostet. Die Kommunikation erfolgt über https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx | Das Aktivieren von Lizenzen. |

#### Recording Server-Dienst

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **80** | HTTP | Kameras, NVRs, Encoder<br>Untereinander verbundene Standorte | Authentifizierung, Konfiguration und Datenstreams, Video und Audio.<br>Anmelden |
| **443** | HTTPS | Kameras, NVRs, Encoder | Authentifizierung, Konfiguration und Datenstreams, Video und Audio. |
| **554** | RTSP | Kameras, NVRs, Encoder | Datenstreams, Video und Audio. |
| **7563** | TCP | Untereinander verbundene Standorte | Datenstreams und Ereignisse. |
| **11000** | TCP | Failover-Aufzeichnungsserver | Abfrage des Status der Aufzeichnungsserver. |
| **40001 - 40099** | HTTP | Mobil-Server-Dienst | Push-Video auf dem Mobile Server.<br>Dieser Portbereich ist standardmäßig abgeschaltet. |

#### Failover Server-Dienst und Failover Recording Server-Dienst

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **11000** | TCP | Failover-Aufzeichnungsserver | Abfrage des Status der Aufzeichnungsserver. |

#### Event Server-Dienst

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **80** | HTTP | API Gateway und die Management | Aufrufen der Konfigurations-API |

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| | | Server | über API Gateway |
| **443** | HTTPS | API Gateway und die Management Server | Aufrufen der Konfigurations-API über API Gateway |
| **443** | HTTPS | Milestone Customer Dashboard über https://service.milestonesys.com/ | Senden Sie Status, Ereignisse und Fehlermeldungen vom XProtect-System an Milestone Customer Dashboard. |

**Log Server-Dienst**

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **443** | HTTP | Log-Server | Weiterleitung von Nachrichten an den Log-Server. |

API Gateway

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **443** | HTTPS | Management Server | RESTful API |
| **22332** | WS/WSS HTTP/HTTPS* | Management Client | Ereignis-/Statusabonnement, Events Rest API, Websockets Messaging API und Alarms REST API. |

**Kameras, Encoder und I/O-Geräte (eingehende Verbindungen)**

| Portnummer | Protokoll | Verbindungen von... | Zweck |
|---|---|---|---|
| **80** | TCP | Aufzeichnungsserver und Failover-Aufzeichnungsserver | Authentifizierung, Konfiguration und Datenstreams; Video und Audio. |
| **443** | HTTPS | Aufzeichnungsserver und Failover-Aufzeichnungsserver | Authentifizierung, Konfiguration und Datenstreams; Video und Audio. |
| **554** | RTSP | Aufzeichnungsserver und Failover-Aufzeichnungsserver | Datenstreams; Video und Audio. |

**Kameras, Encoder und I/O-Geräte (ausgehende Verbindungen)**

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **25** | SMTP | Aufzeichnungsserver und Failover-Aufzeichnungsserver | Senden von Ereignis-Mitteilungen (veraltet). |
| **5432** | TCP | Aufzeichnungsserver und Failover-Aufzeichnungsserver | Senden von Ereignis-Mitteilungen.<br>Der Port ist standardmäßig abgeschaltet. |
| **22337** | HTTP | Log-Server | Weiterleitung von Nachrichten an den Log-Server. |

Nur einige wenige Kameramodelle können ausgehende Verbindungen aufbauen.

**Clientkomponenten (ausgehende Verbindungen)**

**XProtect Smart Client, XProtect Management Client, XProtect Mobile-Server**

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **80** | HTTP | API Gateway und Management Server-Dienst | Authentifizierung und andere APIs in API Gateway. |
| **443** | HTTPS | API Gateway und Management Server-Dienst | Authentifizierung der Basisnutzer bei aktivierter Verschlüsselung und anderen APIs in API Gateway. |
| **443** | HTTPS | Milestone Systems A/S (doc.milestonesys.com auf 52.178.114.226) | Management Client und Smart Client prüfen gelegentlich, ob die Onlinehilfe zur Verfügung steht, indem sie die URL der Hilfe aufrufen. |
| **7563** | TCP | Recording Server-Dienst | Abrufen von Video- und Audiostreams, PTZ-Befehlen. |
| **22331** | TCP | Event Server-Dienst | Alarme. |

#### XProtect Web Client, XProtect Mobile Client

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **8081** | HTTP | XProtect Mobile-Server | Abrufen von Video- und Audiostreams. |
| **8082** | HTTPS | XProtect Mobile-Server | Abrufen von Video- und Audiostreams. |

API Gateway

| Portnummer | Protokoll | Verbindungen zu... | Zweck |
|---|---|---|---|
| **80** | HTTP | Management Server | RESTful API |
| **443** | HTTPS | Management Server | RESTful API |

# Anwendungspools

Das VMS enthält Standard-Anwendungspools wie.NET v4.5, .NET v4.5 Classic und DefaultAppPool. Die auf Ihrem System verfügbaren Anwendungspools werden im Manager der Internetinformationsdienste (IIS) Manager. Zusätzlich zu den oben erwähnten Standard-Anwendungspools wird eine Reihe von VideoOS-Anwendungspools mit dem Milestone XProtect VMS bereitgestellt.

## Anwendungspools in Milestone XProtect

In der folgenden Tabelle finden Sie einen Überblick über die VideoOS-Anwendungspools, die mit Milestone XProtect bereitgestellt werden.

| Name | Identität | Zweck |
|---|---|---|
| .NET v4.5 | ApplicationPoolId | Standard–IIS-Funktion |
| .NET v4.5 Classic | ApplicationPoolId | Standard–IIS-Funktion |
| DefaultAppPool | ApplicationPoolId | Standard–IIS-Funktion |
| VideoOS ApiGateway | NetworkService | Hostet das XProtect API Gateway, das die zukünftige öffentliche API und das Gateway zum VMS ist. |
| VideoOS Classic | NetworkService | Hostet Legacy-Komponenten wie die lokale Hilfe, hauptsächlich zur Erhaltung der Abwärtskompatibilität. |
| VideoOS IDP | NetworkService | Hostet die Identity Provider API. Der Identity Provider erstellt, pflegt und verwaltet Identitätsinformationen für Basisnutzer und bietet Authentifizierungs- und Registrierungsdienste für abhängige Anwendungen oder Dienste. |
| VideoOS IM | NetworkService | Hostet die XProtect Incident Manager API. Mit XProtect Incident Manager können Organisationen Vorfälle dokumentieren und sie mit |

| Name | Identität | Zweck |
|---|---|---|
| | | Sequenzbeweisen (Video und ggf. Audio) aus ihrem XProtect VMS kombinieren. |
| VideoOS Management Server | NetworkService | Hostet die Konfigurations-API, Serverkomponenten-APIs und andere Management Server Dienste und verwaltet die Benutzerautorisierung. |
| VideoOS ReportServer | NetworkService | Hostet die Webanwendung, die für das Erfassen und Erstellen von Berichten für Alarme und Ereignisse zuständig ist. |
| VideoOS ShareService | NetworkService | Hostet den Service, der Lesezeichen und die Freigabe von Live-Video zwischen Benutzern des XProtect Mobile Clients ermöglicht. |

## Arbeiten mit Anwendungspools

Auf der Seite **Anwendungspools** im Fenster **Internetinformationsdienste (IIS)** können Sie Anwendungspools hinzufügen oder Standardeinstellungen für Anwendungspools festlegen sowie die von jedem Anwendungspool gehosteten Anwendungen anzeigen.

### Öffnen Sie die Seite Anwendungspools

1. Öffnen Sie im Windows **Startmenü** den **Manager für Internetinformationsdienste (IIS)**.
2. Klicken Sie im Fenster **Verbindungen** auf den Namen Ihrer Umgebung und dann auf **Anwendungspools**.
3. Klicken Sie unter **Aktionen** auf **Anwendungspool hinzufügen** oder **Standardeinstellungen für Anwendungspool festlegen**, um eine dieser Aufgaben auszuführen.
4. Wählen Sie auf der Seite **Anwendungspools** einen Anwendungspool aus, um weitere Optionen unter **Aktionen** für jeden Anwendungspool anzuzeigen.

# Produktvergleich

XProtect VMS umfasst folgende Produkte:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

# Lizenzierung

## Lizenzen (Erklärung)

### Kostenlos XProtect Essential+

Wenn Sie XProtect Essential+ installiert haben, können Sie das System und acht Gerätelizenzen kostenlos betreiben. Die automatische Lizenzaktivierung ist aktiviert und Hardwaregeräte werden aktiviert, sowie Sie sie zum System hinzufügen.

Nur wenn Sie ein XProtect Produkt mit erweitertem Funktionsumfang erwerben und Ihren SLC (Software License Code) ändern müssen (siehe Softwarelizenzcode ändern auf Seite 132), könnte der Rest dieses Themas und die übrigen Themen in dieser Dokumentation zum Thema Lizenzierung für Sie relevant sein.

### Lizenzen für XProtect VMS-Produkte (außer XProtect Essential+)

**Softwarelizenzdateien und SLCs**

Wenn Sie Ihre Software und Lizenzen kaufen, erhalten Sie in einer E-Mail:

- Eine Bestellbestätigung und eine Softwarelizenzdatei (SLC) mit der Endung .lic, deren Namen Ihrem SLC (Softwarelizenzcode) entspricht
- Ein Abonnement des Milestone Care Service

Ihr SLC ist auch auf Ihrer Bestellbestätigung gedruckt und besteht aus mehreren Nummern und Buchstaben, die mit Bindestrichen angeordnet sind, wie im Folgenden dargestellt:

- Produktversion 2014 oder früher: xxx-xxxx-xxxx
- Produktversion 2016 oder später: xxx-xxx-xxx-xx-xxxxxx

Die Softwarelizenzdatei enthält alle Informationen über Ihre erworbenen VMS-Produkte, XProtect-Erweiterungen und -Lizenzen. Milestone empfiehlt Ihnen, die Informationen zu Ihren SLC abzuspeichern und eine Kopie Ihrer Softwarelizenzdatei für den späteren Gebrauch an einem sicheren Ort aufzubewahren. Sie finden Ihre SLC auch in dem Fenster **Lizenzinformationen** in Management Client. Sie können das Fenster **Lizenzangaben** in dem Fenster **Seitennavigation** im Knoten -> **Grundlagen** -> **Lizenzangaben** öffnen. Sie benötigen die Softwarelizenzdatei oder Ihren SLC, wenn Sie z.B. ein My Milestone Benutzerkonto erstellen, sich um Support an Ihren Händler wenden, oder wenn Sie an Ihrem System Änderungen vornehmen müssen.

**Gesamtverfahren zur Installation und Lizenzierung**

Laden Sie zunächst die Software von unserer Website (https://www.milestonesys.com/downloads/) herunter. Während der Installation (siehe Installation eines neuen XProtect-Systems auf Seite 156) der Software werden Sie aufgefordert, die Software-Lizenzdatei anzugeben. Ohne Softwarelizenzdatei können Sie die Installation nicht abschließen.

Sobald die Installation abgeschlossen ist und Sie einige Kameras hinzugefügt haben, müssen Sie Ihre Lizenzen aktivieren (siehe Lizenzaktivierung (Erklärung) auf Seite 124. Ihre Lizenzen aktivieren Sie in dem Fenster **Lizenzangaben** in Management Client. Dort finden Sie auch eine Übersicht über Ihre Lizenzen für alle Installationen mit demselben SLC. Sie können das Fenster **Lizenzangaben** in dem Fenster **Seitennavigation** im Knoten -> **Grundlagen** -> **Lizenzangaben** öffnen.

## Lizenztypen

Im Lizenzierungssystem gibt es mehrere verschiedene Lizenztypen XProtect.

### Basislizenzen

Sie haben mindestens eine Basislizenz für eines der XProtect VMS-Produkte. Sie haben ggf. auch eine oder mehrere Basislizenzen für XProtect Erweiterungen.

### Gerätelizenzen

Sie haben mindestens einige Gerätelizenzen. Im Allgemeinen brauchen Sie eine Gerätelizenz je Hardwaregerät mit einer Kamera, die sie zu ihren Systemen zufügen wollen. Dies kann sich jedoch von einem Hardwaregerät zum anderen unterscheiden, und je nachdem, ob das Hardwaregerät Milestone unterstützt wird oder nicht. Weitere Informationen finden Sie unter Unterstützte Hardwaregeräte auf Seite 123 und Nicht unterstützte Hardwaregeräte auf Seite 123.

Wenn Sie die Video-Push-Funktion in XProtect Mobile verwenden möchten, brauchen Sie ebenfalls eine Gerätelizenz für jedes Mobilgerät oder Tablet, das Videoaufzeichnungenper Video-Push an Ihr System senden können soll.

Keine Gerätelizenzen sind für Lautsprecher, Mikrofone oder Eingabe- und Ausgabegeräte erforderlich, die an Ihre Kameras angeschlossen werden.

#### Unterstützte Hardwaregeräte

Im Allgemeinen brauchen Sie eine Gerätelizenz je Hardwaregerät mit einer Kamera, die sie zu ihren Systemen zufügen wollen. Manche unterstützte Hardwaregeräte benötigen jedoch mehr als eine Gerätelizenz. Wie viele Gerätelizenzen Ihre Hardwaregeräte brauchen, finden Sie auf der Liste der unterstützten Hardware auf der Website Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Für Videoencoder mit bis zu 16 Kanälen haben Sie nur eine Geräte Lizenz je IP-Adresse eines Videoencoders. Ein Videoencoder kann eine oder mehrere IP-Adressen aufweisen.

Verfügt der Videoencoder jedoch über mehr als 16 Kanäle, ist für den Videoencoder eine Gerätelizenz je aktivierte Kamera erforderlich - auch für die ersten 16 aktivierten Kameras.

#### Nicht unterstützte Hardwaregeräte

Für ein nicht unterstütztes Hardwaregerät ist eine Gerätelizenz je aktivierte Kamera erforderlich, die einen Videokanal nutzt.

Nicht unterstützte Hardwaregeräte erscheinen nicht auf der Liste der unterstützten Hardware auf der Website Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

#### Kameralizenzen für Milestone Interconnect™

Für die Ausführung von Milestone Interconnect benötigen Sie Milestone Interconnect Kameralizenzen an Ihrem zentralen Standort, um Video von Geräten an Remote-Systemen anzusehen. Die Anzahl der erforderlichen Milestone Interconnect Kameralizenzen ist abhängig von der Anzahl der Hardwaregeräte an den entfernten Standorten, von denen Sie Daten empfangen wollen. Beachten Sie, dass ausschließlich XProtect Corporate als zentraler Standort agieren kann.

#### Lizenzen für XProtect Erweiterungen

Die meisten XProtect Erweiterungen erfordern zusätzliche Lizenztypen. Die Softwarelizenzdatei beinhaltet auch Informationen über Ihre Erweiterungslizenzen. Manche Erweiterungen verfügen über eigene separate Softwarelizenzdateien.

## Lizenzaktivierung (Erklärung)

Ihre SLC muss vor der Installation registriert werden (siehe Softwarelizenzcode registrieren auf Seite 153). Die verschiedenen mit Ihren SLCs verbundenen Lizenzen müssen aktiviert werden, damit das installierte XProtect VMS und XProtect Erweiterungen funktionieren und damit die einzelnen Hardwaregeräte Daten an das System senden können. Eine Übersicht über alle XProtect Lizenztypen finden Sie unter Lizenztypen auf Seite 123.

Lizenzen können auf verschiedene Weise aktiviert werden. Diese stehen alle in dem Fenster **Lizenzangaben** zur Verfügung. Welche die beste Aktivierungsmethode ist, hängt von den Richtlinien Ihrer Organisation ab sowie davon, ob Ihr Management Server Internetzugang hat oder nicht. Wenn Sie wissen möchten, wie Sie Ihre Lizenzen aktivieren müssen, siehe Aktivieren Sie Ihre Lizenzen auf Seite 129.

Nach der ersten Lizenzaktivierung für Ihr XProtect VMS brauchen Sie aufgrund der in das XProtect Lizenzierungssystem eingebauten Flexibilität nicht jedes Mal Gerätelizenzen zu aktivieren, wenn Sie ein Hardwaregerät mit einer Kamera hinzufügen. Weitere Informationen zu diesen Flexibilitäten finden Sie unter Kulanzfrist für die Lizenzaktivierung (Erklärung) auf Seite 125 und Geräteänderungen ohne Aktivierung (Erklärung) auf Seite 125.

### Automatische Lizenzaktivierung (Erklärung)

Für eine einfache Wartung und hohe Flexibilität - und wenn die Richtlinien Ihrer Organisation dies erlauben - empfiehlt Ihnen Milestone, die automatische Lizenzaktivierung einzuschalten. Für die automatische Lizenzaktivierung ist es erforderlich, dass der Management Server online ist. Informationen dazu, wie Sie die automatische Lizenzaktivierung aktivieren können, finden Sie unter Automatische Lizenzaktivierung aktivieren auf Seite 129.

**Die Vorteile, wenn Sie die automatische Lizenzaktivierung aktivieren**

- Das System aktiviert Ihre Hardwaregeräte wenige Minuten nachdem Sie Hardwaregeräte hinzugefügt, entfernt oder ersetzt oder sonstige Änderungen vorgenommen haben, die sich auf die Nutzung Ihrer Lizenzen auswirken. Daher brauchen Sie nur selten eine Lizenzaktivierung von Hand zu starten. Ein paar Ausnahmen finden Sie unter Wann eine manuelle Lizenzaktivierung weiterhin erforderlich ist auf Seite 125.
- Die Anzahl der Geräteänderungen ohne Aktivierung beträgt stets null.
- Es befinden sich keine Hardwaregeräte in einer Kulanzfrist, mit dem Risiko abzulaufen.
- Wenn eine Ihrer Basislizenzen innerhalb von 14 Tagen abläuft, wird Ihr XProtect-System als Vorsichtsmaßnahme jede Nacht automatisch versuchen, Ihre Lizenzen zu aktivieren.

**Wann eine manuelle Lizenzaktivierung weiterhin erforderlich ist**

Wenn Sie an Ihrem System eine der folgenden Änderungen vorgenommen haben, ist eine manuelle Lizenzaktivierung erforderlich.

- Weitere Lizenzen erworben (siehe Erhalten zusätzlicher Lizenzen auf Seite 132)
- Erweiterung auf eine neuere oder technisch ausgefeiltere Version des VMS-System (siehe Upgrade-Anforderungen auf Seite 402)
- Kauf oder Erneuerung eines Milestone Care Abonnements
- Die Möglichkeit erhalten, mehr Geräteänderungen ohne Aktivierung vorzunehmen (siehe Geräteänderungen ohne Aktivierung (Erklärung) auf Seite 125)

## Kulanzfrist für die Lizenzaktivierung (Erklärung)

Wenn Sie Ihr VMS installiert und Geräte (Hardwaregeräte, Milestone Interconnect Kameras oder Türlizenzen) hinzugefügt haben, laufen diese Geräte innerhalb einer Kulanzfrist von 30 Tagen, wenn Sie beschlossen haben, die automatische Lizenzaktivierung nicht einzuschalten. Vor Ablauf der 30-tägigen Kulanzfrist, und wenn Sie keine Geräteänderungen ohne Aktivierung mehr übrig haben, müssen Sie entweder Ihre Lizenzen aktivieren, oder Ihre Geräte senden keine Videoaufzeichnungen mehr an Ihr Überwachungssystem.

## Geräteänderungen ohne Aktivierung (Erklärung)

Die Funktionsänderungen der Geräte ohne Aktivierung geben dem XProtect Lizenzierungssystem eine eingebaute Flexibilität. Selbst wenn Sie also beschlossen haben, die Lizenzen von Hand zu aktivieren, brauchen Sie nicht unbedingt jedes Mal Lizenzen zu aktivieren, wenn Sie Hardwaregeräte hinzufügen oder entfernen.

Die Zahl der Geräteänderungen ohne Aktivierung unterscheidet sich von Installation zu Installation und wird anhand verschiedener Variablen berechnet. Eine detaillierte Beschreibung finden Sie unter Berechnung der verfügbaren Anzahl Geräteänderungen ohne Aktivierung (Erklärung) auf Seite 126.

Ein Jahr nach Ihrer letzten Lizenzaktivierung wird die Anzahl der von Ihnen vorgenommenen Geräteänderungen ohne Aktivierung automatisch auf Null zurückgesetzt. Nach dem Zurücksetzen können Sie weiter Geräte hinzufügen und austauschen, ohne die Lizenzen aktivieren zu müssen.

Wenn Ihr Überwachungssystem für längere Zeit offline ist (zum Beispiel ein Überwachungssystem auf einem Schiff, das sich auf großer Fahrt befindet, oder an einem sehr entlegenen Ort ohne Internetzugriff), können Sie sich an Ihren Milestone-Vertriebspartner wenden und um eine höhere Zahl von Geräteänderungen ohne Aktivierung bitten.

Ihrem Distributor müssen Sie erklären, warum Sie meinen, für eine höhere Zahl von Geräteänderungen ohne Aktivierung qualifiziert zu sein. Milestone entscheidet jede Anfrage auf individueller Basis. Wenn Ihnen mehr Geräteänderungen ohne Aktivierung gewährt werden, müssen Sie Ihre Lizenzen aktivieren, um die höhere Zahl im XProtect-System zu registrieren.

## Berechnung der verfügbaren Anzahl Geräteänderungen ohne Aktivierung (Erklärung)

Die verfügbare Anzahl Geräteänderungen ohne Aktivierung wird anhand dreier Variablen berechnet. Wenn Sie über mehrere Installationen der Milestone-Software verfügen, gelten die Variablen für jede von ihnen separat. Die Variablen umfassen:

- **C%** ist ein fester Prozentsatz der Gesamtmenge aktivierter Lizenzen
- **Cmin** ist ein fester Minimalwert der Zahl von Geräteänderungen ohne Aktivierung
- **Cmax** ist ein fester Maximalwert der Zahl von Geräteänderungen ohne Aktivierung

Die Zahl der Geräteänderungen ohne Aktivierung kann nie unter dem **Cmin**-Wert bzw. über dem **Cmax**-Wert liegen. Der anhand der **C%**-Variable errechnete Wert hängt davon ab, wie viele aktivierte Geräte sich in den einzelnen Installationen Ihres Systems befinden. Geräte, die mittels Geräteänderungen ohne Aktivierung hinzugefügt wurden, werden von der **C%**-Variable nicht als aktiviert gezählt.

Milestone definiert die Werte aller drei Variablen, wobei sich die Werte ohne Ankündigung ändern können. Die Werte der Variablen hängen vom jeweiligen Produkt ab.

**Beispiele basieren auf folgenden Werten: C% = 15 %, Cmin = 10 und Cmax = 100**

Sie erwerben 100 Gerätelizenzen. Dann fügen Sie 100 Kameras zum System hinzu. Wenn Sie die automatische Lizenzaktivierung nicht eingeschaltet haben, ist die Anzahl der Geräteänderungen ohne Aktivierung immer noch null. Sie aktivieren Ihre Lizenzen und haben jetzt 15 Geräteänderungen ohne Aktivierung.

Sie erwerben 100 Gerätelizenzen. Dann fügen Sie 100 Kameras zum System hinzu und aktivieren die Lizenzen. Die Anzahl der Geräteänderungen ohne Aktivierung beträgt jetzt 15. Dann beschließen sie, ein Hardwaregeräte aus dem System zu löschen. Jetzt haben Sie 99 aktivierte Geräte, und die Anzahl der Geräteänderungen ohne Aktivierung ist auf 14 zurückgegangenen.

Sie erwerben 1000 Gerätelizenzen. Dann fügen Sie 1000 Kameras hinzu und aktivieren die Lizenzen. Die Zahl Ihrer Geräteänderungen ohne Aktivierung beträgt jetzt 100. Nach der **C%**-Variable müssen Sie jetzt 150 Geräteänderungen ohne Aktivierung gehabt haben, die **Cmax**-Variable erlaubt Ihnen jedoch nur 100 Geräteänderungen ohne Aktivierung.

Sie erwerben 10 Gerätelizenzen. Dann fügen Sie 10 Kameras zum System hinzu und aktivieren die Lizenzen. Die Anzahl Ihrer Geräteänderungen ohne Aktivierung beträgt jetzt 10, wegen der **Cmin**-Variable. Wenn die Anzahl lediglich anhand der **C%**-Variable berechnet würde, hätten Sie lediglich 1 (15% von 10 = 1,5, gerundet auf 1) gehab.

Sie erwerben 115 Gerätelizenzen. Dann fügen Sie 100 Kameras zum System hinzu und aktivieren die Lizenzen. Die Anzahl Ihrer Geräteänderungen ohne Aktivierung beträgt jetzt 15. Sie fügen weitere 15 Kameras hinzu, ohne sie zu aktivieren, wobei Sie 15 von 15 Ihrer Geräteänderungen ohne Aktivierung verbrauchen. Jetzt entfernen Sie 50 der Kameras aus dem System, und die Anzahl der Geräteänderungen ohne Aktivierung nimmt auf 7 ab. Das bedeutet, dass 8 der vorher innerhalb der 15 Geräteänderungen ohne Aktivierung hinzugefügten Kameras in die Karenzfrist fallen. Jetzt fügen Sie 50 neue Kameras hinzu. Da Sie beim letzten Mal, als Sie die Lizenzen aktiviert haben, 100 Kameras zum System hinzugefügt haben, nimmt die Anzahl Geräte ohne Aktivierung auf 15 ab, und die 8 Kameras, die in eine Kulanzfrist gefallen sind, werden wieder zu Geräteänderungen ohne Aktivierung. Die 50 neuen Kameras befinden sich nun in einem Übergangszeitraum.

## Milestone Care™ (Erklärung)

Milestone Care ist der Name des Komplettservice- und Supportprogramms für XProtect-Produkte über deren gesamte Lebensdauer.

Milestone Care gibt Ihnen Zugriff auf Selbsthilfematerialien verschiedener Art, z. B. Knowledge Base-Artikel, Anleitungen und Tutorials auf unserer Support-Website (https://www.milestonesys.com/support/).

Für weitere Vorteile können Sie technisch ausgefeiltere Milestone Care Abonnements kaufen.

### Milestone Care Plus

Wenn Sie ein Milestone Care Plus Abonnement haben, haben Sie auch Zugriff auf kostenlose Updates für Ihr aktuelles XProtect VMS-Produkt und können zu einem Vorteilspreis auf technisch ausgefeiltere XProtect VMS-Produkte aktualisieren. Milestone Care Plus bietet auch zusätzliche Funktionalität:

- Der Kunden Dashboard Dienst
- Die Smart Connect-Funktion
- Die vollständige Push-Benachrichtigungsfunktion

### Milestone Care Premium

Wenn Sie ein Milestone Care Premium-Abonnement besitzen, können Sie das Milestone-Support-Team auch kontaktieren. Denken Sie bitte daran, Angaben zu Ihrer Milestone Care ID zu machen, wenn Sie sich an den Milestone Support wenden.

### Ablauf, Verlängerung und Kauf von technisch ausgefeilteren Milestone Care Abonnements

Das Ablaufdatum der technisch aufwändigeren Milestone Care Plus und Milestone Care Premium Abonnementtypen sehen Sie in dem Fenster **Lizenzangaben** in der Tabelle **Installierte Produkte**. Siehe Installierte Produkte auf Seite 134.

Wenn Sie beschließen, ein Milestone Care-Abonnement zu erwerben oder zu verlängern, nachdem Sie Ihr System installiert haben, müssen Sie Ihre Lizenzen von Hand aktivieren, bevor die korrekten Milestone Care Informationen angezeigt werden. Siehe Lizenzen online aktivieren auf Seite 130 oder Lizenzen offline aktivieren auf Seite 131.

## Lizenzen und Ersatzhardware (Erklärung)

Wenn eine Kamera im System fehlerhaft ist, oder Sie die Kamera aus sonstigen Gründen durch eine neue ersetzen wollen, gibt es einige bewährte Methoden dafür, wie Sie dies tun sollten.

Wenn Sie eine Kamera aus einem Aufzeichnungsserver entfernen, machen Sie damit eine Gerätelizenz frei, verlieren jedoch auch den vollen Zugriff auf alle Datenbanken (Kameras, Mikrofone, Eingabegeräte, Ausgabegeräte) sowie auch die Einstellungen der alten Kamera. Nutzen Sie die entsprechende Option weiter unten, um den Zugriff der alten Kamera auf die Datenbank zu behalten und deren Einstellungen nach Ersatz durch eine neue Kamera wiederzuverwenden.

### Kamera durch eine ähnliche Kamera ersetzen

Wenn Sie eine Kamera durch eine ähnliche Kamera ersetzen (Hersteller, Marke und Modell), und der neuen Kamera dieselbe IP-Adresse zuweisen wieder alten, behalten Sie den vollen Zugriff auf alle Datenbanken, den die alte Kamera hatte. Die neue Kamera verwendet dieselben Datenbanken und Einstellungen weiter wie die alte. In diesem Fall schließen Sie das Netzwerkkabel der alten Kamera an die neue an, ohne irgendwelche Einstellungen in Management Client zu ändern.

### Kamera durch eine andere Kamera ersetzen

Wenn Sie eine Kamera durch eine äandere Kamera ersetzen (Hersteller, Marke und Modell), müssen Sie den Assistenten **Hardware ersetzen** verwenden (siehe Hardware ersetzen auf Seite 373), um alle relevanten Datenbanken der alten Kamera mit der neuen zu verknüpfen und die Einstellungen der alten Kamera weiter zu verwenden.

### Lizenzaktivierung nach Hardwareaustausch

Wenn Sie die automatische Lizenzaktivierung einschalten (siehe Automatische Lizenzaktivierung aktivieren auf Seite 129), wird die neue Kamera automatisch aktiviert.

Wenn die automatische Lizenzaktivierung abgeschaltet ist und alle verfügbaren Geräteänderungen ohne Aktivierung aufgebraucht sind (siehe Geräteänderungen ohne Aktivierung (Erklärung) auf Seite 125), müssen Sie Ihre Lizenzen von Hand aktivieren. Weitere Informationen dazu, wie Lizenzen von Hand aktiviert werden, finden Sie unter Lizenzen online aktivieren auf Seite 130 oder Lizenzen offline aktivieren auf Seite 131.

# Verschaffen Sie sich den Überblick über Ihre Lizenzen

Es gibt viele Gründe, warum Sie sich einen Überblick über Ihre SLCs und die Anzahl der von Ihnen erworbenen Lizenzen sowie über deren Status verschaffen wollen könnten. Hier nur einige davon:

- Sie möchten ein oder mehrere Hardwaregeräte hinzufügen, aber haben Sie auch ungenutzte Gerätelizenzen, oder müssen Sie neue erwerben?
- Endet die Frist für manche Ihrer Hardwaregeräte bald? Dann müssen Sie sie aktivieren, bevor sie keine Daten mehr an das VMS senden.
- Sie wissen von früheren Supportkontakten, dass diese Angaben zu Ihren SLC und Ihrer Milestone Care ID benötigten, damit sie Ihnen helfen konnten. Aber welche?
- Sie verfügen über viele Installationen von XProtect und verwenden dieselbe SLC für alle Installationen, aber wo werden die Lizenzen verwendet und was ist jeweils ihr Status?

Alle oben genannten und weitere Angaben finden Sie im Fenster **Lizenzangaben**.

Sie können das Fenster **Lizenzangaben** in dem Fenster **Seitennavigation** im Knoten -> **Grundlagen** -> **Lizenzangaben** öffnen.

Näheres zu den verschiedenen Informationen und Funktionen, die in dem Fenster **Lizenzangaben** zur Verfügung gestellt werden, finden Sie unter Das Fenster "Lizenzangaben" auf Seite 133.

# Aktivieren Sie Ihre Lizenzen

Lizenzen können auf verschiedene Weise aktiviert werden. Diese stehen alle in dem Fenster **Lizenzangaben** zur Verfügung. Welche die beste Aktivierungsmethode ist, hängt von den Richtlinien Ihrer Organisation ab sowie davon, ob Ihr Management Server Internetzugang hat oder nicht.

Sie können das Fenster **Lizenzangaben** in dem Fenster **Seitennavigation** im Knoten -> **Grundlagen** -> **Lizenzangaben** öffnen.

Näheres zu den verschiedenen Informationen und Funktionen, die in dem Fenster **Lizenzangaben** zur Verfügung gestellt werden, finden Sie unter Das Fenster "Lizenzangaben" auf Seite 133.

## Automatische Lizenzaktivierung aktivieren

Für eine einfache Wartung und hohe Flexibilität - und wenn die Richtlinien Ihrer Organisation dies erlauben - empfiehlt Ihnen Milestone, die automatische Lizenzaktivierung einzuschalten. Für die automatische Lizenzaktivierung ist es erforderlich, dass der Management Server online ist.

Wenn Sie wissen möchten, welche Vorteile es hat, wenn Sie die automatische Lizenzaktivierung einschalten, siehe Automatische Lizenzaktivierung (Erklärung) auf Seite 124.

1. Wählen Sie im Fenster **Seitennavigation** -> im Knoten **Grundlagen** -> **Lizenzangaben Automatische Lizenzaktivierung einschalten**.
2. Geben Sie den Benutzernamen und das Passwort ein, die Sie für die automatische Lizenzaktivierung verwenden möchten:
   - Wenn Sie ein bereits vorhandener Benutzer sind, geben Sie Ihren Benutzernamen und das Passwort ein, um sich im Software-Registrierungssystem anzumelden
   - Wenn Sie ein neuer Benutzer sind, klicken Sie zur Einrichtung eines neuen Benutzerkontos auf den Link **Neuen Benutzer erstellen**, und folgen Sie den Anweisungen zum Registrierungsverfahren. Wenn Sie Ihren Softwarelizenzcode (SLC) noch nicht registriert haben, müssen Sie das nun tun

   Die Anmeldeinformationen werden in einer Datei auf dem Management-Server gespeichert.
3. Klicken Sie auf **OK**.

Wenn Sie Ihren Benutzernamen und/oder das Passwort für die automatische Aktivierung später ändern möchten, klicken Sie auf den Link **Aktivierungs-Anmeldeinformationen bearbeiten**.

## Automatische Lizenzaktivierung deaktivieren

Wenn die automatische Lizenzaktivierung in Ihrer Organisation nicht verwendet werden darf, oder Sie es sich einfach anders überlegt haben, können Sie die automatische Lizenzaktivierung auch abschalten.

Wie Sie sie abschalten, hängt davon ab, ob Sie planen, die automatische Lizenzaktivierung später wieder zu verwenden oder nicht.

**Abschalten, das Passwort jedoch zum späteren Gebrauch beibehalten:**

1. Löschen Sie im Fenster **Seitennavigation** -> im Knoten **Grundlagen** -> **Lizenzangaben** die Option **Automatische Lizenzaktivierung einschalten**. Das Passwort und der Benutzername bleiben weiterhin auf dem Management-Server gespeichert.

**Abschalten und Passwort löschen:**

1. Klicken Sie im Fenster **Seitennavigation** -> im Knoten **Grundlagen** -> **Lizenzangaben** auf **Anmeldedaten für die Aktivierung bearbeiten**.
2. Klicken Sie auf **Passwort löschen**.
3. Bestätigen Sie, dass Sie das Passwort und den Benutzernamen vom Management-Server löschen möchten.

## Lizenzen online aktivieren

Wenn der Management Server Zugriff auf das Internet hat, Sie die Aktivierung aber lieber von Hand starten wollen, ist dies für Sie die einfachste Option zur Aktivierung der Lizenz.

1. Wählen Sie im Fenster **Seitennavigation** -> im Knoten **Grundlagen** -> **Lizenzangaben** die Option **automatische Lizenzaktivierung einschalten**, und dann **Online**.
2. Das Dialogfeld **Online aktivieren** wird angezeigt:
    - Wenn Sie ein bereits vorhandener Benutzer sind, geben Sie Ihren Benutzernamen und das Passwort ein
    - Wenn Sie ein neuer Benutzer sind, klicken Sie zur Einrichtung eines neuen Benutzerkontos auf den Link **Neuen Benutzer erstellen**. Wenn Sie Ihren Softwarelizenzcode (SLC) noch nicht registriert haben, müssen Sie das nun tun
3. Klicken Sie auf **OK**.

Wenn Sie bei der Online-Aktivierung eine Fehlermeldung erhalten, folgen Sie den Anweisungen auf dem Bildschirm, um das Problem zu beheben oder wenden Sie sich an den Milestone-Support.

## Lizenzen offline aktivieren

Wenn Ihre Organisation nicht zulässt, dass der Management Server Zugriff auf das Internet hat, müssen Sie die Lizenzen von Hand und offline aktivieren.

1. Wählen Sie im Fenster **Seitennavigation** den Knoten-> **Grundlagen** -> **Lizenzangaben**, **Lizenzen von Hand aktivieren** > **Offline** > **Lizenz zur Aktivierung exportieren**, um eine License Request File (.lrq) zu exportieren, einschließlich der Angaben zu den von Ihnen hinzugefügten Hardwaregeräten und weiteren Elementen, für die eine Lizenz erforderlich ist.
2. Die License Request File (.lrq) erhält automatisch den gleichen Namen wie Ihre SLC. Wenn Sie mehrere Standorte haben, denken Sie bitte daran, die Dateien umzubenennen, so dass Sie leicht erkennen können, welche Datei zu welchen Standort gehört.
3. Kopieren Sie die License Request File auf einen Computer mit Internetzugang und Protokoll auf unsere Website (https://online.milestonesys.com/), um die aktivierte Software License File (.lic) zu erhalten.
4. Kopieren Sie die .lic-Datei, die Sie erhalten, auf Ihren Computer mit Management Client. Die Datei hat den gleichen Namen erhalten wie Ihre License Request File.
5. Wählen Sie im Fenster **Seitennavigation** den Knoten-> **Grundlagen** -> **Lizenzangaben**, **Lizenzen offline aktivieren** > **Aktivierte Lizenz importieren**, und wählen Sie dann die Aktivierte Software License File aus, um sie zu importieren und damit Ihre Lizenzen zu aktivieren.
6. Klicken Sie auf **Fertig stellen**, um den Aktivierungsvorgang zu beenden.

## Lizenzen nach Übergangszeitraum aktivieren

Wenn Sie sich für die manuelle Lizenzaktivierung entschieden haben, und vergessen haben, eine Lizenz innerhalb der Frist zu aktivieren (Hardwaregerät, Milestone Interconnect Kamera, Türlizenzen, oder sonstige), so steht das Gerät, das die Lizenz nutzt, nicht mehr zur Verfügung und kann keine Daten mehr an das Überwachungssystem senden

Selbst wenn die Frist für eine Lizenz abgelaufen ist, werden die von Ihnen vorgenommene Konfiguration und die Einstellungen für das Gerät gespeichert und später verwendet, wenn die Lizenz aktiviert wird.

Um die Geräte wieder zu aktivieren, die nicht mehr zur Verfügung stehen, aktivieren Sie die Lizenzen von Hand auf die von Ihnen bevorzugte Weise. Weitere Informationen finden Sie unter Lizenzen offline aktivieren auf Seite 131 oder Lizenzen online aktivieren auf Seite 130.

## Erhalten zusätzlicher Lizenzen

Wenn Sie mehr Hardwaregeräte, Milestone Interconnect Systeme, Türen oder sonstige Elemente hinzufügen wollen oder bereits hinzugefügt haben als Sie aktuell über Lizenzen verfügen, müssen Sie zusätzliche Lizenzen erwerben, damit diese Elemente an Ihr System Daten senden können:

- Wenn Sie zusätzliche Lizenzen für Ihr System benötigen, wenden Sie sich an Ihren XProtect Produktpartner

Wenn Sie für Ihre vorhandenesÜberwachungssystemversion neue Lizenzen erworben haben:

- Sorgen Sie einfach für eine manuelle Aktivierung Ihrer Lizenzen, um Zugriff auf die neuen Lizenzen zu erhalten. Weitere Informationen finden Sie unter Lizenzen online aktivieren auf Seite 130 oder Lizenzen offline aktivieren auf Seite 131.

Wenn Sie neue Lizenzen und eine erweiterte Überwachungssystemversion erworben haben:

- Sie erhalten eine aktualisierte Software-Lizenzdatei (.lic) inklusive der neuen Lizenzen und der neuen Version. Bei der Installation der neuen Version müssen Sie die neue Software-Lizenzdatei verwenden. Weitere Informationen finden Sie unter Upgrade-Anforderungen auf Seite 402

## Softwarelizenzcode ändern

Wenn Sie eine Installation mit einem temporären Softwarelizenzcode (SLC) durchführen oder ein Upgrade auf ein höherwertiges XProtect Produkt vorgenommen haben, können Sie Ihren SLC in einen permanenten oder höherwertigen SLC ändern. Sie können Ihren SLC ändern, ohne deinstallieren oder neuinstallieren zu müssen, wenn Sie Ihre neue Softwarelizenzdatei erhalten haben.

Dies können Sie lokal auf dem Management Server oder per Fernzugriff über Management Client vornehmen.

### Vom Taskleistensymbol des Management Servers aus

1. Auf dem Management-Server gehen Sie zum Benachrichtigungsbereich der Taskleiste.

2. Klicken Sie mit der rechten Maustaste auf das **Management-Server**-Symbol und wählen Sie **Lizenz ändern** aus.
3. Klicken Sie auf **Lizenz importieren**.
4. Wählen Sie als nächstes die Softwarelizenzdatei aus, die zu diesem Zweck gespeichert wurde. Wenn Sie fertig sind, wird der Speicherort der ausgewählten Softwarelizenzdatei direkt unter der Schaltfläche **Lizenz importieren** hinzugefügt.
5. Klicken Sie auf **OK**, und Sie sind bereit, den SLC zu registrieren. Siehe Softwarelizenzcode registrieren auf Seite 153.

### Von Management Client

1. Kopieren Sie die .lic-Datei, die Sie erhalten, auf Ihren Computer mit Management Client.
2. Wählen Sie im Bereich **Standortnavigation** -> den Knoten **Basics** -> **Lizenzinformationen**, wählen Sie dann **Lizenz offline aktivieren** > **Aktivierte Lizenz importieren** und wählen Sie dann die zu importierende Softwarelizenzdatei aus.
3. Akzeptieren Sie beim Öffnen, dass die Softwarelizenzdatei eine andere ist als die derzeit verwendete.
4. Sie sind jetzt bereit für die Registrierung der SLC. Siehe Softwarelizenzcode registrieren auf Seite 153.

Die Softwarelizenzdatei wird nur importiert und geändert, aber nicht aktiviert. Denken Sie daran, Ihre Lizenz zu aktivieren. Weitere Informationen finden Sie unter Aktivieren Sie Ihre Lizenzen auf Seite 129.

Im laufenden Betrieb XProtect Essential+ können Sie die Lizenz nur über das Taskleistensymbol des Management Servers ändern. Die Lizenz kann von Management Client nicht geändert werden.

## Das Fenster "Lizenzangaben"

In dem Fenster **Lizenzabgaben** haben Sie den Überblick über alle Lizenzen, die zur selben Softwarelizenzdatei sowohl an diesem Standort als auch an allen anderen Standorten gehören, über Ihre Milestone Care-Abonnements, und Sie können entscheiden, wie Sie ihre Lizenzen aktivieren möchten.

Sie können das Fenster **Lizenzangaben** in dem Fenster **Seitennavigation** im Knoten -> **Grundlagen** -> **Lizenzangaben** öffnen.

Eine grobe Übersicht darüber, wie das XProtect Lizenzsystem funktioniert, finden Sie unter Lizenzen (Erklärung) auf Seite 122.

### Lizenziert für

In diesem Bereich im Fenster **Lizenzangaben** sind die Kontaktangaben des Lizenzeigentümers aufgeführt , die bei der Registrierung der Software eingegeben wurden.

Wenn Sie dem Bereich **Lizenziert für** nicht sehen können, klicken Sie auf die Schaltfläche **Aktualisieren** in der unteren rechten Ecke des Fensters.

Klicken Sie auf **Details bearbeiten**, um die Angaben zum Lizenzinhaber zu bearbeiten. Klicken Sie auf **Endbenutzer-Lizenzvereinbarung**, um die Endbenutzer-Lizenzvereinbarung zu sehen, die Sie vor der Installation angenommen haben.

### Milestone Care

Hier finden Sie Informationen zu Ihrem derzeitigen Milestone Care™ Abonnement. Die Ablaufdaten Ihrer Abonnements sehen Sie in der Tabelle **Installierte Produkte** weiter unten.

Weitere Informationen zu Milestone Care erhalten Sie über die Links, oder unter Milestone Care™ (Erklärung) auf Seite 127.

### Installierte Produkte

Listet folgende Angaben über alle installierten Basislizenzen für XProtect VMS und XProtect Erweiterungen auf, die dieselbe Softwarelizenzdatei nutzen:

- Produkte und Versionen
- Dem Softwarelizenzcode (SLC) der Produkte
- Das Ablaufdatum Ihrer SLC. Normalerweise unbegrenzt
- Das Ablaufdatum Ihres Milestone Care Plus-Abonnements
- Das Ablaufdatum Ihres Milestone Care Premium-Abonnements

**Installed Products**

| Product Version | Software License Code | Expiration Date | Milestone Care Plus | Milestone Care Premium |
|---|---|---|---|---|
| XProtect Corporate 20 R | M01-C01-211-01- | Unlimited | 16-11-20 | 16-11-20 |
| Milestone XProtect Smart Wall | M01-P03-100-01- | Unlimited | Unlimited | |
| Milestone XProtect Access | M01-P01-011-01- | Unlimited | Unlimited | |
| Milestone XProtect Transact | M01-P08-100-01- | Unlimited | Unlimited | |

### Lizenzübersicht - Alle Sites

Hier ist die Anzahl der aktivierten Gerätelizenzen und sonstiger Lizenzen in Ihrer Software License File aufgeführt, sowie die Gesamtzahl der auf Ihrem System verfügbaren Lizenzen. Hier erkennen Sie mit einem Blick, ob Sie Ihr System noch erweitern können, ohne zusätzliche Lizenzen zu erwerben.

Für eine detaillierte Übersicht des Status Ihrer an anderen Standorten aktivierten Lizenzen klicken Sie auf den Link **Lizenzdetails - alle Standorte**. Die verfügbaren angezeigten Informationen finden Sie im Abschnitt **Lizenzdetails - aktueller Standort** weiter unten.

**License Overview - All sites** License Details - All Sites...

| License Type | Activated |
|---|---|
| Device Licenses | 51 out of 100 |
| Milestone Interconnect Camera | 0 out of 100 |
| Access control door | 9 out of 2002 |
| Transaction source | 1 out of 101 |

Wenn Sie über Lizenzen für XProtect Erweiterungen verfügen, finden Sie weitere Einzelheiten zu diesen an den gesonderten Knoten zu XProtect Erweiterungen in dem Fenster **Seitennavigation**.

### Lizenzdetails – aktueller Standort

In der Spalte **Aktiviert** ist die Anzahl der an diesem Standort aktivierten Lizenzen oder sonstigen Lizenzen aufgeführt.

Die Anzahl der verwendeten Geräteänderungen ohne Aktivierung (siehe Geräteänderungen ohne Aktivierung (Erklärung) auf Seite 125) und wie viele Ihnen im Jahr zur Verfügung stehen finden Sie auch in der Spalte **Änderungen ohne Aktivierung**.

Wenn Sie Lizenzen haben, die noch nicht aktiviert sind und deshalb im Übergangszeitraum laufen, sind diese in der Spalte **Im Übergangszeitraum** aufgeführt. Das Ablaufdatum der ersten Lizenz, die abläuft, wird unter der Tabelle in Rot angezeigt.

Wenn Sie vergessen, Lizenzen vor Ablauf des Übergangszeitraums zu aktivieren, senden sie keine Videodaten mehr an das System. Diese Lizenzen sind in der Spalte **Übergangszeitraum abgelaufen** aufgeführt. Weitere Informationen finden Sie unter Lizenzen nach Übergangszeitraum aktivieren auf Seite 131.

Wenn Sie mehr Lizenzen verwendet haben, als verfügbar sind, sind diese in der Spalte **Ohne Lizenz** aufgeführt. Sie können im System nicht verwendet werden. Weitere Informationen finden Sie unter Erhalten zusätzlicher Lizenzen auf Seite 132.

Wenn Sie über Lizenzen innerhalb einer Kulanzfrist, mit abgelaufener Kulanzfrist oder ohne Lizenz verfügen, erhalten Sie, jedes Mal, wenn Sie sich bei Ihrem Management Client anmelden, eine Benachrichtigung zur Erinnerung.

**License Details - Current Site:** [redacted]

| License Type | Activated | Changes without activation | In Grace Period | Grace Period Expired | Without License |
|---|---|---|---|---|---|
| Device Licenses | 32 | 0 out of 10 | 0 | 0 | 0 |
| Milestone Interconnect Camera | 11 | N/A | 0 | 0 | 0 |
| Access control door | 9 | N/A | 0 | 0 | 0 |
| Transaction source | 1 | N/A | 0 | 0 | 0 |

Wenn Sie über Hardwaregeräte verfügen, die mehr als eine Lizenz verwenden, erscheint ein Link mit dem Text **Klicken Sie hier, um den vollständigen Gerätelizenzbericht zu öffnen** unter der Tabelle **Lizenzdetails - aktueller Standort**. Wenn Sie auf den Link klicken, können Sie sehen, wie viele Gerätelizenzen für jedes dieser Hardwaregeräte erforderlich sind.

Geräte ohne Lizenzen sind in Management Client durch ein Ausrufezeichen gekennzeichnet. Das Ausrufezeichen wird auch für andere Zwecke verwendet. Bewegen Sie den Mauszeiger auf das Ausrufezeichen, um die Bedeutung anzuzeigen.

### Funktionen zur Lizenzaktivierung

Unter den drei Tabellen befinden sich folgende Elemente:

- Ein Kontrollkästchen zum Aktivieren der automatischen Lizenzaktivierung und ein Link zum Bearbeiten der Benutzeranmeldedaten zur automatischen Aktivierung. Weitere Informationen finden Sie unter Automatische Lizenzaktivierung (Erklärung) auf Seite 124 und Automatische Lizenzaktivierung aktivieren auf Seite 129.
  Wenn die automatische Aktivierung fehlgeschlagen ist, wird eine Fehlermeldung in Rot angezeigt. Weitere Informationen erhalten Sie über das Link **Einzelheiten**.
  Einige Lizenzen , wie z.B. XProtect Essential+, sind mit eingeschalteter automatischer Lizenzaktivierung installiert, die nicht abgeschaltet werden kann.
- Eine Dropdown-Liste zur manuellen Aktivierung von Lizenzen (online oder offline). Weitere Informationen finden Sie unter Lizenzen online aktivieren auf Seite 130 und Lizenzen offline aktivieren auf Seite 131.
- In der unteren rechten Ecke des Fensters finden Sie die Angabe, wann Ihre Lizenzen zuletzt aktiviert wurden (automatisch oder von Hand) und wann die Angaben in diesem Fenster aktualisiert wurden. Die Zeitstempel stammen vom Server, nicht vom lokalen Computer

# Anforderungen und Hinweise

## Sommerzeit (Erklärung)

Während der Sommerzeit werden die Uhren um eine Stunde nach vorne gestellt, damit es abends länger hell ist und morgens noch dunkler ist. Länder/Regionen verwenden die Sommerzeit unterschiedlich.

Wenn Sie mit einem Überwachungssystem arbeiten, das von sich aus zeitempfindlich ist, ist es wichtig, zu wissen, wie es mit der Sommerzeit umgeht.

> ⚠ Ändern Sie die Sommerzeit-Einstellung nicht während der Sommerzeit, oder wenn Sie Aufnahmen aus der Sommerzeit haben.

**Frühling: Umschalten von Standardzeit auf Sommerzeit**

Die Umstellung von der Standard- auf die Sommerzeit ist einfach, da die Uhr lediglich eine Stunde nach vorne gestellt wird.

Beispiel:

Die Uhr springt von 02:00 Uhr Standardzeit auf 03:00 Uhr Sommerzeit und der Tag hat nur 23 Stunden. In diesem Fall gibt es für die Zeit zwischen 02:00 Uhr und 03:00 Uhr morgens keine Daten, da diese Stunde an diesem Tag nicht existierte.

**Herbst: Umschalten von Sommerzeit auf Standardzeit**

Wenn Sie im Herbst von Sommerzeit auf Standardzeit umschalten, springt die Uhr eine Stunde zurück.

Beispiel:

Die Uhr springt von 02:00 Uhr Sommerzeit auf 01:00 Uhr Standardzeit zurück. Die Stunde wiederholt sich somit und der Tag hat 25 Stunden. Nach 01:59:59 springt die Uhrzeit auf 01:00:00 zurück. Würde das System nicht reagieren, würde die Stunde erneut aufgezeichnet werden, sodass die erste Instanz von 01:30 Uhr durch die zweite Instanz von 01:30 Uhr überschrieben würde.

Um dies zu verhindern, archiviert das System das aktuelle Video für den Fall, dass sich die Systemzeit um mehr als fünf Minuten ändert. Sie können sich die erste Instanz von 01:00 Uhr nicht direkt in Clients ansehen, die Daten werden jedoch aufgezeichnet und sind sicher. Sie können sich das Video in XProtect Smart Client ansehen, indem Sie die archivierte Datenbank direkt öffnen.

## Zeitserver (Erklärung)

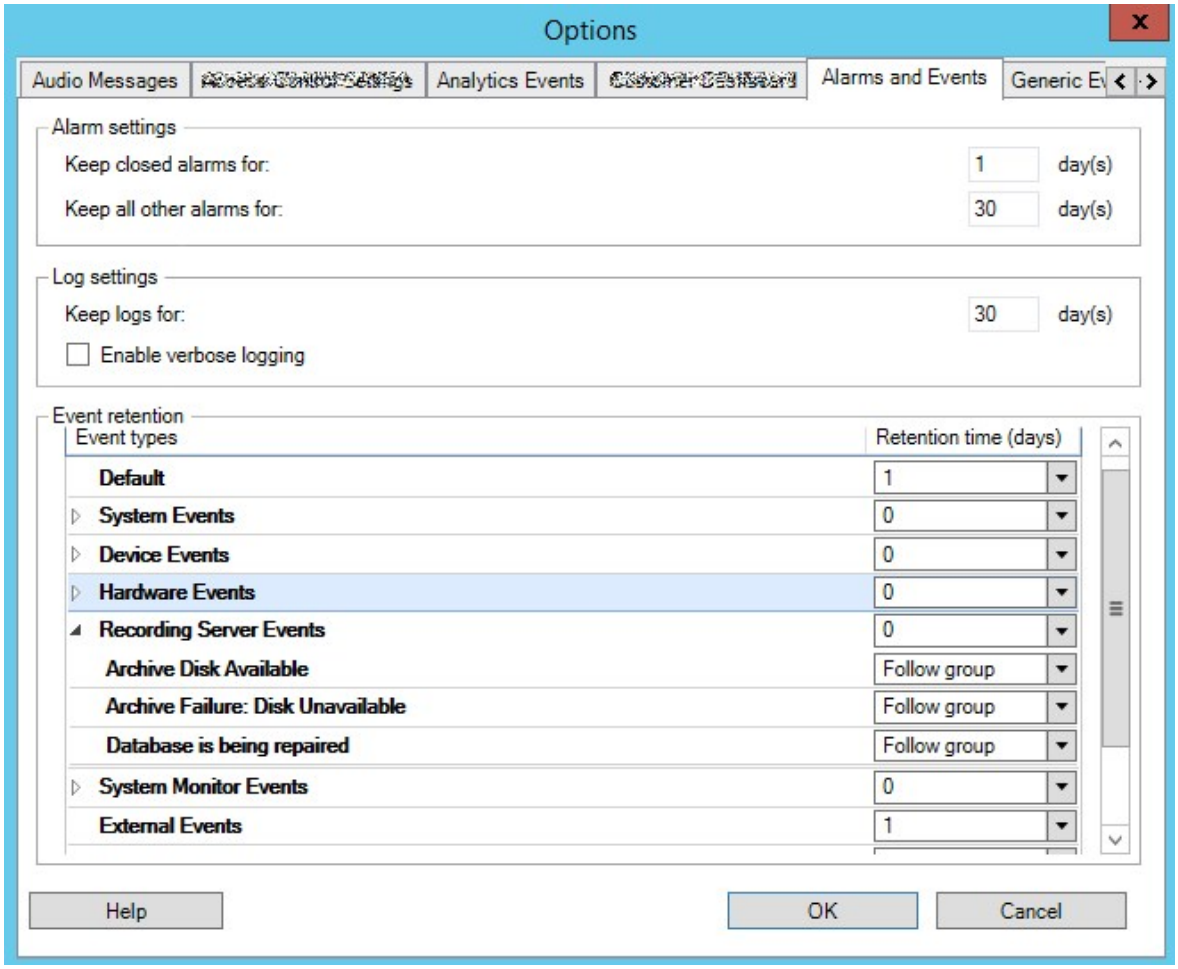
Sobald Ihr System Bilder empfängt, werden diese umgehend mit einem Zeitstempel versehen. Da es sich bei Kameras um separate Einheiten handelt, die über eigene Zeitmessgeräte verfügen können, stimmen die Kamerazeit und die Systemzeit nicht immer überein. Dies kann hin und wieder zu Verwirrung führen. Falls Ihre Kamera Zeitstempel unterstützt, empfiehlt Milestone, die Kamera- und Systemzeit über einen Zeitserver automatisch zu synchronisieren, um konsistente Zeitangaben zu erhalten.

Wenn Sie weitere Informationen zur Konfiguration eines Zeitservers benötigen, suchen Sie auf der Microsoft-Website (https://www.microsoft.com/) nach '**Zeitserver**', '**Zeitservice**' oder ähnlichen Begriffen.

## Größenbegrenzung für die Datenbank

Um zu verhindern, dass die SQL Server-Datenbank (siehe SQL Server Installationen und Datenbanken (Erklärung) auf Seite 35) zu einer Größe anwächst, die sich auf die Leistung Systems auswirkt, können Sie angeben, für wie viele Tage die verschiedenen Arten von Ereignissen und Alarmen in der Datenbank gespeichert werden.

1. Öffnen Sie das Menü **Extras**.
2. Klicken Sie auf **Optionen**, und dann auf die Registerkarte **Alarme und Ereignisse**.




3. Nehmen Sie die erforderlichen Einstellungen vor. Weitere Informationen finden Sie unter Registerkarte „Alarme und Ereignisse“ (Optionen) auf Seite 428.

## IPv6 und IPv4 (Erklärung)

Ihr System unterstützt sowohl IPv6 als auch IPv4. Ebenso wie bei XProtect Smart Client.

IPv6 ist die aktuelle Version des Internet Protocols (IP). Das Internet Protocol bestimmt das Format und die Verwendung von IP-Adressen. IPv6 besteht zusätzlich zur weiter verbreiteten IP-Version IPv4. IPv6 wurde als Lösung der Adressenausschöpfung von IPv4 entwickelt. IPv6-Adressen sind 128-Bit lang, wo hingegen IPv4-Adressen nur 32-Bit lang sind.

Letztendlich bedeutet dies, dass das Anschriftenverzeichnis des Internets von 4,3 Milliarden einzigartigen Adressen auf 340 Sextillionen (340 Billionen Billionen) Adressen angewachsen ist. Ein Wachstumsfaktor von 79 Quadrilliarden (Milliarden Milliarden Milliarden).

Immer mehr Unternehmen nehmen eine Implementierung von IPv6 in ihren Netzwerken vor. Beispielsweise sind alle Gebäude der Bundesbehörden in den Vereinigten Staaten dazu verpflichtet, IPv6-Kompatibel zu sein. Beispiele und Abbildungen in dieser Anleitung setzen jedoch die Verwendung von IPv4 voraus, da diese IP-Version noch immer weiter verbreitet ist. IPv6 funktioniert aber ebenso gut im System.

### Gebrauch des Systems mit IPv6 (Erklärung)

Bei der Verwendung des Systems mit IPv6 treffen folgende Bedingungen zu:

#### Server

Server können oftmals sowohl IPv4 als auch IPv6 verwenden. Wenn allerdings ein Server in Ihrem System (beispielsweise ein Management-Server oder Aufzeichnungsserver) eine bestimmte IP-Version benötigt, müssen alle anderen Server in ihrem System ebenfalls über die selbe IP-Version verbunden werden.

**Beispiel**: Bis auf einen Server in Ihrem System können alle Server sowohl IPv4 als auch IPv6 verwenden. Die Ausnahme stellt ein Server dar, der nur IPv6 nutzen kann. Dies hat zur Folge, dass alle Server über IPv6 kommunizieren müssen.

#### Geräte

Sie können Geräte (z. B. Kameras, Eingänge, Ausgänge, Mikrofone, Lautsprecher) verwenden, die eine andere IP-Version als die der Serverkommunikation nutzen, vorausgesetzt Ihre Netzwerkgeräte und die Aufzeichnungsserver unterstützen die IP-Version des Geräts. Siehe auch Abbildung unten.

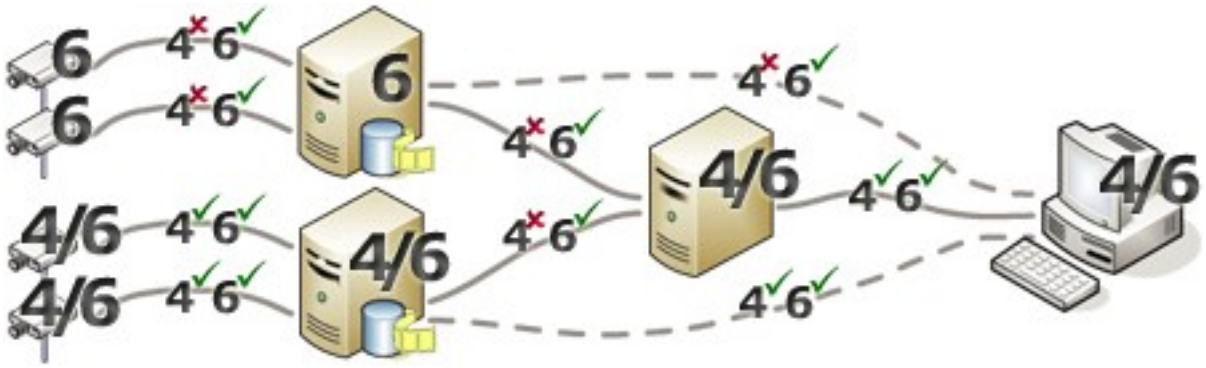
#### Clients

Wenn Ihr System IPv6 verwendet, sollten sich Benutzer mit dem XProtect Smart Client verbinden. Das XProtect Smart Client unterstützt sowohl IPv6 als auch IPv4.

Wenn einer oder mehrere Server in Ihrem System **nur** IPv6 verwenden können, **müssen** XProtect Smart Client-Benutzer IPv6 für die Verbindung dieser Server benutzen. In diesem Zusammenhang ist es wichtig, dass sich XProtect Smart Client-Installationen zuerst mit einem Management-Server für die erste Authentifizierung verbinden und dann mit den erforderlichen Aufzeichnungsservern für den Zugriff auf die Aufzeichnungen.

Allerdings müssen die XProtect Smart Client-Benutzer nicht selbst in einem IPv6-Netzwerk sein, wenn Ihre Netzwerkgeräte die Kommunikation zwischen verschiedenen IP-Versionen unterstützen, und das IPv6-Protokoll auf Ihren Computern installiert haben. Siehe auch Abbildung. Zur Installation von IPv6 auf einem Client-Computer, öffnen Sie die Eingabeaufforderung, geben Sie ***Ipv6 install*** ein, und drücken Sie anschließend **ENTER**.

**Beispielabbildung**




Beispiel: Da ein Server im System nur IPv6 verwenden kann, muss sämtliche Kommunikation mit diesem Server IPv6 verwenden. Allerdings bestimmt dieser Server auch die IP-Version für die Kommunikation zwischen allen anderen Servern im System.

## Schreiben von IPv6-Adressen (Erklärung)

Eine IPv6 wird üblicherweise in acht Blöcken aus vier hexadezimalen Ziffern geschrieben, wobei jeder Block von einem Doppelpunkt getrennt wird.

**Beispiel**: *2001:0B80:0000:0000:0000:0F80:3FA8:18AB*

Durch Auslassen der ersten Nullen in einem Block, können Sie die Adressen kürzen. Beachten Sie auch, dass einige der vierstelligen Blöcke möglicherweise nur aus Nullen bestehen. Wenn solche 0000-Blöcke aufeinanderfolgen, können Sie die Adressen verkürzen, indem Sie die 0000-Blöcke mit zwei Doppelpunkten ersetzen, sofern nur einer dieser doppelten Doppelpunkte in der Adresse auftauchen.

**Beispiel**:
*2001:0B80:0000:0000:0000:0F80:3FA8:18AB* kann verkürzt werden zu

*2001:B80:0000:0000:0000:F80:3FA8:18AB*, wenn die ersten Nullen entfernt werden, oder zu

*2001:0B80::0F80:3FA8:18AB*, wenn die 0000-Blöcke entfernt werden, oder sogar zu

*2001:B80::F80:3FA8:18AB*, wenn sowohl die ersten Nullen als auch die 0000-Blöcke entfernt werden.

## Verwendung von IPv6-Adressen in URLs

IPv6-Adressen enthalten Doppelpunkte. Doppelpunkte werden jedoch auch in anderen Syntaxtypen von Netzwerkadressen verwendet. Beispielsweise verwendet IPv4 einen Doppelpunkt, um IP-Adressen und Portnummern zu trennen, wenn beide in einer URL genutzt werden. IPv6 hat dieses Prinzip übernommen. Zur

Vermeidung von Missverständnissen werden eckige Klammern um IPv6-Adressen geschrieben, wenn sie in URLs verwendet werden.

**Beispiel** einer URL mit einer IPv6-Adresse:
*http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]*, die wiederum auf *http://[2001:B80::F80:3FA8:18AB]* verkürzt werden kann.

**Beispiel** einer URL mit einer IPv6-Adresse und einer Portnummer:
*http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234*, die natürlich gekürzt werden kann auf zum Beispiel *http://[2001:B80::F80:3FA8:18AB]:1234*

Weitere Informationen zu IPv6 finden Sie z.B. auf der IANA-Website (https://www.iana.org/numbers/). IANA (Internet Assigned Numbers Authority) ist die zuständige Organisation für die weltweite Koordination der IP-Adressverteilung.

## Virtuelle Server

Sie können alle Systemkomponenten auf virtualisierten Windows®-Servern wie VMware® und Microsoft® Hyper-V® laufen lassen.

Die Virtualisierung wird oft bevorzugt, um die Hardware-Ressourcen besser auszunutzen. Im Normalfall belasten virtuelle Server, die auf dem Hardware-Hostserver ausgeführt werden, den virtuellen Server nicht übermäßig – und oft auch nicht zur selben Zeit. Die Aufzeichnungsserver zeichnen jedoch alle Kamerabilder und Video-Streams auf. Dies belastet die CPU, den Arbeitsspeicher, das Netzwerk und das Speichersystem. Bei Ausführung auf einem virtuellen Server werden die üblichen Vorteile von Virtualisierung also zu einem Großteil neutralisiert, da Aufzeichnungsserver in vielen Fällen alle verfügbaren Ressourcen belegen.

Bei der Ausführung in einer virtuellen Umgebung muss der physische Speicher des Hardware-Hosts dieselbe Größe aufweisen wie der, der den virtuellen Servern zugewiesen ist. Darüber hinaus muss sichergestellt sein, dass der virtuelle Server, auf dem der Aufzeichnungsserver ausgeführt wird, über genügend CPU und Arbeitsspeicher verfügt – standardmäßig ist das nicht der Fall. Üblicherweise benötigt der Aufzeichnungsserver je nach Konfiguration 2 bis 4 GB. Weitere Engpässe sind die Netzwerkadapter-Zuweisung sowie die Festplattenleistung. Sie sollten in Erwägung ziehen, auf dem Hostserver des virtuellen Servers, auf dem der Aufzeichnungsserver ausgeführt wird, einen physischen Netzwerkadapter zuzuweisen. Dadurch lässt sich leichter sicherstellen, dass der Netzwerkadapter nicht mit dem Datenverkehr zu anderen virtuellen Servern überlastet wird. Wenn der Netzwerkadapter für verschiedene virtuelle Server verwendet wird, kann hoher Netzwerkverkehr dazu führen, dass der Aufzeichnungsserver die konfigurierte Zahl der Bilder nicht abruft und aufzeichnet.

## Mehrere Management-Server (Cluster) (Erklärung)

Die Management-Server kann auf mehreren Servern innerhalb eines Server-Clusters installiert werden. Dies gewährleistet sehr geringe Ausfallzeiten des Systems. Wenn ein Server im Cluster ausfällt, übernimmt ein anderer Server im Cluster automatisch die Aufgabe des ausgefallenen Servers, auf dem der Managementserver läuft.

Es ist nur möglich einen aktiven Management-Server pro Überwachungseinrichtung zu haben. Es können allerdings weitere Management-Server aufgesetzt werden, die bei Ausfällen einspringen.

> Standardmäßig begrenzt der Management Server-Dienst wie oft es innerhalb eines Zeitraums von 6 Stunden zu einem Failover kommt auf zweimal. Wird diese Anzahl überschritten, werden die Management Server Dienste vom Clustering-Dienst nicht automatisch gestartet. Dieser Grenzwert kann an Ihre Bedürfnisse angepasst werden.

## Anforderungen für Cluster

- Zwei Maschinen mit Microsoft Windows Server 2016 oder neuer. Achten Sie bitte darauf, dass:
  - Alle Server, die Sie als Clusterknoten hinzufügen möchten, mit derselben Version von Windows Server laufen
  - Alle Server, die Sie als Clusterknoten hinzufügen möchten, mit derselben Domäne verbunden sind
  - Sie sich als lokaler Administrator am Windows-Konto anmelden können

  Weitere Informationen zu Clustern in Microsoft Windows Servern finden Sie unter Ausfallsichere Cluster https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster.
- Eine Microsoft SQL Server Installation

  **Entweder** externe SQL Server und eine Datenbank, die **außerhalb** des Server-Clusters installiert wird, **oder** ein **interner** SQL Server (geclusterter) Dienst innerhalb des Server-Clusters (zur Erstellung eines internen SQL Server Dienstes ist die Verwendung des Microsoft® SQL Server® Standard oder der Microsoft® SQL Server® Enterprise Version erforderlich, die als geclusterter SQL Server fungieren kann).

  > Beim Herstellen der Verbindung zwischen dem Management Server und der Datenbank werden Sie, je nach den Passworteinstellungen in Ihrer Systemkonfiguration, ggf. dazu aufgefordert, das aktuelle Passwort für die Systemkonfiguration einzugeben. Siehe Passwort für die Systemkonfiguration (Erklärung) auf Seite 359.

> Wenn Sie in einer Failover-Cluster-Umgebung arbeiten, wird empfohlen, den Cluster anzuhalten, bevor Sie Aufgaben im Server Configurator starten. Das liegt daran, dass Server Configurator ggf. Dienste anhalten muss, während die Änderungen angewendet werden, und die Failover-Cluster-Umgebung diese Operation stören könnte.

# Schützen von Aufzeichnungsdatenbanken vor Beschädigungen

Kamera-Datenbanken können beschädigt werden. Es gibt verschiedene Datenbank-Reparatur-Optionen, um ein solches Problem zu lösen. Aber Milestone empfiehlt, dass Sie Maßnahmen ergreifen, um sicherzustellen, dass Ihre Kamera-Datenbanken nicht beschädigt werden.

## Festplattenfehler: Schützen Sie Ihre Laufwerke

Festplattenlaufwerke sind mechanische Geräte, die anfällig für externe Einwirkungen sind. Beispiele für externe Einwirkungen, die zu einer Beschädigung von Festplattenlaufwerken und Kameradatenbanken führen können, sind:

- Erschütterungen (sorgen Sie dafür, dass das Überwachungssystem inklusive seiner Umgebung stabil ist)
- Starke Hitze (sorgen Sie dafür, dass der Server ausreichend Belüftung erhält)
- Starke magnetische Felder (verhindern)
- Stromausfälle (nutzen Sie eine unabhängige Stromversorgung (USV))
- Statische Elektrizität (sorgen Sie dafür, dass Sie sich erden, bevor Sie ein Festplattenlaufwerk anfassen)
- Feuer, Wasser usw. (verhindern)

## Windows Task-Manager: Passen Sie auf beim Beenden von Prozessen

Bei Verwendung des Windows Task-Managers müssen Sie darauf achten, keine Prozesse zu beenden, die Folgen für das Überwachungssystem haben. Wenn Sie eine Anwendung oder einen Systemdienst beenden, indem Sie im Windows Task-Manager auf **Prozess beenden** klicken, kann der Prozess vor der Beendigung weder seinen Status noch seine Daten speichern. Dies kann zu einer Beschädigung von Kameradatenbanken führen.

Wenn Sie versuchen, einen Prozess zu beenden, zeigt der Windows Task-Manager in der Regel eine Warnung an. Falls Sie in der Warnnachricht gefragt werden, ob Sie den Prozess wirklich beenden möchten, klicken Sie auf **Nein** – es sei denn, Sie sind sich ganz sicher, dass das Beenden des Prozesses keine Auswirkungen auf das Überwachungssystem haben wird.

## Stromausfälle: Nutzen Sie eine USV

Der häufigste Grund für beschädigte Datenbanken ist ein plötzliches Herunterfahren des Aufzeichnungsservers, wobei Dateien nicht gespeichert werden und das Betriebssystem nicht ordnungsgemäß heruntergefahren wird. Ursache dafür können Stromausfälle, Personen, die aus Versehen Stromkabel von Servern herausziehen, oder ähnliche Motive sein.

Die beste Methode, um Aufzeichnungsserver vor einem plötzlichen Herunterfahren zu schützen, besteht darin, jeden von ihnen mit einer USV (unabhängigen Stromversorgung) auszustatten.

Die USV dient als batteriebetriebene sekundäre Stromquelle, die bei Problemen mit der Stromversorgung genug Energie für das Speichern geöffneter Dateien und das sichere Herunterfahren Ihres Systems liefert. USVs bieten unterschiedliche Leistungsmerkmale, viele USVs beinhalten jedoch Software für ein automatisches Speichern geöffneter Dateien, für eine Benachrichtigung der Systemadministratoren usw.

Die Auswahl einer USV vom richtigen Typ für die Umgebung Ihres Unternehmens ist ein individueller Prozess. Bei der Evaluierung Ihrer Anforderungen sollten Sie allerdings die Laufzeitlänge beachten, die Ihre USV unterstützen muss, falls es zu einem Stromausfall kommt. Das Speichern geöffneter Dateien und das Herunterfahren eines Betriebssystems können einige Minuten dauern.

## SQL Server-Datenbanktransaktionsprotokoll (Erklärung)

Jedes Mal, wenn in eine SQL Server-Datenbank eine Änderung geschrieben wird, protokolliert die SQL Server-Datenbank diese Änderung in ihrem Transaktionsprotokoll.

Mit dem Transaktionsprotokoll können Sie Änderungen in der SQL Server durch Microsoft® SQL Server Management Studio rückgängig machen. Die SQL Server-Datenbank speichert standardmäßig ihr Transaktionsprotokoll auf unbegrenzte Zeit, was bedeutet, dass das Transaktionsprotokoll mit der Zeit immer mehr Einträge enthält. Das Transaktionsprotokoll befindet sich standardmäßig auf dem Systemlaufwerk, und wenn es sich stetig vergrößert, kann es die ordnungsgemäße Ausführung von Windows beeinträchtigen.

Das gelegentliche Löschen des Transaktionsprotokolls ist eine gute Methode, um ein solches Szenario zu vermeiden. Allerdings macht die Löschung allein das Transaktionsprotokoll nicht kleiner, bereinigt jedoch dessen Inhalt und verhindert so ein unkontrolliertes Wachstum. Ihr VMS-System löscht keine Transaktionsprotokolle. In SQL Server gibt es Methoden zum Löschen des Transaktionsprotokolls. Besuchen Sie die Supportseite von Microsoft https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017 und suchen Sie nach *Kürzung des Transaktionsprotokolls*.

## Mindestsystemanforderungen

Informationen zu den Systemanforderungen der verschiedenen Komponenten und Anwendungen Ihres Systems finden Sie auf der Milestone Website (https://www.milestonesys.com/systemrequirements/).

## Vor dem Start der Installation

Milestone empfiehlt Ihnen, die im nächsten Abschnitt beschriebenen Voraussetzungen zu lesen, bevor Sie die tatsächliche Installation beginnen.

### Server und Netzwerk vorbereiten

**Betriebssystem**

Achten Sie darauf, dass auf allen Servern eine saubere Installation eines Microsoft Windows-Betriebssystems installiert ist und das Betriebssystem mit den neuesten Windows-Updates aktualisiert wurde.

Informationen zu den Systemanforderungen der verschiedenen Komponenten und Anwendungen Ihres Systems finden Sie auf der Milestone Website (https://www.milestonesys.com/systemrequirements/).

**Microsoft® .NET Framework**

Prüfen Sie, ob auf allen Servern Microsoft .NET Framework 4.8 oder höher installiert ist.

**Netzwerk**

Weisen Sie statische IP-Adressen zu oder nehmen Sie DHCP-Reservierungen an allen Systemkomponenten und Kameras vor. Sie müssen verstehen, wie und wann das System Bandbreite verbraucht, um sicherzustellen, dass im Netzwerk ausreichend Bandbreite zur Verfügung steht. Die Hauptlast in Ihrem Netzwerk besteht aus drei Elementen:

- Kamera-Videostreams
- Clients zeigen Video an
- Archivierung von aufgezeichneten Videos

Der Aufzeichnungsserver ruft Videostreams von den Kameras ab, eine konstante Last im Netzwerk nach sich zieht. Clients, die Video anzeigen, verbrauchen Netzwerkbandbreite. Wenn im Inhalt der Client-Ansichten keine Änderungen auftreten, ist die Last konstant. Änderungen im Ansichtsinhalt, Videosuche oder Wiedergabe lassen die Last dynamisch werden.

Die Archivierung von aufgezeichnetem Video ist eine optionale Funktion, die es dem System ermöglicht Aufzeichnungen in einen Netzwerkspeicher zu verschieben, wenn nicht genug Speicherplatz im internen Speicher des Computers vorhanden ist. Dies ist ein geplanter Auftrag, den Sie definieren müssen. Üblicherweise archivieren Sie in einem Netzlaufwerk, wodurch er zu einer geplanten dynamischen Last im Netzwerk wird.

Ihr Netzwerk muss über Bandbreiten-Spielraum verfügen, um diese Spitzen im Datenverkehr zu bewältigen. Damit werden die Reaktionsfähigkeit des Systems und die allgemeine Benutzererfahrung optimiert.

## Active Directory vorbereiten

Wenn Sie Benutzer über den Active Directory-Dienst hinzufügen möchten, muss in Ihrem Netzwerk ein Server vorhanden sein, auf dem Active Directory installiert ist und der als Domänen-Controller fungiert.

Für ein leichteres Benutzer- und Gruppenmanagement empfiehlt Milestone, dass Sie Microsoft Active Directory® bereits installiert und konfiguriert haben, bevor Sie Ihr XProtect-System installieren. Wenn Sie den Management-Server nach der Installation Ihres Systems zum Active Directory hinzufügen, müssen Sie den Management-Server neu installieren und die Benutzer durch die im Active Directory neu definierten Benutzer ersetzen.

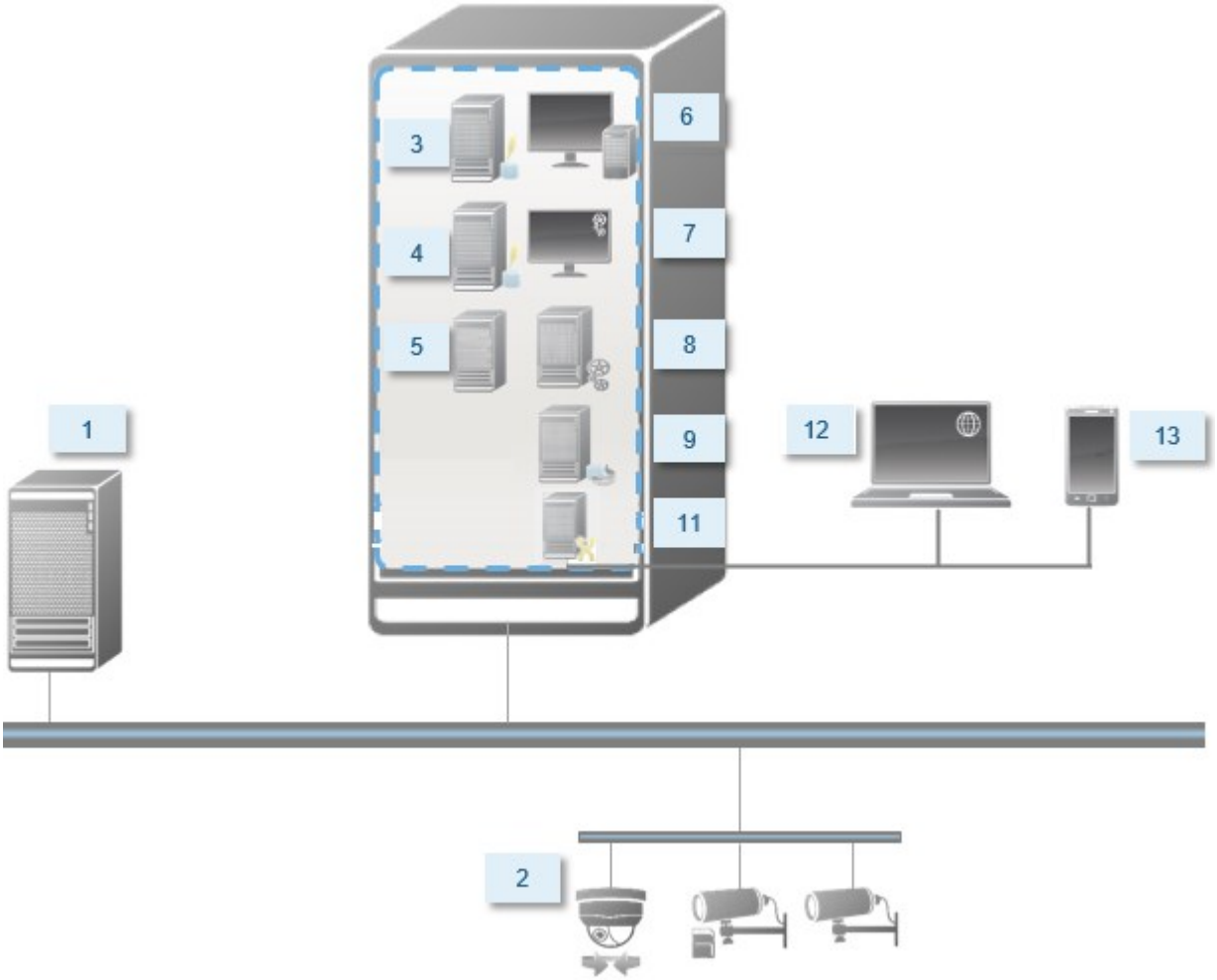
Basisbenutzer werden in Milestone Federated Architecture-Systemen nicht unterstützt. Wenn Sie also beabsichtigen, Milestone Federated Architecture zu verwenden, müssen Sie Benutzer als Windows-Benutzer über den Dienst Active Directory hinzufügen. Wenn Sie Active Directory nicht installieren, folgen Sie bei der Installation bitte den in Installation für Arbeitsgruppen auf Seite 192 angegebenen Schritten.

## Installationsmethode

Im Installationsassistenten müssen Sie festlegen, welche Installationsmethode Sie verwenden. Sie müssen Ihre Auswahl auf den Anforderungen Ihrer Organisation basieren, aber wahrscheinlich haben Sie die Methode bereits gewählt, als Sie das System kauften.

| Optionen | Beschreibung |
|---|---|
| **Einzelcomputer** | Installiert alle Server- und Clientkomponenten sowie SQL Server auf dem aktuellen Computer.<br><br>Nach Abschluss der Installation haben Sie die Möglichkeit, das System mithilfe eines Assistenten zu konfigurieren. Wenn Sie der Fortsetzung zustimmen, durchsucht der Aufzeichnungsserver Ihr Netzwerk nach Hardware, und Sie können auswählen, welche Hardwaregeräte Sie zu Ihrem System hinzufügen möchten. Die maximale Anzahl von Hardwaregeräten, die im Konfigurationsassistenten hinzugefügt werden können, hängt von Ihrer Basislizenz ab. Die Kameraansichten sind außerdem in Ansichten vorkonfiguriert, und eine Standard-Anwenderrolle wird erstellt. Nach der Installation öffnet sich XProtect Smart Client, und das System ist einsatzbereit. |
| **Benutzerdefiniert** | Der Managementserver wird immer von der Liste der Systemkomponenten ausgewählt und wird stets installiert; Sie können jedoch frei auswählen, was auf dem aktuellen Computer zusätzlich zu den übrigen Server- und Client-Komponenten noch installiert werden soll.<br><br>Standardmäßig ist der Aufzeichnungsserver auf der Liste der Komponenten nicht ausgewählt, dies können Sie jedoch ändern. Sie können die nicht ausgewählten Komponenten anschließend auf anderen Computern installieren. |

**Einzelne Computer-Installation**

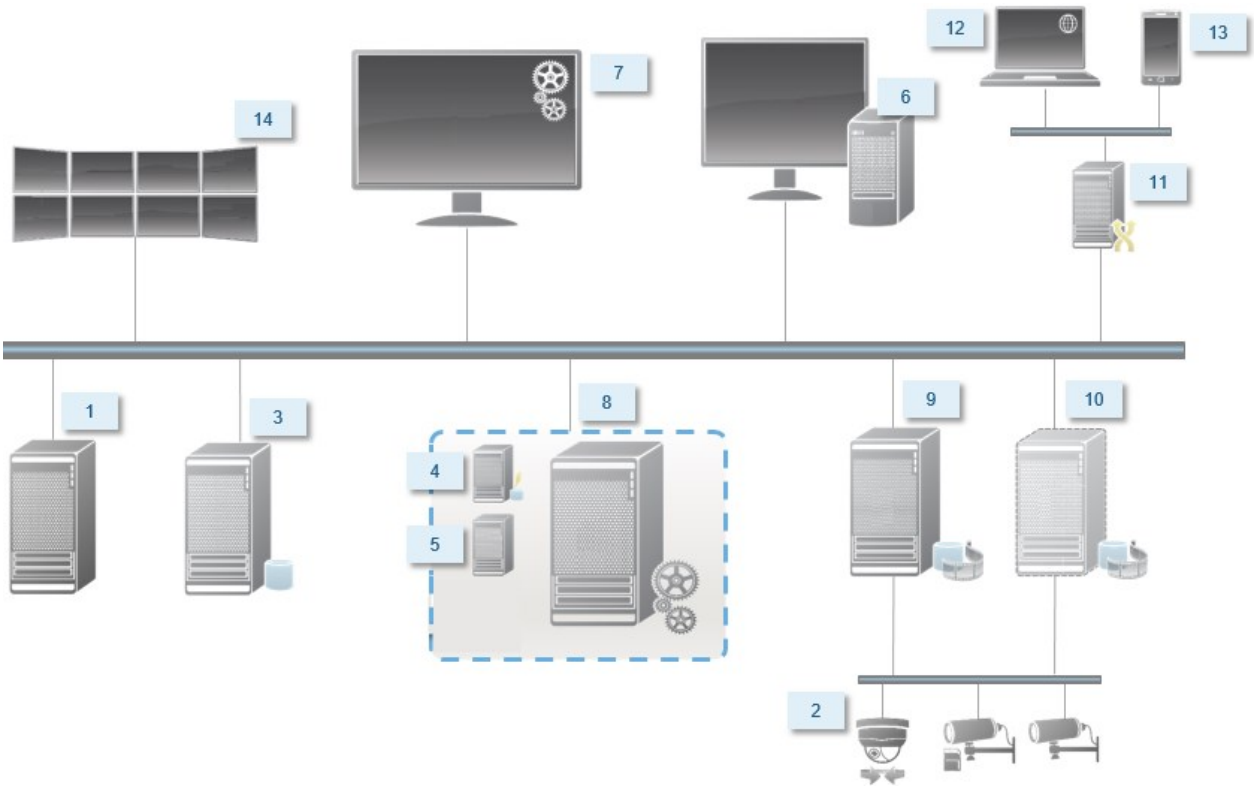



Normalerweise besteht ein System aus folgenden Systemkomponenten:

1. **Active Directory**
2. **Geräte**
3. **Server mit SQL Server**
4. **Ereignisserver**
5. **Log-Server**
6. **XProtect Smart Client**
7. **Management Client**
8. **Managementserver**
9. **Aufzeichnungsserver**

10. **Failover-Aufzeichnungsserver**
11. **XProtect Mobile-Server**
12. **XProtect Web Client**
13. **XProtect Mobile Client**
14. **XProtect Smart Client mit XProtect Smart Wall**

**Benutzerdefinierte Installation - Beispiel für verteilte Systemkomponenten**




## Entscheiden Sie sich für eine Version von SQL Server

Microsoft® SQL Server® Express ist eine kostenlose Version von SQL Server, die verglichen mit anderen Versionen von SQL Server leicht zu installieren und für den Gebrauch vorzubereiten ist. Während der Installation auf einem **Einzelnen Computer** wird Microsoft SQL Server Express installiert, es sei denn, SQL Server ist auf dem betreffenden Computer bereits installiert.

Die XProtect VMS Installation beinhaltet Microsoft SQL Server Express Version 2019. Nicht alle Windows-Betriebssysteme unterstützen diese Version von SQL Server. Bevor Sie XProtect VMS installieren, überprüfen Sie, ob Ihr Betriebssystem SQL Server 2019 unterstützt. Sollte Ihr Betriebssystem diese Version von SQL Server nicht unterstützen, installieren Sie eine unterstützte Version von SQL Server, bevor sie mit der XProtect VMS-Installation beginnen. Angaben zu unterstützten Versionen von SQL Server finden Sie unter https://www.milestonesys.com/systemrequirements/.

Für sehr große Systeme, oder für Systeme mit vielen Transaktionen zu und von den SQL Server-Datenbanken, empfiehlt Milestone Ihnen, die Microsoft® SQL Server® Standard oder Microsoft® SQL Server® Enterprise-Ausgabe von SQL Server auf einem eigenen Computer im Netzwerk und auf einem bestimmten Festplattenlaufwerk zu verwenden, das für keine anderen Zwecke verwendet wird. Die Installation von SQL Server auf einem eigenen Laufwerk verbessert die Leistung des gesamten Systems.

## Dienstkonto auswählen

Sie werden im Rahmen der Installation aufgefordert, ein Konto anzugeben, um die Milestone-Dienste auf diesem Computer auszuführen. Die Dienste werden immer in diesem Konto ausgeführt, unabhängig davon, welcher Benutzer angemeldet ist. Achten Sie darauf, dass das Konto über alle erforderlichen Benutzerrechte verfügt, z. B. über die richtigen Berechtigungen für die Ausführung von Aufgaben, den richtigen Netzwerk- und Dateizugriff und den Zugriff auf freigegebene Netzwerkordner.

Sie können zwischen einem vorab definierten Konto und einem Benutzerkonto wählen. Treffen Sie Ihre Entscheidung basierend auf der Umgebung, in der Sie Ihr System installieren möchten:

**Domänenumgebung**

In einer Domänenumgebung:

- Milestone empfiehlt, dass Sie das eingebaute Netzwerkkonto verwenden

  Es ist einfacher zu verwenden, auch wenn Sie das System auf mehrere Computer erweitern müssen.

- Sie können auch Domänenbenutzerkonten verwenden, aber sie sind möglicherweise schwerer zu konfigurieren

**Arbeitsgruppenumgebung**

In einer Arbeitsgruppenumgebung empfiehlt Ihnen Milestone, ein lokales Benutzerkonto zu verwenden, das über alle erforderlichen Berechtigungen verfügt. Hierbei handelt es sich häufig um das Administratorkonto.

> ⚠ Wenn Sie Ihre Systemkomponenten auf mehreren Computern installiert haben, muss das ausgewählte Benutzerkonto auf allen Computern Ihrer Installationen mit identischem Benutzernamen, Kennwort und Zugriffsberechtigungen konfiguriert werden.

## Kerberos Authentifizierung (Erklärung)

Kerberos ist ein auf Tickets basierendes Netzwerkauthentifizierungsprotokoll. Es wurde als eine starke Authentifizierung für Client/Server oder Server/Server Anwendungen entwickelt.

Nutzen Sie die Kerberos-Authentifizierung als Alternative zum älteren Microsoft NT LAN-Authentifizierungsprotokoll (NTLM).

Eine Kerberos-Authentifizierung erfordert eine gegenseitige Authentifizierung, bei der der Client den Dienst und der Dienst wiederum den Client authentifiziert. Auf diese Weise können Sie eine sicherere Authentifizierung von XProtect-Clients zu XProtect-Servern sicherstellen, ohne Ihr Passwort preiszugeben.

Sie müssen die Service Principal Names (SPN) im Active Directory registrieren, um eine gegenseitige Authentifizierung in Ihrem XProtect VMS zu ermöglichen. Ein SPN ist ein Pseudonym, das auf eine Entität, wie einen XProtect-Serverdienst eindeutig identifiziert. Jeder Dienst, der gegenseitige Authentifizierung verwendet, muss einen registrierten SPN besitzen, damit Clients den Dienst im Netzwerk identifizieren können. Eine gegenseitige Authentifizierung ist ohne ordnungsgemäße registrierte SPN nicht möglich.

Die nachfolgende Tabelle listet die verschiedenen Milestone-Dienste mit den korrespondierenden Portnummern auf, die für eine Registrierung benötigt werden:

| Dienst | Portnummer |
|---|---|
| **Management Server - IIS** | 80 - Konfigurierbar |
| **Management Server - Intern** | 8080 |
| **Recording Server - Data Collector** | 7609 |
| **Failover Server** | 8990 |
| **Event Server** | 22331 |
| **LPR Server** | 22334 |

Die Anzahl der Dienste, die Sie im Active Directory ihrer gegenwärtigen Installation registrieren müssen. Data Collector wird bei der Installation des Management Server, Recording Server, Event Server oder Failover Server Dienstes automatisch installiert.

Sie müssen für den Benutzer, der den Dienst ausführt, zwei SPNs registrieren: einen mit dem Hostnamen und einen mit dem voll qualifizierten Domainnamen.

Wenn Sie den Dienst unter einem Netzwerkdienstkonto ausführen, müssen Sie die zwei SPN für jeden Computer registrieren, die den Dienst ausführen.

Dies ist das Milestone SPN-Benennungsschema:

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

Hier ein Beispiel für SPNs für den Recording Server-Dienst, der auf einem Computer mit den folgenden Spezifikationen ausgeführt wird:

```
Hostname: Record-Server1
Domain: Surveillance.com
```

Zu registrierende SPNs:

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

## Virus scanning exclusions (Erklärung)

Wenn ein Antivirus-Programm wie im Fall anderer Datenbanksoftware auf einem Computer installiert wird, auf dem XProtect-Software ausgeführt wird, ist es wichtig, dass sie spezifische Dateitypen und Ordner und bestimmte Arten von Netzwerkverkehr ausschließen. Wenn Sie diese Ausnahme nicht einrichten, werden Virenscans einen erheblichen Anteil der Systemressourcen beanspruchen. Darüber hinaus kann der Scanprozess vorübergehend Dateien sperren, was zu einer Unterbrechung im Aufzeichnungsprozess oder sogar einer Beschädigung der Datenbanken führen würde.

Wenn Sie den Virenscan ausführen müssen, scannen Sie keine Aufzeichnungsserver-Verzeichnisse, die Aufzeichnungsdatenbanken enthalten (standardmäßig `C:\mediadatabase\`, sowie alle Unterordner). Vermeiden Sie auch den Virenscan in Archivspeicher-Verzeichnissen.

Erstellen Sie die folgenden zusätzlichen Ausschlüsse:

- Dateitypen: .blk, .idx, .pic
- Ordner und Unterordner:
  - `C:\Program Files\Milestone` oder `C:\Program Files (x86)\Milestone`
  - `C:\ProgramData\Milestone\IDP\Logs`
  - `C:\ProgramData\Milestone\KeyManagement\Logs`
  - `C:\ProgramData\ \ MilestoneMIPSDK`
  - `C:\ProgramData\Milestone\XProtect Data Collector Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Event Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Log Server`
  - `C:\ProgramData\Milestone\XProtect Management Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Mobile Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Secure\TablesDb`
- Netzwerkscans an den folgenden TCP-Ports ausschließen:

| Produkt | TCP-Ports |
|---|---|
| XProtect VMS | 80, 8080, 7563, 25, 21, 9000 |
| XProtect Mobile | 8081 |

oder

- Netzwerkscans der folgenden Prozesse ausschließen:

| Produkt | Prozesse |
|---|---|
| XProtect VMS | VideoOS.Recorder.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe |
| XProtect Mobile | VideoOS.MobileServer.Service.exe |

Ihre Organisation hat möglicherweise strenge Richtlinien in Bezug auf Virenscans, es ist jedoch wichtig, dass die oben aufgeführten Ordner und Dateien von Virenscans ausgenommen werden.

## Wie ist XProtect VMS so zu konfigurieren, dass es im FIPS 140-2-konformen Modus läuft?

Um XProtect VMS in einem FIPS 140-2-Betriebsmodus auszuführen, müssen Sie:

- Das Windows-Betriebssystem in einem FIPS 140-2-genehmigten Betriebsmodus ausführen. Siehe die Microsoft-Internetseite zu Informationen dazu, wie FIPS aktiviert wird.
- Achten Sie darauf, dass eigenständige Dritt-Integrationen auf einem FIPS-fähigen Windows-Betriebssystem laufen können
- Stellen Sie Verbindungen zu Geräten so her, dass ein FIPS 140-2-konformer Betriebsmodus gewährleistet ist
- Achten Sie darauf, dass Daten in Mediendatenbanken mithilfe von FIPS 140-2-konformen Chiffren verschlüsselt werden

  Dies erfolgt durch Ausführen des Upgrade-Tools für Mediendatenbanken. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

## Bevor Sie XProtect VMS auf einem FIPS-fähigen System installieren

Während neue Installation von XProtect VMS auf Computern erfolgen können, die FIPS-fähig sind, können Sie kein Upgrade von XProtect VMS durchführen, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist.

Wenn Sie ein Upgrade vornehmen, deaktivieren Sie vor der Installation die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem SQL Server gehosted wird.

Das Installationsprogramm für XProtect VMS prüft die FIPS-Sicherheitsrichtlinie und verhindert die Installation, wenn FIPS aktiviert ist.

Wenn Sie allerdings ein Upgrade von XProtect VMS Version 2020 R3 oder später vornehmen, brauchen Sie FIPS nicht zu deaktivieren.

Wenn Sie die Komponenten von XProtect VMS auf allen Computern installiert und das System für FIPS vorbereitet haben, können Sie die FIPS-Sicherheitsrichtlinie auf Windows auf allen Computern in Ihrem VMS aktivieren.

Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

## Softwarelizenzcode registrieren

Vor der Installation müssen Sie über den Namen und den Speicherort der Softwarelizenzdatei verfügen, die Sie von Milestone erhalten haben.

Sie können eine kostenlose Version von XProtect Essential+ installieren. Diese Version bietet eingeschränkte Funktionen von XProtect VMS für eine begrenzte Zahl von Kameras. Zum Installieren von XProtect Essential+ benötigen Sie eine Internetverbindung.

Der Softwarelizenzcode (SLC) ist auf Ihrer Bestellbestätigung gedruckt und die Softwarelizenzdatei ist nach Ihrer SLC benannt.

Milestone empfiehlt, dass Sie Ihren SLC vor der Installation auf unserer Website (https://online.milestonesys.com/) registrieren. Ihr Händler hat dies gegebenenfalls bereits für Sie erledigt.

## Gerätetreiber (Erklärung)

Ihr System verwendet Videogerätetreiber, um die mit einem Aufzeichnungsserver verbundenen Kameras zu steuern und mit ihnen zu kommunizieren. Die Gerätetreiber müssen auf jeden Aufzeichnungsserver Ihres System installiert werden.

Ab der Ausgabe 2018 R1 sind die Gerätetreiber in zwei Gerätepacks aufgeteilt: das reguläre Gerätepaket mit neueren Treibern und ein Stamm-Gerätepaket mit älteren Treibern.

Das reguläre Gerätepaket wird automatisch installiert, wenn Sie den Aufzeichnungsserver installieren. Später können Sie Treiber aktualisieren, indem Sie eine neuere Version des Treiberpakets installieren. Milestone veröffentlicht neue Versionen der Gerätetreiber in regelmäßigen Abständen und macht sie auf der Download-Seite (https://www.milestonesys.com/downloads/) auf unserer Website als Treiberpakete verfügbar. Bei der Aktualisierung eines Gerätepakets können Sie die neueste Version über jede zuvor installierte Version installieren.

Das Stammgerätepaket kann nur installiert werden, wenn ein reguläres Gerätepaket im System installiert ist. Die Treiber aus dem Stammgerätepaket werden automatisch installiert, wenn eine vorige Version bereits auf Ihrem System installiert ist. Es steht auf der Software-Download-Seite (https://www.milestonesys.com/downloads/) zum manuellen Herunterladen und Installieren zur Verfügung.

Stoppen Sie den Recording Server-Dienst vor der Installation, andernfalls müssen Sie den Computer neu starten.

Damit eine optimale Leistung garantiert ist, sollten Sie immer die neuesten Gerätetreiber verwenden.

## Anforderungen für Offline-Installationen

Wenn Sie das System auf einem Server installieren, der offline ist, benötigen Sie Folgendes:

- Die `Milestone XProtect VMS Products 2023 R3 System Installer.exe`-Datei
- Die Softwarelizenzdatei (SLC) für Ihr XProtect-System
- Ein Medium zur Installation eines Betriebssystems, einschließlich der erforderlichen .NET-Version (https://www.milestonesys.com/systemrequirements/)

# Sichere Kommunikation (Erklärung)

Hypertext Transfer Protocol Secure (HTTPS) ist eine Erweiterung des Hypertext Transfer Protocol (HTTP) für die sichere Kommunikation über ein Computernetzwerk. In HTTPS wird das Kommunikationsprotokoll mithilfe der Transport Layer Security (TLS) oder ihrem Vorläufer, Secure Sockets Layer (SSL), verschlüsselt.

In XProtect VMS wird eine sichere Kommunikation durch die Verwendung von TLS/SSL mit asymmetrischer Verschlüsselung (RSA) erreicht.

TLS/SSL verwendet ein Schlüsselpaar - einen privaten und einen öffentlichen - zur Authentifizierung, Sicherung und Verwaltung sicherer Verbindungen.

Eine Zertifizierungsstelle (CA) ist jeder, der Stammzertifikate ausstellen kann. Dabei kann es sich um einen Internetdienst handeln, der Stammzertifikate ausstellt, oder um jeden, der ein Zertifikat manuell erstellt und verteilt. Eine CA kann Zertifikate für Webdienste ausstellen, d. h. für jede Software, die die Kommunikation über https nutzt. Dieses Zertifikat enthält zwei Schlüssel, einen privaten und einen öffentlichen. Der öffentliche Schlüssel wird auf den Clients eines Web-Dienstes (Dienst-Clients) installiert, indem ein öffentliches Zertifikat installiert wird. Der private Schlüssel dient dazu, Serverzertifikate zu signieren, die auf dem Server installiert werden müssen. Jedes Mal, wenn ein Dienst-Client den Web Service anruft, sendet der Web Service dem Client das Server-Zertifikat, einschließlich des öffentlichen Schlüssels. Der Dienst-Client kann das Serverzertifikat mithilfe des bereits installierten, öffentlichen CA-Zertifikates überprüfen. Der Client und der Server können nun mit Hilfe der öffentlichen und privaten Serverzertifikate einen geheimen Schlüssel austauschen und so eine sichere TLS/SSL-Verbindung aufbauen.

Bei manuell verteilten Zertifikaten müssen die Zertifikate installiert werden, bevor der Client eine solche Überprüfung vornehmen kann.

Siehe Transportschichtsicherheit für weitere Informationen über TLS.

> **!** Zertifikate haben ein Verfalldatum. XProtect VMS gibt Ihnen keine Wahrnung, wenn das Zertifikat in Kürze abläuft. Wenn ein Zertifikat abläuft:
> - Die Clients vertrauen dann nicht mehr dem Aufzeichnungsserver mit dem abgelaufenen Zertifikat und können daher auch nicht mehr mit ihm kommunizieren.
> - Die Aufzeichnungsserver vertrauen dann nicht mehr dem Managementserver mit dem abgelaufenen Zertifikat und können daher auch nicht mehr mit ihm kommunizieren.
> - Die mobilen Geräte vertrauen dann nicht mehr dem Mobile Server mit dem abgelaufenen Zertifikat und können daher auch nicht mehr mit ihm kommunizieren
>
> Um die Zertifikate zu erneuern, folgen Sie den Schritten in dieser Anleitung, wie Sie es bereits getan haben, als Sie Zertifikate erstellt haben.

Weitere Informationen finden Sie im Zertifikate-Leitfaden dazu, wie Sie Ihre XProtect VMS Installationen sichern können.

# Installation

## Installation eines neuen XProtect-Systems

### Installieren Sie XProtect Essential+

Sie können eine kostenlose Version von XProtect Essential+ installieren. Diese Version bietet eingeschränkte Funktionen von XProtect VMS für eine begrenzte Zahl von Kameras. Zum Installieren von XProtect Essential+ benötigen Sie eine Internetverbindung.

Diese Version wird unter Nutzung der Installationsoption **Einzelcomputer** auf einem einzigen Computer installiert. Die Option **Einzelcomputer** installiert alle Server- und Client-Komponenten auf dem aktuellen Rechner.

Milestone empfiehlt Ihnen, vor der Installation den folgenden Abschnitt sorgfältig durchzulesen: Vor dem Start der Installation auf Seite 144.

Für FIPS-Installationen können Sie kein Upgrade von XProtect VMS durchführen, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist. Deaktivieren Sie vor der Installation die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem SQL Server gehosted wird. Wenn Sie allerdings ein Upgrade von XProtect VMS Version 2020 R3 oder später vornehmen, brauchen Sie FIPS nicht zu deaktivieren. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

Nach der Erstinstallation können Sie mit dem Konfigurationsassistenten fortfahren. Je nach Hardware und Konfiguration scannt der Aufzeichnungsserver Ihr Netzwerk nach Hardware. Sie können dann die Hardwaregeräte auswählen, die zu Ihrem System hinzugefügt werden sollen. Kameras sind in Ansichten vorkonfiguriert, und Sie haben die Option zum Aktivieren anderer Geräte wie Mikrofone und Lautsprecher. Sie haben auch die Option, Benutzer entweder mit einer Bedienerrolle oder mit einer Administratorrolle zum System hinzuzufügen. Nach der Installation öffnet sich XProtect Smart Client, und das System ist einsatzbereit.

Andernfalls, wenn Sie den Installationsassistenten schließen, wird XProtect Management Client geöffnet, wo Sie manuelle Konfigurationen vornehmen können, wie z.B. zum Hinzufügen von Hardwaregeräten und Benutzern zum System.

> Wenn Sie Aktualisierungen von einer vorherigen Version des Produkts durchführen, sucht das System nicht nach Hardware oder erzeugt neue Ansichten und Benutzerprofile.

1. Laden Sie die Software aus dem Internet herunter (https://www.milestonesys.com/downloads/) und führen Sie die Datei aus. `Milestone XProtect VMS Products 2023 R3 System Installer.exe` aus.
2. Die Installationsdateien werden entpackt. Abhängig von Ihren Sicherheitsseinstellungen erscheinen eine oder mehrere Windows® Sicherheitswarnungen. Akzeptieren Sie diese, um mit dem Entpacken fortzufahren.
3. Nach Abschluss dieses Vorganges erscheint der **Milestone XProtect VMS** Installationsassistent.
    1. Wählen Sie die während der Installation zu verwendende **Sprache** aus (dies ist nicht die Sprache, die Ihr System nach erfolgter Installation verwendet; diese Einstellung erfolgt später). Klicken Sie auf **Weiter**.
    2. Lesen Sie den *Milestone Endbenutzer-Lizenzvertrag*. Wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen dieser Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
    3. Wählen Sie auf der Seite **Datenschutzeinstellungen** aus, ob Sie wollen, dass Nutzungsdaten weitergegeben werden, und klicken Sie dann auf **Weiter**.

        > Sie dürfen die Datenerfassung nicht aktivieren, wenn Sie möchten, dass das System eine EU-DSGVO-gerechte Installation ist. Weitere Informationen über den Datenschutz und die Erhebung von Nutzungsdaten finden Sie im Datenschutzleitfaden zur DSGVO.

        > Sie können Ihre Datenschutzeinstellungen später jederzeit ändern. Siehe auch Systemeinstellungen (die Dialogbox „Optionen“).

    4. Klicken Sie auf das Link **XProtect Essential+**, um eine kostenlose Lizenzdatei herunterzuladen.

        Die kostenlose Lizenz wird heruntergeladen und erscheint dann im Feld **Speicherort für die Lizenzdatei eingeben oder suchen**. Klicken Sie auf **Weiter**.
4. Wählen Sie **Einzel-Computer**.

    Eine Liste der zu installierenden Komponenten wird angezeigt (Sie können diese Liste nicht bearbeiten). Klicken Sie auf **Weiter**.

5. Geben Sie auf der Seite **Passwort für Systemkonfiguration zuweisen** ein Passwort ein, das Ihre Systemkonfiguration schützt. Dieses Passwort benötigen Sie, falls eine Systemwiederherstellung erforderlich wird oder wenn Sie Ihr System erweitern, z.B. indem Sie Cluster hinzufügen.

   Es ist wichtig, dass Sie dieses Passwort sicher aufbewahren. Wenn Sie dieses Passwort verlieren, sind Sie ggf. nicht mehr in der Lage, Ihre Systemkonfiguration wiederherzustellen.

   Wenn Sie Ihre Systemkonfiguration nicht mit einem Passwort schützen wollen, wählen Sie **Ich möchte kein Passwort zum Schutz der Systemkonfiguration verwenden, und mir ist klar, dass die Systemkonfiguration dann nicht verschlüsselt ist**.

   Klicken Sie auf **Weiter**.

6. Geben Sie auf der Seite **Zuweisung eines Datenschutzpasswortes für einen Mobile Server** ein Passwort ein, um Ihre Untersuchungen zu verschlüsseln. Als Systemadministrator müssen Sie dieses Passwort eingeben, um auf die Daten auf dem Mobilserver zuzugreifen, falls das System wiederhergestellt werden muss oder wenn Sie das System um weitere Mobilserver erweitern wollen.

   Dieses Passwort müssen Sie sicher aufbewahren. Andernfalls können die Daten auf dem Mobile Server evtl. nicht wiederhergestellt werden.

   Wenn Sie kein Passwort zum Schutz Ihrer Untersuchungen festlegen möchte, wählen Sie **Ich möchte kein Passwort zum Schutz der Daten auf dem Mobile Server verwenden und mir ist klar, dass die Untersuchungen dann nicht verschlüsselt werden**.

   Klicken Sie auf **Weiter**.

7. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an:
    1. Geben Sie den Namen des Aufzeichnungsservers im Feld **Aufzeichnungsserver-Name** ein. Der Standardwert ist der Name des Computers.
    2. Das Feld für die **Management-Server-Adresse** zeigt die Adresse und Port-Nummer des Management-Servers: localhost:80.
    3. Wählen Sie im Feld **Wahl des Speicherorts für die Medien-Datenbank** den Speicherort aus, an dem Sie Ihre Video-Aufzeichnungen speichern möchten. Milestone empfiehlt, einen anderen Speicherort für Ihre Videoaufnahmen zu wählen als den Ort der Programminstallation oder das System-Laufwerk. Der Standard-Speicherort ist das Laufwerk mit der höchsten freien Speicherkapazität.
    4. Legen Sie im Feld **Speicherdauer für Videoaufzeichnungen** fest, wie lange Sie die Aufzeichnungen speichern möchten. Sie können einen Wert zwischen 1 und 365,000 Tagen eingeben, wobei die Standardaufbewahrungsdauer 7 Tage beträgt.
    5. Klicken Sie auf **Weiter**.

8. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

   - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

     Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

     > ⚠ Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

   - Zwischen den Aufzeichnungsservern und den Clients

     Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

   - Zwischen dem Mobile Server und den Clients

     Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

   - Zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren

     Um die Verschlüsselung zwischen dem Event Server und den Komponenten zu aktivieren, die mit dem Event Server kommunizieren, einschließlich des LPR Server, wählen Sie im Abschnitt **Event Server und Erweiterungen** ein Zertifikat aus.

   Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

   Weitere Informationen zur Vorbereitung Ihres Systems für die sichere Kommunikation finden Sie unter:

   - Sichere Kommunikation (Erklärung) auf Seite 155
   - Der Milestone Leitfaden zur Zertifizierung

   Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.

9. Tun Sie im Fenster **Auswahl des Dateispeicherorts und der Produktsprache** folgendes:

    1. Wählen Sie im Feld **Dateispeicherort** den Speicherort, an dem Sie die Software installieren wollen.

        > Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

    2. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll.
    3. Klicken Sie auf **Installieren**.

    Die Software wird nun installiert. Microsoft® SQL Server® Express und Microsoft IIS werden während der Installation automatisch installiert, falls dies auf dem betreffenden Computer noch nicht erfolgt ist.

10. Sie werden ggf. aufgefordert, Ihren Computer neu zu starten. Nach dem Neustart erscheinen je nach Ihren Sicherheitseinstellungen möglicherweise eine oder mehrere Windows-Sicherheitswarnungen. Akzeptieren Sie diese, um die Installation abzuschließen.

11. Wenn die Installation abgeschlossen ist, wird eine Liste der auf dem Rechner installierten Komponenten angezeigt.

    Klicken Sie auf **Fortfahren**, um Hardware und Benutzer zum System hinzuzufügen.

    > Wenn Sie jetzt auf **Schließen** klicken, umgehen Sie den Konfigurationsassistenten, und XProtect Management Client wird geöffnet. Sie können das System konfigurieren, z.B. um in Management Client Hardware und Benutzer hinzuzufügen.

12. Geben Sie auf der Seite **Benutzernamen und Passwörter für Hardware eingeben** die Benutzernamen und Passwörter für die Hardware ein, in die Sie die vom Hersteller vorgegebenen geändert haben.

    Das Installationsprogramm sucht im Netzwerk nach dieser Hardware sowie nach Hardware mit Standardanmeldeinformationen des Herstellers.

    Klicken Sie auf **Weiter** und warten Sie ab, während das System nach der Hardware sucht.

13. Wählen Sie auf der Seite **Auswahl der zum System hinzuzufügenden Hardware** die Hardware aus, die Sie zum System hinzufügen wollen. Klicken Sie auf **Weiter** und warten Sie ab, während das System die Hardware hinzufügt.

14. Auf der Seite **Konfiguration der Geräte** können Sie die Hardware beschreibende Namen eingeben, indem Sie auf das Bearbeitungssymbol neben dem Hardwarenamen klicken. Dieser Name wird dann den Hardwaregeräten vorangestellt.

    Erweitern Sie den Hardware-Knoten, um Hardwaregeräte wie Kameras, Lautsprecher und Mikrofone zu aktivieren oder zu deaktivieren.

    > Kameras werden standardmäßig aktiviert, und Lautsprecher und Mikrofone werden standardmäßig deaktiviert.

    Klicken Sie auf **Weiter** und warten Sie ab, während das System die Hardware konfiguriert.

15. Auf der Seite **Benutzer hinzufügen** können Sie zum System Benutzer als Windows-Benutzer oder als Basisbenutzer hinzufügen. Diese Benutzer können entweder die Rolle des Administrators oder die eines Benutzers spielen.

    Definieren Sie den Benutzer und klicken Sie auf **Hinzufügen**.

    Wenn Sie das Hinzufügen von Benutzern beenden, klicken Sie auf **Fortfahren**.

16. Wenn die Installation und Erstkonfiguration beendet sind, erscheint die Seite **Konfiguration ist beendet**, auf der Folgendes angezeigt wird:

    - Eine Liste der zum System hinzugefügten Hardwaregeräte
    - Eine Liste von zum System hinzugefügten Benutzern
    - Die Adressen zum XProtect Web Client und XProtect Mobile-Client, die Sie an Ihre Benutzer weitergeben können

    Wenn Sie auf **Schließen** klicken, wird XProtect Smart Client geöffnet und steht zur Benutzung bereit.

## Systeminstallation - Einzel-Computer-Option

Die Option **Einzelcomputer** installiert alle Server- und Client-Komponenten auf dem aktuellen Rechner.

> Milestone empfiehlt Ihnen, vor der Installation den folgenden Abschnitt sorgfältig durchzulesen: Vor dem Start der Installation auf Seite 144.

Für FIPS-Installationen können Sie kein Upgrade von XProtect VMS durchführen, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist. Deaktivieren Sie vor der Installation die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem SQL Server gehosted wird. Wenn Sie allerdings ein Upgrade von XProtect VMS Version 2020 R3 oder später vornehmen, brauchen Sie FIPS nicht zu deaktivieren. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

Nach der Erstinstallation können Sie mit dem Konfigurationsassistenten fortfahren. Je nach Hardware und Konfiguration scannt der Aufzeichnungsserver Ihr Netzwerk nach Hardware. Sie können dann die Hardwaregeräte auswählen, die zu Ihrem System hinzugefügt werden sollen. Kameras sind in Ansichten vorkonfiguriert, und Sie haben die Option zum Aktivieren anderer Geräte wie Mikrofone und Lautsprecher. Sie haben auch die Option, Benutzer entweder mit einer Bedienerrolle oder mit einer Administratorrolle zum System hinzuzufügen. Nach der Installation öffnet sich XProtect Smart Client, und das System ist einsatzbereit.

Andernfalls, wenn Sie den Installationsassistenten schließen, wird XProtect Management Client geöffnet, wo Sie manuelle Konfigurationen vornehmen können, wie z.B. zum Hinzufügen von Hardwaregeräten und Benutzern zum System.

Wenn Sie Aktualisierungen von einer vorherigen Version des Produkts durchführen, sucht das System nicht nach Hardware oder erzeugt neue Ansichten und Benutzerprofile.

1. Laden Sie die Software aus dem Internet herunter (https://www.milestonesys.com/downloads/) und führen Sie die Datei aus. `Milestone XProtect VMS Products 2023 R3 System Installer.exe` aus.
2. Die Installationsdateien werden entpackt. Abhängig von Ihren Sicherheitsseinstellungen erscheinen eine oder mehrere Windows® Sicherheitswarnungen. Akzeptieren Sie diese, um mit dem Entpacken fortzufahren.
3. Nach Abschluss dieses Vorganges erscheint der **Milestone XProtect VMS** Installationsassistent.
    1. Wählen Sie die während der Installation zu verwendende **Sprache** aus (dies ist nicht die Sprache, die Ihr System nach erfolgter Installation verwendet; diese Einstellung erfolgt später). Klicken Sie auf **Weiter**.
    2. Lesen Sie den *Milestone Endbenutzer-Lizenzvertrag*. Wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen dieser Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
    3. Wählen Sie auf der Seite **Datenschutzeinstellungen** aus, ob Sie wollen, dass Nutzungsdaten weitergegeben werden, und klicken Sie dann auf **Weiter**.

> Sie dürfen die Datenerfassung nicht aktivieren, wenn Sie möchten, dass das System eine EU-DSGVO-gerechte Installation ist. Weitere Informationen über den Datenschutz und die Erhebung von Nutzungsdaten finden Sie im Datenschutzleitfaden zur DSGVO.

> Sie können Ihre Datenschutzeinstellungen später jederzeit ändern. Siehe auch Systemeinstellungen (die Dialogbox „Optionen“).

4. Geben Sie im Feld **Geben Sie den Speicherort der Lizenzdatei ein bzw. navigieren Sie dort hin** die Lizenzdatei an, die Sie von Ihrem XProtect-Anbieter erhalten haben. Alternativ können Sie auch zum Dateispeicherort navigieren , oder Sie klicken auf das Link **XProtect Essential+** um eine kostenlose Lizenzdatei herunterzuladen. Informationen zu den Beschränkungen des kostenlosen XProtect Essential+-Produktes finden Sie unter Produktvergleich auf Seite 120. Das System überprüft Ihre Lizenzdatei, bevor Sie fortfahren können. Klicken Sie auf **Weiter**.

4. Wählen Sie **Einzel-Computer**.

   Eine Liste der zu installierenden Komponenten wird angezeigt (Sie können diese Liste nicht bearbeiten). Klicken Sie auf **Weiter**.

5. Geben Sie auf der Seite **Passwort für Systemkonfiguration zuweisen** ein Passwort ein, das Ihre Systemkonfiguration schützt. Dieses Passwort benötigen Sie, falls eine Systemwiederherstellung erforderlich wird oder wenn Sie Ihr System erweitern, z.B. indem Sie Cluster hinzufügen.

   > Es ist wichtig, dass Sie dieses Passwort sicher aufbewahren. Wenn Sie dieses Passwort verlieren, sind Sie ggf. nicht mehr in der Lage, Ihre Systemkonfiguration wiederherzustellen.

   Wenn Sie Ihre Systemkonfiguration nicht mit einem Passwort schützen wollen, wählen Sie **Ich möchte kein Passwort zum Schutz der Systemkonfiguration verwenden, und mir ist klar, dass die Systemkonfiguration dann nicht verschlüsselt ist**.

   Klicken Sie auf **Weiter**.

6. Geben Sie auf der Seite **Zuweisung eines Datenschutzpasswortes für einen Mobile Server** ein Passwort ein, um Ihre Untersuchungen zu verschlüsseln. Als Systemadministrator müssen Sie dieses Passwort eingeben, um auf die Daten auf dem Mobilserver zuzugreifen, falls das System wiederhergestellt werden muss oder wenn Sie das System um weitere Mobilserver erweitern wollen.

   > ⚠ Dieses Passwort müssen Sie sicher aufbewahren. Andernfalls können die Daten auf dem Mobile Server evtl. nicht wiederhergestellt werden.

   Wenn Sie kein Passwort zum Schutz Ihrer Untersuchungen festlegen möchte, wählen Sie **Ich möchte kein Passwort zum Schutz der Daten auf dem Mobile Server verwenden und mir ist klar, dass die Untersuchungen dann nicht verschlüsselt werden**.

   Klicken Sie auf **Weiter**.

7. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an:

   1. Geben Sie den Namen des Aufzeichnungsservers im Feld **Aufzeichnungsserver-Name** ein. Der Standardwert ist der Name des Computers.
   2. Das Feld für die **Management-Server-Adresse** zeigt die Adresse und Port-Nummer des Management-Servers: localhost:80.
   3. Wählen Sie im Feld **Wahl des Speicherorts für die Medien-Datenbank** den Speicherort aus, an dem Sie Ihre Video-Aufzeichnungen speichern möchten. Milestone empfiehlt, einen anderen Speicherort für Ihre Videoaufnahmen zu wählen als den Ort der Programminstallation oder das System-Laufwerk. Der Standard-Speicherort ist das Laufwerk mit der höchsten freien Speicherkapazität.
   4. Legen Sie im Feld **Speicherdauer für Videoaufzeichnungen** fest, wie lange Sie die Aufzeichnungen speichern möchten. Sie können einen Wert zwischen 1 und 365,000 Tagen eingeben, wobei die Standardaufbewahrungsdauer 7 Tage beträgt.
   5. Klicken Sie auf **Weiter**.

8. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

   - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

     Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

     > ⚠ Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

   - Zwischen den Aufzeichnungsservern und den Clients

     Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

   - Zwischen dem Mobile Server und den Clients

     Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

   - Zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren

     Um die Verschlüsselung zwischen dem Event Server und den Komponenten zu aktivieren, die mit dem Event Server kommunizieren, einschließlich des LPR Server, wählen Sie im Abschnitt **Event Server und Erweiterungen** ein Zertifikat aus.

   Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

   Weitere Informationen zur Vorbereitung Ihres Systems für die sichere Kommunikation finden Sie unter:

   - Sichere Kommunikation (Erklärung) auf Seite 155
   - Der Milestone Leitfaden zur Zertifizierung

   Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.

9. Tun Sie im Fenster **Auswahl des Dateispeicherorts und der Produktsprache** folgendes:

    1. Wählen Sie im Feld **Dateispeicherort** den Speicherort, an dem Sie die Software installieren wollen.

        > Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

    2. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll.
    3. Klicken Sie auf **Installieren**.

    Die Software wird nun installiert. Microsoft® SQL Server® Express und Microsoft IIS werden während der Installation automatisch installiert, falls dies auf dem betreffenden Computer noch nicht erfolgt ist.

10. Sie werden ggf. aufgefordert, Ihren Computer neu zu starten. Nach dem Neustart erscheinen je nach Ihren Sicherheitseinstellungen möglicherweise eine oder mehrere Windows-Sicherheitswarnungen. Akzeptieren Sie diese, um die Installation abzuschließen.

11. Wenn die Installation abgeschlossen ist, wird eine Liste der auf dem Rechner installierten Komponenten angezeigt.

    Klicken Sie auf **Fortfahren**, um Hardware und Benutzer zum System hinzuzufügen.

    > Wenn Sie jetzt auf **Schließen** klicken, umgehen Sie den Konfigurationsassistenten, und XProtect Management Client wird geöffnet. Sie können das System konfigurieren, z.B. um in Management Client Hardware und Benutzer hinzuzufügen.

12. Geben Sie auf der Seite **Benutzernamen und Passwörter für Hardware eingeben** die Benutzernamen und Passwörter für die Hardware ein, in die Sie die vom Hersteller vorgegebenen geändert haben.

    Das Installationsprogramm sucht im Netzwerk nach dieser Hardware sowie nach Hardware mit Standardanmeldeinformationen des Herstellers.

    Klicken Sie auf **Weiter** und warten Sie ab, während das System nach der Hardware sucht.

13. Wählen Sie auf der Seite **Auswahl der zum System hinzuzufügenden Hardware** die Hardware aus, die Sie zum System hinzufügen wollen. Klicken Sie auf **Weiter** und warten Sie ab, während das System die Hardware hinzufügt.

14. Auf der Seite **Konfiguration der Geräte** können Sie die Hardware beschreibende Namen eingeben, indem Sie auf das Bearbeitungssymbol neben dem Hardwarenamen klicken. Dieser Name wird dann den Hardwaregeräten vorangestellt.

    Erweitern Sie den Hardware-Knoten, um Hardwaregeräte wie Kameras, Lautsprecher und Mikrofone zu aktivieren oder zu deaktivieren.

    > Kameras werden standardmäßig aktiviert, und Lautsprecher und Mikrofone werden standardmäßig deaktiviert.

    Klicken Sie auf **Weiter** und warten Sie ab, während das System die Hardware konfiguriert.

15. Auf der Seite **Benutzer hinzufügen** können Sie zum System Benutzer als Windows-Benutzer oder als Basisbenutzer hinzufügen. Diese Benutzer können entweder die Rolle des Administrators oder die eines Benutzers spielen.

    Definieren Sie den Benutzer und klicken Sie auf **Hinzufügen**.

    Wenn Sie das Hinzufügen von Benutzern beenden, klicken Sie auf **Fortfahren**.

16. Wenn die Installation und Erstkonfiguration beendet sind, erscheint die Seite **Konfiguration ist beendet**, auf der Folgendes angezeigt wird:

    - Eine Liste der zum System hinzugefügten Hardwaregeräte
    - Eine Liste von zum System hinzugefügten Benutzern
    - Die Adressen zum XProtect Web Client und XProtect Mobile-Client, die Sie an Ihre Benutzer weitergeben können

    Wenn Sie auf **Schließen** klicken, wird XProtect Smart Client geöffnet und steht zur Benutzung bereit.

## Systeminstallation - Benutzerdefiniert

Mit der Option **Benutzerdefiniert** wird der Managementserver installiert. Sie können jedoch auswählen, welche sonstigen Server- und Client-Komponenten Sie auf dem aktuellen Computer installieren wollen. Standardmäßig ist der Aufzeichnungsserver auf der Liste der Komponenten nicht ausgewählt. Abhängig von Ihrer Auswahl können Sie die nicht ausgewählten Komponenten anschließend auf anderen Computern installieren. Weitere Informationen zu jeder Systemkomponente und ihrer Rolle finden Sie unter Produktübersicht auf Seite 33. Die Installation auf anderen Computern erfolgt über die Download-Webseite des Management Servers mit dem Namen Download Manager. Weitere Informationen zur Installation über den Download Manager siehe Download Manager/Download-Webseite auf Seite 198.

> Milestone empfiehlt Ihnen, vor der Installation den folgenden Abschnitt sorgfältig durchzulesen: Vor dem Start der Installation auf Seite 144.

Für FIPS-Installationen können Sie kein Upgrade von XProtect VMS durchführen, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist. Deaktivieren Sie vor der Installation die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem SQL Server gehosted wird. Wenn Sie allerdings ein Upgrade von XProtect VMS Version 2020 R3 oder später vornehmen, brauchen Sie FIPS nicht zu deaktivieren. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

1. Laden Sie die Software aus dem Internet herunter (https://www.milestonesys.com/downloads/) und führen Sie die Datei aus. `Milestone XProtect VMS Products 2023 R3 System Installer.exe` aus.
2. Die Installationsdateien werden entpackt. Abhängig von Ihren Sicherheitsseinstellungen erscheinen eine oder mehrere Windows® Sicherheitswarnungen. Akzeptieren Sie diese, um mit dem Entpacken fortzufahren.
3. Nach Abschluss dieses Vorganges erscheint der **Milestone XProtect VMS** Installationsassistent.
    1. Wählen Sie die während der Installation zu verwendende **Sprache** aus (dies ist nicht die Sprache, die Ihr System nach erfolgter Installation verwendet; diese Einstellung erfolgt später). Klicken Sie auf **Weiter**.
    2. Lesen Sie den *Milestone Endbenutzer-Lizenzvertrag*. Wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen dieser Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
    3. Wählen Sie auf der Seite **Datenschutzeinstellungen** aus, ob Sie wollen, dass Nutzungsdaten weitergegeben werden, und klicken Sie dann auf **Weiter**.

        Sie dürfen die Datenerfassung nicht aktivieren, wenn Sie möchten, dass das System eine EU-DSGVO-gerechte Installation ist. Weitere Informationen über den Datenschutz und die Erhebung von Nutzungsdaten finden Sie im Datenschutzleitfaden zur DSGVO.

        Sie können Ihre Datenschutzeinstellungen später jederzeit ändern. Siehe auch Systemeinstellungen (die Dialogbox „Optionen“).

    4. Geben Sie im Feld **Geben Sie den Speicherort der Lizenzdatei ein bzw. navigieren Sie dort hin** die Lizenzdatei an, die Sie von Ihrem XProtect-Anbieter erhalten haben. Alternativ können Sie auch zum Dateispeicherort navigieren , oder Sie klicken auf das Link **XProtect Essential+** um eine kostenlose Lizenzdatei herunterzuladen. Informationen zu den Beschränkungen des kostenlosen XProtect Essential+-Produktes finden Sie unter Produktvergleich auf Seite 120. Das System überprüft Ihre Lizenzdatei, bevor Sie fortfahren können. Klicken Sie auf **Weiter**.

4. Wählen Sie **Benutzerdefiniert**. Eine Liste der zu installierenden Komponenten wird angezeigt. Mit Ausnahme des Management-Servers sind alle Komponenten in der Liste optional. Der Aufzeichnungsserver und der Mobile Server sind standardmäßig nicht ausgewählt. Wählen Sie die Systemkomponenten aus, die Sie installieren möchten, und klicken Sie dann auf **Weiter**.

   Damit Ihr System korrekt funktioniert, müssen Sie mindestens eine Instanz von XProtect API Gateway installieren.

   In den unten aufgeführten Schritten werden alle Systemkomponenten installiert. Wenn Sie ein stärker verteiltes System erstellen möchten, installieren Sie weniger Systemkomponenten auf diesem Computer und die übrigen Systemkomponenten auf anderen Computern. Wenn Sie einen Installationsschritt nicht wiedererkennen, so liegt dies wahrscheinlich daran, dass Sie die Installation der Systemkomponente, zu der diese Seite gehört, nicht ausgewählt haben. Fahren Sie in diesem Fall mit dem nächsten Schritt fort. Siehe auch Installation über Download Manager (Erklärung) auf Seite 176, Installation eines Aufzeichnungsserver über Download Manager auf Seite 177 und Stille Installation über eine Befehlszeilenoberfläche (Erklärung) auf Seite 183.

5. Nur wenn auf dem Computer mehr als eine IIS-Website zur Verfügung steht, wird die Seite **Wählen Sie eine Website auf dem IIS aus, die Sie mit Ihrem XProtect System verwenden möchten** angezeigt. Sie müssen auswählen, welche Website Sie mit Ihrem XProtect System verwenden wollen. Wählen Sie eine Website mit HTTPS-Bindung. Klicken Sie auf **Weiter**.

   Falls Microsoft® IIS auf dem Computer noch nicht installiert ist, wird es installiert.

6. Wählen Sie auf der Seite **Auswählen Microsoft SQL Server** die SQL Server aus, die Sie verwenden möchten. Siehe auch SQL Server Optionen während der benutzerdefinierten Installation auf Seite 175. Klicken Sie auf **Weiter**.

   Wenn Sie auf Ihrem lokalen Computer keine SQL Server haben, können Sie Microsoft SQL Server Express installieren; auf einem größeren, verteilten System würden Sie in Ihrem Netzwerk jedoch typischerweise einen eigenen SQL Server verwenden.

7. Wählen oder erstellen Sie unter SQL ServerDatenbank auswählenSQL Server (wird nur angezeigt, wenn Sie einen vorhandenen ausgewählt haben), eine Datenbank zum Speichern Ihrer Systemkonfiguration. Wenn Sie sich für eine vorhandene SQL Server-Datenbank entscheiden, entscheiden Sie, ob vorhandene Daten **beibehalten** oder **überschrieben** werden sollen. Falls Sie ein Upgrade durchführen, wählen Sie die Option die vorhandenen Daten beizubehalten, damit Sie Ihre Systemkonfiguration nicht verlieren. Sieh auch SQL Server Optionen während der benutzerdefinierten Installation auf Seite 175. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Datenbankeinstellungen** entweder **Datenbank vom Installationsprogramm erstellen oder neu erstellen lassen** oder **Eine bereits erstellte Datenbank verwenden**.
9. Wenn Sie Ihre Datenbanken automatisch erstellen oder neu erstellen lassen möchten, wählen Sie **Datenbank vom Installationsprogramm erstellen oder neu erstellen lassen**und klicken Sie auf **Weiter**.
10. Um Datenbanken zu verwenden, die Sie für diesen Zweck eingerichtet haben, oder um bereits erstellte Datenbanken zu verwenden, wählen Sie **Vorgefertigte Datenbank verwenden**. Sie gelangen dann auf die **Erweiterte Datenbankeinstellungen** Seite.
11. Auf der Seite **Erweitertes Datenbank-Setup** geben Sie den Server- und den Datenbanknamen für die XProtect-Komponenten ein.
12. Wählen Sie entweder **Windows-Authentifizierung, dem Serverzertifikat nicht vertrauen (empfohlen)** oder **Windows-Authentifizierung, dem Serverzertifikat vertrauen** oder wählen Sie **Azure Active Directory Integrated, dem Serverzertifikat nicht vertrauen (empfohlen)** aus.

    Das zu für die Installation zu verwendende Konto muss abhängig vom zu verwendenden Authentifizierungstypen in Azure AD oder Windows AD erstellt worden sein. Multi-Faktor-Authentifizierung (MFA) wird für die Konten nicht unterstützt.

    Die Option **(Serverzertifikat nicht vertrauen)** wird für die Windows-Authentifizierung empfohlen und ist für das integrierte Azure Active Directory obligatorisch. Das sorgt dafür, dass die Serverzertifikate vor der Installation validiert und verifiziert werden. Weitere Informationen über ungültige Serverzertifikate finden Sie in der Installationprotokolldatei. Mit der Option **Windows-Authentifizierung, dem Serverzertifikat vertrauen** überspringen Sie die Validierung der Serverzertifikate.

13. Klicken Sie auf das Symbol, um die Verbindung zu überprüfen. Indem Sie auf das Symbol klicken, validieren Sie auch die Serverzertifikate.
14. Klicken Sie auf **Weiter**.

15. Geben Sie auf der Seite **Passwort für Systemkonfiguration zuweisen** ein Passwort ein, das Ihre Systemkonfiguration schützt. Dieses Passwort benötigen Sie, falls eine Systemwiederherstellung erforderlich wird oder wenn Sie Ihr System erweitern, z.B. indem Sie Cluster hinzufügen.

   Es ist wichtig, dass Sie dieses Passwort sicher aufbewahren. Wenn Sie dieses Passwort verlieren, sind Sie ggf. nicht mehr in der Lage, Ihre Systemkonfiguration wiederherzustellen.

   Wenn Sie Ihre Systemkonfiguration nicht mit einem Passwort schützen wollen, wählen Sie **Ich möchte kein Passwort zum Schutz der Systemkonfiguration verwenden, und mir ist klar, dass die Systemkonfiguration dann nicht verschlüsselt ist**.

   Klicken Sie auf **Weiter**.

16. Geben Sie auf der Seite **Zuweisung eines Datenschutzpasswortes für einen Mobile Server** ein Passwort ein, um Ihre Untersuchungen zu verschlüsseln. Als Systemadministrator müssen Sie dieses Passwort eingeben, um auf die Daten auf dem Mobilserver zuzugreifen, falls das System wiederhergestellt werden muss oder wenn Sie das System um weitere Mobilserver erweitern wollen.

    Dieses Passwort müssen Sie sicher aufbewahren. Andernfalls können die Daten auf dem Mobile Server evtl. nicht wiederhergestellt werden.

    Wenn Sie kein Passwort zum Schutz Ihrer Untersuchungen festlegen möchte, wählen Sie **Ich möchte kein Passwort zum Schutz der Daten auf dem Mobile Server verwenden und mir ist klar, dass die Untersuchungen dann nicht verschlüsselt werden**.

    Klicken Sie auf **Weiter**.

17. Wählen Sie auf **Auswahl des Dienstkontos für den Aufzeichnungsserver** entweder **Dieses vorgegebene Konto** aus, oder **Dieses Konto**, um das Dienstkonto für den Aufzeichnungsserver auszuwählen.

    Geben Sie ggf. ein Passwort ein.

    Der Benutzername für das Konto muss aus einem einzigen Wort bestehen. Es darf keine Leerzeichen enthalten.

    Klicken Sie auf **Weiter**.

18. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an:
    1. Geben Sie den Namen des Aufzeichnungsservers im Feld **Aufzeichnungsserver-Name** ein. Der Standardwert ist der Name des Computers.
    2. Das Feld für die **Management-Server-Adresse** zeigt die Adresse und Port-Nummer des Management-Servers: localhost:80.
    3. Wählen Sie im Feld **Wahl des Speicherorts für die Medien-Datenbank** den Speicherort aus, an dem Sie Ihre Video-Aufzeichnungen speichern möchten. Milestone empfiehlt, einen anderen Speicherort für Ihre Videoaufnahmen zu wählen als den Ort der Programminstallation oder das System-Laufwerk. Der Standard-Speicherort ist das Laufwerk mit der höchsten freien Speicherkapazität.
    4. Legen Sie im Feld **Speicherdauer für Videoaufzeichnungen** fest, wie lange Sie die Aufzeichnungen speichern möchten. Sie können einen Wert zwischen 1 und 365,000 Tagen eingeben, wobei die Standardaufbewahrungsdauer 7 Tage beträgt.
    5. Klicken Sie auf **Weiter**.

19. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

    - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

      Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

      > Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

    - Zwischen den Aufzeichnungsservern und den Clients

      Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

    - Zwischen dem Mobile Server und den Clients

      Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

    - Zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren

      Um die Verschlüsselung zwischen dem Event Server und den Komponenten zu aktivieren, die mit dem Event Server kommunizieren, einschließlich des LPR Server, wählen Sie im Abschnitt **Event Server und Erweiterungen** ein Zertifikat aus.

    Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

    Weitere Informationen zur Vorbereitung Ihres Systems für die sichere Kommunikation finden Sie unter:

    - Sichere Kommunikation (Erklärung) auf Seite 155
    - Der Milestone Leitfaden zur Zertifizierung

    Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.

20. Wählen Sie auf der Seite **Dateispeicherort und Produktsprache auswählen** den **Speicherort** für die Programmdateien aus.

    > Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

21. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll. Klicken Sie auf **Installieren**.

    Die Software wird nun installiert. Nach Abschluss der Installation wird Ihnen eine Liste mit den erfolgreich installierten Systemkomponenten angezeigt. Klicken Sie auf **Schließen**.

22. Sie werden ggf. aufgefordert, Ihren Computer neu zu starten. Nach dem Neustart erscheinen je nach Ihren Sicherheitseinstellungen möglicherweise eine oder mehrere Windows-Sicherheitswarnungen. Akzeptieren Sie diese, um die Installation abzuschließen.

23. Konfigurieren Sie Ihr System in Management Client. Siehe Aufgabenliste für die Erstkonfiguration auf Seite 206.

24. Installieren Sie, je nach Ihrer Auswahl, die sonstigen Systemkomponenten auf den übrigen Computern durch den Download Manager. Siehe Installation über Download Manager (Erklärung) auf Seite 176.

### SQL Server Optionen während der benutzerdefinierten Installation

Entscheiden Sie sich, welche SQL Server und Datenbank in Verbindung mit den u.a. Optionen verwendet werden soll.

SQL Server Optionen

- **Installieren Sie Microsoft® SQL Server® Express auf diesem Computer**: Diese Option wird nur angezeigt, wenn SQL Server auf diesem Computer nicht installiert ist
- **Verwenden Sie SQL Server auf diesem Computer**: Diese Option wird nur angezeigt, wenn SQL Server bereits auf dem Computer installiert ist
- **Wählen Sie einen SQL Server in Ihrem Netzwerk aus, indem Sie folgende Suche ausführen**: Hiermit können Sie nach allen SQL Server Installationen suchen, die im Subnetz Ihres Netzwerks sichtbar sind
- **Wählen Sie einen SQL Server in Ihrem Netzwerk aus**: Hiermit können Sie die Adresse (den Hostnamen oder die IP-Adresse) von SQL Server eingeben, den Sie mithilfe einer Suche ggf. nicht finden können

SQL Server-Datenbankoptionen:

- **Neue Datenbank erstellen**: Vor allem für Neuinstallationen
- **Vorhandene Datenbank verwenden**: Vor allem für Upgrades bestehender Installationen. Milestone empfiehlt Ihnen, die vorhandene SQL Server-Datenbank beizubehalten und die darin enthaltenen Daten dort zu belassen, damit Sie Ihre Systemkonfiguration nicht verlieren. Sie können auch auswählen, ob Sie die Daten in der SQL Server-Datenbank überschreiben wollen

# Installation neuer XProtect-Komponenten

## Installation über Download Manager (Erklärung)

Falls Sie Systemkomponenten auf anderen Computern installieren wollen als auf dem, auf dem der Managementserver installiert ist, müssen Sie diese Systemkomponenten über die Downloadseite des Management Server installieren Download Manager.

1. Gehen Sie von dem Computer, auf dem Management Server installiert ist, zur Downloadseite des Management Server. Wählen Sie im Windows **Start** menü **Milestone** > **Administrative Installationsseite** aus und notieren oder kopieren Sie die Internetadresse zur späteren Verwendung bei der Installation der Systemkomponenten auf den anderen Computern. Die Adresse hat typischerweise die Form *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Melden Sie sich bei jedem der übrigen Computer an, um eine oder mehrere der sonstigen Systemkomponenten zu installieren:
   - Recording Server(Weitere Informationen finden Sie unter Installation eines Aufzeichnungsserver über Download Manager auf Seite 177 oder Automatische Installation eines Aufzeichnungsservers auf Seite 185)
   - Management Client (Weitere Informationen finden Sie unter Installieren Sie einen Management Client durch Download Manager auf Seite 177)
   - Smart Client
   - Event Server Denken Sie daran, das API Gateway nach der Installation neu zu starten. Wenn Sie den Computer später umbenennen, müssen Sie das API Gateway auch neu starten.

     > ⚠ Wenn Sie die Event Server in einer FIPS-konformen Umgebung installieren, müssen Sie den Windows-FIPS 140-2-Modus vor der Installation deaktivieren.

   - Log Server (Weitere Informationen finden Sie unter Stille Installation eines Log-Servers auf Seite 188)
   - Mobile Server (Weitere Informationen finden Sie im Handbuch für den XProtect Mobile Server)
3. Öffnen Sie einen Internetbrowser, geben Sie die Adresse der Downloadseite des Management Server in das Adressfeld ein und laden Sie das jeweilige Installationsprogramm herunter.
4. Führen Sie das Installationsprogramm aus.

Siehe Systeminstallation - Benutzerdefiniert auf Seite 168, wenn Sie bei den Auswahlmöglichkeiten und Enstellungen in den verschiedenen Installationsschritten im Zweifel sind.

## Installieren Sie einen Management Client durch Download Manager

Wenn es mehrere Administratoren für das XProtect-System gibt oder Sie das XProtect-System einfach von mehreren Computern aus verwalten möchten, können Sie die Installation des Management Client wie folgt durchführen.

> Der Management Client wird stets auf dem Management-Server installiert.

1. Gehen Sie von dem Computer, auf dem Management Server installiert ist, zur Downloadseite des Management Server. Wählen Sie im Windows **Start** menü **Milestone** > **Administrative Installationsseite** aus und notieren oder kopieren Sie die Internetadresse zur späteren Verwendung bei der Installation der Systemkomponenten auf den anderen Computern. Die Adresse hat typischerweise die Form *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Melden Sie sich an dem Computer an, auf dem Sie die Systemkomponente installieren möchten.
1. Öffnen Sie einen Internet-Browser und geben Sie die Adresse der Download-Webseite des Management Server in das Adressfeld ein und drücken Sie die Eingabetaste.
3. Klicken Sie auf **Alle Sprachen**, um das Management Client-Installationsprogramm aufzurufen. Führen Sie die heruntergeladene Datei aus.
4. Klicken Sie in allen Meldungen auf **Ja**. Das Entpacken beginnt.
5. Wählen Sie die Sprache für das Installationsprogramm aus. Klicken Sie auf **Weiter**.
6. Lesen Sie und akzeptieren Sie die Lizenzvereinbarung. Klicken Sie auf **Weiter**.
7. Wählen Sie den Dateispeicherort und die Produktsprache. Klicken Sie auf **Installieren**.
8. Die Installation ist abgeschlossen. Es wird eine Liste der erfolgreich installierten Komponenten angezeigt. Klicken Sie auf **Schließen**.
9. Klicken Sie auf das Symbol auf dem Desktop, um die Management Client zu öffnen.
10. Der Management Client-Anmeldedialog wird angezeigt.
11. Geben Sie den Hostnamen oder die IP-Adresse des Management-Servers im Feld **Computer** an.
12. Wählen Sie Anmeldung und geben Sie Ihren Benutzernamen und Ihr Passwort ein. Klicken Sie auf **Verbinden**. Der Management Client wird gestartet.

    Um alle Einzelheiten über die Funktionen in der Management Client nachzulesen und was Sie mit Ihrem System erreichen können, klicken Sie auf **Hilfe** im Werkzeugmenü.

## Installation eines Aufzeichnungsserver über Download Manager

Wenn Ihre Systemkomponenten auf separate Computer verteilt sind, können Sie die Aufzeichnungsserver installieren, indem Sie den untenstehenden Anweisungen folgen.

Der Aufzeichnungsserver ist bereits installiert, wenn Sie eine **Einzelcomputer**-Installation vorgenommen haben. Aber Sie können die gleichen Anweisungen befolgen, um weitere Aufzeichnungsserver hinzuzufügen, wenn Sie mehr Kapazität benötigen.

Wenn Sie einen Failover-Aufzeichnungsserver installieren müssen, siehe Installation eines Failover-Aufzeichnungsservers Download Manager auf Seite 181.

1. Gehen Sie von dem Computer, auf dem Management Server installiert ist, zur Downloadseite des Management Server. Wählen Sie im Windows **Start** menü **Milestone** > **Administrative Installationsseite** aus und notieren oder kopieren Sie die Internetadresse zur späteren Verwendung bei der Installation der Systemkomponenten auf den anderen Computern. Die Adresse hat typischerweise die Form *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Melden Sie sich an dem Computer an, auf dem Sie die Systemkomponente installieren möchten.
3. Öffnen Sie einen Internet-Browser und geben Sie die Adresse der Download-Webseite des Management Server in das Adressfeld ein und drücken Sie die Eingabetaste.
4. Laden Sie das Installationsprogramm für den Aufzeichnungsserver herunter, indem Sie **Alle Sprachen** unter dem **Installationsprogramm für den Aufzeichnungsserver** auswählen. Speichern Sie das Installationsprogramm, oder führen Sie es direkt von der Webseite aus aus.
5. Wählen Sie die **Sprache**, die Sie für die Installation verwenden wollen. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Wählen Sie einen Installationstyp** aus:

   **Typisch**, um einen Aufzeichnungsserver mit den Standardwerten zu installieren, oder

   **Benutzerdefiniert**, um einen Aufzeichnungsserver mit benutzerdefinierten Werten zu installieren.

7. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an:
    1. Geben Sie den Namen des Aufzeichnungsservers im Feld **Aufzeichnungsserver-Name** ein. Der Standardwert ist der Name des Computers.
    2. Das Feld für die **Management-Server-Adresse** zeigt die Adresse und Port-Nummer des Management-Servers: localhost:80.
    3. Wählen Sie im Feld **Wahl des Speicherorts für die Medien-Datenbank** den Speicherort aus, an dem Sie Ihre Video-Aufzeichnungen speichern möchten. Milestone empfiehlt, einen anderen Speicherort für Ihre Videoaufnahmen zu wählen als den Ort der Programminstallation oder das System-Laufwerk. Der Standard-Speicherort ist das Laufwerk mit der höchsten freien Speicherkapazität.
    4. Legen Sie im Feld **Speicherdauer für Videoaufzeichnungen** fest, wie lange Sie die Aufzeichnungen speichern möchten. Sie können einen Wert zwischen 1 und 365,000 Tagen eingeben, wobei die Standardaufbewahrungsdauer 7 Tage beträgt.
    5. Klicken Sie auf **Weiter**.
8. Die Seite **IP-Adressen der Aufzeichnungsserver** wird nur angezeigt, wenn Sie **Benutzerdefiniert** ausgewählt haben. Geben Sie die Anzahl der Aufzeichnungsserver an, die Sie auf diesem Computer installieren wollen. Klicken Sie auf **Weiter**.
9. Wählen Sie auf **Auswahl des Dienstkontos für den Aufzeichnungsserver** entweder **Dieses vorgegebene Konto** aus, oder **Dieses Konto**, um das Dienstkonto für den Aufzeichnungsserver auszuwählen.

    Geben Sie ggf. ein Passwort ein.

    > Der Benutzername für das Konto muss aus einem einzigen Wort bestehen. Es darf keine Leerzeichen enthalten.

    Klicken Sie auf **Weiter**.

10. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

    - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

      Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

      > Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

    - Zwischen den Aufzeichnungsservern und den Clients

      Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

    - Zwischen dem Mobile Server und den Clients

      Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

    - Zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren

      Um die Verschlüsselung zwischen dem Event Server und den Komponenten zu aktivieren, die mit dem Event Server kommunizieren, einschließlich des LPR Server, wählen Sie im Abschnitt **Event Server und Erweiterungen** ein Zertifikat aus.

    Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

    Weitere Informationen zur Vorbereitung Ihres Systems für die sichere Kommunikation finden Sie unter:

    - Sichere Kommunikation (Erklärung) auf Seite 155
    - Der Milestone Leitfaden zur Zertifizierung

    Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.

11. Wählen Sie auf der Seite **Dateispeicherort und Produktsprache auswählen** den **Speicherort** für die Programmdateien aus.

    > Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

12. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll. Klicken Sie auf **Installieren**.

    Die Software wird nun installiert. Nach Abschluss der Installation wird Ihnen eine Liste mit den erfolgreich installierten Systemkomponenten angezeigt. Klicken Sie auf **Schließen**.

13. Sobald der Aufzeichnungsserver installiert wurde, können Sie dessen Betriebszustand dem Recording Server Manager-Task-Leistensymbol entnehmen und diesen in Management Client konfigurieren. Weitere Informationen finden Sie unter Aufgabenliste für die Erstkonfiguration auf Seite 206.

## Installation eines Failover-Aufzeichnungsservers Download Manager

> ⚠ Wenn Sie Workgroups betreiben, müssen Sie für Failover-Recordingserver die alternative Installationsmethode verwenden (siehe Installation für Arbeitsgruppen auf Seite 192).

1. Gehen Sie von dem Computer, auf dem Management Server installiert ist, zur Downloadseite des Management Server. Wählen Sie im Windows **Start** menü **Milestone** > **Administrative Installationsseite** aus und notieren oder kopieren Sie die Internetadresse zur späteren Verwendung bei der Installation der Systemkomponenten auf den anderen Computern. Die Adresse hat typischerweise die Form *http://[management server address]/installation/Admin/default-en-US.htm*.

   Melden Sie sich an dem Computer an, auf dem Sie die Systemkomponente installieren möchten.

2. Öffnen Sie einen Internet-Browser und geben Sie die Adresse der Download-Webseite des Management Server in das Adressfeld ein und drücken Sie die Eingabetaste.

3. Laden Sie das Installationsprogramm für den Aufzeichnungsserver herunter, indem Sie **Alle Sprachen** unter dem **Installationsprogramm für den Aufzeichnungsserver** auswählen. Speichern Sie das Installationsprogramm, oder führen Sie es direkt von der Webseite aus aus.

4. Wählen Sie die **Sprache**, die Sie für die Installation verwenden wollen. Klicken Sie auf **Weiter**.

5. Wählen Sie auf der Seite **Installationstyp auswählen Failover** aus, um einen Aufzeichnungsserver als Failover-Server zu installieren.

6. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an. Den Namen des ausfallsicheren Aufzeichnungsservers, die Adresse des Managementservers und den Pfad zur Mediendatenbank. Klicken Sie auf **Weiter**.

7. Auf der Seite **Dienstkonto für den Aufzeichnungsserver auswählen** müssen Sie beim Installieren eines ausfallsicheren Aufzeichnungsservers dasjenige Benutzerkonto verwenden, das den Namen **Dieses Konto** trägt. Hiermit wird das Failover-Benutzerkonto erstellt. Geben Sie ggf. ein Passwort ein und bestätigen Sie es. Klicken Sie auf **Weiter**.

8. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

   - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

     Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

     > Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

   - Zwischen den Aufzeichnungsservern und den Clients

     Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

   - Zwischen dem Mobile Server und den Clients

     Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

   - Zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren

     Um die Verschlüsselung zwischen dem Event Server und den Komponenten zu aktivieren, die mit dem Event Server kommunizieren, einschließlich des LPR Server, wählen Sie im Abschnitt **Event Server und Erweiterungen** ein Zertifikat aus.

   Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

   Weitere Informationen zur Vorbereitung Ihres Systems für die sichere Kommunikation finden Sie unter:

   - Sichere Kommunikation (Erklärung) auf Seite 155
   - Der Milestone Leitfaden zur Zertifizierung

   Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.

9. Wählen Sie auf der Seite **Dateispeicherort und Produktsprache auswählen** den **Speicherort** für die Programmdateien aus.

   > Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

10. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll. Klicken Sie auf **Installieren**.

    Die Software wird nun installiert. Nach Abschluss der Installation wird Ihnen eine Liste mit den erfolgreich installierten Systemkomponenten angezeigt. Klicken Sie auf **Schließen**.

11. Sobald der ausfallsichere Aufzeichnungsserver installiert wurde, können Sie dessen Betriebszustand dem Failover Server-Symbol Aufzeichnungsserver-Dienst entnehmen und diesen in Management Client konfigurieren. Weitere Informationen finden Sie unter Aufgabenliste für die Erstkonfiguration auf Seite 206.

## Installieren von XProtect VMS mit nicht standardmäßigen Ports

Eine Installation von XProtect VMS erfordert bestimmte Ports. Insbesondere der Management Server und API Gateway laufen im IIS, wobei bestimmte Ports verfügbar sein müssen. Dieses Thema beschreibt die Installation von XProtect VMS und die Verwendung von nicht standardmäßigen Ports auf dem IIS. Dies gilt auch, wenn nur die API Gateway installiert wird.

Eine Übersicht über alle Ports, die das VMS verwendet, finden Sie im XProtect VMS Administratorhandbuch (https://doc.milestonesys.com/2023r3/de-DE/portal/htm/chapter-page-mc-administrator-manual.htm).

Wenn IIS noch nicht auf dem System installiert ist, installiert die XProtect VMS das IIS und verwendet die Standard-Website mit Standard-Ports.

Um die Verwendung des XProtect VMS-Standards zu vermeiden, installieren Sie zuerst den IIS. Fügen Sie optional eine neue Website hinzu oder fahren Sie mit der Standard-Website fort.

Fügen Sie eine Bindung für HTTPS hinzu, falls sie noch nicht vorhanden ist, und wählen Sie ein gültiges Zertifikat auf dem Computer aus. (Sie müssen es während der Installation von XProtect VMS auswählen). Ändern Sie die Portnummern der HTTP und HTTPS-Bindungen auf verfügbare Ports Ihrer Wahl.

Führen Sie das XProtect VMS-Installationsprogramm aus und wählen Sie eine **benutzerdefinierte** Installation.

Während der Installation erscheint die Seite **eine Website auswählen auf IIS zur Verwendung mit Ihrem XProtect-System**, wenn mehr als eine Website verfügbar ist. Sie müssen auswählen, welche Website Sie mit Ihrem XProtect System verwenden wollen. Das Installationsprogramm verwendet die geänderten Portnummern.

## Stille Installation über eine Befehlszeilenoberfläche (Erklärung)

Mit der stillen Installation können Systemadministratoren den XProtect VMS und die Smart Client-Software über ein großes Netzwerk ohne Mitwirkung der Anwender und mit möglichst wenig Störung für den Endanwender installieren und aktualisieren.

Die Installationsdateien XProtect VMS und Smart Client (.exe-Dateien) haben unterschiedliche Befehlszeilenargumente. Sie haben jeweils einen eigenen Satz Befehlszeilenparameter, die in einer Befehlszeilenoberfläche direkt oder über eine Datei mit Argumenten aktiviert werden können. In der Befehlszeilenoberfläche können Sie zusammen mit den Installationsdateien auch Befehlszeilenoptionen verwenden.

Sie können die Installationsdateien für XProtect, ihre Befehlszeilenparameter und ihre Befehlszeilenoptionen mit Tools für die stille Verteilung und Installation mit Software wie Microsoft System Center Configuration Manager (SCCM, auch als ConfigMgr bekannt) kombinieren. Weitere Informationen zu solchen Tools finden Sie auf der Internetseite des Herstellers. Sie können Milestone Software Manager auch für die Ferninstallation und für die Aktualisierung von XProtect VMS, Device-Packs und Smart Client verwenden. Weitere Informationen finden Sie im Administratorhandbuch für Milestone Software Manager.

**Dateien mit Befehlszeileparametern und -argumenten**

Bei der stillen Installationen können Sie Einstellungen angeben, die mit den verschiedenen Komponenten des VMS-Systems verknüpft sind sowie mit deren interner Kommunikation, mit Dateien mit Befehlszeilenparametern und -Argumenten. Dateien mit Befehlszeilenparametern und -Argumenten sollten nur für Neuinstallationen verwendet werden, da Sie die Einstellungen, die die Befehlszeilenparameter darstellen, während eines Upgrades nicht ändern können.

Um die verfügbaren Befehlszeilenparameter anzusehen und Dateien mit Argumenten für ein Installationsprogramm zu erzeugen, navigieren Sie in der Befehlszeilenoberfläche zu dem Verzeichnis, in dem sich das Installationsprogramm befindet, und geben Sie den folgenden Befehl ein:

```
[NameOfExeFile].exe --generateargsfile=[path]
```

Beispiel:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

In der gespeicherten Datei mit den Argumenten (Arguments.xml) hat jeder Befehlszeilenparameter eine Beschreibung, die dessen Zweck angibt. Sie können die Datei mit den Argumenten verändern und abspeichern, damit die Werte der Befehlszeilenparameter die Bedürfnisse Ihrer Installation erfüllen.

Wenn Sie eine Datei mit Argumenten gemeinsam mit deren Installationsprogramm verwenden wollen, verwenden Sie die Befehlszeilenoption `--arguments`, indem Sie den folgenden Befehl eingeben:

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

Beispiel:

```
Milestone XProtect VMS Products 2023 R3 System Installer.exe --quiet
--arguments=C:\temp\arguments.xml
```

**Befehlszeilenoptionen**

In der Befehlszeilenoberfläche können Sie Installationsdateien auch mit Befehlszeilenoptionen kombinieren. Die Befehlszeilenoptionen verändern allgemein das Verhalten eines Befehls.

Um eine vollständige Liste der Befehlszeilenoptionen angezeigt zu bekommen, navigieren Sie in der Befehlszeilenoberfläche zu dem Verzeichnis, in dem sich das Installationsprogramm befindet, und geben Sie `[NameOfExeFile].exe --help` ein. Damit die Installation erfolgreich ist, müssen Sie für Befehlszeilenoptionen, die einen Wert erfordern, einen solchen angeben.

Sie können sowohl Befehlszeilenparameter als auch Befehlszeilenoptionen im selben Befehl verwenden. Verwenden Sie die Befehlszeilenoption `--parameters` und trennen Sie die einzelnen Befehlszeilenparameter mit einem Doppelpunkt (:). In dem Beispiel weiter unten sind `--quiet`, `--showconsole` und `--parameters` Befehlszeilenoptionen, und `ISFAILOVER` und `RECORDERNAME` sind Befehlszeilenparameter:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

## Automatische Installation eines Aufzeichnungsservers

Bei der stillen Installation werden Sie nicht benachrichtigt, wenn die Installation abgeschlossen ist. Um benachrichtigt zu werden, fügen Sie zu dem Befehl die Befehlszeilenoption `--showconsole` hinzu. Das Taskleistensymbol Milestone XProtect Recording Server erscheint, wenn die Installation abgeschlossen ist.

In dem Beispielbefehl weiter unten müssen der Text in den eckigen Klammern ([ ]) und auch die eckigen Klammern selbst durch echte Werte ersetzt werden. Beispiel: anstatt "[path]" könnten Sie eingeben `d:\program files\`, `d:\record\` oder `\\network-storage-02\surveillance`. Verwenden Sie die Befehlszeilenoption `--help`, um etwas zu den zulässigen Formaten für den Wert jeder Befehlszeileoption zu lesen.

1. Melden Sie sich an dem Computer an, auf dem die Komponente Recording Server installiert werden soll.
2. Öffnen Sie einen Internetbrowser und geben Sie die Adresse der Download-Webseite des Management Server ein, die das Ziel des Administrators sein soll, und drücken Sie die Eingabetaste.

   Diese Adresse hat typischerweise die Form `http://[management server address]:[port]/installation/Admin/default-en-US.htm`.
3. Laden Sie das Installationsprogramm für den Aufzeichnungsserver herunter, indem Sie **Alle Sprachen** unter dem **Installationsprogramm für den Recording Server** auswählen.
4. Öffnen Sie die von Ihnen gewünschte Befehlszeilenoberfläche. Zum Öffnen von Windows Command Prompt, öffnen Sie das Startmenü von Windows und geben Sie **cmd** ein.
5. Navigieren Sie zu dem Verzeichnis, in dem sich die heruntergeladene Installationsdatei befindet.
6. Setzen Sie die Installation nach einem der beiden weiter unten aufgeführten Szenarien fort:

**Szenario 1: Upgrade einer vorhandenen Installation oder Installation auf einem Server mit der Management Server-Komponente mit Standardwerten**

- Geben Sie den folgenden Befehl ein, dann beginnt die Installation.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

**Szenario 2: Installation in einem verteilten System**

1. Geben Sie den folgenden Befehl ein, um eine Datei mit Argumenten mit Befehlszeilenparametern zu erzeugen.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=
[path]
```

2. Öffnen Sie die Datei mit den Argumenten (Arguments.xml) von dem angegebenen Pfad aus und ändern Sie ggf. die Werte der Befehlszeilenparameter.

> Achten Sie darauf, den Befehlszeilenparametern SERVERHOSTNAME und SERVERPORT gültige Werte zuzuordnen. Andernfalls kann die Installation nicht abgeschlossen werden.

4. Speichern Sie die Datei mit den Argumenten.
5. Kehren Sie zur Befehlszeilenoberfläche zurück und geben Sie den u.a. Befehl ein, um die Installation mit den in der Datei mit den Argumenten angegebenen Werte für die Befehlszeilenparameter vorzunehmen.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=[path]\[filename]
```

## Stille Installation von XProtect Smart Client

Bei der stillen Installation werden Sie nicht benachrichtigt, wenn die Installation abgeschlossen ist. Um benachrichtigt zu werden, fügen Sie zu dem Befehl die Befehlszeilenoption `--showconsole` hinzu. Auf dem Desktop erscheint ein Link zu XProtect Smart Client, wenn die Installation abgeschlossen ist.

In dem Beispielbefehl weiter unten müssen der Text in den eckigen Klammern ([ ]) und auch die eckigen Klammern selbst durch echte Werte ersetzt werden. Beispiel: anstatt "[path]" könnten Sie eingeben `d:\program files\`, `d:\record\` oder `\\network-storage-02\surveillance`. Verwenden Sie die Befehlszeilenoption `--help`, um etwas zu den zulässigen Formaten für den Wert jeder Befehlszeileoption zu lesen.

1. Öffnen Sie einen Internetbrowser und geben Sie die Adresse der Download-Webseite des Management Server in die Adresszeile ein, die das Ziel beim Endbenutzer sein soll, und drücken Sie die Eingabetaste.

   Diese Adresse hat typischerweise die Form `http://[management server address]:[port]/installation/default-en-US.htm`.

2. Laden Sie das Installationsprogramm XProtect Smart Client herunter, indem Sie **Alle Sprachen** unter dem Installationsprogramm **XProtect Smart Client** auswählen.

3. Öffnen Sie die von Ihnen gewünschte Befehlszeilenoberfläche. Zum Öffnen von Windows Command Prompt, öffnen Sie das Startmenü von Windows und geben Sie **cmd** ein.

4. Navigieren Sie zu dem Verzeichnis, in dem sich die heruntergeladene Installationsdatei befindet.

5. Setzen Sie die Installation nach einem der beiden weiter unten aufgeführten Szenarien fort:

   **Szenario 1: Upgrade einer vorhandenen Installation, oder Installation mit Standardwerten für die Befehlszeilenparameter**

   - Geben Sie den folgenden Befehl ein, dann beginnt die Installation.

     ```
     "XProtect Smart Client 2023 R3 Installer.exe" --quiet
     ```

   **Szenario 2: Installation mit benutzerdefinierten Werten für die Befehlszeilenparameter mithilfe einer xml-Argumentdatei als Eingabe**

   1. Geben Sie den folgenden Befehl ein, um eine XML-Datei mit Argumenten mit Befehlszeilenparametern zu erzeugen.

      ```
      "XProtect Smart Client 2023 R3 Installer.exe" --generateargsfile=[path]
      ```

   2. Öffnen Sie die Datei mit den Argumenten (Arguments.xml) von dem angegebenen Pfad aus und ändern Sie ggf. die Werte der Befehlszeilenparameter.

   3. Speichern Sie die Datei mit den Argumenten.

   4. Kehren Sie zur Befehlszeilenoberfläche zurück und geben Sie den u.a. Befehl ein, um die Installation mit den in der Datei mit den Argumenten angegebenen Werte für die Befehlszeilenparameter vorzunehmen.

      ```
      "XProtect Smart Client 2023 R3 Installer.exe" --quiet --arguments=[path]\[filename]
      ```

## Stille Installation eines Log-Servers

Bei der stillen Installation werden Sie nicht benachrichtigt, wenn die Installation abgeschlossen ist. Um benachrichtigt zu werden, fügen Sie zu dem Befehl die Befehlszeilenoption `--showconsole` hinzu.

In dem Beispielbefehl weiter unten müssen der Text in den eckigen Klammern ([ ]) und auch die eckigen Klammern selbst durch echte Werte ersetzt werden. Beispiel: anstatt "[path]" könnten Sie eingeben `d:\program files\`, `d:\record\` oder `\\network-storage-02\surveillance`. Verwenden Sie die Befehlszeilenoption `--help`, um etwas zu den zulässigen Formaten für den Wert jeder Befehlszeileoption zu lesen.

1. Melden Sie sich an dem Computer an, auf dem die Komponente Log Server installiert werden soll.
2. Öffnen Sie einen Internetbrowser und geben Sie die Adresse der Download-Webseite des Management Server ein, die das Ziel des Administrators sein soll, und drücken Sie die Eingabetaste.

   Diese Adresse hat typischerweise die Form `http://[management server address]:[port]/installation/Admin/default-en-US.htm`.
3. Laden Sie das Installationsprogramm für den Log-Server herunter, indem Sie **Alle Sprachen** unter dem **Installationsprogramm für den Log-Server** auswählen.
4. Öffnen Sie die von Ihnen gewünschte Befehlszeilenoberfläche. Zum Öffnen von Windows Command Prompt, öffnen Sie das Startmenü von Windows und geben Sie **cmd** ein.
5. Navigieren Sie zu dem Verzeichnis, in dem sich die heruntergeladene Installationsdatei befindet.
6. Setzen Sie die Installation nach einem der beiden weiter unten aufgeführten Szenarien fort:

**Szenario 1: Upgrade einer vorhandenen Installation, oder Installation mit Standardwerten für die Befehlszeilenparameter**

- Geben Sie den folgenden Befehl ein, dann beginnt die Installation.

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --showconsole
```

**Szenario 2: Installation mit benutzerdefinierten Werten für die Befehlszeilenparameter mithilfe einer XML-Argumentdatei als Eingabe**

1. Geben Sie den folgenden Befehl ein, um eine XML-Datei mit Argumenten mit Befehlszeilenparametern zu erzeugen.

```
"XProtect Log Server 2023 R3 Installer x64.exe" --generateargsfile=
[path]
```

2. Öffnen Sie die Datei mit den Argumenten (Arguments.xml) von dem angegebenen Pfad aus und ändern Sie ggf. die Werte der Befehlszeilenparameter.

3. Speichern Sie die Datei mit den Argumenten.
4. Kehren Sie zur Befehlszeilenoberfläche zurück und geben Sie den u.a. Befehl ein, um die Installation mit den in der Datei mit den Argumenten angegebenen Werte für die Befehlszeilenparameter vorzunehmen.

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --arguments=
[path]\[filename] --showconsole
```

## Automatische Installation mit einem dedizierten Dienstkonto

Wenn Sie XProtect VMS automatisch installieren möchten, müssen Sie das Installationsprogramm mit den Argumenten in der unteren Tabelle starten. Argumente müssen erstellt und in einer XML-Datei für Argumente gespeichert werden, die Sie vor der Installation generieren.

| Argument | Beschreibung |
|---|---|
| `--quiet` | Erzwingt die automatische Installation. |
| `--arguments` | Der Pfad zur XML-Datei für Argumente mit vollständiger Konfiguration. Beispielpfad: `C:\Arguments.xml`. |
| `--license` | Der Pfad zur Lizenzdatei. |

### Installation mit einem dedizierten Dienstkonto

Diese Beschreibung basiert auf dem Einsatz eines dedizierten Dienstkontos für integrierte Sicherheit. Diese Dienste werden immer auf dem dedizierten Konto ausgeführt, unabhängig davon, welcher Benutzer angemeldet ist. Sie müssen sicherstellen, dass dieses Konto alle erforderlichen Berechtigungen hat, zum Beispiel zum Ausführen von Aufgaben und Aufrufen von Netzwerk, Dateien und freigegebenen Ordnern.

Das Dienstkonto muss in einer XML-Datei für Argumente mit den folgenden Schlüsseln festgelegt werden:

| |
|---|
| `SERVICEACCOUNT` |
| `SERVICEACCOUNT_NONLOC` |

Das Passwort für das Dienstkonto muss in Klartext im Wert für den folgenden Schlüssel angegeben werden:

```
ENCRYPTEDPASSWORD
```

Beispiel: Befehlszeile zum Start der Installation im automatischen Modus:

```
"Milestone XProtect VMS Products 2023 R2 System Installer.exe" --quiet --
arguments=C:\Arguments.xml --license=C:\M01-C01-231-01-ABCDEF.lic
```

Beispiel: Argumentedatei basierend auf dem Einsatz eines dedizierten Dienstkontos

```
<?xml version="1.0" encoding="utf-8"?>
<CommandLineArguments xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="urn:milestone-systems">
  <InstallEnvironment>
    <Parameters>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>USERACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT_NONLOC</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>sampleaccountpasswordplaintext</Value>
        <Key>ENCRYPTEDPASSWORD</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>%PROGRAMFILES%\Milestone</Value>
        <Key>TARGETDIR</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsXPCO</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsDPInstaller</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>false</Value>
        <Key>LEGACY</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>yes</Value>
        <Key>SQL-KEEP-DATA</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>no</Value>
        <Key>SQL-CREATE-DATABASE</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>True</Value>
```

```
        <Key>IS_EXTERNALLY_MANAGED</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_MS</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IDP;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IDP</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IM;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IM</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_ES</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_
LogServerV2;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated;Application
Name=Surveillance_LogServerV2</Value>
        <Key>SQL_CONNECTION_STRING_LOG</Key>
      </KeyValueParametersOfStringString>
    </Parameters>
  </InstallEnvironment>
</CommandLineArguments>
```

Zu erfüllende Voraussetzungen vor dem Durchführen der Installation:

- Das Dienstkonto sowie das für die Installation verwendete Konto müssen erstellt werden.
- Das Dienstkonto muss für die Anmeldung als Dienst auf dem Computer, auf dem die Installation durchgeführt wird, zugelassen sein. Siehe als Dienst anmelden.
- Die von XProtect zu verwendenden Datenbanken müssen erstellt werden und die Datenbanken müssen in der XML-Datei für die Argumente benannt werden, zum Beispiel:

| Datenbankname |
| --- |
| Überwachung |
| Surveillance_IDP |
| Surveillance_IM |
| Surveillance_LogServerV2 |

- Die Datenbanken müssen gemäß der folgenden Liste konfiguriert sein:

| Datenbankkonfiguration |
|---|
| Die Standardkollation muss auf Folgendes festgelegt werden: „SQL_Latin1_General_CP1_CI_AS“ |
| ALLOW_SNAPSHOT_ISOLATION muss festgelegt werden auf EIN |
| READ_COMMITTED_SNAPSHOT muss festgelegt werden auf EIN |

- Eine SQL Server Anmeldung muss für das Dienstkonto und für das Konto erstellt werden, das für die Installation in jeder der Datenbanken verwendet wird. Ein Datenbankbenutzer muss in jeder der Datenbanken erstellt werden und der Benutzer muss ein Mitglied der Rolle db_owner in jeder Datenbank sein.

## Installation für Arbeitsgruppen

Wenn Sie keine Domäneneinrichtung mit einem Active Directory-Server verwenden, sondern eine Workgroup-Einrichtung, gehen Sie bei der Installation wie folgt vor.

> Alle Computer in einer verteilten Einrichtung müssen entweder in einer Domäne oder in einer Workgroup sein.

1. Melden Sie sich mit einem allgemeinen Administratorkonto bei Windows an.

   > Achten Sie darauf, das gleiche Konto auf allen Computern im System zu verwenden.

2. Starten Sie abhängig von Ihren Anforderungen die Installation des Management- oder des Aufzeichnungsservers und klicken Sie auf **Benutzerdefiniert**.
3. Entsprechend Ihrer Auswahl in Schritt 2 wählen Sie die Option zur Installation des Management Server- oder des Recording Server-Dienstes aus, wobei Sie ein allgemeines Administratorkonto benutzen können.
4. Beenden Sie die Installation.
5. Wiederholen Sie die Schritte 1-4, um weitere, zu verbindende Systeme zu installieren. Sie müssen alle unter Verwendung eines allgemeinen Administratorkontos installiert werden.

# Installation in einem Cluster

Bevor Sie in einem Cluster installieren, siehe Mehrere Management-Server (Cluster) (Erklärung) auf Seite 141 und Anforderungen für Cluster auf Seite 142.

Die Beschreibungen und Illustrationen unterscheiden sich ggf. von dem, was auf Ihren Bildschirm angezeigt wird.

**Zum Installieren des Management-Servers:**

1. Installieren Sie den Management-Server und alle seine Unterkomponenten auf dem ersten Server im Cluster.

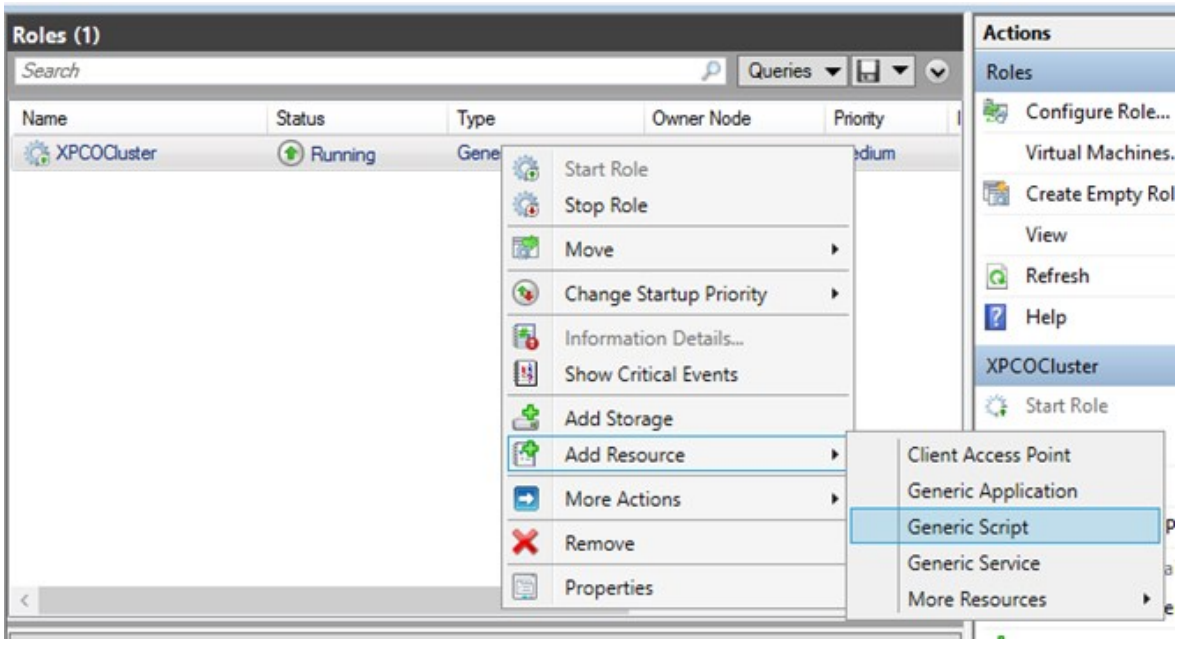
   Der Managementserver muss mit einem bestimmten Benutzer installiert werden und nicht als Netzwerkdienst. Hierfür ist es erforderlich, dass Sie zur Installation die Option **Benutzerdefiniert** verwenden. Der spezifische Benutzer muss außerdem Zugriff zum gemeinsamen Netzlaufwerk haben, und vorzugsweise ein Passwort, das nicht abläuft.

**Konfigurieren Sie als nächstes den Dienst Management Server als allgemeinen Dienst im ausfallsicheren Cluster:**

1. Gehen Sie auf dem letzten Server, auf dem Sie den Managementserver installiert haben, auf **Start** > **Administrative Hilfsmittel**, öffnen Sie das **Failover Cluster Management** von Windows. Erweitern Sie im Fenster **Failover Cluster Management** Ihren Cluster, klicken Sie mit der rechten Maustaste auf **Rollen** und wählen Sie **Rolle konfigurieren**.


2. Klicken Sie auf der Seite **Assistent für hohe Verfügbarkeit**, > **Bevor Sie beginnen**, auf **Weiter**.
3. Wählen Sie auf der Seite **Rolle auswählen** die Option **Allgemeiner Dienst** und klicken Sie auf **Weiter**.

4. Wählen Sie auf der Seite **Dienst auswählen** den **Milestone XProtect Management Server** Dienst und klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Client-Zutrittspunkt** den Namen an (Hostname des Clusters), den die Clients verwenden, wenn sie auf den Dienst zugreifen. Der Hostname muss sich vom Namen des Clusters unterscheiden. Klicken Sie auf **Weiter**.
6. Klicken Sie Fenster im **Speicher auswählen** auf **Weiter**, da kein Speicher für den Dienst erforderlich ist.
7. Auf der Seite **Registrierungseinstellungen replizieren** klicken Sie auf **Weiter**, da keine Registrierungseinstellungen repliziert werden sollen.
8. Klicken Sie auf der **Bestätigungsseite** auf **Weiter**, nachdem Sie überprüft haben, ob der Cluster-Dienst entsprechend Ihren Anforderungen konfiguriert ist.
9. Klicken Sie auf der Seite **Hohe Verfügbarkeit konfigurieren** auf **Weiter**.
10. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertigstellen**, um die Konfiguration des Management-Servers als allgemeinen Dienst im Failover-Cluster abzuschließen.
11. Klicken Sie mit der rechten Maustaste auf die Rolle, die Sie gerade erstellt haben, und klicken Sie auf **Ressource hinzufügen** > **Generisches Skript**. Wählen Sie Milestone XProtect Event Server, um den **Milestone XProtect Event Server** Dienst als Ressource zum **Milestone XProtect Management Server Cluster** Dienst hinzuzufügen.




12. Wiederholen Sie Schritt 11 und fügen Sie alle erforderlichen Dienste im Cluster hinzu, z. B. Log Server. Milestone XProtect Event Server und Data Collector server sollten beide als Dienste hinzugefügt werden, um eine optimale Bereitstellung zu erreichen. Des Weiteren sollte Milestone XProtect Event Server als abhängiger Dienst des Management-Servers eingestellt werden, so dass der Event Server mit stoppt, wenn der Management-Server stoppt.

13. Alle hinzugefügten Dienste werden im unteren Bereich des Fensters angezeigt.


**Aktualisierung der Cluster-URL:**

Wenn Sie Konfigurationsänderungen vornehmen, halten Sie auf dem Microsoft Failover Cluster Manager die Steuerung und Überwachung des Dienstes an, damit der Server Configurator die Änderungen vornehmen kann, und starten bzw. stoppen Sie den Management Server Dienst. Wenn Sie den Startyp des Failover Cluster Service auf "Manuell" ändern, sollte dies nicht zu Konflikten mit dem Server Configurator führen.

Auf den Management Server Computern:

1. Starten Sie den Server Configurator auf jedem der Computer, auf denen ein Managementserver installiert ist.
2. Gehen Sie auf die Seite **Registrierung**.
3. Klicken Sie auf das Bleistiftsymbol (), damit Sie die Adresse des Management Servers bearbeiten können.
4. Ändern Sie die Adresse des Managements Servers in die URL des Clusters, z.B. `http://MyCluster`.
5. Klicken Sie auf **Registrieren**.

Auf Computern mit Komponenten, die den Management Server verwenden (z.B. Recording Server, Mobile Server, Event Server, , API Gateway):

1. Starten Sie den Server Configurator auf jedem der Computer.
2. Gehen Sie auf die Seite **Registrierung**.
3. Ändern Sie die Adresse des Managements Servers in die URL des Clusters, z.B. `http://MyCluster`.
4. Klicken Sie auf **Registrieren**.

## Verwenden Sie ein Zertifikat für einen externen IDP in einer Cluster-Umgebung

Bei der Installation von XProtect in einer Einzelserver-Umgebung werden die Konfigurationsdaten des externen IDP mithilfe der Data Protection API (DPAPI) geschützt. Wenn Sie den Management Server in einem Cluster einrichten, müssen die Konfigurationsdaten des externen IDP mit einem Zertifikat geschützt werden, damit ein reibungsloses Knoten-Failover gewährleistet ist.

Weitere Informationen dazu, wie ein Zertifikat erstellt wird, finden Sie unter Der Milestone Leitfaden zur Zertifizierung.

Sie müssen das Zertifikat in den persönlichen Zertifikatspeicher importieren und das Zertifikat auf dem Computer als vertrauenswürdig einstufen.

Um den Datenschutz einzurichten, müssen Sie den Daumenabdruck des Zertifikats in die Identity Provider Konfiguration aufnehmen.

1. Importieren Sie das Zertifikat in den persönlichen Zertifikatspeicher, und achten Sie darauf, dass:
   - das Zertifikat gültig ist
   - das Identity Provider app pool (IDP) Konto über Berechtigungen für den privaten Schlüssel des Zertifikats verfügt.

   Weitere Informationen darüber, wie Sie überprüfen können, ob das Konto über Berechtigungen für den privaten Schlüssel des Zertifikats verfügt, finden Sie unter Der Milestone Leitfaden zur Zertifizierung.
2. Suchen Sie die Datei `appsettings.json` im Installationspfad des Identity Provider (`[Installationspfad]\Milestone\XProtect Management Server\IIS\Identity Provider`).
3. Legen Sie den Daumenabdruck des Zertifikats fest im Abschnitt:

   ```
   "DataProtectionSettings": {
    "ProtectKeysWithCertificate": {
     "Thumbprint": ""
    }

   },
   ```
4. Wiederholen Sie den 3. Schritt auf allen Management-Server-Knoten.
5. Erzwingen Sie einen Knoten-Failover, damit die Einrichtung der Zertifikate korrekt erfolgt.
6. Melden Sie sich erneut über den Management-Client an und wenden Sie die Konfiguration des externen Anbieters an. Wenn die Konfiguration bereits angewendet wurde, müssen Sie das Client-Geheimnis vom externen IDP erneut in den Management-Client eingeben.

### Fehlerbehebung, wenn eine externe IDP-Konfiguration mit einem Zertifikat geschützt ist

**Ungültiges Zertifikat/abgelaufenes Zertifikat**

Wenn das konfigurierte Thumbprint-Zertifikat ein nicht vertrauenswürdiges oder abgelaufenes Zertifikat darstellt, kann der Identity Provider nicht starten. Im Protokoll Identity Provider (`C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`) wird klar angegeben, ob das Zertifikat ungültig ist.

**Lösung:**

Achten Sie darauf, dass das Zertifikat auf dem Computer gültig ist und dass ihm vertraut wird.

**Fehlende Berechtigungen für private Schlüssel von Zertifikaten**

Der Identity Provider kann die Daten ohne Zugriffsrechte auf die privaten Schlüssel nicht schützen. Wenn der Identity Provider nicht die Berechtigung hat, wird die folgende Fehlermeldung in die Protokolldatei des Identity Provider (`C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`) geschrieben:

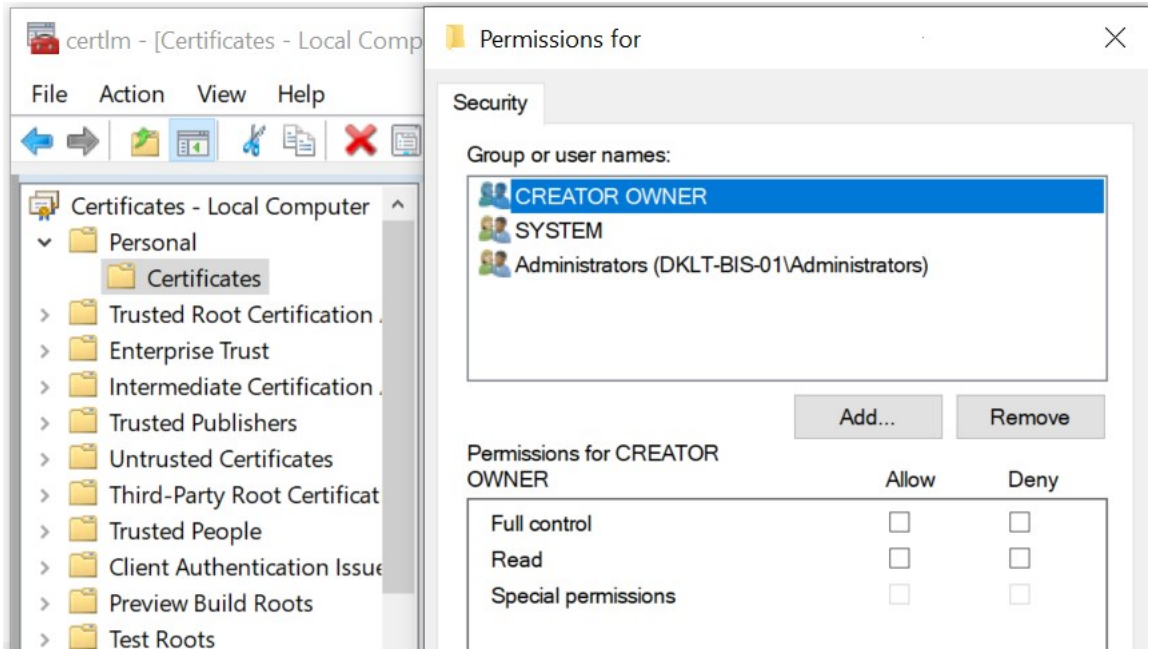
```
ERROR- An exception occurred while processing the key element '<key id="
[installation specific]" version="1" />'.
Internal.Cryptography.CryptoThrowHelper+WindowsCryptographicException:
Keyset does not exist
```

**Lösung:**

Vergewissern Sie sich, dass das Identity Provider app pool (IDP)-Konto über Berechtigungen für die privaten Schlüssel des Zertifikats verfügt.

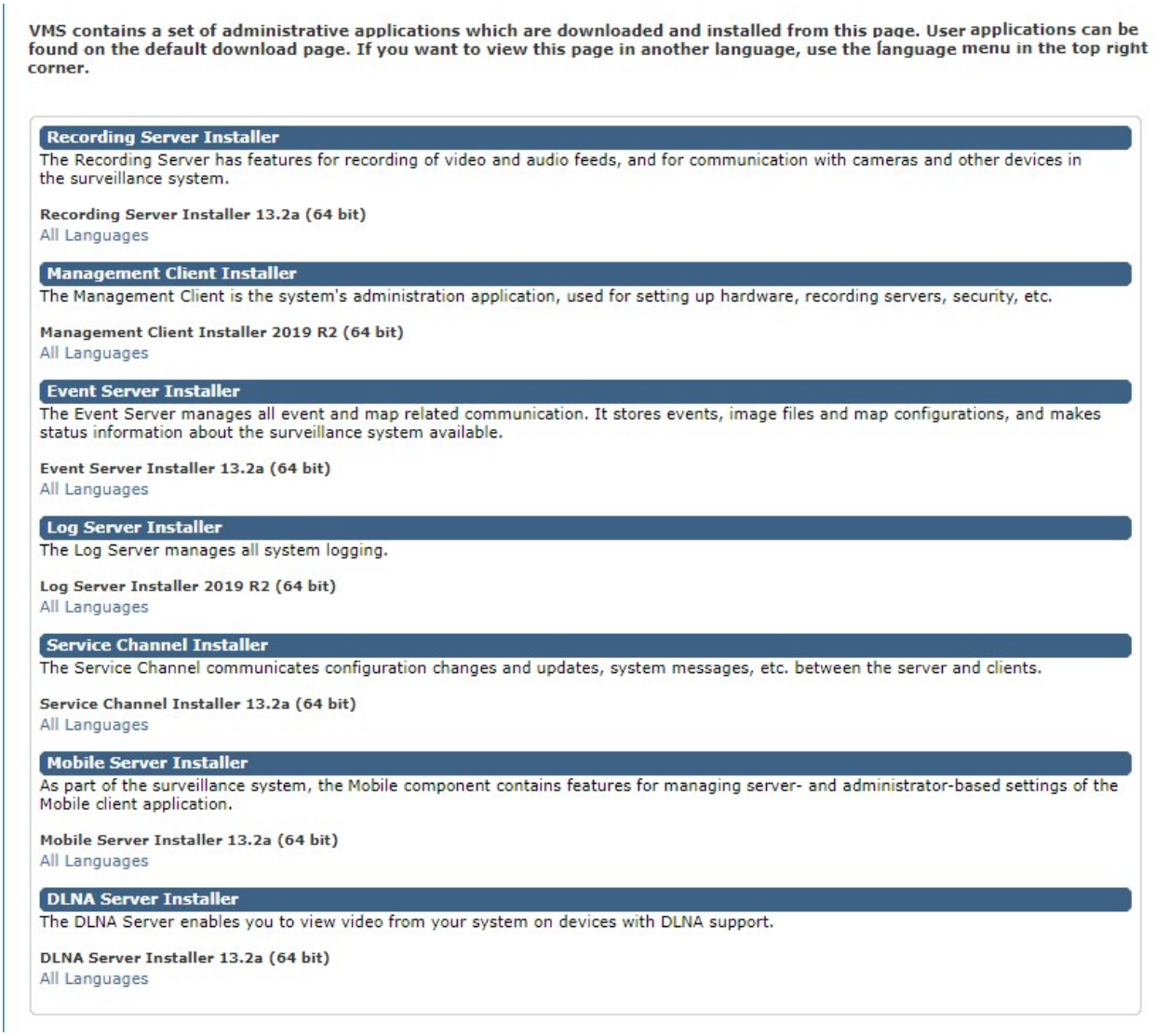
**Prüfen Sie die Berechtigungen für einen privaten Schlüssel eines Zertifikats:**

1. Wählen Sie **Start** in der Windows-Taskleiste und öffnen Sie das Tool "Computerzertifikate verwalten" (certlm.msc).
2. Navigieren Sie zum persönlichen Zertifikatspeicher und suchen Sie das Zertifikat, das für die Verschlüsselung verwendet wird.
3. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **Alle Aufgaben** > **Private Schlüssel verwalten**.
4. Vergewissern Sie sich unter **Berechtigungen**, dass das Identity Provider app pool (IDP)-Konto über Leseberechtigungen verfügt.




## Download Manager/Download-Webseite

Der Management-Server verfügt über eine integrierte Webseite. Über diese Webseite können Administratoren und Endbenutzer die benötigten XProtect-Systemkomponenten von einem beliebigen Speicherort – lokal oder remote – herunterladen und installieren.


VMS contains a set of administrative applications which are downloaded and installed from this page. User applications can be found on the default download page. If you want to view this page in another language, use the language menu in the top right corner.

**Recording Server Installer**
The Recording Server has features for recording of video and audio feeds, and for communication with cameras and other devices in the surveillance system.

**Recording Server Installer 13.2a (64 bit)**
All Languages

**Management Client Installer**
The Management Client is the system's administration application, used for setting up hardware, recording servers, security, etc.

**Management Client Installer 2019 R2 (64 bit)**
All Languages

**Event Server Installer**
The Event Server manages all event and map related communication. It stores events, image files and map configurations, and makes status information about the surveillance system available.

**Event Server Installer 13.2a (64 bit)**
All Languages

**Log Server Installer**
The Log Server manages all system logging.

**Log Server Installer 2019 R2 (64 bit)**
All Languages

**Service Channel Installer**
The Service Channel communicates configuration changes and updates, system messages, etc. between the server and clients.

**Service Channel Installer 13.2a (64 bit)**
All Languages

**Mobile Server Installer**
As part of the surveillance system, the Mobile component contains features for managing server- and administrator-based settings of the Mobile client application.

**Mobile Server Installer 13.2a (64 bit)**
All Languages

**DLNA Server Installer**
The DLNA Server enables you to view video from your system on devices with DLNA support.

**DLNA Server Installer 13.2a (64 bit)**
All Languages

Die Webseite kann zwei Gruppen von Inhalt anzeigen und zwar standardmäßig in der Sprache, die der Sprache der Systeminstallation entspricht:

- Eine Webseite richtet sich an **Administratoren**, die so wichtige Systemkomponenten herunterladen und installieren können. In den meisten Fällen wird die Webseite am Ende der Management-Server-Installation automatisch geladen. Sie zeigt den Standardinhalt an. Auf dem Management-Server (Sie können über das Windows **Start**-Menü auf die Webseite zugreifen) wählen Sie **Programme** > **Milestone** > **Administrative Installationsseite** aus. Andernfalls können Sie die URL eingeben:

  *http://[Management-Server-Adresse]:[Port]/installation/admin/*

  [Management-Server-Adresse] ist die IP-Adresse oder der Hostname des Management-Servers und [Port] ist die Portnummer, auf deren Nutzung das IIS auf dem Management-Server konfiguriert ist.

- Eine Webseite richtet sich an die **Endbenutzer**, um ihnen den Zugriff auf Client-Anwendungen per Standardkonfiguration zu ermöglichen. Auf dem Management-Server (Sie können über das Windows **Start**-Menü auf die Webseite zugreifen) wählen Sie **Programme** > **Milestone** > **Öffentliche Installationsseite** aus. Andernfalls können Sie die URL eingeben:

  *http://[Management-Server-Adresse]:[Port]/installation/*

  [Management-Server-Adresse] ist die IP-Adresse oder der Hostname des Management-Servers und [Port] ist die Portnummer, auf deren Nutzung das IIS auf dem Management-Server konfiguriert ist.

Die zwei Webseiten haben einige standardmäßige Inhalte, also können Sie sie sofort nach der Installation nutzen. Als Administrator können Sie jedoch mit dem Download Manager anpassen, was auf den Webseiten angezeigt werden soll. Sie können auch Komponenten zwischen den beiden Versionen der Webseite verschieben. Zum Verschieben einer Komponente klicken Sie mit der rechten Maustaste darauf. Dann wählen Sie die Webseiten-Version aus, in die Sie die Komponente verschieben wollen.

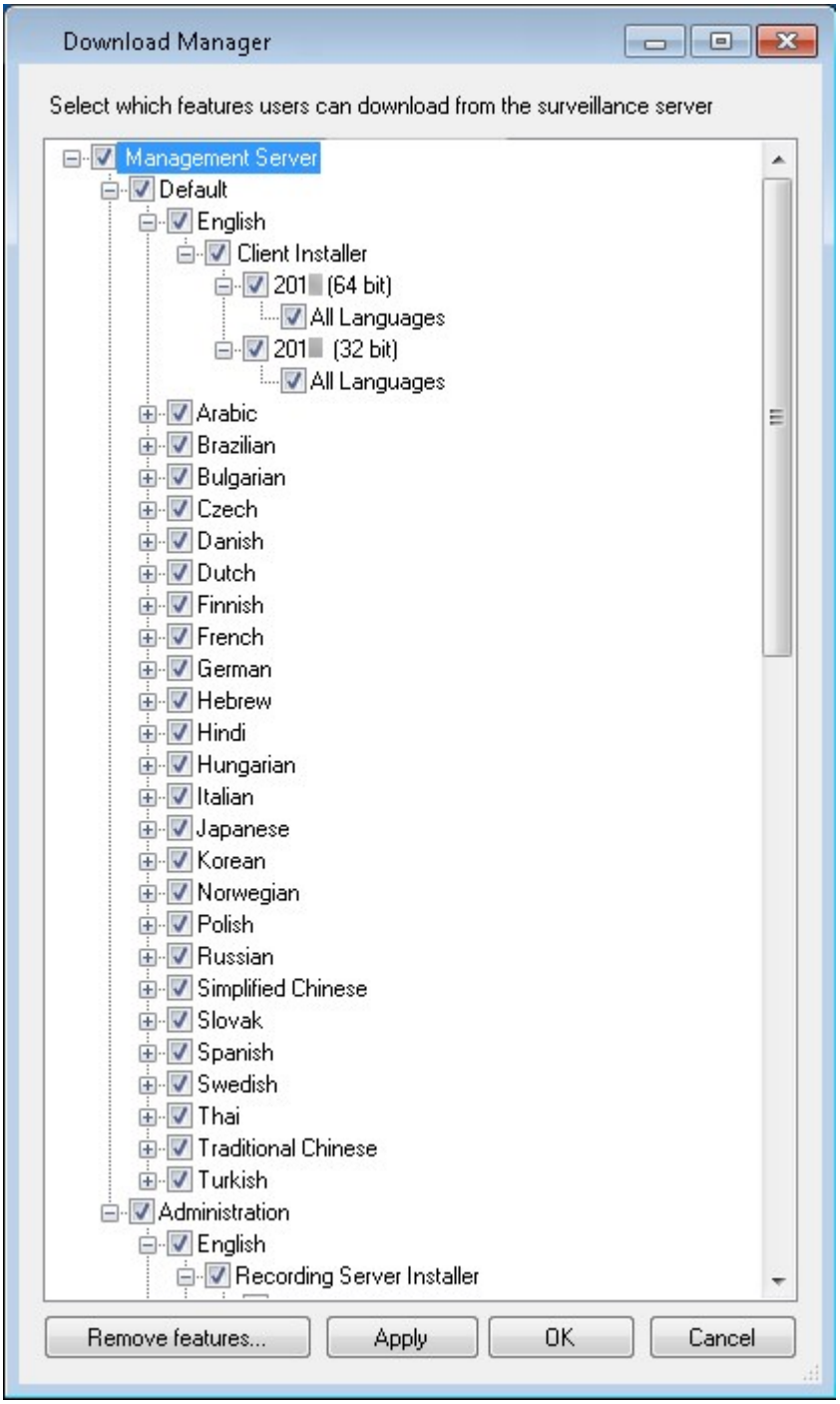
Obwohl Sie kontrollieren können, welche Komponenten Benutzer herunterladen und in Download Manager installieren können, können Sie es nicht als Hilfsmittel zur Benutzerrechteverwaltung verwenden. Solche Berechtigungen werden durch Rollen bestimmt, die in der Management Client festgelegt werden.

Auf dem Management-Server (Sie können XProtect Download Manager über das Windows **Start**-Menü auf die Webseite zugreifen) wählen Sie **Programme** > **Milestone** > **XProtect Download Manager** aus.

## Download Manager Standardkonfiguration

Das Download Manager besitzt eine Standardkonfiguration. Dies gewährleistet, dass die Benutzer Ihres Unternehmens von Beginn an auf die Standardkomponenten zugreifen können.

Die Standardkonfiguration besitzt ein Standard-Setup mit der Möglichkeit, zusätzliche oder optionale Komponenten herunterzuladen. Üblicherweise erreichen Sie die Webseite vom Computer des Management-Servers, Sie können jedoch auch von anderen Computern auf sie zugreifen.




- Die erste Ebene: Bezieht sich auf Ihr XProtect Produkt
- Die zweite Ebene: Bezieht sich auf die zwei Versionen der Webseite. **Standard** bezieht sich auf die Webseitenversion, die von den Endbenutzern gesehen wird. **Administration** bezieht sich auf die Webseitenversion, die von den Systemadministratoren gesehen wird
- Die dritte Ebene: Bezieht sich auf die Sprachen, in der die Webseite verfügbar ist

- Die vierte Ebene: Bezieht sich auf die Komponenten, die den Benutzern bereitgestellt sind oder werden können
- Die fünfte Ebene: Bezieht sich auf bestimmte Versionen jeder Komponente, die den Benutzern bereitgestellt sind oder werden können
- Die sechste Ebene: Bezieht sich auf die Sprachversionen der Komponenten, die den Benutzern bereitgestellt sind oder werden können

Die Tatsache, dass anfänglich nur Standardkomponenten verfügbar sind und nur in derselben Sprachversion wie das System an sich, hilft die Installationszeit zu verringern und auf dem Server Platz zu sparen. Es besteht keine Notwendigkeit für eine Komponente oder eine Sprachversion auf dem Server, wenn sie von niemandem verwendet wird.

Falls erforderlich, können Sie weitere Komponenten oder Sprachen hinzufügen und ungewollte Sprachen oder Komponenten verbergen oder entfernen.

## Download Manager Standardinstallationsprogramme (Benutzer)

Standardmäßig stehen die folgenden Komponenten für eine separate Installation auf der Download-Webseite des Management-Servers, die sich an Endbenutzer richtet, zur Verfügung (gesteuert vom Download Manager):

- Aufzeichnungsserver, einschließlich Failover-Aufzeichnungsservern. Failover-Aufzeichnungsserver werden zunächst als Aufzeichnungsserver heruntergeladen und installiert. Während der Installation legen Sie dann fest, dass Sie einen Failover-Aufzeichnungsserver benötigen.
- Management Client
- XProtect Smart Client
- Event Server, wird in Verbindung mit der Kartenfunktionalität verwendet
- Log-Server, wird zur Bereitstellung der zum Protokollieren der Systemdaten erforderlichen Funktionalität verwendet
- XProtect Mobile-Server
- Innerhalb Ihrer Organisation sind möglicherweise weitere Optionen verfügbar.

Zur Installation von Device Packs siehe Installationsprogramm für Treiberpaket - muss heruntergeladen werden auf Seite 204.

## Hinzufügen/Veröffentlichen von Komponenten des Download Manager-Installationsprogramms

Sie müssen zwei Verfahrensschritte abschließen, um Nicht-Standard-Komponenten und neue Versionen auf der Download-Seite des Management-Servers verfügbar zu machen.

Als Erstes müssen Sie neue und/oder Nicht-Standard-Komponenten zum Download Manager hinzufügen. Dann nutzen Sie ihn zum Abgleich, welche Komponenten in den jeweiligen Sprachversionen der Webseite verfügbar sein sollen.

Falls der Download Manager geöffnet ist, schließen Sie ihn vor der Installation neuer Komponenten.

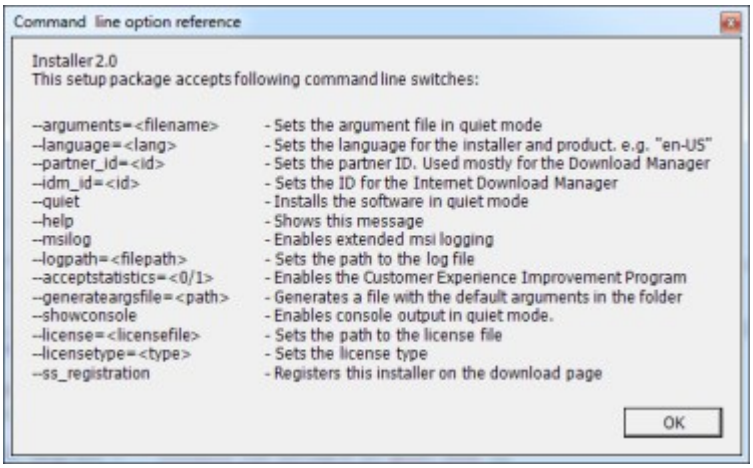
**Hinzufügen neuer Dateien bzw. Nicht-Standard-Dateien zum Download Manager:**

1. Gehen Sie auf dem Computer, auf den Sie die Komponente(n) heruntergeladen haben, zum Windows-**Startmenü** und öffnen Sie die *Eingabeaufforderung*
2. Geben Sie in der *Eingabeaufforderung* den Namen der Datei (*.exe*) mit dem Zusatz [space]*--ss_registration* ein und führen Sie den Befehl aus

   Beispiel: *MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

   Die Datei wird nun zum Download Manager hinzugefügt, aber nicht auf dem aktuellen Computer installiert.

Wenn Sie eine Übersicht über die Befehle des Installationsprogramms benötigen, geben Sie in der *Eingabeaufforderung* [Leertaste]*--help* ein. Dann wird das folgende Fenster angezeigt:



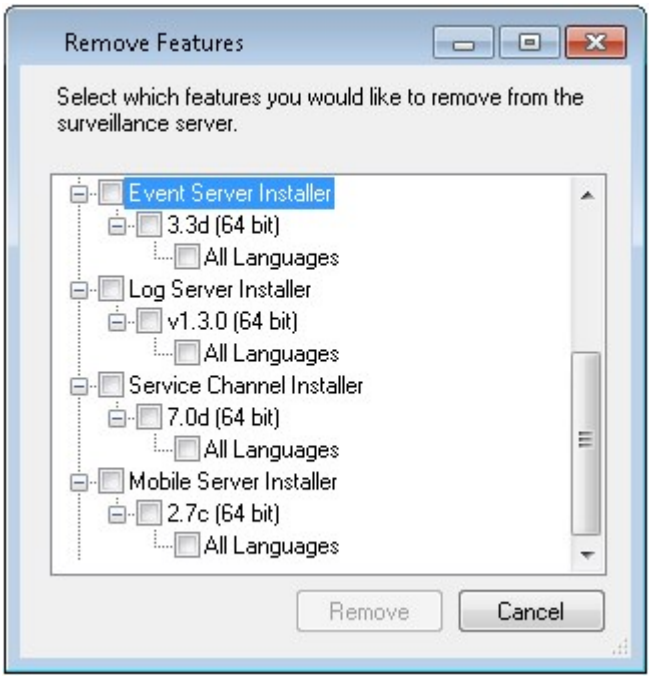

Wenn Sie neue Komponenten installiert haben, werden sie standardmäßig im Download Manager ausgewählt. Sie sind sofort über die Webseite für die Benutzer zugänglich. Sie können die Funktionen auf der Webseite stets ein- oder ausblenden. Dazu markieren Sie die Kontrollkästchen in der Baumstruktur des Download Managers bzw. Sie heben deren Auswahl auf.

Sie können die Abfolge ändern, in der die Komponenten auf der Webseite angezeigt werden. Ziehen Sie die Komponentenelemente in der Baumstruktur des Download Managers einfach per Drag & Drop in die gewünschte Position.

## Ausblenden/Entfernen der Download Manager Installationsprogrammkomponenten

Sie haben drei Möglichkeiten:

- **Komponenten** auf der Webseite ausblenden. Dazu heben Sie die Auswahl der Kontrollkästchen in der Baumstruktur des Download Managers auf. Die Komponenten auf dem Management-Server installiert und durch die Markierung der Kontrollkästchen in der Baumstruktur des Download Managers können Sie die Komponenten schnell wieder zugänglich machen
- **Verschieben Sie die Installation der Komponenten** auf den Management-Server. Die Komponenten werden vom Download Manager entfernt, aber die Installationsdateien für die Komponenten sind in `C:\Program Files (x86)\Milestone\XProtect Download Manager` verfügbar, sodass Sie diese bei Bedarf später neu installieren können
    1. Im Download Manager, klicken Sie auf **Funktionen entfernen**.
    2. Wählen Sie im Fenster **Funktionen entfernen** die Funktion(en), die Sie entfernen wollen.




    3. Klicken Sie auf **OK** und dann auf **Ja**.
- **Installationsdateien für nicht benötigte Funktionen** vom Management-Server entfernen. Dadurch können Sie Speicherplatz auf dem Server sparen, wenn Sie wissen, dass Ihre Organisation bestimmte Funktionen nicht verwenden wird

## Installationsprogramm für Treiberpaket - muss heruntergeladen werden

Das Treiberpaket (enthält Gerätetreiber), das in Ihrer ursprünglichen Installation beinhaltet ist, ist nicht in Download Manager enthalten. Wenn Sie das Treiberpaket neu installieren müssen oder das Installationsprogramm des Treiberpakets verfügbar machen möchten, müssen Sie zuerst die aktuellste Version zum Download Manager hinzufügen oder veröffentlichen:

1. Das aktuelle reguläre Treiberpaket erhalten Sie auf der Download-Seite auf der Website Milestone (https://www.milestonesys.com/downloads/).
2. Auf der gleichen Seite können Sie auch das Stammtreiberpaket mit älteren Treibern herunterladen. Besuchen Sie die fogende Website, um zu prüfen, ob Ihre Kameras Treiber aus dem Legacy-Treiberpaket verwenden: (https://www.milestonesys.com/community/business-partner-tools/device-packs/).
3. Veröffentlichen/Fügen Sie es zum Download Manager hinzu, indem Sie den *--ss_registration*-Befehl verwenden.

Wenn Sie keine Verbindung zum Netzwerk haben, können Sie den gesamten Aufzeichnungsserver vom Download Manager aus erneut installieren. Die Installationsdateien für den Aufzeichnungsserver sind lokal auf Ihrem Computer gespeichert, wodurch Sie automatisch eine erneute Installation des Treiberpakets vornehmen können.

## Installationsprotokolldateien und Fehlersuche

Während einer Installation, eines Upgrades oder einer Deinstallation werden Protokolleinträge in verschiedenen Installationsprotokolldateien vorgenommen: Zur Hauptprotokolldatei für die Installation `installer.log` und zu den Protokolldateien zu den verschiedenen Systemkomponenten, die Sie installieren. Alle Protokolleinträge haben Zeitstempel, und die neuesten Protokolleinträge befinden sich am Ende der Protokolldateien.

`Sie` können alle Installationsprotokolldateien in dem Verzeichnis `C:\ProgramData\Milestone\Installer\` finden. Protokolldateien mit Bezeichnungen wie *I.log oder *I[integer].log sind Protokolldateien zu neuen Installationen oder Upgrades, deren Protokolldateien mit Bezeichnungen wie *U.log oder *U[integer].log Deinstallationen betreffen. Wenn Sie einen Server mit bereits installiertem XProtect-System von einem Milestone-Partner erworben haben, sind vielleicht keine Installationsprotokolldateien vorhanden.

Die Protokolldateien enthalten Informationen zu den Befehlszeilenparametern und Befehlszeilenoptionen und deren Werten, die während einer Installation, für ein Upgrade oder zur Deinstallation verwendet wurden. Um die Befehlszeilenparameter in den Protokolldateien zu finden, suchen Sie nach **Command Line:** oder **Parameter '**, je nach der Protokolldateien.

Für die Fehlersuche ist die Protokolldatei für die Hauptinstallation installer.log die erste Anlaufstelle. Wenn es während der Installation zu Ausnahmen, Fehlern oder Warnungen bekommen ist, wurden diese protokolliert. Probieren Sie eine Suche nach **exception**, **error** oder **warning**. "Exitcode: 0" bedeutet eine erfolgreiche Installation, und "Exitcode: 1" das Gegenteil. Anhand Ihrer Erkenntnisse aus den Protokolldateien finden Sie evtl. eine Lösung in der Milestone Knowledge Base. Wenn nicht, wenden Sie sich an Ihren Milestone-Partner, und stellen Sie ihm die entsprechenden Installationsprotokolldateien zur Verfügung.

# Konfiguration

## Aufgabenliste für die Erstkonfiguration

Die folgende Checkliste enthält die ersten Aufgaben zur Konfiguration Ihres Systems. Einige davon haben Sie möglicherweise bereits während der Installation abgeschlossen.

Eine ausgefüllte Prüfliste an sich garantiert nicht, dass das System den genauen Anforderungen Ihrer Organisation entspricht. Damit das System mit den Anforderungen Ihrer Organisation übereinstimmt, empfiehlt Milestone, dass Sie das System kontinuierlich überwachen und anpassen.

Beispielsweise ist es ratsam, die Empfindlichkeitseinstellungen für die Bewegungserkennung durch einzelne Kameras unter unterschiedlichen, physischen Bedingungen zu testen, wenn das System ausgeführt wird, einschließlich von Tag/Nacht und bei windigem/ruhigem Wetter.

Das Einrichten der Regeln, die die meisten Aktionen festlegen, die Ihr System ausführt, einschließlich des Zeitpunkts der Aufzeichnung eines Videos, ist ein weiteres Beispiel für eine Konfiguration, die Sie gemäß den Anforderungen Ihrer Organisation ändern können.

| Schritt | Beschreibung |
|---|---|
| ☑ | Sie haben die erste Installation Ihres Systems fertig gestellt.<br>Siehe Installation eines neuen XProtect-Systems auf Seite 156. |
| ☑ | Ändern Sie den SLC in einen permanenten SLC (bei Bedarf).<br>Siehe Softwarelizenzcode ändern auf Seite 132. |
| ☑ | Melden Sie sich bei Management Client an.<br>Siehe Anmeldung (Erklärung) auf Seite 30. |
| ☐ | Prüfen Sie, ob die Speichereinstellungen jedes Aufzeichnungsservers Ihren Einstellungen entsprechen.<br>Siehe Lagerung und Archivierung (Erklärung) auf Seite 59. |
| ☐ | Prüfen Sie, ob die Archivierungseinstellungen jedes Aufzeichnungsservers Ihren Einstellungen entsprechen.<br>Siehe Speicher- und Aufzeichnungseinstellungen (Eigenschaften) auf Seite 449. |

| Schritt | Beschreibung |
|---|---|
| ☐ | Erkennt die Hardware, Kameras oder Video-Encoder, die jedem Aufzeichnungsserver hinzugefügt werden.<br>Siehe Hardware hinzufügen auf Seite 229. |
| ☐ | Konfigurieren Sie die einzelnen Kameras jedes Aufzeichnungsservers.<br>Siehe Kameras (Geräteknoten) auf Seite 469. |
| ☐ | Aktivieren Sie die Speicherung und Archivierung für einzelne Kameras oder für eine Gruppe von Kameras. Dies erfolgt über einzelne Kameras oder über die Gerätegruppe.<br>Siehe Anbinden eines Geräts oder eine Gruppe von Geräten an einen Speicher auf Seite 213. |
| ☐ | Geräte aktivieren und konfigurieren.<br>Siehe Geräte (Geräteknoten) auf Seite 466. |
| ☐ | Das Verhalten des Systems wird in großem Umfang von Regeln festgelegt. In den zu erstellenden Regeln ist festgelegt, wann die Kameras aufzeichnen sollen, wann Pan-Tilt-Zoom-Kameras (PTZ) aufzeichnen und wann Benachrichtigungen verschickt werden sollen.<br>Regeln erstellen.<br>Siehe Regeln und Ereignisse (Erklärung) auf Seite 82. |
| ☐ | Rollen zum System hinzufügen.<br>Siehe Rollen und Berechtigungen einer Rolle (Erklärung) auf Seite 71. |
| ☐ | Fügen Sie zu jeder der Rollen Benutzer oder Gruppen von Benutzern hinzu.<br>Siehe Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen auf Seite 309. |
| ☐ | Lizenzen aktivieren.<br>Siehe Lizenzen online aktivieren auf Seite 130 oder Lizenzen offline aktivieren auf Seite 131. |

Weitere Informationen dazu, wie das System in dem Fenster **Seitennavigation** konfiguriert wird siehe Der Bereich Site-Navigation auf Seite 411.

# Aufzeichnungsserver

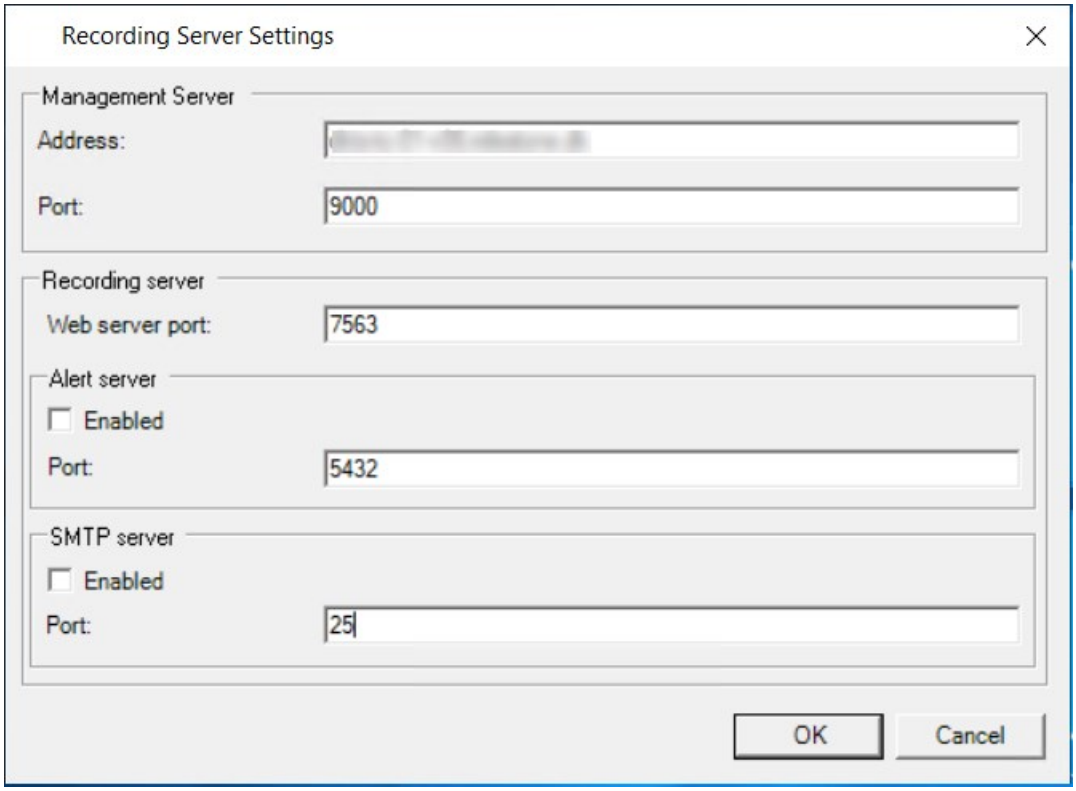
## Ändern oder überprüfen Sie die Basiskonfiguration eines Aufzeichnungsservers

Wenn Management Client nicht alle installierten Aufzeichnungsserver auflistet, wurden wahrscheinlich die Einstellungsparameter (zum Beispiel: IP-Adresse oder Hostname des Management-Servers) während der Installation falsch konfiguriert.

Sie müssen die Aufzeichnungsserver nicht neu installieren, um die Parameter des Management-Servers festzulegen, aber Sie können seine Grundeinstellungen ändern/bestätigen:

1. Auf dem ausführendem Computer des Aufzeichnungsservers, klicken Sie mit der rechten Maustaste auf das **Aufzeichnungsserver**-Symbol im Benachrichtigungsbereich.
2. Wählen Sie **Recording Server Service stoppen** aus.
3. Klicken Sie nochmals auf das **Aufzeichnungsserver**-Symbol und wählen Sie **Einstellungen ändern**.

   Das Fenster **Aufzeichnungsserver-Einstellungen** wird angezeigt.



4. Überprüfen oder ändern Sie z.B. die folgenden Einstellungen:
    - **Management Server**: **Adresse**: Geben Sie die IP-Adresse oder den Hostnamen des Management Servers an, mit dem der Aufzeichnungsserver verbunden sein soll.
    - **Management Server**: **Port**: Geben Sie die bei der Kommunikation mit dem Management-Server zu verwendende Portnummer an. Sie können dies ggf. ändern, die Portnummer muss jedoch stets der Portnummer entsprechen, die auf dem Management Server eingerichtet wurde. Siehe Vom System verwendete Ports auf Seite 103.
    - **Aufzeichnungsserver**: **Web-Server-Port**: Geben Sie die bei der Kommunikation mit dem Aufzeichnungsserver zu verwendende Portnummer an. Siehe Vom System verwendete Ports auf Seite 103.
    - **Aufzeichnungsserver**: **Alarm-Server-Port**: Aktivieren Sie die Portnummer und geben Sie die bei der Kommunikation mit dem Alarm-Server des Aufzeichnungsservers zu verwendende Portnummer an, der auf Ereignismeldungen von Geräten wartet. Siehe Vom System verwendete Ports auf Seite 103.
    - **SMTP-Server**: **Port**: Aktivieren Sie die Portnummer und geben Sie die bei der Kommunikation mit dem Dienst Simple Mail Transfer Protocol (SMTP) des Aufzeichnungsservers zu verwendende Portnummer an. Siehe Vom System verwendete Ports auf Seite 103.
5. Klicken Sie auf **OK**.
6. Um den Recording Server-Dienst wieder zu starten, klicken Sie mit der rechten Maustaste auf das **Aufzeichnungsserver**-Symbol und wählen Sie **Recording Server Dienst** starten aus.

> ⚠ Ein Anhalten des Recording Server-Dienstes hat zur Folge, dass Sie kein Live-Video aufzeichnen oder anschauen können, während Sie die Grundeinstellungen des Aufzeichnungsservers bestätigen/ändern.

## Registrieren eines Aufzeichnungsservers

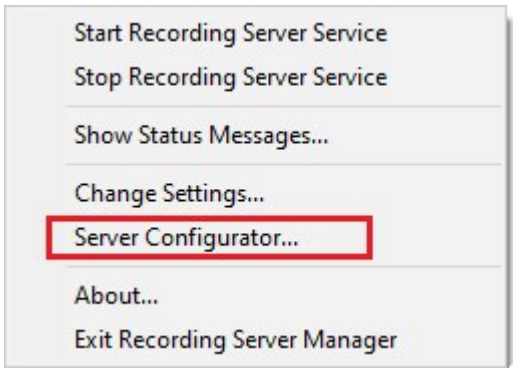
Bei der Installation eines Aufzeichnungsserver wird dieser meist automatisch registriert. Die Registrierung müssen Sie jedoch manuell vornehmen, wenn:

- Sie haben den Aufzeichnungsserver ersetzt
- Der Aufzeichnungsserver wurde offline installiert und hinterher zum Managementserver hinzugefügt
- Ihr Managementserver verwendet nicht die Standardports. Die Portnummern sind von der Konfiguration der Verschlüsselung abhängig. Weitere Informationen finden Sie unter Vom System verwendete Ports auf Seite 103

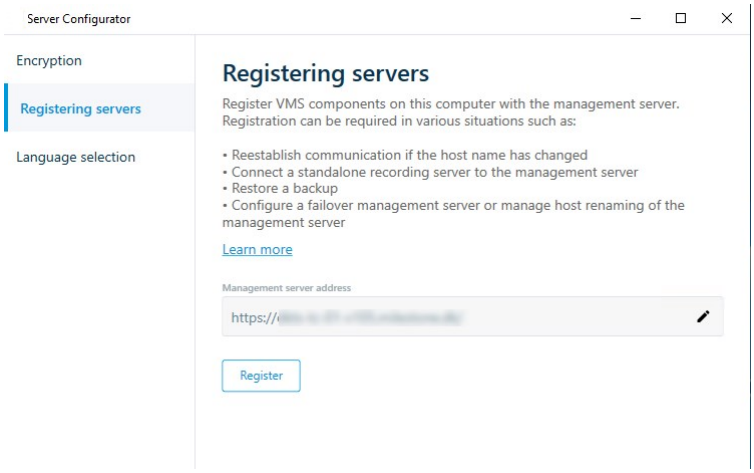
- Eine automatische Registrierung ist fehlgeschlagen, z.B. nach einer Änderung der Adresse des Managementservers, einer Umbenennung des Computers, auf dem der Aufzeichnungsserver läuft, oder nach Aktivierung oder Deaktivierung der Einstellungen für die Verschlüsselung der Serverkommunikation. Weitere Informationen zur Änderung der Adresse des Management Servers finden Sie unter Ändern des Hostnamens des Computers mit den Managementserver.

Bei der Registrierung eines Aufzeichnungsservers wird dieser für eine Verbindung mit Ihrem Management-Server konfiguriert. Der Teil des Managementservers, der sich um die Registrierung kümmert, ist der Dienst Authorization Server.

1. Öffnen Sie Server Configurator entweder vom Windows-Startmenü oder vom Taskleistensymbol für den Aufzeichnungsserver aus.




2. Wählen Sie unter Server Configurator **Serverregistrierung**.




3. Überprüfen Sie die Adresse des Managementservers sowie das Schema (http oder https), zu dem die Server auf dem Computer eine Verbindung herstellen sollen, und klicken Sie dann auf **Registrieren**.

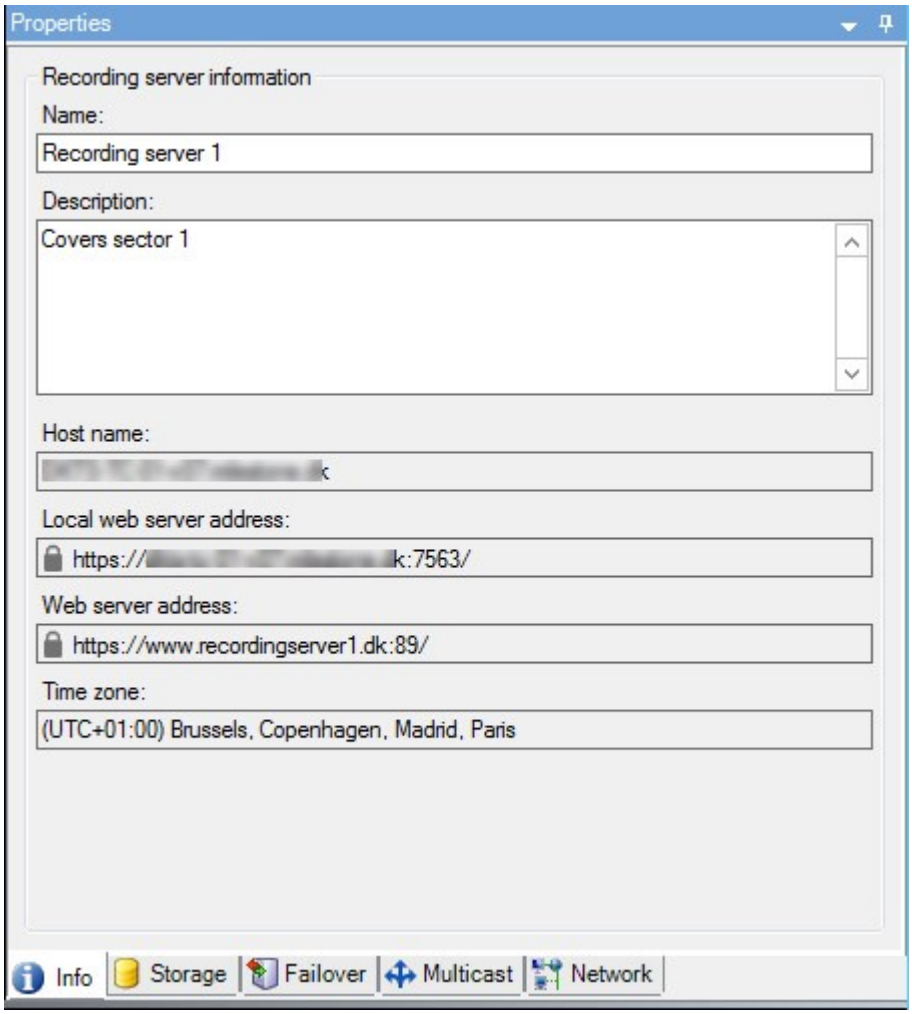
Dann erscheint eine Bestätigung, die besagt, dass die Registrierung auf dem Management Server erfolgreich war.

Siehe auch Ersetzen eines Aufzeichnungsservers auf Seite 367.

## Verschlüsselungsstatus an Clients anzeigen

Um zu überprüfen, ob Ihr Aufzeichnungsserver eine Verschlüsselung verwendet:

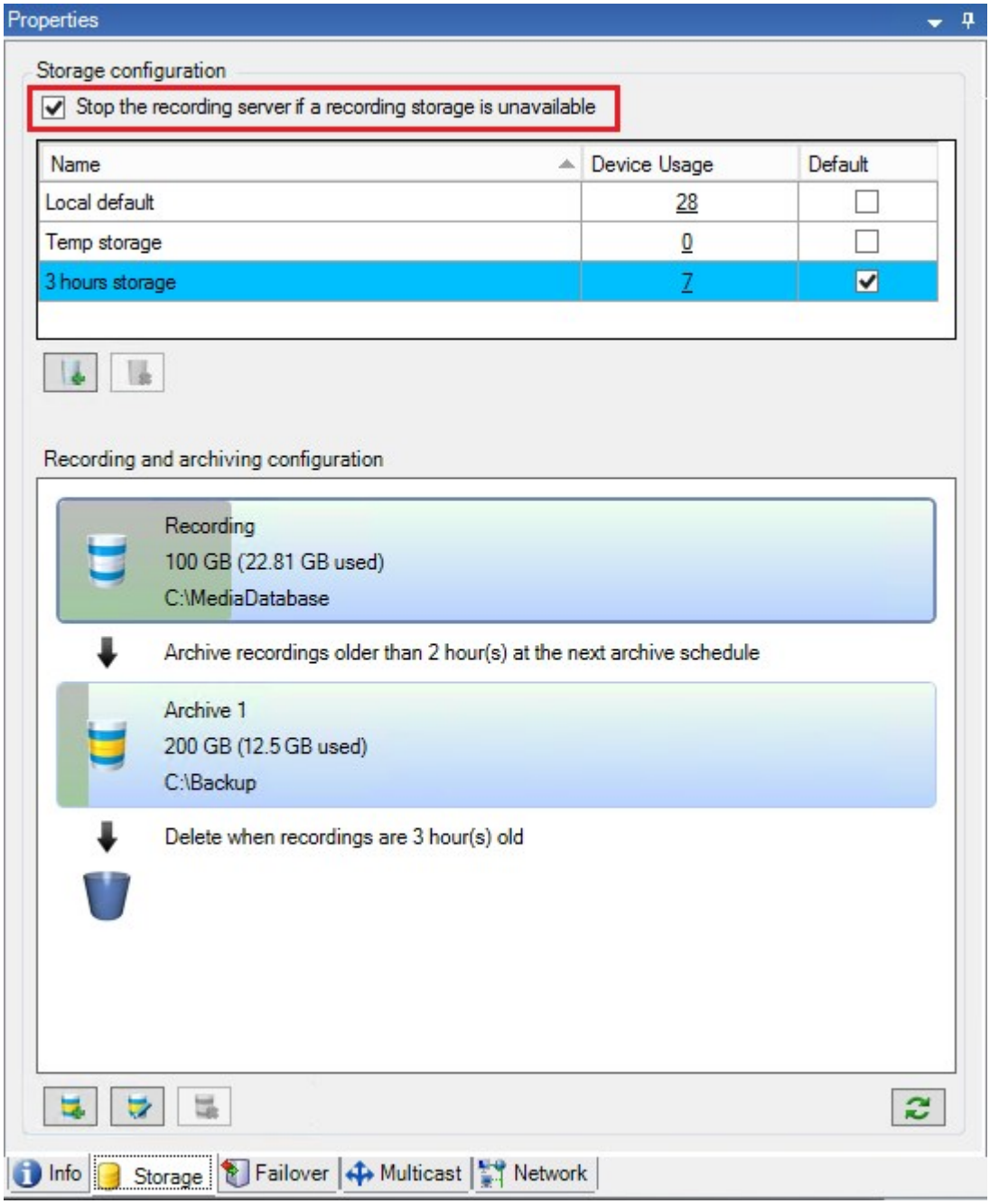
1. Öffnen Sie den Management Client.
2. Wählen Sie im Bereich **Standort-Navigation** die Optionen **Server** > **Aufzeichnungsserver**. Daraufhin wird eine Liste mit Aufzeichnungsservern geöffnet.
3. Wählen Sie in dem Fenster **Übersicht** den jeweiligen Aufzeichnungsserver aus und gehen Sie auf die Registerkarte **Info**.
   Wenn die Verschlüsselung zu Clients und Servern, die Datenstreams vom Aufzeichnungsserver abrufen, aktiviert ist, erscheint ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der des optionalen Webservers.




## Geben Sie an, wie das System sich verhalten soll, wenn kein Speicherplatz für Aufzeichnungen verfügbar ist

Der Aufzeichnungsserver läuft standardmäßig weiter auch wenn der Speicher für die Aufzeichnungen nicht mehr zur Verfügung steht. Wenn Ihr System mit ausfallsicheren Aufzeichnungsservern konfiguriert wurde, können Sie bestimmen, dass der Aufzeichnungsserver nicht mehr ausgeführt werden soll, damit die ausfallsicheren Server übernehmen:

1. Gehen Sie auf dem jeweiligen Aufzeichnungsserver auf die Registerkarte **Speicher**.
2. Wählen Sie die Option **Aufzeichnungsserver anhalten, wenn kein Speicherplatz für Aufzeichnungen zur Verfügung steht**.



## Einen neuen Speicher hinzufügen

Wenn Sie einen neuen Speicher hinzufügen, erstellen Sie stets einen Aufzeichnungsspeicher mit einer vordefinierten Aufzeichnungsdatenbank namens **Aufzeichnung**. Sie können die Datenbank nicht umbenennen. Neben der Aufzeichnungsdatenbank kann ein Speicher eine Reihe verschiedener Archive beinhalten.

1. Um einem ausgewählten Aufzeichnungsserver einen zusätzlichen Speicher hinzuzufügen, klicken Sie auf die Schaltfläche  unter der Liste **Speicherkonfiguration**. Das Dialogfeld **Speicher- und Aufzeichnungseinstellungen** wird angezeigt.
2. Geben Sie die entsprechenden Einstellungen an (siehe Speicher- und Aufzeichnungseinstellungen (Eigenschaften) auf Seite 449).
3. Klicken Sie auf **OK**.

Bei Bedarf können Sie in Ihrem neuen Speicher Archive erstellen.

## Erstellen eines Archivs in einem Speicher

Ein Speicher hat kein Standardarchiv; Sie können jedoch je nach Bedarf Archive erstellen.

1. Wählen Sie den gewünschten Speicher in der Liste **Aufzeichnungs- und Archivierungskonfiguration** aus.
2. Klicken Sie auf die Schaltfläche  unter der Liste **Aufzeichnungs- und Archivierungskonfiguration**.
3. Geben Sie im Dialogfeld **Archiveinstellungen** die erforderlichen Einstellungen an (siehe Eigenschaften der Archiveinstellungen auf Seite 451).
4. Klicken Sie auf **OK**.

## Anbinden eines Geräts oder eine Gruppe von Geräten an einen Speicher

Sobald ein Speicher für einen Aufzeichnungsserver konfiguriert wurde, können Sie ihn für einzelne Geräte wie Kameras, Mikrofone oder Lautsprecher bzw. eine Gruppe von Geräten aktivieren. Außerdem können Sie festlegen, welche Speicherbereiche eines Aufzeichnungsservers Sie für das bestimmte Gerät oder die Gruppe verwenden möchten.

1. Erweitern Sie **Geräte**, und wählen Sie je nach Bedarf **Kameras**, **Mikrofone** oder **Lautsprecher** aus.
2. Wählen Sie das Gerät oder eine Gerätegruppe aus.
3. Wählen Sie die Registerkarte **Aufzeichnung**.
4. Wählen Sie im Bereich **Speicher** die Option **Auswählen**.
5. Wählen Sie im angezeigten Dialogfeld die Datenbank aus, in der die Aufzeichnungen des Geräts gespeichert werden sollen, und klicken Sie auf **OK**.
6. Klicken Sie in der Symbolleiste auf **Speichern**.

Wenn Sie auf der Registerkarte „Speicher“ des Aufzeichnungsservers auf die Gerätenutzungszahl klicken, ist das Gerät im angezeigten Nachrichtenbericht sichtbar.

Geräte deaktiviert:

Deaktivierte Geräte werden standardmäßig nicht im Fenster **Übersicht** angezeigt.

Um alle deaktivierten Geräte anzuzeigen, klicken Sie oben im Fenster **Übersicht** auf **Filter** um die Registerkarte **Filter** zu öffnen, und wählen Sie **Deaktivierte Geräte anzeigen**.

Um deaktivierte Geräte wieder auszublenden, deaktivieren Sie die Option **Deaktivierte Geräte anzeigen**.

## Bearbeiten der Einstellungen für einen ausgewählten Speicher oder ein ausgewähltes Archiv

1. Wählen Sie zur Bearbeitung eines Speichers dessen Aufzeichnungsdatenbank in der Liste **Aufzeichnungs- und Archivierungskonfiguration** aus. Wählen Sie die Archivdatenbank aus, um ein Archiv zu bearbeiten.
2. Klicken Sie auf die Schaltfläche **Aufzeichnungsspeicher bearbeiten**  unter der Liste **Aufzeichnungs- und Archivierungskonfiguration**.
3. Bearbeiten Sie entweder eine Aufzeichnungsdatenbank oder ein Archiv.

Wenn Sie die maximale Größe einer Datenbank ändern, sorgt das System für eine automatische Archivierung aller Aufzeichnungen, die das neue Limit überschreiten. Je nach den Archivierungseinstellungen werden die Aufzeichnungen automatisch im nächsten Archiv archiviert bzw. gelöscht.

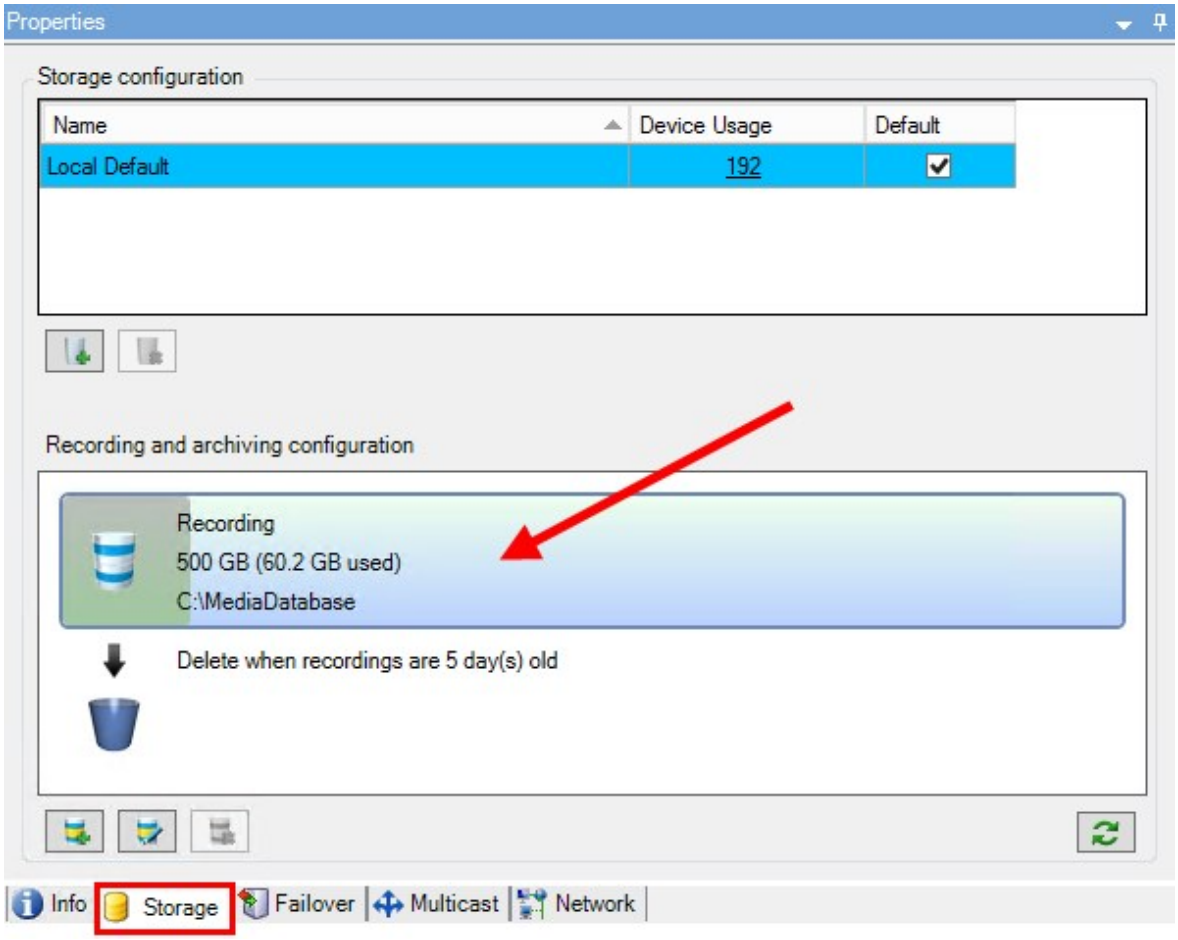
## Digitale Signaturen für Export aktivieren

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Sie können digitale Signatur für aufgezeichnete Videos aktivieren, sodass Client-Benutzer überprüfen können, dass das aufgezeichnete Video seit seiner Aufnahme nicht manipuliert wurde. Das Verifizieren der Echtzeit des Videos führt der Benutzer in XProtect Smart Client – Player durch, nachdem das Video exportiert wurde.

Das Signieren muss auch in XProtect Smart Client > auf der Registerkarte **Exporte** > **Exporteinstellungen** > **XProtect Format** > **Digitale Signatur einbeziehen** aktiviert werden. Anderenfalls wird die Schaltfläche **Signaturen verifizieren** in XProtect Smart Client – Player nicht angezeigt.

1. Erweitern Sie im Bereich **Standort-Navigation** den Knoten **Server**.
2. Klicken Sie auf **Aufzeichnungsserver**.
3. Klicken Sie im Übersichtsfenster auf den Aufzeichnungsserver, für den Sie die Signatur aktivieren möchten.
4. Klicken Sie unten im Bereich **Eigenschaften** auf die Registerkarte **Speicher**.




5. Doppelklicken Sie im Bereich **Aufzeichnungs- und Archivierungskonfiguration** auf den horizontalen Balken, der die Aufzeichnungsdatenbank repräsentiert. Das Fenster **Speicher- und Aufzeichnungseinstellungen** wird geöffnet.
6. Aktivieren Sie das Kontrollkästchen **Signatur**.
7. Klicken Sie auf **OK**.

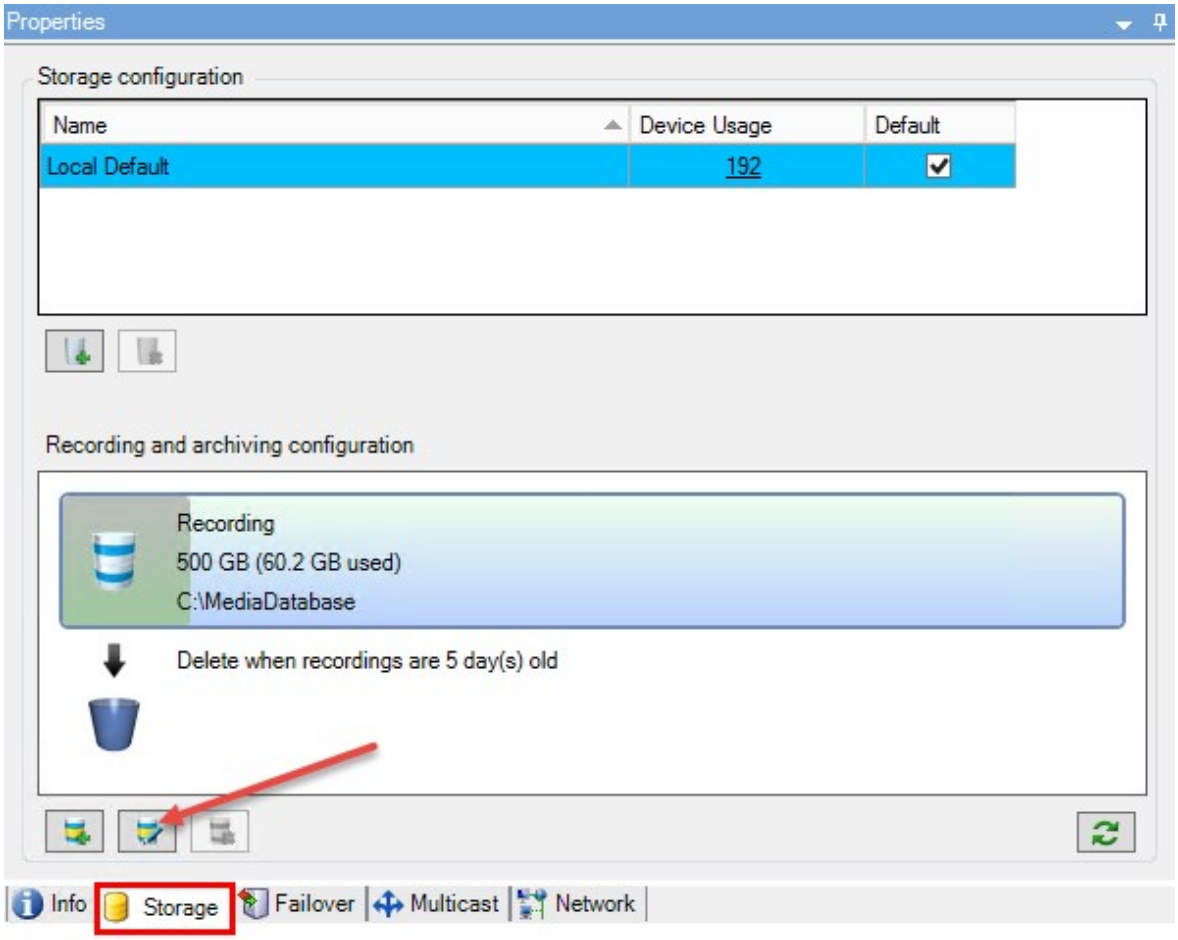
## Verschlüsseln Sie Ihre Aufzeichnungen

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

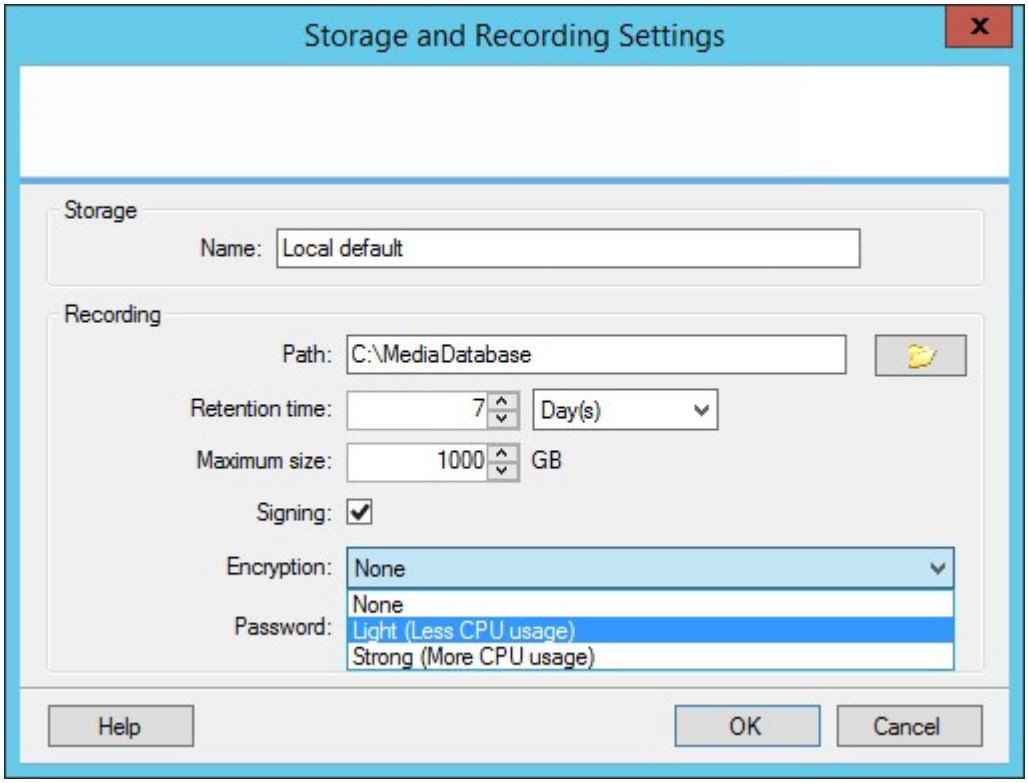
Sie können Ihre Aufzeichnungen sichern, indem Sie im Speicher und in den Archiven Ihres Aufzeichnungsservers die Verschlüsselung aktivieren. Sie können zwischen leichter und starker Verschlüsselung wählen. Wenn Sie die Verschlüsselung aktivieren, müssen Sie auch ein Passwort angeben.

Die Aktivierung oder Änderung von Verschlüsselungseinstellungen oder Passwort kann zeitraubend sein, abhängig von der Größe der Datenbank und der Leistungsfähigkeit des Laufwerks. Sie können die Fortschritte unter **Laufende Aufgaben** verfolgen. **Stoppen Sie** den Aufzeichnungsserver nicht, während diese Aufgabe läuft.

1. Klicken Sie auf die Schaltfläche **Aufzeichnungsspeicher bearbeiten** unter der Liste **Konfiguration der Aufzeichnung und Archivierung**.



2. Geben Sie in dem eingeblendeten Dialogfeld das Verschlüsselungsniveau an.




3. Sie werden automatisch zum Dialogfeld **Passwort einrichten** geleitet. Geben Sie ein Passwort ein und klicken Sie auf **OK**.

## Sichern archivierter Aufzeichnungen

Viele Unternehmen wollen Aufzeichnungen mithilfe von Bandlaufwerken oder ähnlichen Medien sichern. Wie Sie das genau machen, hängt von den individuellen Anforderungen und den im Unternehmen verwendeten Sicherungsmedien ab. Berücksichtigen Sie jedoch folgende Hinweise:

**Sichern von Archiven anstelle von Kameradatenbanken**

Erstellen Sie Sicherungen stets anhand des Inhalts von Archiven, nicht anhand der einzelnen Kameradatenbanken. Wenn Sie Sicherungen auf Grundlage des Inhalts einzelner Kameradatenbanken erzeugen, können Freigabeverletzungen und andere Fehlfunktionen auftreten.

Sorgen Sie bei der Planung von Sicherungen dafür, dass sich der Sicherungsauftrag nicht mit den festgelegten Archivierungszeiten überschneidet. Um die Archiv-Zeitpläne der einzelnen Aufzeichnungsserver in jedem der Speicherbereiche eines Aufzeichnungsservers anzuzeigen, rufen Sie die Registerkarte **Speicher** auf.

Um sicherzustellen, dass die Archivierung nicht während der Sicherung erfolgt, können Sie das Archiv aushängen (unmounten), die Sicherung durchführen, und dann wieder einhängen (mounten). Das Ein- und Aushängen von Archiven erfolgt über Milestone Integration Platform VMS API.

**Kennenlernen der Archivstruktur für gezielte Sicherungen**

Bei der Archivierung von Aufzeichnungen speichern Sie diese in einer bestimmten Struktur des Archivs, die verschiedene Unterverzeichnisse umfasst.

Bei der gesamten regulären Nutzung Ihres Systems ist die Struktur mit Unterverzeichnissen für die Benutzer des Systems vollkommen transparent, wenn sie Aufzeichnungen mit XProtect Smart Client durchsuchen. Dies gilt sowohl für archivierte als auch für nicht archivierte Aufzeichnungen. Wenn Sie Ihre archivierten Aufzeichnungen sichern möchten (siehe Archivstruktur (Erklärung) auf Seite 64), ist es hilfreich, wenn Sie die Unterverzeichnisstruktur kennen (siehe Sicherung und Wiederherstellung einer Systemkonfiguration auf Seite 356).

## Löschen eines Archivs aus einem Speicher

1. Wählen Sie das gewünschte Archiv in der Liste **Aufzeichnungs- und Archivierungskonfiguration** aus.

   Sie können lediglich das letzte Archiv in der Liste löschen. Das Archiv muss nicht leer sein.

2. Klicken Sie auf die Schaltfläche  unter der Liste **Aufzeichnungs- und Archivierungskonfiguration**.
3. Klicken Sie auf **Ja**.

   Bei nicht verfügbaren Archiven, z. B. Offline-Archiven, kann nicht überprüft werden, ob das Archiv Medien mit Beweissicherungen enthält, jedoch kann das Archiv nach Bestätigung durch den Benutzer gelöscht werden.

   Verfügbare Archive (Online-Archive), die Medien mit Beweissicherungen enthalten, können nicht gelöscht werden.

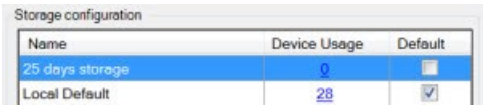
## Löschen eines Speichers

Sie können den/die Standardspeicher, den/die Geräte als Aufzeichnungsspeicher für Live-Aufzeichnungen verwenden, nicht löschen.
Dies bedeutet, dass Sie ggf. Geräte (siehe Hardware verschieben auf Seite 368) sowie noch nicht archivierte Aufzeichnungen auf ein anderes Speichergerät verschieben müssen, bevor Sie den Speicher löschen.

1. Zur Anzeige einer Liste der Geräte, die den Speicher verwenden, klicken Sie auf die Gerätenutzungszahl.

   > Wenn der Speicher Daten von Geräten aufweist, die auf einen anderen Aufzeichnungsserver verschoben wurden, wird eine Warnung angezeigt. Klicken Sie auf den Link, um die Liste mit Geräten anzuzeigen.

2. Befolgen Sie die in Verschieben nicht archivierter Aufzeichnungen von einem Speicher in einen anderen auf Seite 220 angegebenen Schritte.
3. Fahren Sie fort, bis Sie alle Geräte verschoben haben.
4. Wählen Sie den Speicher aus, den Sie löschen möchten.




5. Klicken Sie auf die Schaltfläche  unter der Liste **Speicherkonfiguration**.
6. Klicken Sie auf **Ja**.

## Verschieben nicht archivierter Aufzeichnungen von einem Speicher in einen anderen

Auf der Registerkarte **Aufzeichnung** des Geräts können Sie Aufzeichnungen von einer Live-Aufzeichnungsdatenbank in eine andere verschieben.

1. Wählen Sie den Gerätetyp aus. Wählen Sie im Fenster **Übersicht** das gewünschte Gerät aus.
2. Klicken Sie auf die Registerkarte **Aufzeichnung**. Klicken Sie oben im Bereich **Speicher** auf **Auswählen**.
3. Wählen Sie die Datenbank im Dialogfeld **Speicher auswählen** aus.
4. Klicken Sie auf **OK**.
5. Wählen Sie im Dialogfeld **Aufzeichnungsaktion**, ob Sie bereits vorhandene – aber noch **nicht archivierte** – Aufzeichnungen in den neuen Speicher verschieben bzw. löschen möchten.
6. Klicken Sie auf **OK**.

## Failover-Aufzeichnungsserver zuweisen

Auf der Registerkarte **Failover** eines Aufzeichnungsservers können Sie zwischen drei Failover-Einrichtungsarten wählen:

- Keine Failover-Einrichtung
- Einrichtung primärer/sekundärer Failover-Gruppen (Cold-Standby)
- Eine Hot-Standby-Einrichtung

Wenn Sie sich für **b** und **c** entscheiden, müssen Sie den gewünschten Server/die gewünschten Gruppen auswählen. Bei **b** können Sie außerdem eine sekundäre Failover-Gruppe einrichten. Sollte der Aufzeichnungsserver nicht mehr verfügbar sein, übernimmt ein Failover-Aufzeichnungsserver aus der primären Failover-Gruppe. Wenn Sie zudem eine sekundäre Failover-Gruppe ausgewählt haben, übernimmt ein Failover-Aufzeichnungsserver aus der sekundären Gruppe in dem Fall, dass alle Failover-Aufzeichnungsserver in der primären Failover-Gruppe ausgelastet sind. So riskieren Sie nur für den seltenen Fall, dass alle Failover-Aufzeichnungsserver in der primären als auch in der sekundären Failover-Gruppe ausgelastet sind, dass es keine Failover-Lösung gibt.

1. Wählen Sie im Bereich **Standort-Navigation** die Optionen **Server** > **Aufzeichnungsserver**. Daraufhin wird eine Liste mit Aufzeichnungsservern geöffnet.
2. Wählen Sie im Fenster **Übersicht** den gewünschten Aufzeichnungsserver aus, und öffnen Sie die Registerkarte **Failover**.
3. Wählen Sie zur Auswahl der Failover-Einrichtungsart zwischen folgenden Optionen aus:
   - **Keine**
   - **Primäre Failover-Servergruppe/Sekundäre Failover-Servergruppe**
   - **Hot-Standby-Server**

   Sie können eine Failover-Gruppe nicht als primäre und auch als sekundäre Failover-Gruppe festlegen und ebenso nicht reguläre Failover-Server, die bereits Teil einer Failover-Gruppe sind, als Hot-Standby-Server auswählen.
4. Klicken Sie als Nächstes auf **Erweiterte Failover-Einstellungen**. Daraufhin öffnet sich das Fenster **Erweiterte Failover-Einstellungen**, in dem alle mit dem ausgewählten Aufzeichnungsserver verbundenen Geräte aufgelistet werden. Wenn Sie die Option **Keine** gewählt haben, sind außerdem die erweiterten Failover-Einstellungen verfügbar. Das System speichert alle Einstellungen für spätere Failover-Einrichtungen.
5. Um die Stufe der Failover-Unterstützung zu ermitteln, wählen Sie für jedes Gerät in der Liste **Vollständiger Support**, **Nur live** oder **Deaktiviert** aus. Klicken Sie auf **OK**.
6. Bearbeiten Sie die Portnummer, wenn erforderlich, im Feld **Kommunikationsport des Failover-Dienstes (TCP)**.

Wenn Sie Failover-Support aktivieren und der Aufzeichnungsserver so konfiguriert ist, dass er weiterläuft, wenn kein Aufzeichnungsspeicher verfügbar ist, übernimmt der Failover-Aufzeichnungsserver nicht. Damit der Failover-Support funktioniert, müssen Sie auf der Registerkarte **Speicher** die Option **Aufzeichnungsserver stoppen, wenn ein Aufzeichnungsspeicher nicht verfügbar ist** auswählen.

## Aktivieren Sie Multicasting für den Recording-Server

Bei der herkömmlichen Netzwerkkommunikation wird jedes Datenpaket von genau einem Absender an genau einen Empfänger gesendet. Dieser Prozess wird als „Unicasting“ bezeichnet. Mit Multicasting können Sie jedoch ein Datenpaket (von einem Server) an mehrere Empfänger (Clients) in einer Gruppe senden. Multicasting kann dabei helfen, den Bandbreitenbedarf zu reduzieren.

- Wenn Sie **Unicasting** nutzen, muss die Quelle einen Datenstream pro Empfänger übertragen
- Bei Verwendung von **Multicasting** wird für jedes Netzwerksegment hingegen nur ein Datenstream benötigt

Beim hier beschriebenen Multicasting handelt es sich **nicht** um ein Streaming von Videodaten von einer Kamera an Server, sondern von Servern an Clients.

Beim Multicasting arbeiten Sie mit einer definierten Gruppe von Empfängern, je nach Optionen wie IP-Adressbereichen, der Fähigkeit zum Aktivieren/Deaktivieren von Multicasts für einzelne Kameras, der Fähigkeit zum Festlegen der maximal akzeptablen Datenpaketgröße (MTU), der Maximalzahl an Routern, zwischen denen ein Datenpaket übertragen werden muss (TTL) usw.

Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet.

Multicasting sollte nicht mit **Broadcasting** verwechselt werden, bei dem Daten an alle gesendet werden, die mit dem Netzwerk verbunden sind, selbst wenn die Daten möglicherweise nicht für alle relevant sind:

| Name | Beschreibung |
|---|---|
| **Unicasting** | Sendet Daten von genau einer Quelle an genau einen Empfänger. |
| **Multicasting** | Sendet Daten von einer einzelnen Quelle an verschiedene Empfänger in einer klar definierten Gruppe. |
| **Broadcasting** | Sendet Daten von einer einzelnen Datenquelle an alle im Netzwerk. Somit kann Broadcasting die Geschwindigkeit im Netzwerk deutlich reduzieren. |

Wenn Sie Multicasting verwenden möchten, muss Ihre Netzwerkinfrastruktur den IP-Multicasting-Standard IGMP (Internet Group Management Protocol) unterstützen.

- Aktivieren Sie auf der Registerkarte **Multicast** das Kontrollkästchen **Multicast**

Wenn auf einem oder mehr Servern bereits der gesamte IP-Adressbereich für Multicast genutzt wird, müssen Sie zunächst einige IP-Adressen für Multicast freigeben, bevor Sie Multicasting auf zusätzlichen Aufzeichnungsservern aktivieren können.

Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet.

## Aktivieren von Multicasting für einzelne Kameras

Multicasting funktioniert nur, wenn Sie die Option für die entsprechenden Kameras aktivieren:

1. Wählen Sie im Fenster **Übersicht** den Aufzeichnungsserver und die gewünschte Kamera aus.
2. Aktivieren Sie auf der Registerkarte **Client** das Kontrollkästchen **Live-Multicast**. Wiederholen Sie diesen Schritt für alle entsprechenden Kameras.

Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet.

## Festlegen von öffentlichen Adressen und Ports

Wenn Sie auf das VMS mit XProtect Smart Client über ein öffentliches oder nicht vertrauenswürdiges Netzwerk zugreifen müssen, Milestone sollten Sie eine sichere Verbindung über VPN verwenden. So wird gewährleistet, dass die Kommunikation zwischen XProtect Smart Client und dem VMS-Server geschützt ist.

Die öffentliche IP-Adresse eines Aufzeichnungsservers legen Sie auf der Registerkarte **Netzwerk** fest.

**Wozu dient eine öffentliche Adresse?**

Clients können Verbindungen über das lokale Netzwerk oder das Internet herstellen. In beiden Fällen muss das Überwachungssystem dazu in der Lage sein, geeignete Adressen bereitzustellen, damit Clients auf Live-Videos und Videoaufzeichnungen der Aufzeichnungsserver zugreifen können:

- Wenn Clients eine lokale Verbindung herstellen, muss das Überwachungssystem mit lokalen Adressen und Portnummern antworten
- Wenn Clients eine Verbindung über das Internet herstellen, muss das Überwachungssystem mit der öffentlichen Adresse des Aufzeichnungsservers antworten. Dies ist die Adresse der Firewall oder des NAT-Routers (Network Address Translation) und oftmals auch eine andere Portnummer. Die Adresse und der Port können dann an die lokale Adresse und den lokalen Port des Servers weitergeleitet werden.

1. Zum Aktivieren des öffentlichen Zugriffs wählen Sie das Kontrollkästchen **Öffentlichen Zugriff ermöglichen** aus.
2. Legen Sie die öffentliche Adresse des Aufzeichnungsservers fest. Geben Sie die Adresse der Firewall oder des NAT-Routers ein, damit Clients, die über das Internet auf das Überwachungssystem zugreifen, eine Verbindung zu den Aufzeichnungsservern herstellen können.
3. Geben Sie eine öffentliche Portnummer an. Es wird empfohlen, für die Firewall oder den NAT-Router andere Portnummern als für die Lokalen zu verwenden.

Wenn Sie einen öffentlichen Zugriff nutzen, konfigurieren Sie die Firewall oder den NAT-Router so, dass an die öffentliche Adresse gesendete Anfragen an die lokale Adresse und Ports von relevanten Aufzeichnungsservern weitergeleitet werden.

#### Zuweisen lokaler IP-Bereiche

Sie definieren eine Liste lokaler IP-Bereiche, deren Ursprung vom Überwachungssystem als lokales Netzwerk erkannt werden sollte:

- Klicken Sie auf der Registerkarte **Netzwerk** auf **Konfigurieren**

## Gerätebaum filtern

Der Gerätebaum im Fenster **Übersicht** kann sehr groß werden, wenn Sie über viele registrierte Geräte verfügen. Sie können den Gerätebaum filtern, um die Geräte, mit denen Sie arbeiten möchten, leichter zu finden.

Durch Bereitstellen von Filterbegriffen, die nur für bestimmte Geräte gelten, können Sie nur diese spezifischen Geräte anzeigen.

#### Gerätebaum filtern

- Klicken Sie im oberen Teil des Fensters **Übersicht** auf **Filter**, um die Registerkarte **Filter** zu öffnen.
- Geben Sie im Feld **Zum Filtern von Geräten hier eingeben** ein oder mehrere Filterkriterien ein und klicken Sie auf **Filter anwenden**, um die Geräteliste zu filtern.

#### Eigenschaften der Filterkriterien

Die Filterkriterien werden auf die Feldwerte Gerätename, Gerätekurzname, Hardwareadresse (IP), Geräte-ID und Hardware-ID angewendet.

Beim Filtern von Hardware-ID- und Geräte-ID-Feldwerten werden teilweise Filterübereinstimmungen nicht angezeigt. Daher müssen Sie bei der Filterung nach Hardware-ID oder Geräte-ID die vollständige und genaue Identifikationsnummer angeben.

Teilweise Filterübereinstimmungen werden für die Feldwerte „Gerätename“, „Gerätekurzname“ und „Hardwareadresse“ angezeigt, sodass der Filterbegriff „Kamera“ alle Geräte anzeigt, die das Wort „Kamera“ im Gerätenamen enthalten.

Bei den Filterkriterien wird nicht zwischen Groß- und Kleinschreibung unterschieden, d. h. die Verwendung von "kamera" oder "Kamera" als Filterkriterien führt zu denselben Ergebnissen.

### Festlegen mehrerer Filterkriterien

Sie können mehrere Filterkriterien festlegen und so das Filtern des Gerätebaums weiter einschränken. Bei Anwendung des Filters werden alle definierten Filterkriterien mit einem UND verknüpft, d. h. sie sind kumulativ.

Zum Beispiel, wenn Sie zwei Filterkriterien eingegeben haben: „Kamera“ und „Lager“, in der Liste werden alle Geräte angezeigt, die die Wörter „Kamera“ und „Lager“ im Gerätenamen enthalten, aber keine Geräte, die die Wörter „Kamera“ und „Parkplatz“ im Gerätenamen enthalten, und auch keine Geräte, die nur das Wort "Kamera" im Gerätenamen enthalten.

Entfernen Sie jedes einzelne Filterkriterium aus dem Filterfeld, um Ihren Filter zu erweitern, wenn der Filter zu restriktiv ist. Der Filter wird automatisch auf den Gerätebaum angewendet, wenn Filterkriterien entfernt werden.

### Zurücksetzen des Filters

Wenn Sie alle Filterkriterien aus dem Filterfeld entfernen, wird das Fenster **Übersicht** zurückgesetzt und zeigt wieder alle Geräte an.

Durch Drücken von **F5** können Sie ebenfalls den Filter zurücksetzen und das Kontrollkästchen **Deaktivierte Geräte anzeigen** deaktivieren.

### Geräte deaktiviert:

Deaktivierte Geräte werden standardmäßig nicht im Fenster **Übersicht** angezeigt.

Um alle deaktivierten Geräte anzuzeigen, klicken Sie oben im Fenster **Übersicht** auf **Filter** um die Registerkarte **Filter** zu öffnen, und wählen Sie **Deaktivierte Geräte anzeigen**.

Um deaktivierte Geräte wieder auszublenden, deaktivieren Sie die Option **Deaktivierte Geräte anzeigen**.

# Failover-Server

## Failover-Aufzeichnungsserver einrichten und aktivieren

> Wenn Sie den Failover-Aufzeichnungsserver deaktiviert haben, müssen Sie ihn aktivieren, bevor er von den Standard-Aufzeichnungsservern übernehmen kann.

Tun Sie das Folgende, um einen Failover-Aufzeichnungsserver zu aktivieren und dessen grundlegenden Eigenschaften zu bearbeiten:

1. Wählen Sie auf der Tafel **Seitennavigation Server** > **Failover-Server** aus. Dadurch öffnet sich eine Liste von installierten Failover-Aufzeichnungsserver und Failover-Gruppen.
2. Wählen Sie im Fenster **Übersicht** den erwünschten Failover-Aufzeichnungsserver aus.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Aktiviert**. Der Failover-Aufzeichnungsserver ist nun aktiviert.
4. Um die Eigenschaften des Failover-Aufzeichnungsservers zu bearbeiten, gehen Sie auf die Registerkarte **Info**.
5. Wenn Sie fertig sind, gehen Sie auf die Registrierkarte **Netzwerk**. Hier können Sie die öffentliche IP-Adresse des Failover-Aufzeichnungsservers und mehr definieren. Dies ist wichtig, wenn Sie NAT (Network Address Translation) und Portweiterleitung verwenden. Weitere Informationen finden Sie auf der Registerkarte **Netzwerk** des Standard-Aufzeichnungsservers.
6. Wählen Sie im Bereich **Standort-Navigation** die Optionen **Server** > **Aufzeichnungsserver**. Wählen Sie den Aufzeichnungsserver aus, für den Sie eine ausfallsichere Unterstützung wünschen, und weisen Sie ausfallsichere Aufzeichnungsserver zu (siehe Registerkarte „Failover“ (Aufzeichnungsserver) auf Seite 453).

Um den Status eines Failover-Aufzeichnungsservers anzuzeigen, halten Sie die Maus über das Failover Recording Server Manager-Taskleistensymbol im Benachrichtigungsbereich. Ein Tooltip wird angezeigt, der den Text enthält, der im Feld Beschreibung des Failover-Aufzeichnungsservers eingegeben wurde. Dies kann Ihnen dabei helfen festzustellen, für welchen Aufzeichnungsserver der Failover-Aufzeichnungsserver zur Übernahme konfiguriert wurde.

> Der Failover-Aufzeichnungsserver pingt den Management-Server regelmäßig, um sicherzustellen, dass er online ist und bei Bedarf die Konfiguration der Standard-Aufzeichnungsserver anfordern und empfangen kann. Wenn Sie das Pingen blockieren, kann der Failover-Aufzeichnungsserver nicht von Standard-Aufzeichnungsserver übernehmen.

## Gruppieren von Failover-Aufzeichnungsservern für Cold-Standby

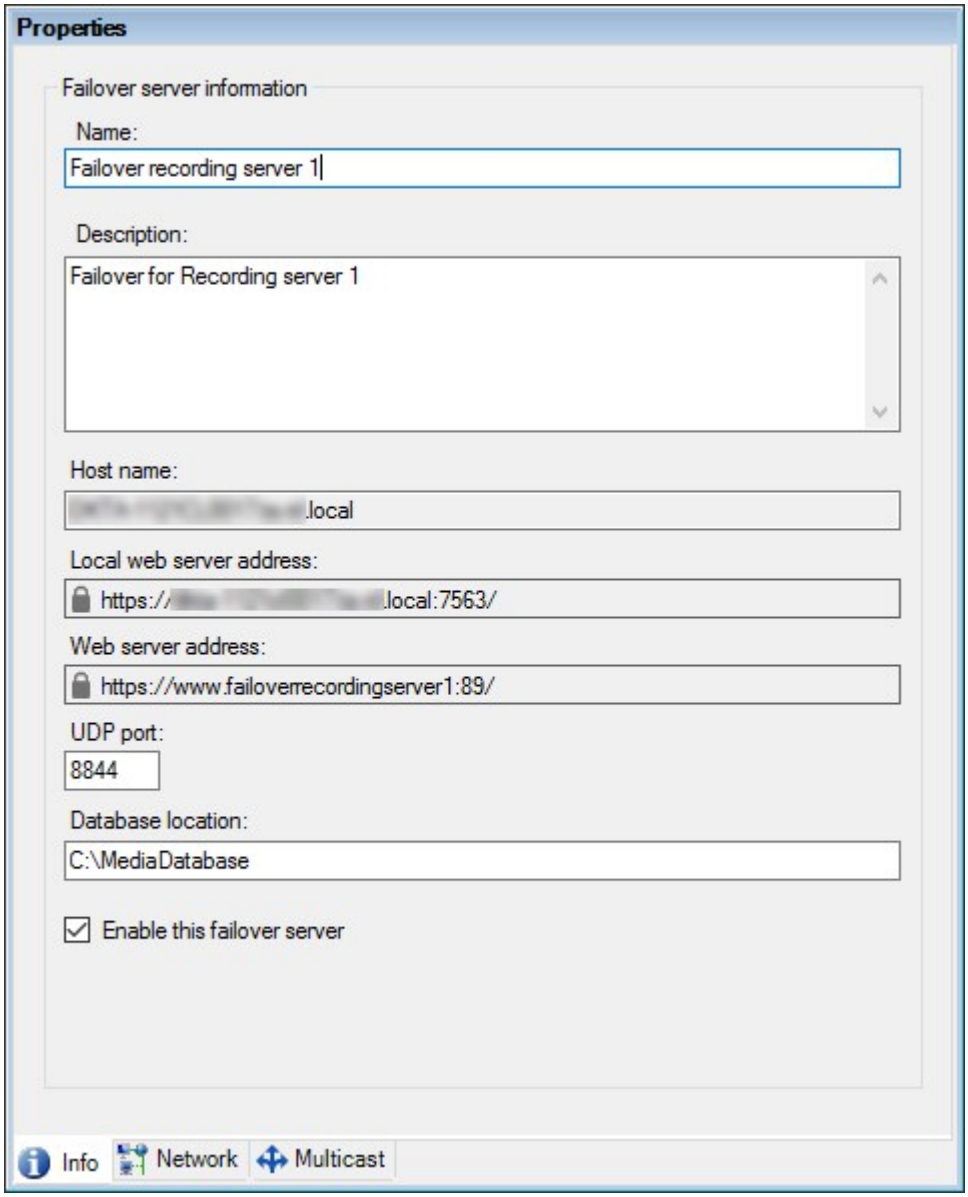
1. Wählen Sie **Server** > **Failover-Server**. Dadurch öffnet sich eine Liste von installierten Failover-Aufzeichnungsserver und Failover-Gruppen.
2. Klicken Sie im Bereich **Übersicht** mit der rechten Maustaste auf **Failover-Gruppen** und wählen Sie **Gruppe hinzufügen**.
3. Geben Sie einen Namen (in diesem Beispiel *Failover-Gruppe 1*) und eine Beschreibung (optional) Ihrer neuen Gruppe an. Klicken Sie auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf die gerade erstellte Gruppe (*Failover-Gruppe 1*). Wählen Sie **Gruppenmitglieder bearbeiten**. Dadurch öffnet sich das Fenster **Gruppenmitglieder auswählen**.
5. Nutzen Sie Drag-and-Drop oder die Tasten, um den/die ausgewählten Failover-Aufzeichnungsserver von links nach rechts zu bewegen. Klicken Sie auf **OK**. Der/die ausgewählten Failover-Aufzeichnungsserver sind jetzt Teil der neu erstellten Gruppe (*Failover-Gruppe 1*).
6. Gehen Sie zur Registerkarte **Sequenz**. Klicken Sie auf **Nach oben** und **Nach unten**, um die interne Sequenz der regulären Failover-Aufzeichnungsserver in der Gruppe zu bestimmen.

## Verschlüsselungsstatus auf einem Failover-Aufzeichnungsserver anzeigen

Um zu prüfen, ob Ihr Failover-Aufzeichnungsserver eine Verschlüsselung verwendet, tun Sie bitte folgendes:

1. Wählen Sie auf der Tafel **Seitennavigation Server** > **Failover-Server** aus. Daraufhin wird eine Liste mit Failover-Aufzeichnungsservern geöffnet.
2. Wählen Sie in dem Fenster **Übersicht** den jeweiligen Aufzeichnungsserver aus und gehen Sie auf die Registerkarte **Info**.
   Wenn die Verschlüsselung zu Clients und Servern, die Datenstreams vom Aufzeichnungsserver abrufen, aktiviert ist, erscheint ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der des

optionalen Webservers.




## Anzeigen von Statusmeldungen

1. Klicken Sie auf dem Failover-Aufzeichnungsserver mit der rechten Maustaste auf das **Milestone Failover Recording Server-Dienst**-Symbol.
2. Wählen Sie **Statusmeldungen anzeigen**. Das Fenster **Failover-Server-Statusmeldungen** wird mit Zeitstempel-Statusmeldungen eingeblendet.

### Anzeigen von Versionsinformationen

Die Kenntnis der genauen Version Ihres **Failover Recording Server-Dienstes** ist hilfreich, wenn Sie sich an den Produktsupport wenden wollen.

1. Klicken Sie auf dem Failover-Aufzeichnungsserver mit der rechten Maustaste auf das **Milestone Failover Recording Server-Dienst**-Symbol.
2. Wählen Sie **Info**.
3. Ein kleines Dialogfeld öffnet sich und zeigt die exakte Version Ihres **Failover Recording Server-Dienstes** an.

## Hardware

### Hardware hinzufügen

Sie haben mehrere Optionen, um zu den Aufzeichnungsservern in Ihrem System Hardware hinzuzufügen.

> ⚠ Wenn Ihre Hardware sich hinter einem NAT-fähigen Router oder einer Firewall befindet, müssen Sie möglicherweise eine andere Portnummer bestimmen und den Router/die Firewall so konfigurieren, dass die von der Hardware genutzten Port- und IP-Adressen zugewiesen werden.

Der Assistent zum **Hardware hinzufügen** hilft Ihnen dabei, in Ihrem Netzwerk Hardware wie etwa Kameras und Videoencoder zu finden und diese den Aufzeichnungsservern in Ihrem System hinzuzufügen. Mit dem Assistenten können Sie auch Remote-Server für Milestone Interconnect-Einrichtungen hinzufügen. Fügen Sie jeweils nur bei **einem Aufzeichnungsserver** zur selben Zeit Hardware hinzu.

1. Um auf **Hardware hinzufügen** zuzugreifen, klicken Sie mit der rechten Maustaste auf den notwendigen Aufzeichnungsserver und wählen Sie **Hardware hinzufügen**.
2. Wählen Sie eine der Assistentenoptionen (siehe unten) und folgen Sie den Anweisungen auf dem Bildschirm.
3. Nach der Installation können Sie die Hardware und Geräte im Fenster **Übersicht** sehen.

> ⚠ Bestimmte Hardwaregeräte müssen vorkonfiguriert werden, wenn die Hardware zum ersten Mal hinzugefügt wird. Ein zusätzlicher Assistent zur **Vorkonfiguration von Hardwaregeräten** erscheint, wenn solche Hardwaregeräte hinzugefügt werden. Weitere Informationen dazu finden Sie unter Hardwarevorkonfiguration (Erklärung) auf Seite 55.

#### Hardware hinzufügen (Dialog)

Hardware steht entweder für:

- Die physische Einheit, die mit dem Aufzeichnungsserver des Überwachungssystems direkt über IP verbunden ist, beispielsweise eine Kamera, ein Videoencoder, ein I/O-Modul
- Ein Aufzeichnungsserver an einem Remote-System in einer Milestone Interconnect-Einrichtung

Weitere Informationen dazu, wie Sie Hardware zu Ihrem System hinzufügen können, finden Sie unter Hardware hinzufügen auf Seite 229.

| Name | Beschreibung |
|---|---|
| **Express** (empfohlen) | Das System scannt das lokale Netzwerk des Aufzeichnungsservers automatisch nach neuer Hardware.<br><br>Wählen Sie das Kontrollkästchen **Hardware auf anderen Aufzeichnungsservern anzeigen** aus, um zu erfahren, ob erkannte Hardware auf anderen Aufzeichnungsservern läuft.<br><br>Sie können diese Option jedes Mal auswählen, wenn Sie Ihrem Netzwerk neue Hardware hinzufügen und diese in Ihrem System verwenden wollen.<br><br>Sie können diese Option nicht verwenden, um Remote-Systeminstallationen in Milestone Interconnect-Einstellungen hinzuzufügen.<br><br>Zum Hinzufügen von sowohl HTTP- als auch HTTPS-Hardware führen Sie die **Express**-Erkennung mit ausgewählter Optionsschaltfläche **HTTPS (Sicher)** aus, und dann mit ausgewählter Optionsschaltfläche **HTTP (Unsicher)**. |
| **Adressbereich scannen** | Das System scannt Ihr Netzwerk nach relevanter Hardware und Milestone Interconnect-Remote-Systeminstallationen auf Basis Ihrer Angaben zu:<br><br>• Hardware-Benutzernamen und Passwörtern. Dies ist nicht nötig, wenn Ihre Hardware die werksseitig voreingestellten Benutzernamen und Passwörter verwendet<br>• Treiber<br>• IP-Bereiche (nur IPv4)<br>• Portnummer (Standardport 80)<br><br>Sie können diese Option auswählen, wenn Sie nur einen Teil Ihres Netzwerks scannen möchten, beispielsweise bei einer Systemerweiterung. |

| Name | Beschreibung |
|---|---|
| **Manuell** | Bestimmen Sie die Einzelheiten zu allen Hardware- und Milestone Interconnect-Remote-Systeminstallationen separat. Dies kann eine gute Vorgehensweise sein, wenn Sie nur wenige Hardware-Einheiten hinzufügen möchten und ihre IP-Adressen, relevanten Benutzernamen und Passwörter kennen oder eine Kamera die automatische Erkennungsfunktion nicht unterstützt. |
| **Fernverbindungs-Hardware** | Das System scannt nach Hardware, die über einen über Fernzugriff verbundenen Server verbunden ist.<br>Sie können diese Option nutzen, wenn Sie beispielsweise Server für die Axis One-click Camera Connection installiert haben.<br>Sie können diese Option nicht verwenden, um Remote-Systeminstallationen in Milestone Interconnect-Einstellungen hinzuzufügen. |

## Hardware aktivieren/deaktivieren

Hinzugefügte Hardware ist standardmäßig **aktiviert**.

So können Sie erkennen, ob Hardware aktiviert oder deaktiviert ist:

verwenden
Deaktiviert

**Um hinzugefügte Hardware zu deaktivieren, z.B. aus Lizenz- oder Leistungsgründen**

1. Erweitern Sie den Aufzeichnungsserver und klicken Sie mit der rechten Maustaste auf die Hardware, die Sie deaktivieren möchten.
2. Wählen Sie **Aktiviert**, um die Option zu aktivieren oder zu deaktivieren.

## Bearbeiten von Hardware

Klicken Sie mit der rechten Maustaste auf die hinzugefügte Hardware und wählen Sie **Hardware bearbeiten** aus, um die Netzwerkkonfiguration und die Einstellungen für die Benutzerberechtigungen der Hardware in Management Client zu ändern.

### Hardware bearbeiten (Dialog)

Für manche Hardwaregeräte erlaubt Ihnen der Dialog **Hardware bearbeiten** auch, Einstellungen direkt auf das jeweilige Hardwaregerät anzuwenden.

Wenn die Optionsschaltfläche **Einstellungen Management Client bearbeiten ausgewählt ist**, zeigt der Dialog **Hardware bearbeiten** die Einstellungen, die Management Client für die Verbindung zur Hardware verwendet. Damit das Hardwaregerät korrekt zum System hinzugefügt wird, nehmen Sie die gleichen Einstellungen vor, die Sie auch für die Verbindung zur Hardwarekonfigurationsoberfläche des Herstellers verwenden:

| Name | Beschreibung |
|---|---|
| **Name** | Zeigt den Namen der Hardware neben der ermittelten IP-Adresse an (in Klammern). |
| **URL der Hardware** | Die Webadresse der Konfigurationsoberfläche des Herstellers, die typischerweise die IP-Adresse der Hardware enthält. Geben Sie eine gültige Adresse in Ihrem Netzwerk an. |
| **Benutzername** | Der für die Verbindung zur Hardware verwendete Benutzername.<br><br>Der Benutzername, den Sie hier eingeben, ändert nicht den Benutzernamen auf dem Hardwaregerät selbst. Wählen Sie Optionsschaltflächen **Bearbeiten Management Client und Hardwareeinstellungen** aus, um auf unterstützten Hardwaregeräten die Einstellungen zu ändern. |
| **Passwort** | Das für die Verbindung zur Hardware verwendete Passwort.<br><br>Das Passwort, das Sie hier eingeben, ändert nicht das Passwort auf dem Hardwaregerät selbst. Wählen Sie Optionsschaltflächen **Bearbeiten Management Client und Hardwareeinstellungen** aus, um auf unterstützten Hardwaregeräten die Einstellungen zu ändern.<br><br>Weitere Informationen dazu, wie Sie die Passwörter für mehrere Hardwaregeräte auf einmal ändern können, finden Sie unter Passwörter auf Hardwaregeräten ändern auf Seite 237.<br><br>Als Systemadministrator müssen Sie anderen Benutzern die Erlaubnis erteilen, das Passwort im Management Client einzusehen. Weitere Informationen finden Sie unter Rolleneinstellungen unter Hardware. |

Wenn die Option Schaltfläche **Bearbeiten Management Client und Hardwareeinstellungen** ausgewählt ist (für unterstützte Hardware), zeigt der Dialog **Hardware bearbeiten** die Einstellungen, die auch direkt auf das jeweilige Hardwaregerät angewendet werden:

> Wenn mit dieser Optionsschaltfläche die Einstellungen angewendet werden, werden die aktuellen Einstellungen auf dem Hardwaregerät überschrieben. Die Hardware verliert dann für einen Moment die Verbindung zum Aufzeichnungsserver, während die Einstellungen angewendet werden.

| Name | Beschreibung |
|---|---|
| **Name** | Zeigt den Namen der Hardware neben der ermittelten IP-Adresse an (in Klammern). |
| **Netzwerkkonfiguration** | Die Netzwerkeinstellungen der Hardware. Wählen Sie Konfigurieren auf Seite 233 aus, um die Netzwerkeinstellungen anzupassen. |
| **Konfigurieren** | Geben Sie (für unterstützte Hardwaregeräte) anhand der Auswahlliste für die **IP-Version** das Internetprotokoll an.<br>• Für IPv4 müssen die Werte das folgende Format haben: **(0-999).(0-999).(0-999).(0-999)**<br>• Für IPv6 müssen die Werte in acht Gruppen aus Hexadezimalzahlen angeordnet sein, die jeweils mit einem Doppelpunkt getrennt sind. Die Subnetzmaske muss eine Zahl zwischen **0-128** sein.<br>Die Schaltfläche **Prüfen** testet, ob aktuell im System noch ein weiteres Hardwaregerät vorhanden ist, das die angegebene IP-Adresse verwendet.<br>**Prüfen** kann keine Konflikte mit Hardwaregeräten erkennen, die ausgeschaltet sind, sich außerhalb des XProtect VMS-Systems befinden oder aus sonstigen Gründen momentan nicht reagieren. |
| **Benutzername** | Der für die Verbindung zur Hardware verwendete Benutzername und das dazugehörige Level. Wählen Sie aus der Dropdown-Liste einen anderen Benutzer aus und fügen Sie mit Hilfe des unten beschriebenen Feldes **Passwort** ein neues Passwort hinzu.<br>Fügen Sie Benutzer hinzu oder löschen Sie sie mithilfe der unterstrichenen |

| Name | Beschreibung |
|---|---|
| | Aktionen unten im Abschnitt **Berechtigungen** (siehe Benutzer hinzufügen auf Seite 234 oder Benutzer löschen auf Seite 235).<br><br>Wenn Sie einen Benutzer auswählen, der nicht die höchste vom Hersteller vorgegebenen Benutzerebene besitzt, stehen manche Funktionen ggf. nicht zur Verfügung. |
| **Passwort** | Das für die Verbindung zur Hardware verwendete Passwort. Mithilfe des Symbols **Zeigen** können Sie den aktuell eingegebenen Text sehen.<br><br>Wenn Sie das Passwort ändern, lesen Sie in der Dokumentation des Herstellers die Passwortregeln für das jeweilige Hardwaregerät nach, oder verwenden Sie die Schaltfläche **Passwort erzeugen**, um automatisch ein Passwort zu erzeugen, das die Anforderungen erfüllt.<br><br>Weitere Informationen dazu, wie Sie die Passwörter für mehrere Hardwaregeräte auf einmal ändern können, finden Sie unter Passwörter auf Hardwaregeräten ändern auf Seite 237.<br><br>Als Systemadministrator müssen Sie anderen Benutzern die Erlaubnis erteilen, das Passwort im Management Client einzusehen. Weitere Informationen finden Sie unter Rolleneinstellungen unter Hardware. |
| **Benutzer** hinzufügen | Wählen Sie das unterstrichene Link **Hinzufügen** aus, um den Dialog **Benutzer hinzufügen** zu öffnen und zum Hardwaregerät einen Benutzer hinzuzufügen.<br><br>Wenn Sie einen Benutzer hinzufügen, wird dieser der aktuell aktive Benutzer, und die zuvor eingegebenen Anmeldedaten werden überschrieben.<br><br>Wenn Sie das Passwort erstellen, lesen Sie in der Dokumentation des Herstellers die Passwortregeln für das jeweilige Hardwaregerät nach, oder |

| Name | Beschreibung |
|---|---|
| | verwenden Sie die Schaltfläche **Passwort erzeugen**  , um automatisch ein Passwort zu erzeugen, das die Anforderungen erfüllt.<br><br>Das höchste von dem Hardwaregerät erkannte Benutzerlevel wird automatisch vorausgewählt. Es wird empfohlen, das standardmäßig eingestellte **Benutzerlevel** zu ändern.<br><br>  Wenn Sie ein **Benutzerlevel** auswählen, das nicht das höchste vom Hersteller vorgegebene Benutzerlevel ist, stehen manche Funktionen ggf. nicht zur Verfügung. |
| **Benutzer** löschen | Wählen Sie das unterstrichene Link **Löschen** aus, um den Dialog **Benutzer löschen** zu öffnen und Benutzer vom Hardwaregerät zu löschen.<br><br>  Den aktuell aktiven Benutzer können Sie nicht löschen. Verwenden Sie den oben beschriebenen Dialog **Benutzer hinzufügen**, um einen neuen Benutzer einzustellen, und entfernen Sie dann den alten Benutzer mithilfe dieser Oberfläche. |

## Einzelne Geräte aktivieren/deaktivieren

**Kameras** sind standardmäßig **aktiviert**.

**Mikrofone, Lautsprecher, Metadaten, Eingänge** und **Ausgänge** sind standardmäßig **deaktiviert**.

Dies bedeutet, dass Mikrofone, Lautsprecher, Metadaten, Eingänge und Ausgänge einzeln aktiviert werden müssen, bevor Sie diese im System nutzen können. Der Grund ist, dass Überwachungssysteme auf Kameras zurückgreifen, während die Nutzung von Mikrofonen usw. stark von den Bedürfnissen einer Organisation abhängt.

Sie können erkennen, ob Geräte aktiviert oder deaktiviert sind (hier am Beispiel eines Ausgangs):

 Deaktiviert

 Verwenden

Kameras, Mikrofone, Lautsprecher, Metadaten, Eingänge und Ausgänge werden auf dieselbe Weise aktiviert/deaktiviert.

1. Erweitern Sie den Aufzeichnungsserver und das Gerät. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie aktivieren möchten.
2. Wählen Sie **Aktiviert**, um die Option zu aktivieren oder zu deaktivieren.


## Einrichten einer sicheren Verbindung zur Hardware

Sie können mithilfe von SSL (Secure Sockets Layer) eine sichere HTTPS-Verbindung zwischen der Hardware und dem Aufzeichnungsserver einrichten.

Wenden Sie sich an Ihren Kameraanbieter, um ein Hardware-Zertifikat zu erhalten und es hochzuladen, bevor Sie die unten angegebenen Schritte befolgen:

1. Klicken Sie im Bereich **Übersicht** mit der rechten Maustaste auf den Aufzeichnungsserver und wählen Sie die Hardware aus.


2. Aktivieren Sie HTTPS auf der Registerkarte **Einstellungen**. HTTPS ist standardmäßig nicht aktiviert.
3. Geben sie den Port auf dem Aufzeichnungsserver ein, zu dem die HTTPS-Verbindung besteht. Die Portnummer muss mit der Portnummer auf der Startseite des Geräts übereinstimmen.
4. Führen Sie nach Bedarf Veränderungen durch und speichern Sie.

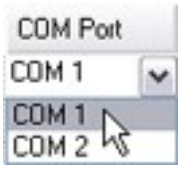
## Aktivieren von PTZ auf einem Videoencoder

Um die Verwendung von PTZ-Kameras auf einem Videoencoder zu aktivieren, führen Sie in der Registerkarte **PTZ** folgende Schritte aus:

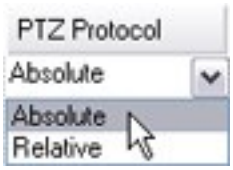
1. Wählen Sie in der Liste der mit dem Videoencoder verbundenen Geräte das Kästchen **PTZ aktivieren** für die relevanten Kameras aus:


2. Überprüfen Sie in der Spalte **PTZ-Geräte-ID** die ID jeder Kamera.

3. Wählen Sie in der Spalte **COM-Port** den Videoencoder, dessen COM-Ports (serielle Kommunikation) für die Steuerung der PTZ-Funktionalität verwendet werden soll:




4. Wählen Sie in der Spalte **PTZ-Protokoll**, welches Positionierungsschema Sie verwenden möchten:




   - **Absolut**: Wenn Benutzer für die Kamera PTZ-Steuerung verwenden, wird die Kamera relativ zu einer festen Position angebracht, oft als Home-Position bezeichnet
   - **Relativ**: Wenn Benutzer für die Kamera PTZ-Steuerung verwenden, wird die Kamera relativ zu einer festen Position angebracht

   Der Inhalt der Spalte **PTZ-Protokoll** variiert stark, abhängig von der Hardware. Einige verfügen über 5 bis 8 unterschiedliche Protokolle. Siehe auch Kameradokumentation.

5. Klicken Sie in der Symbolleiste auf **Speichern**.
6. Nun können Sie die Preset-Positionen und Wachrundgänge für jede PTZ-Kamera konfigurieren:
   - Hinzufügen einer Preset-Position (Typ 1)
   - Hinzufügen eines Wachrundgangprofils

## Passwörter auf Hardwaregeräten ändern

> Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Sie können Passwörter für mehrere Hardwaregeräte auf einmal ändern.

Anfänglich sind die unterstützten Geräte Modelle von Canon, Axis, Bosch, Hanwa, Panasonic, Sony, Hikvision, sowie ONVIF-kompatible Hardwaregeräte; die Benutzeroberfläche zeigt Ihnen jedoch direkt an, ob ein Modell unterstützt wird oder nicht. Sie können auch auf unserer Webseite gehen, um herauszufinden, ob ein bestimmtes Modell unterstützt wird: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> Für Geräte, die keine Gerätepasswortverwaltung unterstützen, müssen Sie das Passwort eines Hardwaregerätes von dessen Webseite aus ändern und dann das neue Passwort von Hand in Management Client eingeben. Weitere Informationen finden Sie unter Bearbeiten von Hardware auf Seite 231.

Sie können aus Folgendem auswählen:

- Lassen Sie das System individuelle Passwörter für jedes Hardwaregerät generieren. Das System erzeugt Passwörter auf der Grundlage der Anforderungen des Herstellers der Hardwaregeräte.
- Verwenden Sie ein einziges benutzerdefiniertes Passwort für alle Hardwaregeräte. Wenn Sie die neuen Passwörter anwenden, verlieren die Hardwaregeräte vorübergehend die Verbindung zum Aufzeichnungsserver. Nachdem Sie die neuen Passwörter angewendet haben, erscheint auf dem Bildschirm das Ergebnis für jedes Hardwaregerät. Bei fehlgeschlagenen Änderungen wird der Grund für das Fehlschlagen angezeigt, wenn das Hardwaregerät solche Informationen unterstützt. Aus dem Assistenten heraus können Sie einen Bericht über erfolgreiche und fehlgeschlagene Passwortänderungen erstellen, die Ergebnisse werden jedoch auch unter **Serverprotokolle** protokolliert.

  > Bei Hardware-Geräten mit ONVIF-Treibern und mehreren Benutzerkonten kann nur ein Administrator von XProtect mit Administratorrechten für das Hardware-Gerät Passwörter vom VMS aus ändern.

**Anforderungen:**

- Das Hardwaregerätemodell unterstützt die Gerätepasswortverwaltung durch Milestone.

Schritte:

1. Wählen Sie in dem Fenster **Seitennavigation** den Knoten **Aufzeichnungsserver** aus.
2. Klicken Sie mit der rechten Maustaste im Bereich Übersicht auf den entsprechenden Aufzeichnungsserver oder auf die jeweilige Hardware.
3. Wählen Sie **Hardwarepasswort ändern** aus. Ein Assistent wird angezeigt.
4. Geben Sie das Passwort unter Verwendung von Groß- und Kleinbuchstaben, Zahlen und den folgenden Zeichen ein: **! ( ) * - . _**

   Die maximale Passwortlänge beträgt 64 Zeichen.

   > Die maximale Passwortlänge für die Bosch FLEXIDOME IP Outdoor 5000 MP NDN-50051 Kamera beträgt 19 Zeichen.

5. Folgen Sie zum Abschluss des Änderungen den Anweisungen auf dem Bildschirm.

   Das Feld **Zuletzt geändertes Passwort** zeigt den Zeitstempel der letzten Passwortänderung an, basierend auf den lokalen Zeiteinstellungen desjenigen Computers, von dem aus das Passwort geändert wurde.

6. Die letzte Seite zeigt das Ergebnis. Wenn das System ein bestimmtes Passwort nicht aktualisieren konnte, klicken Sie auf **Fehlgeschlagen** neben dem Hardwaregerät, um die Begründung angezeigt zu bekommen.
7. Sie können auch auf die Schaltfläche **Bericht drucken** klicken, um die vollständige Liste der erfolgreichen und fehlgeschlagenen Aktualisierungen angezeigt zu bekommen.
8. Wenn Sie das Passwort auf den Hardwaregeräten ändern möchten, die versagt haben, klicken Sie auf **Erneut versuchen**, und der Assistent beginnt erneut mit den Hardwaregeräten, die versagt haben.

   Wenn Sie **Erneut versuchen** auswählen, können Sie nicht mehr auf den Bericht vom ersten Versuch zugreifen, als sie den Assistenten ausgeführt haben.

   Aufgrund der Sicherheitseinschränkungen können manche Hardwaregeräte vorübergehend nicht zur Verfügung stehen, wenn die Passwortänderung mehrmals hintereinander fehlschlägt. Die Sicherheitsbeschränkungen sind von Hersteller zu Hersteller unterschiedlich.

## Firmware auf einem Hardwaregerät aktualisieren

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Management Client erlaubt Ihnen, die Firmware zu einer Hardware zu aktualisieren, die zu Ihrem VMS-System zugefügt wurde. Sie können die Firmware für mehrere Hardwaregeräte gleichzeitig aktualisieren, wenn diese mit derselben Firmwaredatei kompatibel sind.

Die Benutzeroberfläche zeigt Ihnen direkt an, ob ein Modell Firmware Updates unterstützt. Sie können auch auf die Webseite Milestone gehen, um herauszufinden, ob ein bestimmtes Modell unterstützt wird: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> Für Geräte, die keine Firmware Updates unterstützen, müssen Sie die Firmware des jeweiligen Hardwaregerätes von dessen Internetseite aus aktualisieren.

Wenn Sie die Firmware aktualisieren, verlieren die Hardwaregeräte vorübergehend die Verbindung zum Aufzeichnungsserver.

Wenn Sie die Firmware aktualisiert haben, erscheint auf dem Bildschirm das Ergebnis für jedes Hardwaregerät. Bei fehlgeschlagenen Änderungen wird der Grund für das Fehlschlagen angezeigt, wenn das Hardwaregerät solche Informationen unterstützt. Die Ergebnisse werden auch unter **Serverprotokolle** protokolliert.

> Bei Hardware-Geräten mit ONVIF-Treibern und mehreren Benutzerkonten kann nur ein Administrator von XProtect mit Administratorrechten für das Hardware-Gerät die Firmware über das VMS aktualisieren.

**Anforderungen:**

- Das Hardwaregerät unterstützt Firmware Updates von Milestone.

Schritte:

1. Wählen Sie in dem Fenster **Seitennavigation** den Knoten **Aufzeichnungsserver** aus.
2. Klicken Sie mit der rechten Maustaste im Bereich Übersicht auf den entsprechenden Aufzeichnungsserver oder auf die jeweilige Hardware.
3. Wählen Sie **Hardware-Firmware aktualisieren**. Ein Assistent wird angezeigt.
4. Folgen Sie zum Abschluss des Änderungen den Anweisungen auf dem Bildschirm.

   > Sie können die Firmware für mehrere Hardwaregeräte nur dann gleichzeitig aktualisieren, wenn diese mit derselben Firmwaredatei kompatibel sind. Hardware, die über den ONVIF-Treiber hinzugefügt wird, finden Sie unter **Sonstige**, und nicht unter dem Namen ihres Herstellers.

6. Die letzte Seite zeigt das Ergebnis. Wenn das System die Firmware nicht aktualisieren konnte, klicken Sie auf **Fehlgeschlagen** neben dem Hardwaregerät, um die Begründung angezeigt zu bekommen.

> Milestone übernimmt keine Verantwortung für Fehlfunktionen von Hardwaregeräten, wenn inkompatible Firmware-Dateien oder Hardwaregeräte ausgewählt werden.

### Fügen Sie einen externen IDP hinzu und konfigurieren Sie ihn

1. Wählen Sie in Management Client **Extras** > **Optionen** und öffnen Sie die Registerkarte externer **IDP**.
2. Wählen Sie im Abschnitt **externer IDP** die Option **Hinzufügen**.
3. Geben Sie die Informationen für den externen IDP ein. Weitere Informationen zu den erforderlichen Informationen finden Sie unter Externer IDP.

Informationen darüber, wie Sie registrieren können, welche Ansprüche aus dem externen IDP Sie im VMS verwenden möchten, finden Sie unter Registrieren von Ansprüchen aus einem externen IDP.

## Geräte - Gruppen

### Eine Gerätegruppe hinzufügen

1. Klicken Sie im **Übersicht** Fenster mit der rechten Maustaste auf den Gerätetypen unter dem Sie eine Gerätegruppe erstellen möchten.
2. Wählen Sie **Gerätegruppe hinzufügen**.
3. Im Dialogfenster **Gerätegruppe hinzufügen** können Sie Namen und Beschreibung der neuen Gerätegruppe festlegen:


   Die Beschreibung erscheint, wenn sie den Mauszeiger über die Gerätegruppe in der Gerätegruppenliste halten.
4. Klicken Sie auf **OK**. Ein Ordner für die neue Gerätegruppe erscheint in der Liste.
5. Geben Sie weiter an, welche Geräte die Gerätegruppe enthalten soll (siehe Bestimmen, welche Geräte die Gruppe beinhalten soll auf Seite 241).

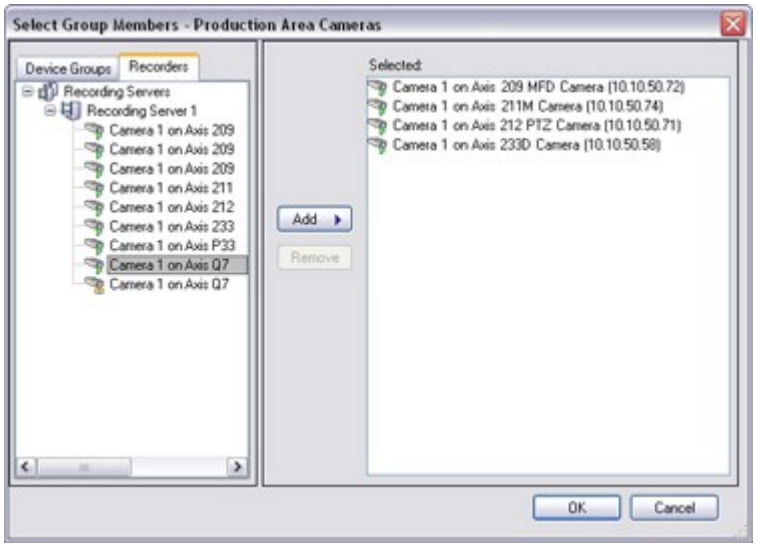
### Bestimmen, welche Geräte die Gruppe beinhalten soll

1. Klicken Sie im **Übersicht** Fenster mit der rechten Maustaste auf den zugehörigen Gerätegruppen-Ordner.
2. Wählen Sie **Mitglieder der Gerätegruppe bearbeiten**.

3. Im Fenster **Gruppenmitglieder auswählen**, wählen Sie eine der Registerkarten, um den Standort des Geräts festzustellen.

   Ein Gerät kann Mitglied mehrerer Gerätegruppen sein.

4. Wählen Sie die einzuschließenden Geräte aus, und klicken Sie auf **Hinzufügen** oder machen Sie einen Doppelklick auf das Gerät:




5. Klicken Sie auf **OK**.

6. Wenn Sie die Begrenzung von 400 Geräten in einer Gruppe überschreiten, können Sie Untergruppen zu den Gerätegruppen hinzufügen:


Geräte deaktiviert:

Deaktivierte Geräte werden standardmäßig nicht im Fenster **Übersicht** angezeigt.

Um alle deaktivierten Geräte anzuzeigen, klicken Sie oben im Fenster **Übersicht** auf **Filter** um die Registerkarte **Filter** zu öffnen, und wählen Sie **Deaktivierte Geräte anzeigen**.

Um deaktivierte Geräte wieder auszublenden, deaktivieren Sie die Option **Deaktivierte Geräte anzeigen**.

## Bestimmen Sie die allgemeinen Eigenschaften für alle Geräte in einer Gerätegruppe

Bei Gerätegruppen können Sie allgemeine Eigenschaften für alle Geräte in einer Gerätegruppe festlegen:

1. Klicken Sie auf die Gerätegruppe im **Übersicht** Bereich.

   Unter **Eigenschaften** sind alle Eigenschaften, **die für alle Geräte der Gruppe verfügbar sind** aufgelistet und in Registerkarten unterteilt.

2. Bestimmen Sie die allgemeinen Eigenschaften.

   In der **Einstellungen**-Registerkarte können Sie zwischen den Einstellungen für **alle** Geräte und Einstellungen für einzelne Geräte wechseln.

3. Klicken Sie in der Symbolleiste auf **Speichern**. Die Einstellungen werden auf den einzelnen Geräten und nicht in den Gerätegruppen gespeichert.

Geräte deaktiviert:

Deaktivierte Geräte werden standardmäßig nicht im Fenster **Übersicht** angezeigt.

Um alle deaktivierten Geräte anzuzeigen, klicken Sie oben im Fenster **Übersicht** auf **Filter** um die Registerkarte **Filter** zu öffnen, und wählen Sie **Deaktivierte Geräte anzeigen**.

Um deaktivierte Geräte wieder auszublenden, deaktivieren Sie die Option **Deaktivierte Geräte anzeigen**.

## Aktivieren/Deaktivieren von Geräten über Gerätegruppen

Sie können Geräte nur über die konfigurierte Hardware aktivieren/deaktivieren. Wenn sie nicht über den „Hardware hinzufügen“-Assistenten aktiviert/deaktiviert wurden, sind Kameragеräte standardmäßig aktiviert und alle anderen Geräte standardmäßig deaktiviert.

Deaktivierte Geräte werden standardmäßig nicht im Fenster **Übersicht** angezeigt.

Um alle deaktivierten Geräte anzuzeigen, klicken Sie oben im Fenster **Übersicht** auf **Filter** um die Registerkarte **Filter** zu öffnen, und wählen Sie **Deaktivierte Geräte anzeigen**.

Um deaktivierte Geräte wieder auszublenden, deaktivieren Sie die Option **Deaktivierte Geräte anzeigen**.

So finden Sie ein Gerät über die zu aktivierenden/deaktivierenden Gerätegruppen:

1. Wählen Sie im Bereich **Standort-Navigation** das Gerät aus.
2. Erweitern Sie im Bereich **Übersicht** die relevante Gruppe und suchen Sie das Gerät.
3. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie **Gehe zu Hardware**.
4. Klicken Sie auf den Plus-Knoten, um alle Geräte auf der Hardware anzuzeigen.
5. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie aktivieren/deaktivieren möchten, und wählen Sie **Aktiviert**.

# Geräte - Kameraeinstellungen

## Kameraeinstellungen anzeigen oder bearbeiten

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die jeweilige Kamera aus.
3. Öffnen Sie die Registerkarte **Einstellungen**.

Sie können Einstellungen anzeigen oder bearbeiten, wie etwa:

- Standardbildrate
- Auflösung
- Komprimierung
- Die maximale Anzahl an Bildern zwischen Keyframes
- Bildschirmanzeige Datum/Uhrzeit/Text für eine ausgewählte Kamera oder für alle Kameras in einer Gerätegruppe

Die Kameratreiber bestimmen den Inhalt der Registerkarte **Einstellungen**. Die Treiber variieren je nach Kameratyp.

Für Kameras, die mehr als einen Streamtyp unterstützen, z.B. MJPEG und MPEG-4/H.264/H.265, können Sie Multi-Streaming verwenden, siehe Multi-streaming verwalten auf Seite 251.

### Vorschau

Wenn Sie eine Einstellung verändern müssen, können Sie die Auswirkungen schnell überprüfen, wenn Sie den Bereich **Vorschau** aktiviert haben.

- Um die **Vorschau** zu verwenden, klicken Sie auf das Menü **Anzeigen**, und klicken Sie dann auf **Vorschaufenster**.

Sie können über den Bereich **Vorschau** keine Veränderungen der Bildrate erkennen, da die Miniaturansicht im Bereich **Vorschau** eine andere Bildrate nutzt, die im Dialogfeld **Optionen** festgelegt ist.

### Leistung

Wenn Sie die Einstellungen für die **Max. Bilder zwischen Keyframes** und **Max. Bilder zwischen Keyframes-Modus** ändern, kann die Leistung einiger Funktionen im XProtect Smart Client verringert werden. Der XProtect Smart Client benötigt beispielsweise einen Keyframe, um Video anzeigen zu können, also verzögert ein längerer Zeitraum zwischen den Keyframes das Starten von XProtect Smart Client.

### Hardware wird hinzugefügt

Weitere Informationen dazu, wie Sie Hardware zu Ihrem System hinzufügen können, finden Sie unter Hardware hinzufügen auf Seite 229.

## Unterstützung für Fischaugen-Linse aktivieren und deaktivieren

Die Unterstützung für Fischaugen-Linsen ist standardmäßig deaktiviert.

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Aktivieren oder deaktivieren Sie auf der Registerkarte **Fischaugenobjektiv** das Kontrollkästchen **Unterstützung für Fischaugenobjektiv aktivieren**.

Einstellungen für Fischaugen-Linse bestimmen

1. Wählen Sie auf der Registerkarte **Fischaugenobjektiv** den Objektivtyp aus.
2. Die physische Position/Ausrichtung der Kamera können Sie in der Liste **Kameraposition/Kameraausrichtung** bestimmen.
3. Wählen Sie eine Registered Panomorph Lens (RPL)-Nummer aus der Liste der **ImmerVision Enables® Panomorph-RPL-Nummern**.

   Dies gewährleistet eine ordnungsgemäße Identifikation und Konfiguration der Linse, die mit der Kamera verwendet wird. Sie finden normalerweise die RPL-Nummer auf der Linse selbst oder auf der Box mit der sie geliefert wurde. Einzelheiten zu ImmerVision, Panomorph-Objektiven und RPLs siehe die Website von Immervision (https://www.immervisionenables.com/).

   Wenn Sie das Objektivorofil **Allgemeine Entzerrung** auswählen, denken Sie daran, das gewünschte **Sichtfeld** zu konfigurieren.

# Geräte - Aufzeichnung

## Aufzeichnung aktivieren oder deaktivieren

Aufzeichnung ist standardmäßig aktiviert. Aufzeichnung aktivieren oder deaktivieren:

1. Wählen Sie im Bereich **Standort-Navigation Aufzeichnungsserver** aus.
2. Wählen Sie passende Gerät in der **Übersicht** aus.
3. In der **Aufzeichnen**-Registerkarte, wählen Sie das **Aufzeichnung**-Kontrollkästchen an oder ab.

Sie müssen die Aufzeichnung für das Gerät aktivieren, bevor Sie Daten mit der Kamera aufzeichnen können. Eine Regel zum Bestimmen der Umstände eines Geräts, bei denen es aufzeichnet, funktioniert nicht, wenn Sie die Aufzeichnung für das Gerät deaktiviert haben.

## Aktivieren der Aufzeichnung auf zugehörigen Geräten

Bei Kameras können Sie die Aufzeichnung zugehöriger Geräte aktivieren, wie zum Beispiel von Mikrofonen, die mit dem selben Aufzeichnungsserver verbunden sind. Dies bedeutet, dass zugehörige Geräte aufzeichnen, wenn die Kamera aufzeichnet.

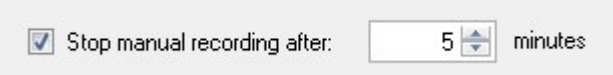
Die Aufzeichnung auf zugehörigen Geräten ist bei neuen Kameras standardmäßig aktiviert, kann jedoch nach Bedarf an- und ausgeschaltet werden. Bei bestehenden Kameras im System ist das Kontrollkästchen standardmäßig nicht angewählt.

1. Wählen Sie im Bereich **Standort-Navigation Aufzeichnungsserver** aus.
2. Wählen Sie die zugehörige Kamera im Bereich **Übersicht** aus.
3. Aktivieren oder deaktivieren Sie auf der Registerkarte **Aufzeichnen** das Kontrollkästchen **Auf den entsprechenden Geräten Aufzeichnen**.
4. In der **Client**-Registerkarte, bestimmen Sie die Geräte, die zu dieser Kamera gehören.

Wenn Sie die Aufzeichnung auf zugehörigen Geräten, die mit einem anderen Aufzeichnungsserver verbunden sind, aktivieren möchten, müssen Sie eine Regel erstellen.

## Manuelle Aufzeichnung verwalten

**Manuelle Aufzeichnung danach anhalten** ist standardmäßig mit einer Aufzeichnungszeit von fünf Minuten aktiviert. Dadurch ist gewährleistet, dass das System alle Aufzeichnungen anhält, die von den XProtect Smart Client-Benutzern gestartet wurden.




1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie passende Gerät in der **Übersicht** aus.
3. Aktivieren oder deaktivieren Sie auf der Registerkarte **Aufzeichnen** das Kontrollkästchen **Manuelle Aufzeichnung beenden nach**.

Bestimmen Sie eine Aufzeichnungszeit bei Aktivierung. Die Anzahl der festgelegten Minuten muss von ausreichender Größe sein, um den Anforderungen der verschiedenen manuellen Aufzeichnungen zu entsprechen, ohne dabei das System zu überladen.

Zu Rollen hinzufügen:

Sie müssen den Client-Benutzern auf jeder Kamera in **Rollen** auf der Registerkarte **Gerät** die Berechtigung erteilen, Aufzeichnungen manuell zu starten und zu beenden.

Bei Regeln verwenden:

Die verfügbaren Ereignisse bei der Erstellung von Regeln im Bezug auf manuelle Aufzeichnungen sind:

- Manuelle Aufzeichnung gestartet
- Manuelle Aufzeichnung gestoppt

## Bildrate der Aufzeichnung festlegen

Sie können die Bildrate der Aufzeichnung von JPEG festlegen.

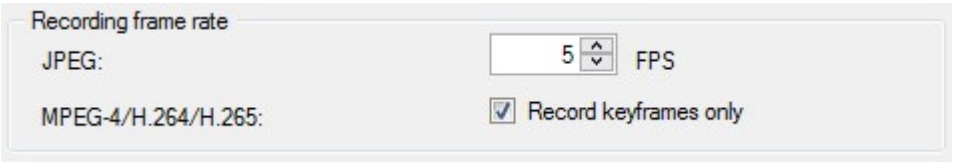
1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie passende Gerät in der **Übersicht** aus.
3. Auf der Registerkarte **Aufzeichnen**, in der **Framerate für Aufzeichnungen: die Box (JPEG)**, wählen Sie die Framerate für Aufzeichnungen (in FPS, Frames per Second) aus.


## Keyframe-Aufzeichnung aktivieren

Sie können die Keyframe-Aufzeichnung für MPEG-4/H.264/H.265-Streams aktivieren. Dies hat zur Folge, dass das System je nach Regeleinstellungen zwischen alleinigen Keyframe-Aufzeichnungen und Aufzeichnungen aller Bilder wechselt.

Sie können beispielsweise zum Sparen von Speicherplatz das System Keyframes aufzeichnen lassen, wenn keine Bewegung in Sicht ist und zu allen Bildern wechseln, wenn Bewegung erkannt wird.

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie passende Gerät in der **Übersicht** aus.
3. Aktivieren Sie auf der Registerkarte **Aufzeichnung** das Kontrollkästchen **Nur Keyframes aufzeichnen**.




4. Erstellen Sie eine Regel, nach der die Funktion aktiviert wird, siehe Aktionen und Stoppaktionen.

## Aktivieren der Aufzeichnung auf zugehörigen Geräten

Bei Kameras können Sie die Aufzeichnung zugehöriger Geräte aktivieren, wie zum Beispiel von Mikrofonen, die mit dem selben Aufzeichnungsserver verbunden sind. Dies bedeutet, dass zugehörige Geräte aufzeichnen, wenn die Kamera aufzeichnet.

Die Aufzeichnung auf zugehörigen Geräten ist bei neuen Kameras standardmäßig aktiviert, kann jedoch nach Bedarf an- und ausgeschaltet werden. Bei bestehenden Kameras im System ist das Kontrollkästchen standardmäßig nicht angewählt.

1. Wählen Sie im Bereich **Standort-Navigation Aufzeichnungsserver** aus.
2. Wählen Sie die zugehörige Kamera im Bereich **Übersicht** aus.
3. Aktivieren oder deaktivieren Sie auf der Registerkarte **Aufzeichnen** das Kontrollkästchen **Auf den entsprechenden Geräten Aufzeichnen**.
4. In der **Client**-Registerkarte, bestimmen Sie die Geräte, die zu dieser Kamera gehören.

Wenn Sie die Aufzeichnung auf zugehörigen Geräten, die mit einem anderen Aufzeichnungsserver verbunden sind, aktivieren möchten, müssen Sie eine Regel erstellen.

## Fernaufzeichnungen abspeichern und abrufen

Damit im Fall von Netzwerkproblemen alle Fernaufzeichnungen gespeichert werden, können Sie das automatische Abrufen von Aufzeichnungen nach Wiederherstellung der Verbindung aktivieren.

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie passende Gerät in der **Übersicht** aus.
3. Wählen Sie Unter **Fernaufzeichnungen** die Option **Fernaufzeichnungen nach Wiederherstellung der Verbindung automatisch abrufen** aus. Dann können Aufzeichnungen nach Wiederherstellung der Verbindung automatisch abgerufen werden

> Die Option der Fernaufzeichnung steht nur zur Verfügung, wenn die ausgewählte Kamera lokalen Speicher unterstützt oder eine Kamera mit einer Milestone Interconnect-Einstellung ist.

Die Art der ausgewählten Hardware bestimmt woher Aufzeichnungen bezogen werden:

- Bei einer Kamera mit lokalem Aufzeichnungsspeicherort werden die Aufzeichnungen von diesem lokalen Aufzeichnungsspeicherort abgerufen
- Bei einem Milestone Interconnect-Remote-Systeminstallation werden Aufzeichnungen von den Aufzeichnungsservern dieses Systems abgerufen

Sie können die folgende Funktion unabhängig vom automatischen Abruf verwenden:

- Manuelle Aufzeichnung
- Die **Abrufen und Speichern der Fernaufzeichnungen von <Geräte>** Regel
- Die Regel **Abrufen und Speichern der Fernaufzeichnungen zwischen <Start- und Endzeit> von <Geräte>**

### Aufzeichnungen löschen

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wenn Sie im Bereich **Übersicht** das entsprechende Gerät aus und wählen Sie die Registerkarte **Aufzeichnung** aus.
3. Klicken Sie auf die Schaltfläche **Alle Aufzeichnungen löschen**, um alle Aufzeichnungen für das Gerät oder die Gerätegruppe zu löschen.

Diese Methode kann nur verwendet werden, wenn Sie alle Geräte in der Gruppe zum selben Server hinzugefügt haben. Geschützte Daten werden nicht gelöscht.

## Geräte - Streaming

### Adaptives Streaming (Erklärung)

Adaptives Streaming ist eine Streaming-Methode, die verwendet wird, wenn mehrere Live-Video-Streams in der gleichen Ansicht angezeigt werden. Sie ermöglicht es den Clients, automatisch die Live-Video-Streams auszuwählen, die in ihrer Auflösung am besten zu den von den Ansichtselementen angeforderten Streams passen. Adaptives Streaming reduziert die Netzlast und verbessert die Dekodierfähigkeit und Leistung des Client-Computers.

Wenn Sie das adaptive Streaming in XProtect Smart Client aktivieren, können Sie die bestmögliche Übereinstimmung der verfügbaren Video-Streams mit der von einem Ansichtselement angeforderten Auflösung einstellen. Weitere Informationen finden Sie unter Aktivieren von adaptivem Streaming.

In XProtect Smart Client kann das adaptive Streaming sowohl im Live- als auch im Wiedergabemodus angewendet werden. Auf den mobilen Clients ist sie nur im Live-Modus verfügbar.

Bei der Anwendung im Wiedergabemodus wird die Streaming-Methode als adaptive Wiedergabe bezeichnet. Weitere Informationen finden Sie unter Adaptive Wiedergabe (erklärt) auf Seite 249

### Adaptive Wiedergabe (erklärt)

Adaptive Wiedergabe ist eine Konfiguration, die die Verwendung von adaptivem Streaming im Wiedergabemodus ermöglicht.

Für die adaptive Wiedergabe sind zwei Aufzeichnungsströme erforderlich, ein primärer und ein sekundärer Strom. Wenn beide Streams in Management Client aktiviert sind, werden beide Streams aufgezeichnet.

- Wenn Sie Videos aus einem Zeitraum wiedergeben, bevor die sekundäre Aufzeichnung konfiguriert wurde, werden nur die primären Aufzeichnungen wiedergegeben.
- Wenn Sie Videos wiedergeben, die nach der Konfiguration der sekundären Aufzeichnung aufgezeichnet wurden, wird das Video von der primären oder der sekundären Aufzeichnung wiedergegeben, je nachdem, was am besten zur Ansichtsgröße des Clients passt.

Verfügbarkeit

> Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Adaptives Streamen aktivieren

Sie können die adaptive Wiedergabe zusammen mit dem adaptiven Streaming auf der Registerkarte **Erweitert** in den **Smart ClientProfilen** aktivieren, und sie muss auch in XProtect Smart Client unter **Einstellungen** > **Erweitert** > **Adaptives Streaming** aktiviert werden. Weitere Informationen zum Aktivieren von adaptivem Streaming in XProtect Smart Client finden Sie unter Aktivieren des adaptiven Streamings

Fernaufzeichnung

Optional können Sie Fernaufzeichnungen für die adaptive Wiedergabe verwenden. Fernaufzeichnungen ermöglichen es Ihnen, Sequenzen eines Streams mit einer anderen, in der Regel höheren Auflösung als der Rest des Streams anzusehen. So können Sie beispielsweise einen primären Stream mit einer niedrigen Auflösung aufzeichnen und die Aufzeichnungen einer hochauflösenden Quelle zusammenführen. Sie können die zusammengefassten lokalen Aufzeichnungen beim Durchsuchen der Daten aktivieren.

Fernaufzeichnungen werden in der Mediendatenbank gespeichert, und die Auflösung dieser Aufzeichnungen wird an den einzelnen Kameras eingestellt.

Auflösung des wiedergegebenen Videos

Bei der adaptiven Wiedergabe wird die Auflösung des wiedergegebenen Videos durch die aktuellen Auflösungseinstellungen für die primäre und die sekundäre Aufzeichnung bestimmt. Das heißt, dass bei der Wiedergabe die Wahl zwischen dem primären und dem sekundären Stream von der Auflösung abhängt, die derzeit für die jeweiligen Aufzeichnungsströme eingestellt ist.

## Stream hinzufügen

Die Streams, die Sie zur Aufzeichnung hinzufügen, können im Live- und im Wiedergabemodus angezeigt werden.

Sie können das aufgezeichnete Video auch in Ihre Ansichtselement mit aktiviertem adaptivem Streaming ansehen. Adaptives Streaming im Wiedergabemodus wird als adaptive Wiedergabe bezeichnet.

1. Klicken Sie auf die Registerkarte **Streams** auf **Hinzufügen**. Ein zweiter Stream wird zur Liste hinzugefügt.
2. Bearbeiten Sie in der Spalte **Name** den Namen des Streams. Der Name erscheint in XProtect Smart Client.

3. Wählen Sie in der Spalte **Live-Modus** aus, wann Live-Streaming erforderlich ist:
   - **Immer**: Der Stream läuft, auch wenn keine XProtect Smart Client-Benutzer den Stream anfordern.
   - **Niemals**: Der Stream ist ausgeschaltet. Verwenden Sie diese Option nur für Aufzeichnungsstreams, z. B., wenn Sie Aufzeichnungen in hoher Qualität und die Bandbreite benötigen
   - **Bei Bedarf**: Der Stream startet, wenn er von einem beliebigen Client angefordert wird oder wenn der Stream auf Aufzeichnung eingestellt ist
4. Wählen Sie in der Spalte **Standard-Livestream** den Stream aus, der standardmäßig verwendet werden soll, wenn der Client keinen bestimmten Stream anfordert und das adaptive Streaming deaktiviert ist.
5. Wählen Sie in der Spalte **Aufzeichnung** entweder **Primär** oder **Sekundär**. Für die adaptive Wiedergabe müssen Sie von jedem Typ einen Stream erstellen. Das wiedergegebene Video stammt aus dem primären Video-Stream und wird bei Bedarf durch sekundäres Streaming ergänzt. Es muss immer eine Primäraufzeichnung vorhanden sein. Außerdem wird der Stream, den Sie als **Primär** konfigurieren, in verschiedenen Kontexten verwendet, z. B. für die Bewegungserkennung und für den Export aus XProtect Smart Client.
6. Wählen Sie unter **Standardwiedergabe**aus, welcher Stream standardmäßig wiedergegeben werden soll. Wenn die adaptive Wiedergabe nicht konfiguriert ist, wird der Standard-Stream an den Client geliefert.
7. Aktivieren Sie in der Spalte **Fernaufzeichnung verwenden** das Kontrollkästchen, wenn Sie die Fernaufzeichnung verwenden möchten. Weitere Informationen zu Randaufzeichnungen finden Sie unter Fernaufzeichnung auf Seite 250.
8. Klicken Sie auf **Speichern**.

Wenn Sie möchten, dass die Streams überhaupt nicht ausgeführt werden, es sei denn, jemand sieht sich Live-Bilder an, können Sie die **Standardregel - Start des Feeds** anpassen, damit mit dem vordefinierten Ereignis **Live-Client-Feed angefordert** bei Bedarf gestartet wird.

## Multi-streaming verwalten

Zum Betrachten von Live-Videoaufnahmen und zum Abspielen von aufgezeichneten Videos ist nicht unbedingt die gleiche Videoqualität und Bildfrequenz erforderlich.

### Um zu ändern, welcher Stream zum Aufzeichnen verwendet werden soll

Für die adaptive Wiedergabe müssen zwei Streams auf Aufzeichnung eingestellt werden, ein primärer und ein sekundärer Stream. Für das Live-Streaming können Sie so viele Live-Streams einrichten und nutzen, wie die Kamera unterstützt.

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie im Bereich **Übersicht** die jeweilige Kamera aus.
3. Wählen Sie auf der Registerkarte **Streams** den Stream aus, den Sie für die Aufzeichnung verwenden möchten.
4. Wählen Sie die entsprechende Option in der **Live-Modus** Liste. Die Optionen **Bei Bedarf**, **Immer** und **Nie** geben an, wann der Stream im Client angewendet werden soll. Wenn vom Client nichts angefordert wird, wird für die Aufzeichnung der Stream verwendet, bei dem das Kontrollkästchen **Standard-Livestream** aktiviert ist.
5. Um auf einem Stream aufzuzeichnen, wählen Sie entweder **Primär** oder **Sekundär** in der **Aufzeichnungsliste** aus.
6. Um die adaptive Wiedergabe zu verwenden, richten Sie zwei Streams ein und setzen einen der Streams auf **Primär** und den anderen auf **Sekundär**.
7. Um auf einem Stream aufzuzeichnen, wählen Sie entweder den **primären** oder den **sekundären** Stream in der **Aufzeichnungsliste** aus.

### Datenübertragung begrenzen

Sie können mehrere Bedingungen festlegen, damit Videostreams nur dann ausgeführt werden, wenn diese von einem Client betrachtet werden.

Zur Handhabung des Streamings und zur Begrenzung unnötiger Datenübertragungen beginnt das Streaming nicht, wenn die folgenden Bedingungen erfüllt sind:

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie im Bereich **Übersicht** die jeweilige Kamera aus.
3. Wählen Sie auf der Registerkarte **Streams** auf der Liste **Live-Modus** die Option **Bei Bedarf** aus.
4. Aktivieren oder deaktivieren Sie auf der Registerkarte **Aufzeichnen** das Kontrollkästchen **Aufzeichnung**.
5. Deaktivieren Sie auf der Registerkarte **Bewegung** das Kontrollkästchen **Bewegungserkennung**.

Wenn diese Bedingungen erfüllt sind, werden Videosequenzen nur ausgeführt, wenn diese von einem Client angesehen werden.

#### Beispiele

**Beispiel 1, Live-Videos und Videoaufzeichnungen**:

- Für die Anzeige von **Live**-Video bevorzugt Ihre Organisation möglicherweise H.264 bei hoher Bildrate
- Für die Wiedergabe von **Videoaufzeichnungen** bevorzugt Ihre Organisation zur Einsparung von Festplattenspeicher evtl. MJPEG mit einer niedrigeren Bildrate

**Beispiel 2, lokal und fernaufgezeichnete Live-Videos**:

- Für die Anzeige von **Live-Video von einem lokalen Betriebspunkt** bevorzugt Ihre Organisation evtl. H.264 mit hoher Bildrate, um die bestmögliche Videoqualität zu erhalten
- Für die Anzeige von **Live-Video von einem über Fernzugriff verbundenen Betriebspunkt** bevorzugt Ihre Organisation evt. MJPEG mit niedrigerer Bildrate und Qualität, um Netzwerk-Bandbreite einzusparen

**Beispiel 3, adaptives Streaming**:

- Zur Anzeige von **Live-Video und zur Senkung der Arbeitsbelastung der CPU und GPU des XProtect Smart Client Computers** bevorzugt Ihre Organisation evtl. H.264/H.265 mit mehreren hohen Bildraten in unterschiedlicher Auflösung, die bei Verwendung von adaptivem Streaming der von XProtect Smart Client geforderten Auflösung entspricht. Weitere Informationen finden Sie unter Smart Client Profile (Client-Knoten) auf Seite 505.

Wenn Sie **Live Multicast** auf der Registerkarte **Client** der Kamera aktivieren (siehe die Registerkarte Client (Geräte)), so funktioniert dies nur auf dem Standard -Videostream.

Selbst wenn Kameras Multi-Streaming unterstützen, können die Multi-Streaming-Kapazitäten zwischen den einzelnen Kameras variieren. Weitere Informationen finden Sie in der Kameradokumentation.

Ob eine Kamera verschiedene Typen von Streams bietet, sehen Sie auf der Registerkarte **Einstellungen (Geräte)**.

# Geräte - Speicher

## Verwalten von Voralarm-Puffern

Kameras, Mikrofone und Lautsprecher unterstützen Voralarm-Puffern. Bei Lautsprechern werden die Streams nur gesendet, wenn der XProtect Smart Client-Benutzer die Funktion **Ausgabe Lautsprecher** verwendet. Dies hat zur Folge, dass je nachdem wie Ihre Lautsprecher-Streams ausgelöst werden, keine oder nur geringes Voralarm-Puffern zur Verfügung steht.

In den meisten Fällen werden Lautsprecher darauf eingestellt, die Aufzeichnung zu beginnen, wenn der XProtect Smart Client-Benutzer die Funktion **Ausgabe Lautsprecher** verwendet. In solchen Fällen steht der Voralarm-Puffer für Lautsprecher nicht zur Verfügung.

Für die Verwendung der Voralarm-Puffer-Funktion müssen die Geräte aktiviert sein und einen Stream an das System senden.

### Aktivieren und Deaktivieren der Vorpufferung

Das Voralarm-Puffern wird standardmäßig mit einem Voralarm-Puffer von drei Sekunden aktiviert und dem Speicherort im Speicher.

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie passende Gerät in der **Übersicht** aus.
3. Aktivieren oder Deaktivieren Sie auf der Registerkarte **Aufzeichnen** das Kontrollkästchen **Pre-buffer**.
4. In der **Client**-Registerkarte, bestimmen Sie die Geräte, die zu dieser Kamera gehören.

### Angabe des Speicherortes und des Vorpufferzeitraums

Temporäre Voralarm-Puffer-Aufzeichnungen werden entweder im Speicher oder auf der Festplatte gespeichert:

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie im Bereich **Übersicht** das entsprechende Gerät aus wählen Sie dann die Registerkarte **Aufzeichnung**.
3. Wählen Sie auf der Liste **Speicherort** die Option **Speicher** oder **Festplatte** und geben Sie die Anzahl Sekunden an.
4. Wenn Sie einen Voralarm-Puffer-Zeitraum benötigen, der 15 Sekunden überschreitet, wählen Sie **Festplatte**.

Die Anzahl der festgelegten Sekunden muss groß genug sein, um den in den verschiedenen Aufzeichnungsregeln gesetzten Anforderungen zu entsprechen.

Wenn Sie den Standort zu **Speicher** ändern, senkt das System den Zeitraum automatisch auf 15 Sekunden.

### Verwendung von Vorpufferung in Regeln

Bei der Erstellung von Regeln, welche eine Aufzeichnung auslösen, können Sie die Option wählen, dass Aufzeichnungen einige Zeit vor dem eigentlichen Ereignis starten (Voralarm-Puffer).

**Beispiel**: Die nachfolgende Regel legt fest, dass eine Aufzeichnung der Kamera beginnen soll, wenn 5 Sekunden vorher Bewegung von der Kamera erkannt wird.

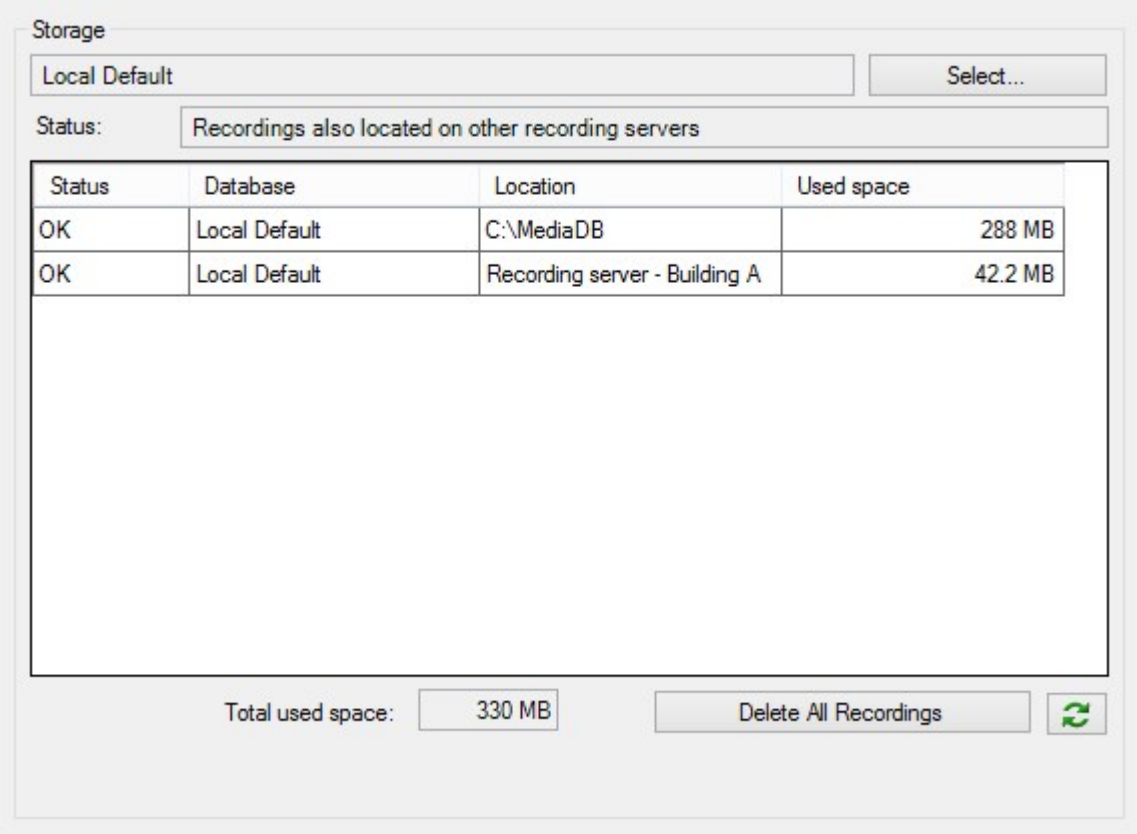

Sie müssen auf dem aufzeichnenden Gerät das Voralarm-Puffern aktivieren und die Länge des Voralarm-Puffers mindestens mit der in der Regel festgelegten Länge abgleichen, um die Voralarm-Puffer-Aufzeichnungsfunktion in der Regel zu verwenden.

## Status von Datenbanken für Geräte beobachten

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wenn Sie im Bereich **Übersicht** das entsprechende Gerät aus und wählen Sie die Registerkarte **Aufzeichnung** aus.

Unter **Speicherort** können sie Datenbanken für ein Gerät oder eine Gerätegruppe, die zum gleichen Aufzeichnungsserver gehören, überwachen und verwalten.

Über der Tabelle wird die ausgewählte Datenbank und ihr Status angezeigt. In diesem Beispiel ist die ausgewählte Datenbank der **Lokale Standard** und der Status sind **Aufzeichnungen, die sich auch auf anderen Aufzeichnungsservern befinden**. Der andere Server ist der Aufzeichnungsserver in Gebäude A.




**Mögliche Status für die ausgewählte Datenbank**

| Name | Beschreibung |
|---|---|
| **Aufzeichnungen befanden sich auch auf anderen Aufzeichnungsservern** | Die Datenbank ist aktiv und wird ausgeführt und besitzt auch Aufzeichnungen an Speicherorten auf anderen |

| Name | Beschreibung |
|---|---|
| | Aufzeichnungsservern. |
| **Archive befinden sich auch am alten Speicherort** | Die Datenbank ist aktiv und wird ausgeführt und besitzt auch Archive an anderen Speicherorten. |
| **Aktiv** | Die Datenbank ist aktiv und wird ausgeführt. |
| **Die Daten für einige der ausgewählten Geräte werden zurzeit an einen anderen Speicherort verschoben** | Die Datenbank ist aktiv und wird ausgeführt und das System bewegt Daten für ein oder mehrere ausgewählte Geräte in einer Gruppe von einem Standort zum anderen. |
| **Die Daten für das Gerät werden gerade an einen anderen Speicherort verschoben** | Die Datenbank ist aktiv und wird ausgeführt und das System bewegt Daten für ein oder mehrere ausgewählte Geräte in einer Gruppe von einem Standort zum anderen. |
| **Informationen nicht verfügbar im Failover-Modus** | Das System kann keine Statusinformationen über die Datenbank sammeln, wenn sich die Datenbank im Failover-Modus befindet. |

Weiter unten im Fenster können Sie den Status jeder Datenbank sehen (**OK**, **Offline** oder **Alter Speicherort**), den Standort jeder Datenbank und wie viel Speicherplatz diese verwenden.

Sie können im Feld **Gesamter genutzter Speicherplatz** den gesamten genutzten Speicherplatz am Speicherort sehen, wenn alle Server online sind.

Weitere Informationen zur Konfiguration des Speichers finden Sie auf der Registerkarte Speicher (Aufzeichnungsserver).

## Geräte von einem Speichermedium zum anderen verschieben

Wenn Sie einen neuen Speicherort für Aufzeichnungen auswählen, werden vorhandene Aufzeichnungen nicht mit umgezogen. Diese verbleiben am aktuellen Speicherort zu den Bedingungen, die durch die Konfiguration des Speichers vorgegeben werden, zu dem sie gehören.

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wenn Sie im Bereich **Übersicht** das entsprechende Gerät aus und wählen Sie die Registerkarte **Aufzeichnung** aus.

3. Klicken Sie auf **Auswählen...** unter **Speicher**, um ein Speichermedium für Aufzeichnungen auszuwählen, auf dem Ihre Geräte ihre Aufzeichnungen ablegen können.

Die Aufzeichnungen werden entsprechend der Konfiguration für die Speichermedien archiviert, die Sie auswählen.

# Geräte - Bewegungserkennung

## Bewegungserkennung (Erklärung)

Die Konfiguration der Bewegungserkennung ist ein Schlüsselelement in Ihrem System: Die Konfiguration der Bewegungserkennung bestimmt, wann das System Bewegungsereignisse erstellt und wann Video aufgezeichnet wird.

Beispielsweise hilft die optimale Konfiguration der Bewegungserkennung jeder Kamera später dabei, unnötige Aufzeichnungen zu vermeiden. Je nach physischem Standort der Kamera könnte es von Vorteil sein, die Einstellungen der Bewegungserkennung unter verschiedenen Voraussetzungen, wie z. B. Tages-/Nachtzeit und windiges/ruhiges Wetter, zu testen.

Sie können Einstellungen vornehmen, die im Bezug zur Anzahl der benötigten Änderungen in der Sicht einer Kamera stehen, um die Änderung als Bewegung erkennen zu lassen. Sie können z.B. Intervalle zwischen Bewegungserkennungsanalysen und Bereichen der Ansicht vorgeben, in denen Bewegung ignoriert werden soll. Sie können auch die Genauigkeit der Bewegungserkennung anpassen und dadurch die Last auf die Systemressourcen.

### Bildqualität

Bevor Sie für eine Kamera die Bewegungserkennung konfigurieren, empfiehlt Ihnen Milestone, zuvor die Einstellungen für die Bildqualität der Kamera zu konfigurieren, z.B. die Auflösung, das Video-Codec und die Stream-Einstellungen. Dies können Sie für das Gerät auf der Registerkarte **Einstellungen** in dem Fenster **Eigenschaften** tun. Wenn Sie später die Einstellungen der Bildqualität ändern, sollten Sie die Konfiguration der Bewegungserkennung danach unbedingt testen.

### Verdeckte Bildbereiche

In Bereichen mit dauerhaft verdeckten Bildbereichen findet keine Bewegungserkennung statt.

## Aktivieren und Deaktivieren von Bewegungserkennung

### Geben Sie die Standardeinstellungen für die Bewegungserkennung für Kameras an

1. Klicken Sie im Menü **Extras** auf **Optionen**.
2. Aktivieren Sie auf der Registerkarte **Allgemein** unter **Beim Hinzufügen neuer Kamerageräte automatisch aktivieren** das Kontrollkästchen **Bewegungserkennung**.

### Bewegungserkennung für eine bestimmte Kamera aktivieren oder deaktivieren

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die jeweilige Kamera aus.
3. Aktivieren oder Deaktivieren Sie auf der Registerkarte **Bewegung** das Kontrollkästchen **Bewegungserkennung**.

> Bei Deaktivierung der Bewegungserkennung für eine Kamera, funktionieren Regeln bezüglich der Bewegungserkennung für diese Kamera nicht.

## Hardwarebeschleunigung aktivieren oder deaktivieren

Die automatische, hardwarebeschleunigte Videodekodierung zur Bewegungserkennung ist die Standardeinstellung, wenn Sie eine Kamera hinzufügen. Der Aufzeichnungsserver verwendet ggf. GPU-Ressourcen. Dies reduziert die CPU-Last während der Videobewegungsanalyse und verbessert die allgemeine Leistung des Aufzeichnungsservers.

### Zum Aktivieren oder Deaktivieren der Hardwarebeschleunigung

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie im Bereich **Übersicht** die jeweilige Kamera aus.
3. Wählen Sie auf der Registerkarte **Bewegung** unter **Hardwarebeschleunigung** die Option **Automatik** aus, um die Hardwarebeschleunigung zu aktivieren, oder wählen Sie **Aus**, um die Einstellung zu deaktivieren.

#### Verwendung von GPU-Ressourcen

Die hardwarebeschleunigte Videodekodierung zur Bewegungserkennung verwendet GPU-Ressourcen bei:

- Intel-CPUs, die Intel Quick Sync unterstützen
- NVIDIA® an Ihren Aufzeichnungsserver angeschlossene Grafikkarten

### Lastausgleich und Leistung

Der Lastenausgleich zwischen den verschiedenen Ressourcen erfolgt automatisch. In dem **Systemmonitor** Knoten können Sie überprüfen, ob die aktuelle Bewegungsanalysen-Last der NVIDIA GPU-Ressourcen innerhalb der angegebenen Grenzen von dem **Systemmonitor Schwellenwerten** Knoten liegt. Die NVIDIA GPU-Lastenanzeigen sind:

- NVIDIA-Dekodierung
- NVIDIA-Speicher
- NVIDIA-Rendering

Wenn die Last zu hoch ist, können Sie GPU-Ressourcen zu Ihrem Recording-Server hinzufügen, indem Sie mehrfache NVIDIA Displayadapter installieren. Milestone empfiehlt nicht die Verwendung der Scalable Link-Interface (SLI)-Konfiguration Ihrer NVIDIA-Grafikkarten.

NVIDIA-Produkte haben unterschiedliche Rechenleistungen.

Für die hardwarebeschleunigte Videodekodierung zur Bewegungserkennung mit GPUs von NVIDIA ist die Compute-Fähigkeit in der Version 6.x (Pascal) oder neuer erforderlich.

- Die Version der Compute-Fähigkeit für Ihr NVIDIA-Produkt finden Sie auf der Website von NVIDIA (https://developer.nvidia.com/cuda-gpus/).
- Um zu sehen, ob die Videobewegungserkennung für eine bestimmte Kamera hardwarebeschleunigt ist, aktivieren Sie die Protokollierung in der Protokolldatei des Aufzeichnungsservers. Stellen Sie die Ebene auf **Debug** ein. Diagnosen werden in DeviceHandling.log protokolliert. Das Protokoll folgt dem Muster: [zeit] [274] DEBUG – [guid] [Name] Konfigurierte Decodierung: Automatisch: Tatsächliche Decodierung: Intel/NVIDIA

Die BS-Version des Aufzeichnungsservers und die CPU-Generation können die Leistung hardwarebeschleunigter Videobewegungserkennung beeinflussen. Bei älteren Versionen ist die GPU-Speicherzuweisung oft das Nadelöhr (der typische Grenzwert liegt zwischen 0,5 GB und 1,7 GB).

Auf Windows 10/Server 2016 basierende Systeme und CPUs der sechsten Generation (Skylake) oder höher können 50 % des Systemspeichers der GPU zuweisen und dadurch dieses Nadelöhr eliminieren oder reduzieren.

Intel-CPUs der sechsten Generation bieten hardwarebeschleunigte Dekodierung von H.265. Dadurch ist die Leistung für diese CPU-Versionen mit H.264 vergleichbar.

## Manuelle Empfindlichkeit für die Definition von Bewegung aktivieren

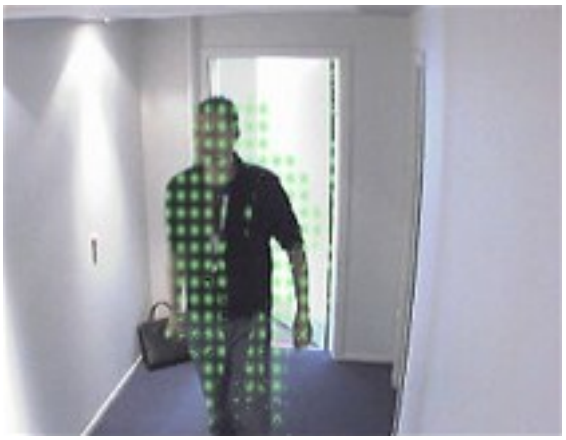
Die Empfindlichkeitseinstellung legt fest, **wie sehr sich ein Pixel** in den Bildern der Kamera verändern muss, bevor dies als Bewegung registriert wird.

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und dann **Kameras**.
2. Wählen Sie im Bereich **Übersicht** die jeweilige Kamera aus.
3. Wählen Sie das Kontrollkästchen **Manuelle Empfindlichkeit** in der Registerkarte **Bewegung** aus.
4. Ziehen Sie den Schieberegler nach links für eine höhere Empfindlichkeit und nach rechts für eine niedrigere Empfindlichkeit.

   Je **höher** die Empfindlichkeit, desto weniger Veränderungen sind in jedem Pixel erlaubt, bevor es als Bewegung registriert wird.

   Je **niedriger** die Empfindlichkeit, desto mehr Veränderungen sind in jedem Pixel erlaubt, bevor es als Bewegung registriert wird.

   Pixel in denen Bewegung erkannt wird, werden im Vorschaubild Grün hervorgehoben.
5. Wählen Sie eine Position für den Schieberegler aus, bei der nur Erkennungen hervorgehoben werden, die Sie als Bewegungen erachten.



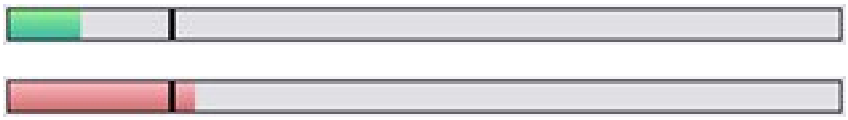
Anhand der Zahl an der rechten Seite des Schiebereglers, können Sie die genaue Empfindlichkeit zwischen Kameras vergleichen und einstellen.

## Geben Sie eine Schwelle für Bewegungen an

Die Bewegungserkennung bestimmt, **wie viele Pixel** sich im Bild verändern müssen, bevor dies als Bewegung registriert wird.

1. Ziehen Sie den Schieberegler nach links für eine höhere Bewegungsrate und nach rechts für eine niedrigere Bewegungsrate.
2. Wählen Sie eine Position für den Schieberegler aus, bei der nur Erkennungen registriert werden, die Sie als Bewegungen erachten.

Die schwarze vertikale Linie in der Bewegungsanzeigeleiste zeigt den Schwellenwert der Bewegungserkennung: Wenn die erkannte Bewegung über dem ausgewählten Schwellenwert liegt, verändert sich die Farbe des Balkens von Grün zu Rot und zeigt so eine positive Erkennung an.



Bewegungsanzeigeleiste: wechselt die Farbe von Grün auf Rot, wenn Schwellenwert überschritten wird und zeigt so eine positive Bewegungserkennung an.

## Geben Sie für die Bewegungserkennung Ausschlussbreiche an

Sie können alle Einstellungen für eine komplette Gruppe Kameras einstellen, jedoch bietet es sich an, die Ausnahmebereiche pro Kamera festzulegen.

> Bereiche mit permanenten Privatzonenmasken sind auch von der Bewegungserkennung ausgeschlossen. Wählen Sie das Kontrollkästchen **Privatzonenmasken zeigen**, um sie anzuzeigen.

Die Deaktivierung der Bewegungserkennung in bestimmten Bereichen hilft Ihnen die Erkennung irrelevanter Bewegungen zu vermeiden, z. B. wenn die Kamera einen Bereich abdeckt, in dem sich ein Baum im Wind bewegt oder Autos regelmäßig im Hintergrund vorbeifahren.

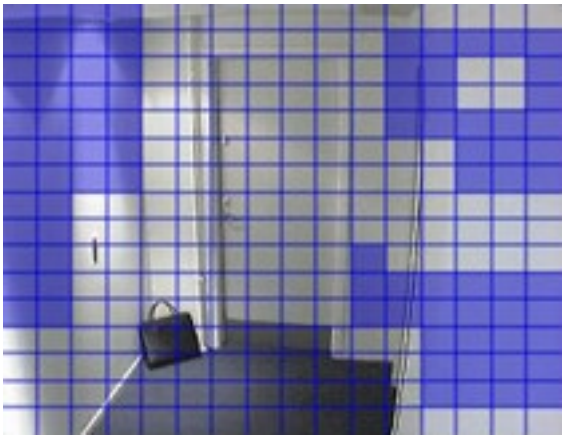
Bei der Verwendung von Ausschlussbereichen mit PTZ-Kameras und der Anwendung von Pan/Tilt/Zoom auf die Kamera, wird der Ausschlussbereich **nicht** entsprechend bewegt, da der Bereich im Bild der Kamera festgestellt wird und nicht am Objekt.

1. Für die Verwendung von Ausschlussbereichen, wählen Sie das Kontrollkästchen **Ausschlussbereiche verwenden** an.

   Ein Raster teilt das Vorschaubild in auswählbare Abschnitte.

2. Ziehen Sie den Mauszeiger mit gedrückter linker Maustaste über die erforderlichen Bereiche im Vorschaubild, um Ausschlussbereiche festzulegen. Die rechte Maustaste leert einen Rasterabschnitt.

Sie können so viele Ausschlussbereiche festlegen, wie Sie benötigen. Ausschlussbereiche werden in blau angezeigt:



Die blauen Ausschlussbereiche werden nur im Vorschaubild in der Registerkarte **Bewegung** angezeigt und nicht in einem anderen Vorschaubild oder im Management Client oder Access Client.

# Geräte - voreingestellte Kamerapositionen

## Als Ausgangsposition setzen

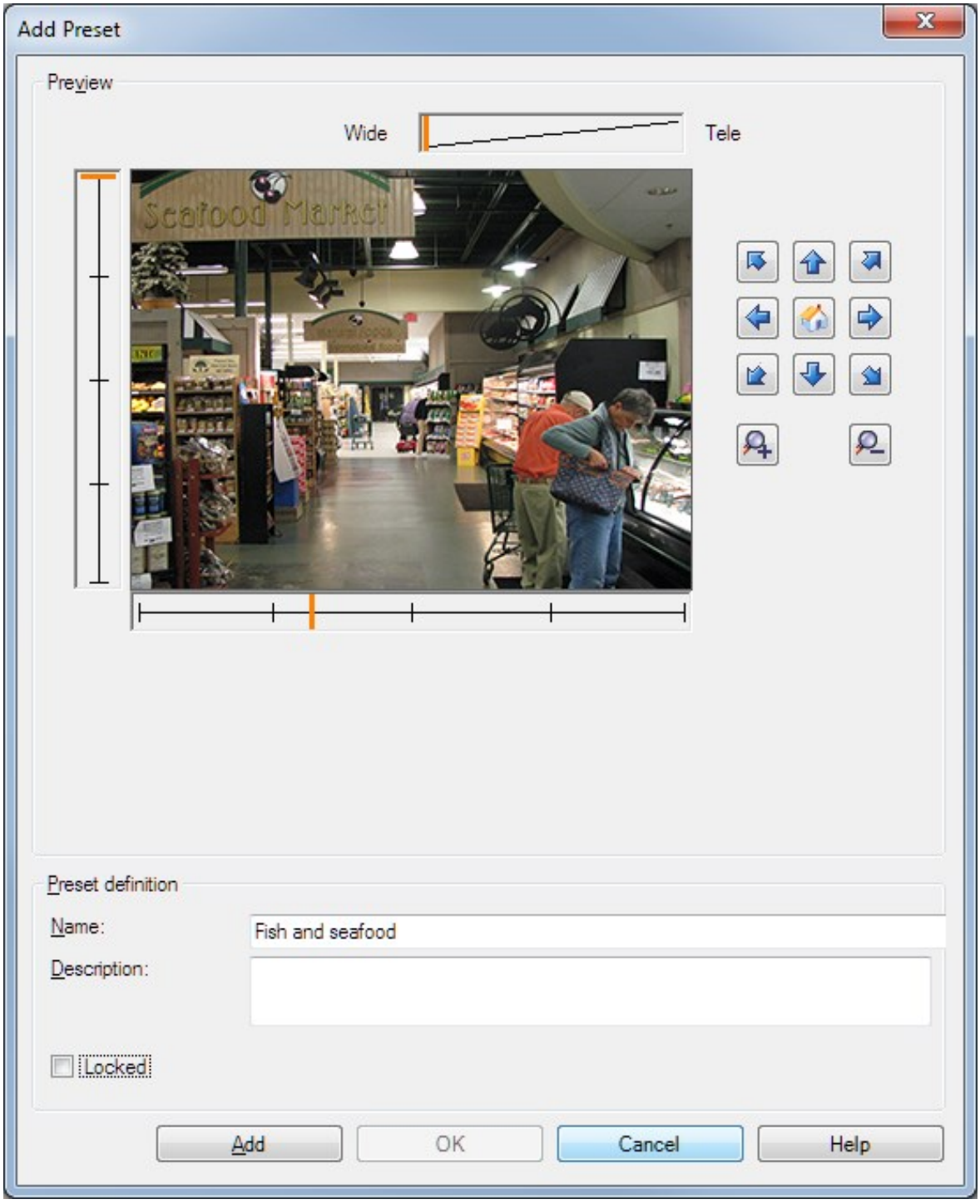
Auf der Startseite der Kamera legen Sie die Preset Position der Kamera fest. Die auf der Startseite verfügbaren PTZ-Funktionen hängen von der jeweiligen Kamera ab.

## Hinzufügen einer Preset-Position (Typ 1)

Um eine Preset Position für die Kamera hinzuzufügen:

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.

3. Klicken Sie auf der Registerkarte **Voreinstellungen** auf **Neu**. Das Fenster **Voreinstellung hinzufügen** erscheint:



4. Das Fenster **Voreinstellung hinzufügen** zeigt ein Live-Vorschaubild der Kamera an. Navigieren Sie die Kamera mit den Navigationsschaltflächen und/oder den Schiebereglern zur erforderlichen Position.
5. Bestimmen Sie im Feld **Name** einen Namen für die Preset Position.
6. Sie können optional eine Beschreibung der Preset-Position in das Feld **Beschreibung** eingeben.
7. Wählen Sie **Gesperrt**, wenn Sie die Preset Position sperren möchten. Nur Benutzer mit ausreichenden Rechten können die Position anschließend wieder entsperren.
8. Klicken Sie auf **Hinzufügen**, um Voreinstellungen zu bestimmen. Fügen Sie so lange Voreinstellungen hinzu, bis Sie mit diesen zufrieden sind.
9. Klicken Sie auf **OK**. Das Fenster **Voreinstellung hinzufügen** schließt sich und fügt die Position in die Liste der verfügbaren Preset Positionen für die Kamera auf der Registerkarte **Voreinstellungen** ein.

## Verwendung der Preset Positionen der Kamera (Typ 2)

Alternativ zur Festlegung von Preset Positionen im System können Sie bei einigen PTZ-Kameras Preset Positionen auf der Kamera selbst festlegen. Dies können Sie normalerweise über eine produktspezifische Konfigurationswebseite durchführen.

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Wählen Sie auf der Registerkarte **Voreinstellungen** die Option **Voreinstellungen des Gerätes verwenden** aus, um die Voreinstellungen in das System zu importieren.

   Alle Voreinstellungen, die Sie zuvor für die Kamera festgelegt haben, werden gelöscht. Alle definierten Regeln und Zeitpläne für Wachrundgänge sind hierdurch betroffen und die für die XProtect Smart Client-Benutzer verfügbaren Voreinstellungen werden entfernt.
4. Klicken Sie auf **Löschen**, um überflüssige Voreinstellungen zu löschen.
5. Klicken Sie auf **Bearbeiten**, wenn Sie den Anzeigenamen der Voreinstellung ändern möchten (siehe Umbenennen einer Preset-Positionen (nur Typ 2)).
6. Wenn Sie solche gerätedefinierten Voreinstellungen später bearbeiten möchten, können Sie dies an der Kamera machen und importieren sie dann erneut.

## Voreingestellte Standardposition einer Kamera als Standard zuweisen

Bei Bedarf können Sie eine Preset Position einer PTZ-Kamera als die Standard-Preset Position der Kamera festlegen.

Eine Standard-Preset Position kann hilfreich sein, da sie Ihnen gestattet, Regeln zu definieren, die bestimmen, dass PTZ-Kameras unter bestimmten Umständen in die Standard-Preset Position gehen. Zum Beispiel nachdem Sie die PTZ-Kamera manuell bedient haben.

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Wählen Sie auf der Registerkarte **Voreinstellungen** unter **Voreingestellte Positionen** die Voreinstellung auf Ihrer Liste der vorgestellten Positionen aus.
4. Aktivieren Sie unter der Liste das Kontrollkästchen **Standard-Voreinstellung**.

Sie können nur eine Preset Position als Standard-Preset Position definieren.

Wenn Sie **Standardvoreinstellung als PTZ-Ausgangsposition verwenden** in **Optionen** > **Allgemein** gewählt haben, wird die Standardvoreinstellung anstelle der definierten Ausgangsposition der PTZ-Kamera verwendet.

## Festlegen der Standardvoreinstellung als PTZ-Ausgangsposition

Benutzer von Management Client und XProtect Smart Client mit den erforderlichen Benutzerberechtigungen können das System so einrichten, dass es die standardmäßige Preset Position anstelle der Ausgangsposition der PTZ-Kameras verwendet, wenn die Schaltfläche **Home** in einem Client gedrückt ist.

Für die Kamera muss eine Preset Position festgelegt werden. Wenn keine standardmäßige Preset Position definiert ist, wird beim Aktivieren der Schaltfläche **Home** in einem Client nichts ausgelöst.

Einstellen der PTZ-Ausgangsposition aktivieren

1. Wählen Sie **Tools** > **Optionen**.

2. Wählen Sie auf der Registerkarte **Allgemein** in der Gruppe **Aufzeichnungsserver** die Option **Standardvoreinstellung als PTZ-Ausgangsposition** verwenden.

3. Weisen Sie eine Preset Position als standardmäßige Preset Position für die Kamera zu.

Zuweisen einer standardmäßigen Preset PositionVoreingestellte Standardposition einer Kamera als Standard zuweisen auf Seite 265

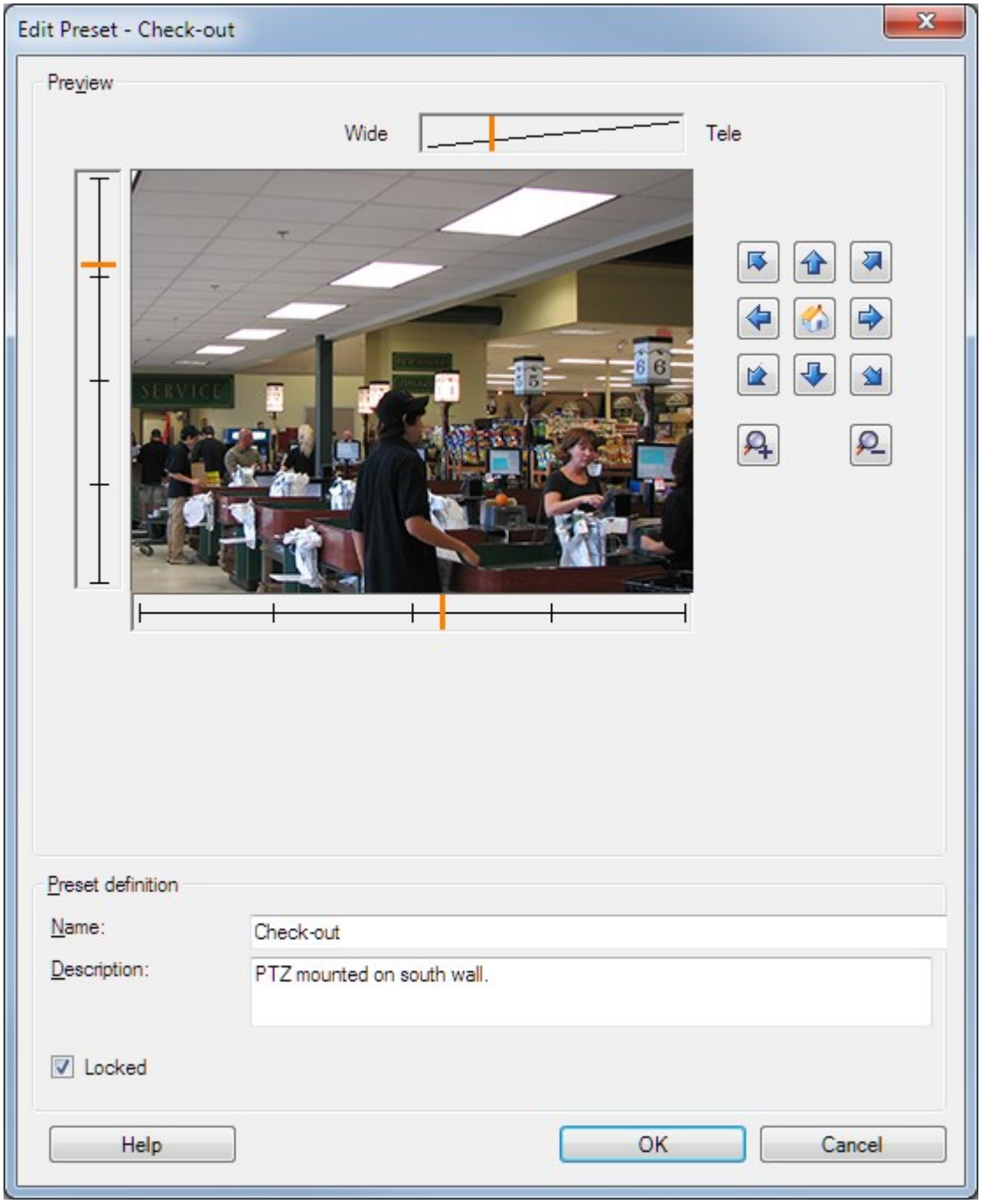
Siehe auch Systemeinstellungen (die Dialogbox "Optionen") auf Seite 412

## Bearbeiten einer voreingestellten Position für eine Kamera (nur Typ 1)

So bearbeiten Sie eine vorhandene, im System definierte Preset Position:

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und dann **Kameras**.
2. Wählen Sie im Bereich **Übersicht** die jeweilige Kamera aus.
3. Wählen Sie auf der Registerkarte **Voreinstellungen** unter Voreingestellte Position aus der Liste der verfügbaren voreingestellten Positionen für die Kamera die voreingestellte Position aus.

4. Klicken Sie auf **Bearbeiten**. Das Fenster **Voreinstellung bearbeiten** wird geöffnet:



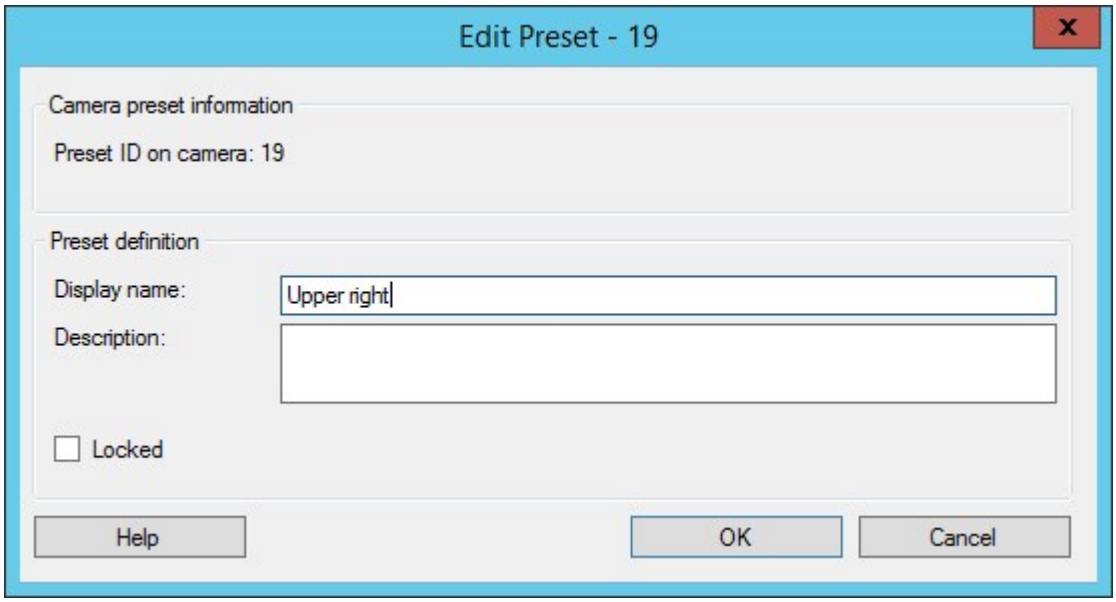

5. Das Fenster **Voreinstellung bearbeiten** zeigt ein Live-Video der Preset Position an. Ändern Sie die Preset Position mit den Navigationsschaltflächen und/oder den Schiebereglern nach Bedarf.
6. Ändern Sie den Namen/die Nummer und die Beschreibung der Preset Position bei Bedarf.
7. Wählen Sie **Gesperrt**, wenn Sie die Preset Position sperren möchten. Nur Benutzer mit ausreichenden Rechten können die Position anschließend wieder entsperren.

8. Klicken Sie auf **OK**.

## Umbenennen einer voreingestellten Position für eine Kamera (nur Typ 2)

So bearbeiten Sie den Namen einer in der Kamera definierten Preset Position:

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Wählen Sie die Preset Position in der Liste verfügbarer Voreinstellungen für die Kamera in der Registerkarte **Voreinstellungen** aus.
4. Klicken Sie auf **Bearbeiten**. Das Fenster **Voreinstellung bearbeiten** wird geöffnet:




5. Ändern Sie den Namen und fügen Sie bei Bedarf eine Beschreibung der Preset Position hinzu.
6. Wählen Sie **Gesperrt**, wenn Sie den Namen der Voreinstellung sperren möchten. Sie können einen voreingestellten Namen sperren, wenn Sie verhindern möchten, dass Benutzer in XProtect Smart Client oder Benutzer mit eingeschränkten Sicherheitsberechtigungen den voreingestellten Namen aktualisieren oder die Voreinstellung löschen. Gesperrte Voreinstellungen werden durch das Symbol  angezeigt. Nur Benutzer mit ausreichenden Rechten können den voreingestellten Namen nachträglich entsperren.
7. Klicken Sie auf **OK**.

## Testen einer Preset-Position (nur Typ 1)

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Wählen Sie die Preset Position in der Liste verfügbarer Preset Positionen für die Kamera in der Registerkarte **Voreinstellungen** aus.
4. Klicken Sie auf **Aktivieren**.
5. Die Kamera wird zur ausgewählten Preset Position bewegt.

# Geräte - Patrouillen

## Patrouillenprofile und manuelle Patrouillen (Erklärung)

Wachrundgangprofile legen fest, wie Wachrundgänge ablaufen sollen. Dazu gehören die Reihenfolge, in der sich die Kamera zwischen Preset-Positionen bewegen soll, und wie lange sie in jeder Position bleiben soll. Sie können eine unbegrenzte Zahl von Wachrundgangprofilen erstellen und sie in Ihren Regeln verwenden. Beispielsweise können Sie eine Regel erstellen, die festlegt, dass während der Öffnungszeiten tagsüber ein Wachrundgangprofil und nachts ein anderes Profil verwendet werden sollen.

### Manueller Wachrundgang

Bevor Sie ein Wachrundgangprofil z. B. in einer Regel anwenden, können Sie es mit einem manuellen Wachrundgang testen. Sie können einen manuellen Wachrundgang auch verwenden, um einen Wachrundgang von einem anderen Benutzer oder von einem Wachrundgang mit aktivierter Regel zu übernehmen, sofern Sie eine höhere PTZ-Priorität haben.

Wenn sich die Kamera bereits auf einem Wachrundgang befindet oder durch einen anderen Benutzer gesteuert wird, können Sie manuelle Wachrundgänge nur starten, wenn Sie eine höhere Priorität haben.

Wenn Sie einen manuellen Wachrundgang starten, während die Kamera einen Wachrundgang mit aktiver Regel durchführt, nimmt das System diesen Wachrundgang wieder auf, sobald Sie Ihren manuellen Wachrundgang beenden. Wenn ein anderer Benutzer einen manuellen Wachrundgang durchführt, Sie aber höhere Priorität besitzen und Ihren manuellen Wachrundgang starten, wird der manuelle Wachrundgang des anderen Benutzers nicht wieder aufgenommen.

Wenn Sie Ihren manuellen Wachrundgang nicht selbst beenden, wird er fortgesetzt bis ein Wachrundgang mit aktiver Regel oder ein Benutzer mit höherer Priorität übernimmt. Wenn der System-Wachrundgang mit aktiver Regel endet, nimmt das System Ihren manuellen Wachrundgang wieder auf. Wenn ein anderer Benutzer einen manuellen Wachrundgang startet, endet Ihr manueller Wachrundgang und wird nicht wieder aufgenommen.

Wenn Sie Ihre manuelle Wachrundgang beenden und für Ihr Patrouillenprofil eine Endposition festgelegt haben, kehrt die Kamera in diese Position zurück.

## Hinzufügen eines Wachrundgangprofils

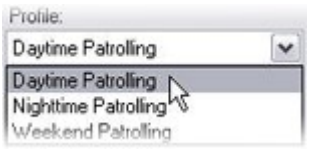
Bevor Sie mit Patrouillen arbeiten können, müssen Sie auf der Registrierkarte **Voreinstellungen** mindestens zwei voreingestellte Positionen für die Kamera angeben, siehe Voreingestellte Position hinzufügen (Typ 1).

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Klicken Sie auf der Registerkarte **Patrouillen** auf **Hinzufügen**. Das Dialogfeld **Profil hinzufügen** wird angezeigt.
4. Geben Sie im Dialogfeld **Profil hinzufügen** einen Namen für das Wachrundgangprofil an.
5. Klicken Sie auf **OK**. Wenn der Name nicht einzigartig ist, ist die Schaltfläche deaktiviert.

Das neue Wachrundgangprofil wird zur Liste **Profil** hinzugefügt. Sie können nun die Preset Position und andere Einstellungen für das Wachrundgangprofil festlegen.

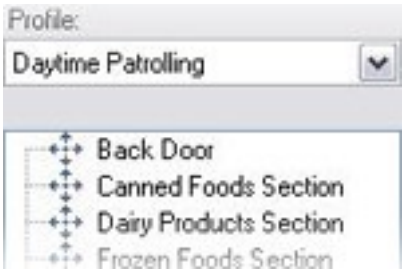
## Festlegen von Preset-Positionen in einem Wachrundgangprofil

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Wählen Sie auf der Registerkarte **Patrouillen** auf der Liste **Profile** das Patrouillenprofil aus:




4. Klicken Sie auf **Hinzufügen**.
5. Wählen Sie im Dialogfeld **PTZ-Voreinstellungen auswählen** die voreingestellten Positionen für Ihr Patrouillenprofil aus:

6. Klicken Sie auf **OK**. Die ausgewählten Voreinstellungsoptionen werden der Liste für Preset Positionen für das Wachrundgangprofil hinzugefügt:



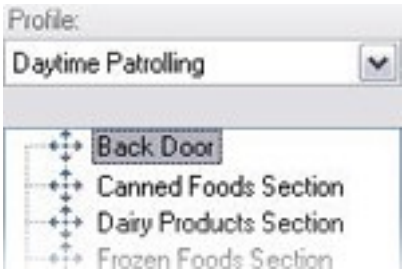

7. Die Kamera nutzt die Preset Position oben in der Liste als ersten Stopp, wenn sie einen Wachrundgang entsprechend dem Wachrundgangprofil ausführt. Die zweite Preset Position von oben ist der zweite Stopp usw.

## Festlegen der Zeit in jeder Preset Position

Während des Wachrundgangs verbleibt die PTZ-Kamera standardmäßig 5 Sekunden an jeder Preset Position, die im Wachrundgang festgelegt ist.

So ändern Sie die Anzahl an Sekunden:

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Wählen Sie auf der Registerkarte **Patrouillen** auf der Liste **Profile** das Patrouillenprofil aus.
4. Wählen Sie die Preset Position, deren Zeit Sie ändern wollen, aus:




5. Legen Sie die Zeit im Feld **Zeit an Position (s)** fest.
6. Wiederholen Sie diese Schritte ggf. für andere Preset Positionen.

## Übergänge anpassen (PTZ)

Standardmäßig wird der Zeitraum, den die Kamera zur Bewegung von einer Preset Position zur nächsten benötigt, der sogenannte **Übergang**, auf drei Sekunden geschätzt. In diesem Zeitraum ist die Bewegungserkennung auf der Kamera standardmäßig deaktiviert, da sonst wahrscheinlich irrelevante Bewegung erkannt wird, während sich die Kamera zwischen den Preset Positionen bewegt.

Sie können Übergangsgeschwindigkeiten nur anpassen, wenn Ihre Kamera PTZ-Scanning unterstützt und Preset Positionen auf Ihrem System-Server konfiguriert und gespeichert werden (PTZ-Kamera Typ 1). Andernfalls ist der Schieberegler **Geschwindigkeit** ausgegraut.

Sie können Folgendes anpassen:

- Die geschätzte Übergangszeit
- Die Geschwindigkeit, mit der sich die Kamera während eines Übergangs bewegt

So passen Sie Übergänge zwischen den unterschiedlichen Preset Positionen an:

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Wählen Sie auf der Registerkarte **Patrouillen** auf der Liste **Profile** die Patrouillenprofile aus.
4. Aktivieren Sie das Kontrollkästchen **Übergänge anpassen**.

   Übergangsanzeigen werden zur Liste der Preset Positionen hinzugefügt.
5. Wählen Sie auf der Liste den Übergang aus.

   
   
6. Legen Sie die geschätzte Übergangszeit (in Sekunden) im Feld **Geschätzte Zeit (Sek.)** fest.

   
   
7. Verwenden Sie den Schieberegler **Geschwindigkeit**, um die Übergangszeit festzulegen. Wenn sich der Schieberegler ganz rechts befindet, bewegt sich die Kamera in ihrer standardmäßigen Geschwindigkeit. Je weiter Sie den Schieberegler nach links bewegen, desto langsamer bewegt sich die Kamera während des ausgewählten Übergangs.
8. Wiederholen Sie dies bei Bedarf für weitere Übergänge.

## Eine Position für die Patrouille angeben

Sie können angeben, dass sich die Kamera am Ende des im ausgewählten Wachrundgangprofil voreingestellten Wachrundgangs an eine bestimmte Preset Position bewegen soll.

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Wählen Sie auf der Registerkarte **Patrouillen** auf der Liste **Profile** das jeweilige Patrouillenprofil aus.
4. Aktivieren Sie das Kontrollkästchen **Am Ende des Wachgangs zu bestimmter Position gehen**. Das Dialogfeld **Voreinstellung auswählen** wird geöffnet.
5. Wählen Sie die Endposition und klicken Sie dann auf **OK**.

   Sie können jede Preset Position der Kamera als Endposition auswählen. Sie sind nicht auf die im Wachrundgangprofil verwendeten Preset Positionen beschränkt.

6. Die ausgewählte Position wird der Liste „Profil“ hinzugefügt.

Am Ende des im ausgewählten Wachrundgangprofil festgelegten Wachrundgang bewegt sich die Kamera zur festgelegten Endposition.

## PTZ-Sitzungen reservieren und freigeben

Abhängig vom Überwachungssystem können Sie PTZ-Sitzungen reservieren.

Administratoren mit Sicherheitsberechtigungen zum Ausführen einer reservierten PTZ-Sitzung können die PTZ-Kamera in dieser Betriebsart betreiben. So wird verhindert, dass andere Benutzer die Kontrolle über die Kamera übernehmen. Bei einer reservierten PTZ-Sitzung wird das standardmäßige PTZ-Prioritätssystem ignoriert, um zu verhindern, dass Benutzer mit einer höheren PTZ-Priorität die Sitzung unterbrechen.

Sie können die Kamera in einer reservierten PTZ-Sitzung sowohl von XProtect Smart Client als auch von Management Client aus bedienen.

Das Reservieren einer PTZ-Sitzung kann hilfreich sein, wenn Sie dringende Aktualisierungen oder Wartungsarbeiten an einer PTZ-Kamera oder deren Voreinstellungen vornehmen müssen, ohne dabei von anderen Benutzern gestört zu werden.

### Eine PTZ-Sitzung reservieren

1. Wählen Sie im Bereich **Standort-Navigation Geräte** aus, und wählen Sie dann **Kameras** aus.
2. Wählen Sie im Bereich **Übersicht** die zugehörige PTZ-Kamera aus.
3. Wählen Sie auf der Registerkarte **Voreinstellungen** die PTZ-Sitzung aus und klicken Sie dann auf **Reserviert**.

Sie können eine reservierte PTZ-Sitzung nicht starten, wenn ein Benutzer mit höherer Priorität die Kamera steuert oder wenn ein anderer Benutzer die Kamera bereits reserviert hat.

### Freigeben einer PTZ-Sitzung

Die Schaltfläche **Freigeben** ermöglicht es Ihnen, Ihre aktuelle PTZ-Sitzung freizugeben, sodass ein anderer Benutzer die Kamera steuern kann. Wenn Sie auf **Freigeben** klicken, wird die PTZ-Sitzung sofort beendet und ist für den nächsten Benutzer verfügbar, der die Kamera bedient.

Administratoren, denen die Sicherheitsberechtigung **PTZ-Sitzung freigeben** zugewiesen wurde, sind berechtigt, die reservierte PTZ-Sitzung anderer Benutzer jederzeit freizugeben. Dies kann beispielsweise nützlich sein, wenn die PTZ-Kamera oder ihre Voreinstellungen beibehalten werden müssen oder andere Benutzer in Ausnahmesituationen die Kamera aus Versehen gesperrt haben.

## Festlegen von PTZ-Sitzungs-Zeitüberschreitungen

Management Client und XProtect Smart Client Benutzer mit den erforderlichen Benutzerrechten können die Überwachung von PTZ-Kameras von Hand unterbrechen.

Sie können festlegen, wie viel Zeit vergehen soll, bevor alle PTZ-Kameras in Ihrem System reguläre Wachrundgänge wieder aufnehmen:

1. Wählen Sie **Tools** > **Optionen**.
2. Wählen Sie auf der Registerkarte **Allgemein** im Fenster **Optionen** den Zeitraum in der:
   - Liste **Zeitüberschreitung für manuelle PTZ-Sitzungen** (standardmäßig 15 Sekunden).
   - Liste **Zeitüberschreitung für Anhalten von Wachrundgängen** (standardmäßig 10 Minuten).
   - Liste **Zeitüberschreitung für reservierte PTZ-Sitzungen** (standardmäßig 1 Stunde).

   Diese Einstellungen betreffen alle PTZ-Kameras in Ihrem System.

Sie können die Zeitüberschreitungen individuell für jede Kamera ändern.

1. Klicken Sie im Bereich **Standort-Navigation** auf **Kamera**.
2. Wählen Sie im Bereich „Übersicht“ die Kamera aus.
3. Wählen Sie auf der Registerkarte **Voreinstellungen** den Zeitraum in der:
   - Liste **Zeitüberschreitung für manuelle PTZ-Sitzung** (standardmäßig 15 Sekunden).
   - Liste **Zeitüberschreitung für Anhalten von Wachrundgang** (standardmäßig 10 Minuten).
   - Liste **Zeitüberschreitung für reservierte PTZ-Sitzung** (standardmäßig 1 Stunde).

   Diese Einstellungen betreffen nur diese Kamera.

# Geräte - Ereignisse für Regeln

## Fügen Sie ein Ereignis für ein Gerät hinzu oder löschen Sie es

### Ein Ereignis hinzufügen

1. Wählen Sie im Fenster **Übersicht** ein Gerät aus.
2. Wählen Sie die Registerkarte **Ereignisse** und klicken Sie auf **Hinzufügen**. Dies öffnet das Fenster **Treiberereignis auswählen**.
3. Wählen sie ein Ereignis aus. Sie können nur ein Ereignis zur selben Zeit auswählen.
4. Wenn Sie eine Gesamtliste aller Ereignisse anschauen möchten, aus der Sie Ereignisse hinzufügen können, die bereits hinzugefügt wurden, wählen Sie **Bereits hinzugefügte Ereignisse anzeigen**.
5. Klicken Sie auf **OK**.
6. Klicken Sie in der Symbolleiste auf **Speichern**.

### Ereignis löschen

> Wenn Sie ein Ereignis löschen, betrifft dies alle Regeln, die dieses Ereignis verwenden.

1. Wählen Sie im Fenster **Übersicht** ein Gerät aus.
2. Wählen Sie die Registerkarte **Ereignisse** und klicken Sie auf **Löschen**.

#### Ereigniseigenschaften festlegen

Sie können die Eigenschaften für jedes hinzugefügte Ereignis festlegen. Die Anzahl der Eigenschaften hängt vom Gerät und Ereignis ab. Damit das Ereignis funktioniert wie beabsichtigt, müssen Sie sowohl auf dem Gerät als auch auf der Registerkarte **[Ereignisse]** einige oder alle Eigenschaften in identischer Weise festlegen.

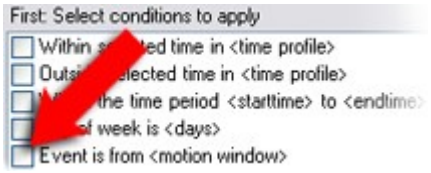
#### Verwenden von mehreren Instanzen eines Ereignisses

Sie können ein Ereignis mehr als einmal hinzufügen, um verschiedene Eigenschaften für verschiedene Instanzen eines Ereignisses zu bestimmen.

> Das folgende Beispiel bezieht sich speziell auf Kameras.

**Beispiel**: Sie haben die Kamera mit zwei Bewegungsfenstern eingestellt, nämlich A1 und A2. Sie haben zwei Instanzen für das Ereignis Bewegung gestartet (HW) hinzugefügt. In den Eigenschaften einer Instanz haben Sie die Verwendung des Bewegungsfenster A1 festgelegt. In den Eigenschaften der anderen Instanz haben Sie die Verwendung des Bewegungsfenster A2 festgelegt.

Wenn Sie ein Ereignis in einer Regel verwenden, können Sie festlegen, dass das Ereignis auf erkannte Bewegung in einem bestimmten Bewegungsfenster reagieren sollte, damit die Regel ausgelöst wird:




# Geräte - aus Datenschutzgründen abgedeckte Bildbereiche

## Aktivieren/Deaktivieren von Privatsphärenausblendung

Die Funktion für „Privatsphärenausblendung“ ist standardmäßig nicht aktiviert.

So aktivieren/deaktivieren Sie die Funktion „Privatsphärenausblendung“ für eine Kamera:

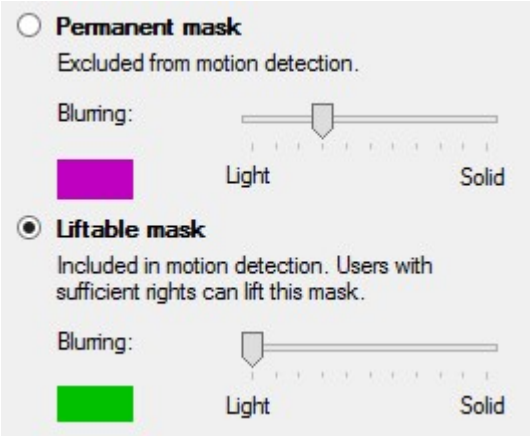
1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie die zugehörige Kamera im Bereich **Übersicht** aus.
3. Aktivieren oder Deaktivieren Sie auf der Registerkarte **Vergedeckte Bildbereiche** das Kontrollkästchen **Verdeckte Bildbereiche**.

> In einer Milestone Interconnect-Einstellung ignoriert ein zentraler Standort die Privatzonenmasken in einem Remote-System. Wenn Sie die gleichen Privatzonenmasken anwenden möchten, müssen Sie diese am zentralen Standort neu festlegen.

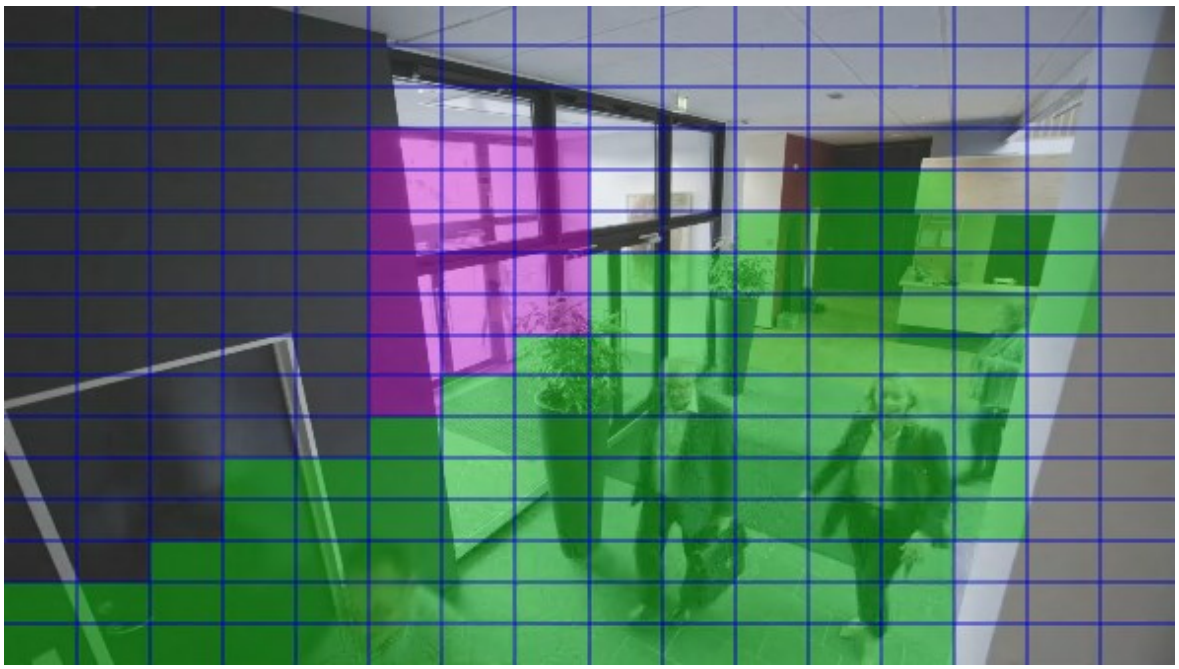
## Privatzonenmasken festlegen

Wenn Sie die Privatsphärenausblendung-Funktion auf der Registerkarte **Privatzonenmaske** aktivieren, kommt ein Raster zur Anwendung auf die Kameravorschau.

1. Wählen Sie im Bereich **Standort-Navigation** die **Geräte** aus.
2. Wählen Sie im Bereich **Übersicht** die jeweilige Kamera aus.
3. Wählen Sie auf der Registerkarte **Abgedeckte Bildbereiche** zum Abdecken von Bereichen aus Datenschutzgründen, zunächst **Permanent verdecken** oder **Entfernbare Verdeckung** aus, um anzugeben, ob Sie eine dauerhafte oder eine entfernbare Verdeckung wünschen.




4. Ziehen Sie den Mauszeiger über die Vorschau. Klicken Sie mit der linken Maustaste, um eine Gitterzelle auszuwählen. Klicken Sie mit der rechten Maustaste, um eine Gitterzelle zu löschen.
5. Sie können so viele Privatzonenmasken festlegen, wie Sie benötigen. Bereiche mit permanenten Privatzonenmasken erscheinen in Violett und Bereiche mit aufhebbaren Privatzonenmasken in Grün.



6. Bestimmen Sie, wie die Abdeckung der Bereiche im Video erscheinen soll, wenn dieses im Client gezeigt wird. Benutzen Sie die Schieber, um von einer leichten Unschärfe auf eine voll intransparente Maske zu wechseln.

   Permanente Privatzonenmasken werden auch auf der Registerkarte **Motion** eingeblendet.

7. Prüfen Sie in XProtect Smart Client, ob die Privatzonenmasken so eingeblendet werden, wie von Ihnen festgelegt.

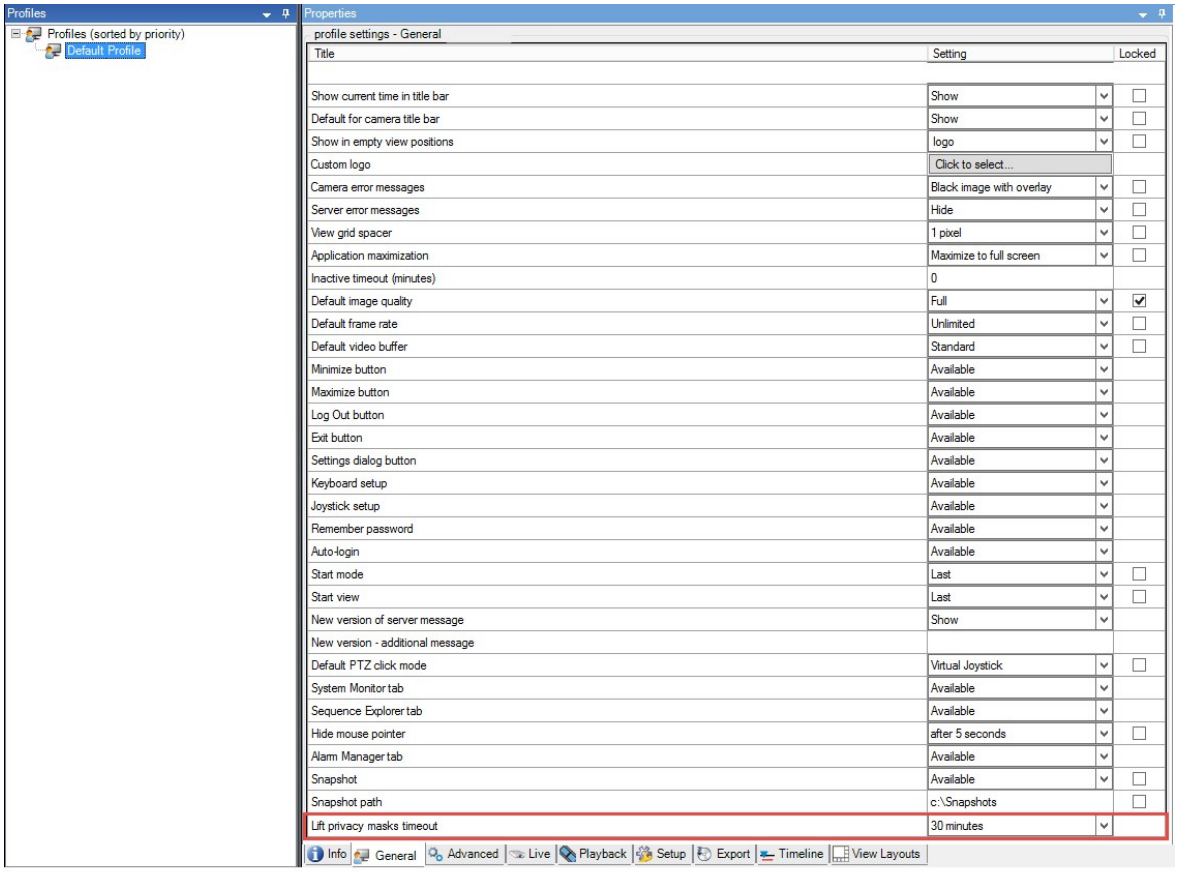
## Ändern des Timeout für aufgehobene Privatzonenmasken

Als Standard werden Privatzonenmasken in XProtect Smart Client für 30 Minuten aufgehoben und anschließend automatisch wieder eingesetzt, aber das können Sie ändern.

Wenn Sie das Timeout ändern, erinnern Sie sich daran, dies für das Smart Client-Profil zu tun, in Verbindung mit der Rolle welche die Genehmigung hat, Privatzonenmasken aufzuheben.

Änderung des Timeout:

1. Wählen Sie unter **Smart Client Profile** das entsprechende Smart Client-Profil aus.
2. Auf der Registerkarte **Allgemein** finden Sie **Timeout Aufheben von Privatzonenmasken**.




3. Wählen Sie zwischen den Werten:
   - **2 Minuten**
   - **10 Minuten**
   - **30 Minuten**
   - **1 Stunde**
   - **2 Stunden**
   - **Bis abgemeldet**
4. Klicken Sie auf **Speichern**.

## Benutzerberechtigung zum Aufheben von Privatzonenmasken erteilen

Als Standard hat kein Benutzer die Berechtigung, Privatzonenmasken in XProtect Smart Client aufzuheben.

Aktivieren/deaktivieren der Berechtigung:

1. Wählen Sie im Bereich **Standort-Navigation** die Option **Sicherheit** aus und wählen Sie dann **Rollen** aus.
2. Wählen Sie die Rolle aus, der Sie die Erlaubnis erteilen wollen, verdeckte Bildbereiche freizulegen.
3. Auf der Registerkarte **Allgemeine Sicherheit** wählen Sie **Kameras**.
4. Wählen Sie das Kontrollkästchen **Genehmigen** für die Berechtigung zum **Aufheben von Privatzonenmasken**.

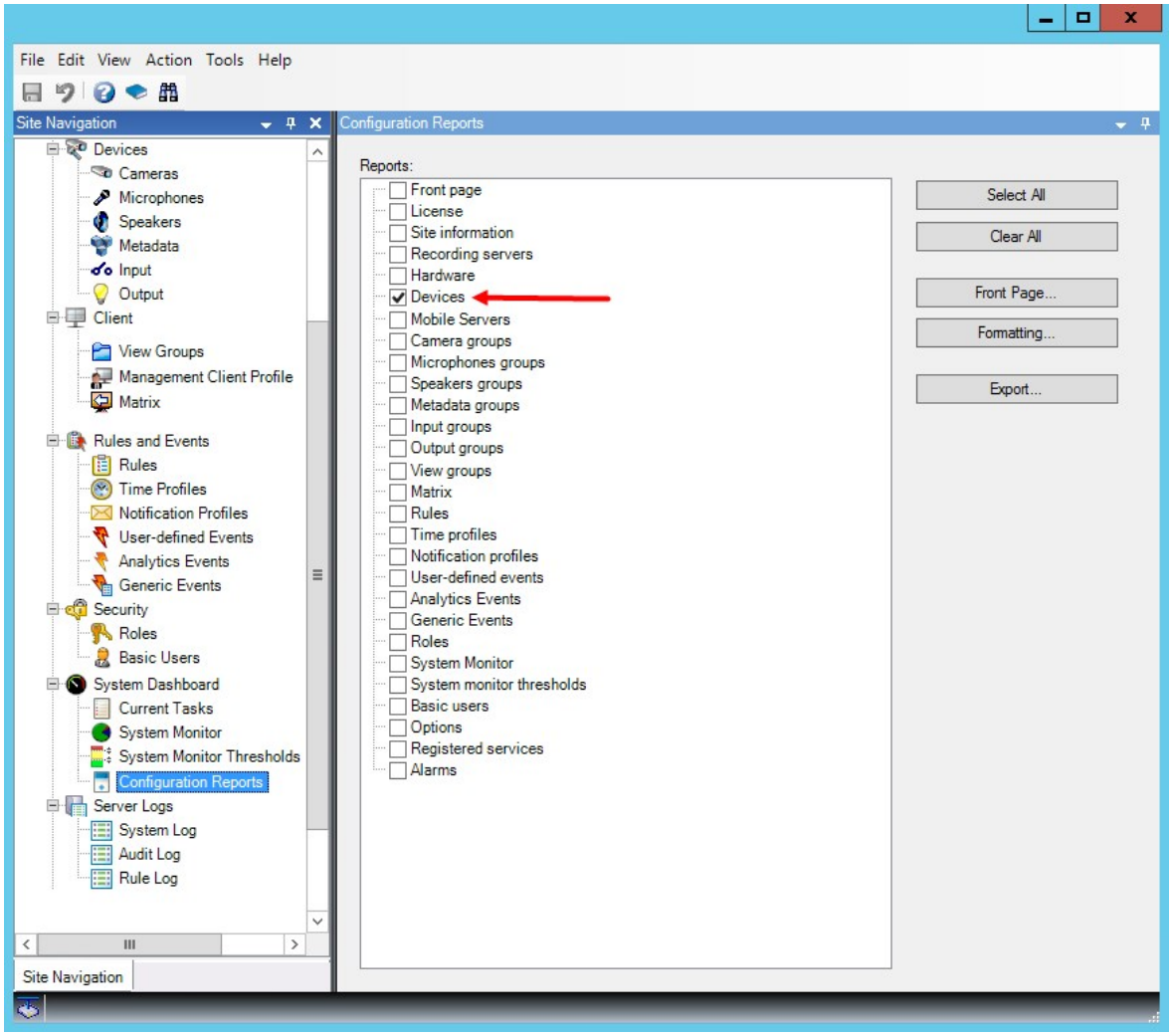
Benutzer, denen Sie diese Rolle zugewiesen haben, können Privatzonenmasken, die als aufhebbare Privatzonenmasken konfiguriert sind, selbst aufheben und das Aufheben auch für andere Benutzer XProtect Smart Client genehmigen.

## Erstellen Sie einen Bericht von der Konfiguration Ihrer Privatsphärenausblendung

Der Gerätebericht enthält Informationen über die aktuellen Einstellungen der Privatsphärenausblendung Ihrer Kameras.

Zum Konfigurieren eines Berichts:

1. Wählen Sie aus dem Bereich **Standortnavigation** das **System Dashboard** aus.
2. Wählen Sie unter **Konfigurationsberichte** den Bericht **Geräte**.




3. Wenn Sie den Bericht ändern wollen, können Sie die Titelseite und die Formatierung wechseln.
4. Klicken Sie auf **Export** und das System erstellt den Bericht als PDF-Datei.

Weitere Informationen zu Berichten finden Sie unter Einen Bericht mit Ihrer Systemkonfiguration ausdrucken auf Seite 321.

# Clients

## Ansichtsgruppen (Erklärung)

Die Art und Weise wie das System Video von einer oder mehreren Kameras in Clients anzeigt, wird Ansicht genannt. Eine Ansichtsgruppe ist ein Behälter für eine oder mehrere logische Gruppen solcher Ansichten. In Clients wird eine Ansichtsgruppe als ausklappbarer Ordner dargestellt, von dem Benutzer Gruppen und die

gewünschte Ansicht auswählen können:


Beispiel von XProtect Smart Client: Ein Pfeil zeigt eine Ansichtsgruppe an, die eine logische Gruppe beinhaltet (Annehmlichkeiten genannt), die wiederum 3 Ansichten enthält.

Standardmäßig wird jede Rolle, die Sie in der Management Client festlegen, auch als Ansichtsgruppe erstellt. Wenn Sie eine Rolle in der Management Client hinzufügen, erscheint diese Rolle standardmäßig als Ansichtsgruppe zur Verwendung in Clients.

- Sie können eine Ansichtsgruppe auf Grundlage einer Rolle zu Benutzern/Gruppen mit relevanter Rolle zuteilen. Sie können diese Ansichtsgruppenberechtigungen ändern, indem Sie dies in der Rolle nachträglich einrichten
- Eine rollenbasierte Ansichtsgruppe hat den Namen der Rolle inne.

  **Beispiel**: Wenn Sie eine Rolle mit dem Namen **Aufbauen eines Sicherheitspersonals** erstellen, erscheint es in XProtect Smart Client als Ansichtsgruppe namens **Aufbauen eines Sicherheitspersonals**.

  Abgesehen von den Ansichtsgruppen, die Sie beim Hinzufügen von Rollen erhalten, können Sie beliebig viele andere Ansichtsgruppen erstellen. Sie können auch Ansichtsgruppen entfernen, einschließlich derer, die automatisch beim Hinzufügen von Rollen erstellt werden
- Selbst wenn beim Hinzufügen einer Rolle jedes Mal eine Ansichtsgruppe erstellt wird, brauchen Ansichtsgruppen keinen Rollen zu entsprechen. Sie können nach Bedarf jede Ihrer Ansichtsgruppen hinzufügen, umbenennen oder entfernen

> Wenn Sie eine Ansichtsgruppe umbenennen, müssen sich bereits verbundene Client-Benutzer ausloggen und wieder einloggen, bevor die Namensänderung sichtbar wird.

## Ansichtsgruppe hinzufügen

1. Rechtsklick auf **Ansichtsgruppen** und dann **Ansichtsgruppe hinzufügen** auswählen. Dies öffnet das Dialogfenster **Ansichtsgruppe hinzufügen**.
2. Geben Sie den Namen und optional eine Beschreibung der neuen Ansichtsgruppe ein und klicken Sie dann auf **OK**.

Keine Rolle kann die neu hinzugefügte Ansichtsgruppe verwenden, solange Sie solche Berechtigungen nicht angegeben haben. Wenn Sie festgelegt haben, welche Rollen die neu hinzugefügte Ansichtsgruppe verwenden können, müssen sich bereits verbundene Client-Benutzer, die die entsprechenden Rollen haben, ab- und wieder anmelden, bevor sie die Ansichtsgruppe sehen können.

# Smart Client-Profile

## Hinzufügen und Konfigurieren eines Smart Client-Profils

Sie müssen ein Smart Client-Profil erstellen, bevor Sie es konfigurieren können.

1. Klicken Sie mit der rechten Maustaste auf **Smart Client-Profile**.
2. Wählen Sie **Smart Client-Profil hinzufügen** aus.
3. Geben Sie im Dialogfenster **Smart Client-Profil hinzufügen** einen Namen und eine Beschreibung des neuen Profils ein und klicken Sie dann auf **OK**.
4. Klicken Sie im Bereich **Überblick** auf das erstellte Profil, um es zu konfigurieren.
5. Passen Sie die Einstellungen auf einer, mehreren oder allen verfügbaren Registerkarten an und klicken Sie auf **OK**.

## Kopieren eines Smart Client-Profils

Wenn Sie ein Smart Client-Profil mit komplizierten Einstellungen oder Berechtigungen haben und ein ähnliches Profil benötigen, kann es einfacher sein, ein bereits vorhandenes Profil zu kopieren und kleinere Anpassungen an der Kopie vorzunehmen, als ein Profil von Grund auf neu zu erstellen.

1. Klicken Sie auf **Smart Client-Profile**, klicken Sie mit der rechten Maustaste auf das Profil im Bereich **Übersicht**, wählen Sie **Smart Client-Profil kopieren** aus.
2. Es erscheint ein Dialogfenster; geben Sie dem kopierten Profil einen neuen einmaligen Namen und eine Beschreibung. Klicken Sie auf **OK**.
3. Klicken Sie im Bereich **Überblick** auf das gerade erstellte Profil, um es zu konfigurieren. Dies können Sie tun, indem Sie die Einstellungen auf einer, mehreren oder allen verfügbaren Registerkarten anpassen. Klicken Sie auf **OK**.

## Erstellen und Einrichten von Smart Client-Profilen, Rollen und Zeitprofilen

Wenn Sie mit Smart Client-Profilen arbeiten, ist ein Verständnis der Interaktionen zwischen Smart Client-Profilen, Rollen und Zeitprofilen von höchster Bedeutung:

- Smart Client-Profile betreffen die Einstellungen für Benutzerrechte in XProtect Smart Client
- Rollen beziehen sich auf Sicherheitseinstellungen in Clients, MIP SDK und mehr
- Zeitprofile beziehen sich auf zeitliche Aspekte der beiden Profiltypen

Zusammen bieten diese drei Funktionen einzigartige Möglichkeiten zur Steuerung und Anpassung der XProtect Smart Client Benutzerberechtigungen.

**Beispiel**: Sie benötigen einen Benutzer in Ihrer XProtect Smart Client-Einrichtung, der nur Live-Video (keine Wiedergaben) von ausgewählten Kameras sehen darf, und das nur während der normalen Arbeitszeit (8:00–16:00 Uhr). Eine Einrichtung könnte folgendermaßen vonstattengehen:

1. Erstellen Sie ein Smart Client-Profil und nennen Sie es beispielsweise **Nur Live**.
2. Legen Sie die benötigten Live-/Wiedergabeeinstellungen für **Nur Live** fest.
3. Erstellen Sie ein Zeitprofil und nennen Sie es beispielsweise **Nur Tag**.
4. Legen Sie die benötigte Zeitspanne für **Nur Tag** fest.
5. Erstellen Sie eine neue Rolle und nennen Sie sie beispielsweise **Bewachen (ausgewählte Kameras)**.
6. Legen Sie fest, welche Kameras **Bewachen (ausgewählte Kameras)** verwenden kann.
7. Weisen Sie das Smart Client Profil **Nur Live** und das Zeitprofil **Nur Tagsüber** der Rolle **Wache (ausgewählte Kameras)** zu, um die drei Elemente zu verbinden.

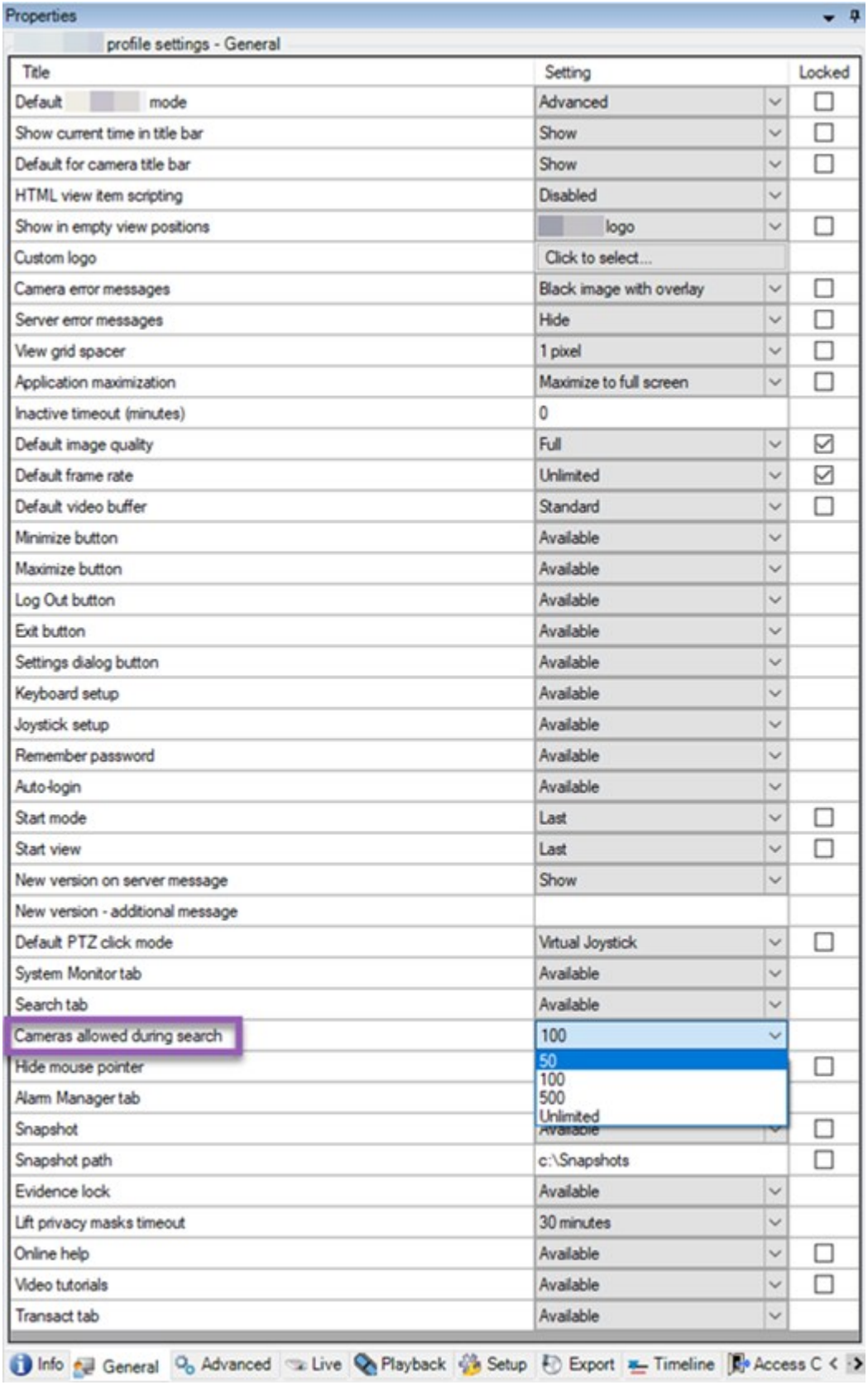
Sie haben jetzt durch die Vermischung dieser drei Funktionen das gewünschte Ergebnis und können sie problemlos weiter verfeinern und anpassen. Sie können die Einrichtung auch in einer anderen Reihenfolge vornehmen. Beispielsweise können Sie die Rolle zuerst erstellen und dann das Smart Client-Profil sowie das Zeitprofil, oder in jeder beliebigen Reihenfolge.

## Legen Sie die während einer Suche erlaubte Anzahl Kameras fest

Sie können konfigurieren, wie viele Kameras die Bediener in XProtect Smart Client zu einer Suche hinzufügen können. Der Standardwert ist **100**. Wenn der Grenzwert für die Anzahl Kameras überschritten wird, erhält der Bediener eine Warnung.

1. Erweitern Sie in XProtect Management Client **Client** > **Smart Client Profile**.
2. Wählen Sie das entsprechende Profil aus.

3. Klicken Sie auf die Registerkarte **Allgemein**.


Properties
profile settings - General
Title
Setting
Locked
Default mode
Advanced
Show current time in title bar
Show
Default for camera title bar
Show
HTML view item scripting
Disabled
Show in empty view positions
logo
Custom logo
Click to select...
Camera error messages
Black image with overlay
Server error messages
Hide
View grid spacer
1 pixel
Application maximization
Maximize to full screen
Inactive timeout (minutes)
0
Default image quality
Full
Default frame rate
Unlimited
Default video buffer
Standard
Minimize button
Available
Maximize button
Available
Log Out button
Available
Exit button
Available
Settings dialog button
Available
Keyboard setup
Available
Joystick setup
Available
Remember password
Available
Auto-login
Available
Start mode
Last
Start view
Last
New version on server message
Show
New version - additional message
Default PTZ click mode
Virtual Joystick
System Monitor tab
Available
Search tab
Available
Cameras allowed during search
100
50
100
500
Unlimited
Hide mouse pointer
Alarm Manager tab
Snapshot
Snapshot path
c:\Snapshots
Evidence lock
Available
Lift privacy masks timeout
30 minutes
Online help
Available
Video tutorials
Available
Transact tab
Available
Info
General
Advanced
Live
Playback
Setup
Export
Timeline
Access C

4. Wählen Sie unter **Kameras**, die bei der Suche zugelassen sind, einen der folgenden Werte aus:
    - **50**
    - **100**
    - **500**
    - **Unbegrenzt**
5. Speichern Sie Ihre Änderungen.

## Standardeinstellungen für den Export ändern

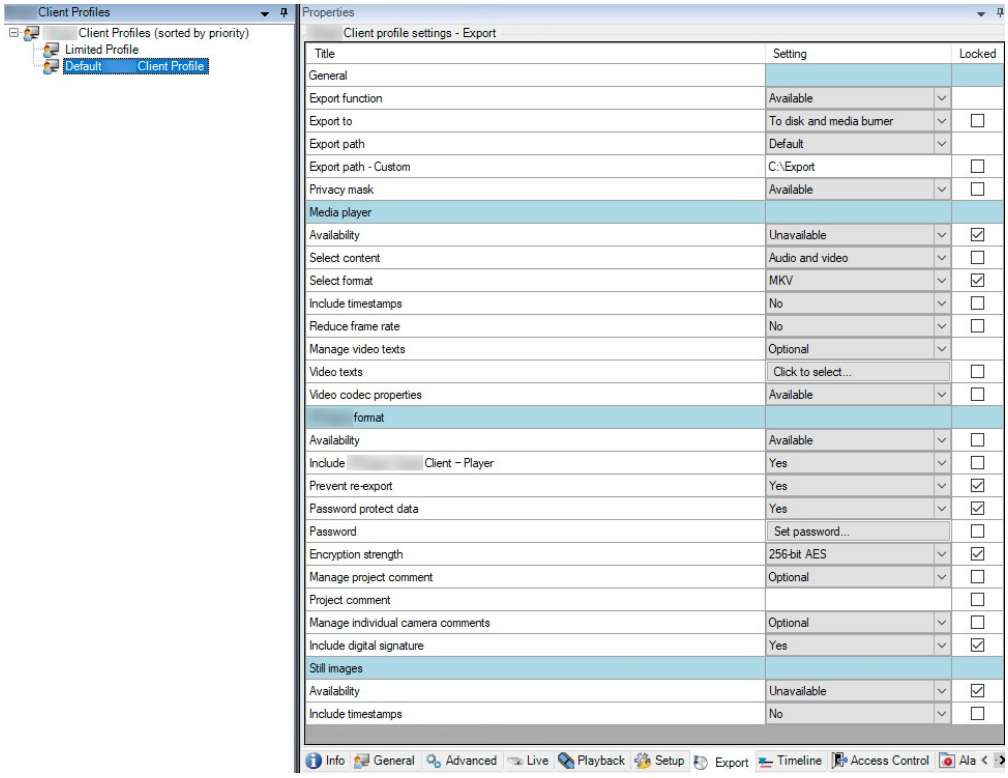
Bei der Installation Ihres XProtect VMS-Systems werden die Standard-Exporteinstellungen, die die Exportoptionen in XProtect Smart Client festlegen, so eingeschränkt, dass sie ein Höchstmaß an Sicherheit gewährleisten. Sie können diese Einstellungen so ändern, dass dem Bediener mehr Optionen zur Verfügung stehen.

**Standardeinstellungen**

- Nur das Format XProtect ist verfügbar
    - Ein erneuter Export wird verhindert
    - Exporte sind mit Passwort geschützt
    - 256-Bit AES-Verschlüsselung
    - Digitale Signaturen werden hinzugefügt
- Der Export im Format MKV oder AVI ist nicht möglich
- Standbilder können nicht exportiert werden

Schritte:

1. Erweitern Sie in XProtect Management Client **Client** > **Smart Client Profile**.
2. Wählen Sie **Standard Smart Client-Profile** aus.
3. Wählen Sie im Bereich **Eigenschaften** die Registerkarte **Export** aus.




4. Um in XProtect Smart Client ein eingeschränktes Format verfügbar zu machen, suchen Sie die entsprechende Einstellung und wählen Sie **Verfügbar** aus.
5. Damit der Bediener in XProtect Smart Client eine Einstellung ändern kann, deaktivieren Sie das Kontrollkästchen **Gesperrt** neben der entsprechenden Einstellung.
6. Ändern Sie ggf. weitere Einstellungen.
7. (optional) Melden Sie sich bei XProtect Smart Client an, um zu überprüfen, ob Ihre Einstellungen übernommen wurden.

# Management Client-Profile

## Hinzufügen und Konfigurieren eines Management Client-Profils

Wenn Sie das Standardprofil nicht verwenden möchten, können Sie ein Management Client-Profil erstellen, um dieses zu konfigurieren.

1. Klicken Sie mit der rechten Maustaste auf **Management Client-Profile**.
2. Wählen Sie **Management Client-Profil hinzufügen** aus.
3. Geben Sie im Dialogfenster **Management Client-Profil hinzufügen** einen Namen und eine Beschreibung des neuen Profils ein und klicken Sie dann auf **OK**.
4. Klicken Sie im Bereich **Überblick** auf das erstellte Profil, um es zu konfigurieren.
5. Aktivieren oder deaktivieren Sie auf der Registerkarte **Profil** Funktionen des Management Client-Profils.

## Kopieren eines Management Client-Profils

Wenn Sie ein Management Client-Profil mit Einstellungen haben, die Sie gerne wiederverwenden möchten, können Sie ein bereits vorhandenes Profil kopieren und kleine Änderungen an der Kopie vornehmen, anstatt ein Profil von Grund auf neu zu erstellen.

1. Klicken Sie auf **Management Client-Profil**, klicken Sie mit der rechten Maustaste auf das Profil im Bereich **Übersicht**, wählen Sie **Management Client-Profil kopieren** aus.
2. Es erscheint ein Dialogfenster; geben Sie dem kopierten Profil einen neuen einmaligen Namen und eine Beschreibung. Klicken Sie auf **OK**.
3. Klicken Sie im Bereich **Übersicht** auf das Profil und gehen Sie zur Registerkarte **Info** oder **Profil**, um das Profil zu konfigurieren.

## Verwaltung der Sichtbarkeit von Funktionen für ein Management Client-Profil

Ordnen Sie Management Client-Profile Rollen zu, damit die Benutzeroberfläche nur die Funktionen der jeweiligen Administratorrolle anzeigt.

### Verknüpfung eines Management Client-Profils mit einer Rolle

1. Erweitern Sie den Knoten **Sicherheit** und klicken Sie auf **Rollen**.
2. Auf der Registerkarte **Info** im Fenster **Rolleneinstellungen** können Sie ein Profil mit einer Rolle verknüpfen. Weitere Informationen finden Sie auf der Registerkarte Info (Rollen).

### Allgemeine Verwaltung des Zugriffs auf Systemfunktionen für eine Rolle

Management Client-Profile regeln nur die visuelle Aufstellung von Systemfunktionen, nicht den tatsächlichen Zugriff dazu.

Für die allgemeine Verwaltung des Zugriffs auf Systemfunktionen für eine Rolle:

1. Erweitern Sie den Knoten **Sicherheit** und klicken Sie auf **Rollen**.
2. Klicken Sie auf die Registerkarte **Allgemeine Sicherheit** und aktivieren Sie die jeweiligen Kontrollkästchen. Weitere Informationen finden Sie unter Registerkarte „Gesamtsicherheit“ (Rollen) auf Seite 556.

Achten Sie auf der Registerkarte **Allgemeine Sicherheit** darauf, dass die Sicherheitsberechtigung **Verbinden** aktiviert ist, um allen Rollen den Zugriff auf die Management Server zu gewähren.

Neben der integrierten Administratorrolle können nur Benutzer, die einer Rolle zugeordnet wurden, der das Recht zur **Verwaltung von Sicherheitsberechtigungen** auf dem Management-Server in der Registerkarte **Gesamtsicherheit** gewährt wurde, Management Client-Profile hinzufügen, bearbeiten und löschen.

### Begrenzung der Sichtbarkeit von Funktionen für ein Profil

Sie können die Einstellungen für die Sichtbarkeit aller Management Client-Elemente ändern. Standardmäßig können über das Management Client-Profil alle Funktionen im Management Client angezeigt werden.

1. Erweitern Sie den Knoten "Client" und klicken Sie auf Management Client-Profile.
2. Wählen Sie ein Profil aus und klicken Sie auf die Registerkarte "Profil".
3. Deaktivieren Sie die Kontrollkästchen für die jeweilige Funktion, um die Sichtbarkeit der Funktion aus Management Client für jeden Management Client Benutzer zu entfernen, der eine mit diesem Management Client Profil verknüpfte Rolle hat.

# Matrix

## Matrix und Matrix Empfänger (Erklärung)

Matrix ist eine Funktion zur Remote-Verteilung von Videoaufzeichnungen.

Ein Matrix Empfänger ist ein Computer mit XProtect Smart Client, der in Matrix als Empfänger Management Client definiert ist.

Wenn Sie Matrix verwenden, können Sie Videoaufzeichnungen im Push-Verfahren von einer beliebigen Kamera in Ihrem Systemnetzwerk an einen beliebigen Matrix-Empfänger übertragen.

Eine Liste der Matrix in der Management Client hinzugefügten Empfänger sehen Sie, wenn Sie **Client** im Bereich **Standortnavigation** erweitern und dann **Matrix** auswählen. Eine Liste von Matrix-Konfigurationen wird im Bereich **Eigenschaften** angezeigt.

In Management Client müssen Sie jeden Matrix Empfänger hinzufügen, von dem Sie von Matrix ausgelöste Videoaufzeichnungen empfangen möchten.

## Regeln dafür festlegen, wie Videoaufzeichnungen an Matrix-Empfänger gesendet werden

Damit Video an Matrix-Empfänger gesendet wird, müssen Sie die Matrix-Empfänger in einer Regel einschließen, welche die Übertragung des Videos an den zugehörigen Matrix-Empfänger auslöst. Dafür müssen Sie folgendes tun:

1. Erweitern Sie im Bereich **Standort-Navigation Regeln und Ereignisse** > **Rules**. Klicken Sie mit der rechten Maustaste auf **Regeln**, um den Assistenten für **Regel verwalten** zu öffnen. Beim ersten Schritt wählen Sie einen Regeltypen aus und im Zweiten eine Bedingung.
2. In Schritt 3 von **Regel verwalten** (**Schritt 3: Aktionen**) wählen Sie die Aktion **Auf Matrix Ansicht stellen <Geräte>** aus.
3. Klicken Sie auf den Matrix-Link in der Beschreibung der ersten Regel.
4. Im Dialogfenster **Matrix-Konfiguration auswählen**, wählen Sie den relevanten Matrix-Empfänger und klicken Sie auf **OK**.
5. Klicken Sie auf den Link **Geräte** in der Beschreibung der ersten Regel und wählen Sie aus, von welcher Kamera aus Sie das Video an den Matrix-Empfänger senden möchten, und klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.
6. Klicken Sie auf **Fertig**, wenn die Regel abgeschlossen ist oder legen Sie nach Bedarf weitere Aktionen und/oder eine Anhalte-Aktion fest.

Wenn Sie einen Matrix-Empfänger entfernen, funktioniert keine der Regeln mehr, die diesen Matrix-Empfänger beinhalten.

## Matrix Empfänger hinzufügen

Zum Hinzufügen eines vorhandenen Matrix Empfängers in Management Client:

1. Klappen Sie **Clients** aus und wählen Sie **Matrix**.
2. Klicken Sie mit der rechten Maustaste auf **Matrix Konfigurationen** und wählen Sie **Hinzufügen Matrix** aus.
3. Füllen Sie die Felder im Dialogfenster **Hinzufügen Matrix** aus.
    1. Im Feld **Adresse** geben Sie die IP-Adresse oder den Hostname des Matrix-Empfängers ein.
    2. Geben Sie in das Feld **Port** die von der Matrix Empfängerinstallation verwendete Portnummer ein.
4. Klicken Sie auf **OK**.

Sie können nun die Matrix-Empfänger in Regeln verwenden.

Ihr System bestätigt nicht, ob die Portnummer oder Passwort korrekt ist oder ob Portnummer, Passwort oder Typ dem tatsächlichen Matrix-Empfänger entspricht. Stellen Sie also sicher, dass Sie die richtigen Informationen eingeben.

### Dasselbe Video an mehrere XProtect Smart Client Ansichten senden

Sie können dasselbe Video an Matrix Positionen in mehreren der XProtect Smart Client Ansichten senden, vorausgesetzt, die Matrix Positionen der Ansichten haben dieselbe Portnummer und dasselbe Passwort:

1. Erstellen Sie in XProtect Smart Client die zugehörigen Ansichten und Matrix Positionen, welche die gleiche Portnummer und Passwörter teilen.
2. In Management Client, fügen Sie die relevanten XProtect Smart Client als Matrix-Empfänger hinzu.
3. Sie können die Matrix-Empfänger in einer Regel einschließen.

## Regeln und Ereignisse

### Regeln hinzufügen

Wenn Sie Regeln hinzufügen, werden Sie durch den Assistenten **Regeln verwalten** geführt, in dem nur relevante Optionen aufgeführt sind.

Somit ist gewährleistet, dass in einer Regel keine erforderlichen Elemente fehlen. Je nach Regelinhalt empfiehlt er automatisch passende Stopp-Aktionen, d. h. was geschehen soll, wenn die Regel nicht mehr gilt. Dadurch wird sichergestellt, dass Sie nicht unbeabsichtigt eine endlose Regel erstellen.

#### Ereignisse

Wenn Sie eine Regel auf Ereignisbasis hinzufügen, können Sie verschiedene Arten von Ereignissen auswählen.

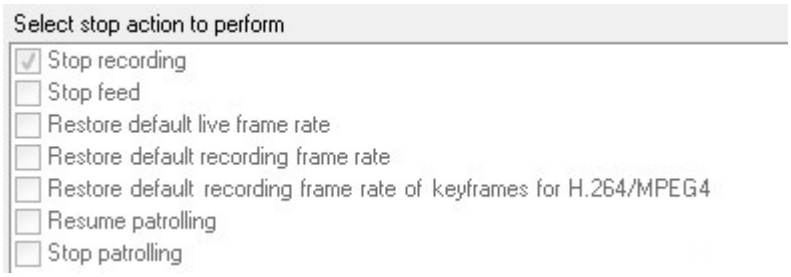
- Siehe Übersicht über Ereignisse, um sich eine Übersicht zu verschaffen und eine Beschreibung der Ereignistypen zu erhalten, die Sie auswählen können.

#### Aktionen und Stoppaktionen

Wenn Sie Regeln hinzufügen, können Sie verschiedene Aktionen auswählen.

Einige der Aktionen erfordern eine Stopp-Aktion. Wenn Sie z. B. die Aktion **Aufzeichnung starten** auswählen, beginnt die Aufzeichnung und wird u.U. unbegrenzt lange fortgesetzt. Aus diesem Grund hat die Aktion **Aufzeichnung starten** eine obligatorische Stopp-Aktion namens **Aufzeichnung stoppen**.

Der Assistent **Regel verwalten** stellt sicher, dass Sie Stopp-Aktionen festlegen, wenn dies erforderlich ist:




Auswählen von Stopp-Aktionen. Beachten Sie in dem Beispiel die obligatorische Stopp-Aktion (ausgewählt, ausgegraut), die irrelevanten Stopp-Aktionen (ausgegraut) und die optionalen Stopp-Aktionen (auswählbar).

- Unter Aktionen und Stoppaktionen finden Sie eine Übersicht über die Start- und Stoppaktionen, die Sie auswählen können.

### Regel erstellen

1. Klicken Sie mit der rechten Maustaste auf das Objekt in **Regeln** > **Regel hinzufügen**. Dadurch öffnet sich der Assistent **Regel verwalten**. Der Assistent begleitet Sie beim Bestimmen des Inhalts Ihrer Regel.
2. Geben Sie in den Feldern **Name** bzw. **Beschreibung** einen Namen und eine Beschreibung für die neue Regel an.
3. Wählen Sie den passenden Bedingungstyp für die Regel: entweder eine Regel, die eine oder mehrere Aktionen durchführt, wenn ein bestimmtes Ereignis eintritt, oder eine Regel, die eine oder mehrere Aktionen durchführt, wenn Sie einen bestimmten Zeitraum eingeben.
4. Klicken Sie auf **Weiter**, um mit dem zweiten Schritt des Assistenten fortzufahren. Definieren Sie im zweiten Schritt des Assistenten weitere Bedingungen für die Regel.

5. Wählen Sie eine oder mehrere Bedingungen aus, zum Beispiel **Der Wochentag ist <Tag>**:


Bearbeiten Sie die Beschreibung der Regel entsprechend Ihrer Auswahl im unteren Teil des Assistenten-Fensters:


Klicken Sie auf die unterstrichenen Elemente in **fetter Kursivschrift**, um ihren genauen Inhalt zu bestimmen. Wenn Sie zum Beispiel auf den Link **Tage** in unserem Beispiel klicken, können Sie einen oder mehrere Wochentage auswählen, an denen die Regel gelten soll.

6. Wenn Sie Ihre Bedingungen festgelegt haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt des Assistenten fortzufahren und auszuwählen, welche Aktionen die Regel abdecken soll. Dem Inhalt und der Komplexität Ihrer Regel entsprechend müssen Sie unter Umständen weitere Schritte festlegen, wie beispielsweise Stopp-Ereignisse und Stopp-Aktionen. Wenn eine Regel zum Beispiel vorsieht, dass ein Gerät eine bestimmte Aktion während eines bestimmten Zeitintervalls (zum Beispiel Donnerstag zwischen 08:00 und 10:30 Uhr) durchführt, könnte Sie der Assistent darum bitten, festzulegen, was nach Ablauf dieses Zeitintervalls geschehen soll.
7. Ihre Regel ist standardmäßig nach der Erstellung aktiv, wenn ihre Bedingungen erfüllt sind. Wenn Sie nicht wollen, dass die Regel sofort aktiv ist, entfernen Sie das Häkchen bei **Aktiv**.
8. Klicken Sie auf **Fertigstellen**.

## Regeln validieren

Sie können den Inhalt einer einzelnen Regel oder aller Regeln auf einmal validieren. Wenn Sie eine Regel erstellen, stellt der Assistent **Regel verwalten** sicher, dass alle Elemente der Regel gültig sind.

Wenn eine Regel einige Zeit lang bestanden hat, können ein oder mehrere Bestandteile der Regel durch eine andere Konfiguration beeinträchtigt worden sein, wodurch die Regel nicht mehr funktionieren könnte. Wenn beispielsweise eine Regel durch ein bestimmtes Zeitprofil ausgelöst wird, funktioniert die Regel nicht, wenn Sie das Zeitprofil gelöscht haben oder, wenn Sie keine Rechte mehr darauf haben. Es kann schwierig sein, den Überblick über solche unbeabsichtigten Konfigurationsauswirkungen zu behalten.

Die Regelvalidierung hilft Ihnen dabei, nachzuvollziehen, welche Regeln beeinträchtigt wurden. Die Validierung erfolgt pro Regel und jede Regel wird für sich genommen validiert. Sie können Regeln nicht untereinander validieren, zum Beispiel um herauszufinden, ob eine Regel im Konflikt zu einer anderen Regel steht, auch nicht mit der Funktion **Alle Regeln validieren**.

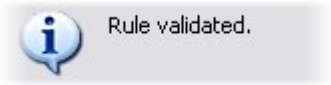
### Eine Regel validieren

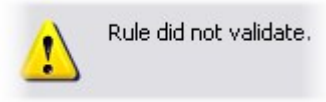
1. Klicken Sie auf **Regeln** und wählen Sie die Regel aus, die sie validieren wollen.
2. Klicken Sie mit der rechten Maustaste auf die Regel und klicken Sie dann auf **Regel validieren.**
3. Klicken Sie auf **OK**.

### Alle Regeln validieren

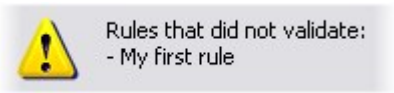
1. Klicken Sie mit der rechten Maustaste auf die **Regeln** und klicken Sie dann auf **Alle Regeln validieren**. .
2. Klicken Sie auf **OK**.

Ein Dialogfeld informiert Sie darüber, ob die Regel(n) erfolgreich validiert wurde(n) oder nicht. Wenn Sie sich dafür entschieden haben, mehr als eine Regel zu validieren, und eine oder mehrere Regeln nicht erfolgreich waren, so werden in der Dialogbox die Namen der betreffenden Regeln aufgeführt.








Sie können nicht validieren, ob die Konfiguration von Anforderungen außerhalb der Regel verhindert, dass die Regel funktioniert. Beispiel: Eine Regel, die bestimmt, dass die Aufzeichnung starten soll, wenn eine Bewegung von einer bestimmten Kamera erkannt wird, wird validiert, wenn die Bestandteile in der Regel selbst korrekt sind, auch wenn die Bewegungserkennung, die auf der Kameraebene aktiviert wird, nicht für die entsprechende Kamera aktiviert wurde.

## Bearbeiten, Kopieren und Umbenennen einer Regel

1. Klicken Sie im Bereich **Übersicht** mit der rechten Maustaste auf die entsprechende Regel.
2. Wählen Sie entweder:

   **Regel bearbeiten** oder **Regel kopieren** oder **Regel umbenennen**. Der Assistent **Regel verwalten** wird geöffnet.
3. Wenn Sie **Regel kopieren** auswählen, öffnet sich der Assistent und zeigt eine Kopie der ausgewählten Regel an. Klicken Sie auf **Beenden**, um eine Kopie zu erstellen.
4. Wenn Sie **Regel bearbeiten** auswählen, öffnet sich der Assistent, und Sie können Ihre Änderungen eingeben. Klicken Sie auf **Beenden**, um die Änderungen anzunehmen.
5. Wenn Sie **Regel umbenennen** auswählen, können Sie den Text für den Namen der Regel direkt umbenennen.

## Deaktivieren und Aktivieren einer Regel

Ihr System wendet eine Regel an, sobald die Bedingungen der Regel erfüllt sind. Die Regel ist somit aktiv. Wenn Sie nicht möchten, dass eine Regel aktiv ist, können Sie die Regel deaktivieren. Wenn Sie die Regel deaktivieren, wendet das System die Regel nicht an; nicht einmal, wenn die Bedingungen der Regel erfüllt sind. Sie können eine deaktivierte Regel später einfach wieder aktivieren.

**Deaktivieren einer Regel**

1. Wählen Sie im Bereich **Übersicht** die Regel aus.
2. Entfernen Sie im Bereich **Eigenschaften** das Häkchen bei **Aktiv**.
3. Klicken Sie in der Symbolleiste auf **Speichern**.
4. Ein Symbol mit einem roten „x“ bedeutet, dass die Regel in der Liste **Regeln** deaktiviert ist:


**Aktivieren einer Regel**

Wenn Sie die Regel wieder aktivieren wollen, wählen Sie die Regel aus, setzen Sie ein Häkchen bei **Aktivieren** und speichern Sie die Einstellung.

## Bestimmen eines Zeitprofils

1. Klicken Sie in der Liste **Zeitprofile** mit der rechten Maustaste auf **Zeitprofile** > **Zeitprofil hinzufügen**. Das Fenster **Zeitprofile** wird geöffnet.
2. Geben Sie im Fenster **Zeitprofil** einen Namen für das neue Zeitprofil in das Feld **Name** ein. Optional können Sie eine Beschreibung für das neue Zeitprofil im Feld **Beschreibung** eingeben.

3. Wählen Sie im Kalender des Fensters **Zeitprofil** entweder die **Tagesansicht**, **Wochenansicht** oder **Monatsansicht** aus, klicken mit der rechten Maustaste und wählen Sie dann entweder **Einzelne Zeit hinzufügen** oder **Serienzeit hinzufügen** aus.
4. Wenn Sie die Zeiträume für das Zeitprofil bestimmt haben, klicken Sie im Fenster **Zeitprofil** auf **OK**. Das System fügt Ihr neues Zeitprofil zu der Liste **Zeitprofile** hinzu. Wenn Sie das Zeitprofil später bearbeiten oder löschen möchten, können Sie dies ebenfalls über die Liste **Zeitprofile** tun.

### Hinzufügen einer einzelnen Zeit

Wenn Sie **Einzelne Zeit hinzufügen** auswählen, erscheint das Fenster **Zeit auswählen**:


Auf Ihrem Computer wird möglicherweise ein anderes Uhrzeit- und Datumsformat verwendet.

1. Bestimmen Sie im Fenster **Zeit auswählen** eine **Startzeit** und eine **Endzeit**. Wenn die Zeit ganze Tage abdecken soll, setzen Sie ein Häkchen bei **Ganztägiges Ereignis**.
2. Klicken Sie auf **OK**.

### Wiederholte Zeit hinzufügen

Wenn Sie **Serienzeit hinzufügen** auswählen, erscheint das Fenster **Serienzeit auswählen**:


1. Bestimmen Sie im Fenster **Zeit auswählen** den Zeitraum, das Serienmuster und die Seriendauer.
2. Klicken Sie auf **OK**.

Ein Zeitprofil kann mehrere Zeiträume beinhalten. Wenn Sie möchten, dass Ihr Zeitprofil weitere Zeiträume beinhaltet, fügen Sie weitere einzelne Zeiten oder Serienzeiten hinzu.

#### Wiederholte Zeit

Wenn Sie eine Aktion einrichten, die nach einem detaillierten, sich wiederholenden Zeitplan ausgeführt werden soll.

Beispielsweise:

- Jede Woche Dienstags, alle 1 Stunde(n) zwischen 15:00 und 15:30
- Am 15. alle 3 Monat(e) um 11:45 Uhr
- Jeden Tag alle 1 Stunde(n) zwischen 15:00 und 19:00 Uhr

Die Zeit basiert auf den örtlichen Zeiteinstellungen des Servers, auf dem Management Client installiert ist.

## Bearbeiten eines Zeitprofils

1. Klicken Sie in der Liste **Zeitprofile** im Bereich **Übersicht** mit der rechten Maustaste auf das gewünschte Zeitprofil und wählen Sie **Zeitprofil bearbeiten** aus. Das Fenster **Zeitprofile** wird geöffnet.
2. Bearbeiten Sie das Zeitprofil nach Bedarf. Wenn Sie Änderungen am Zeitprofil vorgenommen haben, klicken Sie im Fenster **Zeitprofil** auf **OK**. Sie kehren zur Liste **Zeitprofile** zurück.


Im Fenster **Zeitprofilinformation** können Sie das Zeitprofil nach Bedarf bearbeiten. Beachten Sie, dass ein Zeitprofil mehrere Zeiträume beinhalten kann und dass Zeiträume wiederkehren können. Die kleine Monatsübersicht in der Ecke rechts oben kann Ihnen dabei helfen, schnell einen Überblick über die Zeiträume zu erhalten, die von einem Zeitprofil abgedeckt werden, da Daten mit festgelegten Zeiten fett hervorgehoben werden.

In diesem Beispiel zeigen die Daten in Fettdruck, dass Sie Zeiträume für mehrere Tage bestimmt haben und dass Sie für eine Serienzeit für Montage bestimmt haben.

## Tageslängen-Zeitprofile erstellen

1. Erweitern Sie den Ordner **Regeln und Ereignisse** > **Zeitprofile**.
2. Klicken Sie auf der Liste **Zeitprofile** mit der rechten Maustaste auf **Zeitprofile** und wählen Sie **Hinzufügen eines Tageslängen-Zeitprofils** aus.
3. In den Fenster **Tageslängen-Zeitprofil** finden Sie weiter unten die Tabelle mit den Eigenschaften, in die Sie die erforderlichen Informationen eintragen können. Für die Regelung der Übergangszeiten zwischen Tag und Nacht können Sie die Aktivierung und Deaktivierung des Profils verschieben. Zeit und Monatsnamen werden entsprechend den Sprach- und Regionseinstellungen Ihres Computers angezeigt.
4. Um den Ort der eingegebenen geographischen Koordinaten auf einer Karte zu sehen, klicken Sie auf **Position in Browser anzeigen**. Dadurch wird ein Browser mit einer Karte geöffnet, auf der Sie den Standort sehen können.
5. Klicken Sie auf **OK**.

### Eigenschaften der Tageslängen-Zeitprofile

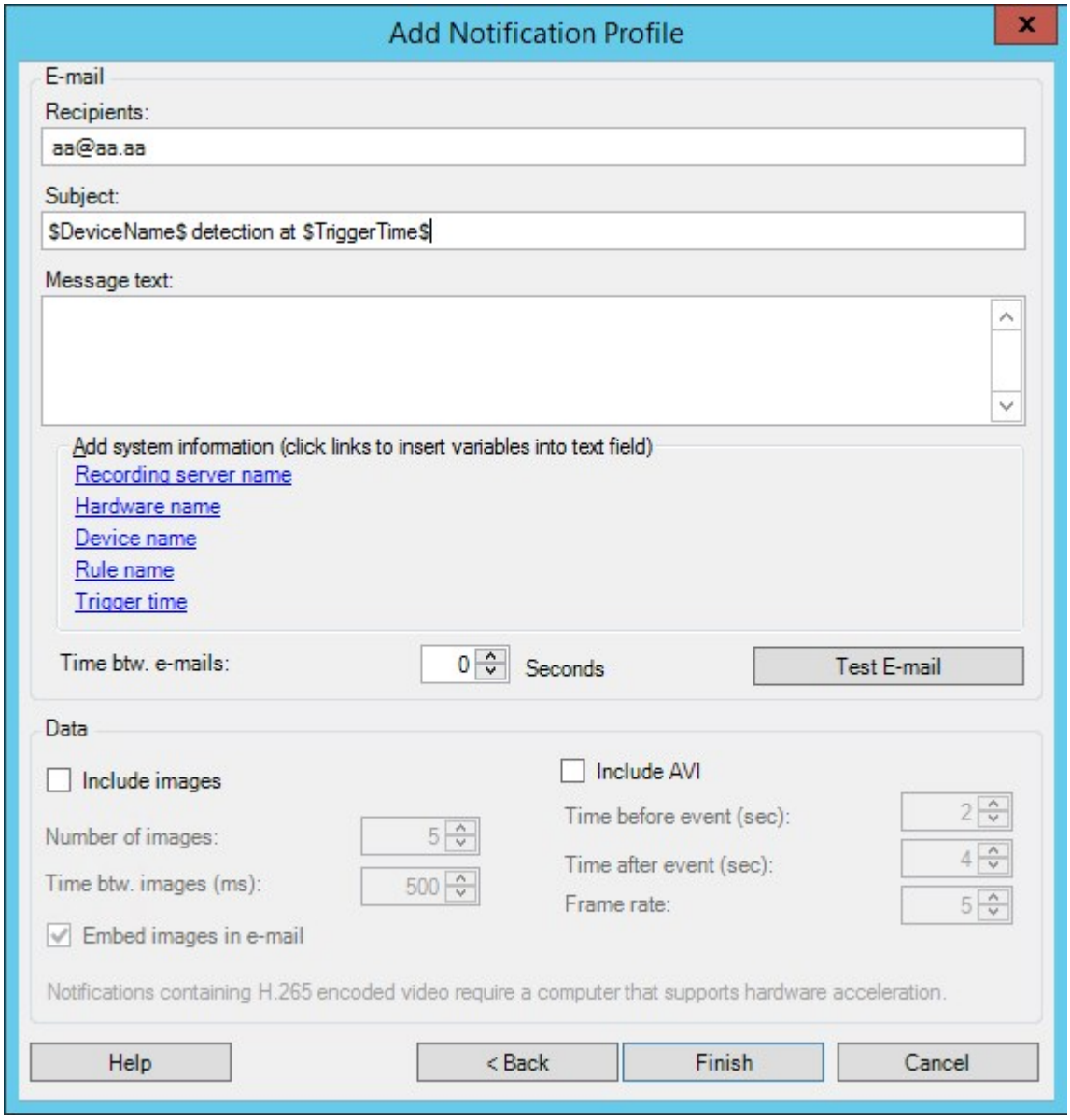
| Name | Beschreibung |
|---|---|
| **Name** | Der Name des Profils. |
| **Beschreibung** | Eine Beschreibung des Profils (optional). |
| **Geokoordinaten** | Die geographischen Koordinaten, die den physischen Standort der Kamera(s) anzeigen, die dem Profil zugeordnet sind. |
| **Offset Sonnenaufgang** | Anzahl der Minuten (+/-), um die die Aktivierung des Profils durch den Sonnenaufgang verschoben wird. |
| **Offset Sonnenuntergang** | Anzahl der Minuten (+/-), um die die Deaktivierung des Profils durch den Sonnenuntergang verschoben wird. |
| **Zeitzone** | Zeitzone, die den physischen Standort der Kamera(s) anzeigt. |

## Hinzufügen von Benachrichtigungsprofilen

Bevor Sie ein Benachrichtigungsprofil erstellen können, müssen Sie die Einstellungen für den ausgehenden Mailserver für die E-Mailbenachrichtigungen festlegen. Weitere Informationen finden Sie unter Anforderungen an die Erstellung von Benachrichtigungsprofilen.

1. Erweitern Sie **Regeln und Ereignisse** und klicken Sie mit der rechten Maustaste auf **Benachrichtigungsprofile** > **Benachrichtigungsprofil hinzufügen**. Der Assistent **Benachrichtigungsprofil hinzufügen** wird geöffnet.
2. Geben Sie Namen und Beschreibung ein. Klicken Sie auf **Weiter**.

3. Geben Sie Empfänger, Betreff, Nachrichtentext und Zeit zwischen E-Mails ein:




4. Um an die angegebenen Empfänger eine Test-E-Mailbenachrichtigung zu senden, klicken Sie auf **Test-E-Mail**.

5. Um Voralarm-Standbilder einzubinden, wählen Sie **Bilder einschließen** und geben Folgendes ein: die Anzahl der Bilder, die Zeit zwischen den Bildern und, ob die Bilder in die E-Mails eingebettet werden sollen oder nicht.

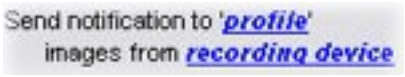
6. Um AVI-Videoclips einzubinden, wählen Sie **AVI beifügen** und bestimmen Sie die Zeit vor und nach dem Ereignis sowie die Bildrate.

> Benachrichtigungen mit H.265-verschlüsselten Videodaten erfordern einen Computer, der die Hardwarebeschleunigung unterstützt.

7. Klicken Sie auf **Fertigstellen**.

## Benachrichtigungen per E-Mail nach Regeln auslösen

1. Klicken Sie mit der rechten Maustaste auf das Objekt **Regeln**, und klicken Sie dann auf **Regel hinzufügen** oder **Regel bearbeiten**.
2. Klicken Sie in dem Assistenten **Regel verwalten** auf **Weiter**, um zu der Liste **Auszuführende Aktionen auswählen** zu gelangen, und wählen Sie dann **Benachrichtigung senden an <Profil>**.
3. Wählen Sie das jeweilige Benachrichtigungsprofil und wählen Sie die Kameras aus, von denen die Aufzeichnungen kommen sollen, die in den Benachrichtigungen an das Benachrichtigungsprofil per E-Mail enthalten sein sollen.




In den Benachrichtigungen an das Benachrichtigungsprofil können nur dann Aufzeichnungen enthalten sein, wenn tatsächlich etwas aufgezeichnet wird. Wenn Sie Standbilder oder AVI-Videoclips in den E-Mailbenachrichtigungen einschließen möchten, überprüfen Sie, ob die Regel bestimmt, dass eine Aufzeichnung erfolgen soll. Das folgende Beispiel basiert auf einer Regel, die sowohl die Aktion **Aufzeichnung starten** als auch **Benachrichtigung senden an** enthält:


## Benutzerdefiniertes Ereignis hinzufügen

> Ungeachtet dessen, wie Sie benutzerdefinierte Ereignisse verwenden möchten, müssen Sie jedes benutzerdefinierte Ereignis über Management Client hinzufügen.

1. **Regeln und Ereignisse** ausklappen > **Benutzerdefinierte Ereignisse**.
2. Im Bereich **Übersicht**, klicken Sie mit der rechten Maustaste auf **Ereignisse** > **Benutzerdefiniertes Ereignis** hinzufügen.
3. Geben Sie einen Namen für das neue benutzerdefinierte Ereignis ein und klicken Sie dann auf **OK**. Das neu hinzugefügte benutzerdefinierte Ereignis wird nun in der Liste im Bereich **Übersicht** angezeigt.

Der Benutzer kann nun das benutzerdefinierte Ereignis in XProtect Smart Client von Hand auslösen, wenn er dazu berechtigt ist.

Bei Löschung eines benutzerdefinierten Ereignisses ist jede Regel, die von ihr verwendet wurde, betroffen. Ein entferntes benutzerdefiniertes Ereignis verschwindet auch nur von XProtect Smart Client, wenn die XProtect Smart Client-Benutzer sich abmelden.

## Benutzerdefiniertes Ereignis umbenennen

Wenn Sie ein benutzerdefiniertes Ereignis umbenennen, müssen bereits verbundene XProtect Smart Client-Benutzer ausloggen und wieder einloggen, bevor die Namensänderung sichtbar wird.

1. **Regeln und Ereignisse** ausklappen > **Benutzerdefinierte Ereignisse**.
2. Wählen Sie das benutzerdefinierte Ereignis im Bereich **Übersicht** aus.
3. Überschreiben Sie den bestehenden Namen im Bereich **Eigenschaften**.
4. Klicken Sie in der Symbolleiste auf **Speichern**.

## Ein Analyseereignis hinzufügen und bearbeiten

### Ein Analyseereignis hinzufügen

1. Erweitern Sie **Regeln und Ereignisse**, klicken Sie mit der rechten Maustaste auf **Analyseereignisse** und wählen Sie **Neu hinzufügen** aus.
2. Geben Sie im Fenster **Eigenschaften** einen Namen für das Ereignis in das Feld **Name** ein.
3. Falls nötig, geben Sie im Feld **Beschreibung** einen Beschreibungstext ein.
4. Klicken Sie in der Symbolleiste auf **Speichern**. Sie können die Gültigkeit eines Ereignisses testen, durch Anklicken von **Ereignis testen**. Sie können jederzeit Fehler, die im Test angezeigt werden korrigieren und den Test so oft wie Sie möchten und zu jeder Zeit neu ausführen.

### Ein Analyseereignis bearbeiten

1. Klicken Sie auf ein bestehendes Analyseereignis, um das Fenster **Eigenschaften** anzeigen zu lassen, in dem Sie relevante Felder bearbeiten können.
2. Sie können die Gültigkeit eines Ereignisses testen, durch Anklicken von **Ereignis testen**. Sie können jederzeit Fehler, die im Test angezeigt werden korrigieren und den Test so oft wie Sie möchten und zu jeder Zeit neu ausführen.

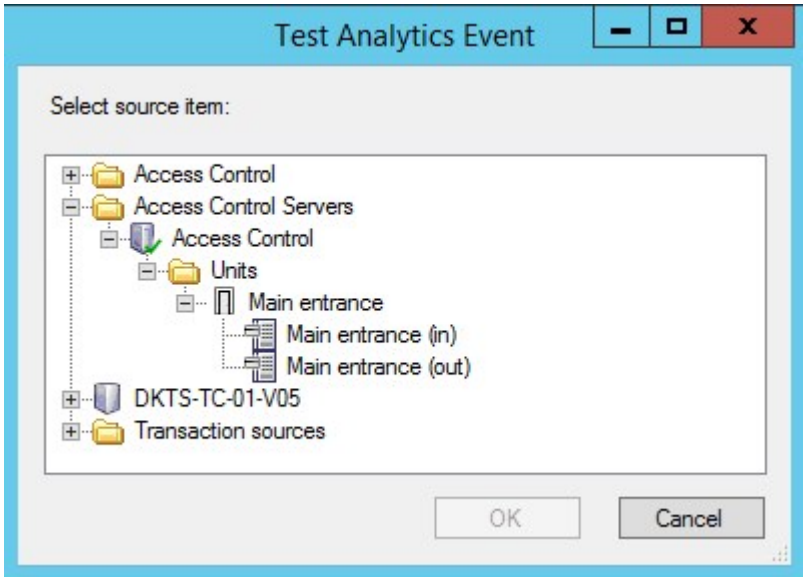
### Einstellungen für Analyseereignisse bearbeiten

Gehen Sie in der Symbolleiste auf **Tools** > **Optionen** > Registerkarte **Analyseereignisse**, um relevante Einstellungen zu bearbeiten.

## Ein Analyseereignis testen

Wenn Sie ein Analytikereignis erstellt haben, können Sie die Anforderungen testen (siehe Ein Analyseereignis hinzufügen und bearbeiten auf Seite 304), z.B. ob die Analytikereignisfunktion in Management Client aktiviert wurde.

1. Wählen Sie ein bestehendes Analyseereignis aus.
2. KlickenSieindenEigenschaftenaufdieSchaltfläche**Ereignistesten**.EinFenstermitallenmöglichenQuellendes Ereignisseserscheint.




3. Wählen Sie die Quelle für Ihr Testereignis, zum Beispiel eine Kamera. Das Fenster wird geschlossen und ein neues Fenster erscheint, welches vier Bedingungen fordert, damit das Analyseereignis funktioniert.

Sie können als zusätzlichen Test in XProtect Smart Client bestätigen, dass das Analyseereignis an den Event Server gesendet wurde. Dafür öffnen Sie einfach XProtect Smart Client und sehen dann das Ereignis auf der Registerkarte **Alarm-Manager**.

## Hinzufügen eines generischen Ereignisses

Sie können generische Ereignisse definieren und damit der VMS dabei helfen, bestimmte Zeichenketten in TCP- und UDP-Paketen von einem externen System zu erkennen. Dem generischen Ereignis entsprechend können Sie den Management Client dazu konfigurieren, Aktionen auszulösen, z. B. mit der Aufzeichnung oder Alarme zu starten.

**Voraussetzungen**
Sie haben generische Ereignisse aktiviert sowie die zugelassenen Quellen und Ziele bestimmt. Weitere Informationen finden Sie unter Registerkarte „Generische Ereignisse“ (Optionen) auf Seite 430.

Ein Generisches Ereignis hinzufügen:

1. Erweitern Sie **Regeln und Ereignisse**.
2. Klicken Sie mit der rechten Maustaste auf **Generisches Ereignis** und wählen Sie die Option **Neu hinzufügen** aus.
3. Geben Sie die erforderlichen Informationen und Eigenschaften ein. Weitere Informationen finden Sie unter Generische Ereignis- und Datenquellen (Eigenschaften) auf Seite 551.
4. (Optional) Um zu validieren, ob ein Suchausdruck gültig ist, geben Sie den Suchstring in das Feld **Prüfen Sie, ob der Ausdruck mit dem Ereignis-String übereinstimmt** ein, das dem erwarteten Paket entspricht:
   - **Übereinstimmung** - der String kann mit dem Suchausdruck validiert werden
   - **Keine Übereinstimmung** - der Suchausdruck ist ungültig. Ändern Sie ihn und versuchen Sie es erneut

Im XProtect Smart Client können Sie überprüfen, ob Ihre generischen Ereignisse vom Event Server empfangen wurden. Das können Sie in der **Alarmliste** auf der Registerkarte **Alarm-Manager** machen, indem Sie **Ereignisse** auswählen.

# Authentifizierung

## Ansprüche von einem externen IDP registrieren

1. Wählen Sie in Management Client **Extras** > **Optionen** und öffnen Sie die Registerkarte externer **IDP**.
2. Wählen Sie im Abschnitt **externer IDP** die Option **Hinzufügen**.
3. Wählen Sie im Abschnitt **Registrierte Ansprüche** die Option **Hinzufügen**.

4. Machen Sie erforderlichen Angaben zu dem Anspruch. Weitere Informationen finden Sie unter Ansprüche registrieren.

## Zuordnung von Ansprüchen aus einer externen IDP zu Rollen in XProtect

Auf der Seite externer IDP muss der Administrator Ansprüche anlegen, die aus einem Namen und einem Wert bestehen. Später wird der Anspruch einer Rolle im VMS zugeordnet, und die Berechtigungen des Benutzers werden durch die Rolle bestimmt.

1. Erweitern Sie im **Navigationsbereich** in Management Client den Knoten **Sicherheit** und wählen Sie **Rollen** aus.
2. Wählen Sie eine Rolle, wählen Sie die Registerkarte **Externer IDP** und wählen Sie dann **Hinzufügen** aus.
3. Wählen Sie einen externen IDP und einen Anspruchsnamen und geben Sie einen Anspruchswert ein.

   Der Anspruchsname muss genau so geschrieben werden wie der Anspruchsname aus dem externen IDP.

4. Wählen Sie **OK**.

Wenn ein externer IDP im externen IDP gelöscht wird, werden auch alle Benutzer gelöscht, die über den externen IDP mit dem VMS verbunden sind. Alle registrierten Ansprüche, die mit dem externen IDP verbunden sind, werden entfernt und auch alle Zuordnungen zu Rollen.

## Anmeldung über einen externen IDP

Bei XProtect Smart Client, XProtect Management Client, XProtect Web Client, und dem XProtect Mobile-Client können Sie sich mit einem externen IDP anmelden.

1. Wählen Sie unter **Authentifizierung** im Anmeldedialogfeld in XProtect Smart Client oder XProtect Management Client den externen IDP und wählen Sie **Anmelden** aus. Bei der ersten Anmeldung werden Sie auf eine Webseite umgeleitet, die zum externen IDP gehört.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und melden Sie sich an. Nachdem Sie sich angemeldet haben, kehren Sie zum XProtect-Client zurück. Sie sind nun eingeloggt.

Unter **Extras** > **Optionen** > **Externer IDP** können Sie den Namen des externen IDP konfigurieren, der auf der Liste **Authentifizierung** angezeigt wird.

Wenn der externe IDP deaktiviert ist, z. B. durch eine Wiederherstellung oder eine Passwortänderung, wird die Option zur Anmeldung über einen externen IDP auf der Liste **Authentifizierung** nicht angeboten. Und wenn der externe IDP deaktiviert ist, verschwindet das vom externen IDP empfangene Client-Geheimnis aus dem Feld **Client-Geheimnis** auf der Registerkarte **Externer IDP** unter **Extras** > **Optionen**.

## Sicherheit

### Hinzufügen und Verwalten einer Rolle

1. Erweitern Sie **Sicherheit** und klicken Sie mit der rechten Maustaste auf **Rollen**.
2. Wählen Sie **Rolle hinzufügen**. Das Dialogfeld **Rolle hinzufügen** öffnet sich.
3. Geben Sie einen Namen und eine Beschreibung für die neue Rolle ein und klicken Sie auf **OK**.
4. Die neue Rolle wird der Liste **Rollen** hinzugefügt. Standardmäßig ist eine neue Rolle nicht mit Benutzern oder Gruppen verknüpft, aber mit einigen Standardprofilen.
5. Um verschiedene Smart Client- und Management Client-Profile, Beweissicherungsprofile oder Zeitprofile auszuwählen, klicken Sie auf die Dropdown-Listen.
6. Sie können jetzt Benutzer/Gruppen der Rolle zuweisen und festlegen, auf welche Systemfunktionen sie Zugriff haben.

Weitere Informationen finden Sie unter Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen auf Seite 309 und Rollen (Sicherheitsknoten) auf Seite 553.

### Kopieren, Umbenennen oder Löschen einer Rolle

#### Kopieren einer Rolle

Wenn Sie eine Rolle mit komplizierten Einstellungen und/oder Berechtigungen haben und eine ähnliche oder fast ähnliche Rolle benötigen, kann es einfacher sein, die bereits vorhandene Rolle zu kopieren und kleinere Anpassungen an der Kopie vorzunehmen, als von Grund auf eine neue Rolle zu erstellen.

1. Erweitern Sie **Sicherheit**, klicken Sie auf **Rollen**, klicken Sie mit der rechten Maustaste auf die gewünschte Rolle und wählen Sie **Rolle kopieren**.
2. Es erscheint ein Dialogfenster; geben Sie der kopierten Rolle einen neuen einmaligen Namen und eine Beschreibung.
3. Klicken Sie auf **OK**.

#### Umbenennen einer Rolle

Wenn Sie eine Rolle umbenennen, ändert sich damit nicht der Name der Ansichtsgruppe, die auf der Rolle basiert.

1. Erweitern Sie **Sicherheit** und klicken Sie mit der rechten Maustaste auf **Rollen**.
2. Klicken Sie mit der rechten Maustaste auf die gewünschte Rolle und wählen Sie **Rolle umbenennen**.
3. Es erscheint ein Dialogfenster; ändern Sie den Namen der Rolle.
4. Klicken Sie auf **OK**.

Löschen einer Rolle

1. Erweitern Sie **Sicherheit** und klicken Sie auf **Rollen**.
2. Klicken Sie mit der rechten Maustaste auf die zu löschende Rolle und wählen Sie **Rolle löschen**.
3. Klicken Sie auf **Ja**.

> Wenn Sie eine Rolle löschen, entfernen Sie damit nicht die Ansichtsgruppe, die auf der Rolle basiert.

### Effektive Rollen anzeigen

Mit der Funktion „Effektive Rollen“ können Sie alle Rollen eines ausgewählten Benutzers oder einer ausgewählten Gruppe ansehen. Das ist praktisch bei der Verwendung von Gruppen und es ist die einzige Methode zum Überprüfen, welche Rollen ein bestimmter Benutzer hat.

1. Öffnen Sie das Fenster **Effektive Rollen**, indem Sie **Sicherheit** erweitern, mit der rechten Maustaste auf **Rollen** klicken und dann **Effektive Rollen** auswählen.
2. Wenn Sie Informationen über einen Basisnutzer erhalten möchten, geben Sie den Namen in das Feld **Benutzername** ein. Klicken Sie auf **Aktualisieren**, um die Rollen des Benutzers anzuzeigen.
3. Wenn Sie Windows-Benutzer oder -Gruppen in Active Directory verwenden, klicken Sie auf die **...**-Schaltfläche zum Durchsuchen. Wählen Sie den Objekttyp, geben Sie den Namen ein und klicken Sie dann auf **OK**. Die Rollen des Benutzers werden automatisch angezeigt.

### Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen

Um Windows-Benutzer oder -Gruppen oder Basisnutzer Rollen zuzuweisen oder aus Rollen zu entfernen:

1. Erweitern Sie **Sicherheit** und wählen Sie **Rollen**. Wählen Sie dann die gewünschte Rolle im Bereich **Übersicht**:
2. Wählen Sie unten im Bereich **Eigenschaften** die Registerkarte **Benutzer und Gruppen**.
3. Klicken Sie auf **Hinzufügen** und wählen Sie zwischen **Windows-Benutzer** und **Basisnutzer**.

Zuweisen von Windows-Benutzern und -Gruppen zu einer Rolle

1. Wählen Sie **Windows-Benutzer**. Dadurch öffnen sich die Dialogfelder **Benutzer auswählen** und **Computer und Gruppen**:
2. Verifizieren Sie, dass der erforderliche Objekttyp festgelegt wurde. Wenn Sie z. B. einen Computer hinzufügen möchten, klicken Sie auf **Objekttypen** und markieren Sie **Computer**. Verifizieren Sie, dass die gewünschte Domäne im Feld **Von diesem Speicherort** festgelegt ist. Wenn nicht, klicken Sie auf **Standorte**, um zur gewünschten Domäne zu navigieren.
3. In das Feld **Auszuwählende Objektnamen eingeben** geben Sie die gewünschten Benutzernamen, Initialen oder andere Identifikationsarten ein, die Active Directory erkennen kann. Verwenden Sie die Funktion **Namen überprüfen**, um zu verifizieren, dass Active Directory die Namen oder Initialen erkennt, die Sie eingegeben haben. Alternativ können Sie die Funktion **"Erweitert..."** verwenden, um nach Benutzern oder Gruppen zu suchen.
4. Klicken Sie auf **OK**. Die ausgewählten Benutzer/Gruppen werden jetzt der Benutzerliste der Registerkarte **Benutzer und Gruppen** hinzugefügt, denen Sie die ausgewählte Rolle zugeteilt haben. Sie können weitere Benutzer und Gruppen hinzufügen, indem sie mehrere Namen eingeben, die mittels eines Strichpunkts (**;**) voneinander abgetrennt sind.

Zuweisen von Basisnutzer zu einer Rolle

1. Wählen Sie **Basisnutzer**. Das Dialogfeld **Basisnutzer zum Hinzufügen zur Rolle auswählen** öffnet sich:
2. Wählen die Basisnutzer aus, die Sie dieser Rolle zuweisen möchten.
3. Optional: Klicken Sie auf **Neu**, um einen neuen Basisnutzer zu erstellen.
4. Klicken Sie auf **OK**. Die ausgewählten Basisnutzer werden jetzt der Basisnutzerliste der Registerkarte **Benutzer und Gruppen** hinzugefügt, denen Sie die ausgewählte Rolle zugeteilt haben.

Entfernen von Benutzern und Gruppen aus einer Rolle

1. Wählen Sie auf der Registerkarte **Benutzer und Gruppen** den Benutzer oder die Gruppe aus, die Sie entfernen möchten, und klicken Sie auf **Entfernen** im unteren Teil der Registerkarte. Sie können mehrere Benutzer oder Gruppen oder bei Bedarf eine Kombination von Gruppen und einzelnen Benutzern auswählen.
2. Bestätigen Sie, dass Sie die ausgewählten Benutzer und/oder Gruppen entfernen möchten. Klicken Sie auf **Ja**.

Ein Benutzer kann auch Rollen durch Gruppenmitgliedschaften haben. Wenn das der Fall ist, können Sie den einzelnen Benutzer nicht aus der Rolle entfernen. Gruppenmitglieder können auch als Personen Rollen haben. Um herauszufinden, welche Rollen Benutzer, Gruppen oder einzelne Gruppenmitglieder haben, verwenden Sie die Funktion **Effektive Rollen anzeigen**.

### Erstellen von Basisnutzer

In Milestone XProtect VMSgibt es zwei Arten von Benutzerkonten:  Basisnutzer und Windows Nutzer.

Basisnutzer sind Benutzerkonten, die Sie in Milestone XProtect VMS erstellen. Es handelt sich um ein dediziertes Systembenutzerkonto mit einem grundlegenden Benutzernamen und einem Passwort für die Authentifizierung des einzelnen Nutzers.

Windows Nutzer sind Benutzerkonten, die Sie über Microsofts Active Directoryhinzufügen.

Es gibt einige Unterschiede zwischen Basisnutzern und Windows Nutzern:

-  Basisnutzer authentifizieren sich durch einen Benutzernamen und ein Passwort und bestehen speziell für ein System/Standort. Beachten Sie, dass selbst wenn ein Basisnutzer, der an einem föderalen Standort erstellt wurde, denselben Namen und dasselbe Passwort hat wie ein Basisnutzer an einem anderen föderalen Standort, der Basisnutzer nur Zugang zu dem Standort hat, an dem er erstellt wurde.
-  Windows Nutzer authentifizieren sich auf Basis ihrer Windows Anmeldung und sind auf einen bestimmten Computer beschränkt.

#### Konfiguration der Anmeldeeinstellungen für Basisnutzer

Sie können die Anmeldeeinstellungen für Basisnutzer in einer JSON-Datei definieren, die sich hier befindet: `\\Program Files\Milestone\Management Server\IIS\IDP\appsettings.json`.

In dieser Datei können Sie die folgenden Parameter festlegen:

| | |
|---|---|
| LoginSettings | |
| "ExpireTimeInMinutes": 5 | Definieren Sie die Zeitspanne (in Minuten), nach der eine Anmeldesitzung abläuft, wenn der Benutzer nichts unternimmt. |
| LockoutSettings | |
| "LockoutTimeSpanInMinutes": 5 | Definieren Sie die Dauer (in Minuten), für die ein Benutzer gesperrt wird. |
| "MaxFailedAccessAttempts": 5 | Legen Sie die Anzahl der Anmeldeversuche eines Benutzers fest, bevor er gesperrt wird. |
| PasswordSettings | |
| "RequireDigit": true | Legen Sie fest, ob im Kennwort Basisziffern (0 bis 9) erforderlich |

| | |
|---|---|
| | sind. |
| "RequireLowercase": true | Legen Sie fest, ob im Kennwort Kleinbuchstaben verwendet werden müssen. |
| "RequireNonAlphanumeric": true | Legen Sie fest, ob im Passwort Sonderzeichen (~!@#$%^&*_-+=\|\(){}[]:;"'<>,.?/) verwendet werden müssen. |
| "RequireUppercase": true | Legen Sie fest, ob im Passwort Großbuchstaben verwendet werden müssen. |
| "RequiredLength": 8 | Legen Sie fest, wie viele Zeichen das Passwort haben muss. Das Passwort muss mindestens {0} und darf höchstens 255 Zeichen haben. |
| "RequiredUniqueChars": 1 | Legen Sie fest, wie viele einmalige Zeichen das Passwort mindestens haben muss.<br>Wenn Sie zum Beispiel die Anzahl der einmaligen Zeichen auf 2 festlegen, werden Passwörter wie – aaaaaa, aa, a, b, bb, bbbbbbb – abgelehnt.<br>Dagegen werden - abab, abc, aaab usw. - akzeptiert, da das Passwort mindestens zwei einmalige Zeichen enthält.<br>Die Erhöhung der Anzahl einmaliger Zeichen in einem Passwort erhöht die Passwortstärke, da wiederholte Sequenzen vermieden werden, die leicht zu erraten sind. |

So erstellen Sie einen Basisnutzer auf Ihrem System:

1. Erweitern Sie **Sicherheit** > **Basisnutzer**.
2. Klicken Sie mit der rechten Maustaste auf das Feld **Basisnutzer**, und wählen Sie die Option **Basisnutzer erstellen** aus.
3. Geben Sie einen Benutzernamen und ein Passwort an. Wiederholen Sie das Passwort, um sicherzugehen, dass Sie es richtig eingegeben haben.

   Das Passwort muss der Komplexität entsprechen, die in der Datei **appsettings.json** festgelegt ist (siehe Konfiguration der Anmeldeeinstellungen für Basisnutzer auf Seite 311).
4. Geben Sie an, ob der Basisnutzer bei der nächsten Anmeldung sein Passwort ändern soll. Milestone empfiehlt Ihnen, das Kontrollkästchen zu aktivieren, damit Basisnutzer bei der Erstanmeldung ihre eigenen Passwörter angeben können.

Sie sollten das Kontrollkästchen nur deaktivieren, wenn Sie Basisnutzer anlegen, die ihr Passwort nicht ändern können. Solche Basisnutzer sind z. B. Systembenutzer, die für die Authentifizierung von Plug-ins und Serverdiensten verwendet werden.

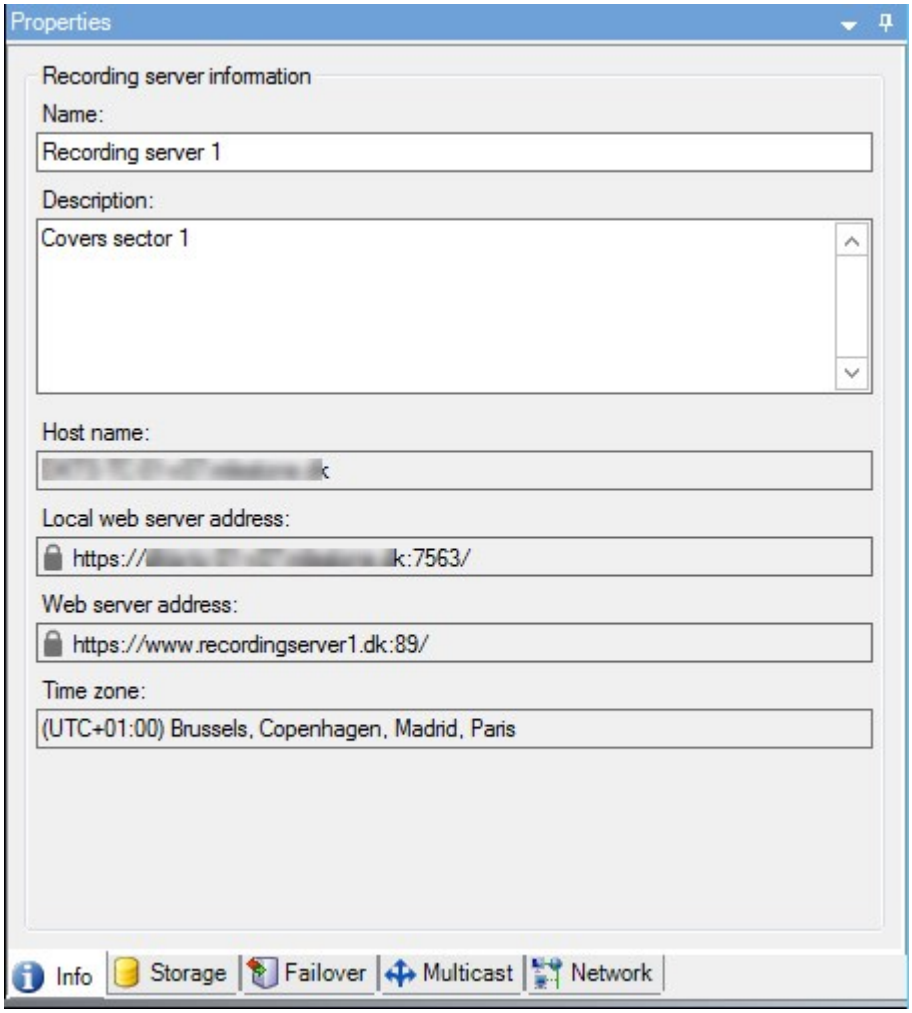
5. Geben Sie den Status des Basisnutzers als **Aktiv** oder **Ausgesperrt** an.
6. Klicken Sie auf **OK**, um den Basisnutzer zu erstellen.

### Verschlüsselungsstatus an Clients anzeigen

Um zu überprüfen, ob Ihr Aufzeichnungsserver eine Verschlüsselung verwendet:

1. Öffnen Sie den Management Client.
2. Wählen Sie im Bereich **Standort-Navigation** die Optionen **Server** > **Aufzeichnungsserver**. Daraufhin wird eine Liste mit Aufzeichnungsservern geöffnet.

3. Wählen Sie in dem Fenster **Übersicht** den jeweiligen Aufzeichnungsserver aus und gehen Sie auf die Registerkarte **Info**.
   Wenn die Verschlüsselung zu Clients und Servern, die Datenstreams vom Aufzeichnungsserver abrufen, aktiviert ist, erscheint ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der des optionalen Webservers.




# System-Dashboard

## Anzeige aktuell laufender Aufgaben auf Aufzeichnungsservern

Das Fenster **Aktuelle Aufgaben** zeigt eine Übersicht über laufende Aufgaben für den ausgewählten Aufzeichnungsserver. Wenn Sie eine Aufgabe ausgelöst haben, die über längere Zeit im Hintergrund läuft, können Sie das Fenster **Aktuelle Aufgaben** öffnen, um zu sehen, welche Fortschritte die Aufgabe macht. Beispiele für langwierige Aufgaben, die vom Benutzer ausgelöst werden können, sind Firmware-Updates und das Verschieben von Hardware. Dort finden Sie Informationen zur Anfangszeit, zur geschätzten Endzeit und zum Fortschritt der Aufgabe.

Wenn eine Aufgabe nicht die erwarteten Fortschritte macht, ist die Ursache dafür wahrscheinlich in Ihrer Hardware oder Ihrem Netzwerk zu finden. Beispiele hierfür sind: der Server läuft nicht, ein Serverfehler, eine zu geringe Bandbreite oder ein Verbindungsabbruch.

1. Wählen Sie aus dem Bereich **Standortnavigation** das **System Dashboard** > **Aktuelle Aufgaben** aus.
2. Wählen Sie einen Aufzeichnungsserver, um dessen aktuelle Aufgaben angezeigt zu bekommen.

Die Angaben in dem Fenster **Aktuelle Aufgaben** werden nicht dynamisch aktualisiert, sondern zeigen eine Momentaufnahme der aktuellen Aufgaben in dem Augenblick, wo Sie das Fenster öffnen. Wenn Sie das Fenster schon länger geöffnet haben, aktualisieren Sie die Informationen, indem Sie auf die Schaltfläche **Aktualisieren** in der unteren rechten Ecke des Fensters klicken.

## Systemmonitor (Erklärung)

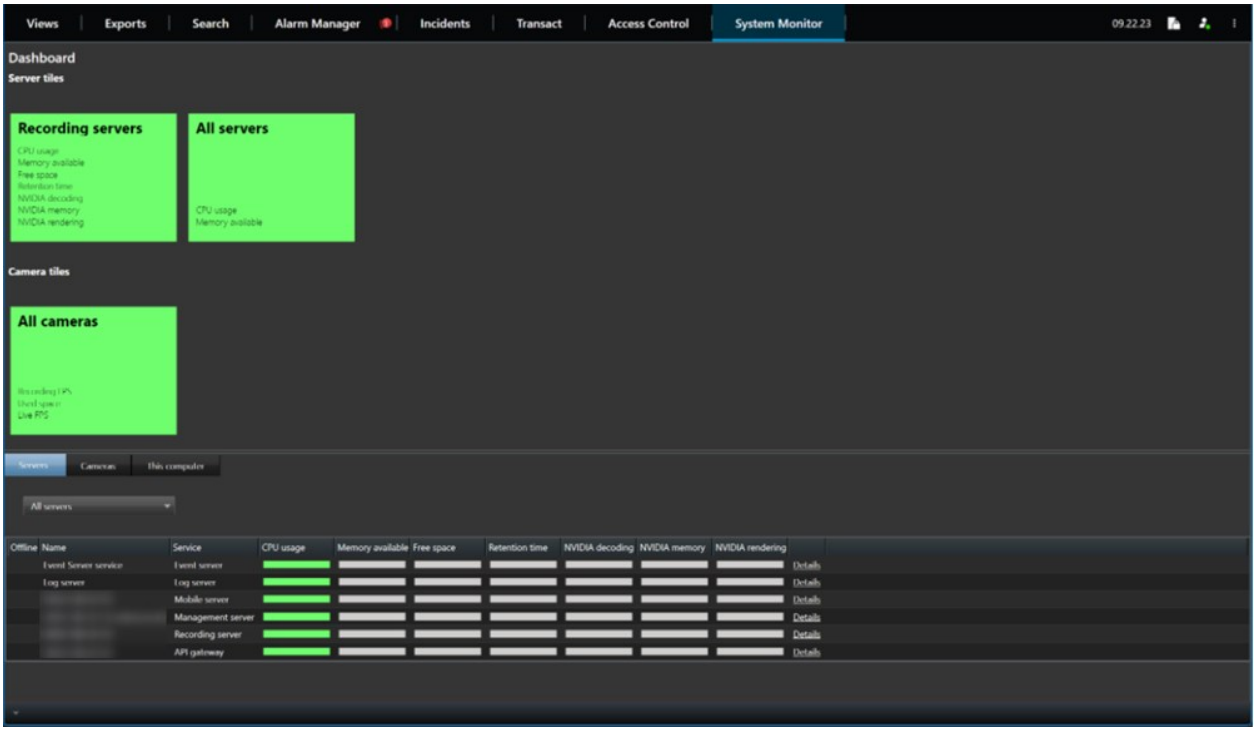
Für die System-Monitorfunktion ist es erforderlich, dass der Dienst Data Collector läuft und nur auf Computern funktioniert, die einen Gregorianischen (westlichen) Kalender verwenden.

### Systemmonitor-Dashboard (Erklärung)

Auf dem **System-Monitor-Dashboard** können Sie sich leicht einen Überblick über den Zustand Ihres VMS-Systems verschaffen. Der Zustand Ihrer Hardware wird durch Kacheln und deren Farben visuell dargestellt: Grün (läuft), Gelb (Warnung) und Rot (kritisch). Die Kacheln verfügen auch über Symbole, die Fehler oder Warnungen anzeigen, wenn sich ein oder mehrere Hardwaregeräte in einem fehlerhaften Zustand befinden.

Das System zeigt standardmäßig Kacheln, die alle **Aufzeichnungsserver**, **Alle Server** und **Alle Kameras** darstellen. Sie können die Überwachungsparameter für diese Standardkacheln nach Ihren Bedürfnissen anpassen und auch neue Kacheln erstellen. Zum Beispiel können Sie Kacheln einrichten, die einen einzelnen Server, eine einzelne Kamera oder eine Gruppe von Kameras oder Server widerspiegelt.

Überwachungsparameter sind beispielsweise die CPU-Auslastung oder verfügbarer Speicher eines Servers. Eine Kachel überwacht nur die Überwachungsparameter, die Sie zu der Kachel hinzugefügt haben. Weitere Informationen dazu finden Sie unter Fügen Sie auf dem Systemmonitor-Dashboard eine neue Kamera oder eines Server-Kachel hinzu auf Seite 319, Löschen einer Kamera- oder Server-Kachel auf dem Systemmonitor-Dashboard auf Seite 319 und Löschen Sie auf dem Systemmonitor-Dashboard eine Kamera- oder Server-Kachel auf Seite 319.




## Schwellenwerte des Systemmonitors (Erklärung)

Mit den Schwellenwerten für den Systemmonitor können Sie die Schwellenwerte festlegen und anpassen, wann Kacheln auf dem **System Monitor Dashboard** visuell anzeigen sollen, dass Ihre Systemhardware ihren Zustand ändert. Zdie CPU Auslastung eines Servers zum Beispiel von normal (grün) in den Verhandlungszustand (gelb) oder von einem Planungszustand (gelb) in einem kritischen Zustand (rot).

Das System verfügt über standardmäßig eingestellte Schwellenwerte für alle Hardwaregeräte desselben Typs, so dass Sie den Zustand Ihrer System Hardware von dem Moment ab überwachen können, wo Ihr System installiert wird und Sie Hardware hinzufügen. Sie können auch Schwellenwerte für einzelne Server, Kameras, Festplatten und Speichermedien einrichten. Informationen dazu, wie die Schwellenwerte geändert werden, finden Sie unter Schwellenwerte dafür bearbeiten, wann sich Hardwarezustände ändern sollen auf Seite 320.

Um sicherzustellen, dass Sie keinen **Kritischen** oder **Alarm**-Zustand sehen, falls die Nutzung oder Belastung Ihrer Systemhardware lediglich für einen Moment eine obere Schwelle erreicht, verwenden Sie das **Berechnungsintervall**. Bei korrekt eingestelltem Berechnungsintervall erhalten Sie keine falsch positiven Alarme wegen überschrittener Schwellenwerte, sondern nur solche wegen länger anhaltender Probleme z.B. mit der CPU-Auslastung oder Speichernutzung.

Sie können auch Regeln einrichten (siehe Regeln (Erklärung)), um bestimmte Maßnahmen zu ergreifen oder Alarme zu aktivieren, wenn sich ein Schwellenwert von einem Zustand zum anderen ändert.

## Lassen Sie sich den aktuellen Zustand Ihrer Hardware anzeigen und beheben Sie ggf. Fehler

Auf dem **System-Monitor-Dashboard** können Sie sich leicht einen Überblick über den Zustand Ihres VMS-Systems verschaffen. Der Zustand Ihrer Hardware wird durch Kacheln und deren Farben visuell dargestellt: Grün (läuft), Gelb (Warnung) und Rot (kritisch). Die Kacheln verfügen auch über Symbole, die Fehler oder Warnungen anzeigen, wenn sich ein oder mehrere Hardwaregeräte in einem fehlerhaften Zustand befinden.

Sie können die Schwellenwerte dafür bearbeiten, wann Ihre Hardware sich in einem der drei Zustände befindet. Weitere Informationen finden Sie unter Schwellenwerte dafür bearbeiten, wann sich Hardwarezustände ändern sollen auf Seite 320.

Das **System Monitor Dashboard** beantwortet solche Fragen wie: Laufen alle Serverdienste und Kameras? Reicht die CPU-Auslastung und der verfügbare Speicher auf den verschiedenen Servern, um alles aufzuzeichnen und zum Anschauen bereitzustellen?

1. Wählen Sie aus dem Bereich **Standortnavigation** das **System Dashboard** > **Systemmonitor** aus.
2. Wenn alle Kacheln grün sind und keine Warnungen oder Fehler anzeigen, sind alle Überwachungsparameter und alle Server und Kameras, die von den Kacheln dargestellt werden, in Ordnung und laufen.
   Zeigt eine oder mehrere der Kacheln eine Warnung oder einen Fehler an, oder ist sie ganz gelb oder rot, wählen Sie eine dieser Kacheln aus, um den Fehler zu beheben.
3. Auf der Liste der Hardware mit Überwachungsparametern (unten im Fenster) finden Sie die Hardware, die nicht läuft. Bewegen Sie Ihren Mauszeiger über das rote Kreuz neben der Hardware, um zu lesen, was das Problem ist.
4. Wählen Sie optional **Details** rechts neben der Hardware, um zu prüfen, wie lange das Problem schon besteht. Aktivieren Sie die Sammlung von Verlaufsdaten, um den Zustand Ihrer Hardware im Lauf der Zeit sehen zu können. Weitere Informationen finden Sie unter Verlaufsdaten zu Hardwarezuständen sammeln auf Seite 318.
5. Suchen Sie nach einer Möglichkeit, das Problem zu lösen. Z. B. durch Neustart des Computers oder des Serverdienstes, durch Austausch defekter Hardware oder sonstige Maßnahmen.

## Prüfen Sie den Zustand Ihrer Hardware im zeitlichen Verlauf und drucken Sie einen Bericht aus

Mit der Funktion **Systemmonitor** können Sie sich leicht einen Überblick über den Zustand Ihres VMS-Systems verschaffen. Auch über eine längere Zeitspanne.

Gibt es Zeiträume, in denen die CPU-Auslastung, die Bandbreite oder die Hardware problematisch sind? Die Antworten hierauf finden Sie mithilfe der System-Monitor-Funktion. So können Sie entscheiden ob Sie Ihre Hardware aufrüsten oder Hardware neue kaufen müssen, um dies in Zukunft zu vermeiden.

Denken Sie daran, die Sammlung von Verlaufsdaten zu aktivieren. Siehe Verlaufsdaten zu Hardwarezuständen sammeln auf Seite 318.

1. Wählen Sie aus dem Bereich **Standortnavigation** das **System Dashboard** > **Systemmonitor** aus.
2. Wählen Sie in dem Fenster **System Monitor** eine Kachel mit der Hardware aus, von der Sie wissen wollen, wie sich deren Zustand entwickelt hat, oder wählen Sie im unteren Teil des Fensters einen Server oder eine Kamera aus.
3. Wählen Sie rechts neben dem jeweiligen Server oder der jeweiligen Kamera **Details** aus.


4. Wählen Sie für Server **Verlauf** rechts neben der Hardware, die Sie untersuchen wollen. Wählen Sie für Kameras das Link aus.
5. Wenn Sie einen Bericht ausdrucken möchten, wählen Sie das Symbol PDF aus.

Sie können nur historische Berichte von Daten des Aufzeichnungsservers erstellen, bei dem sich das Gerät derzeit befindet.

Wenn Sie auf die Details des Systemmonitors von einem Server-Betriebssystem aus zugreifen, könnten Sie eine Meldung bezüglich **Internet Explorer erweiterte Sicherheitskonfiguration** bekommen. Folgen Sie den Anweisungen, um die Seite **System Monitor** zu den **Vertrauenswürdigen Seiten der Zone** hinzuzufügen, bevor Sie fortfahren.

## Verlaufsdaten zu Hardwarezuständen sammeln

Sie können die Sammlung von Verlaufsdaten der Hardware des Systems aktivieren, um Grafiken zum Zustand Ihrer Hardware im Lauf der Zeit sehen zu können und einen Bericht auszudrucken. Weitere Informationen finden Sie unter Prüfen Sie den Zustand Ihrer Hardware im zeitlichen Verlauf und drucken Sie einen Bericht aus auf Seite 317.

1. Wählen Sie aus dem Bereich **Standortnavigation** das **System Dashboard** > **Systemmonitor** aus.
2. Wählen Sie in dem Fenster **Systemmonitor Benutzerdefiniert** aus.
3. Wählen Sie in dem Fenster **Dashboard benutzerdefiniert anpassen**, das sich dann öffnet, die Option **Verlaufsdaten sammeln** aus.
4. Wählen Sie ein Intervall für die Probeentnahme aus. Je kürzer das Intervall, desto größer die Last für die SQL Server Datenbank, Bandbreite oder sonstige Hardware. Das Intervall für die Probeentnahme von Verlaufsdaten bestimmt auch, wie detailliert die Grafiken ausfallen.

## Fügen Sie auf dem Systemmonitor-Dashboard eine neue Kamera oder eines Server-Kachel hinzu

Wenn Sie Ihre Kameras oder Server nach deren physischen Standorten in kleineren Gruppen überwachen wollen, oder wenn Sie bestimmte Hardware mit verschiedenen Überwachungsparametern überwachen wollen, können Sie in dem Fenster **Systemmonitor** weitere Kacheln hinzufügen.

1. Wählen Sie aus dem Bereich **Standortnavigation** das **System Dashboard** > **Systemmonitor** aus.
2. Wählen Sie in dem Fenster **Systemmonitor Benutzerdefiniert** aus.
3. Werden Sie in dem Fenster **Dashboard anpassen**, das sich dann öffnet, unter **Server-Kacheln** oder **Kamera-Kacheln** die Option **Neu** aus.
4. Im Fenster **Neue Server-Kachel/Neue Kamerakachel**, wählen Sie die Kameras oder Server, die Sie überwachen möchten.
5. Aktivieren oder deaktivieren Sie unter **Überwachungsparameter** die Kontrollkästchen für beliebige Parameter, die Sie zu der Kachel hinzufügen oder daraus entfernen wollen.
6. Wählen Sie **OK**. Der neue Server- oder Kamerakachel wurde nun zu den angezeigten Kacheln in Ihrem Dashboard hinzugefügt.

## Löschen einer Kamera- oder Server-Kachel auf dem Systemmonitor-Dashboard

Wenn Sie Ihre Kameras oder Server mit anderen Überwachungsparametern überwachen wollen, können Sie diese einstellen.

1. Wählen Sie aus dem Bereich **Standortnavigation** das **System Dashboard** > **Systemmonitor** aus.
2. Wählen Sie in dem Fenster **Systemmonitor Benutzerdefiniert** aus.
3. Wählen Sie in dem Fenster **Dashboard anpassen**, das sich dann öffnet, unter **Server-Kacheln** oder **Kamera-Kacheln** die Option **Bearbeiten** aus.
4. Wählen Sie im Fenster **Dashboard bearbeiten Server-/Kamera-Kachel** alle Kameras oder Server, eine Kamera- oder Servergruppe oder einzelne Kameras oder Server aus, um deren Überwachungsparameter zu ändern.
5. Wählen Sie unter **Überwachungsparameter** die Überwachungsparameter aus, die Sie überwachen wollen.
6. Wählen Sie **OK**.

## Löschen Sie auf dem Systemmonitor-Dashboard eine Kamera- oder Server-Kachel

Wenn Sie die als Kacheln dargestellte Hardware nicht mehr zu überwachen brauchen, können Sie die Kachel löschen.

1. Wählen Sie aus dem Bereich **Standortnavigation** das **System Dashboard** > **Systemmonitor** aus.
2. Wählen Sie in dem Fenster **Systemmonitor Benutzerdefiniert** aus.
3. Wählen Sie in dem Fenster **Dashboard anpassen**, das sich dann öffnet, unter **Server-Kacheln** oder **Kamera-Kacheln** die Kachel aus, die Sie ändern wollen.
4. Wählen Sie **Löschen** aus.

## Schwellenwerte dafür bearbeiten, wann sich Hardwarezustände ändern sollen

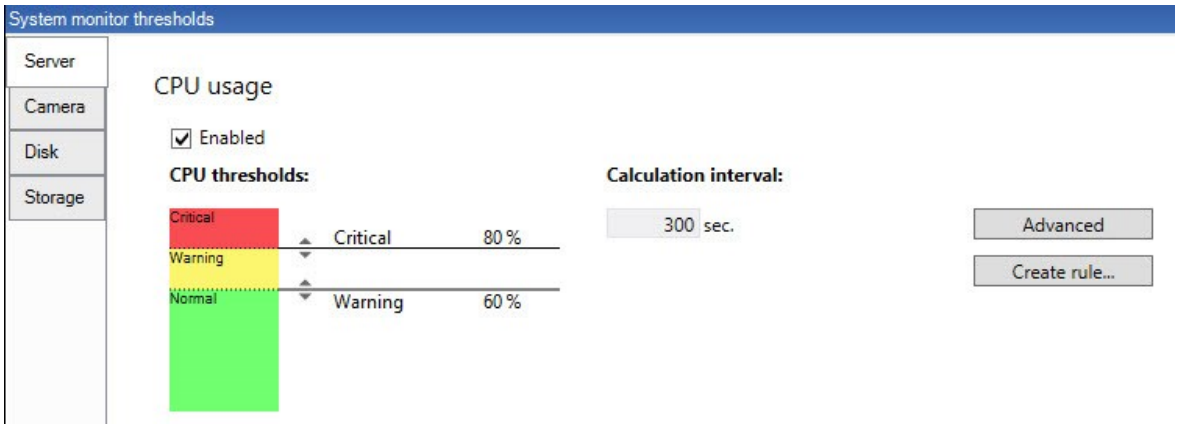
Auf dem **System Monitor Dashboard** können Sie die Schwellenwerte dafür bearbeiten, wann Ihre Hardware zwischen den drei Zuständen wechselt. Weitere Informationen finden Sie unter Schwellenwerte des Systemmonitors (Erklärung) auf Seite 316.

Sie können die Schwellenwerte für verschiedene Arten von Hardware ändern. Weitere Informationen finden Sie unter System-Monitor-Schwellenwerte (der Knoten "System Dashboard") auf Seite 614.

Das System ist standardmäßig so eingerichtet, dass es die Schwellenwerte für alle Einheiten desselben Hardwaretyps anzeigt, z.B. aller Kameras oder Server. Diese standardmäßig voreingestellten Werte können Sie ändern.

Sie können auch Schwellenwerte für einzelne Server oder Kameras einrichten, oder für eine Untergruppe davon, damit z.B. einige der Kameras eine mehr **Liveaufnahmen pro Sekunde** oder **Aufzeichnungen pro Sekunde** machen als andere Kameras.

1. Wählen Sie aus dem Bereich **Standortnavigation** das **System Dashboard** > **Systemmonitorschwellenwerte** aus.
2. Aktivieren Sie das Kontrollkästchen **Aktiviert** für die jeweilige Hardware, wenn Sie sie nicht bereits aktiviert haben. Die Abbildung unten zeigt ein Beispiel.




3. Ziehen Sie den Schieberegler für Schwellenwerte hoch oder runter, um den Schwellenwert zu erhöhen bzw. zu reduzieren. Für jedes Stück Hardware stehen zwei Schieberegler zur Verfügung, die in der Steuerung für die Schwellenwerte erscheinen und mit denen die Zustände **Normal**, **Warnung** und **Kritisch** getrennt werden.
4. Geben Sie einen Wert für das Berechnungsintervall an oder behalten Sie den Standardwert bei.

5. Wenn Sie die Werte für einzelne Hardwaregeräte einstellen wollen, wählen Sie **Erweitert**.
6. Wenn Sie Regeln für bestimmte Ereignisse oder innerhalb bestimmter Zeitspannen angeben wollen, wählen Sie **Regel erstellen**.
7. Sobald Sie die Schwellenwerte und Berechnungsintervalle eingestellt haben, wählen Sie im Menü **Datei** > **Speichern** aus.

## Beweissicherungen im System anzeigen

**Beweismittelsicherung** unter dem Knoten **System Dashboard** zeigt eine Übersicht über alle geschützten Daten im aktuellen Überwachungssystem.

Sie können eine Beweismittelsicherung finden, indem Sie z.B. danach filtern, wer sie erstellt hat oder wann sie erstellt wurde.

1. Wählen Sie aus dem Bereich **Standortnavigation** die Option **System Dashboard** > **Beweismittelsicherung** aus.
2. Hier finden Sie eine Übersicht und die jeweiligen Beweismittelsicherung. Sie können nach den verschiedenen Metadaten zu den Beweismittelsicherung filtern und sortieren.

Alle im Fenster **Beweismittelsicherung** gezeigten Informationen stellen Momentaufnahmen dar. Drücken Sie F5, um zu aktualisieren.

## Einen Bericht mit Ihrer Systemkonfiguration ausdrucken

Beim Installieren und Konfigurieren Ihres VMS-Systems treffen Sie zahlreiche Auswahlen, die Sie ggf. dokumentieren wollen. Im Lauf der Zeit ist es auch schwer, sich an alle Einstellungen zu erinnern, die Sie seit der Installation und Erstkonfiguration geändert haben - oder auch nur in den letzten zwei Monaten. Darum können Sie einen Bericht mit allen Ihren Konfigurationsseinstellungen ausdrucken.

Wenn Sie einen Konfigurationsbericht erstellen (PDF-Format), können Sie beliebige mögliche Elemente Ihres Uhren und Systems in den Bericht aufnehmen. Sie können beispielsweise Lizenzen, Gerätekonfigurationen, Alarmkonfigurationen und vieles mehr hinzufügen. Sie können die Option **Sensible Daten ausschließen** auswählen, um einen GDPR-konformen Bericht zu erstellen (standardmäßig aktiviert). Außerdem können Sie den Zeichensatz, die Seiteneinrichtung und das Deckblatt nach Ihren Bedürfnissen gestalten.

1. Erweitern Sie **System Dashboard** und wählen Sie **Konfigurationsberichte** aus.
2. Wählen Sie die Elemente aus, die sie in Ihren Bericht aufnehmen oder davon ausschließen wollen.
3. **Optional**: Wenn Sie ausgewählt haben, dass Sie ein Deckblatt mit einschließen wollen, wählen Sie **Deckblatt** aus, um die Informationen auf Ihrem Deckblatt anzupassen. In dem Fenster, das dann erscheint, können Sie die erforderlichen Angaben eingeben.
4. Wählen Sie **Formatierung**, um den Zeichensatz, die Seitengröße und die Ränder nach Ihren Bedürfnissen anzupassen. Wählen Sie im neuen Fenster die gewünschten Einstellungen.
5. Wenn Sie bereit für den Export sind, wählen Sie **Export** und wählen Sie einen Namen und einen Speicherort für Ihren Bericht aus.

Nur Benutzer mit Administratorberechtigung im VMS-System können Konfigurationsberichte erstellen.

# Metadaten

## Suchkategorien und Suchfilter für Metadaten anzeigen

Benutzer von XProtect Management Client mit Administratorrechten können die Milestone Standardkategorien für die Metadatensuche und die Suchfilter in XProtect Smart Client ein- und ausblenden. Diese Suchkategorien und Suchfilter werden standardmäßig verborgen. Sich diese anzeigen zu lassen ist hilfreich, wenn Ihr Videoüberwachungssystem die Anforderungen dafür erfüllt (siehe Suchanforderungen für Metadaten auf Seite 621).

Diese Einstellung betrifft alle XProtect Smart Client Benutzer.

Die Einstellung hat keine Auswirkungen auf die Sichtbarkeit von:

- Sonstige Milestone Suchkategorien und Suchfilter die keine Metadaten betreffen, z. B. **Bewegung**, **Lesezeichen**, **Alarme** und **Ereignisse**
- Suchkategorien und Suchfilter von Drittanbietern

1. In XProtect Management Client, im Bereich **Seitennavigation**, wählen Sie **Nutzung von Metadaten** > **Metadatensuche**.
2. Wählen Sie im Bereich **Metadatensuche** die Suchkategorie aus, für die Sie die Anzeigeeinstellungen ändern möchten.
3. Um die Sichtbarkeit einer Suchkategorie oder eines Suchfilters zu aktivieren, aktivieren Sie das entsprechende Kontrollkästchen. Um die Sichtbarkeit einer Suchkategorie oder eines Suchfilters zu deaktivieren, deaktivieren Sie das entsprechende Kontrollkästchen.

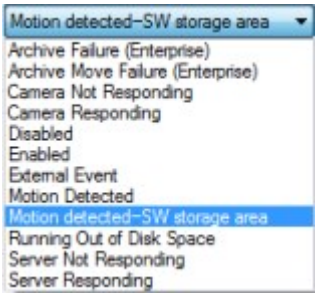
# Alarme

## Hinzufügen eines Alarms

Um einen Alarm zu definieren, müssen Sie eine Alarmdefinition erstellen, auf der Sie beispielsweise festlegen, was den Alarm auslöst, wie der Anwender reagieren soll und wodurch oder wann der Alarm angehalten wird. Detaillierte Informationen zu den Einstellungen finden Sie unter Alarmdefinitionen (Alarmknoten).

1. Im Bereich **Standort-Navigation** erweitern Sie **Alarme** und klicken mit der rechten Maustaste auf **Alarmdefinitionen**.
2. Wählen Sie **Neu hinzufügen** aus.

3. Tragen Sie diese Eigenschaften ein:
    - **Name**: Geben Sie einen Namen für die Alarmdefinition ein. Der Name der Alarmdefinition erscheint immer, wenn die Alarmdefinition aufgelistet wird.
    - **Anweisungen**: Hier können Sie Anweisungen für den Anwender eingeben, der den Alarm erhält.
    - **Auslösendes Ereignis**: Wählen Sie mit Hilfe der Dropdown-Menüs einen Ereignistyp und eine Ereignismeldung aus, die bei Auslösung des Alarms verwendet werden soll.

      *Eine Liste auswählbarer auslösender Ereignisse. Das hervorgehobene wird mithilfe von Analyseereignissen erstellt und angepasst.*
    - **Quellen**: Wählen Sie die Kameras oder anderen Geräte aus, von denen das alarmauslösende Ereignis stammen soll. Ihre Optionen hängen vom Ereignistyp ab, den Sie ausgewählt haben.
    - **Zeitprofil**: Wenn Sie möchten, dass der Alarm während eines bestimmten Zeitintervalls aktiviert wird, wählen Sie die Optionsschaltfläche und dann ein Zeitprofil im Dropdown-Menü aus.
    - **Ereignisgesteuert**: Wenn Sie möchten, dass die Alarmdefinition durch ein Ereignis ausgelöst wird, wählen Sie die Optionsschaltfläche aus und bestimmen Sie ein Ereignis, das die Alarmdefinition starten soll. Sie müssen auch ein Ereignis bestimmen, das die Alarmdefinition beenden soll.
4. Bestimmen Sie im Dropdown-Menü **Zeitgrenze** eine Zeitgrenze, an welcher eine Aktion des Anwenders erforderlich ist.
5. Bestimmen Sie im Dropdown-Menü **Ausgelöste Ereignisse**, welches Ereignis ausgelöst werden soll, wenn die Zeitgrenze überschritten wurde.
6. Legen Sie weitere Einstellungen fest, z. B. zugehörige Kameras und anfänglicher Eigentümer des Alarms.

## Anpassen der Berechtigungen für individuelle Alarmdefinitionen

Wenn Sie möchten, dass nur spezifische Benutzer Alarme ansehen und verwalten können, lassen sich die Berechtigungen für die Alarmdefinition von XProtect Management Client anpassen. Auf diese Weise können Sie Folgendes sicherstellen:

- Dass die Benutzer nur Alarme erhalten, die für sie relevant sind.
- Dass keine unberechtigten Benutzer auf Alarme reagieren können.

Verwenden Sie Rollen zum Gruppieren von Benutzern, welche dieselben Berechtigungen für alle Alarmdefinitionen haben sollten.

So ändern Sie die Berechtigungen für eine Alarmdefinition:

1. Im Bereich **Site-Navigation** erweitern Sie **Sicherheit** und wählen die Rolle aus, für die Sie die Berechtigungen bearbeiten möchten.
2. Rufen Sie die Registerkarte **Alarme** auf und erweitern Sie **Alarmdefinitionen**, um sich eine Liste der von Ihnen definierten Alarme anzusehen.
3. Wählen Sie eine Alarmdefinition aus, um die Berechtigungen zu modifizieren.

# Verschlüsselung aktivieren

## Die Verschlüsselung zum und vom Managementserver aktivieren

Sie können die wechselseitige Verbindung zwischen dem Managementserver und dem davon abhängigen Data Collector verschlüsseln, wenn Sie einen Remote Server des folgenden Typs haben:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

Wenn Ihr System mehrere Aufzeichnungsserver oder Remote-Server enthält, müssen Sie auf allen Servern eine Verschlüsselung aktivieren.

Wenn Sie die Verschlüsselung für eine Server-Gruppe konfigurieren, muss sie entweder mit Zertifikaten aktiviert werden, die zum selben CA-Zertifikat gehören, oder, wenn die Verschlüsselung deaktiviert ist, muss sie auf allen Computern in der Server-Gruppe deaktiviert werden.

**Voraussetzungen:**

- Einem Server-Authentifizierungszertifikat wird auf dem Computer vertraut, auf dem der Managementserver gehostet wird

Aktivieren Sie zunächst die Verschlüsselung auf dem Managementserver.

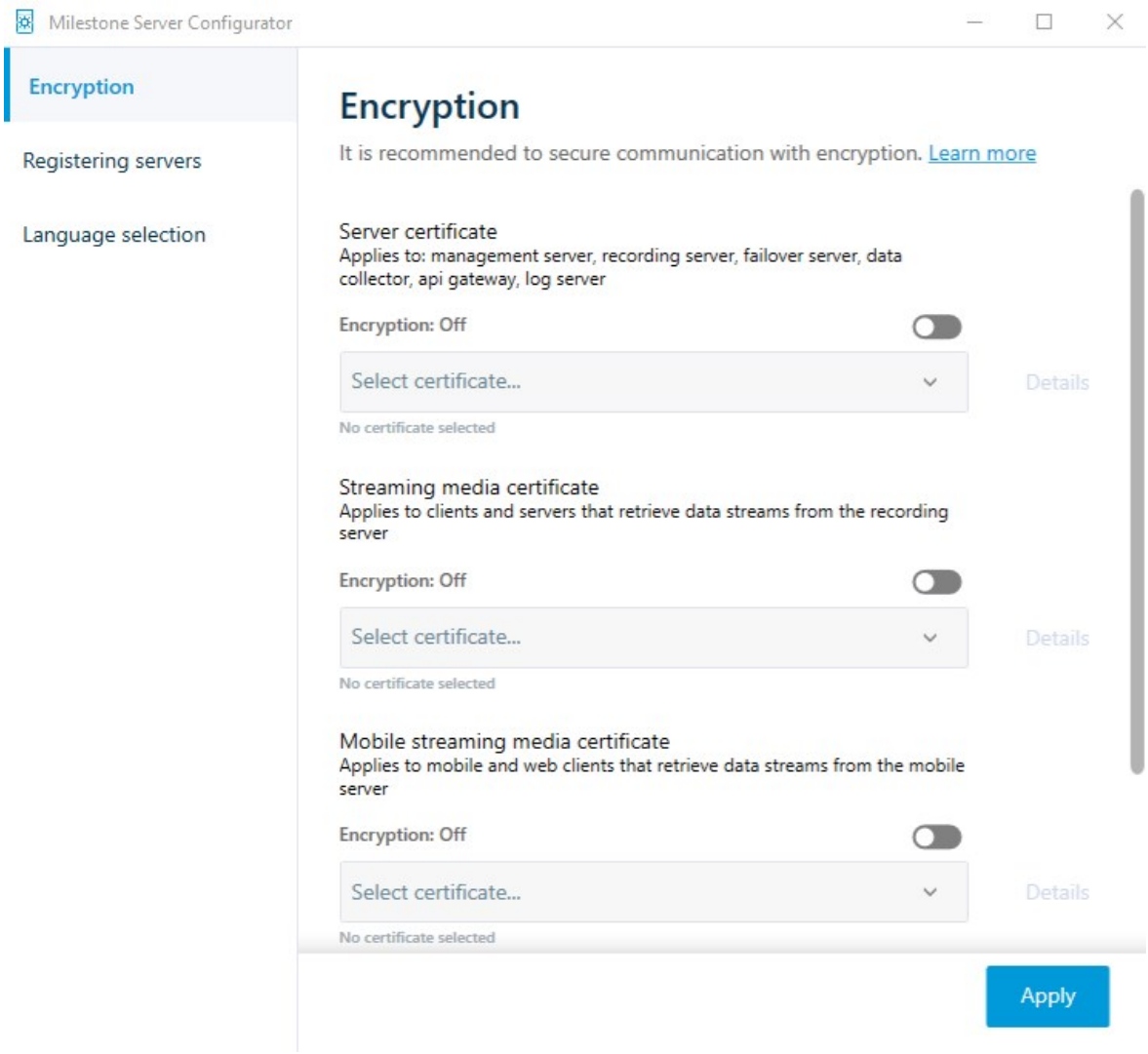
Schritte:

1. Öffnen Sie auf einem Computer mit installiertem Management Server die **Server Configurator** von:
   - Das Windows-Startmenü

   oder

   - Das Management Server Manager durch Klicken mit der rechten Maustaste auf das Symbol Management Server Manager auf der Taskleiste des Computers
2. Aktivieren Sie in der **Server Configurator**, unter **Serverzertificat** die **Verschlüsselung**.
3. Klicken Sie auf **Zertifikat auswählen**, um eine Liste der eindeutigen Themennamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und die auf dem lokalen Computer im Windows Certificate Store installiert sind.
4. Wählen Sie ein Zertifikat aus, das zur Verschlüsselung der Kommunikation zwischen dem Aufzeichnungsserver, dem Management-Server, dem Failover-Server und Data Collector server verwendet werden soll.

   Wählen Sie **Einzelheiten** aus, um die Angaben zum Windows Certificate Store zu dem ausgewählten Zertifikat anzuzeigen.




5. Klicken Sie auf **Anwenden**.

Um die Aktivierung der Verschlüsselung abzuschließen, ist der nächste Schritt die Aktualisierung der Verschlüsselungseinstellungen auf jedem Aufzeichnungsserver und auf jedem Server mit Data Collector (Event Server, Log Server, LPR Server und Mobile Server).

Weitere Informationen finden Sie unter Verschlüsselung für Aufzeichnungsserver oder Remote Server aktivieren auf Seite 326.

## Verschlüsselung für Aufzeichnungsserver oder Remote Server aktivieren

Sie können die wechselseitige Verbindung zwischen dem Managementserver und dem Aufzeichnungsserver oder sonstigen Remote Servern verschlüsseln, die Data Collector verwenden.

Wenn Ihr System mehrere Aufzeichnungsserver oder Remote-Server enthält, müssen Sie auf allen Servern eine Verschlüsselung aktivieren.

Weitere Informationen finden Sie im Zertifikate-Leitfaden dazu, wie Sie Ihre XProtect VMS Installationen sichern können.

> Wenn Sie die Verschlüsselung für eine Server-Gruppe konfigurieren, muss sie entweder mit Zertifikaten aktiviert werden, die zum selben CA-Zertifikat gehören, oder, wenn die Verschlüsselung deaktiviert ist, muss sie auf allen Computern in der Server-Gruppe deaktiviert werden.

**Voraussetzungen:**

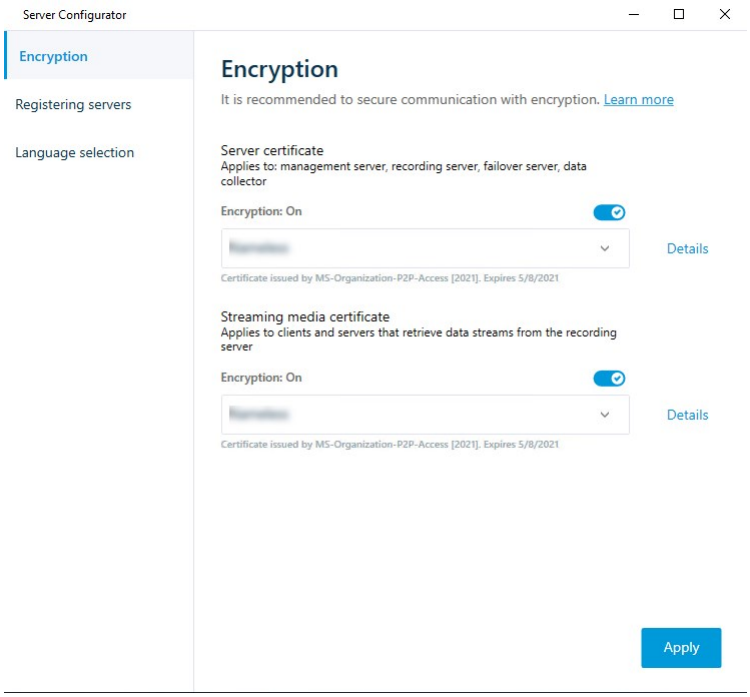
- Sie haben auf dem Management Server die Verschlüsselung aktiviert, siehe Die Verschlüsselung zum und vom Managementserver aktivieren auf Seite 324.

1. Öffnen Sie auf einem Computer mit installiertem Management Server oder Recording Server die **Server Configurator** vom:
   - Das Windows-Startmenü

   oder
   - Server Manager, durch Klicken mit der rechten Maustaste auf das Symbol Server Manager in der Taskleiste des Computers
2. Aktivieren Sie in der **Server Configurator**, unter **Serverzertificat** die **Verschlüsselung**.
3. Klicken Sie auf **Zertifikat auswählen**, um eine Liste der eindeutigen Themennamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und die auf dem lokalen Computer im Windows Certificate Store installiert sind.
4. Wählen Sie ein Zertifikat aus, das zur Verschlüsselung der Kommunikation zwischen dem Aufzeichnungsserver, dem Management Server, dem Failover-Server und dem Datensammlerserver verwendet werden soll.

   Wählen Sie **Einzelheiten** aus, um die Angaben zum Windows Certificate Store zu dem ausgewählten Zertifikat anzuzeigen.

   Der Benutzer des Dienstes Recording Server hat Zugriff zum privaten Schlüssel erhalten. Diesem Zertifikat muss auf allen Clients vertraut werden.




5. Klicken Sie auf **Anwenden**.

> Wenn Sie Zertifikate anwenden, wird der Aufzeichnungsserver angehalten und neu gestartet. Das Anhalten des Dienstes Recording Server bedeutet, dass Sie keine Live-Videoaufnahmen machen und anschauen können, während Sie die Basiskonfiguration des Aufzeichnungsservers überprüfen oder ändern.

## Aktivieren Sie die Verschlüsselung auf dem Ereignisserver

Sie können die zweiseitige Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, verschlüsseln, , einschließlich des LPR Server.

> Wenn Sie die Verschlüsselung für eine Server-Gruppe konfigurieren, muss sie entweder mit Zertifikaten aktiviert werden, die zum selben CA-Zertifikat gehören, oder, wenn die Verschlüsselung deaktiviert ist, muss sie auf allen Computern in der Server-Gruppe deaktiviert werden.

**Voraussetzungen:**

- Einem Server-Authentifizierungszertifikat wird auf dem Computer vertraut, auf dem der Ereignisserver gehostet wird

Aktivieren Sie zunächst die Verschlüsselung auf dem Ereignisserver.

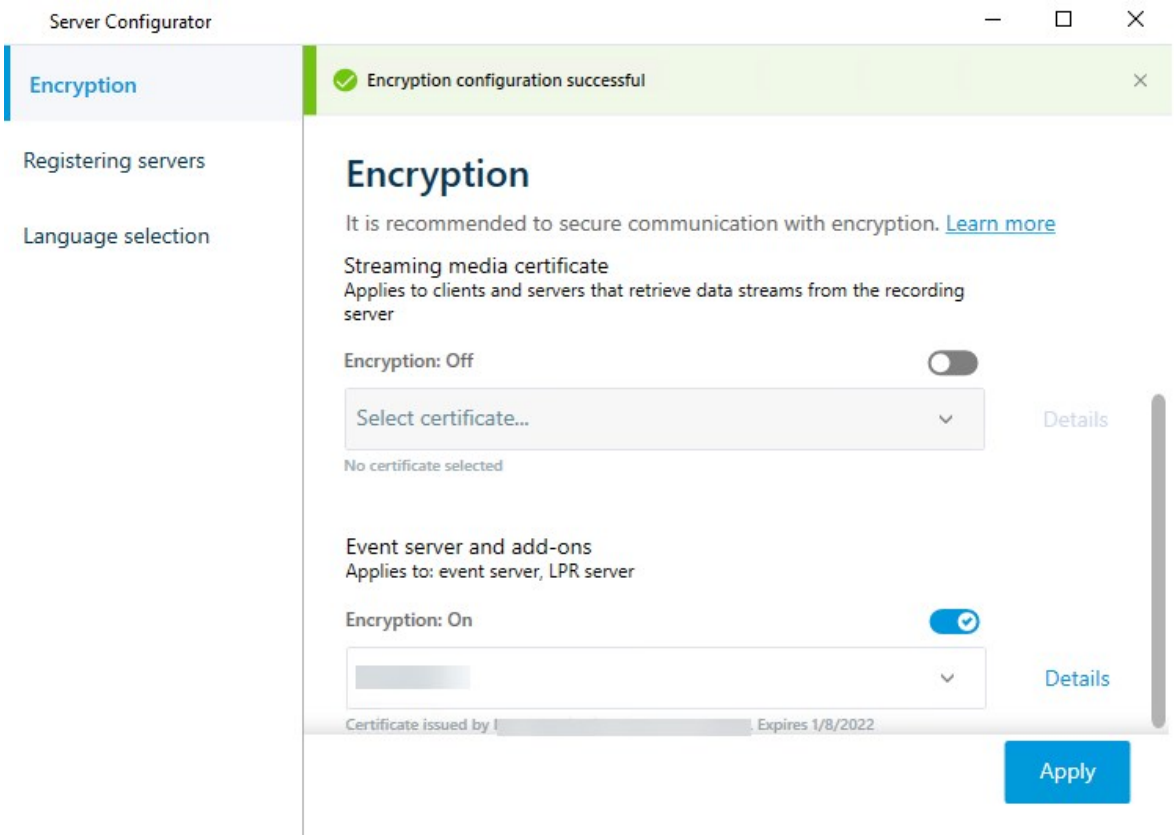
Schritte:

1. Öffnen Sie auf einem Computer mit installiertem Ereignisserver die **Server Configurator** von:
   - Das Windows-Startmenü

   oder

   - Das Event Server durch Klicken mit der rechten Maustaste auf das Symbol Event Server auf der Taskleiste des Computers
2. Aktivieren Sie im **Server Configurator**, unter **Ereignisserver und Add-ons** die Option **Verschlüsselung**.
3. Klicken Sie auf **Zertifikat auswählen**, um eine Liste der eindeutigen Themennamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und die auf dem lokalen Computer im Windows Certificate Store installiert sind.
4. Wählen Sie ein Zertifikat zur Verschlüsselung der Kommunikation zwischen dem Ereignisserver und den zugehörigen Add-ons.

   Wählen Sie **Einzelheiten** aus, um die Angaben zum Windows Certificate Store zu dem ausgewählten Zertifikat anzuzeigen.




5. Klicken Sie auf **Anwenden**.

Zum Abschluss der Aktivierung der Verschlüsselung müssen Sie als Nächstes die Verschlüsselungseinstellungen für jede zugehörige Erweiterung aktualisieren.LPR Server

## Verschlüsselung zu Clients und Servern aktivieren

Sie können Verbindungen vom Aufzeichnungsserver zu Clients und Servern verschlüsseln, die Daten vom Aufzeichnungsserver streamen.

> Wenn Sie die Verschlüsselung für eine Server-Gruppe konfigurieren, muss sie entweder mit Zertifikaten aktiviert werden, die zum selben CA-Zertifikat gehören, oder, wenn die Verschlüsselung deaktiviert ist, muss sie auf allen Computern in der Server-Gruppe deaktiviert werden.

**Voraussetzungen:**

- Dem zu verwendenden Serverauthenfizierungszertifikat wird von allen Computern vertraut, die Dienste ausführen, die Datenstreams vom Aufzeichnungsserver abrufen
- XProtect Smart Client und alle Dienste, die Datenströme vom Aufzeichnungsserver abrufen, müssen die Version 2019 R1 oder später haben
- Manche der Lösungen von Drittanbietern, die mit Hilfe von Versionen von MIP SDK erstellt wurden, die vor der Version 2019 R1 lagen, müssen ggf. aktualisiert werden

Schritte:

1. Öffnen Sie auf einem Computer mit installiertem Aufzeichnungsserver die **Server Configurator** von:
   - Das Windows-Startmenü

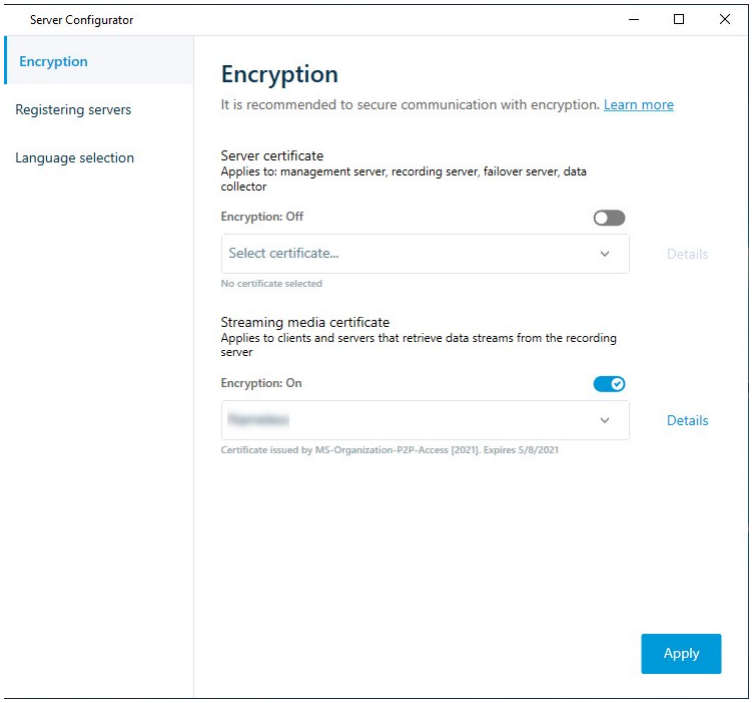
   oder

   - Das Recording Server Manager durch Klicken mit der rechten Maustaste auf das Symbol Recording Server Manager auf der Taskleiste des Computers
2. Aktivieren Sie in der **Server Configurator**, unter **Zertifikat für Streaming-Medien** die **Verschlüsselung**.
3. Klicken Sie auf **Zertifikat auswählen**, um eine Liste der eindeutigen Themennamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und die auf dem lokalen Computer im Windows Certificate Store installiert sind.
4. Wählen Sie ein Zertifikat aus, das für die Verschlüsselung der Kommunikation zwischen den Clients und Servern verwendet werden soll, die Datenstreams vom Aufzeichnungsserver abrufen.

   Wählen Sie **Einzelheiten** aus, um die Angaben zum Windows Certificate Store zu dem ausgewählten Zertifikat anzuzeigen.

   Der Benutzer des Dienstes Recording Server hat Zugriff zum privaten Schlüssel erhalten. Diesem

Zertifikat muss auf allen Clients vertraut werden.




5. Klicken Sie auf **Anwenden**.

> Wenn Sie Zertifikate anwenden, wird der Aufzeichnungsserver angehalten und neu gestartet. Das Anhalten des Dienstes Recording Server bedeutet, dass Sie keine Live-Videoaufnahmen machen und anschauen können, während Sie die Basiskonfiguration des Aufzeichnungsservers überprüfen oder ändern.

Um zu überprüfen, ob der Aufzeichnungsserver eine Verschlüsselung verwendet, s. Verschlüsselungsstatus anzeigen.

## Aktivieren Sie die Verschlüsselung auf dem mobilen Server.

Damit bei sicheren Verbindungen zwischen dem Mobile Server und Clients und Diensten ein HTTPS-Protokoll verwendet werden kann, müssen Sie auf dem Server ein gültiges Zertifikat anwenden. Das Zertifikat bestätigt, dass der Zertifikatsinhaber berechtigt ist, sichere Verbindungen herzustellen.

Weitere Informationen finden Sie im Zertifikate-Leitfaden dazu, wie Sie Ihre XProtect VMS Installationen sichern können.

Wenn Sie die Verschlüsselung für eine Server-Gruppe konfigurieren, muss sie entweder mit Zertifikaten aktiviert werden, die zum selben CA-Zertifikat gehören, oder, wenn die Verschlüsselung deaktiviert ist, muss sie auf allen Computern in der Server-Gruppe deaktiviert werden.

Von einer ZS (Zertifizierungsstelle) ausgestellte Zertifikate verfügen über eine Zertifikatkette, deren Root das Root-Zertifikat der Zertifizierungsstelle ist. Wenn einem Gerät oder Browser dieses Zertifikat präsentiert wird, vergleicht es das Stammzertifikat mit den im Betriebssystem (Android, iOS, Windows usw.) vorinstallierten Stammzertifikaten. Ist das Stammzertifikat in der Liste der vorinstallierten Zertifikate enthalten, garantiert das Betriebssystem gegenüber dem Benutzer, dass die Verbindung ausreichend sicher ist. Diese Zertifikate werden für einen Domänennamen ausgestellt und sind nicht kostenlos erhältlich.

Schritte:

1. Öffnen Sie auf einem Computer mit installiertem Management Server die **Server Configurator** von:
   - Das Windows-Startmenü

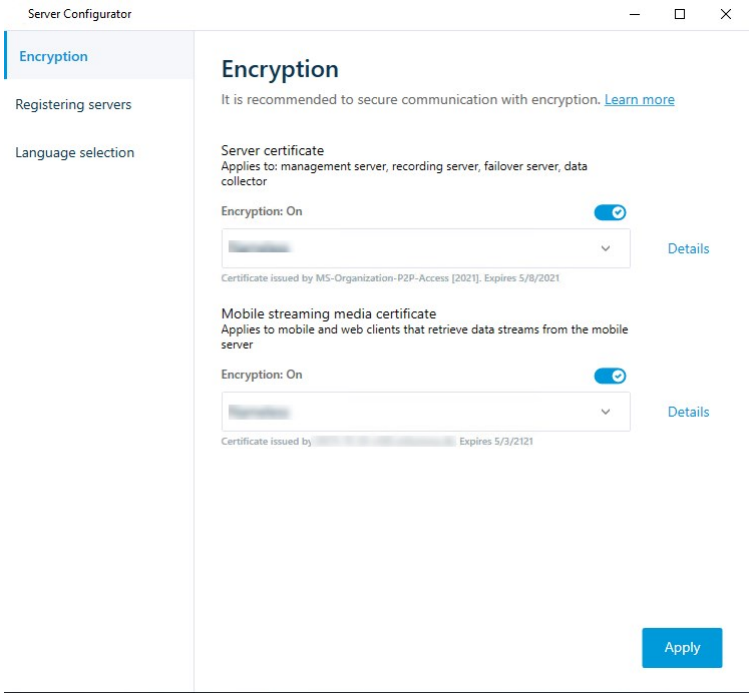
   oder

   - Das Mobile Server Manager durch Klicken mit der rechten Maustaste auf das Symbol Mobile Server Manager auf der Taskleiste des Computers
2. Aktivieren Sie in der **Server Configurator**, unter **Zertifikat für mobile Streaming-Medien** die **Verschlüsselung**.
3. Klicken Sie auf **Zertifikat auswählen**, um eine Liste der eindeutigen Themennamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und die auf dem lokalen Computer im Windows Certificate Store installiert sind.
4. Wählen Sie ein Zertifikat für die Verschlüsselung der Kommunikation zwischen XProtect Mobile Client und XProtect Web Client mit dem Mobile Server aus.

   Wählen Sie **Einzelheiten** aus, um die Angaben zum Windows Certificate Store zu dem ausgewählten Zertifikat anzuzeigen.

   Der Benutzer des Dienstes Mobile Server hat Zugriff zum privaten Schlüssel erhalten. Diesem Zertifikat

muss auf allen Clients vertraut werden.




5. Klicken Sie auf **Anwenden**.

Wenn Sie Zertifikate anwenden, wird der Mobile Server-Dienst neu gestartet.

# Milestone Federated Architecture

## Einrichten Ihres Systems für föderale Standorte

Um Ihr System auf die Milestone Federated Architecture vorzubereiten, müssen Sie bestimmte Entscheidungen beim Installieren des Management Servers treffen. Je nachdem wie Ihre IT-Infrastruktur aufgebaut ist, können Sie zwischen drei verschiedenen Möglichkeiten wählen.

**Möglichkeit 1: Verbinden von Standorten aus derselben Domäne (mit einem gemeinsamen Domänen-Benutzer)**

Vor der Installation des Managementservers müssen Sie einen Common Domain User erstellen und diesen auf allen Servern, die zur Hierarchie der Federated Site gehören, als Administrator konfigurieren. Wie Sie die Standorte miteinander verbinden, hängt von dem erstellten Benutzerkonto ab.

**Mit einem Windows-Benutzerkonto**

1. Beginnen Sie die Installation des Produkts auf dem Server, der als Management-Server dienen soll, und wählen Sie **Benutzerdefiniert**.
2. Wählen Sie die Installation des Management Server-Dienstes über ein Benutzerkonto. Das ausgewählte Benutzerkonto muss das Administratorkonto sein, das auf allen Management-Servern verwendet wird. Sie müssen dasselbe Benutzerkonto verwenden, wenn Sie die anderen Management-Server in der Hierarchie der föderalen Standorte installieren.
3. Beenden Sie die Installation. Wiederholen Sie die Schritte 1-3 zum Installieren aller weiteren Systeme, die Sie zur Hierarchie der föderalen Standorte hinzufügen wollen.
4. Hinzufügen eines Standorts zur Hierarchie (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 335).

**Mit einem eingebauten Windows-Benutzerkonto (Netzwerkdienst)**

1. Beginnen Sie die Installation des Produkts auf dem ersten Server, der als Management-Server dienen soll, und wählen Sie **Einzelcomputer** oder **Benutzerdefiniert** aus. Dadurch wird der Management-Server über ein Netzwerkdienstkonto installiert. Wiederholen Sie diesen Schritt für alle Standorte in Ihrer Hierarchie der föderalen Standorte.
2. Melden Sie sich bei dem Standort an, der in der Hierarchie der föderalen Standorte als zentraler Standort dienen soll.
3. Im Management Client erweitern Sie **Sicherheit** > **Rollen** > **Administratoren**.
4. Auf der Registerkarte **Benutzer und Gruppen**: auf **Hinzufügen** klicken und **Windows-Benutzer** auswählen.
5. Im Dialogfeld **Computer** als Objekttyp auswählen, den Servernamen des föderalen Standorts eingeben und auf **OK** klicken, um den Server zur **Administrator**-Rolle des zentralen Standorts hinzuzufügen. Wiederholen Sie diesen Schritt, bis Sie alle föderalen Standorte auf diese Weise hinzugefügt haben, und schließen Sie die Anwendung.
6. Melden Sie sich bei jedem föderalen Standort an und fügen Sie die folgenden Server auf die oben beschriebene Weise zur **Administrator**-Rolle hinzu:
   - Der Server des übergeordneten Standorts.
   - Die Server der untergeordneten Standorte, die Sie direkt mit diesem föderalen Standort verbinden möchten.
7. Hinzufügen eines Standorts zur Hierarchie (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 335).

**Möglichkeit 2: Verbinden von Standorten aus unterschiedlichen Domänen**

Stellen Sie zum Verbinden von Standorten unterschiedlicher Domänen sicher, dass eine Vertrauensstellung zwischen den Domänen besteht. Sie können eine Vertrauensstellung zwischen unterschiedlichen Domänen in der Domänenkonfiguration von Microsoft Windows einrichten. Sobald Sie eine Vertrauensstellung zwischen

den unterschiedlichen Domänen an jedem Standort in der Hierarchie der föderalen Standorte geschaffen haben, folgen Sie einfach der Beschreibung bei Möglichkeit 1. Weitere Informationen über die Einrichtung einer Vertrauensstellung zwischen Domänen finden Sie auf der Microsoft Website (https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/).

Milestone empfiehlt Milestone Interconnect für die Erstellung von vernetzten Systemen mit mehreren Standorten und Domänen.

**Möglichkeit 3 Verbinden von Standorten in Arbeitsgruppen**

Wenn Sie Standorte innerhalb von Arbeitsgruppen verbinden wollen, muss dasselbe Administratorkonto auf allen Servern vorhanden sein, die Sie in der Hierarchie der föderalen Standorte verbinden wollen. Sie müssen vor der Installation des Systems das Administratorkonto festlegen.

1. Melden Sie sich mit einem allgemeinen Administratorkonto bei **Windows** an.
2. Beginnen Sie die Installation des Produkts und klicken Sie auf **Benutzerdefiniert**.
3. Installieren Sie den Management Server-Dienst unter Verwendung des allgemeinen Administratorkontos.
4. Beenden Sie die Installation. Wiederholen Sie die Schritte 1-4, um weitere, zu verbindende Systeme zu installieren. Sie müssen all diese Systeme mit dem allgemeinen Administratorkonto installieren.
5. Hinzufügen eines Standorts zur Hierarchie (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 335).

Milestone empfiehlt Milestone Interconnect zur Erstellung von vernetzten Systemen mit mehreren Standorten, wenn die Standorte nicht zu einer Domäne gehören.

Sie können Domänen und Arbeitsgruppen nicht mischen. Das bedeutet, dass Sie nicht Standorte von einer Domäne mit Standorten von einer Arbeitsgruppe verbinden können und umgekehrt.

## Hinzufügen eines Standorts zur Hierarchie

Bei der Erweiterung Ihres Systems können Sie Standorte zu Ihrem obersten Standort und zu dessen untergeordneten Standorten hinzufügen, solange das System korrekt konfiguriert ist.

Stellen Sie beim Hinzufügen eines unsicheren Systems zu Milestone Federated Architecture sicher, dass **Nicht sichere Verbindungen zum Server zulassen** unter **Tools** > **Optionen** > **Allgemeine Einstellungen** in Management Client aktiviert ist.

1. Wählen Sie den Bereich **Hierarchie der föderalen Standorte** aus.
2. Wählen Sie den Standort aus, dem Sie einen untergeordneten Standort hinzufügen möchten, klicken Sie mit der rechten Maustaste, und klicken Sie dann auf **Standort der Hierarchie hinzufügen**.
3. Geben Sie die URL des angeforderten Standorts in das Fenster **Standort der Hierarchie hinzufügen** ein und klicken Sie auf **OK**.
4. Der übergeordnete Standort sendet eine Verknüpfungsanfrage an den untergeordneten Standort und nach einer Weile wird dem Bereich **Hierarchie der föderalen Standorte** eine Verknüpfung zwischen den beiden Standorten hinzugefügt.
5. Können Sie die Verknüpfung zum untergeordneten Standort ohne Genehmigungsanfrage an den Administrator des untergeordneten Standorts einrichten, gehen Sie zu Schritt 7.

   Ist dies **nicht** der Fall, wird für den untergeordneten Standort das Symbol für eine ausstehende Genehmigung angezeigt, bis der Administrator des untergeordneten Standortes die Anfrage genehmigt hat.
6. Vergewissern Sie sich, dass der Administrator der Kind-Seite die Verknüpfungsanfrage von der Elternseite genehmigt (siehe Zustimmen der Aufnahme in die Hierarchie auf Seite 336).
7. Die neue Verknüpfung zwischen übergeordnetem und untergeordnetem Standort wird eingerichtet und der Bereich **Hierarchie der föderalen Standorte** wird mit dem Symbol für den neuen untergeordneten Standort aktualisiert.

## Zustimmen der Aufnahme in die Hierarchie

Wenn ein untergeordneter Standort eine Link-Anfrage von einem potenziell übergeordneten Standort erhalten hat, dessen Administrator keine Administratorrechte für den untergeordneten Standort besitzt, wird er mit dem Symbol "Warte auf Annahme" gekennzeichnet.

Gehen Sie zum Akzeptieren einer Verknüpfungsanfrage wie folgt vor:

1. Melden Sie sich am Standort an.
2. Klicken Sie im Bereich **Verbundstandorthierarchie** mit der rechten Maustaste auf den Standort und dann auf **Einbindung in die Hierarchie annehmen**.

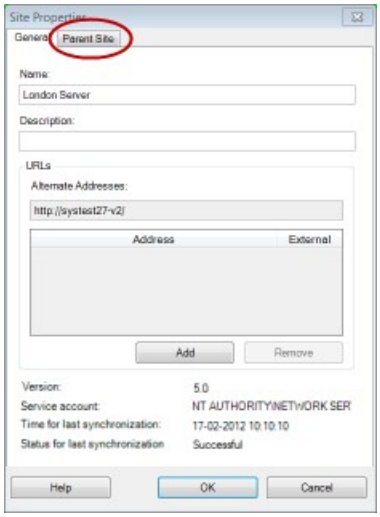
   Führt der Standort die XProtect Expert-Version aus, klicken Sie mit der rechten Maustaste auf das **Site-Navigationsfenster**.
3. Klicken Sie auf **Ja**.
4. Die neue Verknüpfung zwischen übergeordnetem und untergeordnetem Standort wird eingerichtet und der Bereich **Hierarchie der föderalen Standorte** wird mit dem normalen Standortsymbol für den ausgewählten Standort aktualisiert.

Es kann einige Zeit dauern, bis Änderungen für untergeordnete Standorte, die vom übergeordneten Standort weit entfernt sind, im Bereich **Hierarchie der föderalen Standorte** angezeigt werden.

## Festlegen von Standorteigenschaften

Sie können Eigenschaften auf Ihrem Heimatstandort und dessen untergeordneten Standorten anzeigen und möglicherweise auch bearbeiten.

1. Wählen Sie im Management Client im Bereich **Hierarchie der föderalen Standorte** den entsprechenden Standort aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Eigenschaften** aus.




2. Ändern Sie ggf. Folgendes:

   Die Registerkarte **Allgemein** (siehe Allgemein auf Seite 640)

   Die Registerkarte **Eltern-Standort** (siehe Registerkarte „Übergeordneter Standort“ auf Seite 640) **(steht nur an Kind-Standorten zur Verfügung)**

   Aufgrund von Synchronisierungsproblemen kann es einige Zeit dauern, bis Änderungen an entfernten untergeordneten Standorten im Bereich **Standort-Navigation** angezeigt werden.

## Standorthierarchie aktualisieren

Das System synchronisiert die Hierarchie regelmäßig automatisch in allen Ebenen Ihrer Einrichtung mit übergeordneten und untergeordneten Standorten. Sie können auch manuell eine Aktualisierung durchführen, wenn die Änderungen sofort in der Hierarchie angezeigt werden sollen und Sie nicht bis zur nächsten automatischen Synchronisierung warten möchten.

Sie müssen für eine manuelle Aktualisierung an einem Standort angemeldet sein. Durch eine Aktualisierung werden nur für diesen Standort seit der letzten Synchronisierung gespeicherte Änderungen angezeigt. Es kann also sein, dass Änderungen weiter unten in der Hierarchie durch diese manuelle Aktualisierung nicht angezeigt werden, wenn die Änderungen den Standort noch nicht erreicht haben.

1. Melden Sie sich am entsprechenden Standort an.
2. Klicken Sie im Bereich **Hierarchie der föderalen Standorte** mit der rechten Maustaste auf den obersten Standort und klicken Sie auf **Standorthierarchie aktualisieren**.

   Das dauert ein paar Sekunden.

## Anmelden an anderen Standorten in der Hierarchie

Sie können sich an anderen Standorten anmelden und diese verwalten. Der Standort, an dem Sie angemeldet sind, ist Ihr Heimatstandort.

1. Klicken Sie im Bereich **Hierarchie der föderalen Standorte** mit der rechten Maustaste auf den Standort, an dem Sie sich anmelden möchten.
2. Klicken Sie auf **An Standort anmelden**.

   Das Management Client für diesen Standort wird geöffnet.
3. Geben Sie die Anmeldeinformationen ein und klicken Sie auf **OK**.
4. Nach der Anmeldung können Sie sich um Ihre Verwaltungsaufgaben für diesen Standort kümmern.

## Aktualisieren der Standortinformationen von Kindstandorten

Dieser Abschnitt ist nur relevant, wenn Sie XProtect Corporate oder XProtect Expert 2014 oder neuer verwenden.

In einer großen Milestone Federated Architecture Einrichtung mit vielen Kind-Standorten verliert man leicht den Überblick, und die Kontaktinformationen der Administratoren aller Kind-Standorte können schwer zu finden sein.

Deshalb können Sie zusätzliche Informationen zu jedem Kind-Standort hinzufügen, und diese Informationen stehen dann den Administratoren am zentralen Standort zur Verfügung.

Die Informationen zum Standort können Sie lesen, wenn Sie Ihren Mauszeiger über den Namen des Standortes im Bereich **Föderale Standorthierarchie** bewegen. Zum Aktualisieren der Informationen zum Standort:

1. Melden Sie sich am Standort an.
2. Klicken Sie auf den Bereich **Standortnavigation** und wählen Sie **Standortinformationen**.
3. Klicken Sie auf **Bearbeiten** und fügen Sie in jeder Kategorie die entsprechenden Informationen hinzu.

### Trennen eines Standorts von der Hierarchie

Wenn Sie einen Standort von seinem übergeordneten Standort trennen, wird die Verknüpfung zwischen den Standorten unterbrochen. Sie können Standorte vom zentralen Standort, vom Standort selbst oder vom übergeordneten Standort trennen.

1. Klicken Sie im Bereich **Hierarchie der föderalen Standorte** mit der rechten Maustaste auf den Standort und klicken Sie auf **Standort von Hierarchie trennen**.
2. Klicken Sie auf **Ja**, um den Bereich **Hierarchie der föderalen Standorte** zu aktualisieren.

   Verfügt der getrennte Standort über untergeordnete Standorte, wird er zum neuen obersten Standort dieses Zweigs der Hierarchie und das normale Standortsymbol  ändert sich zu einem Symbol für den obersten Standort  .
3. Klicken Sie auf **OK**.

Die Änderungen an der Hierarchie werden nach einer manuellen Aktualisierung oder einer automatischen Synchronisierung angezeigt.

## Milestone Interconnect

### Einen Remote-Standort zum zentralen Milestone Interconnect-Standort hinzufügen

Sie können Remote-Systeme zum zentralen Standort hinzufügen, mittels des Assistenten für **Hardware hinzufügen**.

**Voraussetzungen**

- Genügend Milestone Interconnect Kameralizenzen (siehe Milestone Interconnect und Lizenzierung auf Seite 97).
- Ein weiteres konfiguriertes und funktionierendes XProtect System mit einem Benutzerkonto (Basisbenutzer, lokaler Windows-Benutzer oder Windows Active Directory-Benutzer) mit Berechtigungen für die Geräte, auf die das zentrale XProtect Corporate-System zugreifen können soll
- Die Netzwerkverbindung zwischen dem zentralen XProtect Corporate-Standort und den Remote-Systemenen mit Zugriff oder Port-Forwarding zu den verwendeten Ports der Remote-Systemen.

Zum Hinzufügen eines Remote-Systems:

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Erweitern Sie im Bereich **Übersicht** den jeweiligen Aufzeichnungsserver und klicken Sie mit der rechten Maustaste.
3. Wählen Sie **Hardware hinzufügen** aus, um den Assistenten zu starten.
4. Wählen Sie auf der ersten Seite **Adressbereichssuche** oder **Manuell** und klicken Sie dann auf **Weiter**.

5. Benutzernamen und Passwörter festlegen. Das Benutzerkonto muss auf dem Remote-Systeminstallation voreingestellt werden. Sie können Benutzernamen und Passwörter nach Bedarf hinzufügen, indem Sie auf **Hinzufügen** klicken. Wenn Sie bereit sind, klicken Sie auf **Weiter**.
6. Wählen Sie die zu verwendenden Treiber für einen Scan. In diesem Fall, wählen Sie die Milestone-Treiber aus. Klicken Sie auf **Weiter**.
7. Bestimmen Sie die IP-Adressen und Portnummern, die Sie scannen möchten. Die Standardeinstellung ist Port 80. Klicken Sie auf **Weiter**.

   Warten Sie, bis Ihr System die Remote-Standorte erkannt hat. Eine Statusanzeige zeigt den Erkennungsfortschritt. Im Falle einer erfolgreichen Erkennung erscheint eine **Erfolgsmeldung** in der **Status**-Spalte. Sollte ein Hinzufügen fehlschlagen, können Sie über die **Fehlgeschlagen**-Meldung den Grund erfahren.
8. Aktivieren oder deaktivieren Sie erfolgreich erkannte Systeme. Klicken Sie auf **Weiter**.
9. Warten Sie, während Ihr System die Hardware erkennt und gerätespezifische Informationen sammelt. Klicken Sie auf **Weiter**.
10. Aktivieren oder Deaktivieren Sie erfolgreich erkannte Hardware und Geräte. Klicken Sie auf **Weiter**.
11. Wählen Sie eine Standard-Gruppe. Klicken Sie auf **Fertigstellen**.
12. Nach der Installation können Sie das System und dessen Geräte im Bereich **Übersicht** sehen.

    Je nach den Benutzerrechten des ausgewählten Benutzers am entfernten Standort erhält der zentrale Standort Zugriff auf alle Kameras und Funktionen oder auf einen Teil davon.

## Benutzerrechte zuweisen

Sie konfigurieren die Benutzerberechtigungen für eine vernetzte Kamera so, wie Sie es auch für andere Kameras tun, nämlich indem Sie eine Rolle erstellen und den Zugriff auf Funktionen zuweisen.

1. Erweitern Sie auf der zentralen Seite, in dem Fenster **Standort-Navigation** das Feld **Sicherheit** und wählen Sie **Rollen** aus.
2. Klicken Sie in dem Übersichtsfenster mit der rechten Maustaste auf die eingebaute Administratorrolle und wählen Sie **Rolle hinzufügen** aus (siehe Rolle hinzufügen und verwalten).
3. Benennen Sie die Rolle und konfigurieren Sie die Einstellungen auf der Registerkarte **Gerät** (siehe die Registerkarte Gerät (Rollen)) und die Registerkarte **Fernaufzeichnungen** (siehe die Registerkarte Fernaufzeichnungen (Rollen)).

## Hardware des Remote-Systems aktualisieren

Wenn die Konfiguration am Remote-System beispielsweise durch das Hinzufügen und Entfernen von Kameras und Ereignissen verändert wurde, müssen Sie die Konfiguration am zentralen Standort aktualisieren, damit die neue am Remote-System wiedergespiegelt wird.

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Erweitern Sie im Bereich **Übersicht** den benötigten Aufzeichnungsserver und wählen das jeweilige Remote-System aus. Machen Sie einen Rechtsklick darauf.
3. Wählen Sie **Hardware aktualisieren**. Dies öffnet das Dialogfenster **Hardware aktualisieren**.
4. Das Dialogfenster zeigt alle Änderungen (Geräte, die entfernt, aktualisiert oder hinzugefügt wurden) im Remote-Systeminstallation, ab dem Zeitpunkt der Einrichtung oder letzten Aktualisierung Ihrer Milestone Interconnect-Einstellung. Klicken Sie auf **Bestätigen**, um Ihren zentralen Standort mit diesen Änderungen zu aktualisieren.

## Aktivieren der direkten Wiedergabe von der Kamera am Remote-System

Wenn Ihr zentraler Standort permanent mit den Remote-Systemen verbunden ist, können Sie Ihr System so konfigurieren, dass die Benutzer die Aufzeichnungen direkt von den Remote-Systemen abspielen können. Weitere Informationen finden Sie unter Milestone Interconnect-Einrichtungen (Erklärung) auf Seite 97.

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Erweitern Sie im Bereich **Übersicht** den benötigten Aufzeichnungsserver und wählen das jeweilige Remote-System aus. Wählen Sie die relevante verbundene Kamera.
3. Wählen Sie im Eigenschaften Bereich, die Registerkarte **Aufzeichnen**, und wählen Sie dann die Option **Wiedergabe der Aufzeichnungen von Remote-Systeminstallation**.
4. Klicken Sie in der Symbolleiste auf **Speichern**.

In einer Milestone Interconnect-Einstellung ignoriert ein zentraler Standort die Privatzonenmasken in einem Remote-System. Wenn Sie die gleichen Privatzonenmasken anwenden möchten, müssen Sie diese am zentralen Standort neu festlegen.

## Abruf von Fernaufzeichnungen von Kamera an Remote-System

Sollte Ihr zentraler Standort **nicht** permanent mit den Remote-Systemen verbunden sein, können Sie Ihr System so konfigurieren, dass es Fernaufzeichnungen zentral speichert und den Abruf von Fernaufzeichnungen durchführt, wenn die Netzwerkverbindung optimal dafür ist. Weitere Informationen finden Sie unter Milestone Interconnect-Einrichtungen (Erklärung) auf Seite 97.

Damit die Benutzer Aufzeichnungen auch tatsächlich abrufen können, müssen Sie diese Erlaubnis für die jeweiligen Rollen aktivieren (siehe Rollen (Sicherheit)).

Zur Konfigurierung Ihres Systems:

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Erweitern Sie im Bereich **Übersicht** den benötigten Aufzeichnungsserver und wählen das jeweilige Remote-System aus. Wählen Sie den relevanten Remote-Server aus.
3. Wählen Sie im Bereich Eigenschaften die Registerkarte **Fernabruf** aus und aktualisieren Sie die Einstellungen (siehe Registerkarte „Fernabfrage“ auf Seite 465).

Wenn aus irgendeinem Grund das Netzwerk ausfällt, verliert der zentrale Standort Aufzeichnungssequenzen. Sie können daher Ihr System darauf konfigurieren, dass der zentrale Standort automatisch Fernaufzeichnungen abruft, um solche Zeiträume zu überbrücken, sobald das Netzwerk wiederhergestellt wurde.

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Erweitern Sie im Bereich **Übersicht** den benötigten Aufzeichnungsserver und wählen das jeweilige Remote-System aus. Wählen Sie die gewünschte Kamera.
3. Wählen Sie im Bereich Eigenschaften die Registerkarte **Aufzeichnung** und wählen Sie dann die Option **Fernaufzeichnungen automatisch abrufen wenn die Verbindung wiederhergestellt wird** (siehe Fernaufzeichnen abspeichern und abrufen).
4. Klicken Sie in der Symbolleiste auf **Speichern**.

Als Alternative können Sie Regeln verwenden oder bei Bedarf den Abruf von Fernaufzeichnungen von XProtect Smart Client starten.

In einer Milestone Interconnect-Einstellung ignoriert ein zentraler Standort die Privatzonenmasken in einem Remote-System. Wenn Sie die gleichen Privatzonenmasken anwenden möchten, müssen Sie diese am zentralen Standort neu festlegen.

## Konfigurieren Sie Ihren zentralen Standort, so dass er auf Ereignisse von Remote-Systemen reagiert

Sie können Ereignisse am Remote-System so einstellen, dass Regeln und Alarme am zentralen Standort ausgelöst werden und dadurch sofortige Reaktion auf Ereignisse am Remote-System folgen kann. Dies erfordert, dass die Remote-Systeme verbunden und online sind. Die Anzahl und Typ der Ereignisse ist abhängig von den Konfigurationen und Voreinstellungen an den Remote-Systemen.

Die Liste der unterstützten Ereignisse finden Sie auf der Milestone Website (https://www.milestonesys.com/).

Sie können voreingestellte Ereignisse nicht löschen.

**Anforderungen**:

- Wenn Sie benutzerdefinierte/manuelle Ereignisse vom Remote-System als auslösende Ereignisse verwenden möchten, müssen Sie diese zuerst am Remote-System erstellen
- Vergewissern Sie sich, dass Sie über eine aktuelle Liste der Ereignisse von den entfernten Standorten verfügen (siehe Hardware des Remote-Systems aktualisieren auf Seite 340).

**Hinzufügen eines benutzerdefinierten/manuellen Ereignisses von einem Remote-System:**

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Unter Übersicht wählen Sie den passenden Remote-Server und dann die Registerkarte **Ereignisse**.
3. Diese Liste enthält voreingestellte Ereignisse. Klicken Sie auf **Hinzufügen**, um benutzerdefinierte oder manuelle Ereignisse vom Remote-System aus der Liste einzuschließen.

**Verwenden eines Ereignisses an einem Remote-System, um einen Alarm am zentralen Standort auszulösen:**

1. Am zentralen Standort, erweitern Sie **Alarme** und wählen dann **Alarmdefinitionen** aus.
2. Im Bereich Übersicht, klicken Sie mit der rechten Maustaste auf **Alarmdefinitionen** und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie Werte nach Bedarf ein.
4. Im Feld **Ereignis auslösen**, können Sie zwischen den unterstützten voreingestellten und benutzerdefinierten Ereignissen auswählen.
5. Im Feld **Quellen**, können Sie den Remote-Server auswählen, von dessen assoziierten Remote-Server Sie Alarme erhalten möchten.
6. Speichern Sie die Konfiguration, wenn Sie fertig sind.

**Verwenden eines Ereignisses an einem Remote-System zum Auslösen einer regelbasierten Aktion am zentralen Standort:**

1. Erweitern Sie am zentralen Standort **Regeln und Ereignisse** und wählen dann **Regeln**.
2. Im Übersichtsbereich, klicken Sie mit der rechten Maustaste auf **Regeln** und dann auf **Regeln hinzufügen**.
3. Im erscheinenden Assistenten wählen Sie **Eine Aktion durchführen bei <Ereignis>**.
4. Im Bereich **Regelbeschreibung bearbeiten**, klicken Sie auf **Ereignis** und wählen zwischen den voreingestellten und benutzerdefinierten Ereignissen aus. Klicken Sie auf **OK**.
5. Klicken Sie auf **Geräte/Aufzeichnungsserver/Management-Server** und wählen Sie den Remote-Server des Remote-Systems für den der zentrale Standort eine Aktion starten soll. Klicken Sie auf **OK**.
6. Klicken Sie auf **Weiter**, um zur nächsten Seite des Assistenten zu gelangen.
7. Wählen Sie die Bedingungen aus, die auf diese Regel zutreffen sollen. Wenn Sie keine Bedingungen auswählen, gilt die Regel immer. Klicken Sie auf **Weiter**.
8. Wählen Sie eine Aktion aus und bestimmen Sie die Einzelheiten im Bereich **Regelbeschreibung bearbeiten**. Klicken Sie auf **Weiter**.
9. Wählen Sie bei Bedarf ein Kriterium zum Stoppen. Klicken Sie auf **Weiter**.
10. Wählen Sie bei Bedarf eine Aktion zum Stoppen. Klicken Sie auf **Fertigstellen**.

# Fernzugriffsdienste

## Fernzugriffsdienste (Erklärung)

> Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Die Funktion Fernzugriffsdienste enthält die von Axis Communications entwickelte Kameraverbindungstechnik Axis One-click. Damit kann das System Video- (und Audio-)Aufnahmen von externen Kameras abrufen, wo Firewalls und/oder die Routernetzwerkkonfiguration normalerweise verhindern, dass Verbindungen zu solchen Kameras hergestellt werden. Die eigentliche Kommunikation findet dann über sichere Tunnelserver (ST-Server) statt. ST-Server verwenden VPN. Innerhalb eines VPN können nur solche Geräte betrieben werden, die über einen gültigen Schlüssel verfügen. Dies ermöglicht einen sicheren Tunnel, wo öffentliche Netzwerke auf sichere Weise Daten austauschen können.

**Mit den Fernzugriffsdiensten können Sie**

- Innerhalb des Axis Dispatch Service Anmeldedaten bearbeiten
- ST-Server hinzufügen, bearbeiten und entfernen
- Axis One-click-Kameras anmelden/abmelden und bearbeiten
- Gehen Sie zu der Hardware, die zu der Axis One-Click-Kamera gehört

## Installieren einer sicheren Tunnelserverumgebung für die Kameraverbindung auf einen Klick

Bevor Sie die Verbindung zur Axis One-click-Kamera benutzen können, müssen Sie zunächst eine geeignete ST-Server Umgebung installieren. Für die Arbeit mit sicheren Tunnelserver (ST-Server) Umgebungen und Axis One-click-Kameras müssen Sie sich zunächst an Ihren Systemanbieter wenden, damit er Ihnen den erforderlichen Benutzernamen und das dazugehörige Passwort für Axis Dispatch Services zur Verfügung stellt.

**Voraussetzungen**

- Wenden Sie sich an Ihren Systemanbieter, um den erforderlichen Benutzernamen und das dazugehörige Passwort für die Axis-Dispatch-Dienste zu erhalten
- Achten Sie darauf, dass Ihre Kameras das Axis Video Hosting System unterstützen. Gehen Sie auf die Internetseite von Axis. Dort finden Sie die unterstützten Geräte (https://www.axis.com/products/axis-guardian)
- Aktualisieren Sie ggf. die Firmware Ihrer Axis-Kameras. Gehen Sie auf die Internetseite von Axis, um die Firmware herunterzuladen (https://www.axis.com/support/firmware)

1. Gehen Sie auf der Startseite jeder Kamera auf **Basiseinrichtung**, **TCP/IP**, und wählen Sie **AVHS aktivieren** und **Immer** aus.
2. Gehen Sie von Ihrem Management Server auf die Milestone Downloadseite (https://www.milestonesys.com/downloads/) und laden Sie die Software **AXIS One-Click** herunter. Führen Sie das Programm zum Einrichten eines geeigneten Axis Secure Tunnel Framework aus.

### Sichere Tunnelserver hinzufügen oder bearbeiten

Die Kommunikation für Fernverbindungsdienste erfolgt über sichere Tunnelserver (ST-Server).

1. Gehen Sie wie folgt vor:
   - Um einen ST-Server hinzuzufügen, klicken Sie mit der rechten Maustaste auf den obersten Knoten **Axis Secure Tunnel Server** und wählen Sie dann **Axis Secure Tunnel Server hinzufügen** aus
   - Zum Bearbeiten eines ST-Servers klicken Sie mit der rechten Maustaste darauf und wählen Sie **Axis Secure Tunnel Server bearbeiten** aus
2. Geben Sie in das Fenster, das sich dann öffnet, die entsprechenden Informationen ein.
3. Wenn Sie sich dafür entscheiden, bei der Installation der **Axis One-Click Connection Komponente** die Anmeldeinformationen zu verwenden, wählen Sie das Kontrollkästchen **Anmeldeinformationen verwenden** aus und geben Sie denselben Benutzernamen und dasselbe Passwort ein, das Sie auch für die Komponente **Axis One-Click Connection** verwendet haben.
4. Klicken Sie auf **OK**.

### Registrieren Sie eine neue Axis One-Click-Kamera

1. Klicken Sie zum Registrieren einer Kamera unter einem ST-Server mit der rechten Maustaste darauf, und wählen Sie **Axis One-Click-Kamera registrieren** aus.
2. Geben Sie in das Fenster, das sich dann öffnet, die entsprechenden Informationen ein.
3. Klicken Sie auf **OK**.
4. Die Kamera erscheint nun unter dem jeweiligen ST-Server.

Die Kamera kann in den folgenden Farben codiert sein:

| Farbe | Beschreibung |
|---|---|
| **Rot** | Eingangsstatus. Registriert, jedoch nicht mit dem ST-Server verbunden. |
| **Gelb** | Registriert. Mit dem ST-Server verbunden, jedoch nicht als Hardware hinzugefügt. |
| **Grün** | Als Hardware hinzugefügt. Ist mit dem ST-Server verbunden, oder auch nicht. |

Wenn Sie eine neue Kamera hinzufügen, ist deren Status stets grün. Der Verbindungsstatus wird von den **Geräten** an **Aufzeichnungsservern** in dem Fenster **Übersicht** angezeigt. Im Bereich **Übersicht** können Sie Ihre Kameras gruppieren, um einen besseren Überblick zu haben. Wenn Sie sich dafür entscheiden, Ihre Kamera zu diesem Zeitpunkt **nicht** beim Axis Dispatch Service anzumelden, können Sie dies später nachholen, indem Sie mit der rechten Maustaste das Kontextmenü aufrufen (und **Axis One-Click-Kamera bearbeiten** auswählen).

# Smart Maps

## Geographische Hintergründe (Erklärung)

Bevor ein Benutzer von XProtect Smart Client einen geographischen Hintergrund auswählen kann, müssen Sie zunächst in XProtect Management Client die geographischen Hintergründe konfigurieren.

- **Einfache Weltkarte** – Verwenden des standardmäßigen geografischen Hintergrunds, der in XProtect Smart Client zur Verfügung steht. Hierfür ist keine Konfiguration erforderlich. Diese Karte ist als allgemeine Referenz gedacht und enthält keine Funktionen wie Ländergrenzen, Städte oder sonstige Einzelheiten. Aber wie die anderen geografischen Hintergründe auch, enthält sie georeferenzierte Daten
- **Bing Maps** – Verbinden mit Bing Maps
- **Google Maps** – Verbinden mit Google Maps
- **Milestone Map Service** - Stellen Sie eine Verbindung zu einem Anbieter für kostenlose Karten her. Wenn Sie Milestone Map Service aktiviert haben, ist keine weitere Einrichtung erforderlich.

  Siehe Milestone Map Service aktivieren

- **OpenStreetMap** - verbinden mit:
  - Ein kommerzieller Kachelserver Ihrer Wahl
  - Ihr eigener, ein Online- oder ein lokaler Kachelserver

  Siehe Angabe des OpenStreetMap-Kachelservers

> Die Bing Maps- und Google Maps-Optionen benötigen Zugriff zum Internet, und Sie müssen einen Schlüssel von Microsoft oder Google kaufen.
>
> Milestone Map Service erfordert einen Internetzugang.
>
> Soweit Sie nicht Ihren eigenen, lokalen Kachelserver verwenden, ist für OpenStreetMap ein Internetzugang erforderlich.

Wenn Sie möchten, dass das System eine EU-DSGVO-konforme Installation hat, müssen die folgenden Dienste verwendet werden:

- Bing Maps
- Google Maps
- Milestone Map Service

Weitere Informationen über den Datenschutz und die Erhebung von Nutzungsdaten finden Sie im Datenschutzleitfaden zur DSGVO.

Standardmäßig stellen Bing Maps und Google Maps Satellitenbilder (Satellit) dar. Sie können die Bilder in XProtect Smart Client ändern, z.B. in Luft- oder Bodenaufnahmen, um verschiedene Einzelheiten sehen zu können.

## Aktivieren Sie Bing Maps oder Google Maps in Management Client

Sie können einen Schlüssel mehreren Benutzern durch deren Eingabe für ein Smart Client-Profil im Management Client zur Verfügung stellen. Alle Nutzer, die diesem Profil zugewiesen sind, können den Schlüssel verwenden.

Schritte:

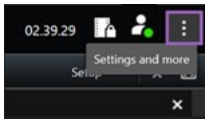
1. Klicken Sie in Management Client im Bereich **Standort-Navigation** auf **Smart Client Profile**.
2. Wählen Sie in dem Fenster **Smart Client**-Profile das entsprechende Smart Client-Profil aus.
3. Klicken Sie im Bereich **Eigenschaften** auf die Registerkarte **Smart Map**:
   - Für Bing Maps geben Sie Ihren Basis- oder Enterprise-Schlüssel im Feld **Bing Maps-Schlüssel** ein
   - Für Google Maps geben Sie Ihren Maps Static API Schlüssel in dem Feld **Privater Schlüssel für Google Maps** ein
4. Um zu verhindern, dass XProtect Smart Client der Betreiber einen anderen Schlüssel verwendet, aktivieren Sie das Kontrollkästchen **Gesperrt**.

## Aktivieren Sie Bing Maps oder Google Maps in XProtect Smart Client

Um zuzulassen, dass XProtect Smart Client Betreiber einen anderen Schlüssel verwenden als den vom Smart Client-Profil, müssen Sie den Schlüssel in den Einstellungen in XProtect Smart Client eingeben.

Schritte:

1. Öffnen in XProtect Smart Client Sie das Fenster **Einstellungen**.




2. Klicken Sie auf **Smart Map**.
3. Unternehmen Sie folgende Schritte, abhängig vom gewünschten Kartendienst:
   - Für Bing Mapsgeben Sie den Schlüssel im Feld **Bing Maps Schlüssel** ein. Siehe auch Smart-Map-Integration mit Bing Maps (Erklärung) auf Seite 93.
   - Für Google Mapsgeben Sie den Schlüssel im Feld **Privater Schlüssel für Google Maps** ein. Siehe auch Smart-Map-Integration mit Google Maps (Erklärung) auf Seite 92.

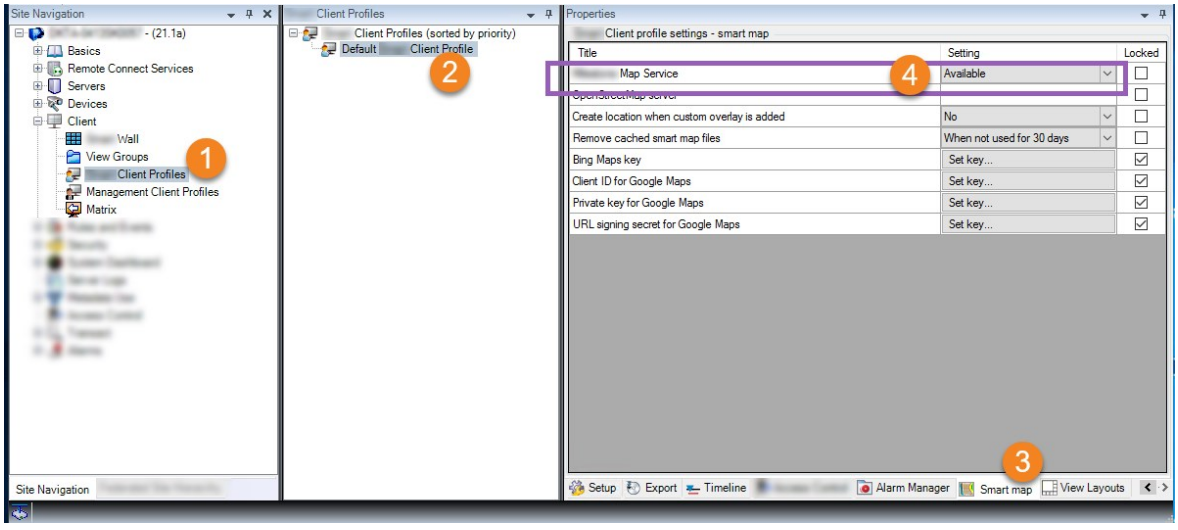
## Aktivieren Sie Milestone Map Service

Milestone Map Service ist ein Online-Dienst, mit dem Sie eine Verbindung zum Kachelserver von Milestone Systems herstellen können. Dieser Kachelserver verwendet einen kostenlosen, kommerziell erhältlichen Kartendienst.

Wenn Sie auf Ihrer Smart Map Milestone Map Service aktiviert haben, verwendet die Smart Map Milestone Map Service als geographischen Hintergrund.

Schritte:

1. Erweitern Sie im Fenster **Standort-Navigation** den Knoten **Client** und klicken Sie auf **Smart Client Profile**.
2. Wählen Sie das passende Smart Client-Profil in der Übersicht aus.
3. Klicken Sie im Bereich **Eigenschaften** auf die Registerkarte **Smart Map**.




4. Wählen Sie in dem Feld **Milestone Map Service Verfügbar**.

5. Um diese Einstellung in XProtect Smart Client zu erzwingen, wählen Sie das Kontrollkästchen **Gesperrt** aus. Dann können die XProtect Smart Client Bediener Milestone Map Service nicht aktivieren oder deaktivieren.
6. Speichern Sie die Änderungen.

Sie können Milestone Map Service auch im Fenster **Einstellungen** in XProtect Smart Client aktivieren.

Milestone Map Service erfordert einen Internetzugang.

Wenn Sie sich hinter einer restriktiven Firewall befinden, ist es wichtig, den Zugriff auf die verwendeten Domänen zu ermöglichen. Möglicherweise müssen Sie ausgehenden Datenverkehr für Milestone Map Service über maps.milestonesys.com auf jedem Computer zulassen, auf dem Smart Client ausgeführt wird.

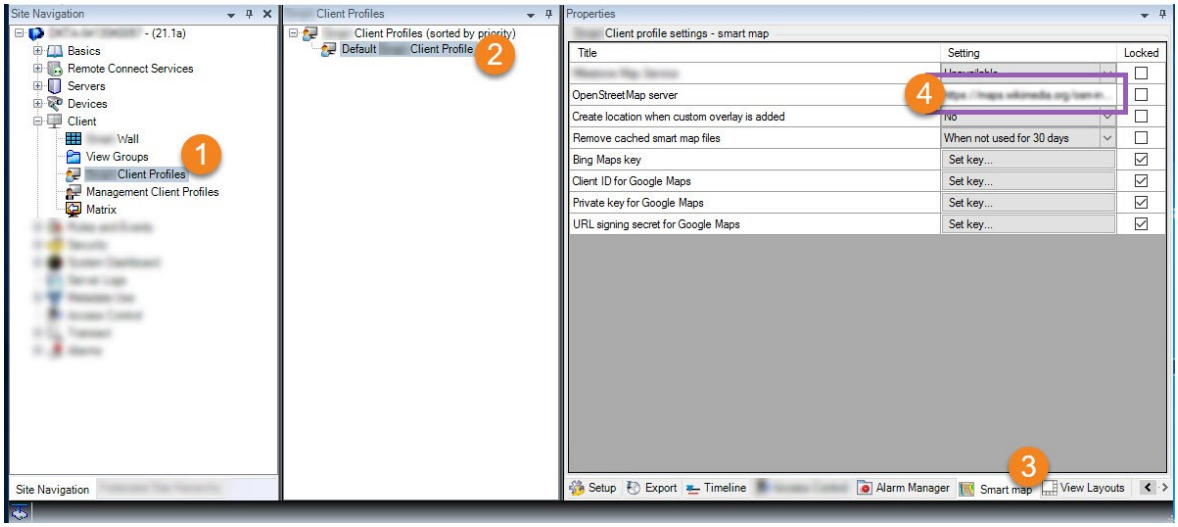
## Geben Sie den OpenStreetMap Tile Server an

Falls Sie die Option **OpenStreetMap** als geographischen Hintergrund für Ihre Smart Map verwenden, müssen Sie angeben, von wo die gekachelten Bilder abgerufen werden. Dies können Sie tun, indem Sie die Adresse entweder eines kommerziellen oder lokalen Kachelservers angeben, z. B. wenn Ihre Organisation über eigene Karten für Bereiche wie Flughäfen oder Häfen verfügt.

Sie können die Adresse des Tile Servers auch in dem Fenster **Einstellungen** in XProtect Smart Client angeben.

Schritte:

1. Erweitern Sie im Fenster **Standort-Navigation** den Knoten **Client** und klicken Sie auf **Smart Client Profile**.
2. Wählen Sie das passende Smart Client-Profil in der Übersicht aus.
3. Klicken Sie im Bereich **Eigenschaften** auf die Registerkarte **Smart Map**.



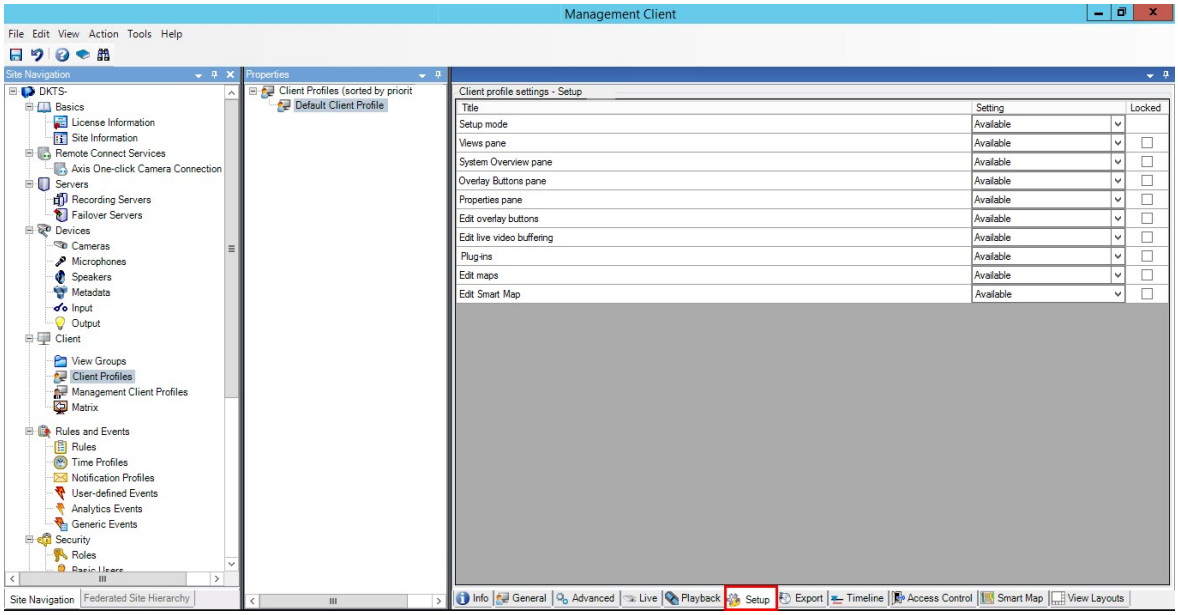

4. Geben Sie in dem Feld **OpenStreetMap-Server** die Adresse des Tile Servers ein.
5. Um diese Einstellung in XProtect Smart Client zu erzwingen, wählen Sie das Kontrollkästchen **Gesperrt** aus. Dann kann das XProtect Smart Client Betriebspersonal die Adresse nicht ändern.
6. Speichern Sie die Änderungen.

## Aktivieren der Smart Map-Bearbeitung

Anwender können die Smart Maps im Setup-Modus im XProtect Smart Client nur dann bearbeiten, wenn die Bearbeitung im Management Client aktiviert ist. Wenn diese Funktion nicht aktiviert ist, müssen Sie die Bearbeitung für jedes relevante Smart Client-Profil aktivieren.

Schritte:

1. Erweitern Sie im Fenster **Standort-Navigation** den Knoten **Client**.
2. Klicken Sie auf **Smart Client-Profile**.




3. Wählen Sie das passende Smart Client-Profil in der Übersicht aus.
4. Klicken Sie im Bereich **Eigenschaften** auf die Registerkarte **Einrichten**.
5. Wählen Sie aus der Liste **Smart Map bearbeiten** den Punkt **Verfügbar** aus.
6. Wiederholen Sie diese Schritte für jedes relevante Smart Client-Profil.
7. Speichern Sie Ihre Änderungen. Wenn sich Benutzer, die dem von Ihnen ausgewählten Smart Client-Profil zugewiesen sind, das nächste Mal beim XProtect Smart Client anmelden, werden sie Smart Maps bearbeiten können.

> Wählen Sie in der Liste **Smart Map bearbeiten Nicht verfügbar** aus, um die Bearbeitungsfunktion zu deaktivieren.

## Aktivieren Sie die Bearbeitung von Geräten auf einer der Smart Map

Sie müssen die Bearbeitung von Geräten für jede Rolle aktivieren, um z.B.:

- Ein Eingabegerät oder ein Mikrofon aus einer Smart Map zu positionieren
- Das Sichtfeld einer Kamera auf einer Smart Map einzustellen

Den Bedienern kann gestattet werden, die folgenden Gerätetypen auf Smart Maps zu bearbeiten:

- Kameras
- Eingabegeräte
- Mikrofone

**Voraussetzungen**
Vergewissern Sie sich, bevor Sie beginnen, dass die Bearbeitung von Smart Maps aktiviert ist (siehe Aktivieren der Smart Map-Bearbeitung auf Seite 350). Überprüfen Sie dafür das Smart Client-Profil, mit dem die Rolle des Anwenders verbunden ist.

Schritte:

1. Erweitern Sie den Knoten **Sicherheit** > **Rollen**.
2. Wählen Sie im Fenster **Rollen** die Rolle aus, mit der Ihr Anwender verbunden ist.
3. Um der Rolle Bearbeitungsrechte zu erteilen:
   - Wählen Sie die Registerkarte **Allgemeine Sicherheit** aus, und wählen Sie im Bereich **Einstellungen für Rollen** den Gerätetyp aus (z.B. **Kameras** oder **Eingabe**)
   - Wählen Sie in der Spalte **Zulassen** das Kontrollkästchen **Vollständige Kontrolle** oder **Bearbeiten** aus
4. Speichern Sie die Änderungen.

Um die Bearbeitung einzelner Geräte zu aktivieren, gehen Sie auf die Registerkarte **Gerät** und wählen Sie das jeweilige Gerät aus.

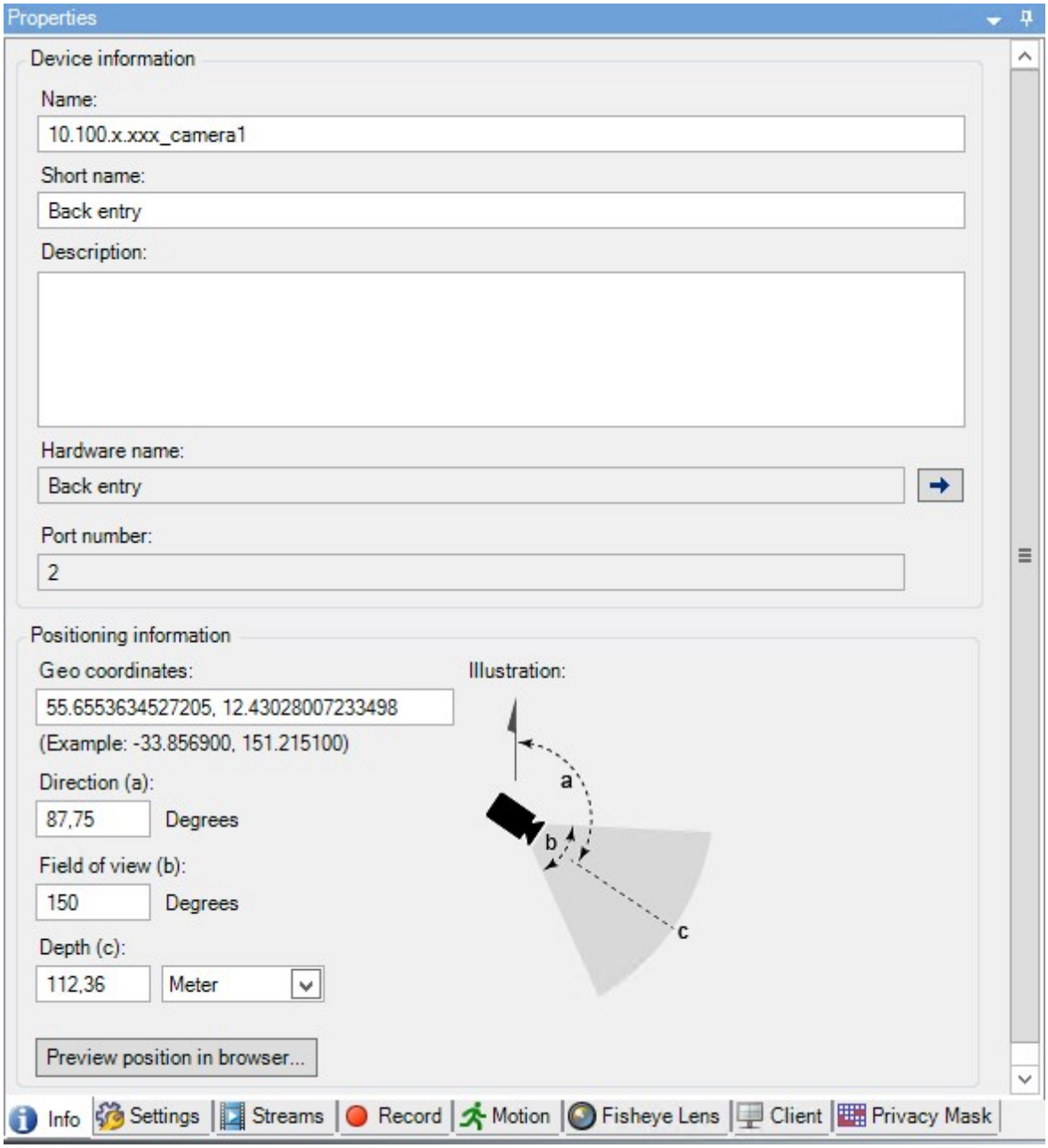
## Definition der Geräteposition und der Kamerablickrichtung, des Sichtfeldes und der Tiefe (Smart Map)

Um sich zu vergewissern, dass ein Gerät korrekt auf der Smart Map positioniert ist, können Sie die geographischen Koordinaten des Gerätes festlegen. Für Kameras können Sie außerdem die Richtung, das Blickfeld und die Raumtiefe festlegen. Mit jeder der o.g. Einstellungen wird das Gerät beim nächsten Mal, wenn ein Bediener die Smart Map in XProtect Smart Client lädt, automatisch zur Smart Map hinzugefügt.

Schritte:

1. Erweitern Sie in Management Client den Knoten **Geräte** und wählen Sie den Gerätetyp aus (z.B. **Kameras** oder **Eingabe**).
2. Wählen Sie im Bereich **Geräte** das jeweilige Gerät aus.

3. ScrollenSieaufderRegisterkarte**Info**herunterzu**Positionierungsinformationen**.




4. Geben Sie im Feld **Geokoordinaten** den Breitengrad und den Längengrad der Koordinaten in dieser Reihenfolge an. Verwenden Sie einen Dezimalpunkt und trennen Sie Breitengrad und Längengrad mit einem Komma.

- Für Kameras:
    1. Geben Sie in das Feld **Richtung** einen Wert zwischen 0 und 360 Grad ein.
    2. Geben Sie in das Feld **Sichtfeld** einen Wert zwischen 0 und 360 Grad ein.
    3. Geben Sie in das Feld **Tiefe** die Blicktiefe ein, entweder in Metern oder in Fuß.

5. Speichern Sie die Änderungen.

Sie können die Eigenschaften auch auf den Aufzeichnungsservern festlegen.

## Smart Map konfigurieren mit Milestone Federated Architecture

Wenn Sie in einer Milestone Federated Architecture Smart Map verwenden, erscheinen alle Geräte von den verbundenen Standorten auf der Smart Map. Folgen Sie den unten angegebenen Schritten, um Smart Map in einer föderalen Architektur einzurichten.

Allgemeine Informationen über Milestone Federated Architecture finden Sie unter Konfigurieren von Milestone Federated Architecture auf Seite 98.

1. Bevor Sie den Hauptstandort mit den Kindstandorten verbinden, vergewissern Sie sich, dass die geographischen Koordinaten aller Geräte an allen Standorten angegeben wurden. Die geographischen Koordinaten werden automatisch hinzugefügt, wenn ein Gerät auf der Smart Map in XProtect Smart Client positioniert wird. Sie können sie in Management Client in den Geräteeigenschaften jedoch auch von Hand hinzufügen. Weitere Informationen finden Sie unter Definition der Geräteposition und der Kamerablickrichtung, des Sichtfeldes und der Tiefe (Smart Map) auf Seite 352.
2. Sie müssen die Smart Client-Anwender als Windows-Benutzer am übergeordneten Standort und an allen föderalen Standorten festlegen. Zumindest am Hauptstandort müssen die Windows-Benutzer über die Berechtigung zur Bearbeitung von Smart Maps verfügen. So können die Benutzer die Smart Map für den Hauptstandort und für alle Kindstandorte bearbeiten. Als Nächstes müssen Sie festlegen, ob die Windows-Benutzer an den untergeordneten Standorten die Berechtigung zum Bearbeiten von Smart Maps benötigen. In Management Client erstellen Sie zuerst die Windows-Benutzer unter **Rollen**, und dann aktivieren Sie Smart Map-Bearbeitung. Weitere Informationen finden Sie unter Aktivieren der Smart Map-Bearbeitung auf Seite 350.
3. Fügen Sie am Hauptstandort die untergeordneten Standorte als Windows-Benutzer zu einer Rolle mit Administratorberechtigungen hinzu. Wenn Sie den Objekttyp angeben, aktivieren Sie das Kontrollkästchen **Computer**.
4. An jedem der Unterstandorte müssen Sie den Hauptstandort als Windows-Benutzer derselben Administratorrolle hinzufügen, die am Hauptstandort verwendet wird. Wenn Sie den Objekttyp angeben, aktivieren Sie das Kontrollkästchen **Computer**.

5. Stellen Sie sicher, dass Sie am Hauptstandort das Fenster der **Hierarchie der föderalen Standorte** sehen können. Gehen Sie in Management Client auf **Ansicht** und wählen Sie **Hierarchie der föderalen Standorte** aus. Fügen Sie jeden der untergeordneten Standorte zum übergeordneten Standort hinzu. Weitere Informationen finden Sie unter Hinzufügen eines Standorts zur Hierarchie auf Seite 335.
6. Nun können Sie testen, ob Milestone Federated Architecture in XProtect Smart Client funktioniert. Melden Sie sich am Hauptstandort als Administrator oder Bediener an und öffnen Sie eine Ansicht, die die Smart Map enthält. Wenn die Einrichtung korrekt erfolgt ist, erscheinen alle Geräte vom Hauptstandort und von den Kindstandorten auf der Smart Map. Wenn Sie sich bei einem der Kindstandorte anmelden, sehen Sie nur die Geräte von diesem Standort und von dessen Kindstandorten.

Um Geräte auf einer Smart Map zu bearbeiten, z. B. die Kameraposition und den Kamerawinkel, benötigen die Benutzer die Berechtigung, Geräte zu bearbeiten. Weitere Informationen finden Sie unter Aktivieren Sie die Bearbeitung von Geräten auf einer der Smart Map auf Seite 351.

# Wartung

## Sicherung und Wiederherstellung einer Systemkonfiguration

Milestone empfiehlt Ihnen, regelmäßig Sicherungskopien Ihrer Systemkonfiguration zu erstellen, damit Sie sie im Notfall wiederherstellen können.

Auch wenn es selten vorkommt, dass Ihre Konfiguration verloren geht, kann es dennoch unter unglücklichen Umständen passieren. Es ist wichtig, dass Sie Ihre gesicherten Daten schützen, entweder durch technische oder durch organisatorische Maßnahmen.

### Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung)

Das System enthält eine integrierte Sicherungsfunktion, welche die gesamte Systemkonfiguration sichert und die Sie im Management Client definieren können. Die Log-Server-Datenbank und die Protokolldateien (einschließlich Auditprotokolldateien) sind nicht in dieser Sicherung eingeschlossen.

Sollte Ihr System besonders groß sein, empfiehlt Milestone, dass Sie planmäßige Sicherungen einrichten. Dies geschieht über das Tool eines Drittanbieters: Microsoft® SQL Server Management Studio. Diese Sicherung schließt die gleichen Daten als manuelle Sicherung ein.

Während einer Sicherung bleibt Ihr System online.

Die Sicherung Ihrer System-Konfiguration kann einige Zeit in Anspruch nehmen. Die Sicherungsdauer hängt ab von:

- Ihre Systemkonfiguration
- Ihre Hardware
- Ob Sie SQL Server, die Event Server- und Management Server-Komponenten auf einem einzigen Server oder auf mehreren Servern installiert haben

Jedes Mal, wenn Sie eine manuelle und planmäßige Datensicherung durchführen, wird die Transaktionsprotokolldatei der SQL Server-Datenbank geleert. Näheres dazu, wie die Transaktionsprotokolldatei gelöscht wird, finden Sie unter SQL Server-Datenbanktransaktionsprotokoll (Erklärung) auf Seite 144.

> ⚠ Stellen Sie bei der Erstellung der Sicherung sicher, dass Sie die Passworteinstellungen in Ihrer Systemkonfiguration kennen.

Für FIPS 140-2-konforme Systeme mit Exporten und archivierten Mediendatenbanken von XProtect VMS Versionen vor 2017 R1, die mit nicht FIPS-konformen Ziffern verschlüsselt sind, ist es erforderlich, die Daten an einem Ort zu archivieren, von wo aus weiterhin auf sie zugegriffen werden kann, wenn FIPS aktiviert wurde. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

## Gemeinsamen Sicherungsordner auswählen

Vor der Sicherung und Wiederherstellung einer Systemkonfiguration müssen Sie einen Sicherungsordner für diesen Zweck bestimmen.

1. Klicken Sie mit der rechten Maustaste auf das Symbol für den Management Server-Dienst im Benachrichtigungsbereich und wählen Sie **Gemeinsamen Sicherungsordner auswählen** aus.
2. Finden Sie im erscheinendem Fenster den gewünschten Dateipfad.
3. Klicken Sie zweimal auf **OK**.
4. Wenn Sie gefragt werden, ob Sie Dateien im aktuellen Sicherungsordner löschen möchten, klicken Sie je nach Bedarf auf **Ja** oder **Nein**.

## Manuelle Sicherung der Systemkonfiguration

1. Wählen Sie aus der Menüleiste **Datei** > **Konfiguration sichern**.
2. Lesen Sie den Hinweis im Dialogfenster und klicken Sie auf **Sicherung**.
3. Geben Sie einen Dateinamen für die .cnf-Datei ein.
4. Geben Sie einen Zielordner an und klicken Sie auf **Speichern**.
5. Warten Sie bis die Sicherung fertiggestellt wurde und klicken Sie dann auf **Schließen**.

Alle relevanten Systemkonfigurationsdateien sind in einer einzigen .cnf-Datei zusammengefasst, die an einem festgelegtem Ort gespeichert wird. Während der Sicherung werden zuerst alle Sicherungsdateien in einen temporären Backup-Systemordner auf dem Management-Server exportiert. Sie können einen anderen temporären Ordner auswählen, in dem Sie mit der rechten Maustaste auf das Management Server-Dienst-Symbol des Benachrichtigungsbereichs klicken und „Gemeinsamen Sicherungsordner auswählen“ auswählen.

## Wiederherstellen einer Systemkonfiguration aus einer manuellen Sicherung

**Wichtige Information**

- Sowohl der installierende Benutzer als auch der wiederherstellende Benutzer müssen lokale Administratoren der Systemkonfiguration der SQL Server-Datenbank auf dem Management-Server sein, **und** auch auf SQL Server
- Bis auf Ihre Aufzeichnungsserver, muss Ihr System für die Dauer der Wiederherstellung vollständig heruntergefahren werden. Dies könnte einige Zeit in Anspruch nehmen
- Eine Sicherung kann nur auf dem System wiederhergestellt werden, in dem sie erstellt wurde. Stellen Sie sicher, dass die Einrichtung der zu dem Zeitpunkt möglichst ähnlich ist, als die Sicherung durchgeführt wurde. Ansonsten könnte die Wiederherstellung fehlschlagen
- Wenn Sie bei der Wiederherstellung dazu aufgefordert werden, das Passwort für die Systemkonfiguration einzugeben, müssen Sie ein Passwort für die Systemkonfiguration eingeben, das zu dem Zeitpunkt gültig war, als das Backup erstellt wurde. Ohne dieses Passwort können Sie Ihre Konfiguration aus dem Backup nicht wiederherstellen.
- Wenn Sie eine Sicherung der SQL Server-Datenbank vornehmen, und sie anschließend auf einem frisch aufgesetzten SQL Server wiederherstellen, funktionieren die Fehlermeldungen aus der SQL Server-Datenbank nicht und Sie erhalten nur eine generische Fehlermeldung vom SQL Server. Um dies zu vermeiden, installieren Sie zunächst Ihr XProtect-System neu mithilfe eines frischen SQL Server und stellen Sie dann dessen Sicherungskopie wieder her
- Wenn die Wiederherstellung während der Validierungsphase fehlschlägt, können Sie die alte Konfiguration erneut starten, da keine Änderungen vorgenommen haben
  Wenn die Wiederherstellung an anderer Stelle im Prozess fehlschlägt, können Sie nicht zur alten Konfiguration zurückkehren
  Solange die Backup-Datei nicht beschädigt ist, können Sie eine weitere Wiederherstellung vornehmen
- Die Wiederherstellung ersetzt die aktuelle Konfiguration. Dies bedeutet, dass jegliche Änderungen an der Konfiguration seit der letzten Sicherung verloren gehen
- Es werden keine Protokolle (einschließlich Auditprotokolle) wiederhergestellt
- Sobald die Wiederherstellung gestartet wurde, kann diese nicht abgebrochen werden

**Wiederherstellung**

1. Klicken Sie mit der rechten Maustaste auf das Symbol für den Management Server-Dienst im Benachrichtigungsbereich und wählen Sie **Konfiguration wiederherstellen** aus.
2. Lesen Sie den wichtigen Hinweis, und klicken Sie auf **Wiederherstellen**.
3. Suchen Sie im Dialogfenster 'Datei öffnen' das Verzeichnis mit der Sicherungsdatei der Systemkonfiguration, wählen Sie diese aus und klicken Sie dann auf **Öffnen**.

   Die Sicherungsdatei befindet sich auf dem Management Client-Computer. Sollte Management Client auf einem anderen Server installiert sein, kopieren Sie die

Sicherungsdatei zu diesen Server, bevor Sie ein Zielverzeichnis auswählen.

4. Das Fenster **Konfiguration wiederherstellen** öffnet. Warten Sie bis die Wiederherstellung beendet ist und klicken Sie dann auf **Schließen**.

## Passwort für die Systemkonfiguration (Erklärung)

Sie können sich aussuchen, ob Sie die Gesamtsystemkonfiguration schützen wollen, indem Sie ein Passwort für die Systemkonfiguration festlegen. Sobald Sie ein Passwort für die Systemkonfiguration festgelegt haben, werden alle Backups mit diesem Passwort geschützt. Die Passworteinstellungen werden auf demjenigen Computer gespeichert, auf dem der Management Server in einem sicheren Ordner läuft. Dieses Passwort benötigen Sie für:

- Die Wiederherstellung der Konfiguration aus einem Backup, das mit anderen Passworteinstellungen erstellt wurde als den aktuellen
- Umzug oder Installation des Management Servers auf einem anderen Computer aufgrund eines Hardwarefehlers (Wiederherstellung)
- Die Konfiguration eines zusätzlichen Management Servers in einem System mit Clustering

Das Passwort für die Systemkonfiguration kann während oder nach der Installation festgelegt werden. Das Passwort muss den Anforderungen von Windows an die Komplexität entsprechen, die in der Windows-Passwortrichtlinie festgelegt sind.

Es ist wichtig, dass Systemadministratoren dieses Passwort sicher aufbewahren. Wenn Sie ein Passwort für die Systemkonfiguration festgelegt haben, und Sie wollen ein Backup wiederherstellen, werden Sie ggf. dazu aufgefordert, das Passwort für die Systemkonfiguration einzugeben. Ohne dieses Passwort können Sie Ihre Konfiguration nicht aus dem Backup wiederherstellen.

## Passworteinstellungen für die Systemkonfiguration

Die Passworteinstellungen für die Systemkonfiguration können geändert werden. In den Passworteinstellungen für die Systemkonfiguration haben Sie die folgenden Optionen:

- Sie können sich aussuchen, ob Sie die Systemkonfiguration mit einem Passwort schützen wollen, indem Sie ein Passwort für die Systemkonfiguration festlegen
- Sie können das Passwort für die Systemkonfiguration ändern

- Sie können sich dafür entscheiden, die Systemkonfiguration nicht mit einem Passwort zu schützen, indem Sie ggf. vorhandene Passwörter für die Systemkonfiguration entfernen

## Die Passworteinstellungen für die Systemkonfiguration ändern

Wenn Sie das Passwort ändern, ist es wichtig, dass die Systemadministratoren die mit den verschiedenen Backups verbundenen Passwörter sicher aufbewahren. Bei der Wiederherstellung eines Backup werden Sie ggf. dazu aufgefordert, das Passwort für die Systemkonfiguration einzugeben, das zu dem Zeitpunkt gültig war, als das Backup erstellt wurde. Ohne dieses Passwort können Sie Ihre Konfiguration nicht aus dem Backup wiederherstellen.

Nachdem Sie das Passwort geändert haben, und wenn Ihr Management Server und Ihr Event Server auf getrennten Computern installiert sind, Süssen sie das aktuelle Passwort für die Systemkonfiguration auch am Event Server eingeben. Näheres hierzu finden Sie unter Aktuelles Passwort für die Systemkonfiguration eingeben (Event Server).

Um die Änderungen anzuwenden, müssen Sie die Management Server Dienste neu starten.

1. Suchen Sie das Taskleistensymbol für den Management Server und achten Sie darauf, dass der Dienst läuft.
2. Klicken Sie mit der rechten Maustaste auf das Symbol für den Management Server-Dienst im Benachrichtigungsbereich und wählen Sie **Einstellungen für Systemkonfigurationspasswort ändern** aus.
3. Das Fenster zum Ändern der Einstellungen für das Passwort für die Systemkonfiguration wird angezeigt.

**Vergeben Sie ein Passwort**

1. Geben Sie das neue Passwort in das Feld **Neues Passwort** ein.
2. Geben Sie das neue Passwort in das Feld **Neues Passwort bestätigen** ein und drücken Sie **Eingabe**.
3. Lesen Sie die Benachrichtigung und klicken Sie dann auf **ja**, um die Änderung anzunehmen.
4. Warten Sie auf die Bestätigung der Änderung und wählen Sie dann **Schließen**.
5. Um die Änderungen anzuwenden, müssen Sie die Management Server Dienste neu starten.
6. Achten Sie nach dem Neustart darauf, dass der Management Server läuft.

**Entfernen Sie den Passwortschutz**

Falls Sie keinen Passwortschutz benötigen, können Sie sich dafür entscheiden, ihn wegzulassen:

1. Aktivieren Sie das Kontrollkästchen: **Ich möchte meine Systemkonfiguration nicht mit einem Passwort schützen, und mir ist klar, dass die Systemkonfiguration dann nicht verschlüsselt ist**.
2. Lesen Sie die Benachrichtigung und klicken Sie dann auf **ja**, um die Änderung anzunehmen.
3. Warten Sie auf die Bestätigung der Änderung und wählen Sie dann **Schließen**.
4. Um die Änderungen anzuwenden, müssen Sie die Management Server Dienste neu starten.
5. Achten Sie nach dem Neustart darauf, dass der Management Server läuft.

## Geben Sie die Einstellungen für das Passwort für die Systemkonfiguration ein (Wiederherstellung)

Wenn die Datei mit den Passworteinstellungen aufgrund eines Hardwarefehlers oder aus anderen Gründen gelöscht wird, müssen Sie die Einstellungen für das Passwort für die Systemkonfiguration eingeben, um auf die Datenbank zugreifen zu können, die die Systemkonfiguration enthält. Während der Installation auf Ihrem neuen Computer werden Sie aufgefordert, die Passworteinstellungen für die Systemkonfiguration einzugeben.

Falls jedoch die Datei, die die Passworteinstellungen enthält, gelöscht oder beschädigt wird, und der Computer, auf dem der Managementserver läuft, keine sonstigen Probleme hat, haben Sie die Option, die Passworteinstellungen für die Systemkonfiguration einzugeben:

1. Suchen Sie das Taskleistensymbol für den Management Server.
2. Klicken Sie mit der rechten Maustaste auf das Symbol für den Management Server-Dienst im Benachrichtigungsbereich und wählen Sie **Passwort für die Systemkonfiguration eingeben** aus.
3. Das Fenster "Ändern der Passworteinstellungen für die Systemkonfiguration" wird angezeigt.

**Die Systemkonfiguration ist passwortgeschützt**

1. Geben Sie das Passwort in das Feld **Passwort** ein und drücken Sie **Eingabe**.
2. Warten Sie, bis das Passwort übernommen wird. Wählen Sie **Schließen**.
3. Achten Sie darauf, dass der Management Server läuft.

**Die Systemkonfiguration ist nicht passwortgeschützt**

1. Aktivieren Sie das Kontrollkästchen: **Dieses System verwendet kein Passwort für die Systemkonfiguration** und wählen Sie **Eingabe**.
2. Warten Sie, bis die Einstellung übernommen wird. Wählen Sie **Schließen**.
3. Achten Sie darauf, dass der Management Server läuft.

## Manuelle Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung)

Wenn Sie eine manuelle Sicherung der -Datenbank des Management-Servers durchführen möchten, die Ihre Systemkonfiguration enthält, sollten Sie darauf achten, dass Ihr System online bleibt. Der standardmäßig vergebene Name für die Datenbank des Management-Servers ist **Surveillance**.

Hier einige Dinge, die Sie vor dem Beginn der Sicherung beachten sollten:

- Sie können eine Sicherung der SQL Server-Datenbank nicht zum Kopieren von Systemkonfigurationen auf andere Systeme verwenden
- Die Sicherung der SQL Server-Datenbank kann einige Zeit in Anspruch nehmen. Es hängt von Ihrer Systemkonfiguration, Ihrer Hardware und davon ab, ob Ihr SQL Server, Ihr Management-Server und Ihr Management Client auf demselben Computer installiert sind
- Protokolle, einschließlich Auditprotokolle, werden in der Datenbank des Log-Servers gespeichert und werden daher **nicht** bei der Sicherung der Datenbank des Management-Servers mit gesichert. Der standardmäßig vergebene Name für die Datenbank des Log-Servers ist **SurveillanceLogServerV2**. Beide SQL Server-Datenbanken werden auf die gleiche Art und Weise gesichert.

## Sicherung und Wiederherstellung der Event-Server-Konfiguration (Erklärung)

Der Inhalt Ihrer Event-Server-Konfiguration ist bei der Sicherung und Wiederherstellung Ihrer Systemkonfiguration mit eingeschlossen.

Bei der ersten Ausführung des Event-Servers werden dessen Konfigurationsdateien alle automatisch in die SQL Server Datenbank verschoben. Sie können die wiederhergestellte Konfiguration auf den Event-Server anwenden, ohne ihn neustarten zu müssen und der Event-Server kann während des Ladens der Konfigurationswiederherstellung jegliche externe Kommunikation starten und stoppen.

## Planmäßige Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung)

Der Management-Server speichert die Systemkonfiguration in einer SQL Server-Datenbank. Milestone empfiehlt regelmäßige Datensicherungen dieser Datenbank, um die Daten im Notfall wiederherstellen zu können. Auch wenn es selten vorkommt, dass die Systemkonfiguration verloren geht, kann es dennoch unter unglücklichen Umständen passieren. Zum Glück dauert dies lediglich 1 Minute, und die Datensicherung hat den weiteren Vorteil, dass dabei das Transaktionsprotokoll der SQL Server-Datenbank geleert wird.

Wenn Sie ein kleineres System besitzen und keine planmäßigen Sicherungen benötigen, können Sie Ihre Systemkonfiguration auch manuell sichern. Eine Anleitung hierzu finden Sie unter Manuelle Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung) auf Seite 362.

Achten Sie bei der Sicherung/Wiederherstellung Ihrer Management-Server darauf, dass die SQL Server-Datenbank mit der Systemkonfiguration der Sicherung/Wiederherstellung mit berücksichtigt wird.

**Anforderungen an die Verwendung von planmäßiger Sicherung und Wiederherstellung**

Microsoft® SQL Server Management Studio, ein auf der Website (https://www.microsoft.com/downloads/) des Anbieters kostenlos zum Herunterladen angebotenes Tool.

Abgesehen von der Verwaltung von SQL Server und der zugehörigen Datenbanken, beinhaltet das Tool einfach nutzbare Sicherungs- und Wiederherstellungsfunktionen. Laden Sie das Tool herunter und installieren Sie es auf Ihrem Management-Server.

## Sicherung der Systemkonfiguration mit planmäßiger Sicherung

1. Öffnen Sie im Windows-Startmenü Microsoft® SQL Server Management Studio.
2. Geben Sie bei der Verbindung den Namen des erforderlichen SQL Server an. Benutzen Sie das Konto mit dem Sie die SQL Server-Datenbank erstellt haben.
    1. Suchen Sie die SQL Server-Datenbank, die Ihre gesamte Systemkonfiguration enthält, einschließlich des Event-Servers, der Aufzeichnungsserver, Kameras, Eingaben, Ausgaben, Benutzern, Regeln, Wachrundgangsprofilen usw. Der standardmäßig vergebene Name für diese SQL-Datenbank ist **Surveillance**.
    2. Führen Sie eine Sicherung der SQL Server-Datenbank durch und stellen achten Sie auf folgendes:
        - Überprüfen Sie, ob die ausgewählte SQL Server-Datenbank die richtige ist
        - Bestätigen Sie, dass der Sicherungstyp **Vollständig** ist
        - Legen Sie den Termin für die wiederkehrende Sicherung. Näheres zu planmäßigen und automatischen Sicherungen erfahren Sie auf der Microsoft-Website (https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017
        - Bestätigen Sie, dass der vorgeschlagene Pfad zufriedenstellend ist oder wählen Sie einen alternativen Pfad aus
        - Wählen Sie **Bestätigung bei Sicherungsende** aus und **Checksum ausführen, bevor auf Medium geschrieben wird**
3. Folgen Sie den Anweisungen im Tool bis zum Ende.

Erwägen Sie auch eine Sicherung der Datenbank des Log-Servers mitsamt Ihren Protokollen nach der gleichen Methode. Der Standardname für die SQL Server-Datenbank des Log-Servers ist **SurveillanceLogServerV2**.

## Wiederherstellen einer Systemkonfiguration aus einer planmäßigen Sicherung

**Voraussetzungen**

Damit während der Wiederherstellung der Datenbank der Systemkonfiguration keine Änderungen an der Systemkonfiguration vorgenommen werden, stoppen Sie den:

- Management Server Service (siehe Serverdienste verwalten auf Seite 377)
- Event Server Dienst (erfolgt über Windows-**Dienste** (suchen Sie auf Ihrem Computer nach **services.msc**. Suchen Sie innerhalb von **Dienste** nach **Milestone XProtect Event Server**))
- World Wide Web Publishing Service, auch als Internet Information Service (IIS) bekannt. Wie der IIS angehalten wird, erfahren Sie unter (https://technet.microsoft.com/library/cc732317(WS.10).aspx/)

Öffnen Sie Microsoft® SQL Server Management Studio vom Windows-**Startmenü** aus.

Machen Sie im Tool Folgendes:

1. Geben Sie bei der Verbindung den Namen Ihres SQL Server an. Verwenden Sie das Konto, unter dem die SQL Server-Datenbank erstellt wurde.
2. Suchen Sie die SQL Server-Datenbank (deren standardmäßig vergebene Name **Surveillance** ist), die Ihre vollständige Systemkonfiguration enthält, einschließlich des Event-Servers, der Aufzeichnungsserver, Kameras, Eingaben, Ausgaben, Benutzer, Regeln, Wachrundgangsprofilen usw.
3. Führen Sie eine Wiederherstellung der SQL Server-Datenbank durch und achten Sie darauf:
   - Auswählen, um **vom** Gerät zu sichern
   - Auswählen von Sicherungsmedium **Datei**
   - Suchen Sie Ihre Sicherungsdatei (**.bak** aus und wählen Sie sie aus
   - Auswählen, um **bereits bestehende Datenbank zu überschreiben**
4. Folgen Sie den Anweisungen im Tool bis zum Ende.

Verwenden Sie die gleiche Methode zur Wiederherstellung der SQL Server-Datenbank des Log-Servers mit Ihren Protokollen. Der Standardname für die SQL Server-Datenbank des Log-Servers ist **SurveillanceLogServerV2**.

> Das System funktioniert nicht, während der Management Server-Dienst angehalten wird. Es ist wichtig daran zu denken, alle Dienste nach der Wiederherstellung der Datenbank wieder zu starten.

## Sicherung der Datenbank des Log-Servers

Bearbeiten Sie die Datenbank des Log-Servers mit der gleichen Methode wie die oben beschriebene Bearbeitung der Systemkonfiguration. Die Datenbank des Log-Servers enthält alle Ihre Systemprotokolle, einschließlich der von Aufzeichnungsservern und Kameras gemeldeten Fehler. Der standardmäßig vergebene Name für die Datenbank des Log-Servers ist **SurveillanceLogServerV2**.

Die SQL Server-Datenbank befindet sich auf dem SQL Server des Log-Servers. Log-Server und Management-Server haben typischerweise ihre SQL Server-Datenbanken auf demselben SQL Server. Die Sicherung der

Datenbank des Log-Servers ist nicht von unbedingter Wichtigkeit, da sie keinerlei Systemkonfigurationen enthält, allerdings könnte Ihnen der Zugriff auf Systemprotokolle aus der Zeit vor der Sicherung/Wiederherstellung des Management-Servers von Nutzen sein.

### Fehler bei der Sicherung und Wiederherstellung sowie weitere Problemfälle (Erklärung)

- Wenn Sie nach Ihrer letzten Sicherung der Systemkonfiguration den Event-Server oder andere registrierte Dienste, wie z. B. den Log-Server verschoben haben sollten, müssen Sie die Konfiguration der registrierten Dienste für Ihr neues System auswählen. Sie können die neue Konfiguration beibehalten, nachdem das System zur alten Version wiederhergestellt wurde. Sie können einfach entscheiden, indem Sie einen Blick auf die Hostnamen der Dienste werfen.
- Wenn die Wiederherstellung der Systemkonfiguration fehlschlägt, weil der Event-Server nicht am angegeben Ort aufzufinden ist (beispielsweise, wenn Sie eine ältere Einrichtung registrierter Dienste gewählt haben), sollten Sie eine erneute Wiederherstellung durchführen.
- Wenn Sie bei der Wiederherstellung der Konfiguration von einem Backup das Passwort für die Systemkonfiguration falsch eingeben, müssen Sie das Passwort für die Systemkonfiguration eingeben, das zu dem Zeitpunkt gültig war, als das Backup erstellt wurde.

## Den Management-Server bewegen

Der Management-Server speichert die Systemkonfiguration in einer SQL Server-Datenbank. Sollten Sie den Management-Server von einem physischen Server zu einen anderen verschieben, ist es besonders wichtig, sicherzustellen, dass Ihr neuer Management-Server ebenfalls Zugriff zu dieser SQL Server-Datenbank bekommt. Die Systemkonfigurationsdatenbank kann auf zwei Arten gespeichert werden:

- **Netzwerk SQL Server**: Wenn Sie Ihre Systemkonfiguration in einer SQL Server-Datenbank auf einem SQL Server in Ihrem Netzwerk speichern, können Sie auf den Speicherort der Datenbank auf diesem SQL Server verweisen, wenn Sie die Management-Server-Software auf Ihrem neuen Management-Server installieren. In diesem Fall gilt lediglich der folgende Absatz zum Hostnamen des Management-Servers und zur IP-Adresse, und Sie sollten den Rest dieses Themas ignorieren:

  **Hostname und IP-Adresse des Management-Servers**: Wenn Sie den Management-Server von einem physischen Server zum anderen verschieben, erweist es sich am Einfachsten dem neuen Server den gleichen Hostnamen und IP-Adresse wie dem Alten zu geben. Dies liegt daran, dass der Aufzeichnungsserver sich automatisch mit dem Hostnamen und der IP-Adresse des alten Management-Servers verbindet. Wenn Sie dem neuen Management-Server einen neuen Hostnamen bzw. eine neue IP-Adresse geben, kann der Aufzeichnungsserver den Management-Server nicht mehr finden. Sie müssen dann jeden Recording Server-Dienst in Ihrem System von Hand anhalten, die URL des dort angegebenen Management-Servers ändern, den Aufzeichnungsserver erneut registrieren, und wenn dies erfolgt ist, den Recording Server Dienst starten.

- **Lokal SQL Server**: Wenn Sie Ihre Systemkonfiguration in einer SQL Server-Datenbank auf einem SQL Server auf dem Management-Server selbst speichern, ist es wichtig, dass Sie die Datenbank mit der Systemkonfiguration des bestehenden Management-Servers vor dem Verschieben sichern. Durch die Sicherung der SQL Server-Datenbank und anschließende Wiederherstellung auf einem SQL Server auf dem neuen Management-Server vermeiden Sie, nach dem Umzug Ihre Kameras, Regeln, Zeitprofile usw. neu konfigurieren zu müssen

> Wenn Sie den Management Server verschieben, brauchen Sie für die Wiederherstellung das aktuelle Passwort für die Systemkonfiguration, siehe Passwort für die Systemkonfiguration (Erklärung) auf Seite 359.

**Voraussetzungen**

- **Das Installationsdatei der Software für die Installation auf dem neuen Management-Server**
- **Die Software-Lizenzdatei (.lic)**, die Sie erhalten haben als Sie das System gekauft und zuerst installiert haben. Sie sollten nicht die aktivierte Software-Lizenzdatei verwenden, die Sie nach einer manuellen Offline-Aktivierung einer Lizenz erhalten haben. Eine aktivierte Software-Lizenzdatei enthält Informationen über den spezifischen Server, auf dem das System installiert ist. Daher kann eine aktivierte Software-Lizenzdatei beim Umzug auf einen neuen Server nicht wiederverwendet werden

Wenn Sie beim Umzug auch Ihre Systemsoftware upgraden, haben Sie eine neue Software-Lizenzdatei erhalten. Verwenden Sie diese einfach.

- **Nur lokale SQL Server Benutzer: Microsoft® SQL Server Management Studio**
- Was geschieht, während der Management-Server nicht mehr verfügbar ist? Nicht verfügbare Management-Server (Erklärung) auf Seite 366)
- Log-Serverdatenbank kopieren (siehe Sicherung der Datenbank des Log-Servers auf Seite 364)

## Nicht verfügbare Management-Server (Erklärung)

- **Aufzeichnungsserver können weiterhin aufzeichnen**: Jeder derzeitige laufende Aufzeichnungsserver erhielt eine Kopie Ihrer Konfiguration vom Management-Server, damit sie weiterhin arbeiten und Aufzeichnungen selbstständig speichern können, während der Management-Server heruntergefahren ist. Planmäßige und durch Bewegung ausgelöste Aufzeichnung funktioniert daher weiterhin, und durch Ereignisse ausgelöste Aufzeichnung ebenfalls, wenn die Ereignisse in Relation zum Management-Server oder einem anderen Aufzeichnungsserver besteht, da diese durch den Management-Server geleitet werden

- **Aufzeichnungsserver speichern Protokolldaten vorübergehend lokal**: Sie senden automatisch Protokolldaten zum Management-Server, wenn dieser wieder zur Verfügung steht:
  - **Clients können sich nicht anmelden**: Clientzugriff wird durch den Management-Server autorisiert. Ohne den Management-Server können sich Clients nicht anmelden
  - **Clients, die bereits angemeldet sind, können für bis zu 4 Stunden angemeldet bleiben**: Wenn Clients sich anmelden, werden sie vom Management Server autorisiert und können bis zu 4 Stunden lang mit Aufzeichnungsservern kommunizieren. Wenn Sie es schaffen, den neuen Management Server innerhalb von 4 Stunden in Betrieb zu nehmen, werden viele Ihrer Benutzer nicht betroffen sein
  - **Keine Fähigkeit zur Konfiguration des Systems**: Ohne den Management-Server können Sie die Systemkonfiguration nicht ändern

Milestone empfiehlt, dass Sie Ihre Benutzer über die Möglichkeit von Verbindungsabbrüchen mit dem Überwachungssystem, während der Ausfallzeit des Management-Servers, informieren.

### Verschieben der Systemkonfiguration

Das Bewegen Ihrer Systemkonfiguration ist ein Prozess mit drei Schritten:

1. Führen Sie eine Sicherung Ihrer Systemkonfiguration durch. Dies entspricht exakt der Erstellung einer geplanten Sicherungskopie. Siehe auch Sicherung der Systemkonfiguration mit planmäßiger Sicherung auf Seite 363.
2. Installieren Sie den neuen Management-Server auf dem neuen Server. Siehe „planmäßige Sicherung“, Schritt 2.
3. Stellen Sie Ihre Systemkonfiguration im neuen System wieder her. Siehe auch Wiederherstellen einer Systemkonfiguration aus einer planmäßigen Sicherung auf Seite 363.

## Ersetzen eines Aufzeichnungsservers

Wenn ein Aufzeichnungsserver ausfällt und Sie möchten ihn mit einem neuen Server ersetzen, der die Einstellungen des alten Aufzeichnungsservers übernimmt:

1. Rufen Sie die Aufzeichnungsserver-ID des alten Aufzeichnungsserver ab:
   1. Wählen Sie **Aufzeichnungsserver**, dann wählen Sie im Bereich **Übersicht** den alten Aufzeichnungsserver aus.
   2. Wählen Sie die Registerkarte **Speicher** aus.
   3. Drücken und halten Sie die STRG-Taste auf Ihrer Tastatur, während Sie die Registerkarte **Info** auswählen.

4. Kopieren Sie die Aufzeichnungsserver-ID in den unteren Teil der Registerkarte **Info**. Kopieren Sie nicht den Begriff *ID*, sondern nur die Zahl selbst.


2. Ersetzen Sie die Aufzeichnungsserver-ID auf dem neuen Aufzeichnungsserver:
    1. Stoppen Sie den Recording Server-Dienst auf dem alten Aufzeichnungsserver und stellen Sie dann in den Windows-**Diensten** den **Starttyp** auf **Deaktiviert**.

> **!** Es ist äußerst wichtig, dass Sie nicht zwei Aufzeichnungsserver mit identischer ID zur gleichen Zeit starten.

    2. Öffnen Sie auf dem neuen Aufzeichnungsserver ein Explorerfenster und gehen Sie zu `C:\ProgramData\Milestone\XProtect Recording Server` oder den Pfad, wo Ihr Aufzeichnungsserver untergebracht ist.
    3. Öffnen Sie die Datei `RecorderConfig.xml`.
    4. Löschen Sie die ID, die zwischen den Tags *<id>* und *</id>* angegeben ist.


    5. Fügen Sie die kopierte Aufzeichnungsserver-ID zwischen den Tags *<id>* und *</id>* ein. Speichern Sie die *RecorderConfig.xml*-Datei.
    6. Gehen Sie in die Registry: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation`.
    7. Öffnen Sie **RecorderIDOnMachine** und ersetzen Sie die alte Aufzeichnungsserver-ID mit der neuen ID.
3. Registrieren Sie den neuen Aufzeichnungsserver auf dem Managementserver. Klicken Sie hierfür mit der rechten Maustaste auf das Taskleistensymbol Recording Server Manager und klicken Sie auf **Registrieren**. Weitere Informationen finden Sie unter Registrieren eines Aufzeichnungsservers auf Seite 209.
4. Starten Sie den Recording Server-Dienst neu. Sobald der neue Recording Server-Dienst gestartet wird, wurden alle Einstellungen des alten Aufzeichnungsservers übernommen.

## Hardware verschieben

Sie können Hardware zwischen Aufzeichnungsservern verschieben, die zum selben Standort gehören. Nachdem sie verschoben worden sind, laufen die Hardware und Geräte auf dem neuen Aufzeichnungsserver und neue Aufzeichnungen werden auf diesem gespeichert. Das Verschieben von Hardware und Geräten ist für

Clientbenutzer transparent.

Die Aufzeichnungen auf dem alten Aufzeichnungsserver bleiben dort, bis:

- Das System sie löscht, wenn die Speicherzeit abläuft. Aufzeichnungen, die jemand mit einer Beweismittelsicherung geschützt hat (siehe Beweissicherung (Erklärung) auf Seite 77) werden erst gelöscht, wenn die Speicherfrist für die Beweismittelsicherung abgelaufen ist. Bei der Erstellung von Beweissicherungen bestimmen Sie ihre Speicherzeit. Potenziell läuft die Speicherzeit nie ab
- Sie löschen sie vom neuen Aufzeichnungsserver jedes Geräts auf der Registerkarte **Aufzeichnen**

Sie erhalten eine Warnung, wenn Sie versuchen einen Aufzeichnungsserver zu entfernen, der noch Aufzeichnungen enthält.

> Wenn Sie Hardware auf einen Aufzeichnungsserver verschieben, dem gerade keine Hardware hinzugefügt ist, müssen die Clientbenutzer sich ausloggen und wieder einloggen, um Daten von den Geräten zu empfangen.

Sie können die Funktion zum Verschieben von Hardware für Folgendes nutzen:

- **Lastausgleich**: Falls beispielsweise die Festplatte eines Aufzeichnungsservers überlastet ist, können Sie einen neuen Aufzeichnungsserver hinzufügen und einige Hardware-Einheiten verschieben
- **Upgrade**: Wenn Sie beispielsweise den Hostserver des Aufzeichnungsservers durch ein neueres Modell ersetzen müssen, können Sie einen neuen Aufzeichnungsserver installieren und die Hardware vom alten auf den neuen Server verschieben
- **Ersetzen eines defekten Aufzeichnungsservers**: Wenn der Server beispielsweise offline ist und nie wieder online gehen wird, können Sie die Hardware auf andere Aufzeichnungsserver verschieben und so das System aufrechterhalten. Sie haben keinen Zugriff auf die alten Aufzeichnungen. Weitere Informationen finden Sie unter Ersetzen eines Aufzeichnungsservers auf Seite 367.

**Fernaufzeichnungen**

Wenn Sie Hardware auf einen anderen Aufzeichnungsserver verschieben, bricht das System laufende oder planmäßige Abfragen von verbundenen Standorten oder lokalen Speichern in Kameras ab. Die Aufzeichnungen werden nicht gelöscht, aber die Daten werden von den Datenbanken nicht gespeichert und empfangen wie üblich. Ist dies der Fall, erhalten Sie eine Warnung. Die Abfrage des XProtect Smart Client-Benutzers, der eine Abfrage bei Verschiebung der Hardware gestartet hat, schlägt fehl. Der XProtect Smart Client-Benutzer wird benachrichtigt und kann es später erneut versuchen.

Falls Hardware auf einen Remote-System verschoben wurde, müssen Sie den zentralen Standort mit der Option **Hardware aktualisieren** manuell synchronisieren, um die neue Konfiguration des Remote-Systems widerzuspiegeln. Wenn Sie keine Synchronisierung durchführen, bleiben die verschobenen Kameras vom zentralen Standort abgeschnitten.

## Hardware verschieben (Assistent)

Führen Sie den **Hardware verschieben**-Assistenten aus, um Hardware zwischen Aufzeichnungsservern zu verschieben. Der Assistent führt Sie durch die notwendigen Schritte, um ein oder mehrere Hardware-Geräte zu verschieben.

**Voraussetzungen**
Bevor Sie den Assistenten starten:

- Stellen Sie sicher, dass der neue Aufzeichnungsserver über das Netzwerk Zugriff auf die physische Kamera hat
- Installieren Sie einen Aufzeichnungsserver, auf den Sie die Hardware verschieben wollen (siehe Installation über Download Manager (Erklärung) auf Seite 176 oder Automatische Installation eines Aufzeichnungsservers auf Seite 185)
- Installieren Sie die geleichen Device-Pack-Versionen auf dem neuen Aufzeichnungsserver, die auch auf dem bestehenden Server laufen (siehe Gerätetreiber (Erklärung) auf Seite 154)

So starten Sie den Assistenten:

1. Wählen Sie im Bereich **Standort-Navigation Aufzeichnungsserver** aus.
2. Klicken Sie im Bereich **Übersicht** mit der rechten Maustaste auf den Aufzeichnungsserver, von dem Sie Hardware verschieben möchten, oder auf ein bestimmtes Gerät.
3. Wählen Sie **Hardware verschieben**.

   Es erscheint eine Fehlermeldung, falls der Aufzeichnungsserver, von dem Sie Hardware verschieben, vom Netzwerk getrennt ist. Sie sollten Hardware nur von einem getrennten Aufzeichnungsserver verschieben, wenn Sie sicher sind, dass dieser nie wieder online geht. Falls Sie Hardware trotzdem verschieben und der Server wieder online geht, riskieren Sie ein unerwartetes Verhalten des Systems, da dieselbe Hardware für einige Zeit auf zwei Aufzeichnungsservern läuft. Mögliche Probleme sind beispielsweise Lizenzfehler oder Ereignisse, die nicht an den richtigen Aufzeichnungsserver gesendet werden.

4. Wenn Sie den Assistenten auf der Ebene des Aufzeichnungsservers gestartet haben, erscheint die Seite **Wählen Sie die Hardware, die Sie verschieben möchten**. Wählen Sie die Geräte aus, die Sie verschieben möchten.
5. Wählen Sie auf der Seite **Wählen Sie den Aufzeichnungsserver, auf den Sie die Hardware verschieben möchten** aus der Liste der an diesem Standort installierten Aufzeichnungsservern aus.

6. Auf der Seite **Wählen Sie den Speicher, auf dem Aufzeichnungen zukünftig gespeichert werden sollen** zeigt der Speicherauslastungsbalken die freie Kapazität in der Aufzeichnungsdatenbank nur für Live-Aufzeichnungen an, nicht für Archive. Die gesamte Speicherzeit ist die Speicherzeit für die Aufzeichnungsdatenbank und die Archive.
7. Das System verarbeitet Ihre Anforderung.
8. Klicken Sie auf **Schließen**, wenn die Hardware erfolgreich verschoben wurde. Wenn Sie den neuen Aufzeichnungsserver im Management Client auswählen, können Sie die verschobene Hardware sehen und Aufzeichnungen werden nun auf diesem Server gespeichert.

   Wenn der Vorgang fehlgeschlagen ist, können Sie das Problem unten beheben.

   > In einem vernetzten System müssen Sie den zentralen Standort nach einer Verschiebung von Hardware auf einen Remote-System manuell synchronisieren, um die Änderungen, die Sie oder ein anderer Systemadministrator gemacht haben, widerzuspiegeln.

**Fehlerbehandlung beim Verschieben von Hardware**

Wenn Hardware nicht verschoben werden konnte, kann einer der folgenden Gründe dafür verantwortlich sein:

| Fehlertyp | Fehlerbehandlung |
|---|---|
| Der Aufzeichnungsserver ist nicht verbunden oder befindet sich im Failover-Modus. | Stellen Sie sicher, dass der Aufzeichnungsserver online ist. Sie müssen ihn ggf. registrieren.<br>Falls sich der Server im Failover-Modus befindet, warten Sie und versuchen Sie es dann erneut. |
| Bei dem Aufzeichnungsserver handelt es sich nicht um die aktuellste Version. | Aktualisieren Sie den Aufzeichnungsserver, damit er dieselbe Version wie der Management-Server hat. |
| Der Aufzeichnungsserver konnte in der Konfiguration nicht gefunden werden. | Stellen Sie sicher, dass der Aufzeichnungsserver nicht deinstalliert wurde. |
| Die Aktualisierung der Konfiguration oder die Kommunikation mit der | Achten Sie darauf, dass Ihr SQL Server und die dazugehörige Datenbank verbunden sind und laufen. |

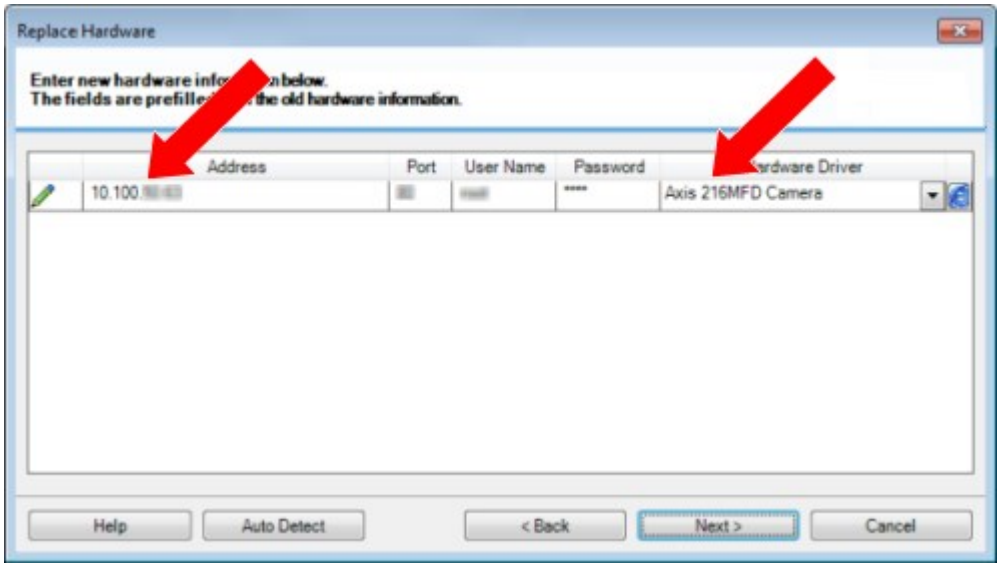
| Fehlertyp | Fehlerbehandlung |
|---|---|
| Konfigurationsdatenbank ist fehlgeschlagen. | |
| Das Beenden der Hardware auf dem aktuellen Aufzeichnungsserver ist fehlgeschlagen | Möglicherweise wurde der Aufzeichnungsserver durch einen anderen Prozess gesperrt, oder er befindet sich im Fehler-Modus.<br>Stellen Sie sicher, dass der Aufzeichnungsserver läuft und versuchen Sie es erneut. |
| Die Hardware ist nicht vorhanden. | Stellen Sie sicher, dass die Hardware, die Sie verschieben möchten, nicht durch einen anderen Benutzer simultan vom System deinstalliert wurde. Dieses Szenario ist sehr unwahrscheinlich. |
| Der Aufzeichnungsserver, dessen Hardware verschoben wurde, ist wieder online, doch Sie haben ihn ignoriert, als er offline war. | Höchstwahrscheinlich waren Sie der Ansicht, dass der alte Aufzeichnungsserver nicht mehr online gehen wird, als Sie den Assistenten zum **Hardware verschieben** gestartet haben, doch der Server ist während des Vorgangs online gegangen.<br>Starten Sie den Assistenten erneut und wählen Sie **Nein** aus, wenn Sie aufgefordert werden zu bestätigen, dass der Server wieder online geht. |
| Der Quellenaufzeichnungsspeicher ist nicht verfügbar. | Sie versuchen, Hardware mit Geräten zu verschieben, die mit einem Aufzeichnungsspeicher konfiguriert sind, der derzeit jedoch offline ist.<br>Ein Aufzeichnungsspeicher ist offline, wenn die Festplatte offline oder anderweitig nicht verfügbar ist.<br>Stellen Sie sicher, dass der Aufzeichnungsserver online ist, und versuchen Sie es erneut. |
| Alle Aufzeichnungsspeicher müssen auf dem Ziel-Aufzeichnungsserver verfügbar sein. | Sie versuchen, Hardware auf einen Aufzeichnungsserver zu verschieben, auf dem derzeit ein oder mehrere Aufzeichnungsspeicher offline sind.<br>Stellen Sie sicher, dass alle Aufzeichnungsspeicher auf dem Ziel-Aufzeichnungsserver online sind.<br>Ein Aufzeichnungsspeicher ist offline, wenn die Festplatte offline oder anderweitig nicht verfügbar ist. |

# Hardware ersetzen

Wenn Sie ein Gerät in Ihrem Netzwerk mit einem anderen ersetzen, müssen Sie die IP-Adressen, den Port, Benutzernamen und das Passwort des neuen Geräts kennen.

Wenn Sie die automatische Lizenzaktivierung eingeschaltet haben (siehe Automatische Lizenzaktivierung (Erklärung) auf Seite 124) und alle Geräteänderungen ohne Aktivierung verwendet haben (siehe Geräteänderungen ohne Aktivierung (Erklärung) auf Seite 125), müssen Sie Ihre Lizenzen von Hand aktivieren **nachdem** Sie Ihre Hardwaregeräte ersetzt haben. Wenn die Anzahl der neuen Hardwaregeräte die Gesamtzahl Ihrer Gerätelizenzen übersteigt, müssen Sie neue Gerätelizenzen erwerben.

1. Erweitern Sie den erforderlichen Aufzeichnungsserver, und klicken Sie mit der rechten Maustaste auf die Hardware, die Sie ersetzen möchten.
2. Wählen Sie **Hardware ersetzen** aus.
3. Der Assistent **Hardware ersetzen** erscheint. Klicken Sie auf **Weiter**.
4. Im Feld **Adresse** des Assistenten (durch roten Pfeil in der Abbildung markiert), geben Sie die IP-Adresse der neuen Hardware ein. Wählen Sie den entsprechenden Treiber aus der Auswahlliste **Hardwaretreiber** aus, wenn dieser Ihnen bekannt ist. Andernfalls wählen Sie die **Automatische Erkennung** aus. Wenn Port, Benutzername oder Passwortdaten der neuen Hardware abweichen, korrigieren Sie dies **bevor der Prozess der automatischen Erkennung (falls benötigt) startet**.



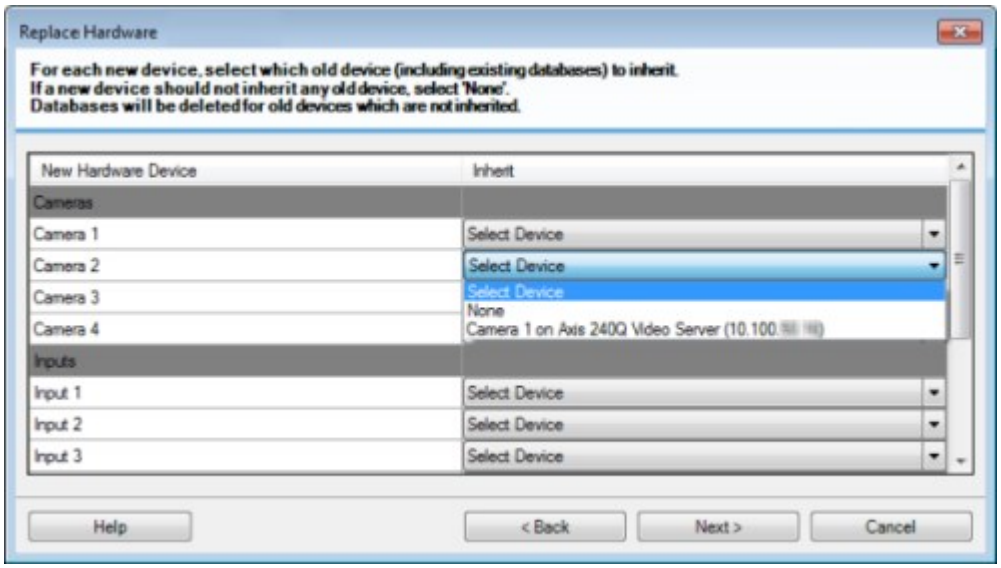

In den Assistenten wurden bereits Daten der vorhandenen Hardware eingetragen. Wenn Sie diese mit einem ähnlichen Gerät ersetzen, können Sie einige Daten gegebenenfalls wiederverwenden (z. B. Port- und Treiberinformationen).

5. Gehen Sie wie folgt vor:
   - Wenn Sie die erforderlichen Gerätetreiber direkt aus der Liste ausgewählt haben, klicken Sie auf **Weiter**
   - Wenn Sie **Automatische Erkennung** in der Liste ausgewählt haben, klicken Sie auf **Automatische Erkennung**, warten Sie auf den erfolgreichen Abschluss dessen (durch ein ✓ ganz links markiert) und klicken Sie dann auf **Weiter**

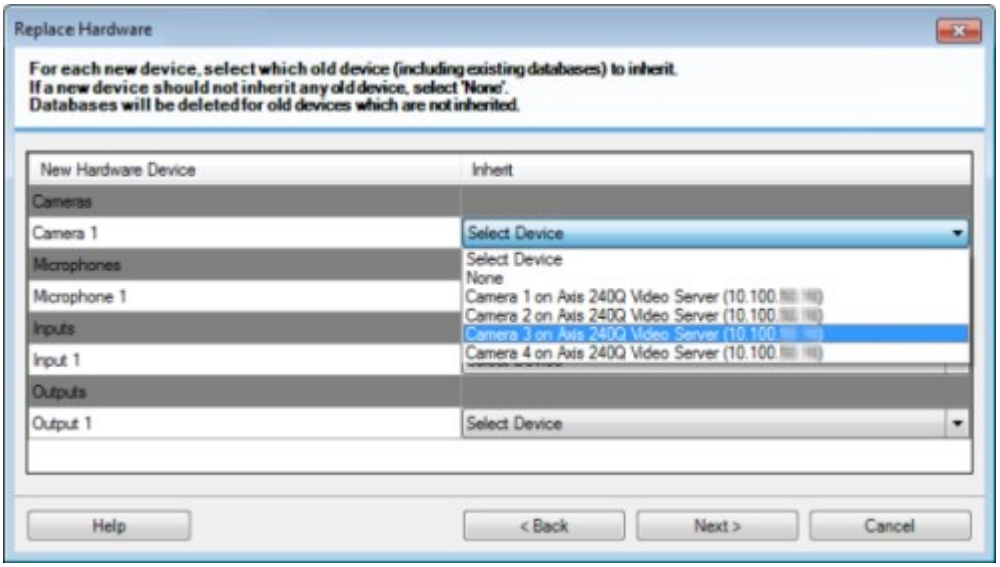
     Dieser Schritt hilft Ihnen dabei Geräte und ihre Datenbanken zusammenzuführen, abhängig von der Anzahl individueller Kameras, Mikrofone, Eingaben, Ausgaben usw., die an der alten bzw. neuen Hardware angebracht ist.

     Es ist wichtig darüber nachzudenken, **wie** man Datenbanken alter Geräte zu den Datenbanken neuer Geräte zusammenfügt. Sie führen die tatsächliche Zusammenführung individueller Geräte mittels der Auswahl einer korrespondierenden Kamera, Mikrofon, Eingabe, Ausgabe oder **Nichts** dergleichen in der Spalte auf der rechten Seite durch.

     > ⚠ Stellen Sie sicher, **alle** Kameras, Mikrofone, Eingaben, Ausgaben, usw. zuzuordnen. Inhalte, denen **Nichts** zugeordnet wird, gehen **verloren**.



Beispiel, in dem die alte Hardware über mehr individuelle Geräte verfügt als die neue:




Klicken Sie auf **Weiter**.

6. Ihnen wird eine Liste mit Hardware angeboten, die Sie hinzufügen, ersetzen oder entfernen können. Klicken Sie auf **Bestätigen**.
7. Der letzte Schritt ist eine Zusammenfassung hinzugefügter, ersetzter und übernommener Geräte und ihren Einstellungen. Klicken Sie auf **In die Zwischenablage kopieren**, um Inhalte in die Windows-Zwischenablage zu kopieren oder/und **Schließen**, um den Assistenten zu beenden.

## Aktualisieren Sie Ihre Hardware-Daten

Damit Ihr Hardware-Gerät und das System dieselbe Firmware-Version verwenden, müssen Sie die Hardware-Daten für das Hardware-Gerät in der Management Client von Hand aktualisieren. Milestone empfiehlt Ihnen, die Hardware-Daten nach jeder Aktualisierung der Firmware Ihres Hardware-Gerätes zu aktualisieren.

Die neuesten Hardware-Daten erhalten Sie wie folgt:

1. Wählen Sie im Bereich **Standort-Navigation Aufzeichnungsserver** aus.
2. Erweitern Sie den gewünschten Aufzeichnungsserver und wählen Sie dann die Hardware aus, für die Sie die neuesten Informationen abrufen möchten.
3. Klicken Sie im Bereich **Eigenschaften** auf der Registerkarte **Info** auf die Schaltfläche **Aktualisieren** im Feld **Letzte Aktualisierung der Hardwaredaten**.

4. Der Assistent prüft nun, ob auf dem System die neueste Firmware für die Hardware läuft.

   Wählen Sie **Bestätigen**, um die Informationen im Management Client zu aktualisieren. Wenn die Aktualisierung abgeschlossen ist, wird die aktuelle Firmware-Version für das vom System erkannte Hardware-Gerät im Feld **Firmware-Version** auf der Registerkarte **Info** angezeigt.

## Ändern des Speicherorts und des Namens einer SQL Server Datenbank

Der Management Server, Event Server, Log-Server, Identity Provider und XProtect Incident Manager verbinden sich mit verschiedenen SQL Server Datenbanken über Connection Strings. Diese Connection Strings werden in der Windows Registry gespeichert. Wenn Sie den Speicherort oder Namen einer SQL Server Datenbank geändert haben, müssen Sie alle Connection Strings bearbeiten, die auf diese SQL Server Datenbank verweisen.

| Datenbank | Verwendet von |
|---|---|
| **Überwachungsdatenbank** | • Management Server Dienst<br>• Event Server Dienst<br>• VideoOS Management Server App-Pool<br>• VideoOS Report Server App-Pool |
| **Surveillance_IDP** | • VideoOS IDP App-Pool |
| **Surveilance_IM** | • VideoOS IM App-Pool |
| **Surveillance_LogServerV2** | • Log Server Dienst |

Bevor Sie fortfahren:

- Sichern Sie die SQL Server Datenbanken und die Windows Registry.
- Stellen Sie sicher, dass der Benutzer, der die zugehörigen Dienste und App-Pools ausführt, der Eigentümer der Datenbank ist.
- Schließen Sie die Inhaltsmigration von der alten SQL Server Datenbank zur neuen ab.

Zur Aktualisierung der Connection Strings mit dem neuen Speicherort und dem Namen einer SQL Server Datenbank:

1. Stoppen Sie alle XProtect VMS Services und App-Pools, welche die SQL Server Datenbank verwenden.

   > Abhängig von Ihrer Systemarchitektur werden die Dienste und App-Pools ggf. auf unterschiedlichen Computern ausgeführt. Sie müssen alle App-Pools und Dienste stoppen, die sich mit derselben SQL Server Datenbank verbinden.

2. Im Registrierungs-Editor gehen Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString`.
3. Aktualisieren Sie die Connection Strings mit dem neuen Speicherort und dem Namen einer SQL Server Datenbank.

   Die Standard-Connection-Strings für alle SQL Server Datenbanken sind:

   - **ManagementServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **EventServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ServerService**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ReportServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IDP**: `Data Source=localhost;Initial Catalog=Surveillance_IDP;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IncidentManager**: `Data Source=localhost;Initial Catalog=Surveillance_IM;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **LogServer**: `Data Source=localhost;Initial Catalog=SurveillanceLogServerV2;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`

4. Starten Sie alle XProtect Dienste und App-Pools, die Sie in Schritt 1 gestoppt haben.

## Serverdienste verwalten

Auf dem Rechner, auf dem Serverdienste laufen, finden Sie Serververwaltungs-Taskleistensymbole im Benachrichtigungsbereich. Über diese Symbole können Sie Informationen über die Serverdienste erhalten und gewisse Aktionen durchführen. Dies schließt beispielsweise das Überprüfen des Status der Dienste ein, sowie eine Ansicht von Protokollen oder Statusmeldungen und das Starten/Stoppen der Dienste.

## Taskleistensymbole für den Servermanager (Erklärung)

Die Taskleistensymbol in der Tabelle zeigen die verschiedenen Zustände der Dienste, die auf dem Managementserver, dem Aufzeichnungsserver, dem ausfallsicheren Aufzeichnungsserver und auf dem Ereignisserver laufen. Diese werden im Benachrichtigungsbereich auf den Computern angezeigt, auf denen die Server installiert sind:

| Management Server Manager Taskleistensymbol | Recording Server Manager Taskleistensymbol | Event Server Manager Taskleistensymbol | Failover Recording Server Manager Taskleistensymbol | Beschreibung |
|---|---|---|---|---|
|  |  |  |  | **Läuft**<br>Erscheint, wenn ein Serverdienst aktiviert ist und gestartet wird.<br>Wenn der Failover Recording Server Dienst läuft, so kann er übernehmen, wenn der Standardaufzeichnungsserver ausfällt. |
|  |  |  |  | **Gestoppt**<br>Erscheint, wenn ein Serverdienst angehalten wurde. |

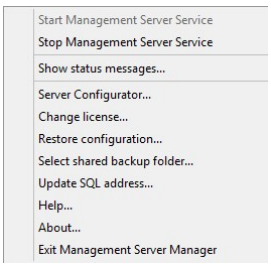
| Management Server Manager Taskleistensymbol | Recording Server Manager Taskleistensymbol | Event Server Manager Taskleistensymbol | Failover Recording Server Manager Taskleistensymbol | Beschreibung |
|---|---|---|---|---|
| | | | | Wenn der Failover Recording Server-Dienst anhält, so kann er nicht übernehmen, wenn der Standardaufzeichnungsserver ausfällt. |
|  |  |  |  | **Starte**<br>Erscheint, wenn ein Serverdienst dabei ist, zu starten. Unter normalen Umständen wechselt das Taskleistensymbol nach kurzer Zeit in **Läuft**. |
|  |  |  | | **Halte an**<br>Erscheint, wenn ein Serverdienst dabei ist, anzuhalten. Unter normalen Umständen wechselt das Taskleistensymbol nach kurzer Zeit in **Angehalten**. |
| |  |  | | **In unbestimmtem Zustand**<br>Erscheint, wenn der Serverdienst zunächst geladen wird, und bis die erste Information erhalten wird, worauf das Taskleistensymbol unter |

| Management Server Manager Taskleistensymbol | Recording Server Manager Taskleistensymbol | Event Server Manager Taskleistensymbol | Failover Recording Server Manager Taskleistensymbol | Beschreibung |
|---|---|---|---|---|
| | | | | normalen Umständen in **Starte** wechselt, und danach in **Läuft**. |
| |  | |  | **Läuft offline**<br>Erscheint typischerweise, wenn der Aufzeichnungsserver oder der ausfallsichere Aufzeichnungsserver läuft, der Management Server Dienst jedoch nicht. |

## Starten oder Stoppen des Management Server-Dienstes

Das Management Server Manager-Taskleistensymbol zeigt den Status des Management Server-Dienstes an, beispielsweise **Läuft**. Durch dieses Symbol können Sie den Management Server-Dienst starten oder stoppen. Wenn Sie den Management Server-Dienst stoppen, können Sie den Management Client nicht nutzen.

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das Management Server Manager-Taskleistensymbol. Ein Kontextmenü erscheint.



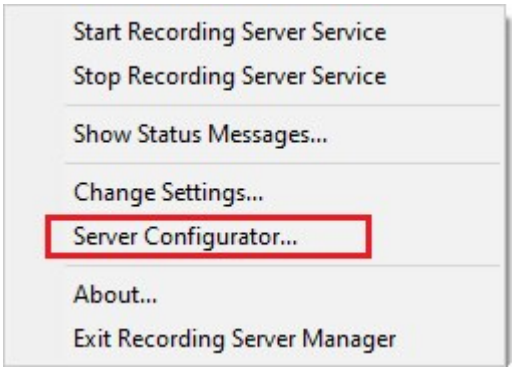

2. Wenn der Dienst angehalten wurde, klicken Sie auf **Management Server-Dienst starten**, um ihn zu starten. Die Änderungen des Taskleistensymbols spiegeln den neuen Status wieder.
3. Um den Dienst anzuhalten, klicken Sie auf **Management Server-Dienst stoppen**.

Weitere Informationen zu den Taskleistensymbolen finden Sie unter Taskleistensymbole für den Servermanager (Erklärung) auf Seite 378.

## Starten oder Stoppen des Recording Server-Dienstes

Das Recording Server Manager-Taskleistensymbol zeigt den Status des Recording Server-Dienstes an, beispielsweise **Läuft**. Durch dieses Symbol können Sie den Recording Server-Dienst starten oder stoppen. Wenn Sie den Recording Server-Dienst stoppen, kann Ihr System nicht mit den Geräten interagieren, die mit dem Server verbunden sind. Dies bedeutet, dass Sie kein aufgezeichnetes oder Live-Video ansehen können.

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das Recording Server Manager-Taskleistensymbol. Ein Kontextmenü erscheint.

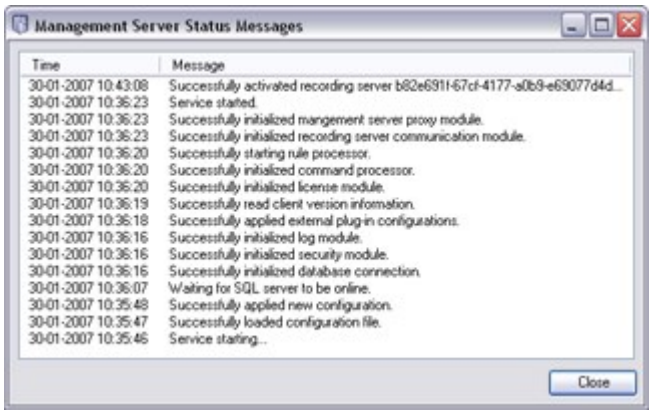



2. Wenn der Dienst angehalten wurde, klicken Sie auf **Recording Server-Dienst starten**, um ihn zu starten. Die Änderungen des Taskleistensymbols spiegeln den neuen Status wieder.
3. Um den Dienst anzuhalten, klicken Sie auf **Recording Server-Dienst stoppen**.

Weitere Informationen zu den Taskleistensymbolen finden Sie unter Taskleistensymbole für den Servermanager (Erklärung) auf Seite 378.

## Statusmeldungen für Management-Server oder Aufzeichnungsserver ansehen

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das relevante Taskleistensymbol. Ein Kontextmenü erscheint.
2. Wählen Sie **Statusmeldungen anzeigen**. Je nach Servertyp wird entweder das Fenster **Management-Server-Statusmeldungen** oder das Fenster **Aufzeichnungsserver-Statusmeldungen** mit Zeitstempel-Statusmeldungen eingeblendet:




## Verschlüsselung verwalten mit dem Server Configurator

Verwenden Sie Server Configurator zum Auswählen von Zertifikaten auf den lokalen Servern für die verschlüsselte Kommunikation und registrieren Sie die Serverdienste, damit sie für die Kommunikation mit den Servern qualifiziert sind.

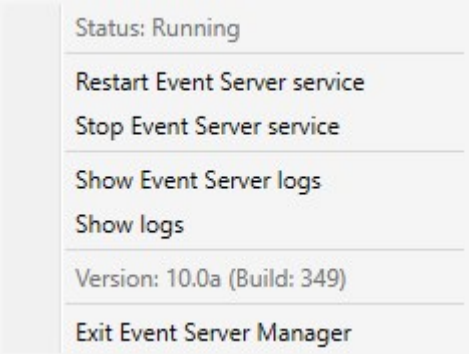
Öffnen Sie Server Configurator entweder vom Windows-Startmenü, vom Taskleistensymbol für den Management-Server oder vom Taskleistensymbol für den Aufzeichnungsserver aus. Siehe Server Configurator (Hilfsprogramm) auf Seite 434.

Weitere Informationen finden Sie im Zertifikate-Leitfaden dazu, wie Sie Ihre XProtect VMS Installationen sichern können.

## Den Event Server Dienst starten, anhalten oder neu starten

Das Event Server Manager-Taskleistensymbol zeigt den Status des Event Server-Dienstes an, beispielsweise **Läuft**. Durch dieses Symbol können Sie den Event Server-Dienst starten, stoppen oder neu starten. Wenn sie den Dienst anhalten funktionieren Teile des Systems nicht mehr, einschließlich Ereignisse und Alarme. Sie können allerdings immer noch Video ansehen und aufzeichnen. Weitere Informationen finden Sie unter Den Event Server-Dienst stoppen auf Seite 383.

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das Event Server Manager-Taskleistensymbol. Ein Kontextmenü erscheint.




2. Wenn der Dienst angehalten wurde, klicken Sie auf **Event Server-Dienst starten**, um ihn zu starten. Die Änderungen des Taskleistensymbols spiegeln den neuen Status wieder.
3. Um den Dienst neu zu starten oder anzuhalten, klicken Sie auf **Event Server-Dienst neu starten** oder **Event Server-Dienst stoppen**.

Weitere Informationen zu den Taskleistensymbolen finden Sie unter Taskleistensymbole für den Servermanager (Erklärung) auf Seite 378.

## Den Event Server-Dienst stoppen

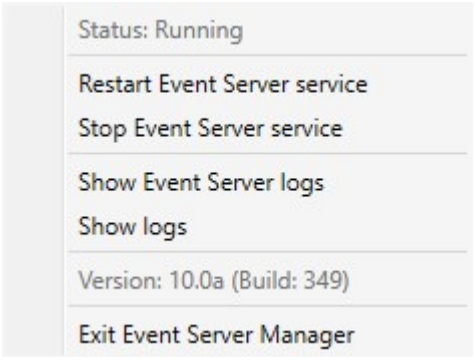
Bei Installation der MIP-Plug-ins auf dem Event-Server müssen Sie zuerst den Event Server-Dienst stoppen und ihn danach neu starten. Viele Bereiche des VMS-Systems funktionieren nicht, solange der Dienst angehalten ist:

- Keinerlei Ereignisse oder Alarme werden auf dem Event-Server gespeichert. System- und Geräteereignisse lösen jedoch immer noch Aktionen, wie das Starten einer Aufzeichnung aus
- XProtect Erweiterungen funktionieren in XProtect Smart Client nicht und können vom Management Client nicht konfiguriert werden.
- Analyseereignisse funktionieren nicht
- Generische Ereignisse funktionieren nicht
- Keinerlei Alarme werden ausgelöst
- In XProtect Smart Client funktionieren Karten-Ansichtselemente, Alarmlisten-Ansichtselemente und der Alarm-Manager-Arbeitsplatz nicht
- MIP Plug-ins im Event-Server können nicht ausgeführt werden
- MIP Plug-ins in Management Client und XProtect Smart Client funktionieren nicht richtig

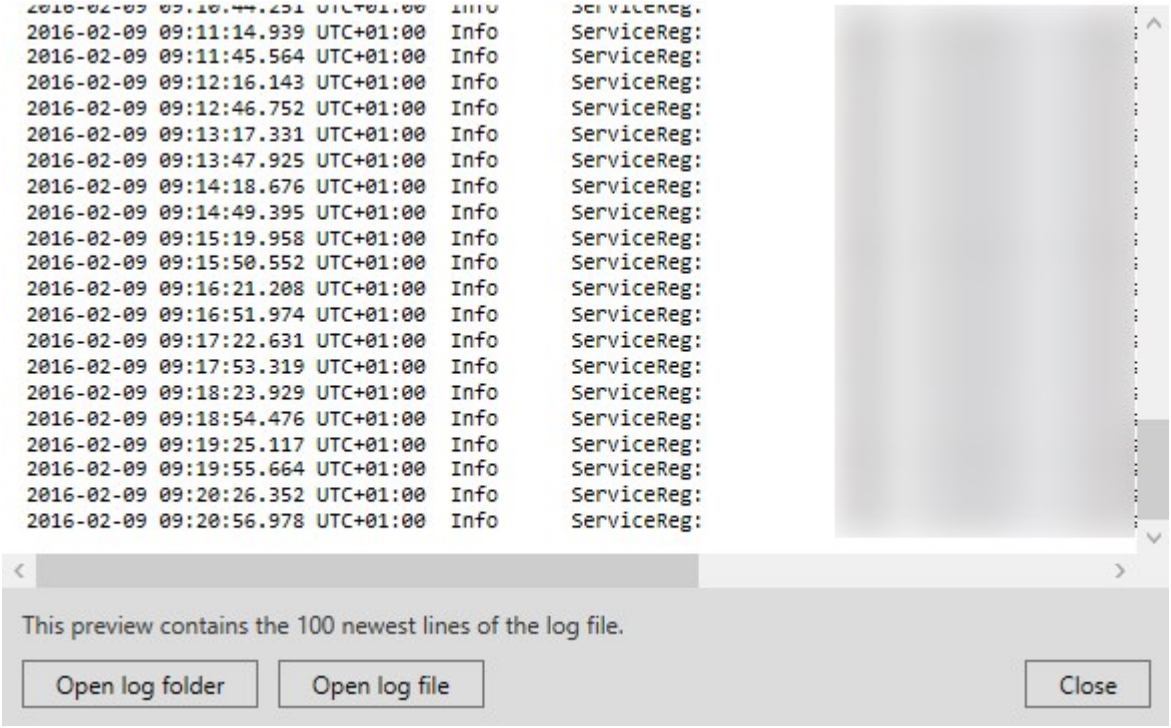
## Event Server oder MIP-Protokolle anzeigen

Sie können Informationen mit Zeitstempel über Event-Server-Aktivitäten im Event-Server-Protokoll ansehen. Informationen über Integrationen von Dritten werden im MIP-Protokoll in einem Unterordner des **Event-Server-**Ordners gespeichert.

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das Event Server Manager-Taskleistensymbol. Ein Kontextmenü erscheint.




2. Klicken Sie zur Ansicht der letzten 100 Zeilen im Event Server-Protokoll auf **Events-Server-Protokolle anzeigen**. Ein Log-Viewer erscheint.




   1. Klicken Sie auf **Protokolldatei öffnen**, um die Protokolldatei anzusehen.
   2. Klicken Sie auf **Protokollordner öffnen**, um den Protokollordner zu öffnen.

3. Zur Ansicht der 100 aktuellsten Zeilen im MIP-Protokoll, gehen Sie zurück in das Kontextmenü und klicken Sie auf **MIP-Protokolle anzeigen**. Ein Log-Viewer wird angezeigt.

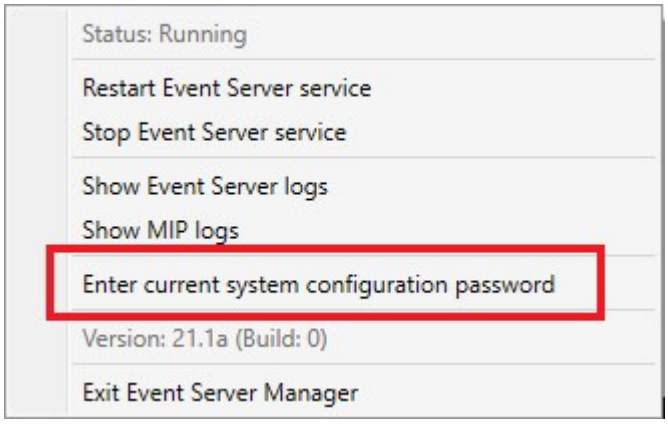
Wenn jemand die Protokolldatei aus dem Protokollverzeichnis entfernt, sind die Menüpunkte ausgegraut. Um die Protokollansicht zu öffnen müssen Sie zunächst die Protokolldatei wieder in ihr Verzeichnis kopieren: `C:\ProgramData\Milestone\XProtect Event Server\logs` oder `C:\ProgramData\Milestone\XProtect Event Server\logs\MIP Logs`.

## Geben Sie das Passwort für die aktuelle Systemkonfiguration ein

Wenn das Passwort für die Systemkonfiguration im Management Server geändert wurde, müssen Sie das aktuelle Passwort für die Systemkonfiguration auch in den Event Server eingeben.

Wenn Sie das aktuelle Passwort nicht in den Event Server eingeben, funktionieren Systemkomponenten wie die Zugangskontrolle nicht mehr.

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das Event Server Manager-Taskleistensymbol. Ein Kontextmenü erscheint.




2. Klicken Sie auf **Aktuelles Passwort für die Systemkonfiguration eingeben**, um das aktuelle Passwort für die Systemkonfiguration einzugeben. Ein Fenster wird angezeigt.
3. Geben Sie das gleiche Passwort für die Systemkonfiguration ein, das auch in den Management Server eingegeben wurde.

# Verwaltung registrierter Dienste

Zeitweise gibt es Server und/oder Dienste, die mit dem System kommunizieren sollten, auch wenn sie nicht direkt Teil des System sind. Einige, aber nicht alle, Dienste können sich automatisch selbst im System registrieren. Dienste, die automatisch registriert werden können:

- Event Server Dienst
- Log Server Dienst

Registrierte Dienste werden automatisch in der Liste registrierter Dienste angezeigt.

Sie können Server/Dienste als registrierte Dienste im Management Client manuell festlegen.

## Registrierte Dienste hinzufügen und bearbeiten

1. Im Fenster **Registrierte Dienste hinzufügen/entfernen**, klicken Sie je nach Bedarf auf **Hinzufügen** oder **Bearbeiten**.
2. Im Fenster **Registrierten Dienst hinzufügen** oder **Registrierten Dienst bearbeiten** (je nach vorheriger Auswahl), können Sie Einstellungen festlegen oder bearbeiten.
3. Klicken Sie auf **OK**.

## Netzwerkkonfiguration verwalten

In den Netzwerkkonfigurationseinstellungen können Sie die LAN- und WAN-Adressen des Management-Servers bestimmen und so eine Kommunikation zwischen Management-Server und vertrauten Servern ermöglichen.

1. Im Fenster **Registrierte Dienste hinzufügen/entfernen**, klicken Sie auf **Netzwerk**.
2. Geben Sie die LAN- und/oder WAN-IP-Adresse des Management-Servers an.

   Wenn alle beteiligten Server (Management-Server und vertraute Server) sich in Ihrem lokalen Netzwerk befinden, können Sie einfach die LAN-Adresse angeben. Wenn ein oder mehrere beteiligte Server über eine Internetverbindung auf das System zugreifen, müssen Sie außerdem die WAN-Adresse angeben.


3. Klicken Sie auf **OK**.

## Eigenschaften registrierter Dienste

Im Fenster **Registrierten Dienst hinzufügen** oder **Registrierten Dienst bearbeiten**, legen Sie folgendes fest:

| Komponente | Voraussetzung |
|---|---|
| **Typ** | Vorgefülltes Feld. |
| **Name** | Name des registrierten Dienstes. Der Name wird nur zu Anzeigezwecken im Management Client verwendet. |
| **URLs** | Klicken Sie auf **Hinzufügen**, um die IP-Adresse oder den Hostnamen des registrierten Dienstes hinzuzufügen. Wenn ein Hostname als Teil einer URL angegeben wird, muss der Host vorhanden und auf dem Netzwerk verfügbar sein. URLs müssen mit *http://* oder *https://* anfangen und dürfen folgende Zeichen nicht enthalten: < > *&* *'* *"* *** *?* *\|* *[* *]* *"*.<br><br>**Beispiel** für ein typisches URL-Format: *http://ipaddress:port/directory* (wobei Port und Verzeichnis optional sind). Sie können bei Bedarf mehr als eine URL hinzufügen. |
| **Vertrauenswürdig** | Wählen Sie diese Option aus, wenn der registrierte Dienst absolut vertrauenswürdig ist (dies ist oft der Fall, doch die Option bietet Ihnen die Flexibilität, den registrierten Dienst hinzuzufügen und ihn dann als vertrauenswürdig zu markieren, indem Sie ihn später bearbeiten).<br><br>Durch das Ändern des Status der Vertrauenswürdigkeit wird auch der Status anderer registrierter Dienste geändert, die eine oder mehrere URLs mit dem relevanten registrierten Dienst gemeinsam haben. |
| **Beschreibung** | Beschreibung des registrierten Dienstes. Die Beschreibung wird nur zu Anzeigezwecken im Management Client verwendet. |
| **Erweitert** | Ein „erweiterter“ Dienst verfügt er über besondere URI-Schemata (z. B. HTTP, HTTPS, TCP oder UDP), die für jede Host-Adresse, die Sie definieren, eingerichtet werden müssen. Daher hat eine Hostadresse mehrere Endpunkte, die jeweils über ein eigenes Schema, eine eigene Hostadresse und einen eigenen IP-Port für dieses Schema verfügen. |

## Entfernen von Gerätetreibern (Erklärung)

Wenn Sie die Gerätetreiber nicht länger auf Ihrem Computer benötigen, können Sie die Treiberpakete aus Ihrem System löschen. Dafür folgen Sie einfach der normalen Prozedur unter Windows zur Deinstallation von Programmen.

Sollten Sie mehrere Treiberpakete installiert haben und Probleme beim Löschen dieser Dateien haben, können Sie das Skript im Installationsordner des Treiberpakets verwenden, um diese vollständig zu löschen.

Bei Entfernen von Gerätetreibern ist die Kommunikation zwischen Aufzeichnungsserver und Kameras nicht länger möglich. Entfernen Sie deshalb Treiberpakete nicht wenn Sie aktualisieren, sondern installieren Sie die neue Version über die Alte. Das können Sie nur entfernen, wenn Sie das gesamte System deinstallieren.

## Deinstallieren eines Aufzeichnungsservers

> ⚠ Wenn Sie einen Aufzeichnungsserver deinstallieren, werden alle im Management Client festgelegten Konfigurationen für diesen Aufzeichnungsserver entfernt, inklusive der **gesamten** mit dem Aufzeichnungsserver assoziierten Hardware (Kameras, Eingabegeräte usw.).

1. Klicken Sie mit der rechten Maustaste im Bereich **Übersicht** auf den Aufzeichnungsserver, den Sie deinstallieren möchten.
2. Wählen Sie **Aufzeichnungsserver deinstallieren**.
3. Wenn Sie sich sicher sind, klicken Sie auf **Ja**.
4. Der Aufzeichnungsserver und die gesamte zugehörige Hardware werden deinstalliert.

## Löschen sämtlicher Hardware auf einem Aufzeichnungsserver

> ⚠ Wenn Sie Hardware löschen, werden alle durch diese Hardware aufgezeichneten Daten dauerhaft gelöscht.

1. Klicken Sie mit der rechten Maustaste auf den Aufzeichnungsserver, von dem Sie sämtliche Hardware löschen möchten.
2. Wählen Sie **Sämtliche Hardware löschen**.
3. Bestätigen Sie die Löschung.

## Ändern des Hostnamens des Management-Server-Computers

Wenn der Management Server mit seinem voll qualifizierten Domänennamen (FQDN) oder seinem Hostnamen adressiert wird, hat eine Änderung des Hostnamens des Computers Auswirkungen innerhalb von XProtect, die zu berücksichtigen und zu behandeln sind.

> ⚠ Im Allgemeinen ist eine Änderung des Hostnamens eines Management-Servers aufgrund der hinterher ggf. erforderlichen Bereinigungsmaßnahmen sorgfältig zu planen.

In den folgenden Abschnitten erhalten Sie einen Überblick über einige der Auswirkungen, wenn der Hostname geändert wird.

## Die Gültigkeit der Zertifikate

Zertifikate werden zum Verschlüsseln der Kommunikation zwischen den Diensten verwendet, und die Zertifikate werden auf allen Computern installiert, auf denen einer oder mehrere der XProtect-Dienste läuft.

Je nachdem, wie die Zertifikate erstellt werden, können sich diese auf den Computer beziehen, auf dem sie installiert sind, und sie sind nur so lange gültig, wie der Computername unverändert bleibt.

Weitere Angaben dazu, wie Zertifikate erstellt werden, finden Sie unter Einführung zu Zertifikaten.

Wenn der Name eines Computers geändert wird, können die verwendeten Zertifikate ungültig werden, und der XProtect VMS kann nicht gestartet werden. Um das System wieder lauffähig zu machen, führen Sie die folgenden Schritte aus:

- Erstellen Sie neue Zertifikate und installieren Sie sie erneut auf allen Computern in der Umgebung.
- Wenden Sie die neuen Zertifikate mithilfe von Server Configurator auf jedem der Computer an, damit die Verschlüsselung mit den neuen Zertifikaten erfolgt.

Hierdurch wird die Registrierung der neuen Zertifikate ausgelöst, und das System ist wieder einsatzfähig.

## Verlust der Eigenschaften von Kundendaten für registrierte Dienste

Wenn Sie eine Registrierung mithilfe des Server Configurator abschließen, z.B. nach einer Adressänderung des Management Servers, werden alle geänderten Angaben für die registrierten Dienste überschrieben. Wenn Sie also Informationen für die registrierten Dienste geändert haben, müssen diese Änderungen für alle Dienste erneut angewendet werden, die beim Management-Server auf dem Computer mit dem geänderten Namen registriert sind.

Die Angaben, die für registrierte Dienste bearbeitet werden können, befinden sich unter **Extras** > **Registrierte Dienste** > **Bearbeiten**:

- Vertrauenswürdig
- Erweitert
- Externe Markierung
- Manuell hinzugefügte URL

## In Milestone Customer Dashboard erscheint der Host unverändert

Milestone Customer Dashboard ist ein kostenloses Online-Tool, mit dem Milestone Partner, Vertriebspartner und XProtect VMS-Nutzer Milestone Software-Installationen und Lizenzen verwalten und überwachen können.

Ändert sich der Name des Managements Servers in einem System, das mit Milestone Customer Dashboard verbunden ist, so wird diese Änderung nicht automatisch in Milestone Customer Dashboard berücksichtigt.

Der alte Hostname erscheint solange in Milestone Customer Dashboard, bis eine neue Lizenzaktivierung abgeschlossen ist. Die Namensänderung führt jedoch zu keinerlei Beschädigungen in Milestone Customer Dashboard, und sobald eine neue Aktivierung erfolgt, wird der Datensatz in der Datenbank mit dem neuen Hostnamen aktualisiert. Weitere Informationen zu Milestone Customer Dashboard finden Sie unter Milestone Customer Dashboard (Erklärung).

## Wenn sich der Hostname ändert, kann dies dazu führen, dass sich die SQL Server-Addresse ändert

Wenn sich auf demselben Computer wie der Management Server SQL Server befindet und sich der Name dieses Computers ändert, ändert sich auch die Adresse von SQL Server. Das heißt, dass die SQL Server Adresse für Komponenten aktualisiert werden muss, die sich auf verschiedenen Computern befinden, sowie für Komponenten auf dem lokalen Computer, die den Computernamen verwenden, und nicht den Localhost, um eine Verbindung zu SQL Server herzustellen. Dies gilt insbesondere für den Event Server, der dieselbe Datenbank verwendet wie der Management Server. Es könnte auch für den Log Server gelten, der eine andere Datenbank verwendet, aber mit großer Wahrscheinlichkeit auf demselben SQL Server.

Siehe Ändern des Speicherorts und des Namens einer SQL Server Datenbank auf Seite 376.

## Der Hostname ändert sich in einen Milestone Federated Architecture

Änderungen am Namen eines Computers, der sich innerhalb einer Milestone Federated Architecture-Einrichtung befindet, haben die folgenden Auswirkungen, und dies gilt sowohl wenn Standorte innerhalb von Arbeitsgruppen verbunden sind als auch über Domänen hinweg.

### Der Host des Standortes ist der Rootknoten in der Architektur

Wenn Sie den Namen des Computers ändern, auf dem die zentrale Seite innerhalb der Architektur läuft, werden alle davon abhängigen Knoten automatisch mit den neuen Adressen verbunden. In diesem Fall sind bei einer Umbenennung also keine Maßnahmen erforderlich.

### Der Host der Seite ist der Kind-knoten in der Architektur

Um Verbindungsprobleme beim Ändern des Namens eines Computers zu vermeiden, auf dem eine oder mehrere föderierte Seiten laufen, müssen Sie zu der betroffenen Seite eine alternative Adresse hinzufügen, bevor der Computer umbenannt wird. Die betroffene Seite ist der Knoten, dessen Hostcomputer umbenannt wird. Weitere Informationen zu Verbindungsproblemen aufgrund unvorbereiteter oder unvorhergesehener Änderungen des Hostnamens, und wie solche Probleme gelöst werden können, finden Sie unter Problem: Eine Elternknoten in einer Milestone Federated Architecture-Einrichtung kann keine Verbindung zu einem Kindknoten herstellen.

Die alternative Adresse muss im Bereich **Eigenschaften** entweder im Bereich **Standortnavigation** oder **Föderierte Standorthierarchie** hinzugefügt werden. Die folgenden Voraussetzungen müssen hierfür erfüllt sein:

- Die alternative Adresse muss hinzugefügt werden, damit sie verfügbar ist, bevor der Hostcomputer umbenannt wird
- Die alternative Adresse muss den zukünftigen Namen des Hostcomputers wiedergeben (wenn dieser umbenannt wurde)

Weitere Informationen dazu, wie Sie in den Bereich **Eigenschaften** gelangen, finden Sie unter Standorteigenschaften festlegen.

> Damit die Aktualisierung möglichst glatt verläuft, stoppen Sie den Management Client auf dem Knoten, der als Elternknoten dient, zu demjenigen, dessen Hostname sich ändert. Ansonsten stoppen Sie den Client und starten Sie ihn neu, nachdem der Computer umbenannt wurde. Weitere Informationen finden Sie unter Starten oder stoppen des Management Server Dienstes.

> Vergewissern Sie sich außerdem, dass die von Ihnen angegebene alternative Adresse im Bereich **Föderierte Standorthierarchie** an Ihrem zentralen Standort erscheint, und wenn nicht, stoppen Sie den Management Client und starten Sie ihn neu.

Sobald der Host umbenannt wurde und Sie den Computer neu gestartet haben, schalten die föderierten Standorte automatisch auf die neue Adresse um.

# Verwaltung von Serverprotokollen

Folgende Arten von Serverprotokollen gibt es:

- Systemprotokoll
- Auditprotokoll
- Von Regeln ausgelöste Protokolle

Sie dienen zur Protokollierung der Systemauslastung. Diese Protokolle stehen in Management Client unter **Server-Protokolle** zur Verfügung.

Informationen zu den für die Fehlersuche und zur Untersuchung von Softwarefehlern verwendeten Protokollen finden Sie unter Debug-Protokolle (Erklärung) auf Seite 396.

## Benutzeraktivitäten, Ereignisse, Maßnahmen und Fehler erkennen

Mithilfe der Protokolle können Sie detaillierte Aufzeichnungen der Benutzeraktivitäten, Ereignisse, Maßnahmen und Fehler im System erhalten.

Um Protokolle im Management Client zu sehen, gehen Sie zum Bereich **Standortnavigation** und wählen Sie **Serverprotokolle** aus.

| Protokolltyp | Was wird protokolliert? |
|---|---|
| **Systemprotokolle** | Systembezogene Informationen |
| **Auditprotokolle** | Benutzeraktivitäten |
| **Von Regel ausgelöste Protokolle** | Regeln, in denen Benutzer die Aktion **Neuen <Protokolleintrag> erstellen** bestimmt haben. Weitere Informationen zu der Aktion <log entry> finden Sie unter Aktionen und Stoppaktionen. |

Wenn Sie die Protokolle in einer anderen Sprache angezeigt bekommen möchten, finden Sie diese unter Registerkarte „Allgemein“ (Optionen) auf Seite 413 unter **Optionen**.

Um Protokolle als Dateien aus kommagetrennten Werten (.csv) zu exportieren, siehe Protokollexport.

Angaben dazu, wie Sie die Einstellungen für die Protokolle ändern können, finden Sie unter Registerkarte „Serverprotokolle“ (Optionen) auf Seite 416.

## Protokolle filtern

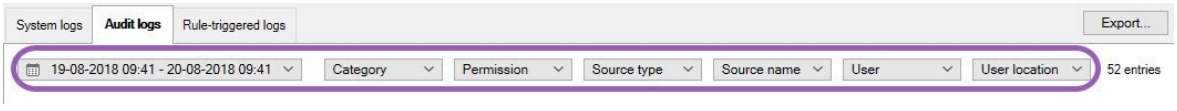
In jedem Protokollfenster können Sie Filter anwenden, um z.B. Protokolleinträge aus einer bestimmten Zeitspanne, für ein bestimmtes Gerät oder für einen bestimmten Benutzer zu sehen.

> Die Filter werden anhand der Protokolleinträge erzeugt, die in der Benutzeroberfläche aktuell sichtbar sind.

1. Wählen Sie aus dem Bereich **Standortnavigation** die **Serverprotokolle**. Standardmäßig erscheint die Registerkarte **Systemprotokolle**.

   Um zwischen Protokolltypen zu navigieren, wählen Sie eine andere Registerkarte aus.

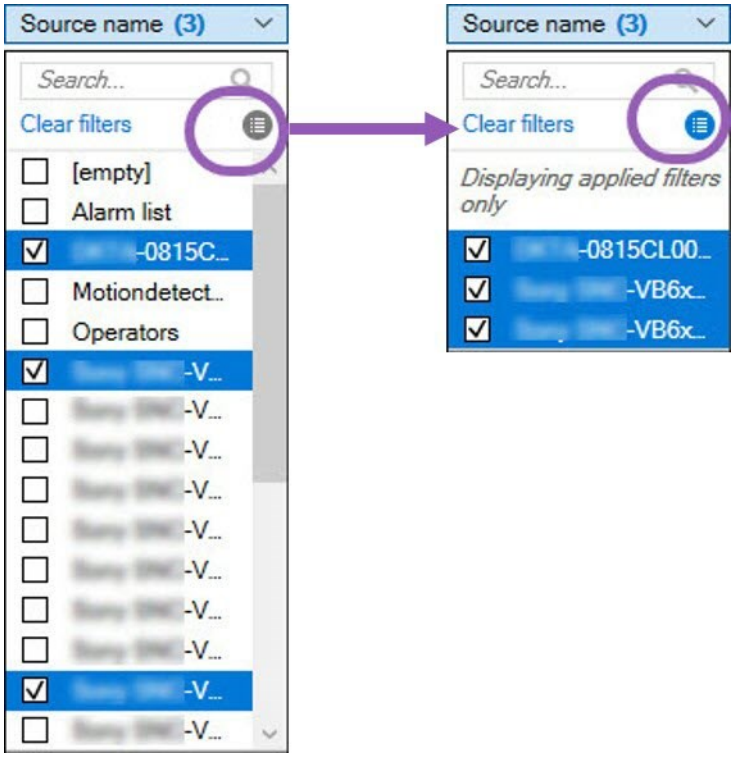
2. Unter den Registerkarten, wählen Sie eine Filtergruppe, zum Beispiel, **Kategorie**, **Quelltyp**, oder **Benutzer** aus.




   Es erscheint eine Liste der Filter. Eine Aufstellung der Filter zeigt maximal 1000 Filter.

3. Wählen Sie einen Filter, um ihn anzuwenden. Wählen Sie den Filter erneut, um ihn zu entfernen.

   Optional: In einer Liste von Filtern, wählen Sie **Nur angewandte Filter anzeigen**, um nur die angewendeten Filter anzuzeigen.



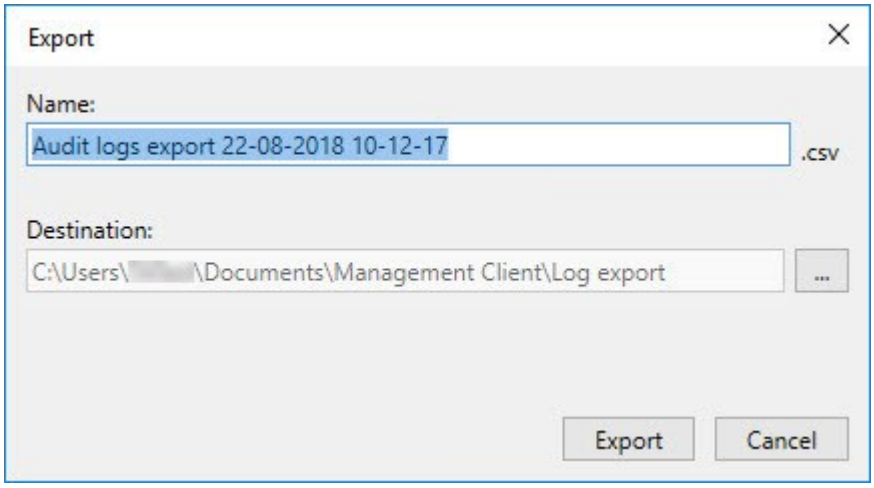

Wenn Sie Protokolle exportieren, ändert sich der Inhalt Ihres Exports je nachdem, welche Filter Sie anwenden. Für Informationen über Ihren Export, siehe Exportprotokolle.

## Protokolle exportieren

Das Exportieren von Protokollen hilft Ihnen, zum Beispiel, Protokolleinträge über den Aufbewahrungszeitraum für Protokolle hinaus zu speichern. Sie können Protokolle als Dateien aus kommagetrennten Werten (.csv) exportieren.

Wie man ein Protokoll exportiert:

1. Wählen Sie **Export** in der oberen rechten Ecke. Das Fenster **Exportieren** wird geöffnet.




2. Im Fenster **Export** des Felds **Name** können Sie einen Namen für die Protokolldatei bestimmen.
3. Standardmäßig werden Protokolldateien im Ordner **Protokollexport** gespeichert. Um einen anderen Standort zu bestimmen, wählen Sie ... rechts vom Feld **Ziel** aus.
4. Wählen Sie **Export** zum Exportieren des Protokolls.

Der Inhalt von Ihr Export ändert sich, je nachdem welche Filter Sie anwenden. Für Informationen über Ihren Export, siehe Filterprotokolle.

## Protokolle durchsuchen

Um ein Protokoll zu durchsuchen, verwenden Sie die **Suchkriterien** oben im Protokollbereich:

1. Geben Sie Ihre Suchkriterien anhand der Liste an.
2. Klicken Sie auf **Aktualisieren**, damit die Protokollseite Ihren Suchkriterien entspricht. Um Ihre Suchkriterien zu löschen und zur Anzeige des gesamten Protokollinhalts zurückzukehren, klicken Sie auf **Löschen**.

Sie können auf eine beliebige Zeile doppelt klicken, um sich alle dargestellten Einzelheiten in einem Fenster mit den **Protokolldetails** anzeigen zu lassen. So können Sie auch Protokolleinträge lesen, die mehr Text enthalten als in einer Zeile angezeigt werden kann.

## Protokollsprache ändern

1. Wählen Sie im unteren Teil des Protokollbereichs, auf der Liste **Anmeldung anzeigen** die gewünschte Sprache aus.

2. Das Protokoll wird nun in der ausgewählten Sprache angezeigt. Wenn Sie das Protokoll das nächste Mal öffnen, erscheint es wieder in der Standardsprache.

## 2018 R2 und früheren Komponenten erlauben, Protokolle aufzuzeichnen

Die 2018 R3 Version des Log-Servers führt eine Authentifizierung für zusätzliche Sicherheit ein. Dies verhindert, dass 2018 R2 und frührere Komponenten Protokolle auf den Log-Server schreiben.

Betroffene Komponenten:

- XProtect Smart Client
- XProtect LPR Plug-In
- LPR Server
- Zutrittskontroll-Plug-in
- Ereignisserver
- Alarm Plug-in

Wenn Sie 2018 R2 oder eine frühere Version einer der oben aufgeführten Komponenten einsetzen, müssen Sie entscheiden, ob die Komponente Protokolle auf dem neuen Log-Server anlegen darf:

1. Wählen Sie **Tools** > **Optionen**.
2. Im Dialogfeld **Optionen** am unteren Rand der Registerkarte **Serverprotokoll**, suchen Sie das Kontrollkästchen **2018 R2 und früheren Komponenten erlauben, Protokolle zu schreiben**.
    - Wählen Sie das Kontrollkästchen, das es 2018 R2 und früheren Komponenten erlaubt, Protokolle aufzuzeichnen
    - Leeren Sie das Kontrollkästchen, um es 2018 R2 und früheren Komponenten zu verbieten, Protokolle aufzuzeichnen

# Fehlerbehandlung

## Debug-Protokolle (Erklärung)

Debug-Protokolle dienen dazu, Defekte und Fehler im System zu erkennen.

Weitere Informationen zu den für die Systemauslastung verwendeten Protokolle finden Sie unter Verwaltung von Serverprotokollen auf Seite 391.

Die Protokolldateien zur Installation finden Sie unter XProtect:

- `C:\ProgramData\Milestone\IDP\Logs`

  > Hierauf können nur IIS-Benutzer und Administratoren zugreifen. Wenn sich der IIS-Benutzer ändert, müssen diese Berechtigungen aktualisiert werden.

- `C:\ProgramData\Milestone\MIPSDK`
- `C:\ProgramData\Milestone\XProtect Data Collector Server\Logs`
- `C:\ProgramData\Milestone\XProtect Event Server\Logs`
- `C:\ProgramData\Milestone\XProtect Log Server`
- `C:\ProgramData\Milestone\XProtect Management Server\Logs`
- `C:\ProgramData\Milestone\XProtect Mobile Server\Logs`
- `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
- `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`

## Problem: Änderungen von SQL Server und Datenbankspeicherorten verhindern den Zugriff auf die Datenbanken

Werden der Speicherort von SQL Server und die VMS-Datenbanken geändert, z.B. durch die Änderung des Hostnamens des Computers, auf dem SQL Server läuft, so verliert der Aufzeichnungsserver den Zugriff auf die Datenbank.

Lösung: Ändern Sie die Verbindungszeichenfolgen, um die Änderung von SQL Server und der Datenbank widerzuspiegeln. Siehe Ändern des Speicherorts und des Namens einer SQL Server Datenbank auf Seite 376.

## Problem: Aufzeichnungsserver läuft aufgrund eines Portkonflikts nicht an

Zu diesem Problem kann nur dann kommen, wenn der Dienst Simple Mail Transfer Protocol (SMTP) läuft, da dieser den Port 25 verwendet. Ist der Port 25 bereits in Gebrauch, so kann der Dienst Recording Server evtl. nicht gestartet werden. Es ist wichtig, dass Portnummer 25 für den SMTP-Dienst des Aufzeichnungsservers zur

Verfügung steht.

**SMTP-Dienst: Überprüfung und Lösungen**

Zur Überprüfung, ob der SMTP-Dienst installiert wurde:

1. Wählen Sie aus dem Windows **Start**-Menü **Systemsteuerung** aus.
2. Klicken Sie in der **Systemsteuerung** doppelt auf **Programme hinzufügen oder entfernen**.
3. Klicken Sie links in dem Fenster **Programme hinzufügen oder entfernen** auf **Windowskomponenten hinzufügen/entfernen**.
4. Wählen Sie in dem Assistenten **Windowskomponenten Internet Information Services (IIS)** aus und klicken Sie auf **Details**.
5. Überprüfen Sie in dem Fenster **Internet Information Services (IIS)** ob das Kontrollkästchen **SMTP-Dienst** ausgewählt ist. Wenn ja, so ist der SMTP-Dienst installiert.

Wenn der SMTP-Dienst installiert ist, wählen Sie eine der folgenden Lösungen:

**Lösung 1: Deaktivieren des SMTP-Dienstes oder Festlegen auf manuelles Starten**

Mit dieser Lösung können Sie den Aufzeichnungsserver starten, ohne jedes Mal den SMTP-Dienst anhalten zu müssen:

1. Wählen Sie aus dem Windows **Start**-Menü **Systemsteuerung** aus.
2. Klicken Sie in der **Systemsteuerung** doppelt auf **Administrative Werkzeuge**.
3. Klicken Sie in **Administrative Werkzeuge** doppelt auf **Dienste**.
4. Klicken Sie in den **Diensten** doppelt auf **Simple Mail Transfer Protocol (SMTP)**.
5. Klicken Sie in dem Fenster **Eigenschaften von SMTP** auf **Anhalten**, und stellen Sie dann den **Starttyp** entweder auf **Manuell** oder auf **deaktiviert**.

   Wenn der SMTP-Dienst auf **Manuell** steht, kann er von dem Fenster **Dienste** aus manuell gesteuert werden, oder von einer Eingabeaufforderung aus mithilfe des Befehls *net start SMTPSVC*.
6. Klicken Sie auf **OK**.

**Lösung 2: Entfernen des SMTP-Dienstes**

Das Entfernen des SMTP-Dienstes kann Auswirkungen auf andere Anwendungen haben, die den SMTP-Dienst nutzen.

1. Wählen Sie aus dem Windows **Start**-Menü **Systemsteuerung** aus.
2. Klicken Sie in der **Systemsteuerung** doppelt auf **Programme hinzufügen oder entfernen**.
3. Klicken Sie links in dem Fenster **Programme hinzufügen oder entfernen** auf **Windowskomponenten hinzufügen/entfernen**.
4. Wählen Sie in dem Assistenten **Windowskomponenten Internet Information Services (IIS)** aus und klicken Sie auf **Details**.
5. Deaktivieren Sie in dem Fenster **Internet Information Services (IIS)** das Kontrollkästchen **SMTP-Dienst**.
6. Klicken Sie auf **OK**, **Weiter**, und **Fertigstellen**.

## Problem: Recording Server geht beim Umschalten auf Management Server Clusterknoten offline

Wenn Sie einen Microsoft-Cluster für Management Server-Redundanz einrichten, so können die Recording Server oder Recording Servers beim Umschalten von Management Server zwischen den Clusterknoten offline gehen.

Um dies zu korrigieren tun Sie folgendes:

> Wenn Sie Konfigurationsänderungen vornehmen, halten Sie auf dem Microsoft Failover Cluster Manager die Steuerung und Überwachung des Dienstes an, damit der Server Configurator die Änderungen vornehmen kann, und starten bzw. stoppen Sie den Management Server Dienst. Wenn Sie den Startyp des Failover Cluster Service auf "Manuell" ändern, sollte dies nicht zu Konflikten mit dem Server Configurator führen.

Auf den Management Server Computern:

1. Starten Sie den Server Configurator auf jedem der Computer, auf denen ein Managementserver installiert ist.
2. Gehen Sie auf die Seite **Registrierung**.
3. Klicken Sie auf das Bleistiftsymbol (  ), damit Sie die Adresse des Management Servers bearbeiten können.
4. Ändern Sie die Adresse des Managements Servers in die URL des Clusters, z.B. `http://MyCluster`.
5. Klicken Sie auf **Registrieren**.

Auf Computern mit Komponenten, die den Management Server verwenden (z.B. Recording Server, Mobile Server, Event Server, , API Gateway):

1. Starten Sie den Server Configurator auf jedem der Computer.
2. Gehen Sie auf die Seite **Registrierung**.
3. Ändern Sie die Adresse des Managements Servers in die URL des Clusters, z.B. `http://MyCluster`.
4. Klicken Sie auf **Registrieren**.

## Problem: Ein Elternknoten in einer Milestone Federated Architecture-Einrichtung kann keine Verbindung zu einem Kindknoten herstellen

Wenn Sie den Hostcomputer eines Standortes umbenannt haben, der als Kindknoten in einer Milestone Federated Architecture fungiert, kann kein Elternknoten eine Verbindung dazu herstellen.

### Zur Wiederherstellung der Verbindung zwischen Eltern-Knoten und der Seite

- Trennen Sie die betroffene Seite von ihrer Elternseite. Weitere Informationen finden Sie unter Eine Seite von der Hierarchie trennen.
- Stellen Sie die Verbindung der Seite mithilfe des neuen Namens ihres Hosts wieder her. Weitere Informationen finden Sie unter Standort der Hierarchie hinzufügen.

Um sich zu vergewissern, dass die Änderungen auch wirksam sind, können Sie den Management Client an dem Knoten anhalten und neu starten, der als Elternknoten für denjenigen dient, dessen Hostname geändert wurde. Weitere Informationen finden Sie unter Starten oder stoppen des Dienstes Management Server.

Weitere Informationen zu den Auswirkungen einer Namensänderung eines Hosts in einer Milestone Federated Architecture Einrichtung finden Sie unter Änderungen des Hostnamens in einer Milestone Federated Architecture.

## Problem: Azure SQL-Datenbankdienst nicht verfügbar

Wenn Sie Azure SQL Database verwenden und während der Installation oder des normalen Betriebs ein Verbindungsproblem auftritt, könnte der Grund dafür sein, dass der SQL-Datenbankdienst vorübergehend nicht verfügbar ist.

Azure SQL Database ist ein Dienst, bei dem der Großteil der herkömmlichen Datenbankwartung von Microsoft übernommen wird. Der Dienst kann für einen kurzen Zeitraum nicht verfügbar sein und wurde entwickelt, um sich bis zu einem gewissen Ausmaß ohne Interaktion des Benutzers selbst wiederherzustellen.

Datenbankfehler werden in den XProtect VMS-Protokolldateien mit einer entsprechenden Vorfall-ID vermerkt, die dem Support von Microsoft bereitgestellt werden kann, falls Azure SQL Database über einen längeren Zeitraum nicht verfügbar ist.

Weitere Informationen finden Sie unter Problembehandlung häufiger Verbindungsprobleme mit der Azure SQL-Datenbank.

# Upgrade

## Upgrade (Erklärung)

Wenn Sie ein Upgrade durchführen, werden alle gegenwärtig auf dem Computer installierten Komponenten mit aktualisiert. Während eines Upgrades ist es nicht möglich, installierte Komponenten zu entfernen. Wenn Sie installierte Komponenten entfernen möchten, verwenden Sie hierfür vor oder nach einem Upgrade die Windows-Funktion **Programme hinzufügen und entfernen**. Bei einem Upgrade werden alle Komponenten, mit Ausnahme der Management-Server-Datenbank, automatisch deinstalliert und ersetzt. Dies schließt die Treiber des Treiberpakets ein.

Die Management-Server-Datenbank enthält alle Systemkonfigurationen (Aufzeichnungsserver-Konfigurationen, Kamerakonfigurationen, Regeln usw.). So lange Sie die Management-Server-Datenbank nicht deinstallieren, müssen Sie Ihre Systemkonfiguration nicht neu konfigurieren, auch wenn Sie vermutlich einige der neuen Funktionen in der neuen Version konfigurieren wollen.

Die Abwärtskompatibilität mit Aufzeichnungsservern von Versionen von XProtect vor der derzeitgen Version ist begrenzt. Auf solchen älteren Aufzeichnungsservern können Sie trotzdem Aufnahmen abrufen, um jedoch ihre Konfiguration zu ändern, müssen sie von derselben Version sein, wie die aktuelle. Milestone empfiehlt ein Upgrade aller Aufzeichnungsserver in Ihrem System.

Wenn Sie ein Upgrade durchführen, das auch Ihre Aufzeichnungsserver umfasst, werden Sie gefragt, ob Sie die Video-Gerätetreiber aktualisieren oder beibehalten wollen. Wenn Sie eine Aktualisierung durchführen, kann es nach dem Neustart Ihres Systems einige Minuten dauern, bis Ihre Geräte den Kontakt zu den neuen Video-Gerätetreibern hergestellt haben. Der Grund dafür sind eine Vielzahl interner Kontrollen der neu installierten Treiber.

Wenn Sie von der Version 2017 R3 oder früher auf die Version 2018 R1 oder später erweitern, und Ihr System über ältere Kameras verfügt, müssen Sie das Gerätepaket mit den Alttreibern manuell von unserer Download-Website (https://www.milestonesys.com/downloads/) herunterladen. Für Angaben darüber, ob Ihre Kameras Treiber aus dem Altgerätepaket verwenden, besuchen Sie diese Seite auf unserer Website (https://www.milestonesys.com/community/business-partner-tools/device-packs/).

Wenn Sie von Version 2018 R1 oder früher auf Version 2018 R2 oder höher aktualisieren, ist es wichtig, dass Sie vor dem Upgrade alle Aufzeichnungsserver in Ihrem System mit einem Sicherheitspatch aktualisieren. Eine Aktualisierung ohne den Sicherheitspatch führt dazu, dass die Aufzeichnungsserver versagen.

Die Anleitung zum Installieren des Sicherheitspatches auf Ihren Aufzeichnungsservern finden Sie auf unserer Website https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/.

Wenn Sie die Verbindung zwischen dem Management Server und den Aufzeichnungsserver verschlüsseln möchten, müssen alle Aufzeichnungsserver mindestens auf 2019 R2 erweitert werden.

Eine Übersicht über die empfohlene Upgrade-Sequenz finden Sie unter Optimale Vorgehensweise beim Upgrade auf Seite 405

## Upgrade-Anforderungen

- Halten Sie Ihre Softwarelizenzdatei (siehe Lizenzen (Erklärung) auf Seite 122) (.lic) bereit:
  - **Service-Pack Upgrade**: Der Assistent könnte Sie während der Installation des Management-Servers zur Spezifikation des Standortes Ihrer Software-Lizenzdatei auffordern. Sie können sowohl die Software-Lizenzdatei verwenden, die Sie nach dem Kauf Ihres Systems bekommen haben (oder neuestem Upgrade) als auch die aktivierte Software-Lizenzdatei, die Sie nach Ihrer letzten Lizenzaktivierung erhalten haben
  - **Versionsupgrade**: Nach dem Kauf der neuen Version, erhalten Sie eine neue Software-Lizenzdatei. Der Assistent fordert Sie während der Installation des Management-Servers zur Spezifikation des Standortes Ihrer neuen Software-Lizenzdatei auf

  Das System überprüft Ihre Software-Lizenzdatei, bevor Sie fortfahren können. Bereits hinzugefügte und andere Geräte, die eine Lizenz benötigen, beginnen dann eine Probeversion. Wenn Sie die automatische Lizenzaktivierung nicht eingeschaltet haben (siehe Automatische Lizenzaktivierung aktivieren auf Seite 129), denken Sie bitte daran, Ihre Lizenzen von Hand zu aktivieren, bevor die Kulanzfrist endet. Sollten Sie keine Software-Lizenzdatei besitzen, kontaktieren Sie bitte Ihren XProtect-Reseller.
- Halten Sie Ihre **neue Produktversion** der Software bereit. Sie können sie von der Downloadseite auf der Website Milestone herunterladen.

- Achten Sie darauf, dass Sie die Systemkonfiguration gesichert haben (siehe Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung) auf Seite 356)

  Der Management-Server speichert die Systemkonfiguration in einer SQL Server-Datenbank. Die SQL Server-Datenbank kann sich in einer SQL Server-Instanz auf dem Computer mit dem Management-Server selbst oder in einer SQL Server-Instanz im Netzwerk befinden.

  Wenn Sie eine SQL Server-Datenbank in einer SQL Server-Instanz in Ihrem Netzwerk verwenden, muss der Management-Server auf der SQL Server-Instanz über Administratorrechte verfügen, wenn Sie die SQL Server-Datenbank erstellen, verschieben oder erweitern wollen. Für die regelmäßige Verwendung und für die Wartung der SQL Server-Datenbank muss der Management-Server lediglich der Besitzer einer Datenbank sein.

- Falls Sie vorhaben, die Verschlüsselung während der Installation zu aktivieren, müssen Sie die entsprechenden Zertifikate auf allen entsprechenden Computern installieren, und diese müssen ihm vertrauen. Weitere Informationen finden Sie unter Sichere Kommunikation (Erklärung) auf Seite 155.

Wenn Sie bereit sind, mit der Erweiterung zu beginnen, folgen Sie den in Optimale Vorgehensweise beim Upgrade auf Seite 405 angegebenen Verfahren.

## Aktualisieren Sie XProtect VMS damit Ihr System im FIPS 140-2-konformen Modus läuft

Ab der Version 2020 R3 ist XProtect VMS so konfiguriert, dass er im Betrieb ausschließlich die FIPS 140-2-zertifizierten Algorithmusinstanzen verwendet.

Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

Für FIPS 140-2-konforme Systeme mit Exporten und archivierten Mediendatenbanken von XProtect VMS Versionen vor 2017 R1, die mit nicht FIPS-konformen Ziffern verschlüsselt sind, ist es erforderlich, die Daten an einem Ort zu archivieren, von wo aus weiterhin auf sie zugegriffen werden kann, wenn FIPS aktiviert wurde.

Das folgende Verfahren beschreibt, was zur Konfiguration von XProtect VMS erforderlich ist, damit es im FIPS 140-2-konformen Modus läuft:

1. Deaktivieren Sie die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem SQL Server gehosted wird.

   Während das Upgrades können Sie XProtect VMS nicht installieren, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist.

2. Achten Sie darauf, dass eigenständige Dritt-Integrationen auf einem FIPS-fähigen Windows-Betriebssystem laufen können.

   Entspricht eine eigenständige Integration nicht FIPS 140-2, so kann sie nicht ausgeführt werden, wenn Sie das Windows-Betriebssystem so einrichten, dass es im FIPS-Modus läuft.

   Gehen Sie wie folgt vor, um dies zu vermeiden:

   - Führen Sie eine Bestandsaufnahme aller Ihrer eigenständigen Integrationen durch, um zu XProtect VMS
   - Wenden Sie sich an die Anbieter dieser Integrationen und fragen Sie sie, ob die Integrationen FIPS 140-2-konform sind
   - Setzen Sie die FIPS 140-2-konformen eigenständigen Integrationen ein

3. Vergewissern Sie sich, dass die Treiber, damit die Kommunikation mit den Geräten, FIPS 140-2-konform sind.

   XProtect VMS wird garantiert und kann die FIPS 140-2-konforme Betriebsart erzwingen, wenn die folgenden Kriterien erfüllt sind:

   - Geräte verwenden nur konforme Treiber, um Verbindungen herzustellen

     Weitere Informationen zu Treibern, die Compliance gewährleisten und erzwingen können, finden Sie im Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung. XProtect VMS
   - Die Geräte verwenden das Device Pack in der Version 11.1 oder höher

     Die Treiber aus den Legacy Driver Device Packs können keine FIPS 140-2-konforme Verbindung garantieren.
   - Die Geräte werden über HTTPS verbunden, und entweder über Secure Real-Time Transport Protocol (SRTP) oder Real Time Streaming Protocol (RTSP) über HTTPS für Video-Stream

     Die Treibermodule können die Einhaltung von FIPS 140-2 durch eine Verbindung über HTTP nicht garantieren. Die Verbindung mag konform sein, es gibt jedoch keine Garantie dafür, dass sie tatsächlich konform ist.
   - Auf dem Computer, auf dem der Aufzeichnungsserver läuft, läuft das Betriebssystem Windows mit aktiviertem FIPS-Modus

4. Achten Sie darauf, dass die Daten in den Mediendatenbanken mithilfe von FIPS 140-2-konformen Chiffren verschlüsselt werden.

   Dies erfolgt durch Ausführen des Upgrade-Tools für Mediendatenbanken. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

5. Bevor Sie im Betriebssystem Windows FIPS aktivieren, und nachdem Sie Ihr XProtect VMS-System konfiguriert und sich vergewissert haben, dass alle Komponenten und Geräte in einer FIPS-fähigen Umgebung laufen können, aktualisieren Sie die Passwörter für Ihre vorhandene Hardware im XProtect Management Client.

   Klicken Sie dazu im Management Client, vom ausgewählten Aufzeichnungsserver in dem Knoten **Aufzeichnungsserver** aus mit der rechten Maustaste und wählen Sie **Hardware hinzufügen...**. Klicken Sie sich durch den Assistenten **Hardware hinzufügen**. Damit werden alle aktuellen Anmeldedaten aktualisiert und so verschlüsselt, dass sie FIPS erfüllen.

Sie können FIPS erst aktivieren, wenn Sie das gesamte VMS aktualisiert haben, einschließlich aller Clients.

## Optimale Vorgehensweise beim Upgrade

Weitere Informationen zu Upgrade-Anforderungen (siehe Upgrade-Anforderungen auf Seite 402), einschließlich der Sicherung von SQL Server Datenbanken, bevor Sie mit dem eigentlichen Upgrade beginnen.

Die Gerätetreiber sind jetzt auf zwei Gerätepakete aufgeteilt: das reguläre Gerätepaket mit neueren Treibern und ein Stammgerätepaket mit älteren Treibern. Das reguläre Gerätepaket wird bei einem Update oder Upgrade ständig automatisch installiert. Wenn Sie ältere Kameras haben, die Gerätetreiber aus dem Stammgerätepaket nutzen, und Sie haben noch kein Stammgerätepaket installiert, installiert das System nicht automatisch das Stammgerätepaket.

Wenn zu Ihrem System ältere auch Kameras gehören, empfiehlt Milestone zu prüfen, ob die Kameras Treiber aus dem Altgerätepaket auf dieser Seite (https://www.milestonesys.com/community/business-partner-tools/device-packs/) verwenden. Um Herauszufinden, ob Sie das Stammpaket bereits installiert haben, schauen Sie in die XProtect Systemordner. Wenn Sie das Altgerätepaket herunterladen müssen, gehen Sie auf die Download-Seite (https://www.milestonesys.com/downloads/).

Wenn Sie ein **Einzelcomputer**-System verwenden, können Sie die neue Software über die bereits vorhandene Installation installieren.

In einem Milestone Interconnect oder Milestone Federated Architecture System müssen Sie zunächst die zentrale Seite aktualisieren und danach die entfernten Seiten.

Führen Sie in einem verteilten System die Aktualisierung in der folgenden Reihenfolge durch:

1. Erweitern Sie den Management Server mit der **Benutzerdefinierten** Option im Installationsprogramm (siehe Systeminstallation - Benutzerdefiniert auf Seite 168).
    1. Auf der Seite des Assistenten, auf der Sie die Komponenten auswählen können, sind bereits alle Komponenten des Managementservers ausgewählt.
    2. Geben Sie SQL Server und die Datenbank an. Entscheiden Sie, ob die SQL Server-Datenbank, die Sie bereits verwenden, beibehalten werden und ob die vorhandenen Daten in der Datenbank verbleiben sollen.

    > Wenn Sie mit der Installation beginnen, verlieren Sie die Funktion des ausfallsicheren Aufzeichnungsservers (siehe Der ausfallsichere Aufzeichnugnsserver (Erklärung) auf Seite 40).

    > Wenn Sie auf dem Management Server die Verschlüsselung aktivieren, bleiben die Aufzeichnungsserver so lange offline, bis sie aufgerüstet werden und Sie die Verschlüsselung zum Management Server aktiviert haben (siehe Sichere Kommunikation (Erklärung) auf Seite 155).

2. Aktualisierung des Failover-Aufzeichnungsservers. Installieren Sie von der Downloadseite ihres Management-Server (die von der Download Manager kontrolliert wird), Recording Server.

    > Wenn Sie vorhaben, die Verschlüsselung auf den Failover-Aufzeichnungsservern zu aktivieren, und Sie die Failoverfunktion erhalten möchten, so aktualisieren Sie die Failover-Aufzeichnungsserver ohne Verschlüsselung und aktivieren Sie diese, nachdem Sie die Aufzeichnungsserver aktualisiert haben.

    Ab diesem Zeitpunkt besteht wieder volle Funktionalität des Failover-Servers.

3. Wenn Sie vorhaben, die Verschlüsselung auf den Aufzeichnungsservern oder den Failover-Aufzeichnungsservern zu den Clients zu aktivieren, und es wichtig ist, dass die Clients während der Aktualisierung Daten abrufen können, so aktualisieren Sie alle Clients und Dienste, die Datenstreams von den Aufzeichnungsservern abrufen, bevor Sie die Aufzeichnungsserver aktualisieren. Diese Clients und Dienste sind:
    - XProtect Smart Client
    - Management Client
    - Management Server
    - XProtect Mobile-Server
    - XProtect Event Server

- DLNA Server Manager
- Milestone Open Network Bridge
- Seiten, die Datenstreams vom Aufzeichnungsserver abrufen durch Milestone Interconnect
- Einige MIP SDK Drittintegrationen

4. Aktualisieren Sie den Aufzeichnungsserver. Sie können Aufzeichnungsserver mithilfe des Installationsassistenten (siehe Installation eines Aufzeichnungsserver über Download Manager auf Seite 177) oder lautlos installieren (siehe Automatische Installation eines Aufzeichnungsservers auf Seite 185). Der Vorteil einer automatischen Installation ist die Möglichkeit zur Ferninstallation.

   > Wenn Sie die Verschlüsselung aktivieren, und dem ausgewählten Serverauthenfizierungszertifikat wird nicht auf allen Computern vertraut, so verlieren diese die Verbindung. Weitere Informationen finden Sie unter Sichere Kommunikation (Erklärung) auf Seite 155.

Folgen Sie diesen Schritten an den weiteren Standorten in Ihrem System.

## Upgrade in einem Cluster

Stellen Sie sicher, dass Sie ein Backup der Datenbank durchführen, bevor Sie den Cluster aktualisieren.

1. Deinstallieren Sie den Management Server-Service auf allen Management-Servern im Cluster.
2. Deinstallieren Sie den Management-Server auf allen Servern im Cluster.
3. Verwenden Sie das Verfahren zur Installation mehrerer Managementserver in einem Cluster, wie unter "In einem Cluster installieren" beschrieben. Lesen Sie Installation in einem Cluster auf Seite 193.

> Achten Sie bei der Installation darauf, den vorhandenen SQL Server und die vorhandene SQL Server-Datenbank zu verwenden, in der die Systemkonfiguration aktuell gespeichert ist. Die Systemkonfiguration wird automatisch aktualisiert.

# Einzelheiten zur Benutzeroberfläche

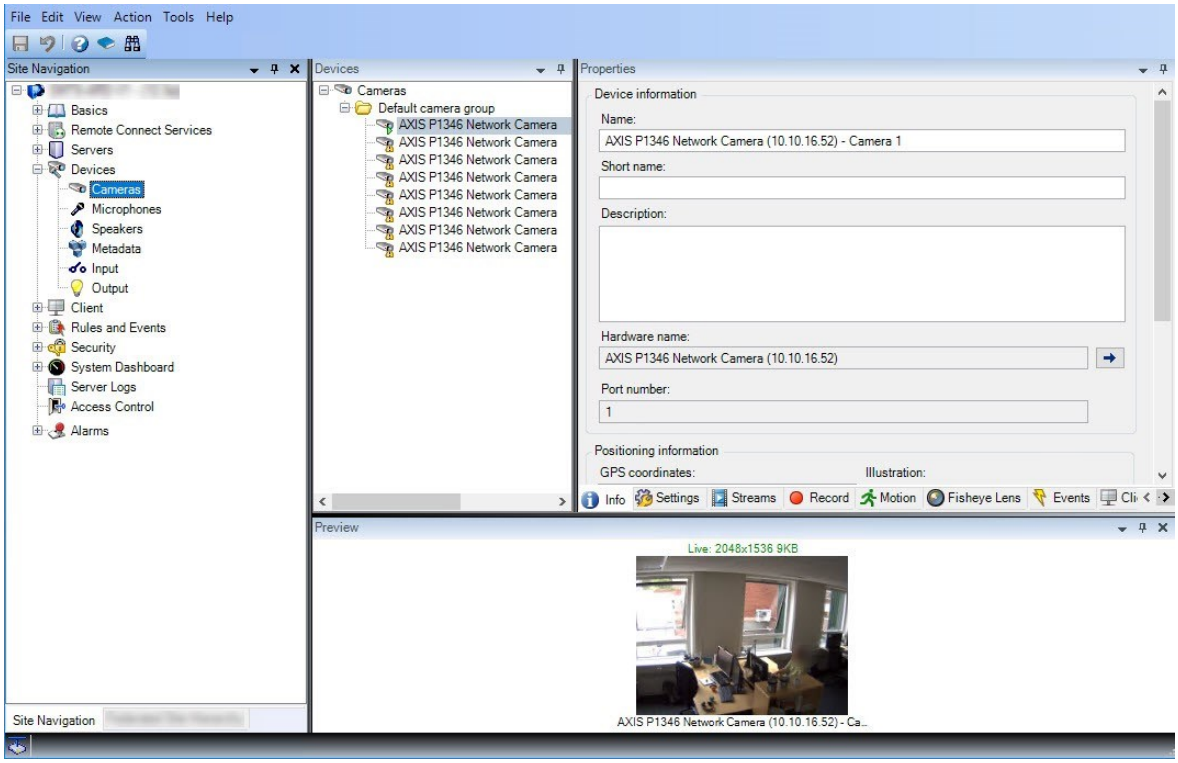
## Hauptfenster und Bereiche

Das Management Client-Fenster ist in Bereiche unterteilt. Die Anzahl der Bereiche und Layouts hängt ab von Ihren:

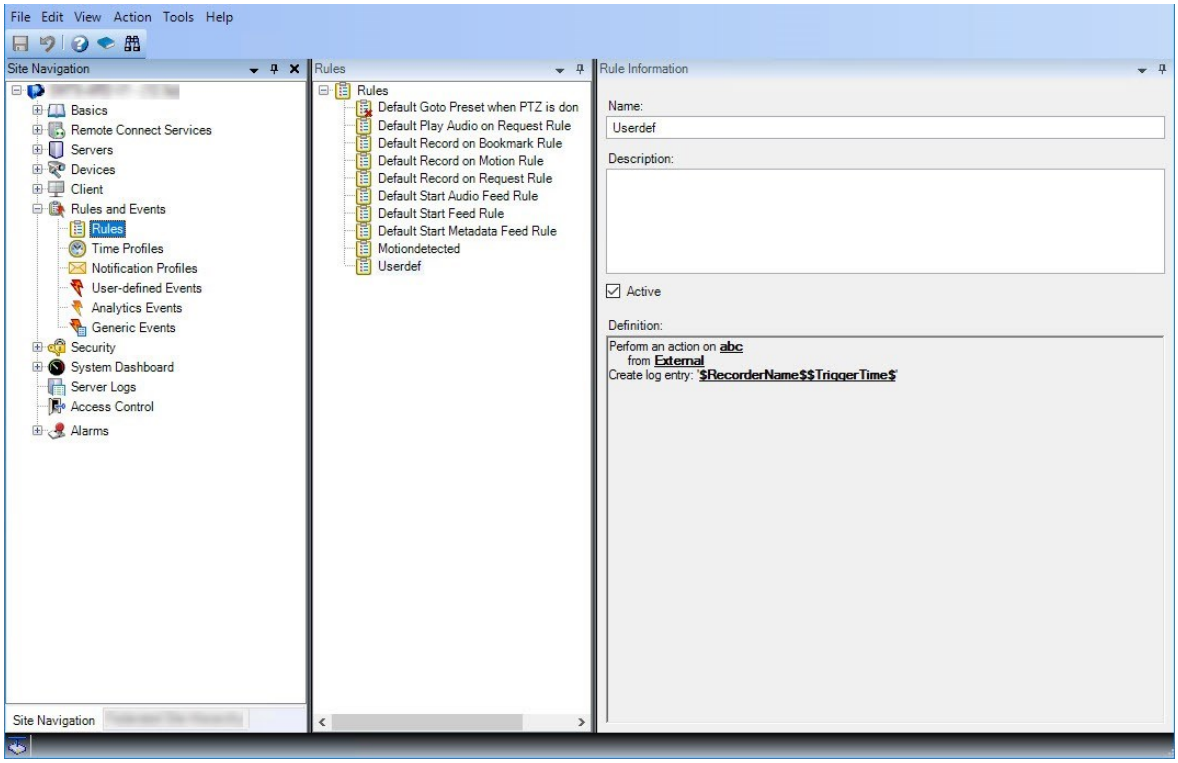
- Systemkonfiguration
- Aufgabe
- Verfügbare Funktionen

Unten finden Sie einige Beispiele typischer Layouts:

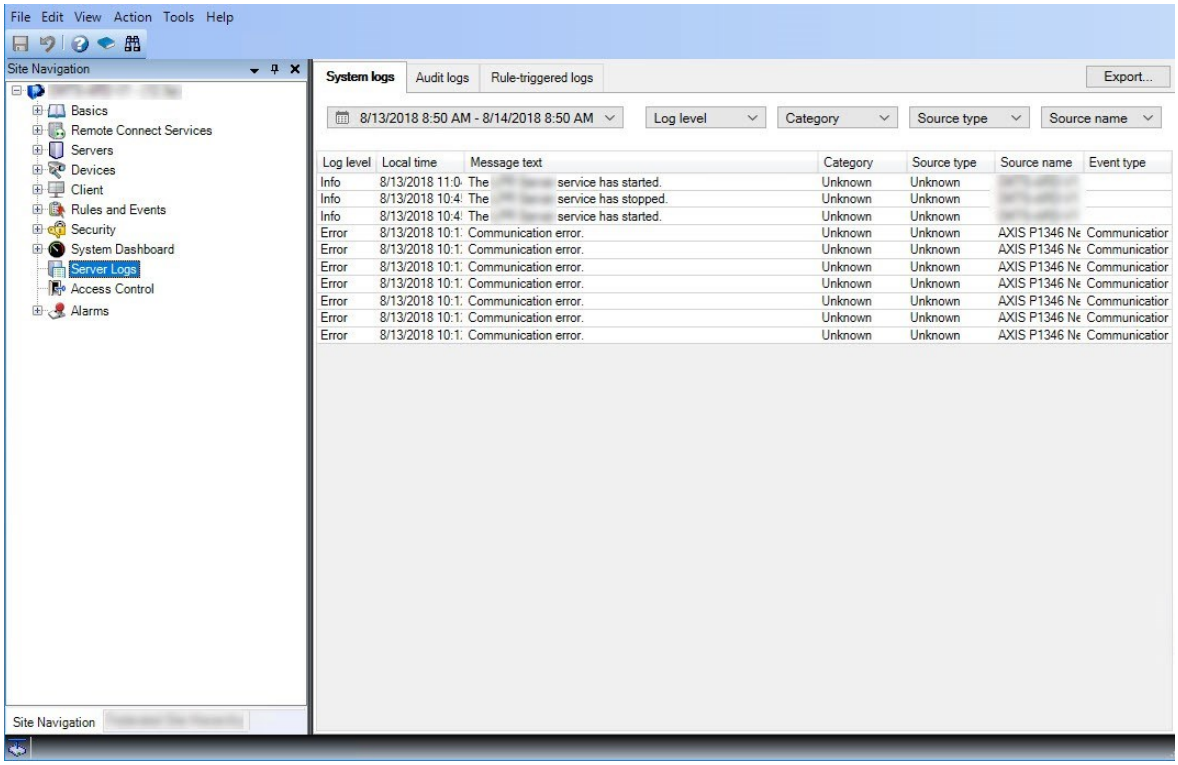
- Wenn Sie mit Aufzeichnungsservern und Geräten arbeiten:




- Wenn Sie mit Regeln, Zeit und Benachrichtigungsprofilen, Benutzern, Rollen arbeiten:

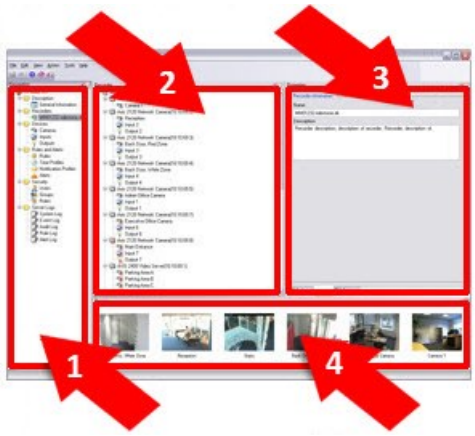


- Wenn Sie sich Protokolle ansehen:




## Bereichslayout

In dieser Darstellung sehen Sie ein typisches Fensterlayout. Da Sie das Layout anpassen können, ist es möglich, dass es auf Ihrem Computer anders aussieht.



1. Fenster „Standort-Navigation“ und „Hierarchie der föderalen Standorte“
2. Übersichtsbereich
3. Eigenschaftenfenster
4. Vorschaufenster

**Der Bereich Site-Navigation**

Dies ist Ihr wichtigstes Navigationselement im Management Client. Es spiegelt den Namen sowie die Einstellungen und Konfigurationen des Standorts wider, an dem Sie sich angemeldet haben. Der Standortname wird oben im Fenster angezeigt. Die Funktionen sind in Kategorien angeordnet, welche der Funktionalität der Software entsprechen.

Im **Site-Navigationsfenster** können Sie Ihr System konfigurieren und verwalten, sodass es Ihren Bedürfnissen entspricht. Wenn Ihr System kein Einzelstandortsystem ist, aber föderale Standorte beinhaltet, beachten Sie, dass Sie diesen Standort im Fenster **Hierarchie der föderalen Standorte** verwalten können.

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

**Der Bereich "Föderierte Seitenhierarchie"**

Dies ist das Navigationselement, in dem alle Milestone Federated Architecture-Standorte in einer Hierarchie mit über- und untergeordneten Standorten angezeigt werden.

Sie können einen beliebigen Standort auswählen und sich dort anmelden. Daraufhin wird der Management Client für den Standort gestartet. Derjenige Standort, bei dem Sie sich angemeldet haben, befindet sich stets oben in der Hierarchie.

**Übersichtsbereich**

Liefert eine Übersicht über das Element, das Sie im Fenster **Standort-Navigation** ausgewählt haben, zum Beispiel in Form einer detaillierten Liste. Wenn Sie im Fenster **Übersicht** ein Element auswählen, werden dessen Eigenschaften meist im Fenster **Eigenschaften** angezeigt. Wenn Sie im Fenster **Übersicht** mit der rechten Maustaste auf ein Element klicken, erhalten Sie Zugriff auf dessen Verwaltungsfunktionen.

**Eigenschaftenfenster**

Zeigt die Eigenschaften des Elements an, das im Fenster **Übersicht** ausgewählt wurde. Die Eigenschaften werden auf verschiedenen zugehörigen Registerkarten angezeigt:

**Vorschaufenster**

Das Fenster **Vorschau** wird angezeigt, wenn Sie mit Aufzeichnungsservern und Geräten arbeiten. Es präsentiert Vorschaubilder der ausgewählten Kameras bzw. Informationen über den Status des aktuellen Geräts. Im Beispiel ist ein Vorschaubild der Kamera dargestellt, inkl. Informationen zur Auflösung und Datenrate des Live-Streams der Kamera:


Standardmäßig beziehen sich die Informationen, die mit den Vorschaubildern einer Kamera angezeigt werden, auf die Live-Streams einer Kamera. Sie werden oberhalb der Vorschau als grüner Text dargestellt. Wenn Sie lieber Informationen zum Aufzeichnungsstream aufrufen möchten (als roter Text dargestellt), wählen Sie im Menü die Optionen **Ansicht** > **Aufzeichnungsstreams** anzeigen.

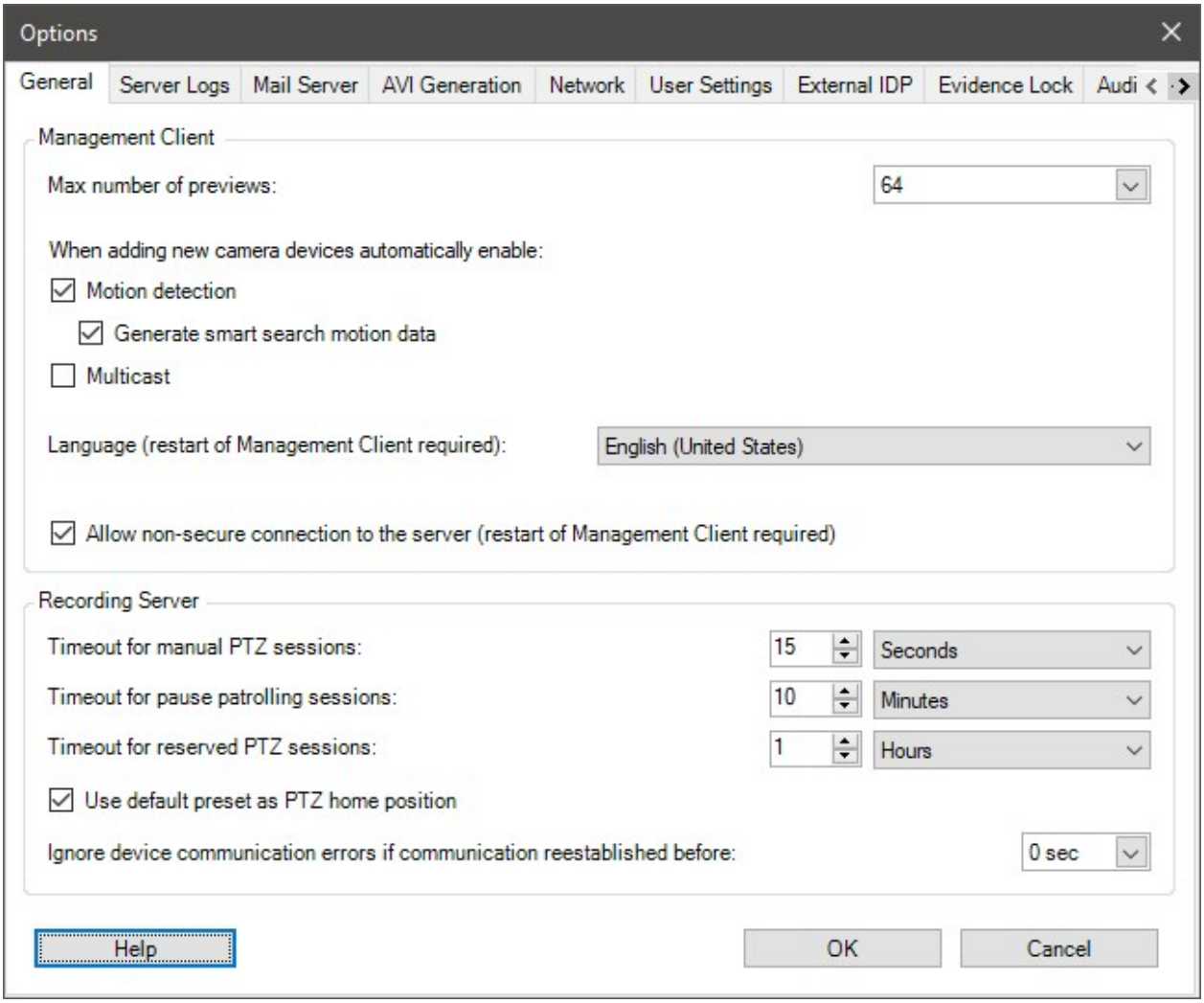
Wenn im **Vorschaufenster** Vorschaubilder verschiedener Kameras mit einer hohen Bildrate angezeigt werden, kann die Leistung darunter leiden. Falls Sie die Anzahl an Vorschaubildern sowie ihre Bildraten ändern möchten, wählen Sie im Menü **Optionen** > **Allgemein**.

## Systemeinstellungen (die Dialogbox "Optionen")

Im Dialogfeld **Optionen** können Sie eine Reihe von Einstellungen bezüglich der allgemeinen Oberfläche und Funktionalität des Systems vornehmen.

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Gehen Sie zu **Tools** > **Optionen**, um das Dialogfeld zu öffnen.




## Registerkarte „Allgemein“ (Optionen)

Auf der Registerkarte „Allgemein“ können Sie allgemeine Einstellungen für den Management Client und den Aufzeichnungsserver festlegen.

### Management Client

| Name | Beschreibung |
|---|---|
| **Maximale Anzahl von Vorschauen** | Wählen Sie die Höchstzahl der Miniaturbilder, die im Bereich **Vorschau** angezeigt werden. Der Standardwert beträgt 64 |

| Name | Beschreibung |
|---|---|
| | Miniaturbilder.<br>Wählen Sie aus dem Menü **Aktion** > **Aktualisieren**, damit die Änderungen übernommen werden.<br>Eine hohe Bildrate zusammen mit einer großen Anzahl an Miniaturbildern kann das System verlangsamen. |
| **Beim Hinzufügen neuer Kamerageräte automatisch aktivieren**: **Bewegungserkennung** | Aktivieren Sie das Kontrollkästchen, um die Bewegungserkennung auf neuen Kameras zu aktivieren, die Sie dem System mithilfe des Assistenten **Hardware hinzufügen** hinzufügen.<br>Diese Einstellung beeinflusst nicht die Einstellungen für die Bewegungserkennung auf bestehenden Kameras.<br>Sie können die Bewegungserkennung einer Kamera auf der Registerkarte **Bewegung** aktivieren und deaktivieren. |
| **Beim Hinzufügen neuer Kamerageräte automatisch aktivieren**: **Bewegungsdaten für Smart Search erzeugen** | Die Erstellung von Bewegungsdaten für Smart Search erfordert, dass die Bewegungserkennung für die Kamera aktiviert ist.<br>Aktivieren Sie das Kontrollkästchen, um die Erzeugung von Smart-Search-Bewegungsdaten für neue Kameras zu aktivieren, wenn Sie diese mit Hilfe des Assistenten **Hardware hinzufügen** zum System hinzufügen.<br>Diese Einstellung beeinflusst nicht die Einstellungen für die Bewegungserkennung auf bestehenden Kameras.<br>Sie können die Erstellung von Smart Search-Bewegungsdaten für eine Kamera auf der Registerkarte **Bewegung** aktivieren und deaktivieren. |
| **Beim Hinzufügen neuer Kamerageräte automatisch aktivieren**: **Multicast** | Aktivieren Sie das Kontrollkästchen, um Multicast auf neuen Kameras zu aktivieren, die Sie mithilfe des Assistenten **Hardware hinzufügen** hinzufügen.<br>Diese Einstellung beeinflusst nicht die Multicast-Einstellungen auf bestehenden Kameras.<br>Sie können Live-Multicasting für eine Kamera auf der Registerkarte **Client** aktivieren und deaktivieren. |
| **Sprache** | Wählen Sie die Sprache des Management Client. |

| Name | Beschreibung |
|---|---|
| | Starten Sie den Management Client neu, um die neue Sprache zu verwenden. |
| **Nicht sichere Verbindung zum Server zulassen** | Aktivieren Sie das Kontrollkästchen, um eine nicht sichere Serververbindung mithilfe des HTTP-Protokolls zuzulassen. (Benutzer werden nicht gefragt, ob eine nicht sichere Serververbindung zugelassen werden soll).<br>Starten Sie den Management Client neu, um diese Einstellung zu verwenden. |

**Aufzeichnungsserver**

| Name | Beschreibung |
|---|---|
| **Zeitüberschreitung für manuelle PTZ-Sitzungen** | Client-Benutzer mit den erforderlichen Benutzerrechten können die Überwachung von PTZ-Kameras von Hand unterbrechen. Wählen Sie aus, wie viel Zeit vergangen sein sollte, bis reguläre Wachrundgänge nach einer manuellen Unterbrechung wieder aufgenommen werden. Diese Einstellung betrifft alle PTZ-Kameras in Ihrem System. Die Standardeinstellung ist 15 Sekunden.<br>Wenn Sie für die Kameras individuelle Zeitüberschreitungen möchten, bestimmten Sie diese auf der Registerkarte **Voreinstellungen** für die Kamera. |
| **Zeitüberschreitung für Sitzungen „Wachrundgang anhalten“** | Client-Benutzer mit einer ausreichenden PTZ-Priorität können Wachrundgänge auf PTZ-Kameras anhalten. Wählen Sie aus, wie viel Zeit vergangen sein sollte, bis reguläre Wachrundgänge nach dem Anhalten wieder aufgenommen werden. Diese Einstellung betrifft alle PTZ-Kameras in Ihrem System. Die Standardeinstellung ist 10 Minuten.<br>Wenn Sie für die Kameras individuelle Zeitüberschreitungen möchten, bestimmten Sie diese auf der Registerkarte **Voreinstellungen** für die Kamera. |
| **Zeitüberschreitung für reservierte PTZ-Sitzungen** | Legen sie eine Standardzeitüberschreitung für reservierte PTZ-Sitzungen fest. Wenn ein Benutzer eine reservierte PTZ-Sitzung ausführt, kann die PTZ-Kamera nicht von anderen verwendet werden, bis sie entweder manuell |

| Name | Beschreibung |
|---|---|
| | freigegeben wurde oder die Zeit überschritten wurde. Die Standardeinstellung ist 1 Stunde.<br>Wenn Sie für die Kameras individuelle Zeitüberschreitungen möchten, bestimmten Sie diese auf der Registerkarte **Voreinstellungen** für die Kamera. |
| **Standardvoreinstellung als PTZ-Ausgangsposition verwenden** | Aktivieren Sie dieses Kontrollkästchen, um die standardmäßige Preset Position anstelle der Ausgangsposition von PTZ-Kameras bei Aktivierung der Schaltfläche **Ausgangsposition** in einem Client zu verwenden.<br>Für die Kamera muss eine Preset Position festgelegt werden. Wenn keine standardmäßige Preset Position definiert ist, wird beim Aktivieren der Schaltfläche **Home** in einem Client nichts ausgelöst.<br>Die Kontrollkästchen sind standardmäßig leer.<br>Zuweisen einer standardmäßigen Preset PositionVoreingestellte Standardposition einer Kamera als Standard zuweisen auf Seite 265 |
| **Geräte-Verbindungsfehler ignorieren, wenn die Verbindung wiederhergestellt wird vor** | Das System protokolliert alle Kommunikationsfehler auf Hardware und Geräten, hier wählen Sie jedoch aus, wie lange ein Kommunikationsfehler vorliegen muss, bevor der Regel-Engine das Ereignis **Kommunikationsfehler** auslöst. |

## Registerkarte „Serverprotokolle“ (Optionen)

Auf der Registerkarte **Serverprotokolle** können Sie Einstellungen für die Management-Server-Protokolle des Systems vornehmen.

Ältere Informationen finden Sie unter Benutzeraktivitäten, Ereignisse, Maßnahmen und Fehler erkennen.

| Name | Beschreibung |
|---|---|
| **Protokolle** | Wählen Sie einen Protokolltyp zum Konfigurieren aus:<br>• Systemprotokolle<br>• Auditprotokolle |

| Name | Beschreibung |
|---|---|
| | • Von Regel ausgelöste Protokolle |
| **Einstellungen** | Deaktivieren oder aktivieren Sie die Protokolle und legen Sie die Speicherzeit fest.<br><br>Erlauben Sie es 2018 R2 und früheren Komponenten, Protokolle aufzuzeichnen. Weitere Informationen finden Sie unter 2018 R2 und früheren Komponenten erlauben, Protokolle aufzuzeichnen.<br><br>Für **Systemprotokolle** können Sie die Nachrichtenstufen festlegen, die Sie protokollieren möchten:<br>• Alle (schließt undefinierte Nachrichten mit ein)<br>• Informationen, Warnungen und Fehler<br>• Warnungen und Fehler<br>• Fehler (Standardeinstellung)<br><br>„Protokollierung der Benutzerzugriffe“ aktivieren für **Auditprotokolle**, wenn das System alle Benutzeraktionen im XProtect Smart Client protokollieren soll. Das sind z. B. Exporte, Aktivierung von Ausgängen und Ansehen von Live-Aufnahmen über Kameras oder die Wiedergabe einer Aufzeichnung.<br><br>Festlegen:<br>• Die Länge einer Wiedergabesequenz<br>Das bedeutet, dass das System nur einen Protokolleintrag erstellt, solange die Wiedergabe durch den Benutzer innerhalb dieses Zeitraums bleibt. Wenn die Wiedergabe diesen Zeitraum überschreitet, erstellt das System einen neuen Protokolleintrag.<br>• Die Anzahl von Aufzeichnungen (Bildern), die ein Benutzer angesehen hat, bis das System einen Protokolleintrag erstellt |

## Registerkarte „Mailserver“ (Optionen)

Auf der Registerkarte **Mailserver** können Sie die Einstellungen für den Mailserver Ihres Systems festlegen. Weitere Informationen finde Sie unter Benachrichtigungsprofile (Erklärung).

| Name | Beschreibung |
|---|---|
| **E-Mail-Absenderadresse** | Geben Sie die E-Mailadresse ein, die als Absender der E-Mailbenachrichtigungen für alle Benachrichtigungsprofile angezeigt werden soll. Beispiel: **sender@organization.org**. |
| **Mail-Server-Adressen** | Geben Sie den Namen des SMTP-Mailservers ein, der e-Mail-Benachrichtigungen sendet. Beispiel: **mailserver.organization.org**. |
| **Mail-Server-Port** | Der für Verbindungen zum Server verwendete TCP-Port. Der Standardport ist 25 für unverschlüsselte Verbindungen, verschlüsselte Verbindungen verwenden typischerweise den Port 465 oder 587. |
| **Die Verbindung zum Server verschlüsseln** | Wenn Sie die Kommunikation zwischen dem Management Server und dem SMTP-Mailserver sichern wollen, aktivieren Sie dieses Kontrollkästchen.<br>Die Verbindung wird mithilfe des E-Mail-Protokollbefehls STARTTLS gesichert. In diesem Modus beginnt die Sitzung zunächst mit einer unverschlüsselten Verbindung, dann wird vom SMTP-Mail- Server ein STARTTLS-Befehl an den Management Server gegeben, um auf die sichere Kommunikation mit SSL umzuschalten. |
| **Server erfordert Login** | Wenn diese Option aktiviert ist, müssen Sie einen Benutzernamen und ein Passwort für die Benutzer zur Anmeldung beim Mailserver festlegen. |

## Registerkarte „AVI-Generierung“ (Optionen)

Auf der Registerkarte **AVI-Generierung** können Sie Komprimierungseinstellungen für die Generierung von AVI-Videoclipdateien festlegen. Diese Einstellungen sind erforderlich, wenn Sie AVI-Dateien an E-Mailbenachrichtigungen anhängen möchten, die von durch Regeln ausgelösten Benachrichtigungsprofilen gesendet werden.

Siehe auch Benachrichtigungen per E-Mail nach Regeln auslösen.

| Name | Beschreibung |
|---|---|
| **Komprimierer** | Wählen Sie den Codec (Komprimierungs-/Dekomprimierungstechnologie) aus, den Sie anwenden möchten. Sollten Sie mehr Codecs auf der Liste zur |

| Name | Beschreibung |
|---|---|
| | Auswahl haben wollen, installieren Sie diese auf dem Management-Server. Nicht alle Kameras unterstützen alle Codecs. |
| **Kompressionsqualität** | (Nicht verfügbar für alle Codecs). Verwenden Sie den Schieberegler, um den Komprimierungsgrad zu wählen (**0** – **100**), der vom Codec durchgeführt werden soll.<br>**0** bedeutet keine Komprimierung, wodurch im Allgemeinen die Bildqualität und die Dateigröße zunimmt. **100** bedeutet maximale Komprimierung, wodurch im Allgemeinen die Bildqualität und die Dateigröße abnimmt.<br>Wenn der Schieberegler nicht verfügbar ist, wird die Komprimierungsqualität ausschließlich durch den ausgewählten Codec bestimmt. |
| **Keyframe alle** | (Nicht verfügbar für alle Codecs). Wenn Sie Keyframes verwenden möchten, aktivieren Sie das Kontrollkästchen und legen Sie die gewünschte Anzahl an Bildern zwischen den Keyframes fest.<br>Keyframes sind einzelne Bilder, die in einem bestimmten Intervall gespeichert werden. Keyframes enthalten die gesamte Ansicht der Kamera, während die folgenden Bilder nur die geänderten Pixel enthalten. So kann die Größe von Dateien beträchtlich verringert werden.<br>Wenn das Kontrollkästchen nicht verfügbar oder nicht aktiviert ist, enthält jedes Bild die gesamte Ansicht der Kamera. |
| **Datenrate** | (Nicht verfügbar für alle Codecs). Wenn Sie eine bestimmte Datenrate festlegen möchten, aktivieren Sie das Kontrollkästchen und legen Sie die Anzahl der Kilobytes pro Sekunde fest.<br>Die Datenrate entscheidet über die Größe der angehängten AVI-Datei.<br>Wenn das Kontrollkästchen nicht verfügbar oder nicht aktiviert ist, wird die Datenrate vom ausgewählten Codec bestimmt. |

## Netzwerk-Registerkarte (Optionen)

Auf der Registerkarte **Netzwerk** können Sie die IP-Adressen der lokalen Clients festlegen, wenn sich die Clients über das Internet mit dem Aufzeichnungsserver verbinden sollen. Das Überwachungssystem erkennt dann, dass sie vom lokalen Netzwerk kommen.

Sie können auch die IP-Version des Systems festlegen: IPv4 oder IPv6. Standardwert ist IPv4.

## Lesezeichen-Registerkarte (Optionen)

> Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Auf der Registerkarte **Lesezeichen** können Sie Einstellungen für Lesezeichen, ihre IDs und Funktionen in XProtect Smart Client festlegen.

| Name | Beschreibung |
|---|---|
| **Präfix der Lesezeichen-ID** | Legen Sie ein Präfix für Lesezeichen fest, das von allen Benutzern von XProtect Smart Client erstellt wird. |
| **Standardmäßige Lesezeichenzeit** | Legen Sie die standardmäßige Start- und Endzeit für Lesezeichen fest, die in XProtect Smart Client erstellt werden.<br>Diese Einstellung muss abgestimmt werden mit:<br>• Die Standardregel für Lesezeichen finden Sie unter Regeln (der Knoten "Regeln und Ereignisse").<br>• Die Vor-Pufferdauer für jede Kamera, siehe Vor-Pufferung verwalten. |

Angaben dazu, wie Sie Lesezeichenberechtigungen einer Rolle festlegen können, finden Sie unter Registerkarte „Geräte“ (Rollen) auf Seite 589.

## Registerkarte „Benutzereinstellungen“ (Optionen)

Auf der Registerkarte **Benutzereinstellungen** können Benutzer ihre bevorzugten Einstellungen festlegen, z. B. ob eine Nachricht angezeigt werden soll, wenn Fernaufzeichnung aktiviert ist.

## Registerkarte des externen IDP (Optionen)

Auf der Registerkarte **Externer IDP** in Management Client können Sie einen externen IDP hinzufügen und konfigurieren sowie Ansprüche aus dem externen IDP registrieren.

| Name | Beschreibung |
|---|---|
| **Aktiviert** | Der externe IDP ist standardmäßig aktiviert. |
| **Name** | Der Name für den externen IDP. Der Name, den Sie hier eingeben, erscheint im Feld **Authentifizierung** im Anmeldefenster Ihres Clients. |
| **Authentifizierungsautorität** | Der URL des externen IDP. |
| **Hinzufügen** | Hinzufügen und konfigurieren eines externen IDP. Wenn Sie **Hinzufügen** wählen, wird das Dialogfeld **Externer IDP** geöffnet und Sie können die Informationen für die Konfiguration eingeben, siehe **Konfigurieren eines externen IDP** unter der Tabelle. |
| **Bearbeiten** | Bearbeiten der Konfiguration des externen IDP. |
| **Entfernen** | Entfernen der Konfiguration des externen IDP.<br><br>Wenn Sie die Konfiguration eines externen IDP löschen, können sich die Benutzer, die über diesen externen IDP authentifiziert werden, nicht mehr am XProtect-VMS anmelden. Wenn Sie den externen IDP wieder hinzufügen, werden bei der Anmeldung neue Benutzer angelegt, da sich die ID des externen IDP geändert hat. |

### Konfiguration eines externen IDP

- Um einen externen IDP hinzuzufügen, wählen Sie **Hinzufügen** im Abschnitt **Externer IDP** und geben Sie die Informationen in der nachstehenden Tabelle ein:

| Name | Beschreibung |
|---|---|
| **Name** | Der Name für den externen IDP, den Sie hier eingeben, erscheint im Feld **Authentifizierung** im Anmeldefenster Ihres Clients. |
| **Client ID** und **Client-** | Muss vom externen IDP bezogen werden. Die Client-ID und das Client-Geheimnis |

| Name | Beschreibung |
|---|---|
| **Geheimnis** | werden benötigt, um sicher mit dem externen IDP zu kommunizieren. |
| **Rückrufpfad** | Teil einer URL für den umgeleiteten Authentifizierungsfluss zur Anmeldung von Benutzern.<br><br>Benutzer werden von einer Anmeldeseite aus angemeldet, die vom externen IDP gehostet wird. Wenn der Authentifizierungsprozess abgeschlossen ist, wird dieser Pfad aufgerufen und der Benutzer wird zum XProtect VMS umgeleitet.<br><br>Der Standardwert ist "/signin-oidc".<br><br>Das Umleitungsformat<br><br>Der URI des Rückrufpfads wird vom Management-Server FQID zusammen mit /idp/ erstellt und der Rückrufpfad auf dem externen Anbieter konfiguriert.<br><br>Beispiele:<br><br>• Umleitung des URI-Formats für den XProtect Smart Client und den XProtect Management Client: [schema]://[management server address]/idp/[callback path]<br><br>• Umleitung des URI-Formats für den XProtect Web Client und den XProtect Mobile-Client: [redirect Uri without “/index.html”]/idp/[callback path]<br><br>Beachten Sie, dass der "idp"-Teil des Rückrufpfads zwischen Groß- und Kleinschreibung unterscheidet und in Kleinbuchstaben eingegeben werden muss. |
| **Aufforderung zur Anmeldung** | Geben Sie dem externen IDP gegenüber an, ob der Benutzer eingeloggt bleiben soll oder ob eine Überprüfung des Benutzers erforderlich ist. Je nach externem IDP kann die Überprüfung eine Passwortüberprüfung oder eine vollständige Anmeldung umfassen. |
| **Für die Erstellung eines Benutzernamens zu verwendender Anspruch** | Geben Sie optional an, welcher Anspruch aus dem externen IDP verwendet werden soll, um einen eindeutigen Benutzernamen für den automatisch bereitgestellten Benutzer im VMS zu erzeugen. Weitere Informationen über eindeutige Benutzernamen, die aufgrund von Ansprüchen erstellt werden, finden Sie unter Eindeutige Benutzernamen für Benutzer von externen IDPs. |
| **Bereiche** | Verwenden Sie optional Bereiche, um die Anzahl der Ansprüche zu begrenzen, die Sie von einem externen IDP erhalten. Wenn Sie wissen, dass die für Ihr VMS relevanten Ansprüche in einem bestimmten Bereich liegen, können Sie den Bereich verwenden, um die Anzahl der Ansprüche zu begrenzen, die Sie aus dem externen IDP erhalten. |

### Ansprüche anmelden

Wenn Sie Ansprüche aus dem externen IDP registriert haben, können Sie die Ansprüche den Rollen im VMS zuordnen, um die Benutzerrechte im VMS zu bestimmen. Weitere Informationen finden Sie unter Zuordnung von Ansprüchen aus einem externen IDP.

- Um Ansprüche aus einem externen IDP zu registrieren, wählen Sie die Option **Hinzufügen** im Abschnitt **Registrierte Ansprüche** und geben Sie die Informationen in der nachstehenden Tabelle ein:

| Name | Beschreibung |
|---|---|
| **Externer IDP** | Der Name des externen IDP. |
| **Name der Forderung** | Bezeichnung des Anspruchs in Freitextform. Die Bezeichnung steht dann bei der Auswahl einer Rolle zur Verfügung. |
| **Anzeigename** | Der Anzeigename eines Anspruchs. |
| **Groß-/Kleinschreibung** | Gibt an, ob beim Wert einer Forderung zwischen Groß- und Kleinschreibung unterschieden wird.<br><br>Beispiele für Werte, bei denen in der Regel zwischen Groß- und Kleinschreibung unterschieden wird:<br><br>- Textdarstellungen von IDs wie z. B. einer Guid: F951B1F0-2FED-48F7-88D3-49EB5999C923 oder OadFgrDesdFesff=<br><br>Beispiele für Werte, bei denen in der Regel nicht zwischen Groß- und Kleinschreibung unterschieden wird:<br><br>- E-Mail-Adressen<br>- Rollenbezeichnungen<br>- Gruppennamen<br><br>. |
| **Hinzufügen**, **Bearbeiten**, **Entfernen** | Registrierung und Pflege von Ansprüchen.<br><br>Wenn Sie einen Anspruch auf der Website des externen IDP ändern, müssen sich die Benutzer erneut beim XProtect Client anmelden. Angenommen ein Benutzer, Bob, z.B. Bediener sein soll. Der Anspruch wird dann auf der Website des externen IDP zu Bob hinzugefügt. Wenn Bob jedoch bereits bei XProtect angemeldet ist, muss er sich erneut anmelden, damit die Änderung wirksam wird. |

### Umleitungs-URIs für Web-Clients

Die Umleitungs-URI ist der Ort, an den der Benutzer nach einer erfolgreichen Anmeldung umgeleitet wird. Die Umleitungs-URIs müssen exakt mit den Adressen der Webclients übereinstimmen. Sie können sich zum Beispiel nicht über einen externen IDP anmelden, wenn Sie XProtect Web Client über **https://localhost:8082/index.html** und die Umleitungs-URI für die von Ihnen hinzugefügten Webclients **https://127.0.0.1:8082/index.html** öffnen.

| Name | Beschreibung |
|---|---|
| **URI** | Der URI von XProtect Web Client im Format **https://[mobile server]:[port]/index.html**. Bei den Umleitungs-URIs wird nicht zwischen Groß- und Kleinschreibung unterschieden. |
| **Hinzufügen**, **Bearbeiten**, **Entfernen** | Registrierung und Verwaltung von Umleitungs-URIs.<br>Wenn Sie URIs entfernen, müssen Sie mindestens eine Umleitungs-URI behalten, damit das System funktioniert. |

## Registerkarte „Customer Dashboard" (Kunden-Dashboard) (Optionen)

Auf der Registerkarte **Customer Dashboard (Kunden Dashboard)** können Sie Milestone Customer Dashboard aktivieren oder deaktivieren.

Kunden Dashboard ist ein Online-Überwachungsdienst, der Systemadministratoren oder anderen Personen, die Zugriff auf Informationen zur Ihrer Systeminstallation haben, eine grafische Übersicht über den aktuellen Status Ihres Systems bietet, einschließlich mögliche technische Probleme wie Kameraausfälle.

Sie können das Kontrollkästchen jederzeit aktivieren oder deaktivieren, um Ihre Kunden–Dashboard-Einstellungen zu ändern.

## Registerkarte Beweissicherung (Optionen)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Auf der Registerkarte **Beweissicherung** können Sie Beweissicherungsprofile bearbeiten und die Dauer festlegen, die Ihre Clientbenutzer auswählen können, um den Schutz der Daten zu gewährleisten.

| Name | Beschreibung |
|---|---|
| **Beweissicherungsprofile** | Eine Liste mit angelegten Beweissicherungsprofilen.<br>Sie können Beweissicherungsprofile hinzufügen und entfernen. Sie können das Standard-Beweissicherungsprofil nicht entfernen. Sie können jedoch die Zeitoptionen und den Namen des Profils ändern. |
| **Sperrzeitoptionen** | Die Beweissicherungsdauer, die Clientbenutzer auswählen können.<br>Verfügbare Optionen sind Stunde(n), Tag(e), Woche(n), Monat(e), Jahr(e), unbestimmt oder benutzerdefiniert. |

Angaben zur Festlegung der Zugriffsberechtigungen einer Rolle für die Beweissicherung finden Sie in den Rolleneinstellungen unter Registerkarte „Geräte“ (Rollen) auf Seite 589.

## Registerkarte „Audionachrichten“ (Optionen)

Über die Registerkarte **Audionachrichten** können Sie Dateien mit Audionachrichten hochladen, deren Sendung durch bestimmte Regeln ausgelöst wird.

Es können maximal 50 Dateien hochgeladen werden und die maximale Größe beträgt 1 MB pro Datei.

| Name | Beschreibung |
|---|---|
| **Name** | Zeigt den Namen einer Nachricht an. Sie geben den Namen beim Hinzufügen der Nachricht ein. Klicken Sie auf **Hinzufügen**, um eine Nachricht auf das System hochzuladen. |
| **Beschreibung** | Zeigt eine Beschreibung der Nachricht an.<br>Sie geben die Beschreibung beim Hinzufügen der Nachricht ein. Sie können als Beschreibung den Verwendungszweck oder die Nachricht selbst angeben. |
| **Hinzufügen** | Damit können Sie Audionachrichten auf das System hochladen.<br>Unterstützt werden die standardmäßigen Audiodateiformate von Windows:<br>• .wav<br>• .wma |

| Name | Beschreibung |
|---|---|
| | • .flac |
| **Bearbeiten** | Damit können Sie den Namen und die Beschreibung bearbeiten oder die jeweilige Datei ersetzen. |
| **Entfernen** | Damit löschen Sie die Audionachricht von der Liste. |
| **Wiedergabe** | Klicken Sie auf diese Schaltfläche, um sich die Audionachricht von dem Computer anzuhören, auf dem Management Client ausgeführt wird. |

Zum Festlegen einer Regel, die die Wiedergabe von Audiodateien auslöst, siehe Eine Regel hinzufügen.

Allgemein weiteres zu den Maßnahmen, die sie in Regeln verwenden können, finden Sie unter Aktionen und Stoppaktionen.

## Die Registerkarte "Privatsphäreneinstellungen"

Auf der Registerkarte **Datenschutzeinstellungen** können Sie die Erhebung von Nutzungsdaten in XProtect Mobile Server, XProtect Mobile Client, XProtect Web Client und XProtect Smart Client aktivieren oder deaktivieren. Klicken Sie dann auf **OK**.

Indem Sie die Erhebung von Nutzungsdaten aktivieren, stimmen Sie der Nutzung der Technologie von Milestone Systems als Drittanbieter durch Google zu, bei dem nicht auszuschließen ist, dass Daten auch in den USA verarbeitet werden. Weitere Informationen über den Datenschutz und die Erhebung von Nutzungsdaten finden Sie im Datenschutzleitfaden zur DSGVO.

## Registerkarte „Zutrittskontrolleinstellungen“ (Optionen)

Zur Nutzung von XProtect Access müssen Sie eine Basislizenz erworben haben, die Ihnen den Zugriff auf diese Funktion erlaubt.

| Name | Beschreibung |
|---|---|
| **Fenster "Entwicklungseigenschaften" anzeigen** | Wenn ausgewählt, erscheinen zusätzliche Entwicklerinformationen für **Zutrittskontrolle** > **Allgemeine Einstellungen**.<br><br>Diese Einstellung sollte nur von Entwicklern verwendet werden, die Zutrittskontrollsysteme integrieren. |

## Registerkarte „Analyseereignisse“ (Optionen)

Auf der Registerkarte **Analyseereignisse** können Sie die Funktion Analyseereignisse aktivieren und genauer bestimmen.

| Name | Beschreibung |
|---|---|
| **Aktivieren** | Legen Sie fest, ob Sie Analyseereignisse verwenden möchten. Standardmäßig ist diese Funktion deaktiviert. |
| **Port** | Legen Sie den Port fest, der von dieser Funktion verwendet werden soll. Die Standardeinstellung ist Port 9090.<br><br>Stellen Sie sicher, dass die entsprechenden VCA-Tool-Hersteller auch diese Portnummer verwenden. Denken Sie beim Ändern der Portnummer daran, auch die Portnummer der Hersteller zu ändern. |
| **Alle Netzwerkadressen** oder **Angegebenen Netzwerkadressen** | Legen Sie fest, ob Ereignisse von allen IP-Adressen/Hostnamen zugelassen werden oder nur Ereignisse von IP-Adressen/Hostnamen, die auf der **Adressliste** (siehe unten) aufgeführt werden. |
| **Adressliste** | Legen Sie eine Liste vertrauenswürdiger IP-Adressen/Hostnamen an. Die Liste filtert eingehende Daten, sodass nur Ereignisse von bestimmten IP-Adressen/Hostnamen zugelassen werden. Sie können die Adressformate beider Domänen-Namen-Systeme (DNS), IPv4 und IPv6 verwenden.<br><br>Sie können Adressen zu Ihrer Liste hinzufügen, indem Sie jede IP-Adresse oder jeden Hostnamen manuell eingeben oder eine externe Adressliste importieren. |

| Name | Beschreibung |
|---|---|
| | • **Manuelle Eingabe**: Geben Sie die IP-Adresse/den Hostnamen in die Adressliste ein. Wiederholen Sie diesen Schritt für alle Adressen<br>• **Importieren**: Klicken Sie auf **Importieren** und öffnen Sie die externe Adressliste. Die externe Liste muss eine .txt-Datei sein und jede IP-Adresse oder jeder Hostname muss auf einer separaten Leitung sein |

## Registerkarte „Alarme und Ereignisse“ (Optionen)

Über die Registerkarte **Alarme und Ereignisse** können Sie Einstellungen für Alarme, Ereignisse und Protokolle festlegen. Weitere Informationen zu diesen Einstellungen finden Sie auch unter Größenbegrenzung für die Datenbank auf Seite 138.

| Name | Beschreibung |
|---|---|
| **Geschlossene Alarme beibehalten für** | Legen Sie eine Anzahl an Tagen fest, für welche die Alarme mit dem Status **Geschlossen** in der Datenbank gespeichert bleiben. Wenn Sie den Wert auf **0** setzen, wird der Alarm gelöscht, nachdem er geschlossen wurde.<br><br>Alarme besitzen immer einen Zeitstempel. Wird der Alarm von einer Kamera ausgelöst, dann wird mit dem Zeitstempel ein Bild vom Zeitpunkt des Alarms gespeichert. Die Alarminformation selbst wird auf dem Event Server gespeichert, während die Videoaufnahmen, die zu dem angehängten Bild gehören, auf dem Server des entsprechenden Überwachungssystems gespeichert werden.<br><br>Behalten Sie die Videoaufnahmen mindestens so lange, wie Sie Ihre Alarme auf dem Event Server behalten wollen, damit Sie die Bilder des Alarms ansehen können. |
| **Alle anderen Alarme beibehalten für** | Legen Sie die Anzahl an Tagen fest, für welche die Alarme mit dem Status **Neu**, **Wird verarbeitet** oder **Zurückgestellt** gespeichert werden. Wenn Sie den Wert auf 0 festlegen, erscheint der Alarm im System, wird aber nicht gespeichert. |

| Name | Beschreibung |
|---|---|
| | Alarme besitzen immer einen Zeitstempel. Wird der Alarm von einer Kamera ausgelöst, dann wird mit dem Zeitstempel ein Bild vom Zeitpunkt des Alarms gespeichert. Die Alarminformation selbst wird auf dem Event Server gespeichert, während die Videoaufnahmen, die zu dem angehängten Bild gehören, auf dem Server des entsprechenden Überwachungssystems gespeichert werden.<br><br>Behalten Sie die Videoaufnahmen mindestens so lange, wie Sie Ihre Alarme auf dem Event Server behalten wollen, damit Sie die Bilder des Alarms ansehen können. |
| **Protokolle beibehalten für** | Legen Sie die Anzahl an Tagen fest, für welche die Protokolle des Event-Servers beibehalten werden sollen. Sollten Sie die Protokolle für einen längeren Zeitraum beibehalten, so stellen Sie sicher, dass der Computer mit dem Event Server über ausreichend Speicherplatz verfügt. |
| **Verbose-Protokollierung aktivieren** | Markieren Sie das Kontrollkästchen, um ein detailliertes Protokoll der Event Server-Kommunikation aufzubewahren. Es wird für die Anzahl an Tagen gespeichert, die im Feld **Protokolle beibehalten für** festgelegt wurde. |
| **Ereignistypen** | Legen Sie die Anzahl an Tagen fest, für welche die Ereignisse in der Datenbank gespeichert werden sollen. Es gibt zwei Möglichkeiten, dies zu tun:<br>• Sie können die Speicherzeit für eine gesamte Ereignisgruppe festlegen. Ereignistypen mit dem Wert **Gruppe folgen** übernehmen den Wert der Ereignisgruppe<br>• Sie können die Speicherzeit für einzelne Ereignistypen auch dann festlegen, wenn Sie einen Wert für eine Ereignisgruppe bestimmen.<br><br>Wenn der Wert **0** beträgt, werden die Ereignisse nicht in der Datenbank gespeichert. |

| Name | Beschreibung |
|---|---|
| | Externe Ereignisse (benutzerdefinierte Ereignisse, generische Ereignisse und Eingangsereignisse) werden standardmäßig auf **0** gesetzt und der Wert kann nicht geändert werden. Der Grund dafür ist, dass diese Ereignistypen so häufig auftreten, dass ihre Speicherung in der Datenbank Leistungsprobleme verursachen könnte. |

## Registerkarte „Generische Ereignisse“ (Optionen)

Auf der Registerkarte **Generische Ereignisse** können Sie generische Ereignisse und Einstellungen zu Datenquellen festlegen.

Für weitere Informationen zum Konfigurieren von generischen Ereignissen siehe Generische Ereignisse (Erklärung).

| Name | Beschreibung |
|---|---|
| **Datenquelle** | Sie können zwischen zwei standardmäßigen Datenquellen wählen und eine benutzerdefinierte Datenquelle einstellen. Die Wahl hängt von Ihrem Drittanbieterprogramm und/oder der Hardware oder Software ab, die Sie als Interface verwenden möchten:<br>**Kompatibel**: Werkseinstellungen sind aktiviert, Echo bei allen Bytes, TCP und UDP, nur IPv4, Port 1234, kein Trennzeichen, nur lokaler Host, aktuelle Codepage-Verschlüsselung (ANSI).<br>**International**: Werkseinstellungen sind aktiviert, Echo nur bei Statistiken, nur TCP, IPv4+6, Port 1235, <CR><LF> als Trennzeichen, nur lokaler Host, UTF-8-Kodierung. (<CR><LF> = 13,10).<br>[Datenquelle A]<br>[Datenquelle B]<br>und so weiter. |

| Name | Beschreibung |
|---|---|
| **Neu** | Anklicken, um eine neue Datenquelle zu definieren. |
| **Name** | Name der Datenquelle. |
| **Aktiviert** | Datenquellen sind standardmäßig deaktiviert. Wählen Sie das Kontrollkästchen aus, um die Datenquelle zu aktivieren. |
| **Zurücksetzen** | Anklicken, um alle Einstellungen der ausgewählten Datenquelle zurückzusetzen. Der Name, der im Feld **Name** eingegeben wurde, bleibt. |
| **Port** | Die Portnummer der Datenquelle. |
| **Protokolltypauswahl** | Protokolle, die vom System beachtet und analysiert werden sollen, um generische Ereignisse zu erkennen:<br>**Beliebig**: Sowohl TCP als auch UDP.<br>**TCP**: Nur TCP.<br>**UDP**: Nur UDP.<br>TCP- und UDP-Pakete, die für generische Ereignisse verwendet werden, dürfen Sonderzeichen enthalten, wie z. B. @, #, +, ~ und andere. |
| **IP-Typauswahl** | Auswählbare IP-Adressentypen: IPv4, IPv6 oder beide. |
| **Separator-Bytes** | Wählen Sie die Separator-Bytes aus, um einzelne generische Ereignisaufzeichnungen zu trennen. Der Standardwert für den Datenquelltyp **International** (siehe **Datenquellen** oben) ist **13,10**. (13,10 = <CR><IF>). |
| **Echotypauswahl** | Verfügbare Formate für die Echorückstrahlung:<br>• **Echo-Statistiken**: Echo für das folgende Format: **[X],[Y],[Z],[Name generisches Ereignis]**<br>**[X]** = Anforderungsnummer.<br>**[Y]** = Zeichenzahl.<br>**[Z]** = Anzahl der Übereinstimmungen mit einem generischen Ereignis.<br>**[Name generisches Ereignis]** = Name, der im Feld **Name** eingegeben wurde. |

| Name | Beschreibung |
|---|---|
| | • **Echo bei allen Bytes**: Echo bei allen Bytes<br>• **Kein Echo**: Unterdrückt alle Echos |
| **Kodierungstypauswahl** | Standardmäßig zeigt die Liste nur die wichtigsten Optionen. Aktivieren Sie **Alle anzeigen**, um alle verfügbaren Kodierungen anzuzeigen. |
| **Zulässige externe IPv4-Adressen** | Bestimmen Sie die IP-Adressen, mit denen Management-Server kommunizieren können muss, um externe Ereignisse zu verwalten. Sie können damit auch IP-Adressen ausschließen, von denen Sie keine Daten möchten. |
| **Zulässige externe IPv6-Adressen** | Bestimmen Sie die IP-Adressen, mit denen Management-Server kommunizieren können muss, um externe Ereignisse zu verwalten. Sie können damit auch IP-Adressen ausschließen, von denen Sie keine Daten möchten. |

# Komponentenmenüs

## Management Client Menüs

### Menü „Datei“

Sie können Änderungen an der Konfiguration speichern und die Anwendung verlassen. Sie können Ihre Konfiguration auch sichern, siehe Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung) auf Seite 356.

### Menü bearbeiten

Sie können Änderungen rückgängig machen.

### Ansichtsmenü

| Name | Beschreibung |
|---|---|
| **Anwendungslayout** | Setzen Sie das Layout der verschiedenen Fenster im Management Client auf |

| Name | Beschreibung |
|---|---|
| **zurücksetzen** | ihre Standardeinstellungen zurück. |
| **Vorschaufenster** | Aktivieren und deaktivieren Sie das Fenster **Vorschau**, wenn Sie mit Aufzeichnungsservern und Geräten arbeiten. |
| **Aufzeichnungs-Streams anzeigen** | Standardmäßig beziehen sich die Informationen, die mit den Vorschaubildern im Fenster **Vorschau** angezeigt werden, auf die Live-Streams der Kameras. Wenn Sie stattdessen lieber Informationen zu Aufzeichnungs-Streams aufrufen möchten, wählen Sie im Menü die Option **Aufzeichnungs-Streams zeigen** aus. |
| **Hierarchie der föderalen Sites** | Standardmäßig ist das Fenster **Hierarchie der föderalen Standorte** aktiviert. |
| **Site-Navigation** | Standardmäßig ist das Fenster **Standortnavigation** aktiviert. |

### Aktionsmenü

Der Inhalt des Menüs **Aktion** unterscheidet sich je nach im **Site-Navigationsfenster** ausgewähltem Element. Die Aktionen, die Sie auswählen können, auf die Sie auch per Klick mit der rechten Maustaste auf das Element zugreifen können.

Die Vor-Pufferdauer für jede Kamera, siehe Vor-Pufferung verwalten.

| Name | Beschreibung |
|---|---|
| **Aktualisieren** | Steht immer zur Verfügung und lädt die angeforderten Informationen aus dem Management-Server neu. |

### Menü „Extras“

| Name | Beschreibung |
|---|---|
| **Registrierte Services** | Verwaltung registrierter Dienste. |

| Name | Beschreibung |
|---|---|
| | Siehe Verwaltung registrierter Dienste auf Seite 386. |
| **Effektive Rollen** | Sehen Sie sich alle Funktionen eines ausgewählten Benutzers oder einer Gruppe an. |
| **Optionen** | Offenet die Dialogbox "Optionen", in der Sie die globalen Systemeinstellungen festlegen und bearbeiten können. Weitere Informationen finden Sie unter Systemeinstellungen (die Dialogbox "Optionen") auf Seite 412. |

### Hilfe-Menü

Sie können auf das Hilfesystem und Informationen über die Version von Management Client zugreifen.

## Server Configurator (Hilfsprogramm)

### Eigenschaften der Registerkarte "Verschlüsselung"

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

> In einer Cluster-Umgebung müssen Sie Ihren Cluster einrichten und darauf achten, dass dieser läuft, bevor Sie Zertifikate für alle Computer in der Cluster-Umgebung erstellen. Danach können Sie die Zertifikate installieren und mithilfe der Server Configurator die Registrierung für alle Knoten im Cluster vornehmen. Weitere Informationen finden Sie im Zertifikate-Leitfaden dazu, wie Sie Ihre XProtect VMS Installationen sichern können.

| Name | Beschreibung | Aufgabe |
|---|---|---|
| **Serverzertifikate** | Wählen Sie das Zertifikat aus, dass zur Verschlüsselung der wechselseitigen Verbindung zwischen dem Management-Server, den Datensammlern, Log-Servern und den Aufzeichnungsservern verwendet werden soll. | Die Verschlüsselung zum und vom Managementserver aktivieren<br><br>Verschlüsselung für Aufzeichnungsserver oder Remote Server aktivieren |

| Name | Beschreibung | Aufgabe |
|---|---|---|
| **Event Server und Erweiterungen** | Wählen Sie das Zertifikat aus, das für die Verschlüsselung der wechselseitigen Verbindung zwischen dem Ereignisserver und den Komponenten verwendet werden soll, die mit dem Ereignisserver kommunizieren, einschließlich der LPR Server. | Aktivieren Sie die Verschlüsselung auf dem Ereignisserver auf Seite 328 |
| **Streamingmedienzertifikat** | Wählen Sie das Zertifikat aus, das für die Verschlüsselung der Kommunikation zwischen den Aufzeichnungsservern und allen Clients, Servern und Integrationen verwendet werden soll, die Datenstreams von den Aufzeichnungsservern abrufen. | Verschlüsselung zu Clients und Servern aktivieren |
| **Zertifikat für mobile Streamingmedien** | Wählen Sie ein Zertifikat aus, das für die Verschlüsselung der Kommunikation zwischen dem Mobile Server und den mobilen und Web Clients verwendet werden soll, die Datenstreams vom Moile Server abrufen. | Aktivieren Sie die Verschlüsselung auf dem mobilen Server. |

Server registrieren

| Name | Beschreibung | Aufgabe |
|---|---|---|
| **Management-Server-Adresse** | Die Adresse des Managementservers enthält typischerweise den Hostnamen oder den voll qualifizierten Domänennamen (FQDN) des Computers.<br>Diese Adresse ist standardmäßig nur von | Klicken Sie hier, um weitere Informationen zu den Folgen zu erhalten, wenn Sie die Adresse des Management Servers von einem Computer aus ändern, auf dem der Management Server installiert ist: |

| Name | Beschreibung | Aufgabe |
|---|---|---|
| | einem Computer im XProtect VMS aktiv, wo der Management Server nicht installiert ist.<br><br>Als Faustregel sollte die Adresse des Management Servers nicht von einem Computer aus geändert werden, auf dem der Management Server installiert ist.<br><br>Verwenden Sie jedoch z.B. den Server Configurator in einer ausfallsicheren Einrichtung, müssen Sie ggf. die Adresse von dem Computer mit dem Management Server aus ändern. Dies kann in einer ausfallsicheren Cluster-Umgebung oder in einem anderen Szenario mit ausfallsicherer Einrichtung sein.<br><br>• Zur Aktivierung des Feldes **Adresse des Managementservers** von einem Computer mit installiertem Management Server klicken Sie auf das Stiftsymbol ( ).<br><br>⚠ Wenn Sie die Adresse des Managements Servers aktualisieren, müssen Sie auf jeden der Computer zugreifen, auf denen Komponenten installiert sind, und die Adresse des Managements Servers auf die neue Adresse aktualisieren. | Ändern des Hostnamens des Management-Server-Computers |
| **Registrieren** | Registrieren Sie die Server, die auf dem Computer mit dem designierten Management Server laufen. | Registrieren eines Aufzeichnungsservers |

### Sprachauswahl

Auf dieser Registerkarte können Sie die Sprache für die Server Configurator auswählen. Die für die Server Configurator eingestellten Sprachen entsprechen den für die Management Client eingestellten Sprachen.

| Name | Beschreibung |
|---|---|
| **Wählen Sie eine Sprache aus** | Wählen Sie die Sprache für die Benutzeroberfläche aus. |

Wenn Sie in einer Failover-Cluster-Umgebung arbeiten, wird empfohlen, den Cluster anzuhalten, bevor Sie Aufgaben im Server Configurator starten. Das liegt daran, dass Server Configurator ggf. Dienste anhalten muss, während die Änderungen angewendet werden, und die Failover-Cluster-Umgebung diese Operation stören könnte.

## Status des Taskleistensymbols

Die Taskleistensymbole in der Tabelle zeigen die verschiedenen Zustände der Dienste, die auf den Servern im XProtect VMS laufen. Die Symbole stehen auf Computern, auf denen die Server installiert sind, zur Verfügung:

| Management Server Manager Taskleistensymbol | Recording Server Manager Taskleistensymbol | Event Server Manager Taskleistensymbol | Failover Recording Server Manager Taskleistensymbol | Beschreibung |
|---|---|---|---|---|
|  |  |  |  | **Läuft**<br>Erscheint, wenn ein Serverdienst aktiviert ist und gestartet wird. |

| Management Server Manager Taskleistensymbol | Recording Server Manager Taskleistensymbol | Event Server Manager Taskleistensymbol | Failover Recording Server Manager Taskleistensymbol | Beschreibung |
|---|---|---|---|---|
| | | | | Wenn der Failover Recording Server Dienst läuft, so kann er übernehmen, wenn der Standardaufzeichnungsserver ausfällt. |
|  |  |  |  | **Gestoppt**<br>Erscheint, wenn ein Serverdienst angehalten wurde.<br>Wenn der Failover Recording Server-Dienst anhält, so kann er nicht übernehmen, wenn der Standardaufzeichnungsserver ausfällt. |
|  |  |  |  | **Starte** |

| Management Server Manager Taskleistensymbol | Recording Server Manager Taskleistensymbol | Event Server Manager Taskleistensymbol | Failover Recording Server Manager Taskleistensymbol | Beschreibung |
|---|---|---|---|---|
| | | | | Erscheint, wenn ein Serverdienst dabei ist, zu starten. Unter normalen Umständen wechselt das Taskleistensymbol nach kurzer Zeit in **Läuft**. |
|  |  |  | | **Halte an**<br>Erscheint, wenn ein Serverdienst dabei ist, anzuhalten. Unter normalen Umständen wechselt das Taskleistensymbol nach kurzer Zeit in **Angehalten**. |
| |  |  | | **In unbestimmtem Zustand**<br>Erscheint, wenn der Serverdienst zunächst geladen wird, und bis die erste Information erhalten wird, worauf das Taskleistensymbol unter normalen Umständen in **Starte** wechselt, und danach in **Läuft**. |
| |  | |  | **Läuft offline**<br>Erscheint typischerweise, wenn der Aufzeichnungsserver oder der ausfallsichere Aufzeichnungsserver läuft, der Management Server Dienst jedoch nicht. |

## Dienste von Taskleistensymbolen aus starten und stoppen

Klicken Sie mit der rechten Maustaste auf die Symbole im Infobereich, um die Taskleistensymbole zu öffnen, wo Sie Dienste starten und stoppen können.

- Starten oder Stoppen des Dienstes Management Server
- Starten oder Stoppen des Dienstes Recording Server

## Management Server Manager (Taskleistensymbol)

Verwenden Sie die Menüpunkte im Management Server Manager Taskleistensymbol, um Aufgaben vom Management Server Manager auszuführen.

| Name | Beschreibung |
|---|---|
| **Start Management Server** und **Stopp Management Server** | Klicken Sie auf den jeweiligen Menüpunkt, um den Dienst Management Server zu starten oder anzuhalten. Wenn Sie den Dienst Management Server stoppen, können Sie den Management Client nicht nutzen.<br>Der Zustand des Dienstes wird durch das Taskleistensymbol angezeigt. Weitere Angaben zu den Zuständen des Taskleistensymbols finden Sie unter Taskleistensymbole für den Server Manager (Erklärung). |
| **Statusmeldungen anzeigen** | Sehen Sie eine Liste der Statusmeldungen mit Zeitstempel. |
| **Zum Ändern der Passworteinstellungen für die Systemkonfiguration** | Vergeben Sie ein Passwort für die Systemkonfiguration oder ändern Sie es. Sie können auch darauf verzichten, die Systemkonfiguration mit einem Passwort zu schützen, indem Sie ggf. vorhandene Passwörter für die Systemkonfiguration entfernen.<br>Die Passworteinstellungen für die Systemkonfiguration ändern |
| **Geben Sie das Passwort für die Systemkonfiguration ein** | Geben Sie ein Passwort ein. Dies gilt z.B., wenn die Datei mit den Passworteinstellungen gelöscht oder beschädigt wird. Näheres hierzu finden Sie unter Einstellungen für das Passwort für die Systemkonfiguration eingeben. |
| **Failover-Management-Server konfigurieren** | Starten Sie den Konfigurationsassistenten für den Failover Management Server oder öffnen Sie die Seite **Eigene Konfiguration verwalten**, um Ihre bestehende Konfiguration zu verwalten. Weitere Informationen zum Failover-Cluster finden Sie unter XProtect Management Server Failover auf Seite 39. |

| Name | Beschreibung |
|---|---|
| **Server Configurator** | Öffnen Sie das **Server Configurator**, um Server zu registrieren und die Verschlüsselung zu verwalten. Weitere Informationen dazu, wie die Verschlüsselung verwaltet wird, finden Sie unter Verschlüsselung mit dem Server Configurator verwalten. |
| **Lizenz ändern** | Ändern Sie auf dem Computer, auf dem der Managementserver läuft, den Softwarelizenzcode. Sie müssen einen neuen Softwarelizenzcode eingeben, wenn Sie z.B. Ihr XProtect System erweitern wollten. Weitere Informationen finden Sie unter Software-Lizenzcode ändern. |
| **Konfiguration wiederherstellen** | Öffnen Sie eine Dialogbox, von der aus Sie die Systemkonfiguration wiederherstellen können. Lesen Sie auf jeden Fall die in der Dialogbox enthaltenen Informationen, bevor Sie auf **Wiederherstellen** klicken. Weitere Informationen finden Sie unter Systemkonfiguration aus einer manuellen Sicherungsdatei wiederherstellen. |
| **Gemeinsamen Sicherungsordner auswählen** | Stellen Sie einen Ordner ein, in dem die Sicherheitskopie gespeichert wird, bevor Sie eine Systemkonfigurationen sichern. Weitere Informationen finden Sie unter Gemeinsamen Ordner für Sicherungskopien auswählen. |
| **SQL-Adresse aktualisieren** | Öffnen Sie einen Assistenten, um die SQL Server Adresse zu ändern. In dem seltenen Fall, dass der Hostname geändert wird, muss die SQL Server Adresse evtl. diesen Änderungen folgen. Weitere Informationen finden Sie unter Ein geänderter Hostname kann dazu führen, dass sich die Addresse des SQL-Servers ändert. |

# Basisknoten

## Lizenzangaben (Basisknoten)

In dem Fenster **Lizenzabgaben** haben Sie den Überblick über alle Lizenzen, die zur selben Softwarelizenzdatei sowohl an diesem Standort als auch an allen anderen Standorten gehören, über Ihre Milestone Care-Abonnements, und Sie können entscheiden, wie Sie ihre Lizenzen aktivieren möchten.

Näheres zu den verschiedenen Informationen und Funktionen, die in dem Fenster **Lizenzangaben** zur Verfügung gestellt werden, finden Sie unter Das Fenster "Lizenzangaben" auf Seite 133.

### Informationen zum Standort (Basisknoten)

In einer großen Milestone Federated Architecture Einrichtung mit vielen Kind-Standorten verliert man leicht den Überblick, und die Kontaktinformationen der Administratoren aller Kind-Standorte können schwer zu finden sein.

Deshalb können Sie zusätzliche Informationen zu jedem Kind-Standort hinzufügen, und diese Informationen stehen dann den Administratoren am zentralen Standort zur Verfügung.

Die folgenden Informationen können hinzugefügt werden:

- Site-Name
- Adresse/Standort
- Administrator(en)
- Weitere Informationen

## Knoten für Remote-Connect-Dienste

### Axis One-click-Kameraanschluss (der Knoten "Remote Connect Services")

Dies sind die Verbindungseigenschaften für die Axis One-Click-Kamera.

| Name | Beschreibung |
|---|---|
| **Kamerapasswort** | Eingabe/bearbeiten. Beim Kauf im Lieferumfang Ihrer Kamera enthalten. Weitere Einzelheiten finden Sie im Handbuch zu Ihrer Kamera, oder gehen Sie auf die Internetseite von Axis (https://www.axis.com/). |
| **Kamerabenutzer** | Siehe die Einzelheiten für das **Kamerapasswort**. |
| **Beschreibung** | Eingabe/Bearbeitung einer Beschreibung für die Kamera. |
| **Externe Adresse** | Eingabe/Bearbeitung der Internetadresse des ST-Servers, mit dem sich die Kamera(s) verbindet (verbinden). |

| Name | Beschreibung |
|---|---|
| **Interne Adresse** | Eingabe/Bearbeitung der Internetadresse des ST-Servers, mit dem sich der Aufzeichnungsserver verbindet. |
| **Name** | Bearbeiten Sie ggf. den Namen des Inhalts. |
| **Authentifizierungsschlüssel des Eigentümers** | Siehe **Kamerapasswort**. |
| **Passwörter** (für Dispatch Server) | Passwort eingeben. Dies muss demjenigen entsprechen, das Sie von Ihrem Systemanbieter erhalten haben. |
| **Passwörter** (für ST-Server) | Passwort eingeben. Dieses muss demjenigen entsprechen, das Sie eingegeben haben, als die Axis One-Click Connection-Komponente installiert wurde. |
| **An-/abmelden beim Axis Dispatch Service** | Geben Sie an, ob sie ihre Axis-Kamera bei Axis Dispatch Service registrieren möchten. Dies kann zum Zeitpunkt der Einrichtung oder später erfolgen. |
| **Seriennummer** | Seriennummer der Hardware, wie vom Hersteller angegeben. Die Seriennummer ist oft, aber nicht immer, mit der MAC-Adresse identisch. |
| **Anmeldedaten verwenden** | Wählen Sie das Kontrollkästchen aus, wenn Sie sich dafür entschieden haben, während der Installation des ST-Servers die Anmeldedaten zu verwenden. |
| **Benutzername** (für den Dispatch Server) | Geben Sie einen Benutzernamen ein. Der Name des Benutzers muss demjenigen entsprechen, den Sie von Ihrem Systemanbieter erhalten haben. |
| **Benutzername** (für den ST-Server) | Geben Sie den Benutzernamen ein. Dieses muss demjenigen entsprechen, das Sie eingegeben haben, als die **Axis One-Click-Connection-Komponente** installiert wurde. |

# Serverknoten

## Server (Knoten)

Dieser Abschnitt beschreibt, wie Aufzeichnungsserver und Failover-Aufzeichnungsserver installiert und konfiguriert werden. Sie lernen außerdem, wie Hardware zum System hinzugefügt und andere Seiten miteinander verbunden werden.

- Aufzeichnungsserver (Server-Knoten) auf Seite 444
- Failover Server (Server-Knoten) auf Seite 459

## Aufzeichnungsserver (Server-Knoten)

Das System verwendet Aufzeichnungsserver zum aufnehmen von Videofeeds und für die Kommunikation mit Kameras und anderen Geräten. Ein Überwachungssystem besteht typischerweise aus mehreren Aufzeichnungsservern.

Aufzeichnungsserver sind Computer, auf denen Sie die Software Recording Server installiert und sie so konfiguriert haben, dass sie mit dem Management-Server kommuniziert. Aufzeichnungsserver werden im Bereich **Übersicht** angezeigt, wenn Sie den **Server**-Ordner ausklappen und dann **Aufzeichnungsserver** auswählen.


Abwärtskompatibilität mit Aufzeichnungsservern älterer Versionen als diese Version des Management-Servers sind eingeschränkt. Sie können mit älteren Versionen immer noch auf Aufzeichnungen der Aufzeichnungsserver zugreifen, allerdings muss für eine Änderung der Konfiguration die Version mit der des Management-Servers übereinstimmen. Milestone empfiehlt, dass Sie die Versionen aller Aufzeichnungsserver in Ihrem System mit denen Ihres Management-Servers abgleichen.

### Das Fenster mit den Einstellungen des Aufzeichnungsservers

Wenn Sie mit der rechten Maustaste auf das Taskleistensymbol Recording Server Manager klicken und **Einstellungen ändern** auswählen, können Sie folgende Angaben vornehmen:

| Name | Beschreibung |
|---|---|
| **Adresse** | IP -Adresse (z.B.: 123.123.123.123) oder Hostname (z.B. "ourserver") des Management Servers, mit dem der Aufzeichnungsserver verbunden sein soll. Diese Angaben sind notwendig, damit der Aufzeichnungsserver mit dem Management Server kommunizieren kann. |
| **Port** | Die bei der Kommunikation mit dem Management-Server zu verwendende Portnummer. Der Standardport ist 9000. Bei Bedarf können Sie dies ändern. |
| **Web-Server-Port** | Zur Bearbeitung von Anfragen vom Webserver zu verwendende Portnummer, z.B. zur Bearbeitung der PTZ-Kamerasteuerungsbefehle und für Browsing- und Live-Anfragen von XProtect Smart Client. Der Standardport ist 7563. Bei Bedarf können Sie dies ändern. |
| **Alarmserverport** | Die zu verwendende Portnummer, wenn der Aufzeichnungsserver auf TCP-Informationen wartet (manche Geräte verwenden TCP zum Versenden von Ereignismeldungen). Der Standardport ist 5432 (standardmäßig deaktiviert). Bei Bedarf können Sie dies ändern. |
| **SMTP-Server-Port** | Die zu verwendende Portnummer, wenn der Aufzeichnungsserver auf Simple Mail Transfer Protocol (SMTP)-Informationen wartet. SMTP ist ein Standard zum Versenden von Benachrichtigungen zwischen Servern per E-Mail. Manche Geräte verwenden SMTP zum Versenden von Ereignismeldungen oder Bildern an den Überwachungssystemserver per E-Mail. Der Standardport ist 25; diesen können Sie aktivieren und deaktivieren. Bei Bedarf können Sie die Portnummer ändern. |
| **Verschlüsselung der Verbindungen vom Management Server zum Aufzeichnungsserver** | Bevor Sie die Verschlüsselung aktivieren und ein Zertifikat zur Serverauthentifizierung von der Liste auswählen, vergewissern Sie sich, dass Sie die Verschlüsselung auf dem Management Server zuerst aktivieren und dass dem Zertifikat des Management Servers auf den Aufzeichnungsservern vertraut wird.<br><br>Weitere Informationen finden Sie unter Sichere Kommunikation (Erklärung) auf Seite 155. |
| **Verschlüsseln Sie die Verbindungen zu Clients und Diensten, die Daten streamen** | Bevor Sie die Verschlüsselung aktivieren und ein Zertifikat zur Authentifizierung des Servers von der Liste auswählen, vergewissern Sie sich, dass dem Zertifikat auf allen Computern vertraut wird, auf denen Dienste |

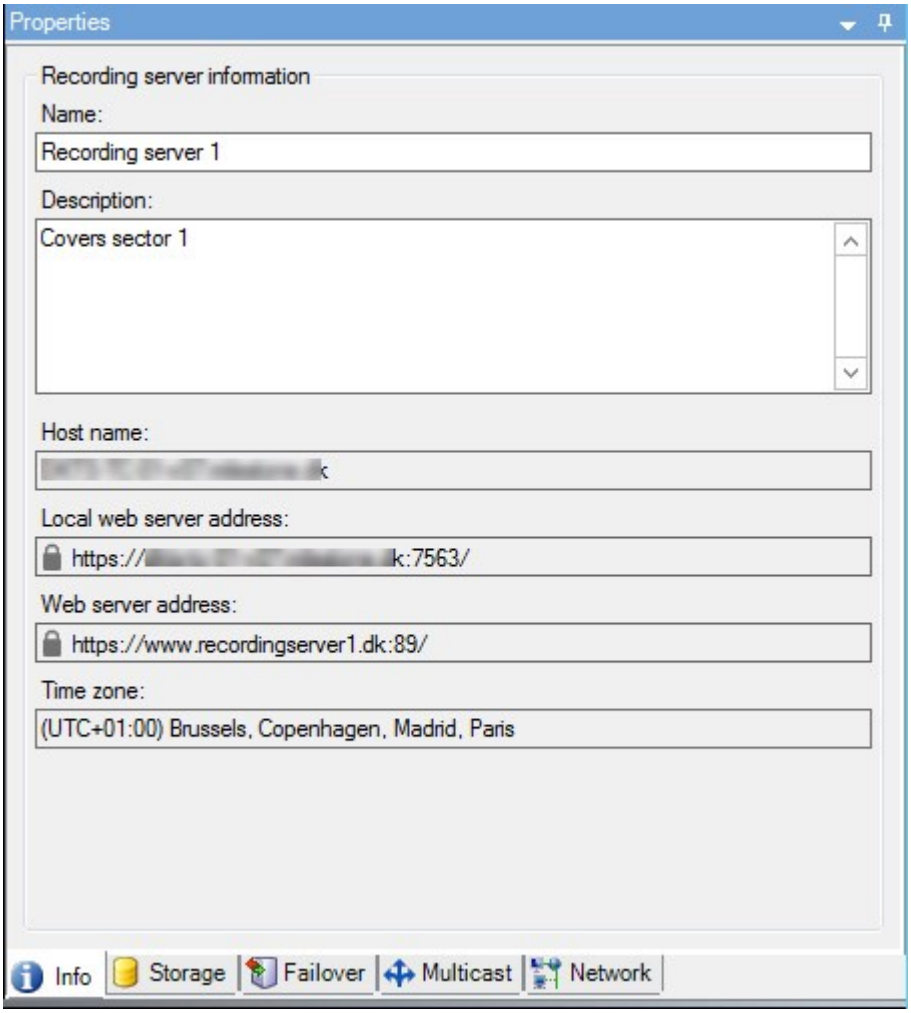
| Name | Beschreibung |
|---|---|
| | laufen, die Datenstreams vom Aufzeichnungsserver abrufen.<br>XProtect Smart Client und alle Dienste, die Datenstreams vom Aufzeichnungsserver abrufen, müssen auf die Version 2019 R1 oder höher aktualisiert werden. Manche Lösungen von Drittanbietern, die mit Hilfe von Versionen von MIP SDK erstellt wurden, die älter sind als die Version 2019 R1, müssen ggf. aktualisiert werden.<br>Weitere Informationen finden Sie unter Sichere Kommunikation (Erklärung) auf Seite 155.<br><br>Um zu überprüfen, ob Ihr Aufzeichnungsserver eine Verschlüsselung verwendet, siehe Verschlüsselungsstatus an Clients anzeigen auf Seite 313. |
| **Details** | Angaben aus dem Windows Certificate Store zu dem ausgewählten Zertifikat anzeigen. |

## Eigenschaften der Aufzeichnungsserver

### Registerkarte „Info“ (Aufzeichnungsserver)

Auf der Registerkate **Info** können Sie den Namen und die Beschreibung des Aufzeichnungsservers überprüfen oder bearbeiten.

Sie können den Host-Namen und die Adressen anschauen. Das Vorhängeschloss-Symbol vor der Adresse des Webservers zeigt die Verschlüsselung der Kommunikation mit den Clients und Diensten an, die Datenstreams von diesem Aufzeichnungsserver abrufen.




| Name | Beschreibung |
|---|---|
| **Name** | Sie können sich aussuchen, ob Sie für den Aufzeichnungsserver einen Namen eingeben wollen. Der Name wird im System und von den Clients verwendet, wenn der Aufzeichnungsserver aufgeführt ist. Der Name muss nicht einzigartig sein.<br>Wenn Sie einem Aufzeichnungsserver einen neuen Namen geben, wird der Name in Management Client global geändert. |
| **Beschreibung** | Sie können sich aussuchen, ob sie eine Beschreibung auswählen möchten, die in mehreren Listen im System auftaucht. Beschreibungen sind nicht obligatorisch. |
| **Hostname** | Zeigt den Hostnamen des Aufzeichnungsservers an. |

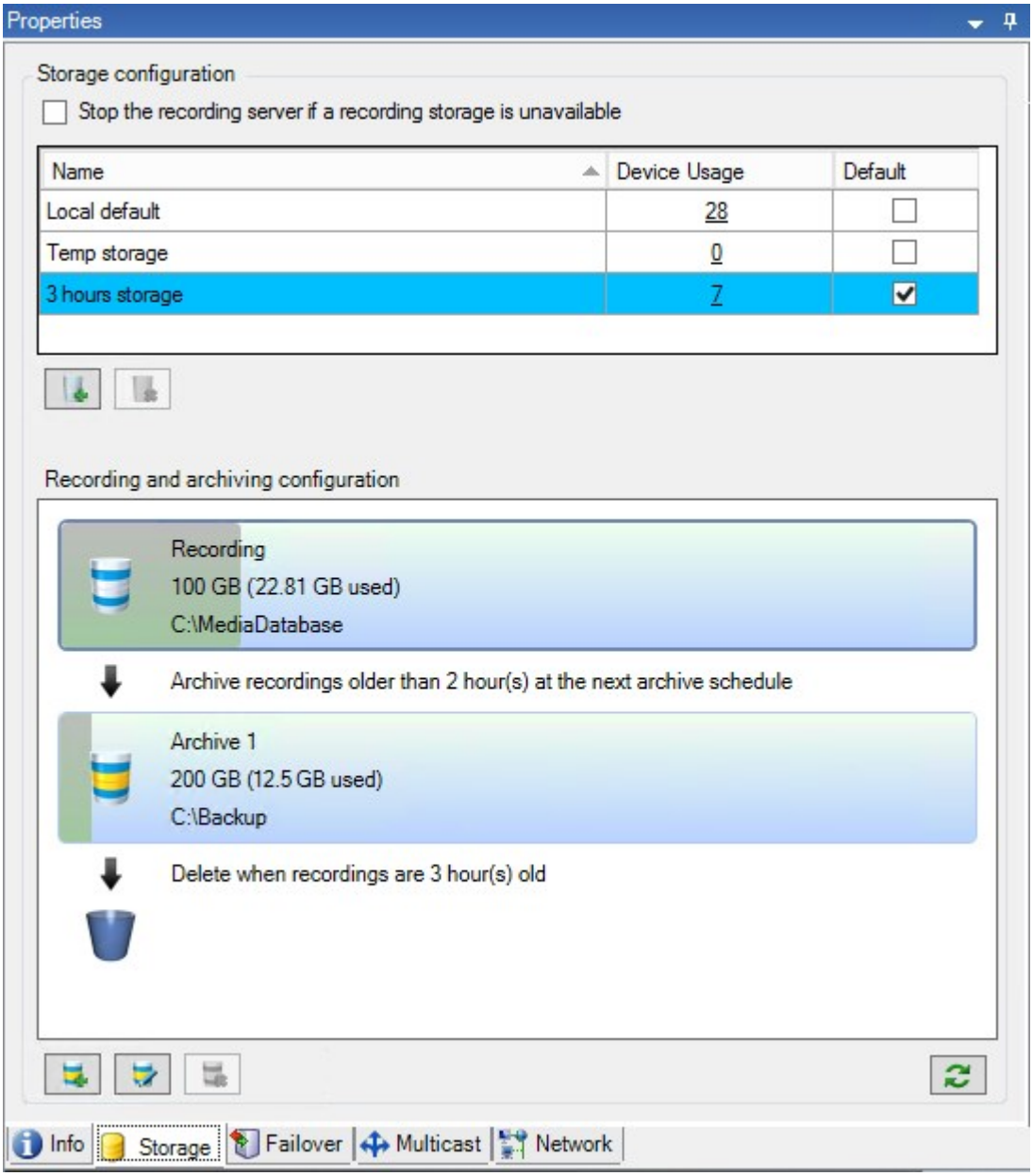
| Name | Beschreibung |
|---|---|
| **Adresse des lokalen Webservers** | Zeigt die lokale Adresse des Webservers des Aufzeichnungsservers an. Sie verwenden die lokale Adresse, zum Beispiel zur Handhabung der PTZ-Kamerasteuerungsbefehle, sowie zur Handhabung von Browsing- und Live-Anforderungen von XProtect Smart Client.<br>Die Adresse enthält die Portnummer, die für die Kommunikation mit dem Webserver verwendet wird (typischerweise Port 7563).<br>Wenn Sie die Verschlüsselung zu Clients und Servern aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, erscheint ein Vorhängeschloss-Symbol, und die Adresse enthält **https** anstelle von **http**. |
| **Adresse des Web-Servers** | Zeigt die öffentliche Adresse des Webservers des Aufzeichnungsservers über das Internet an.<br>Falls Ihre Installation eine Firewall oder einen NAT-Router verwendet, geben Sie bitte die Adresse der Firewall oder des NAT-Routers ein, damit die Clients, die auf das Überwachungssystem im Internet zugreifen, sich mit dem Aufzeichnungsserver verbinden können.<br>Die öffentliche Adresse und die Portnummer geben Sie auf der Registerkarte **Netzwerk** an.<br>Wenn Sie die Verschlüsselung zu Clients und Servern aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, erscheint ein Vorhängeschloss-Symbol, und die Adresse enthält **https** anstelle von **http**. |
| **Zeitzone** | Zeigt die Zeitzone an, in der sich der Aufzeichnungsserver befindet. |

### Registerkarte „Speicher“ (Aufzeichnungsserver)

Auf der Registerkarte **Speicher** können Sie Aufzeichnungen für einen ausgewählten Aufzeichnungsserver einrichten, verwalten und anzeigen.

Zur Aufzeichnung von Speicher und Archiven zeigt die horizontale Leiste die aktuelle Menge an Speicherplatz an. Sie können das Verhalten des Aufzeichnungsservers für den Fall angeben, dass Aufzeichnungsspeicher nicht mehr verfügbar sind. Dies ist vor allem wichtig, wenn Ihr System Failover-Server beinhaltet.

Bei Verwendung von **Beweissicherung** zeigt eine vertikale rote Linie an, welcher Speicherplatz für Aufnahmen mit Beweissicherung verwendet wird.




**Speicher- und Aufzeichnungseinstellungen (Eigenschaften)**

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Geben Sie im Dialogfeld **Speicher- und Aufzeichnungseinstellungen** Folgendes an:

| Name | Beschreibung |
|---|---|
| **Name** | Benennen Sie den Speicher um, falls erforderlich. Die Namen müssen eindeutig sein. |
| **Pfad** | Geben Sie den Pfad zu dem Verzeichnis an, in dem Sie Aufzeichnungen in diesem Speicher speichern. Der Speicher muss sich nicht unbedingt auf dem Aufzeichnungsserver-Computer befinden.<br><br>Wenn das Verzeichnis nicht vorhanden ist, können Sie es erstellen. Netzwerklaufwerke müssen mit dem UNC-Format (Universal Naming Convention) benannt werden, beispielsweise: `\\server\volume\directory\`. |
| **Speicherzeit** | Geben Sie an, wie lange Aufzeichnungen im Archiv bleiben sollen, bevor sie gelöscht oder ins nächste Archiv verschoben werden (je nach Archiveinstellungen).<br><br>Die Speicherzeit muss immer länger als die Speicherzeit des bisherigen Archivs oder der Standard-Aufzeichnungsdatenbank sein. Der Grund dafür ist, dass die Zahl der Speichertage, die für ein Archiv angegeben sind, alle Speicherzeiten beinhaltet, die früher im Prozess angegeben wurden. |
| **Maximale Größe** | Wählen Sie die maximale Gigabyte-Anzahl an Aufzeichnungsdaten aus, die in der Aufzeichnungsdatenbank gespeichert werden sollen.<br><br>Aufzeichnungsdaten, die die angegebene Gigabyte-Anzahl überschreiten, werden automatisch ins erste Archiv auf der Liste verschoben – sofern eines angegeben ist – oder gelöscht.<br><br>⚠ Wenn weniger als 5 GB Speicherplatz frei sind, archiviert das System immer die ältesten Daten in einer Datenbank bzw. löscht diese, wenn kein nächstes Archiv angegeben ist. Wenn weniger als 1 GB frei ist, werden die Daten gelöscht. Eine Datenbank erfordert 250 MB an freiem Speicherplatz. Wenn dieser Grenzwert erreicht wird (wenn Daten nicht schnell genug gelöscht werden), werden erst dann wieder Daten in die Datenbank geschrieben, wenn Sie genügend Platz freigegeben haben. Die tatsächliche Maximalgröße Ihrer Datenbank entspricht der Anzahl der angegebenen Gigabyte minus 5 GB. |
| **Wird signiert** | Ermöglicht eine digitale Signatur für die Aufzeichnungen. Das heißt beispielsweise, |

| Name | Beschreibung |
|---|---|
| | dass das System bestätigt, dass das exportierte Video nicht verändert oder bei der Wiedergabe manipuliert wurde.<br>Das System verwendet den SHA-2-Algorithmus für digitale Signaturen. |
| **Verschlüsselung** | Wählen Sie den Verschlüsselungsgrad der Aufnahmen aus:<br>• Keine<br>• Schwach (weniger CPU-Auslastung)<br>• Stark (Höhere CPU-Auslastung)<br>Das System verwendet den AES-256-Algorithmus zur Verschlüsselung.<br>Bei Auswahl von **Schwach** wird ein Teil der Aufzeichnung verschlüsselt. Bei Auswahl von **Stark** wird die gesamte Aufzeichnung verschlüsselt.<br>Wenn Sie Verschlüsselung aktivieren, müssen Sie nachfolgend auch ein Passwort angeben. |
| **Passwort** | Geben Sie ein Passwort für die Benutzer an, die verschlüsselte Daten anzeigen dürfen.<br>Milestone empfiehlt die Nutzung sicherer Passwörter. Sichere Passwörter enthalten keine Wörter, die in Wörterbüchern zu finden sind oder Bestandteil des Namens des Benutzers sind. Sie umfassen acht oder mehr alphanumerische Zeichen, Groß- und Kleinbuchstaben und Sonderzeichen. |

#### Eigenschaften der Archiveinstellungen

Geben Sie im Dialogfeld **Archiveinstellungen** Folgendes an:

| Name | Beschreibung |
|---|---|
| **Name** | Benennen Sie den Speicher um, falls erforderlich. Die Namen müssen eindeutig sein. |
| **Pfad** | Geben Sie den Pfad zu dem Verzeichnis an, in dem Sie Aufzeichnungen in diesem Speicher speichern. Der Speicher muss sich nicht unbedingt auf dem |

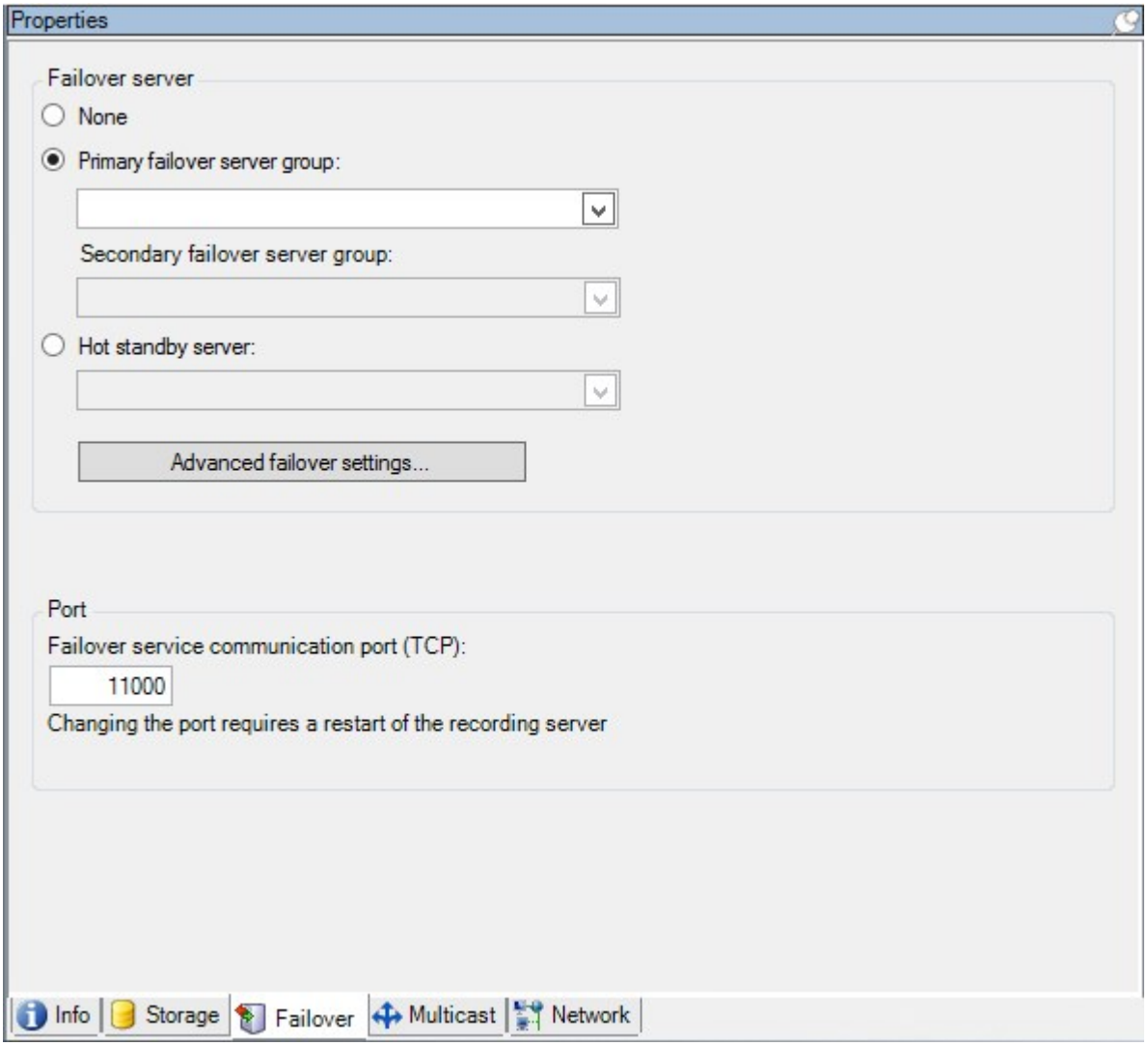
| Name | Beschreibung |
|---|---|
| | Aufzeichnungsserver-Computer befinden.<br><br>Wenn das Verzeichnis nicht vorhanden ist, können Sie es erstellen. Netzwerklaufwerke müssen mit dem UNC-Format (Universal Naming Convention) benannt werden, beispielsweise: `\\server\volume\directory\`. |
| **Speicherzeit** | Geben Sie an, wie lange Aufzeichnungen im Archiv bleiben sollen, bevor sie gelöscht oder ins nächste Archiv verschoben werden (je nach Archiveinstellungen).<br><br>Die Speicherzeit muss immer länger als die Speicherzeit des bisherigen Archivs oder der Standard-Aufzeichnungsdatenbank sein. Der Grund dafür ist, dass die Zahl der Speichertage, die für ein Archiv angegeben sind, alle Speicherzeiten beinhaltet, die früher im Prozess angegeben wurden. |
| **Maximale Größe** | Wählen Sie die maximale Gigabyte-Anzahl an Aufzeichnungsdaten aus, die in der Aufzeichnungsdatenbank gespeichert werden sollen.<br><br>Aufzeichnungsdaten, die die angegebene Gigabyte-Anzahl überschreiten, werden automatisch ins erste Archiv auf der Liste verschoben – sofern eines angegeben ist – oder gelöscht.<br><br>⚠ Wenn weniger als 5 GB Speicherplatz frei sind, archiviert das System immer die ältesten Daten in einer Datenbank bzw. löscht diese, wenn kein nächstes Archiv angegeben ist. Wenn weniger als 1 GB frei ist, werden die Daten gelöscht. Eine Datenbank erfordert 250 MB an freiem Speicherplatz. Wenn dieser Grenzwert erreicht wird (wenn Daten nicht schnell genug gelöscht werden), werden erst dann wieder Daten in die Datenbank geschrieben, wenn Sie genügend Platz freigegeben haben. Die tatsächliche Maximalgröße Ihrer Datenbank entspricht der Anzahl der angegebenen Gigabyte minus 5 GB. |
| **Zeitplan** | Legen Sie einen Archiv-Zeitplan fest, der die zeitlichen Abstände enthält, in denen der Archivierungsprozess gestartet wird. Sie können sehr häufig (im Allgemeinen einmal pro Stunde an 365 Tagen im Jahr) oder sehr selten (zum Beispiel an jedem ersten Montag alle 36 Monate) archivieren. |
| **Bildrate reduzieren** | Wenn Sie bei der Archivierung die Bildrate verringern möchten, wählen Sie die Option **Bildrate reduzieren** und legen Sie die Bilder pro Sekunde (FPS) fest. |

| Name | Beschreibung |
|---|---|
| | Durch eine Reduzierung der Bildraten mit einem bestimmten FPS-Wert nehmen Ihre Aufzeichnungen im Archiv weniger Platz in Anspruch. Gleichzeitig verringert sich jedoch auch die Bildqualität im Archiv.<br>MPEG-4/H.264/H.265 sorgt für eine automatische Minimierung auf Keyframes.<br>0,1 = 1 Bild pro 10 Sekunden. |

Registerkarte „Failover“ (Aufzeichnungsserver)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Wenn Ihr Unternehmen Failover-Aufzeichnungsserver nutzt, können Sie die Registerkarte **Failover** verwenden, um Aufzeichnungsservern Failover-Server zuzuweisen. Siehe Eigenschaften der Registerkarte „Failover“.




Einzelheiten Failover-Aufzeichnungsserver, Installation und Einstellungen, Failover-Gruppen und deren Einstellungen finden Sie unter Der ausfallsichere Aufzeichnugnsserver (Erklärung) auf Seite 40.

**Eigenschaften der Registerkarte „Failover“**

| Name | Beschreibung |
|---|---|
| **Keine** | Wählen Sie eine Einrichtung ohne Failover-Aufzeichnungsserver aus. |
| **Primäre Failover-** | Wählen Sie eine reguläre Failover-Einrichtung mit einer primären und |

| Name | Beschreibung |
|---|---|
| **Servergruppe/Sekundäre Failover-Servergruppe** | möglicherweise einer zweiten Failover-Servergruppe aus. |
| **Hot-Standby-Server** | Wählen Sie eine Hot-Standby-Einrichtung mit einem dedizierten Aufzeichnungsserver als Hot-Standby-Server aus. |
| **Erweiterte Failover-Einstellungen** | Öffnet das Fenster **Erweiterte Failover-Einstellungen**:<br>• **Vollständiger Support**: Aktiviert vollständige Failover-Unterstützung für das Gerät<br>• **Nur live**: Aktiviert Failover-Unterstützung ausschließlich für Live-Streams auf dem Gerät<br>• **Deaktiviert**: Deaktiviert Failover-Unterstützung für das Gerät |
| **Kommunikationsport des Failover-Dienstes (TCP)** | Die standardmäßige Portnummer lautet 11000. Dieser Port wird für die Kommunikation zwischen Aufzeichnungsservern und Failover-Aufzeichnungsservern verwendet. Wenn Sie den Port ändern, **muss** der Aufzeichnungsserver ausgeführt werden und **muss** mit dem Management-Server verbunden sein. |

### Registerkarte „Multicast“ (Aufzeichnungsserver)

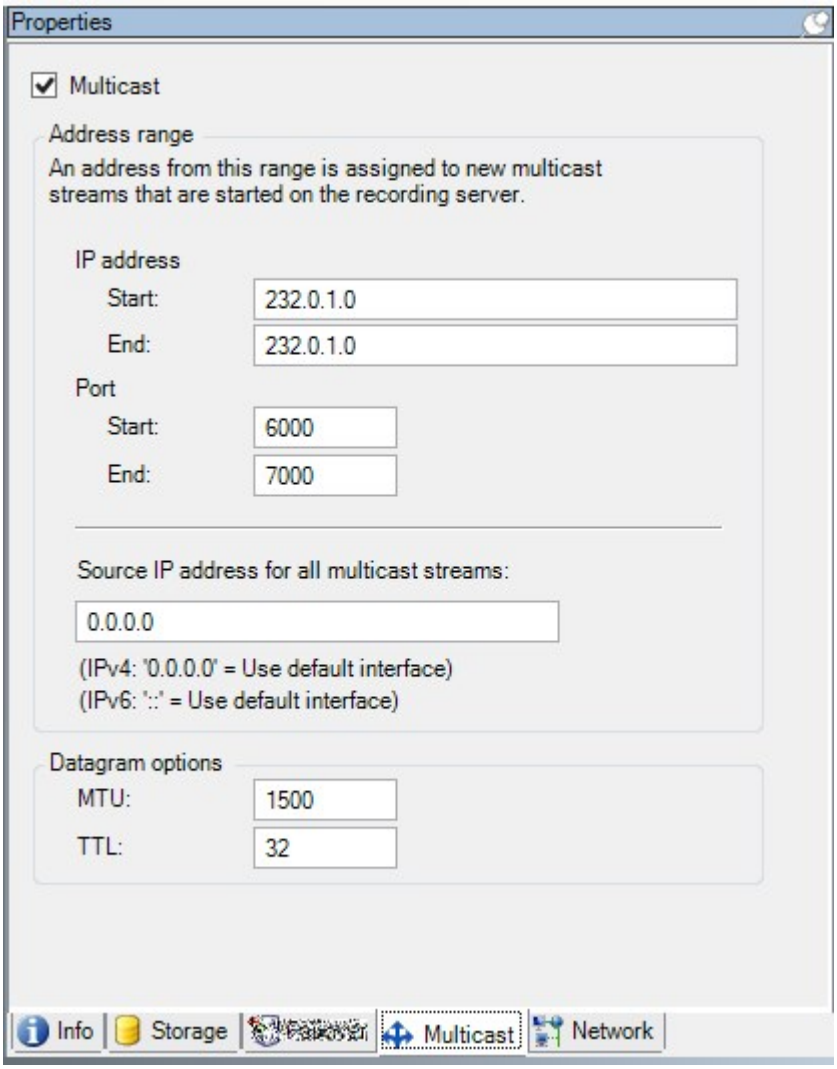
Ihr System unterstützt Multicasting von Live-Streams über Ihre Aufzeichnungsserver. Falls mehrere XProtect Smart Client-Benutzer das Live-Video von derselben Kamera sehen möchten, können mit Hilfe von Multicast wertvolle Systemressourcen eingespart werden. Multicast ist besonders bei der Nutzung der Matrix Funktionalität von großer Bedeutung, da hierbei mehrere Clients Live-Videodaten von derselben Kamera erfordern.

Multicast ist nur möglich für Live-Streams, nicht jedoch für aufgezeichnete Video-/Audio-Dateien.

Wenn ein Aufzeichnungsserver über mehr als eine Netzwerkkarte verfügt, kann Multicast nur auf einer von ihnen aktiviert werden. Im Management Client können Sie festlegen, welche Karte Sie verwenden möchten.

Wenn Sie Failover-Server verwenden, denken Sie daran, auch die IP-Adresse der Netzwerkschnittstellenkarte des Failover Servers anzugeben (siehe Registerkarte Multicast (Failover-Server) auf Seite 462).

Eine erfolgreiche Implementierung von Multicasting setzt zudem voraus, dass Sie Ihre Netzwerkausrüstung so einrichten, dass Multicast-Datenpakete ausschließlich an die gewünschte Gruppe von Empfängern übertragen werden. Wenn nicht, kann es vorkommen, dass sich Multicasting nicht von Broadcasting unterscheidet, wodurch sich die Geschwindigkeit im Netzwerk möglicherweise deutlich reduziert.



### Zuweisen eines IP-Adressbereichs

Legen Sie den Bereich fest, den Sie als Adressen für Multicast-Streams des ausgewählten Aufzeichnungsservers zuweisen möchten. Wenn Benutzer Multicast-Video von diesem Aufzeichnungsserver anzeigen, stellen die Clients Verbindungen mit diesen Adressen her.

Für jeden Multicast-Kamera-Feed müssen die IP-Adresse und die Port-Kombination eindeutig sein (Beispiel für IPv4: 232.0.1.0:6000). Sie können entweder eine IP-Adresse und viele Ports oder viele IP-Adressen und weniger Ports verwenden. Standardmäßig schlägt das System eine einzelne IP-Adresse und einen Bereich von 1.000 Ports vor; Sie können die Einstellungen jedoch bei Bedarf ändern.

IP-Adressen für Multicasting müssen sich im von IANA für dynamische Hostzuordnung definierten Bereich befinden. IANA ist die Organisation, die für die Überwachung der globalen Vergabe von IP-Adressen zuständig ist.

| Name | Beschreibung |
|---|---|
| **IP-Adresse** | Geben Sie im Feld **Start** die erste IP-Adresse des gewünschten Bereichs an. Geben Sie dann im Feld **Ende** die letzte IP-Adresse des gewünschten Bereichs an. |
| **Port** | Geben Sie im Feld **Start** die erste Portnummer des gewünschten Bereichs an. Geben Sie dann im Feld **Ende** die letzte Portnummer des gewünschten Bereichs an. |
| **Quell-IP-Adresse für alle Multicast-Streams** | Sie können Multicast nur auf einer Netzwerkkarte aktivieren. Dieses Feld ist also relevant, wenn Ihr Aufzeichnungsserver über mehr als eine Netzwerkkarte verfügt oder eine Netzwerkkarte mit mehr als einer IP-Adresse aufweist.<br>Wenn Sie die Standardschnittstelle des Aufzeichnungsservers verwenden möchten, belassen Sie den Wert im Feld bei 0.0.0.0 (IPv4) oder :: (IPv6). Wenn Sie eine andere Netzwerkkarte bzw. eine andere IP-Adresse auf der gleichen Netzwerkkarte nutzen möchten, geben Sie die IP-Adresse der gewünschten Schnittstelle an.<br>• IPv4: 224.0.0.0 bis 239.255.255.255.<br>• IPv6, der Bereich wird auf der IANA-Website beschrieben (https://www.iana.org/). |

### Festlegen von Datagramm-Optionen

Legen Sie die Einstellungen für Datenpakete (Datagramme) fest, die über Multicasting übertragen werden sollen.

| Name | Beschreibung |
|---|---|
| **MTU** | Maximale Übertragungseinheit, also die maximal zulässige physische Datenpaketgröße (gemessen in Byte). Nachrichten, die größer als der angegebene MTU-Wert sind, werden vor dem Senden in kleinere Pakete aufgeteilt. Der Standardwert lautet 1500; dies ist auch bei den meisten Windows-Computern und Ethernet-Netzwerken der Standardwert. |
| **TTL** | Gültigkeitsdauer (Time To Live), also die maximal zulässige Zahl an Hops, die ein Datenpaket zurücklegen darf, bevor es verworfen oder zurückgesendet wird. Ein Hop ist ein Punkt zwischen zwei Netzwerkgeräten (meist ein Router). Der Standardwert ist 128. |

### Registerkarte „Netzwerk“ (Aufzeichnungsserver)

> Wenn Sie auf das VMS mit XProtect Smart Client über ein öffentliches oder nicht vertrauenswürdiges Netzwerk zugreifen müssen, Milestone sollten Sie eine sichere Verbindung über VPN verwenden. So wird gewährleistet, dass die Kommunikation zwischen XProtect Smart Client und dem VMS-Server geschützt ist.

Die öffentliche IP-Adresse eines Aufzeichnungsservers legen Sie auf der Registerkarte **Netzwerk** fest.

**Wozu dient eine öffentliche Adresse?**

Clients können Verbindungen über das lokale Netzwerk oder das Internet herstellen. In beiden Fällen muss das Überwachungssystem dazu in der Lage sein, geeignete Adressen bereitzustellen, damit Clients auf Live-Videos und Videoaufzeichnungen der Aufzeichnungsserver zugreifen können:

- Wenn Clients eine lokale Verbindung herstellen, muss das Überwachungssystem mit lokalen Adressen und Portnummern antworten
- Wenn Clients eine Verbindung über das Internet herstellen, muss das Überwachungssystem mit der öffentlichen Adresse des Aufzeichnungsservers antworten. Dies ist die Adresse der Firewall oder des NAT-Routers (Network Address Translation) und oftmals auch eine andere Portnummer. Die Adresse und der Port können dann an die lokale Adresse und den lokalen Port des Servers weitergeleitet werden.

## Failover Server (Server-Knoten)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Ein Failover-Aufzeichnungsserver ist ein zusätzlicher Aufzeichnungsserver, der die Arbeit des eigentlichen Aufzeichnungsservers übernimmt, falls dieser nicht mehr verfügbar ist. Sie können einen Failover-Aufzeichnungsserver in zwei Modi konfigurieren, als **Cold-Standby-Server** oder als **Hot-Standby-Server**.

Sie installieren ausfallsichere Aufzeichnungsserver wie Standard-Aufzeichnungsserver (siehe Installation eines Failover-Aufzeichnungsservers Download Manager auf Seite 181). Sobald Sie Failover-Aufzeichnungsserver installiert haben, werden diese im Management Client angezeigt. Milestone empfiehlt die Installation aller Failover-Aufzeichnungsserver auf separaten Computern. Achten Sie darauf, dass sie Failover-Aufzeichnungsserver mit der korrekten IP-Adresse/dem korrekten Hostnamen des Management-Servers konfigurieren. Die Benutzerberechtigungen für das Benutzerkonto, unter dem der Failover-Server-Dienst ausgeführt wird, werden bei der Installation gegeben. Dies sind:

- Start-/Stopp- Berechtigungen zu starten oder stoppen des ausfallsicheren Aufzeichnungsservers
- Lesende und schreibende Zutrittsberechtigung zum Lesen und Schreiben in der Datei RecorderConfig.xml

Wird für die Verschlüsselung ein Zertifikat ausgewählt, so muss der Administrator dem Benutzer auf dem ausgewählten Zertifikate-Privatschlüssel des Failover-Servers die Lesezugriffsberechtigung geben.

Wenn der Failover-Aufzeichnungsserver von einem Aufzeichnungsserver übernimmt, der eine Verschlüsselung verwendet, so empfiehlt Milestone, dass Sie den Failover-Aufzeichnungsserver ebenfalls dafür vorbereiten, dass er eine Verschlüsselung verwendet. Weitere Informationen finden Sie unter Sichere Kommunikation (Erklärung) auf Seite 155 und Installation eines Failover-Aufzeichnungsservers Download Manager auf Seite 181.

Sie können bestimmen, welche Art von Failover-Unterstützung Sie auf Geräteebene möchten. Für jedes Gerät auf einem Aufzeichnungsserver können Sie vollständige, teilweise oder keine Failover-Unterstützung auswählen. So können Sie Ihren Failover-Ressourcen Prioritäten zuweisen und Failover beispielsweise nur für Video- und nicht für Audiokanäle einrichten oder Failover nur auf wichtigen Kameras haben.

Während ihr System im Failover-Modus ist, können Sie keine Hardware ersetzen oder umziehen, den Aufzeichnungsserver aktualisieren oder Gerätekonfigurationen ändern, wie zum Beispiel Speicherungseinstellungen oder Einstellungen für Videostreams.

**Cold-Standby-Failover-Aufzeichnungsserver**

Bei einem Cold-Standby-Failover-Aufzeichnungsserver gruppieren Sie mehrere Failover-Aufzeichnungsserver in einer Failover-Gruppe. Die gesamte Failover-Gruppe dient dem Zweck, mehrere vorab ausgewählte Aufzeichnungsserver abzulösen, wenn einer von ihnen nicht mehr verfügbar sein sollte. Sie können so viele Gruppen erstellen, wie Sie wollen (siehe Gruppieren von Failover-Aufzeichnungsservern für Cold-Standby auf Seite 227).

Gruppen haben einen klaren Vorteil: Wenn Sie später bestimmen, welche Failover-Aufzeichnungsserver einen Aufzeichnungsserver ablösen sollen, wählen Sie einfach eine Gruppe von Failover-Aufzeichnungsservern aus. Falls die ausgewählte Gruppe aus mehr als einem Failover-Aufzeichnungsserver besteht, haben Sie zur Sicherheit mehr als einen Failover-Aufzeichnungsserver zur Ablösung in Bereitschaft, falls ein Aufzeichnungsserver nicht mehr verfügbar sein sollte. Sie können eine sekundäre Failover-Server-Gruppe bestimmen, welche die Aufgaben der primären Gruppe übernimmt, sollten alle Aufzeichnungsserver der primären Gruppe ausgelastet sein. Ein Failover-Aufzeichnungsserver kann nicht Teil mehrerer Gruppen sein.

Failover-Aufzeichnungsserver in einer Failover-Gruppe sind in einer Sequenz angeordnet. Die Sequenz bestimmt die Reihenfolge, in der die Failover-Aufzeichnungsserver einen Aufzeichnungsserver ablösen. Standardmäßig entspricht die Sequenz der Reihenfolge, in der Sie die Failover-Aufzeichnungsserver in die Failover-Gruppe aufgenommen haben: Der zuerst aufgenommene Server ist der erste in der Sequenz. Bei Bedarf können Sie dies ändern.

**Hot-Standby-Failover-Aufzeichnungsserver**

Bei einem Hot-Standby-Failover-Aufzeichnungsserver bestimmen Sie einen Failover-Aufzeichnungsserver, der nur **einen** Aufzeichnungsserver ablöst. So kann das System diesen Failover-Aufzeichnungsserver im „Standby"-Modus behalten, sodass er mit der korrekten/aktuellen Konfiguration des ihm zugewiesenen Aufzeichnungsservers synchronisiert wird und viel schneller zur Ablösung bereit ist als ein Cold-Standby-Failover-Aufzeichnungsserver. Wie bereits erwähnt, weisen Sie Hot-Standby-Server nur einem Aufzeichnungsserver zu und können sie nicht gruppieren. Sie können Failover-Server, die bereits Teil einer Failover-Gruppe sind, nicht zu Hot-Standby-Aufzeichnungsservern machen.

**Validierung ausfallsicherer Aufzeichnungsserver**

Um zusammengeführte Videodaten vom ausfallsicheren Server auf dem Aufzeichnungsserver zu validlieren müssen Sie dafür sorgen, dass der Aufzeichnungsserver nicht erreichbar ist, indem Sie entweder den Aufzeichnungsserverdienst anhalten oder den Computer abschalten, auf dem der Aufzeichnungsserver installiert ist.

> ⚠ Eine manuelle Unterbrechung des Netzwerks, die Sie dadurch verursachen können, dass Sie das Netzwerkkabel abziehen oder das Netzwerk mit einem Prüfwerkzeug blockieren, ist keine gültige Methode.

### Eigenschaften der Registerkarte "Info" (Failover-Server)

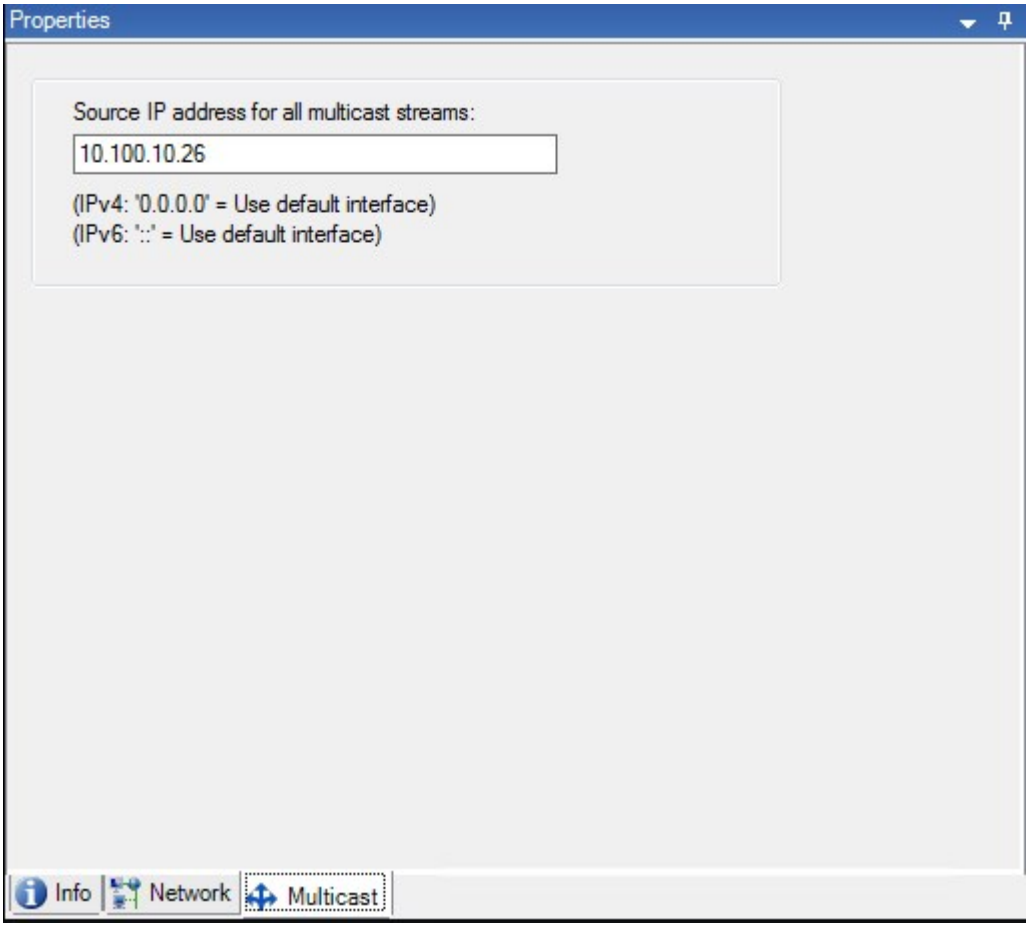
Geben Sie die folgenden Eigenschaften von Failover-Aufzeichnungsservern an:

| Name | Beschreibung |
|---|---|
| **Name** | Der Name des Failover-Aufzeichnungsservers, wie er in Management Client, Protokollen und andernorts auftaucht. |
| **Beschreibung** | Ein optionales Feld, in dem Sie den Failover-Aufzeichnungsserver beschreiben können, z. B. für welchen Aufzeichnungsserver er übernimmt. |
| **Hostname** | Zeigt den Hostnamen des Failover-Aufzeichnungsservers an. Sie können diese nicht ändern. |
| **Adresse des lokalen Webservers** | Zeigt die lokale Adresse des Webservers des Failover-Aufzeichnungsservers an. Sie verwenden die lokale Adresse, zum Beispiel zur Handhabung der PTZ-Kamerasteuerungsbefehle, sowie zur Handhabung von Browsing- und Live-Anforderungen von XProtect Smart Client.<br><br>Die Adresse enthält die Portnummer, die für die Kommunikation mit dem Webserver verwendet wird (typischerweise Port 7563).<br><br>Wenn der Failover-Aufzeichnungsserver von einem Aufzeichnungsserver übernimmt, der eine Verschlüsselung verwendet, müssen Sie auch den Failover-Aufzeichnungsserver so vorbereiten, dass er eine Verschlüsselung verwendet.<br><br>Wenn Sie die Verschlüsselung zu Clients und Servern aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, erscheint ein Vorhängeschloss-Symbol, und die Adresse enthält **https** anstelle von **http**. |
| **Adresse des Web-Servers** | Zeigt die öffentliche Adresse des Webservers des Failover-Aufzeichnungsservers im Internet an.<br><br>Wenn Ihre Installation eine Firewall oder einen NAT-Router verwendet, geben Sie die Adresse der Firewall oder des NAT-Routers ein, damit Clients, die über das Internet auf das Überwachungssystem zugreifen, sich mit dem Failover-Aufzeichnungsserver |

| Name | Beschreibung |
|---|---|
| | verbinden können.<br>Die öffentliche Adresse und die Portnummer geben Sie auf der Registerkarte **Netzwerk** an.<br>Wenn Sie die Verschlüsselung zu Clients und Servern aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, erscheint ein Vorhängeschloss-Symbol, und die Adresse enthält **https** anstelle von **http**. |
| **UDP-Port** | Über diese Portnummer kommunizieren die Failover-Aufzeichnungsserver. Die Standardeinstellung ist Port 8844. |
| **Speicherort der Datenbank** | Bestimmen Sie den vom Failover-Aufzeichnungsserver zur Speicherung von Aufzeichnungen verwendeten Pfad zur Datenbank.<br>Sie können den Datenbankpfad nicht ändern, während der Failover-Aufzeichnungsserver für einen Aufzeichnungsserver übernimmt. Das System wendet die Änderungen an, wenn der Failover-Aufzeichnungsserver nicht mehr für einen Aufzeichnungsserver übernimmt. |
| **Diesen Failover-Server aktivieren** | Abwählen, um den Failover-Aufzeichnungsserver zu deaktivieren (standardmäßig ausgewählt). Sie müssen Failover-Aufzeichnungsserver deaktivieren, bevor sie Aufzeichnungsserver ablösen können. |

### Registerkarte Multicast (Failover-Server)

Wenn Sie Failover-Server verwenden und Multicasting von Live-Streaming aktiviert wurde, müssen Sie die IP-Adressen der Netzwerkkarten sowohl auf den Aufzeichnungsserver und den Failover-Server festlegen.




Weitere Informationen zu Berichten finden Sie unter Aktivieren Sie Multicasting für den Recording-Server auf Seite 222.

### Eigenschaften der Registerkarte "Info" (Failover-Gruppe)

| Feld | Beschreibung |
|---|---|
| **Name** | Der Name der Failover-Gruppe, wie er im Management Client, Protokollen und andernorts auftaucht. |
| **Beschreibung** | Eine optionale Beschreibung, z. B. der physische Serverstandort. |

Eigenschaften der Registerkarte "Sequenz" (Failover-Gruppe)

| Feld | Beschreibung |
|---|---|
| **Failover-Sequenz angeben** | Verwenden Sie **Nach oben** und **Nach unten**, um die gewünschte Sequenz der regulären Failover-Aufzeichnungsserver in der Gruppe festzulegen. |

## Remote Server für Milestone Interconnect

Milestone Interconnect™ erlaubt Ihnen die Integration einer Anzahl kleiner, physisch fragmentierter und entfernter XProtect Installationen mit einer XProtect Corporate zentralen Seite. Sie können diese kleineren Standorte (Remote-Systeme) mobil mitführen, z. B. auf Booten, Bussen oder Zügen. Das bedeutet, dass solche Standorte nicht permanent mit einem Netzwerk verbunden sein müssen.

Registerkarte „Info (Remote-Server)“

| Name | Beschreibung |
|---|---|
| **Name** | Das System verwendet den Namen, wenn der Remote-Server im System und den Clients aufgelistet wird. Der Name muss nicht einzigartig sein.<br>Wenn Sie einen Server neu benennen, wird der Name im Management Client global geändert. |
| **Beschreibung** | Geben Sie eine Beschreibung des Remote-Servers ein (optional).<br>Die Beschreibung taucht in einer Anzahl Listen im System auf. Zum Beispiel, wenn Sie den Mauszeiger über den Hardware-Namen im Bereich **Übersicht** halten. |
| **Modell** | Zeigt das am Remote-System installierte XProtect-Produkt an. |
| **Version** | Zeigt die Version des Remote-Systeminstallation an. |
| **Softwarelizenzcode** | Der Softwarelizenzcode des Remote-Systeminstallation. |

| Name | Beschreibung |
|---|---|
| **Treiber** | Identifiziert den Treiber, der die Verbindung mit dem Remote-Server verwaltet. |
| **Adresse** | Hostname oder IP-Adresse der Hardware. |
| **IE** | Öffnet die Standard-Startseite des Hardware-Anbieters. Sie können diese Seite zur Administration der Hardware oder des Systems nutzen. |
| **Remote-Systeminstallation-ID** | Die einzigartige System-ID des Remote-Systeminstallation, die von XProtect verwendet wird, um beispielsweise Lizenzen zu verwalten. |

### Registerkarte "Einstellungen" (Remote Server)

Auf der Registerkarte **Einstellungen** können Sie den Namen des entfernten Systems sehen.

### Registerkarte „Ereignisse (Remote-Server)“

Sie können Ereignisse aus dem Remote-System in Ihrem zentralen Standort hinzufügen, um Regeln zu erstellen und dadurch sofort auf Ereignisse im Remote-Systeminstallation zu reagieren. Die Anzahl der Ereignisse hängt von den konfigurierten Ereignissen im Remote-Systeminstallation ab. Sie können Standardereignisse nicht löschen.

Falls die Liste unvollständig sein sollte:

1. Klicken Sie mit der rechten Maustaste auf den relevanten Remote-Server im Bereich **Übersicht** und wählen Sie **Hardware aktualisieren**.
2. Das Dialogfeld listet alle Änderungen (deinstallierte, aktualisierte und hinzugefügte Geräte) im Remote-Systeminstallation seit der Einrichtung oder letzten Aktualisierung der Milestone Interconnect-Einrichtung auf. Klicken Sie auf **Bestätigen**, um Ihren zentralen Standort mit diesen Änderungen zu aktualisieren.

### Registerkarte „Fernabfrage“

Auf der Registerkarte **Fernabfrage** können Sie Einstellungen für Abfragen von Fernaufzeichnungen für den Remote-System in einer Milestone Interconnect-Einrichtung verwalten:

Legen Sie folgende Eigenschaften fest:

| Name | Beschreibung |
|---|---|
| **Aufzeichnungen abfragen bei max.** | Bestimmt das Maximum der Bandbreite in Kbits/s für das Abfragen von Aufzeichnungen von einem Remote-System. Wählen Sie das Kontrollkästchen aus, um die Beschränkung von Abfragen zu aktivieren. |
| **Aufzeichnungen abfragen zwischen** | Bestimmt, dass Abfragen von Aufzeichnungen von einem Remote-System auf ein spezifisches Zeitintervall beschränkt sind.<br>Unvollendete Anfragen werden auch zur Endzeit fortgesetzt, bis sie vollendet wurden. Ist die Endzeit also kritisch, muss sie auf einen früheren Zeitpunkt gelegt werden, damit unvollendete Anfragen vollendet werden können.<br>Wenn das System automatisch abgefragt wird oder eine Abfrageanfrage vom XProtect Smart Client außerhalb des Zeitintervalls erhält, wird sie akzeptiert, aber erst gestartet, wenn das ausgewählte Zeitintervall beginnt.<br>Sie können ausstehende, von den Benutzern initiierte Remote-Aufzeichnungs-Abfrageanfragen über **System-Dashboard** -> **Aktuelle Aufgaben** anzeigen. |
| **Parallel auf Geräten abfragen** | Bestimmt die maximale Anzahl der Geräte, von denen Aufzeichnungen simultan abgefragt werden. Ändern Sie den Standardwert, wenn Sie mehr oder weniger Kapazität benötigen, abhängig von Ihren Systemkapazitäten. |

Wenn Sie die Einstellungen ändern, dauert es möglicherweise mehrere Minuten, bis die Änderungen im System widergespiegelt werden.

> Keine der obigen Aussagen trifft auf die direkte Wiedergabe von Fernaufzeichnungen zu.
> Alle Kameras, die direkt wiedergegeben werden sollen, sind zur direkten Wiedergabe verfügbar und nutzen Bandbreite nach Bedarf.

# Geräteknoten

## Geräte (Geräteknoten)

Die Geräte werden in der Management Client angezeigt, wenn Sie Hardware mit dem **Hardware hinzufügen**-Assistenten hinzufügen. Siehe Hardware hinzufügen auf Seite 229.

Sie können Geräte über die Gerätegruppen verwalten, wenn diese die gleichen Eigenschaften haben, siehe Gerätegruppen (Erklärung) auf Seite 58.

Sie können die Geräte auch einzeln verwalten.

Die Aktivierung/Deaktivierung und Umbenennung einzelner Geräte finden auf der Aufzeichnungsserver-Hardware statt. Siehe Aktivieren/Deaktivieren von Geräten über Gerätegruppen.

Für alle sonstigen Konfigurations- und Verwaltungstätigkeiten für Kameras erweitern Sie die Option **Geräte** im Bereich Seitennavigation und wählen Sie ein Gerät aus:

- **Kameras**
- **Mikrofone**
- **Lautsprecher**
- **Metadaten**
- **Eingänge**
- **Ausgaben**

Gruppieren Sie im Bereich „Übersicht“ Ihre Kameras, um einen guten Überblick über sie zu erhalten. Die erste Gruppierung findet im Rahmen des Assistenten **Hardware hinzufügen** statt.

> Informationen zu unterstützter Hardware finden Sie auf der Seite mit der unterstützten Hardware auf der Website Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

### Statussymbole von Geräten

Wenn Sie ein Gerät auswählen, werden Informationen zu seinem aktuellen Status im Bereich **Vorschau** angezeigt.
Die folgenden Symbole zeigen den Status der Geräte an:

| Kamera | Mikrofon | Lautsprecher | Metadaten | Eingang | Ausgang | Beschreibung |
|---|---|---|---|---|---|---|
|  |  |  |  |  |  | **Gerät aktiviert und empfängt Daten**: Das Gerät ist aktiviert und Sie empfangen einen Live-Stream. |
|  |  |  |  | | | **Gerät zeichnet auf**: Das Gerät zeichnet Daten im System auf. |

| Kamera | Mikrofon | Lautsprecher | Metadaten | Eingang | Ausgang | Beschreibung |
|---|---|---|---|---|---|---|
|  |  |  |  |  |  | **Gerät temporär angehalten oder ohne Feed**: Es werden keine Informationen ans System übertragen. Bei einer Kamera können Sie kein Live-Video ansehen. Ein angehaltenes Gerät kann im Gegensatz zu einem deaktivierten Gerät noch mit dem Aufzeichnungsserver kommunizieren, um Ereignisse abzufragen, Einstellungen festzulegen usw. |
|  |  |  |  |  |  | **Geräte deaktiviert**: Kann nicht automatisch durch eine Regel gestartet werden und kann nicht mit dem Aufzeichnungsserver kommunizieren. Wenn eine Kamera deaktiviert ist, können Sie keine Live-Videos oder Aufzeichnungen ansehen. |
|  |  |  |  | | | **Gerätedatenbank wird repariert**. |
|  |  |  |  |  |  | **Gerät benötigt Aufmerksamkeit**: Das Gerät funktioniert |

| Kamera | Mikrofon | Lautsprecher | Metadaten | Eingang | Ausgang | Beschreibung |
|---|---|---|---|---|---|---|
| | | | | | | nicht richtig. Halten Sie den Mauszeiger über das Gerätesymbol, um eine Beschreibung des Problems im Tooltip zu erhalten. |
|  |  |  |  |  |  | **Status unbekannt**: Status des Geräts ist unbekannt, wenn zum Beispiel der Aufzeichnungsserver offline ist. |
|  |  |  |  | | | Einige Symbole können in Kombination auftreten, wie in folgendem Beispiel: **Gerät aktiviert und empfängt Daten** und **Gerät zeichnet auf**. |

## Kameras (Geräteknoten)

Kameraeräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen, und sind standardmäßig aktiviert.

Das System wird mit einer Standardregel zum Start von Feeds geliefert, die sicherstellt, dass Videofeeds von allen verbundenen Kameras automatisch an das System übertragen werden. Die Standardregel kann nach Bedarf abgeschaltet und/oder geändert werden.

Befolgen Sie diese Konfigurationsreihenfolge, um die typischsten Aufgaben im Bereich der Konfiguration eines Kameraeräts auszuführen:

1. Kameraeinstellungen konfigurieren, siehe die Registerkarte Einstellungen (Geräte.
2. Streams konfigurieren, siehe die Registerkarte Streams (Geräte).
3. Bewegungen konfigurieren, siehe die Registerkarte Bewegungen (Geräte).

4. Aufzeichnung konfigurieren, siehe die Registerkarte Aufzeichnung (Geräte) und Datenbanken für Geräte überwachen.
5. Konfigurieren Sie die restlichen Einstellungen nach Bedarf.

## Mikrofone (Geräteknoten)

Mikrofongeräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen. Sie sind standardmäßig nicht aktiviert, daher müssen Sie diese also vor Verwendung entweder während der Anwendung des **Hardware hinzufügen**-Assistenten oder danach aktivieren. Mikrofone benötigen keine separaten Lizenzen. Sie können so viele Mikrofone in Ihrem System anwenden wie nötig.

Sie können Mikrofone vollkommen unabhängig von Kameras verwenden.

Das System wird mit einer Standardregel zum Start von Audiofeeds geliefert, die sicherstellt, dass Audiofeeds von allen verbundenen Mikrofonen automatisch an das System übertragen werden. Die Standardregel kann nach Bedarf abgeschaltet und/oder geändert werden.

Sie können Mikrofongeräte in den folgenden Registerkarten konfigurieren:

- Registerkarte „Info" siehe Registerkarte „Info" (Geräte)
- Registerkarte „Einstellungen“ siehe Registerkarte „Einstellungen“ (Geräte)
- Registerkarte „Aufzeichnen“, siehe Registerkarte „Aufzeichnen“ (Geräte)
- Registerkarte „Ereignisse“ siehe (Geräte)

## Lautsprecher (Geräteknoten)

Lautsprechergeräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen. Sie sind standardmäßig nicht aktiviert, daher müssen Sie diese also vor Verwendung entweder während der Anwendung des **Hardware hinzufügen**-Assistenten oder danach aktivieren. Lautsprecher benötigen keine separaten Lizenzen. Sie können so viele Lautsprecher in Ihrem System nutzen wie nötig.

Sie können Lautsprecher vollkommen unabhängig von Kameras verwenden.

Das System wird mit einer Standardregel zum Start von Audiofeeds geliefert, durch die das Gerät gestartet wird, sodass es bereit ist, benutzeraktiviertes Audio an die Lautsprecher zu versenden. Die Standardregel kann nach Bedarf abgeschaltet und/oder geändert werden.

Sie können Lautsprechergeräte in den folgenden Registerkarten konfigurieren:

- Registerkarte „Info" siehe Registerkarte „Info" (Geräte)
- Registerkarte „Einstellungen“ siehe Registerkarte „Einstellungen“ (Geräte)
- Registerkarte „Aufzeichnen“, siehe Registerkarte „Aufzeichnen“ (Geräte)

## Metadaten (Geräteknoten)

Das System wird mit einer Standardregel zum Start von Feeds geliefert, die sicherstellt, dass Metadatenfeeds von Hardware, die Metadaten unterstützt, automatisch ins System übertragen werden. Die Standardregel kann nach Bedarf abgeschaltet und/oder geändert werden.

Sie können Metadatengeräte in den folgenden Registerkarten konfigurieren:

- Registerkarte „Info" siehe Registerkarte „Info" (Geräte)
- Registerkarte „Einstellungen“ siehe Registerkarte „Einstellungen“ (Geräte)
- Registerkarte „Aufzeichnen“, siehe Registerkarte „Aufzeichnen“ (Geräte)

## Eingabe (Geräteknoten)

Sie können Eingabegeräte vollkommen unabhängig von Kameras verwenden.

> Überprüfen Sie vor der Verwendung eines externen Eingabegeräts mit einem Gerät, dass das Gerät den Sensorbetrieb erkennt. Bei den meisten Geräten wird dies auf der Konfigurationsoberfläche oder über Common-Gateway-Interface-Skriptbefehle (CGI) angezeigt.

Eingabegeräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen. Sie sind standardmäßig nicht aktiviert, daher müssen Sie diese also vor Verwendung entweder während der Anwendung des **Hardware hinzufügen**-Assistenten oder danach aktivieren. Eingabegeräte benötigen keine separaten Lizenzen. Sie können so viele Eingabegeräte in Ihrem System anwenden wie nötig.

Sie können Eingabegeräte in den folgenden Registerkarten konfigurieren:

- Registerkarte „Info" siehe Registerkarte „Info" (Geräte)
- Registerkarte „Einstellungen“ siehe Registerkarte „Einstellungen“ (Geräte)
- Registerkarte „Ereignisse“ siehe (Geräte)

## Ausgabe (Geräteknoten)

Ausgabe kann über Management Client und XProtect Smart Client manuell ausgelöst werden.

> Überprüfen Sie vor der Verwendung eines externen Ausgabegeräts mit einem Gerät, dass dieses Gerät das am Ausgang angebrachte Gerät steuern kann. Bei den meisten Geräten wird dies auf der Konfigurationsoberfläche oder über Common-Gateway-Interface-Skriptbefehle (CGI) angezeigt.

Ausgabegeräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen. Sie sind standardmäßig nicht aktiviert, daher müssen Sie diese also vor Verwendung entweder während der Anwendung des **Hardware hinzufügen**-Assistenten oder danach aktivieren. Ausgabegeräte benötigen keine separaten Lizenzen. Sie können so viele Ausgabegeräte in Ihrem System anwenden wie nötig.

Sie können Ausgabegeräte in den folgenden Registerkarten konfigurieren:

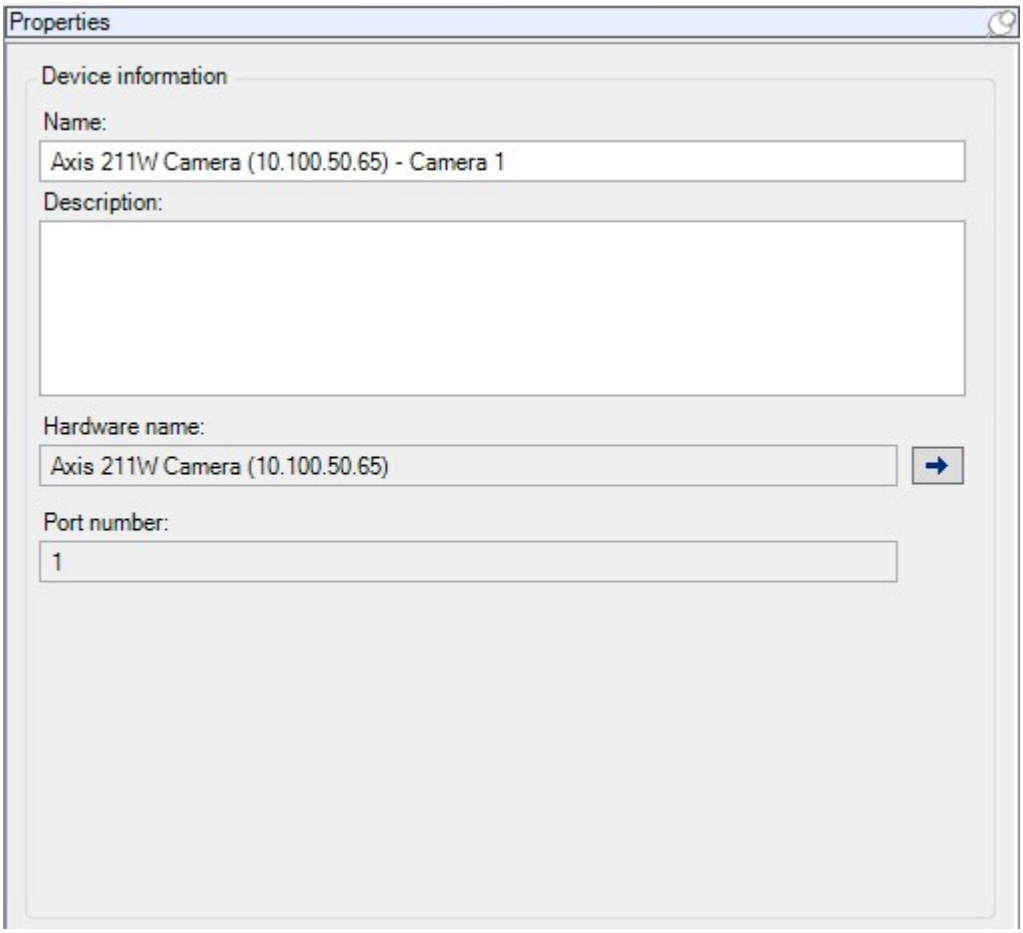
Registerkarte „Info“, siehe

- Registerkarte „Info" siehe Registerkarte „Info" (Geräte)
- Registerkarte „Einstellungen“ siehe Registerkarte „Einstellungen“ (Geräte)

## Die Registerkarten für Geräte

### Registerkarte „Info (Geräte)“

Auf der Registerkarte **Info** können Sie grundlegende Geräteinformationen in einer Anzahl Felder anzeigen und bearbeiten.
Alle Geräte verfügen über eine **Info**-Registerkarte.



Registerkarte „Info“ (Eigenschaften)

| Name | Beschreibung |
|---|---|
| **Name** | Der Name wird verwendet, wenn das Gerät im System und den Clients aufgelistet ist.<br>Wenn Sie ein Gerät neu benennen, wird der Name im Management Client global geändert. |
| **Beschreibung** | Geben Sie eine Beschreibung des Geräts ein (optional).<br>Die Beschreibung taucht in einer Anzahl Listen im System auf. Zum Beispiel, wenn Sie den Mauszeiger über den Namen im Bereich **Übersicht** halten. |
| **Hardware-Name** | Zeigt den Namen der Hardware an, mit der das Gerät verbunden ist. Das Feld kann von hier aus nicht bearbeitet werden, Sie können es jedoch verändern, indem Sie daneben auf **Gehe zu** klicken. So gelangen Sie zu den Hardware-Informationen, wo Sie den Namen ändern können. |
| **Portnummer** | Zeigt den Port an, über den das Gerät an der Hardware angebracht ist.<br>Die Portnummer für Einzelgeräte-Hardware ist normalerweise **1**. Die Portnummer für Mehrfachgeräte-Hardware, wie etwa Video-Server mit mehreren Kanälen, zeigt normalerweise den Kanal an, über den das Gerät angebracht ist, zum Beispiel **3**. |
| **Kurzbezeichnung** | Geben Sie hier eine Kurzbezeichnung für die Kamera ein. Die maximale Zeichenanzahl beträgt 128.<br>Wenn Sie Smart Map verwenden, wird die Kurzbezeichnung automatisch mit der Kamera auf der Smart Map angezeigt. Anderenfalls wird der vollständige Name angezeigt. |
| **Geokoordinaten** | Geben Sie den geografischen Standort der Kamera im Format **latitude, longitude** ein. Der eingegebene Wert bestimmt die Position des Kamerasymbols auf der Smart Map im XProtect Smart Client und XProtect Mobile Client.<br>Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen. |

| Name | Beschreibung |
|---|---|
| **Richtung** | Geben Sie die Blickrichtung der Kamera in Bezug auf eine genau nach Norden zeigende vertikale Achse an. Der eingegebene Wert bestimmt die Richtung des Kamerasymbols auf der Smart Map im XProtect Smart Client und XProtect Mobile Client.<br>Der Standardwert ist 0,0.<br>  Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen. |
| **Sichtfeld** | Geben Sie die Breite des Sichtfelds in Grad ein. Der eingegebene Wert bestimmt den Winkel des Sichtfelds für das Kamerasymbol auf der Smart Map im XProtect Smart Client und XProtect Mobile Client.<br>Der Standardwert ist 0,0.<br>  Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen. |
| **Tiefe** | Geben Sie die Tiefe des Sichtfelds der Kamera in Metern oder Fuß ein. Der eingegebene Wert bestimmt die Länge des Sichtfelds für das Kamerasymbol auf der Smart Map im XProtect Smart Client und XProtect Mobile Client.<br>Der Standardwert ist 0,0.<br>  Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen. |
| **Positionsvorschau im Browser** | Klicken Sie auf die Schaltfläche, um zu überprüfen, ob Sie die richtigen geographischen Koordinaten eingegeben haben. Google Maps öffnet sich an der von Ihnen angegebenen Position in Ihrem Standard-Webbrowser.<br>  Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen. |

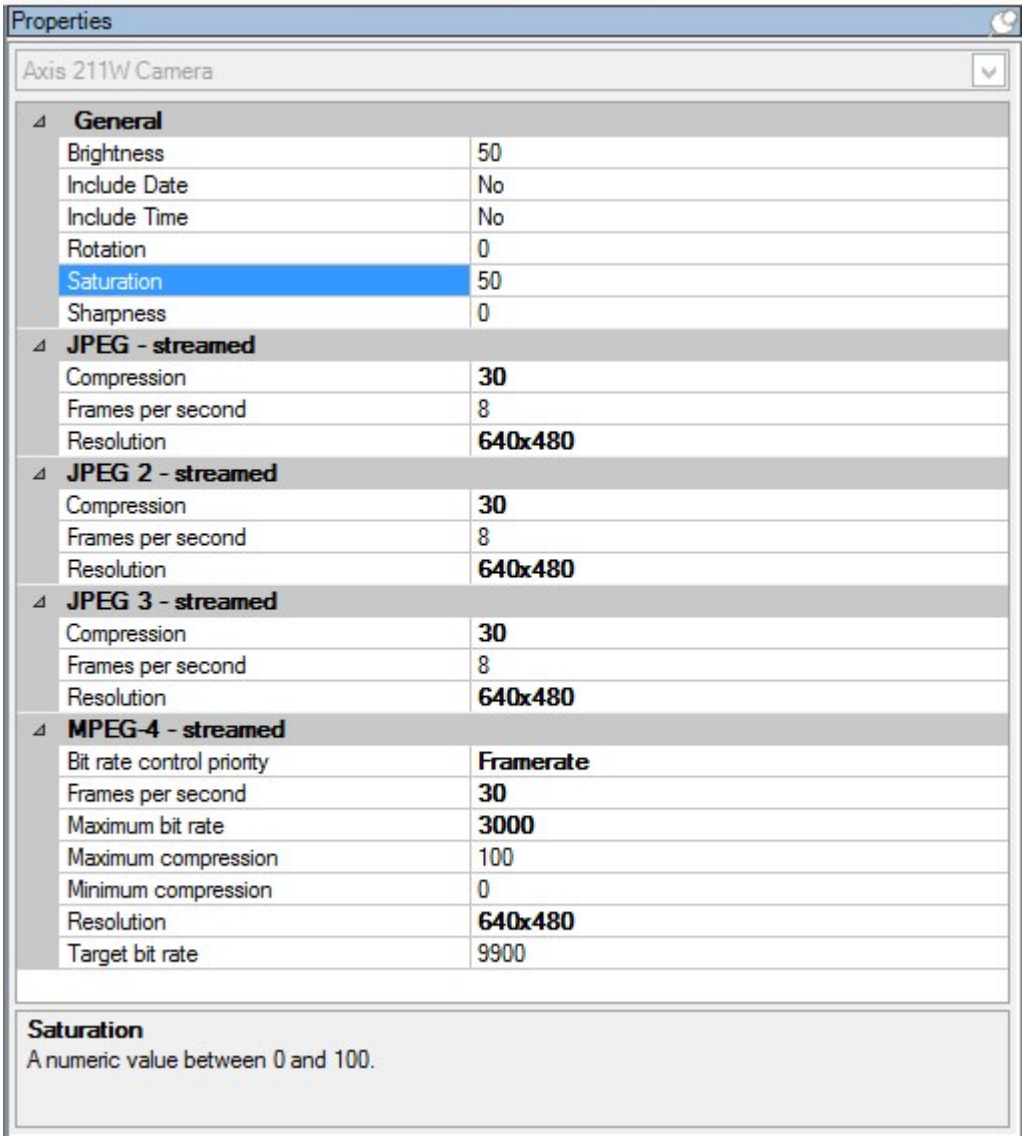
### Registerkarte „Einstellungen“ (Geräte)

Auf der Registerkarte **Einstellungen** können Sie Geräteeinstellungen in einer Anzahl Felder anzeigen und bearbeiten.
Alle Geräte verfügen über eine **Einstellungen**-Registerkarte.

Die Werte erscheinen veränderlich oder schreibgeschützt in einer Tabelle. Wenn Sie eine Einstellung auf einen Nichtstandardwert setzen, erscheint der Wert in Fettdruck.

Der Inhalt der Tabelle hängt vom Gerätetreiber ab.

Erlaubte Bereiche tauchen im Informationsfenster unter der Einstellungstabelle auf:



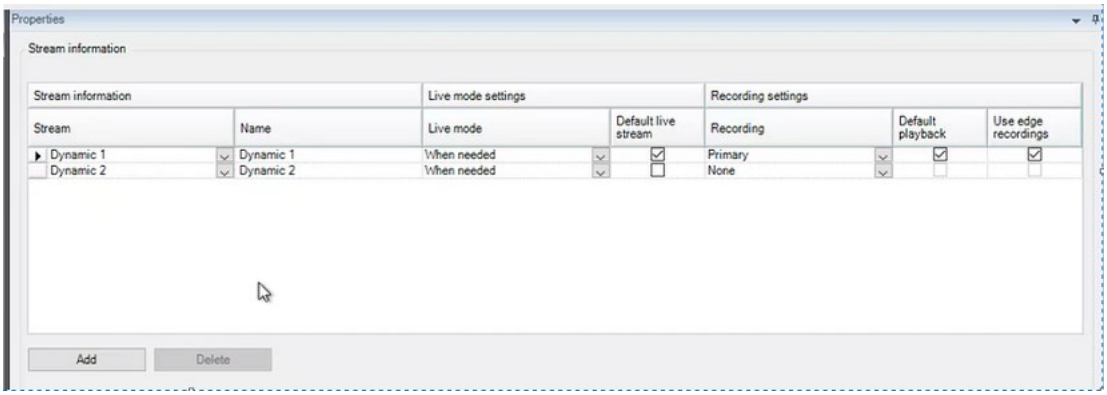

Weitere Informationen zu den Kameraeinstellungen finden Sie unter Kameraeinstellungen anzeigen oder bearbeiten.

### Registerkarte „Streams“ (Geräte)

Folgende Geräte verfügen über eine **Streams**-Registerkarte:

- Kameras

Die Registerkarte **Streams** enthält standardmäßig einen einzigen Stream. Es ist der Standard-Stream der ausgewählten Kamera, der für Live- und Videoaufzeichnungen verwendet wird. Wenn Sie die adaptive Wiedergabe verwenden, müssen zwei Streams erstellt werden.




Aufgaben auf der Registerkarte "Streams"

| Name | Beschreibung |
|---|---|
| **Hinzufügen** | Klicken Sie auf einen Stream, den Sie zur Liste hinzufügen wollen.<br>Stream hinzufügen |

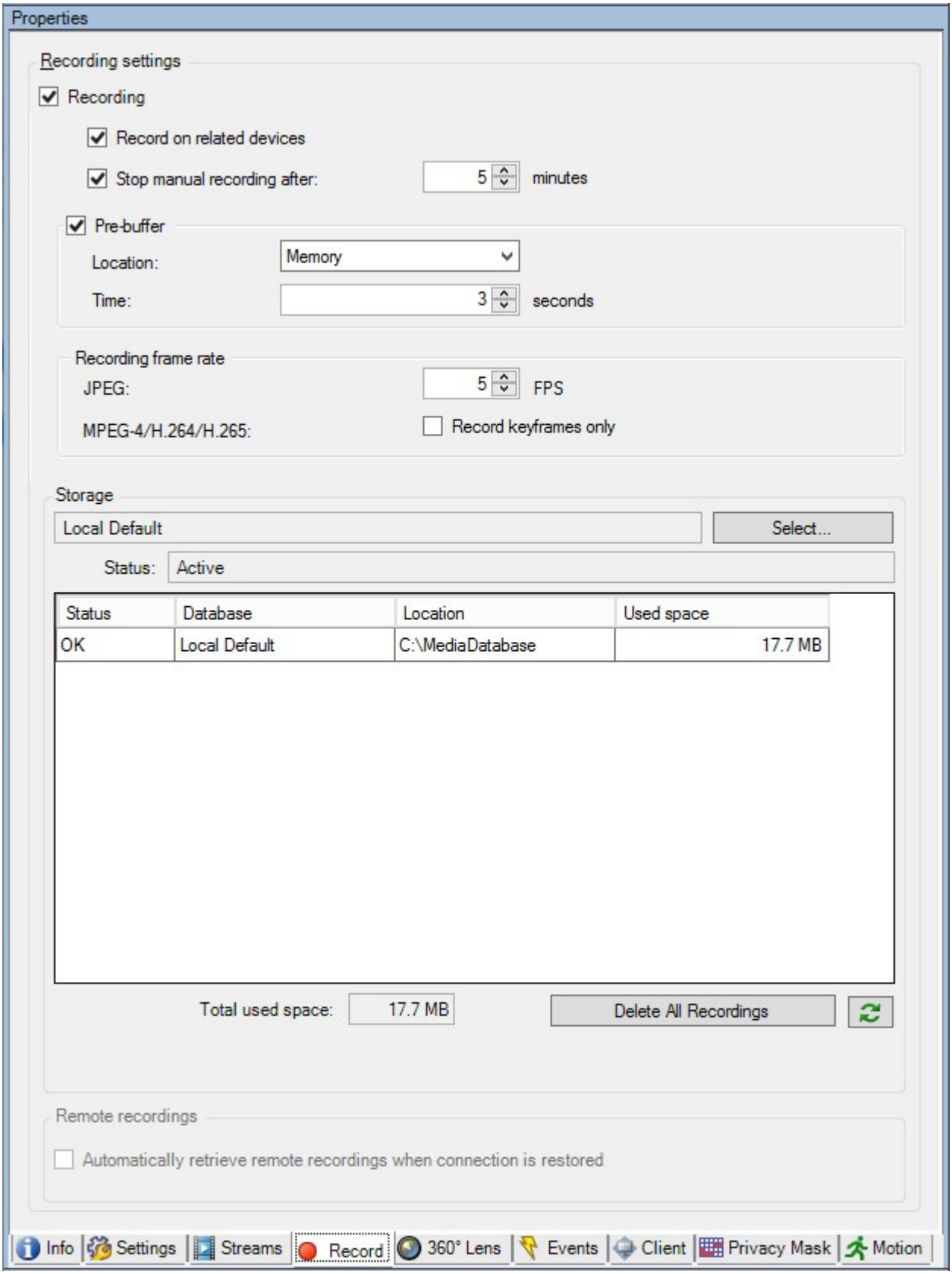
### Registerkarte „Aufzeichnen“ (Geräte)

Die folgenden Geräte besitzen eine **Aufzeichnen** Registerkarte:

- Kameras
- Mikrofone
- Lautsprecher
- Metadaten

Aufzeichnungen eines Geräts werden nur in einer Datenbank gespeichert, wenn Sie die Aufzeichnung aktiviert haben und die Aufzeichnungskriterien erfüllt werden.

Parameter, die für ein Gerät nicht konfiguriert werden können, sind ausgegraut.


Properties
Recording settings
Recording
Record on related devices
Stop manual recording after:
5
minutes
Pre-buffer
Location:
Memory
Time:
3
seconds
Recording frame rate
JPEG:
5
FPS
MPEG-4/H.264/H.265:
Record keyframes only
Storage
Local Default
Select...
Status:
Active
Status
Database
Location
Used space
OK
Local Default
C:\MediaDatabase
17.7 MB
Total used space:
17.7 MB
Delete All Recordings
Remote recordings
Automatically retrieve remote recordings when connection is restored
Info
Settings
Streams
Record
360° Lens
Events
Client
Privacy Mask
Motion

Aufgaben auf der Registerkarte "Aufzeichnen"

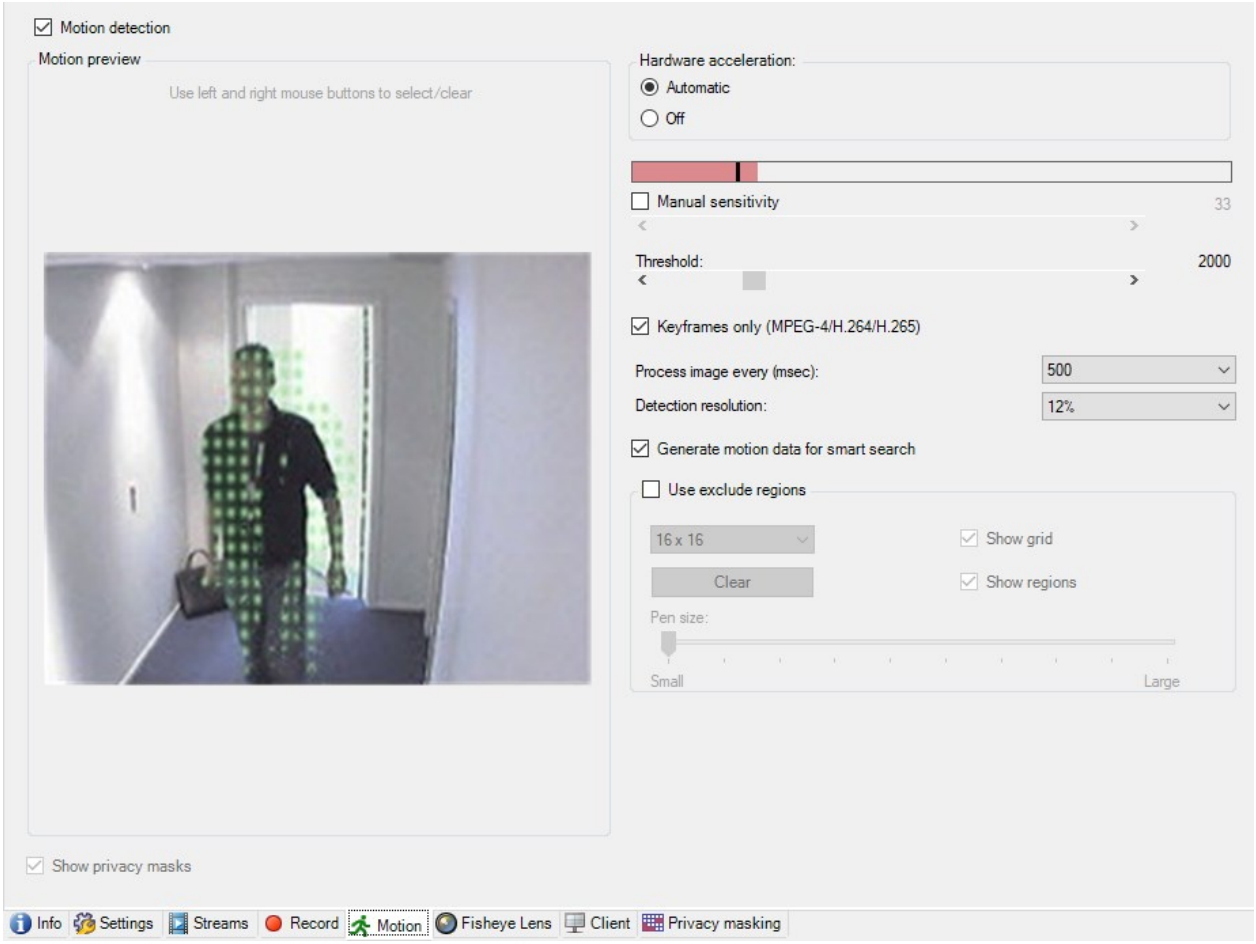
| Name | Beschreibung |
|---|---|
| **Aufzeichnung** | Aufzeichnung aktivieren oder deaktivieren<br>Aktivieren der Aufzeichnung auf zugehörigen Geräten |
| **Vor-Puffer** | Vorpuffern And abspeichern vorgepufferter Aufzeichnungen (Erklärung)<br>Verwalten von Voralarm-Puffern<br>Manuelle Aufzeichnung verwalten |
| **Aufzeichnungsbildrate** | Bildrate der Aufzeichnung festlegen<br>Keyframe-Aufzeichnung aktivieren |
| **Speicher** | Status von Datenbanken für Geräte beobachten |
| **Auswählen** | Geräte von einem Speichermedium zum anderen verschieben |
| **Alle Aufzeichnungen löschen** | Verwenden Sie diese Schaltfläche, wenn Sie alle Geräte in der Gruppe zum selben Server hinzugefügt haben:<br>Aufzeichnungen löschen |
| **Fernaufzeichnungen bei Wiederherstellung der Verbindung automatisch abrufen** | Fernaufzeichnungen abspeichern und abrufen |

### Registerkarte „Bewegung“ (Geräte)

Die folgenden Geräte besitzen eine Registerkarte **Bewegung**:

- Kameras

In der Registerkarte **Bewegung** können Sie die Bewegungserkennung für die ausgewählte Kamera aktivieren und konfigurieren.




Aufgaben auf der Registerkarte "Bewegung"

| Name | Beschreibung |
|---|---|
| **Bewegungserkennung** | Aktivieren und Deaktivieren von Bewegungserkennung |
| **Hardware-Beschleunigung** | Wählen **Automatik** aus, um die Hardwarebeschleunigung zu aktivieren, oder wählen Sie **Aus**, um die Einstellung zu deaktivieren. Weitere Informationen finden Sie unter Hardwarebeschleunigung aktivieren oder deaktivieren. |
| **Privatzonenmasken** | Wenn Sie Bereiche ausgewählt haben, die dauerhaft abgedeckt bleiben, so können Sie das Kontrollkästchen **Verdeckte Bildbereiche** aktivieren, damit die verdeckten Bildbereiche auf der Registerkarte **Bewegung** angezeigt werden. Verdeckte Bildbereiche legen Sie auf der Registerkarte Einrichtung von Privatsphärenausblendung (Geräte) auf Seite 494 fest. |

| Name | Beschreibung |
|---|---|
| | Es gibt keine Bewegungserkennung innerhalb von Bereichen, die von permanenten Privatzonenmasken gedeckt sind. |
| **Manuelle Empfindlichkeit** | Legt fest, **wie sehr sich jedes Pixel** auf dem Bilde verändern muss, damit dies als Bewegung betrachtet wird:<br>Manuelle Empfindlichkeit für die Definition von Bewegung aktivieren |
| **Schwellenwert** | Legt fest, **wie viele Pixel** sich auf dem Bild verändern müssen, damit dies als Bewegung betrachtet wird:<br>Geben Sie eine Schwelle für Bewegungen an |
| **Nur Keyframes (MPEG-4/H.264/H.265)** | Aktivieren Sie dieses Kontrollkästchen, um die Bewegungserkennung nur auf Keyframes zu beschränken, und nicht in dem gesamten Video-Stream. Gilt nur für MPEG-4/H.264/H.265.<br>Die Bewegungserkennung in Keyframes reduziert die verwendete Prozessorleistung für die Ausführung der Analyse. |
| **Bild verarbeiten alle (ms):** | Wählen Sie auf dieser Liste ein Intervall für die Bildverarbeitung aus, um festzulegen, wie oft das System die Analyse zur Bewegungserkennung ausführt.<br>Zum Beispiel, alle 1.000 Millisekunden bedeutet einmal jede Sekunde. Der Standardwert ist auf alle 500 Millisekunden festgelegt.<br>Der Intervall wird angewendet, wenn die tatsächliche Bildrate höher als das hier eingestellte Intervall ist. |
| **Erkennungsauflösung** | Wählen Sie auf dieser Liste eine Erkennensauflösung aus, um die Bewegungserkennungsleistung zu optimieren.<br>Es wird nur der gewählte Bildanteil analysiert, z.B. 25%. Durch die Analyse von 25 % wird nur jedes vierte anstatt alle Pixel untersucht.<br>Mittels optimierter Erkennung wird die benötigte Prozessorleistung für die Analyse verringert, führt jedoch zu einer weniger genauen Bewegungserkennung. |

| Name | Beschreibung |
|---|---|
| **Bewegungsdaten für Smart Search erzeugen** | Wenn Sie dieses Kontrollkästchen aktivieren, erzeugt das System Bewegungsdaten für die Bilder, die für die Bewegungserkennung verwendet werden. Wenn Sie beispielsweise Bewegungserkennung nur in Keyframes auswählen, werden diese Bewegungsdaten auch nur für Keyframes erstellt.<br><br>Durch die zusätzlichen Bewegungsdaten können die Client-Benutzer mittels der Smart Search Funktion schnell und einfach auf Grundlage der Bewegung in einem ausgewählten Bereich des Bildes nach relevanten Aufzeichnungen suchen. Das System erzeugt keine Bewegungsdaten in Bereichen, die permanent verdreckt sind, sondern nur in Bereichen, die vorübergehend verdeckt sind (siehe Bewegungserkennung (Erklärung)).<br><br>Der Schwellenwert für die Bewegungserkennung und Auschlussbereiche beeinflussen die generierten Bewegungsdaten nicht.<br><br>• Unter **Extras** > **Optionen** > **Allgemein** können Sie Standardeinstellungen für die Erzeugung intelligenter Suchdaten für Kameras angeben. |
| **Ausschlussbereiche verwenden** | Bestimmte Bereiche einer Kameraansicht von der Bewegungserkennung ausschließen:<br><br>Geben Sie für die Bewegungserkennung Ausschlussbreiche an |

### Registerkarte „Voreinstellungen“ (Geräte)

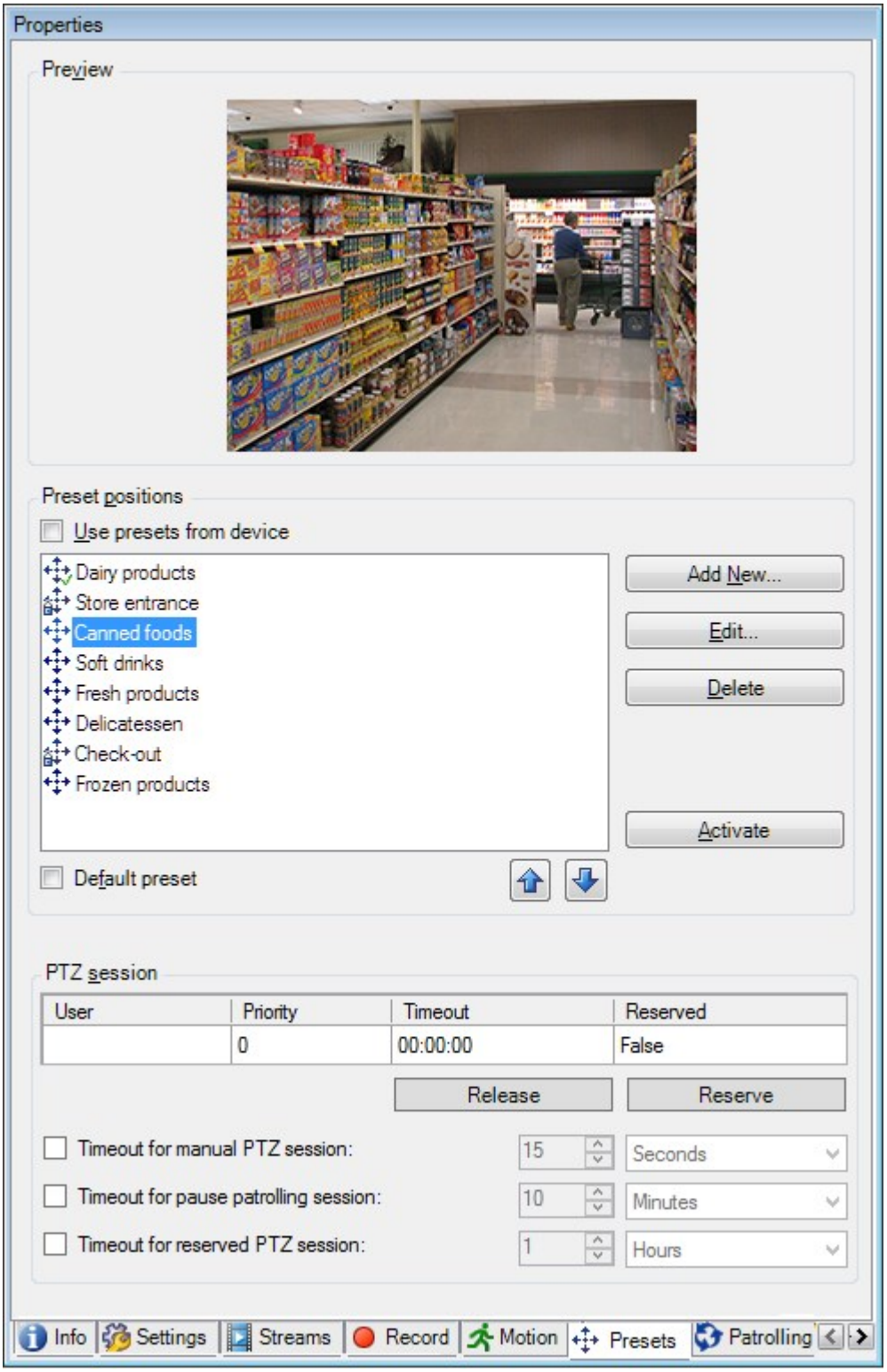
Die folgenden Geräte besitzen eine Registerkarte **Voreinstellungen**:

- PTZ-Kameras, die Preset Positionen unterstützen

Auf der Registerkarte **Voreinstellungen** können Sie Preset Positionen erstellen oder importieren, zum Beispiel:

- Bei Regeln, welche die Bewegung einer PTZ (Pan/Tilt/Zoom)-Kamera zu einer bestimmten Preset Position festlegen, wenn ein Ereignis eintritt
- Bei Wachrundgängen, für die automatische Bewegung einer PTZ-Kamera zwischen mehreren Preset Positionen.
- Für manuelle Aktivierung durch die XProtect Smart Client-Benutzer.

Auf der Registerkarte Gesamtsicherheit (siehe Registerkarte „Gesamtsicherheit“ (Rollen) auf Seite 556) oder auf der Registerkarte PTZ (siehe PTZ-Registerkarte (Rollen) auf Seite 602) weisen Sie Rollen eine PTZ-Erlaubnis zu.


Properties
Preview
Preset positions
Use presets from device
Dairy products
Store entrance
Canned foods
Soft drinks
Fresh products
Delicatessen
Check-out
Frozen products
Add New...
Edit...
Delete
Activate
Default preset
PTZ session
User
Priority
Timeout
Reserved
0
00:00:00
False
Release
Reserve
Timeout for manual PTZ session:
15
Seconds
Timeout for pause patrolling session:
10
Minutes
Timeout for reserved PTZ session:
1
Hours
Info
Settings
Streams
Record
Motion
Presets
Patrolling

Aufgaben auf der Registerkarte "Voreinstellungen"

| Name | Beschreibung |
|---|---|
| **Neu** | Um eine voreingestellte Position für die Kamera hinzuzufügen:<br>Hinzufügen einer Preset-Position (Typ 1) |
| **Voreinstellungen des Geräts verwenden** | Eine vorgestellte Position für eine PTZ-Kamera auf der Kamera selbst hinzufügen:<br>Verwendung der Preset Positionen der Kamera (Typ 2) |
| **Standardvoreinstellung** | Sie können eine der voreingestellten Positionen einer PTZ-Kamera als voreingestellte Standardposition der Kamera festlegen:<br>Voreingestellte Standardposition einer Kamera als Standard zuweisen |
| **Bearbeiten** | So bearbeiten Sie eine vorhandene, im System festgelegte voreingestellte Position:<br>Bearbeiten einer voreingestellten Position für eine Kamera (nur Typ 1)<br>So bearbeiten Sie den Namen einer in der Kamera definierten voreingestellten Position:<br>Umbenennen einer voreingestellten Position für eine Kamera (nur Typ 2) |
| **Gesperrt** | Aktivieren Sie dieses Kontrollkästchen, um eine voreingestellte Position zu sperren. Sie können eine voreingestellte Position sperren, wenn Sie verhindern möchten, dass Benutzer in XProtect Smart Client oder Benutzer mit eingeschränkten Sicherheitsberechtigungen die voreingestellte Position aktualisieren oder löschen. Gesperrte Voreinstellungen werden durch das Symbol  angezeigt.<br>Voreinstellungen sperren Sie im Rahmen der Hinzufügung (siehe Preset-Position hinzufügen (Typ 1)) und der |

| Name | Beschreibung |
|---|---|
| | Bearbeitung (siehe Bearbeiten einer Preset-Position (nur Typ 1)). |
| **Aktivieren** | Klicken Sie auf diese Schaltfläche, um die vorangestellte Position einer Kamera zu testen:<br>Testen einer voreingestellten Position (nur Typ 1). |
| **Reservieren** und **Freigeben** | So verhindern Sie, dass andere Benutzer die Kontrolle über die Kamera übernehmen und die Reservierung freigeben.<br>Administratoren mit Sicherheitsberechtigungen zum Ausführen einer reservierten PTZ-Sitzung können die PTZ-Kamera in dieser Betriebsart betreiben. So wird verhindert, dass andere Benutzer die Kontrolle über die Kamera übernehmen. Wenn Sie über ausreichende Berechtigungen verfügen, können Sie die für andere Benutzer reservierten PTZ-Sitzungen freigeben:<br>PTZ-Sitzungen reservieren und freigeben. |
| **PTZ-Sitzung** | Überwachen Sie, ob das System gerade patrouilliert oder ob ein Benutzer die Kontrolle übernommen hat:<br>PTZ-Sitzungs-Eigenschaften auf Seite 484.<br>Lassen Sie sich den Status von PTZ-Kameras anzeigen und verwalten Sie Zeitüberschreitungen für Kameras:<br>Zeitüberschreitungen für PTZ-Sitzungs festlegen. |

### PTZ-Sitzungs-Eigenschaften

Die Tabelle **PTZ-Sitzung** zeigt den aktuellen Status der PTZ-Kamera an.

| Name | Beschreibung |
|---|---|
| **Benutzer** | Zeigt den Benutzer an, der die Schaltfläche **Reserviert** gedrückt hat und im Augenblick die PTZ-Kamera steuert.<br>Wenn ein Wachrundgang vom System aktiviert wird, wird **Wachrundgang** angezeigt. |
| **Priorität** | Zeigt die PTZ-Priorität des Benutzers an. Sie können PTZ-Sitzungen nur von Benutzern mit einer niedrigeren Priorität übernehmen. |
| **Zeitüberschreitung** | Zeigt die verbleibende Zeit der aktuellen PTZ-Sitzung an. |
| **Reserviert** | Zeigt an, ob die aktuelle Sitzung eine reservierte PTZ-Sitzung ist oder nicht:<br>• **Wahr**: Reserviert<br>• **Falsch**: Nicht reserviert |

Mithilfe der Kontrollkästchen im Abschnitt **PTZ-Sitzung** können Sie die folgenden Zeitüberschreitungen für jede PTZ-Kamera ändern.

| Name | Beschreibung |
|---|---|
| **Zeitüberschreitung für manuelle PTZ-Sitzung** | Legen Sie die Zeitüberschreitung für manuelle PTZ-Sitzungen auf dieser Kamera fest, wenn die gewünschte Zeitüberschreitung vom Standard abweichen soll. Sie können den Standardzeitraum im Menü **Tools** unter **Optionen** festlegen. |
| **Zeitüberschreitung für Wachrundgang-Pausierung von PTZ-Sitzung** | Legen Sie die Zeitüberschreitung für die Pausierung von PTZ-Sitzungen auf dieser Kamera fest, wenn die gewünschte Zeitüberschreitung vom Standard abweichen soll. Sie können den Standardzeitraum im Menü **Tools** unter **Optionen** festlegen. |
| **Zeitüberschreitung für reservierte PTZ-Sitzung** | Legen Sie die Zeitüberschreitung für reservierte PTZ-Sitzungen auf dieser Kamera fest, wenn die gewünschte Zeitüberschreitung vom Standard abweichen soll. Sie können den Standardzeitraum im Menü **Tools** unter **Optionen** festlegen. |

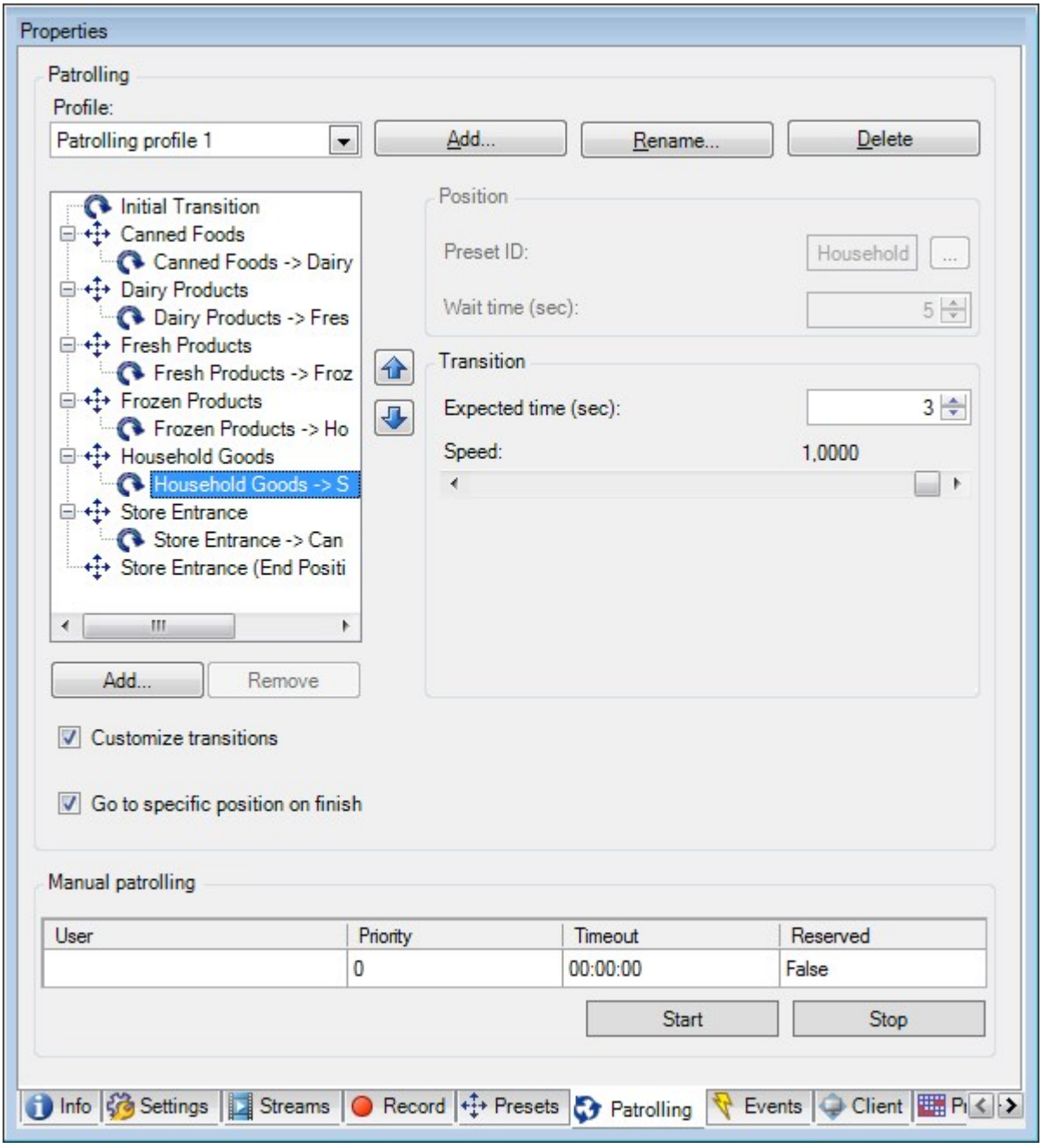
### Registerkarte „Wachrundgang“ (Geräte)

Die folgenden Geräte besitzen eine Registerkarte **Wachrundgang**:

- PTZ-Kameras

Auf der Registerkarte **Wachrundgang** können Sie Wachrundgangprofile erstellen – die automatische Bewegung einer PTZ (Pan/Tilt/Zoom)-Kamera zwischen einer Reihe von voreingestellten Positionen.
Bevor Sie mit Patrouillen arbeiten können, müssen Sie auf der Registrierkarte **Voreinstellungen** mindestens zwei voreingestellte Positionen für die Kamera angeben, siehe Voreingestellte Position hinzufügen (Typ 1)..

Die Registerkarte **Patroullie** zeigt ein Patrouillenprofil mit benutzerdefinierten Übergängen:


Properties
Patrolling
Profile:
Patrolling profile 1
Add...
Rename...
Delete
Initial Transition
Canned Foods
Canned Foods -> Dairy
Dairy Products
Dairy Products -> Fres
Fresh Products
Fresh Products -> Froz
Frozen Products
Frozen Products -> Ho
Household Goods
Household Goods -> S
Store Entrance
Store Entrance -> Can
Store Entrance (End Positi
Position
Preset ID:
Household
Wait time (sec):
5
Transition
Expected time (sec):
3
Speed:
1,0000
Add...
Remove
Customize transitions
Go to specific position on finish
Manual patrolling
User
Priority
Timeout
Reserved
0
00:00:00
False
Start
Stop
Info
Settings
Streams
Record
Presets
Patrolling
Events
Client

Aufgaben auf der Registerkarte "Patrouillen"

| Name | Beschreibung |
|---|---|
| **Hinzufügen** | Hinzufügen eines Wachrundgangprofils |
| **Voreinstellungs-ID** | Festlegen von Preset-Positionen in einem Wachrundgangprofil |
| **Wartezeit (s)** | Festlegen der Zeit in jeder Preset Position |
| **Übergänge anpassen** | Übergänge anpassen (PTZ) |
| **Beim Beenden zu bestimmter Position gehen** | Eine Position für die Patrouille angeben |
| **Manueller Wachrundgang** | Überwachen Sie, ob das System gerade patrouilliert oder ob ein Benutzer die Kontrolle übernommen hat. |
| **Start** und **Stopp** | Verwenden Sie die Schaltflächen **Start** und **Stopp**, um um manuelle Patrouillen einzuleiten und anzuhalten.<br>Siehe Zeitüberschreitungen für PTZ-Sitzungen vorgeben - dort finden Sie Informationen dazu, wie Sie für alle oder für einzelne PTZ-Kameras vorgeben können, wie viel Zeit vergehen muss, bevor regelmäßige Patrouillen wieder aufgenommen werden. |

Eigenschaften manueller Wachrundgänge

Die Tabelle **Manueller Wachrundgang** zeigt den aktuellen Status der PTZ-Kamera an.

| Name | Beschreibung |
|---|---|
| **Benutzer** | Zeigt den Benutzer an, der entweder die PTZ-Sitzung reserviert oder einen manuellen Wachrundgang gestartet hat und im Augenblick die Kamera steuert. |

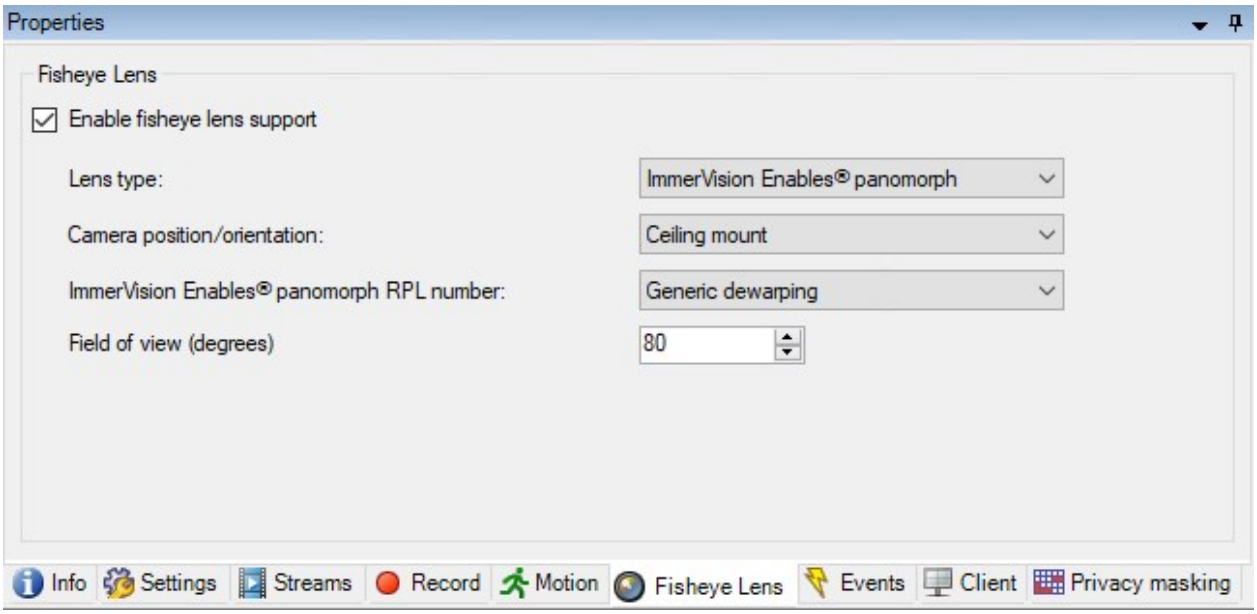
| Name | Beschreibung |
|---|---|
| | Wenn ein Wachrundgang vom System aktiviert wird, wird **Wachrundgang** angezeigt. |
| **Priorität** | Zeigt die PTZ-Priorität des Benutzers an. Sie können PTZ-Sitzungen nur von Benutzern oder Wachrundgangprofilen mit einer niedrigeren Priorität übernehmen. |
| **Zeitüberschreitung** | Zeigt die verbleibende Zeit der aktuellen reservierten oder manuellen PTZ-Sitzungen an. |
| **Reserviert** | Zeigt an, ob die aktuelle Sitzung eine reservierte PTZ-Sitzung ist oder nicht.<br>• **Wahr**: Reserviert<br>• **Falsch**: Nicht reserviert |

### Registerkarte „Fischaugen-Linse“ (Geräte)

Die folgenden Geräte besitzen eine Registerkarte **Fischaugen-Linse**:

- Fixierte Kameras mit einer Fischaugen-Linse

In der Registerkarte **Fischaugen-Linse** können Sie die Unterstützung für Fischaugen-Linsen für die ausgewählte Kamera aktivieren und konfigurieren.



Aufgaben auf der Registerkarte "Fischaugenobjektiv"

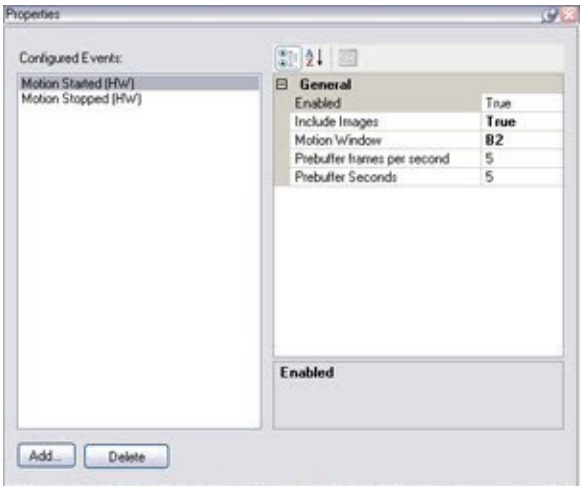
| Name | Beschreibung |
|---|---|
| **Fischaugenobjektiv-Unterstützung aktivieren** | Unterstützung für Fischaugen-Linse aktivieren und deaktivieren |

## Registerkarte „Ereignisse“ (Geräte)

Die folgenden Geräte besitzen eine Registerkarte **Ereignisse**:

- Kameras
- Mikrofone
- Eingänge

Zusätzlich zum Ereignis des Systems, können einige Geräte so eingestellt werden, dass sie Ereignisse auslösen. Sie können diese Ereignisse verwenden, wenn Sie auf Ereignissen basierende Regeln im System erstellen. Eigentlich passieren sie sogar direkt an der Hardware/Gerät als im Überwachungssystem.




Aufgaben auf der Registerkarte "Ereignisse"

| Name | Beschreibung |
|---|---|
| **Hinzufügen** und **Löschen** | Fügen Sie ein Ereignis für ein Gerät hinzu oder löschen Sie es |

Registerkarte „Ereignis“ (Eigenschaften)

| Name | Beschreibung |
|---|---|
| **Konfigurierte Ereignisse** | Welches Ereignis Sie auswählen und in der Liste für **Konfigurierte Ereignisse** hinzufügen können, hängt ganz vom Gerät und seinen Einstellungen ab. Für einige Gerätetypen ist die Liste leer. |
| **Allgemein** | Die Liste der Eigenschaften hängt vom Gerät und dem Ereignis ab. Damit das Ereignis wie gewollt funktioniert, müssen Sie einige oder alle Eigenschaften identisch sowohl auf dem Gerät als auch in dieser Registerkarte festlegen. |

### Registerkarte „Client“ (Geräte)

Die folgenden Geräte besitzen eine Registerkarte **Client**:

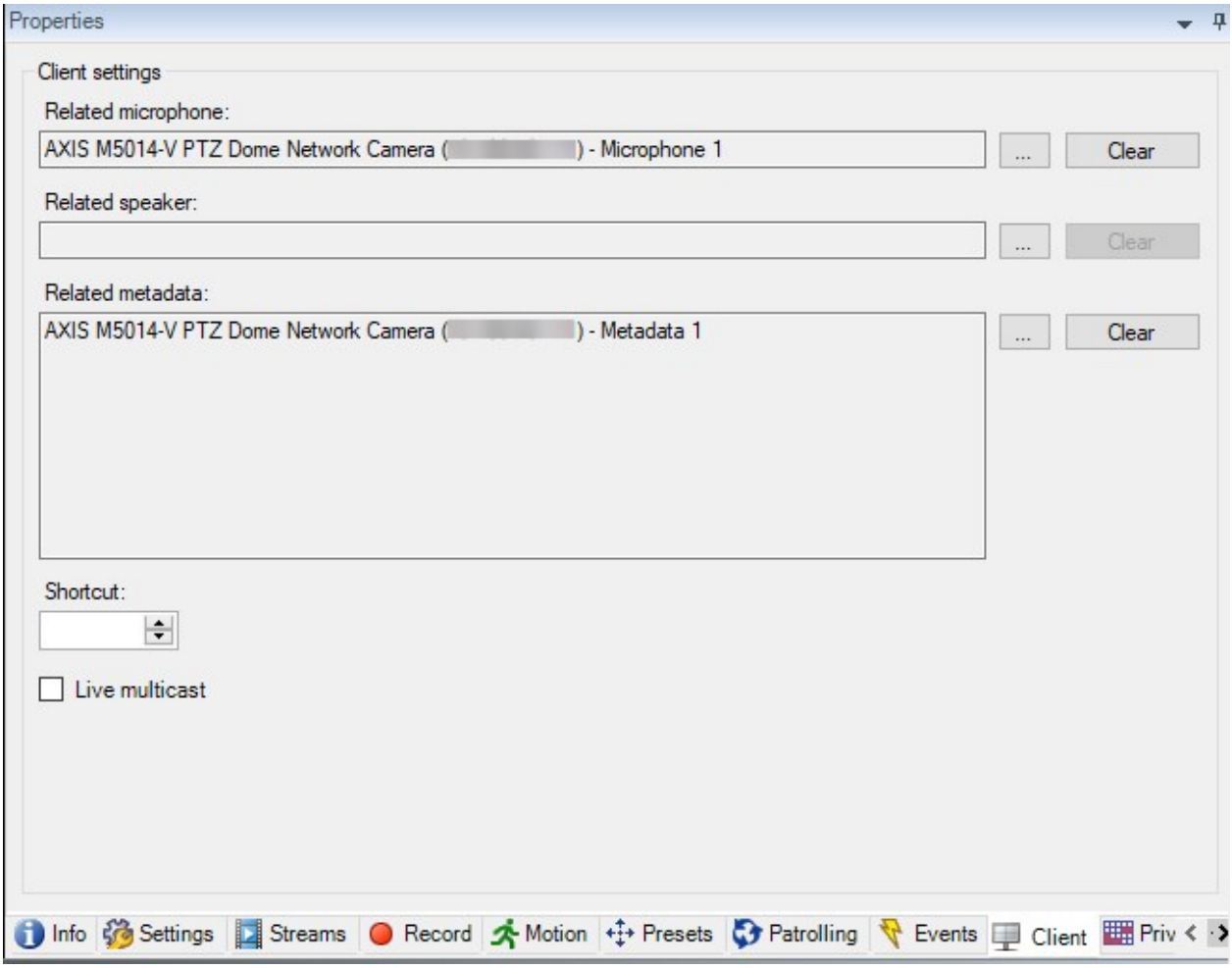
- Kameras

Auf der Registerkarte **Client** können Sie bestimmen, welche anderen Geräte angezeigt und gehört werden, wenn Sie eine Kamera im XProtect Smart Client verwenden.

Die zugehörigeb Geräte zeichnen auf, wann die Kamera aufzeichnet, siehe Aktivieren der Aufzeichnung auf zugehörigen Geräten auf Seite 247.

Sie können außerdem **Live-Multicast** auf der Kamera aktivieren. Es bedeutet, dass die Kamera Live-Streams über den Aufzeichnungsserver an die Clients multicastet.

Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet.




Eigenschaften der Registerkarte „Client“

| Name | Beschreibung |
|---|---|
| **Zugehöriges Mikrofon** | Legen Sie fest, von welchem Mikrofon an der Kamera XProtect Smart Client-Benutzer standardmäßig Audio empfangen. Der XProtect Smart Client-Benutzer kann ggf. manuell wählen, über ein anderes Mikrofon zuzuhören.<br>Geben Sie das Mikrofon an, das zur Push-Videokamera gehört, mit der Video mit Ton gestreamt werden soll.<br>Die zugehörigen Mikrofone zeichnen auf, wenn die Kamera aufzeichnet. |

| Name | Beschreibung |
|---|---|
| **Zugehöriger Lautsprecher** | Legen Sie fest, über welche Lautsprecher an der Kamera XProtect Smart Client-Benutzer standardmäßig sprechen. Der XProtect Smart Client-Benutzer kann bei Bedarf manuell einen anderen Lautsprecher auswählen.<br>Die zugehörigen Lautsprecher zeichnen auf, wenn die Kamera aufzeichnet. |
| **Zugehörige Metadaten** | Legen Sie ein oder mehrere Metadatengeräte an der Kamera fest, von welchem XProtect Smart Client-Benutzer Metadaten empfangen werden können.<br>Zugehörige Metadatengeräte zeichnen auf, wenn die Kamera aufzeichnet. |
| **Verknüpfung** | Definieren Sie Tastenkombinationen zu den Kameras, um die Kameraauswahl für die XProtect Smart Client-Benutzer zu erleichtern.<br>• Erstellen Sie jede Tastenkombination so, dass sie die Kamera eindeutig identifiziert.<br>• Die Kamera Kurzwahlnummer darf nicht länger als vier Ziffern sein. |
| **Live Multicast** | Ihr System unterstützt Multicast von Live-Streams vom Aufzeichnungsserver zum XProtect Smart Client. Zum Aktivieren von Multicast für Live-Streams von der Kamera, wählen Sie bitte das Kontrollkästchen aus.<br>Live-Multicasting funktioniert nur in dem Stream, den Sie auf der Registerkarte **Streams** als Standardstream für die Kamera angegeben haben.<br>Außerdem müssen Sie Multicasting für den Aufzeichnungsserver konfigurieren. Siehe Aktivieren Sie Multicasting für den Recording-Server auf Seite 222. |

| Name | Beschreibung |
|---|---|
| | Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet. |

### Registerkarte Einrichtung von Privatsphärenausblendung (Geräte)

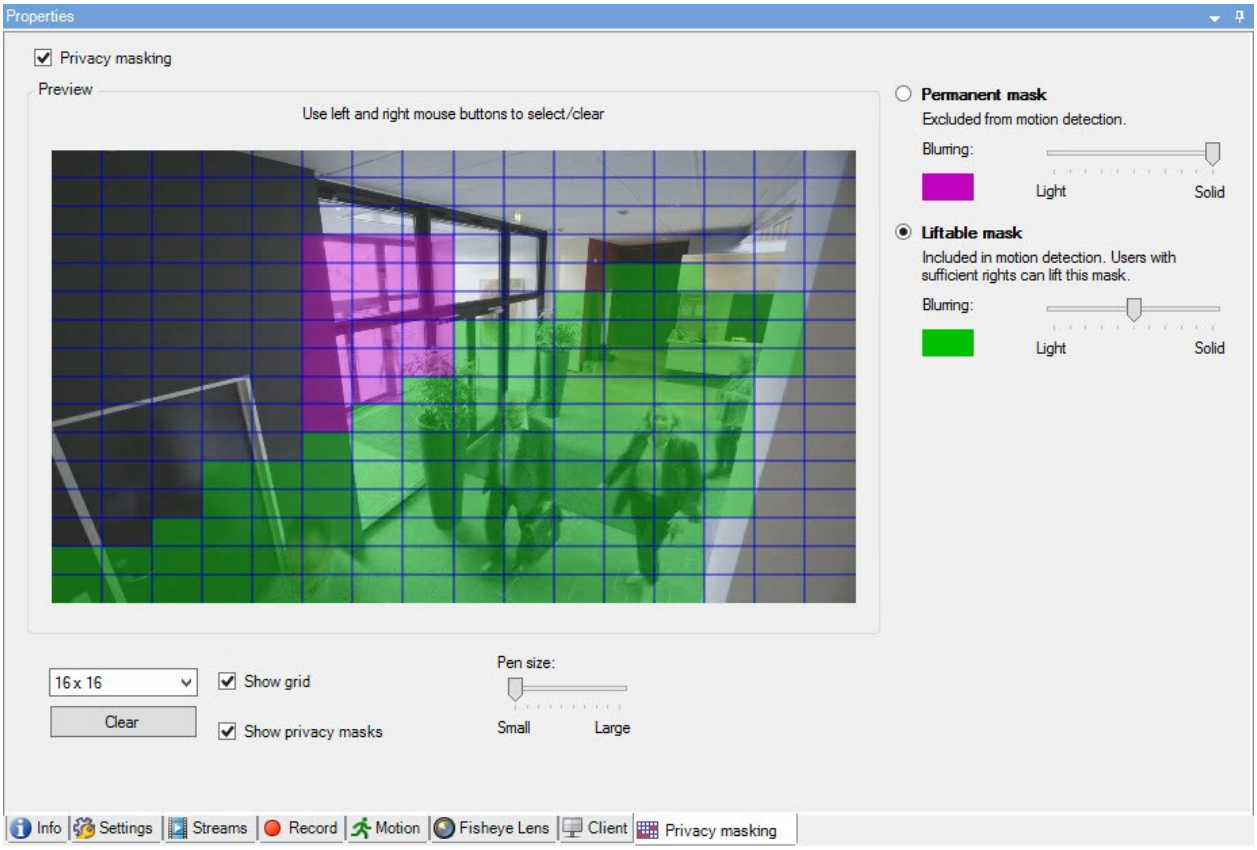
Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

XProtect Essential+ 2018 R1 und neuere Versionen unterstützen die Einrichtung von Privatsphärenausblendung nicht. Wenn Sie also ein Upgrade auf einem System vornehmen, in dem Privatzonenmasken eingerichtet sind, werden diese entfernt.

Folgende Geräte besitzen eine Registerkarte **Privatsphärenausblendung**:

- Kameras

Auf der Registerkarte **Privatsphärenausblendung** können Sie Privatzonenmaske für die ausgewählte Kamera aktivieren und konfigurieren.




Aufgaben auf der Registerkarte "Verdeckte Bildbereiche"

| Name | Beschreibung |
|---|---|
| **Privatsphärenausblendung** | Aktivieren/Deaktivieren von Privatsphärenausblendung<br>Privatsphärenausblendung (Erklärung) |
| **Dauerhaft verdeckt** und **Reversibel verdeckt** | Geben Sie an, ob Sie den Bildbereich dauerhaft oder reversibel verdecken wollen:<br>Privatzonenmasken festlegen |

Aufgaben im Zusammenhang mit verdeckten Bildbereichen

| Aufgabe | Beschreibung |
|---|---|
| Ändern Sie die Zeitüberschreitung für die entfernte Verdeckung von Bildbereichen für das Profil Smart Client in Verbindung mit der Rolle, welche die Genehmigung hat, verdeckte Bildbereiche freizulegen. | Ändern des Timeout für aufgehobene Privatzonenmasken |
| Geben oder entziehen Sie die Erlaubnis für eine Rolle, verdeckte Bildbereiche freizulegen. | Benutzerberechtigung zum Aufheben von Privatzonenmasken erteilen |
| Erstellen Sie einen Gerätebericht, mit Informationen über die aktuellen Einstellungen Ihrer Kameras zum Verdecken von Bildbereichen. | Erstellen Sie einen Bericht von der Konfiguration Ihrer Privatsphärenausblendung |

Registerkarte Privatsphärenausblendung (Eigenschaften)

| Name | Beschreibung |
|---|---|
| **Rastergröße** | Der Wert, den Sie in der Liste Rastergröße ausgewählt haben, bestimmt die Dichte des Rasters, egal ob es gezeigt wird, oder nicht.<br>Wählen Sie zwischen den Werten 8×8, 16×16, 32×32 oder 64×64. |
| **Löschen** | Löscht **alle** Privatzonenmasken, die Sie festgelegt haben. |
| **Gitter zeigen** | Aktivieren Sie das Kontrollkästchen **Gitter anzeigen**, um das Raster sichtbar zu machen. |
| **Privatzonenmasken anzeigen** | Wenn Sie das Kontrollkästchen **Privatzonenmasken anzeigen** (Standard), werden die permanenten Privatzonenmasken in der Vorschau in Violett und die aufhebbaren Privatzonenmasken in Grün dargestellt.<br>Milestone empfiehlt, dass Sie das Kästchen **Privatzonenmasken anzeigen** |

| Name | Beschreibung |
|---|---|
| | ausgewählt lassen, damit Sie und Ihre Kollegen die aktuelle Datenschutz-Konfiguration sehen können. |
| **Stiftgröße** | Verwenden Sie den Schieberegler **Stiftgröße**, um die Größen der Auswahl anzuzeigen, die Sie machen möchten, wenn Sie ins Raster klicken und ziehen, um Bereiche auszuwählen. Der Standard ist klein, was einem Quadrat im Raster entspricht. |
| **Permanente Maske** | Wird in der Vorschau auf dieser Registerkarte und auf der Registerkarte **Motion** in Violett dargestellt.<br><br>Permanente Privatzonenmasken sind immer sichtbar in XProtect Smart Client und können nicht aufgehoben werden. Diese können benutzt werden, um Bereiche des Videos abzudecken, die niemals Überwachung erfordern, wie öffentliche Bereiche, in denen keine Überwachung genehmigt wird. Bewegungserkennung ist von permanenten Privatzonenmasken ausgeschlossen.<br><br>Sie können die Abdeckung von Privatzonenmasken entweder als intransparent oder unscharf angeben. Die Deckungseinstellungen gelten sowohl für Live-Videos als auch für Aufzeichnungen. |
| **Aufhebbare Maske** | Wird in der Vorschau auf dieser Registerkarte in Grün dargestellt.<br><br>Aus Datenschutzgründen verdeckte Bildbereiche können von Benutzern mit ausreichenden Benutzerrechten ggf. aufgehoben werden XProtect Smart Client. Als Standard werden die Privatzonenmasken für 30 Minuten aufgehoben, oder bis der Benutzer sie wieder anwendet. Seien Sie sich darüber im Klaren, dass Privatzonenmasken auf Video von allen Kameras aufgehoben werden, auf die der Benutzer Zugriff hat.<br><br>Wenn der XProtect Smart Client-Benutzer nicht über die Berechtigung verfügt, aus Datenschutzgründen verdeckte Bildbereiche freizulegen, verlangt das System nach einem Benutzer, der dazu berechtigt ist.<br><br>Sie geben die Abdeckung von Privatzonenmasken entweder als intransparent oder als unscharf an. Die Deckungseinstellungen gelten sowohl für Live-Videos als auch für Aufzeichnungen. |
| **Unschärfe** | Benutzen Sie den Schieber, um das Unschärfeniveau der Privatzonenmasken auszuwählen oder die Deckung auf voll intransparent zu stellen. |

| Name | Beschreibung |
|---|---|
| | Als Standard ist die Deckung von Bereichen mit permanenten Privatzonenmasken durchgehend (intransparent). Als Standard sind aufhebbare Privatzonenmasken halbscharf gedeckt.<br><br>Sie können die Client-Benutzer über das Erscheinen von permanenten und aufhebbaren Privatzonenmasken informieren, damit sie in der Lage sind, diese zu unterscheiden. |

## Das Fenster "Hardwareeigenschaften"

Sie haben mehrere Optionen, um zu den Aufzeichnungsservern in Ihrem System Hardware hinzuzufügen.

Wenn Ihre Hardware sich hinter einem NAT-fähigen Router oder einer Firewall befindet, müssen Sie möglicherweise eine andere Portnummer bestimmen und den Router/die Firewall so konfigurieren, dass die von der Hardware genutzten Port- und IP-Adressen zugewiesen werden.

Der Assistent zum **Hardware hinzufügen** hilft Ihnen dabei, in Ihrem Netzwerk Hardware wie etwa Kameras und Videoencoder zu finden und diese den Aufzeichnungsservern in Ihrem System hinzuzufügen. Mit dem Assistenten können Sie auch Remote-Server für Milestone Interconnect-Einrichtungen hinzufügen. Fügen Sie jeweils nur bei **einem Aufzeichnungsserver** zur selben Zeit Hardware hinzu.

### Registerkarte „Info (Hardware)“

Weitere Informationen zu der Registerkarte **Info** für Fernserver finden Sie unter Registerkarte „Info (Remote-Server)“ auf Seite 464.

| Name | Beschreibung |
|---|---|
| **Name** | Geben Sie einen Namen ein. Das System verwendet den Namen, wenn die Hardware im System und den Clients aufgelistet wird. Der Name muss nicht einzigartig sein.<br><br>Wenn Sie Hardware neu benennen, wird der Name im Management Client global geändert. |

| Name | Beschreibung |
|---|---|
| **Beschreibung** | Geben Sie eine Beschreibung der Hardware ein (optional). Die Beschreibung taucht in einer Anzahl Listen im System auf. Zum Beispiel, wenn Sie den Mauszeiger über den Hardware-Namen im Bereich **Übersicht** halten:<br>  |
| **Modell** | Identifiziert das Hardware-Modell. |
| **Seriennummer** | Seriennummer der Hardware, wie vom Hersteller angegeben. Die Seriennummer ist oft, aber nicht immer, mit der MAC-Adresse identisch. |
| **Treiber** | Identifiziert den Treiber, der die Verbindung mit der Hardware verwaltet. |
| **IE** | Öffnet die Standard-Startseite des Hardware-Anbieters. Sie können diese Seite zur Administration der Hardware nutzen. |
| **Adresse** | Hostname oder IP-Adresse der Hardware. |
| **MAC-Adresse** | Legt die Media-Access-Control-Adresse (MAC) der Systemhardware fest. Eine MAC-Adresse ist eine zwölfstellige Hexadezimalzahl, die jedes Gerät in einem Netzwerk eindeutig identifiziert. |
| **Firmware-Version:** | Die Firmware-Version des Hardware-Gerätes. Damit das System die aktuelle Version anzeigt, führen Sie nach jeder Firmware-Aktualisierung den Assistenten zur **Aktualisierung der Hardwaredaten** aus. |
| **Letzte Passwortänderung** | Das Feld **Zuletzt geändertes Passwort** zeigt den Zeitstempel der letzten Passwortänderung an, basierend auf den lokalen Zeiteinstellungen desjenigen Computers, von dem aus das Passwort geändert wurde. |
| **Datum der letzten Aktualisierung der Hardware-Daten:** | Uhrzeit und Datum der letzten Aktualisierung der Hardwaredaten. |

### Registerkarte Einstellungen (Hardware)

Auf der Registerkarte **Einstellungen** können Sie Einstellungen für die Hardware bestätigen oder bearbeiten.

Der Inhalt der Registerkarte **Einstellungen** wird durch die ausgewählte Hardware bestimmt und variiert je nach Hardware-Typ. Im Fall einiger Hardware-Typen enthält die Registerkarte **Einstellungen** keinen oder schreibgeschützten Inhalt.

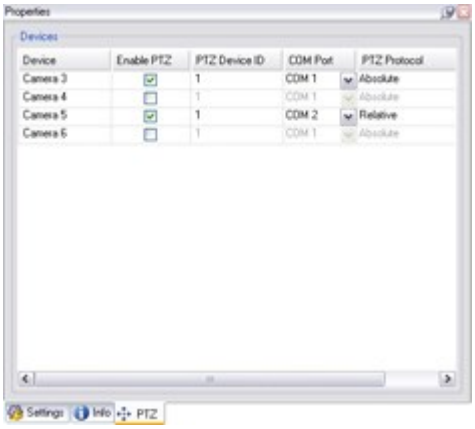
Weitere Informationen zu der Registerkarte **Einstellungen** für Fernserver finden Sie unter Registerkarte "Einstellungen" (Remote Server) auf Seite 465.

### Registerkarte „PTZ (Videoencoder)“

Auf der Registerkarte **PTZ** können Sie PTZ (Pan/Tilt/Zoom) für Videoencoder aktivieren. Die Registerkarte ist verfügbar, wenn das ausgewählte Gerät ein Videoencoder ist oder der Treiber Kameras mit und ohne PTZ unterstützt.

Sie müssen die Verwendung von PTZ separat für jeden Kanal des Videoencoders auf der Registerkarte **PTZ** aktivieren, bevor Sie die PTZ-Funktionen der mit dem Videoencoder verbundenen PTZ-Kameras anwenden können.

Nicht alle Videoencoder unterstützen die Verwendung von PTZ-Kameras. Selbst Videoencoder, welche die Verwendung von PTZ-Kameras unterstützen, müssen möglicherweise konfiguriert werden, bevor diese Kameras benutzt werden können. Dies geschieht üblicherweise durch die Installation zusätzlicher Treiber über eine Browser-basierte Konfigurationsoberfläche auf der IP-Adresse des Geräts.




Die Registerkarte **PTZ** – PTZ ist für zwei Kanäle auf einem Videoencoder aktiviert.

# Clientknoten

## Clients (Knoten)

Dieser Abschnitt beschreibt, wie die Benutzeroberfläche in XProtect Smart Client für Betreiber und in Management Client für Systemadministratoren benutzerdefiniert angepasst wird.

## Smart Wall (Client-Knoten)

### Smart Wall Eigenschaften

#### Registerkarte „Info“

Auf der Registerkarte **Info** für eine Smart Wall Definition können Sie Smart Wall Eigenschaften hinzufügen und bearbeiten.

| Name | Beschreibung |
|---|---|
| **Name** | Der Name der Smart Wall-Definition. Angezeigt in XProtect Smart Client als der Smart Wall Ansichtsgruppenname. |
| **Beschreibung** | Eine Beschreibung der Smart Wall-Definition. Die Beschreibung wird nur intern im XProtect Management Client verwendet. |
| **Statustext** | Kamera- und Systemstatus-Informationen in Kameraansichts-Elementen anzeigen. |
| **Keine Titelleiste** | Die Titelleiste auf allen Ansichtselementen auf der Videowant verbergen. |
| **Titelleiste** | Die Titelleiste auf allen Ansichtselementen auf der Videowant anzeigen. |

#### Die Registerkarte "Voreinstellungen"

Auf der Registerkarte **Voreinstellungen** können Sie für eine Smart Wall Definition Smart WallVoreinstellungen[1] hinzufügen und bearbeiten.

[1]Ein vorgegebenes Layout für einen oder mehrere Smart Wall-Monitore in XProtect Smart Client. Voreinstellungen legen fest, welche Kameras angezeigt werden und wie der Inhalt auf jedem Bildschirm auf der Videowand angeordnet ist.

| Name | Beschreibung |
|---|---|
| **Hinzufügen** | Fügen Sie Ihrer Smart Wall-Definition eine Voreinstellung hinzu.<br>Geben Sie einen Namen und eine Beschreibung für die Voreinstellung ein. |
| **Bearbeiten** | Den Namen oder die Beschreibung einer Voreinstellung bearbeiten. |
| **Löschen** | Eine Voreinstellung löschen. |
| **Aktivieren** | Die Voreinstellung auf die Smart Wall Bildschirme anwenden, die für ihre Verwendung konfiguriert sind. Um eine Voreinstellung automatisch anzuwenden, müssen Sie eine Regel erstellen, die sie verwendet. |

**Die Registerkarte "Layout"**

Auf der Registerkarte **Layout** für eine Smart Wall Definition ordnen Sie die Monitore so an, dass ihre Positionen der Art und Weise entsprechen, wie die physischen Monitore auf der Videowand angebracht sind. Das Layout wird auch in XProtect Smart Client verwendet.

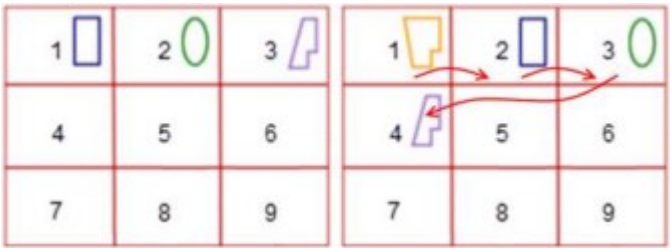
| Name | Beschreibung |
|---|---|
| **Bearbeiten** | Passen Sie die Positionierung der Monitore an. |
| **Bewegung** | Um einen Monitor in eine neue Position zu verschieben, wählen Sie den Monitor aus und ziehen Sie ihn in die gewünschte Position, oder klicken Sie auf eine der Pfeiltasten, um den Monitor in der ausgewählten Richtung zu verschieben. |
| **Zoomschaltfläche** | Verwenden Sie die Zoom-Funktion, um die Smart Wall Layoutvorschau größer oder kleiner zu machen, damit Sie die Monitore richtig positionieren können. |
| **Name** | Der Name des Bildschirms. Der Name wird in XProtect Smart Client angezeigt. |
| **Größe** | Die Größe des physischen Bildschirms an der Videowand. |
| **Seitenverhältnis** | Das Höhe-/Breitenverhältnis des physischen Bildschirms an der Videowand. |

Bildschirmeigenschaften

### Registerkarte „Info“

Auf der Registerkarte **Info** für einen Monitor in einer Smart Wall Voreinstellung können Sie Monitore hinzufügen und Monitoreinstellungen bearbeiten.

| Name | Beschreibung |
|---|---|
| **Name** | Der Name des Bildschirms. Der Name wird in XProtect Smart Client angezeigt. |
| **Beschreibung** | Eine Beschreibung des Bildschirms. Die Beschreibung wird nur intern im XProtect Management Client verwendet. |
| **Größe** | Die Größe des physischen Bildschirms an der Videowand. |
| **Seitenverhältnis** | Das Höhe-/Breitenverhältnis des physischen Bildschirms an der Videowand. |
| **Leere Voreinstellung** | Legt fest, was auf einen Monitor mit leerem Voreinstellungs-Layout angezeigt werden soll, wenn eine neue Smart Wall Voreinstellung ausgelöst oder in XProtect Smart Client ausgewählt wird:<br>• Wählen Sie **Beibehalten**, um den derzeitigen Inhalt auf dem Bildschirm beizubehalten.<br>• Wählen Sie **Löschen**, um den Inhalt zu löschen, damit nichts auf dem Bildschirm angezeigt wird. |
| **Leeres Voreinstellungselement** | Legt fest, was in einem leeren Voreinstellungselement angezeigt werden soll, wenn eine neue Smart Wall Voreinstellung ausgelöst oder in XProtect Smart Client ausgewählt wird:<br>• Wählen Sie **Beibehalten**, um den derzeitigen Inhalt im Layout-Element beizubehalten.<br>• Wählen Sie **Löschen**, um den Inhalt zu löschen, damit nichts im Layout-Element angezeigt wird. |
| **Elementeinfügung** | Legt fest, wie Kameras in das Monitor-Layout eingefügt werden, wenn sie in der XProtect Smart Client angezeigt werden: |

| Name | Beschreibung |
|---|---|
| | • **Unabhängig** - es ändert sich nur der Inhalt der betreffenden Layout-Position. Die übrigen Inhalte im Layout bleiben unverändert.<br>• **Verknüpft** - die Inhalte der Layoutpositionen werden von links nach rechts geschoben. Wird z. B. eine Kamera an der Position 1 eingefügt, wird die Kamera, die sich vorher an der Position 1 befand, an die Position 2 verschoben, und die Kamera, die sich vorher an der Position 2 befand, wird an die Position 3 veerschoben usw., wie in diesem Beispiel dargestellt:<br>  |

**Die Registerkarte "Voreinstellungen"**

In der Registerkarte **Voreinstellungen** für einen Bildschirm in einer Smart Wall-Voreinstellung können Sie Layout und Inhalt der Anzeige in der ausgewählten Smart Wall-Voreinstellung bearbeiten.

| Name | Beschreibung |
|---|---|
| **Voreinstellung** | Eine Liste an Smart Wall Voreinstellungen für die ausgewählte Smart Wall Definition. |
| **Bearbeiten** | Klicken Sie auf **Bearbeiten**, um das Layout und den Inhalt des ausgewählten Bildschirms zu bearbeiten.<br>Klicken Sie doppelt auf eine Kamera, um sie zu entfernen.<br>Klicken Sie auf **Löschen**, um ein neues Layout festzulegen, oder um den Bildschirm in der Smart Wall-Voreinstellung auszuschließen, damit der Bildschirm für andere Inhalte, die nicht von dieser Smart Wall-Voreinstellung gesteuert werden, zur Verfügung steht.<br>Klicken SIe auf  , um das für Ihren Bildschirm gewünschte Layout auszuwählen, und klicken Sie auf **OK**. |

## Smart Client Profile (Client-Knoten)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Auf den folgenden Registerkarten können Sie die Eigenschaften der einzelnen Smart Client Profile festlegen. Sie können die Einstellungen bei Bedarf im Management Client sperren, damit XProtect Smart Client-Benutzer sie nicht ändern können.

Um Smart Client Profile zu erstellen oder zu bearbeiten, erweitern Sie **Client** und wählen Sie **Smart Client Profile**.

### Registerkarte „Info“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Info** | Name und Beschreibung, Priorität vorhandener Profile und ein Überblick über die Rollen, die das Profil verwenden.<br><br>Wenn ein Benutzer mehr als eine Rolle hat und diese Rollen jeweils ein eigenes Smart Client-Profil haben, erhält der Benutzer das Smart Client-Profil mit der höchsten Priorität. |

### Registerkarte Allgemein (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Allgemein** | Einstellungen wie Anzeigen/Verbergen und Minimieren und Maximieren der Menüeinstellungen, An-/Abmeldung, Systemstart, Zeitüberschreitung, Info- und Benachrichtigungsoptionen sowie aktivieren oder deaktivieren bestimmter Registerkarten in XProtect Smart Client. |

| Registerkarte | Beschreibung |
|---|---|
| | Mit den Einstellungen für **Kamerafehlermeldungen**, **Server-Fehlermeldungen**, und **Live-Video-Fehlermeldungen** können Sie einstellen, ob diese Fehlermeldungen als Overlay, als schwarzes Bild mit Overlay oder ausgeblendet angezeigt werden sollen.<br><br>Die **Meldung Live-Video gestoppt** wird angezeigt, XProtect Smart Client wenn die Live-Übertragung der Kamera gestoppt wird. Wenn die Kamera zum Beispiel keine Bilder mehr sendet, obwohl sie verbunden ist.<br><br>⚠ Wenn Sie die Fehlermeldungen von der Kamera **Verbergen**, besteht das Risiko, dass das Bedienpersonal übersieht, dass die Verbindung zu einer Kamera unterbrochen wurde.<br><br>Mit der Einstellung **Kameras während einer Suche erlaubt** können Sie steuern, wie viele Kameras die Bediener in XProtect Smart Client zu Suchen hinzufügen können. Die Begrenzung der Anzahl der Kameras vermeidet eine Überlastung des Systems.<br><br>Die Einstellung **Online-Hilfe** gibt Ihnen die Möglichkeit, das Hilfesystem in XProtect Smart Client zu deaktivieren.<br><br>Die Einstellung **Video-Anleitungen** gibt Ihnen die Möglichkeit, die Schaltfläche **Video-Anleitungen** in XProtect Smart Client zu deaktivieren. Die Schaltfläche leitet den Benutzer auf die Seite mit den Video-Anleitungen um: https://www.milestonesys.com/support/help-yourself/video-tutorials/ |

### Registerkarte Erweitert (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Erweitert** | Erweiterte Einstellungen wie etwa die maximale Anzahl an Dekodierungsthreads, Deinterlacing und Zeitzoneneinstellungen.<br><br>Die **maximale Anzahl an Dekodierungsthreads** steuert, wie viele Dekodierungsthreads zur Dekodierung von Video-Streams verwendet werden. Diese Option trägt zur Verbesserung der Leistung auf Multicore-Computern im Live- und im |

| Registerkarte | Beschreibung |
|---|---|
| | Wiedergabemodus bei. Die genaue Leistungsverbesserung ist abhängig vom Video-Stream. Diese Einstellung ist hauptsächlich relevant, wenn in hohem Maße codierte hochauflösende Videostreams wie H.264/H.265 verwendet werden, bei denen das Leistungssteigerungspotenzial signifikant sein kann. Sie ist weniger relevant, wenn beispielsweise JPEG oder MPEG-4 verwendet wird.<br><br>Bei **Deinterlacing** wandeln Sie das Video in ein Format ohne Interlacing um. Beim Interlacing wird definiert, wie ein Bild auf einem Bildschirm aktualisiert wird. Das Bild wird aktualisiert, indem zunächst die ungeraden Zeilen und dann die geraden Zeilen des Bildes abgetastet werden. Dies ermöglicht eine höhere Bildwiederholrate, weil während jedes Lesevorgangs weniger Informationen verarbeitet werden müssen. Das Interlacing kann jedoch ein Flackern bewirken bzw. die Änderungen an der Hälfte der Bildzeilen können wahrnehmbar sein.<br><br>**Adaptives Streaming** ermöglicht XProtect Smart Client das automatische Auswählen der Live-Videostreams, deren Auflösung am besten zu den Streams passt, die von dem zu betrachteten Gegenstand gefordert wird. Auf diese Weise wird die Belastung der CPU und der GPU gesenkt und damit Dekodierfähigkeit und -leistung des Computers verbessert. Hierfür muss Multi-Streaming von Live-Videostreams in verschiedenen Auflösungen konfiguriert werden, siehe Verwaltung von Multi-Streaming. Das adaptive Streaming kann sowohl im Live- als auch im Wiedergabemodus angewendet werden. Im Wiedergabemodus wird das adaptive Streaming als adaptive Wiedergabe bezeichnet. Die adaptive Wiedergabe setzt voraus, dass zwei Streams auf Aufzeichnung eingestellt sind. Weitere Informationen zum Hinzufügen von Streams für adaptives Streaming im Live-Modus und für adaptive Wiedergabe finden Sie unter Stream hinzufügen auf Seite 250. |

### Registerkarte „Live“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Live** | Verfügbarkeit des Live-Modus und anderer Live-Funktionen, Wiedergabe von Kameras, Schaltflächen für Kamera-Overlays und Begrenzungsrahmen sowie MIP Plug-ins für Live-Aufnahmen. |

### Registerkarte „Wiedergabe“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Wiedergabe** | Verfügbarkeit des Wiedergabemodus und anderer Wiedergabe-Funktionen, Layout für ausgedruckte Berichte, unabhängige Wiedergabe, Lesezeichen und Begrenzungsrahmen  sowie MIP Plug-ins für die Wiedergabe. |

### Registerkarte Einrichtung (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Konfiguration** | Verfügbarkeit allgemeiner Einrichtung/Fensterbereiche/Schaltflächen, auf die Einrichtung bezogenes MIP Plug-in und Berechtigungen zur Bearbeitung einer Karte und zur Bearbeitung der Pufferung für Live-Videoaufzeichnungen. |

### Registerkarte "Export" (Smart Client Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Exportieren** | Pfade, Privatzonenmasken, Video- und Standbildformate und Anweisungen zum Export selbiger, zum Export von Formaten für XProtect Smart Client – Player und vieles mehr. |

### Registerkarte „Zeitachse“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Zeitlinie** | Ob Audio aufgenommen werden soll oder nicht, Zeit- und Bewegungsanzeige und der Umgang mit Wiedergabelücken.<br>Außerdem können Sie auswählen, ob weitere Daten oder weitere Markierungen aus anderen Quellen angezeigt werden sollen. |

### Registerkarte Zutrittskontrolle (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Zutrittskontrolle** | Wählen Sie aus, ob Zutrittsanforderungs-Benachrichtigungen auf dem XProtect Smart Client-Bildschirm angezeigt werden sollen, wenn sie von Ereignissen ausgelöst werden. |

### Registerkarte Alarm-Manager (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Alarm-Manager** | Sie können angeben, ob: |

| Registerkarte | Beschreibung |
|---|---|
| | • Desktop-Benachrichtigungen für Alarme auf den Computern angezeigt werden sollen, auf denen XProtect Smart Client installiert ist. Die Benachrichtigungen erscheinen nur, wenn XProtect Smart Client läuft - auch wenn es minimiert ist<br><br>Desktop-Benachrichtigung für Alarme erscheinen nur, wenn die Alarme bestimmte Prioritäten haben, z.B. **Mittel** oder **Hoch**. Um zu konfigurieren, welche Alarmprioritäten Benachrichtigungen auslösen, gehen Sie auf **Alarme** > **Alarmdateneinstellungen** > **Alarmdatenniveaus**. Aktivieren Sie für jede erforderliche Alarmpriorität das Kontrollkästchen **Desktop-Benachrichtigungen aktivieren**. Siehe Alarmdateneinstellungen (Alarmknoten).<br><br>• Alarme auf den Computern, auf denen XProtect Smart Client installiert sind, akustische Benachrichtigungen abspielen sollen. Die akustischen Benachrichtigungen nur abgespielt werden sollen, wenn XProtect Smart Client läuft - auch wenn es minimiert ist<br><br>Akustische Benachrichtigungen für Alarme nur abgespielt werden sollen, wenn dem Alarm ein Ton zugeordnet ist. Um Töne mit Alarmen zu verknüpfen, gehen Sie zu **Alarme** > **Alarmdateneinstellungen** > **Alarmdatenebenen**. Wählen Sie für jede gewünschte Alarmpriorität den Ton aus, der dem Alarm zugeordnet werden soll. Siehe Alarmdateneinstellungen (Alarmknoten). |

### Registerkarte „Smart Map“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

| Registerkarte | Beschreibung |
|---|---|
| **Smart Map** | Angabe der Einstellungen für die Smart-Map-Funktion. |

| Registerkarte | Beschreibung |
|---|---|
| | Sie können angeben, ob:<br>• Milestone Map Service als geographischer Hintergrund verwendet werden kann<br>• OpenStreetMaps als geographischer Hintergrund verwendet werden kann<br>• XProtect Smart Client erstellt automatisch Standorte, wenn ein Benutzer ein benutzerdefiniertes Overlay zur Smart Map zufügt.<br>Sie können außerdem angeben, wie oft das System Daten in Verbindung mit Smart Maps von Ihrem Computer löschen soll. Damit XProtect Smart Client Smart Map schneller anzeigen kann, speichert der Client die Kartendaten im Cache auf Ihrem Computer. Im Laufe der Zeit kann dies Ihren Computer verlangsamen.<br>Caching kommt nicht zur Anwendung für Google Maps.<br>Wenn Sie Bing Maps oder Google Maps als geographische Hintergründe verwenden möchten, geben Sie einen Bing Maps API-Schlüssel, oder einen Maps Static API-Schlüssel von Google ein. |

## Management Client Profile (Client-Knoten)

Diese Funktion ist nur in XProtect Corporate verfügbar.

### Registerkarte „Info“ (Management Client-Profile)

Auf der Registerkarte **Info** können Sie Folgendes für Management Client-Profile festlegen:

| Komponente | Voraussetzung |
|---|---|
| **Name** | Geben Sie einen Namen für das Management Client-Profil ein. |
| **Priorität** | Verwenden Sie die Pfeile nach oben und unten, um eine Priorität für das Management Client-Profil festzulegen. |

| Komponente | Voraussetzung |
|---|---|
| **Beschreibung** | Geben Sie eine Beschreibung für das Profil ein. Dies ist optional. |
| **Rollen, die das Management Client-Profil** verwenden: | Dieses Feld zeigt die Rollen an, die Sie dem Management Client-Profil zugeordnet haben. Sie können dieses Feld nicht bearbeiten. |

### Registerkarte „Profil“ (Management Client-Profile)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Auf der Registerkarte **Profil** können Sie die Sichtbarkeit der folgenden Elemente von der Oberfläche des Management Client-Benutzers aktivieren oder deaktivieren:

#### Navigation

In diesem Abschnitt können Sie entscheiden, ob ein dem Management Client-Profil zugeordneter Administrator die unterschiedlichen Funktionen im Bereich **Navigation** sehen kann.

| Navigationselement | Beschreibung |
|---|---|
| **Grundlagen** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Lizenzinformationen** und **Standortinformationen** anzuzeigen. |
| **Fernzugriffsdienste** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, die **Axis One-click-Kameraverbindung** anzuzeigen. |
| **Server** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Aufzeichnungsserver** und **Failover-Server** anzuzeigen. |
| **Geräte** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Kameras**, **Mikrofone**, **Lautsprecher**, **Metadaten**, **Eingang** und |

| Navigationselement | Beschreibung |
|---|---|
| | **Ausgang** anzuzeigen. |
| **Client** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Smart Wall**, **Ansichtsgruppen**, **Smart Client-Profile**, **Management Client-Profile** und **Matrix** anzuzeigen. |
| **Regeln und Ereignisse** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Regeln**, **Zeitprofile**, **Benachrichtigungsprofile**, **benutzerdefinierte Ereignisse**, **Analyseereignisse** und **generische Ereignisse** anzuzeigen. |
| **Sicherheit** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Rollen** und **Basisnutzer** anzuzeigen. |
| **System-Dashboard** | Hiermit kann der mit dem Management Client-Profil verbundenen Administratorbenutzer **System Monitor**, **System-Monitor-Schwellen**, **Beweissicherung**, **Aktuelle Aufgaben** und **Konfigurationsberichte** sehen. |
| **Server-Protokolle** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, Systemprotokolle, Auditprotokolle und durch Regeln ausgelöste Protokolle anzuzeigen. |
| **Zutrittskontrolle** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Zutrittskontrollfunktionen** anzuzeigen, wenn Sie Ihrem System Zutrittskontroll-Systemintegrationen oder Plug-ins hinzugefügt haben. |

Details

In diesem Abschnitt können Sie entscheiden, ob ein dem Management Client-Profil zugeordneter Administrator die unterschiedlichen Registerkarten für einen spezifischen Gerätekanal anzeigen darf, wie etwa die Registerkarte **Einstellungen** oder die Registerkarte **Aufzeichnung** für Kameras.

| Gerätekanal | Beschreibung |
|---|---|
| **Kameras** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle kamerabezogenen Einstellungen und Registerkarten |

| Gerätekanal | Beschreibung |
|---|---|
| | anzuzeigen. |
| **Mikrofone** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle mikrofonbezogenen Einstellungen und Registerkarten anzuzeigen. |
| **Lautsprecher** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle lautsprecherbezogenen Einstellungen und Registerkarten anzuzeigen. |
| **Metadaten** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle metadatenbezogenen Einstellungen und Registerkarten anzuzeigen. |
| **Eingang** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle eingangsbezogenen Einstellungen und Registerkarten anzusehen. |
| **Ausgang** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle ausgangsbezogenen Einstellungen und Registerkarten anzusehen. |

Menü „Extras“

In diesem Abschnitt können Sie entscheiden, ob ein dem Management Client-Profil zugeordneter Administrator die Elemente des Menüs **Werkzeuge** ansehen kann.

| Werkzeugmenüoption | Beschreibung |
|---|---|
| **Registrierte Services** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Registrierte Dienste** anzusehen. |
| **Effektive Rollen** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Effektive Rollen** anzusehen. |
| **Optionen** | Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Optionen** anzusehen. |

Föderale Sites

In diesem Abschnitt können Sie entscheiden, ob ein dem Management Client-Profil zugeordneter Administrator den Bereich **Hierarchie der föderalen Standorte** ansehen kann.

# Regel- und Ereignisknoten

## Regeln (der Knoten "Regeln und Ereignisse")

Ihr System umfasst eine Reihe von Standardregeln, die Sie für Grundfunktionen verwenden können, ohne selbst etwas einrichten zu müssen. Sie können die Standardregeln nach Bedarf deaktivieren oder bearbeiten. Wenn Sie die Standardregeln bearbeiten oder deaktivieren, funktioniert das System möglicherweise nicht wie gewünscht und es ist nicht sichergestellt, dass Video- oder Audiofeeds automatisch ins System übertragen werden.

| Standardregel | Beschreibung |
|---|---|
| **Zu Voreinstellung gehen, wenn PTZ ausgeführt wurde** | Stellt sicher, dass PTZ-Kameras in ihre jeweiligen standardmäßigen Preset Positionen gehen, nachdem Sie diese manuell betätigt haben. Diese Regel ist standardmäßig nicht aktiviert.<br>Auch, wenn Sie die Regel aktiviert haben, müssen Sie standardmäßigen Preset-Positionen für die relevanten PTZ-Kameras definiert haben, damit die Regel funktioniert. Gehen Sie dazu zur Registerkarte **Voreinstellungen**. |
| **Audio auf Anfrage abspielen** | Stellt sicher, dass Videos automatisch aufgezeichnet werden, wenn eine externe Anforderung eingeht.<br>Die Anforderung wird immer von einem System ausgelöst, das extern mit Ihrem System integriert wird, und die Regel wird in erster Linie von Integratoren externer Systeme oder Plug-ins verwendet. |
| **Aufzeichnung für Lesezeichen** | Sorgt dafür, dass automatisch ein Video aufgezeichnet wird, wenn ein Anwender ein Lesezeichen im XProtect Smart Client festlegt. Voraussetzung ist, dass die Aufzeichnung für die entsprechenden Kameras aktiviert wurde. Aufzeichnung ist standardmäßig aktiviert.<br>Die Standardaufzeichnungszeit für diese Regel ist: drei |

| Standardregel | Beschreibung |
|---|---|
| | Sekunden, bevor das Lesezeichen gesetzt ist, und 30 Sekunden, nachdem das Lesezeichen gesetzt ist. Sie können die Standardaufzeichnungszeiten in der Regel bearbeiten. Der Voralarm-Puffer, den Sie auf der Registerkarte „Aufzeichnung“ festlegen, muss gleich lang wie oder länger als die Voralarmaufzeichnungszeit sein. |
| **Bei Bewegung aufzeichnen** | Stellt sicher, dass das Video aufgezeichnet wird, solange im Videobild von Kameras Bewegung erkannt wird (vorausgesetzt, Aufzeichnung ist für die relevanten Kameras aktiviert). Aufzeichnung ist standardmäßig aktiviert.<br><br>Die Standardregel legt zwar Aufzeichnungen basierend auf erkannter Bewegung fest, stellt aber nicht sicher, dass das System tatsächlich Video aufzeichnet, da Sie Aufzeichnung bei einer oder mehreren Kameras deaktiviert haben könnten. Auch bei aktivierter Aufzeichnung kann die Qualität der Aufzeichnungen durch die jeweiligen Aufzeichnungseinstellungen der einzelnen Kameras beeinflusst werden. |
| **Aufzeichnung nach Bedarf** | Stellt sicher, dass Videos automatisch aufgezeichnet werden, wenn eine externe Anforderung eingeht (vorausgesetzt, Aufzeichnung ist für die relevanten Kameras aktiviert). Aufzeichnung ist standardmäßig aktiviert.<br><br>Die Anforderung wird immer von einem System ausgelöst, das extern mit Ihrem System integriert wird, und die Regel wird in erster Linie von Integratoren externer Systeme oder Plug-ins verwendet. |
| **Start des Audiofeeds** | Sorgt dafür, dass Audiofeeds aller angeschlossenen Mikrofone und Lautsprecher automatisch an das System übertragen werden.<br><br>Die Standardregel ermöglicht zwar sofort nach der Systeminstallation Zugriff auf die Audiofeeds angeschlossener Mikrofone und Lautsprecher, stellt aber nicht sicher, dass Audio tatsächlich aufgezeichnet wird, da Sie die Aufzeichnungseinstellungen separat festlegen müssen. |

| Standardregel | Beschreibung |
|---|---|
| **Start des Feeds** | Bewirkt, dass Videofeeds aller angeschlossenen Kameras automatisch an das System übertragen werden.<br>Die Standardregel ermöglicht zwar sofort nach der Systeminstallation Zugriff auf die Videofeeds angeschlossener Kameras, stellt aber nicht sicher, dass Video tatsächlich aufgezeichnet wird, da Sie die Aufzeichnungseinstellungen der Kameras separat festlegen müssen. |
| **Start des Metadatenfeeds** | Bewirkt, dass Datenfeeds aller angeschlossenen Kameras automatisch an das System übertragen werden.<br>Die Standardregel ermöglicht zwar sofort nach der Systeminstallation Zugriff auf die Datenfeeds angeschlossener Kameras, stellt aber nicht sicher, dass Daten tatsächlich aufgezeichnet werden, da Sie die Aufzeichnungseinstellungen der Kameras separat festlegen müssen. |
| **Anzeigen der Zutrittsanforderungsbenachrichtigung** | Bewirkt, dass alle Zutrittskontrollereignisse, die als „Zutrittsanforderung“ kategorisiert sind, die Anzeige eine Zutrittsanforderungsbenachrichtigung in XProtect Smart Client auslösen (sofern die Benachrichtigungsfunktion nicht im Smart Client-Profil deaktiviert ist). |

### Wiederherstellung von Standardregeln

Wenn Sie versehentlich eine der Standardregeln löschen, können Sie sie durch Eingabe folgender Daten wiederherstellen:

| Standardregel | Einzugebender Text |
|---|---|
| **Zu Voreinstellung gehen, wenn PTZ ausgeführt wurde** | Aktion für „Manuelle PTZ-Sitzung gestoppt“ von „Alle Kameras“ durchführen<br>Sofort zur Standardvoreinstellung auf dem Gerät wechseln, auf dem das Ereignis aufgetreten ist |
| **Audio auf Anfrage abspielen** | Aktion für „Wiedergabe der Audionachricht von extern |

| Standardregel | Einzugebender Text |
|---|---|
| | anfordern“ durchführen<br>Audionachricht von Metadaten auf den Geräten für Metadaten mit Priorität 1 wiedergeben |
| **Aufzeichnung für Lesezeichen** | Aktion für „Lesezeichenreferenz von allen Kameras, allen Mikrofonen, allen Lautsprechern angefordert“ durchführen, Aufzeichnung drei Sekunden vorher auf dem Gerät starten, auf dem das Ereignis aufgetreten ist<br>Aktion 30 Sekunden nachher durchführen, Aufzeichnung sofort anhalten |
| **Bei Bewegung aufzeichnen** | Aktion für „Bewegung von allen Kameras gestartet“ durchführen, Aufzeichnung drei Sekunden vorher auf dem Gerät starten, auf dem das Ereignis aufgetreten ist<br>Anhalteaktion für „Bewegung gestoppt von allen Kameras“ durchführen, Aufzeichnung drei Sekunden danach anhalten |
| **Aufzeichnung nach Bedarf** | Aktion für „Starten der Aufzeichnung von extern anfordern“ durchführen, Aufzeichnung auf den Geräten von Metadaten sofort starten<br>Stopp-Aktion für „Stoppen der Aufzeichnung von extern anfordern“ durchführen, Aufzeichnung sofort anhalten |
| **Start des Audiofeeds** | Aktion in einem Zeitintervall durchführen, Feed immer bei allen Mikrofonen, allen Lautsprechern starten<br>Aktion durchführen, wenn Zeitintervall endet, Feed sofort stoppen |
| **Start des Feeds** | Aktion in einem Zeitintervall durchführen, Feed immer bei allen Kameras starten<br>Aktion durchführen, wenn Zeitintervall endet, Feed sofort stoppen |
| **Start des Metadatenfeeds** | Aktion in einem Zeitintervall durchführen, Feed immer bei allen Metadaten starten |

| Standardregel | Einzugebender Text |
|---|---|
| | Aktion durchführen, wenn Zeitintervall endet, Feed sofort stoppen |
| **Anzeigen der Zutrittsanforderungsbenachrichtigung** | Aktion für Zugriffsanforderung (Zugriffskontroll-Kategorien) von Systemen [+ Geräten] durchführen<br><br>Integrierte Zugriffsanforderungsbenachrichtigung anzeigen |

## Benachrichtigungsprofile (Regel- und Ereignisknoten)

Legen Sie die folgenden Eigenschaften für Benachrichtigungsprofile fest:

| Komponente | Voraussetzung |
|---|---|
| **Name** | Geben Sie dem Benachrichtigungsprofil einen beschreibenden Namen. Der Name erscheint später immer, wenn Sie eine Regel erstellen und das Benachrichtigungsprofil auswählen. |
| **Beschreibung (optional)** | Geben Sie eine Beschreibung für das Benachrichtigungsprofil ein. Die Beschreibung wird angezeigt, wenn Sie den Mauszeiger über dem Benachrichtigungsprofil auf der Liste **Benachrichtigungsprofile** im Bereich „Übersicht“ ruhen lassen. |
| **Empfänger** | Geben Sie die E-Mailadressen ein, an die die E-Mailbenachrichtigungen des Benachrichtigungsprofils gesendet werden sollen. Wenn Sie mehrere E-Mailadressen eingeben möchten, trennen Sie diese mit einem Strichpunkt ab. Beispiel: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc |
| **Betreff** | Geben Sie hier den Text ein, der als Betreff der E-Mailbenachrichtigung angezeigt werden soll.<br><br>Sie können Systemvariablen, wie z. B. **Gerätename**, in die Betreffzeile oder das Nachrichtentextfeld eingeben. Um Variablen einzufügen, klicken Sie auf die gewünschten Variablenlinks im Kasten unterhalb des Felds. |
| **Nachrichtentext** | Geben Sie hier den Text ein, der im Textteil der E-Mailbenachrichtigungen angezeigt werden soll. Zusätzlich zum Nachrichtentext enthält der Textteil jeder E- |

| Komponente | Voraussetzung |
|---|---|
| | Mailbenachrichtigung automatisch diese Informationen:<br>• Auslöser der E-Mailbenachrichtigung<br>• Quelle aller angehängten Standbilder oder AVI-Videoclips |
| **Zeit zwischen E-Mails** | Bestimmen der Mindestdauer (in Sekunden) zwischen dem Versenden jeder einzelnen E-Mailbenachrichtigung. Beispiele:<br>• Wenn Sie einen Wert von **120** festlegen, vergehen mindestens 2 Minuten zwischen dem Versenden jeder einzelnen E-Mailbenachrichtigung, auch wenn das Benachrichtigungsprofil wieder von einer Regel ausgelöst wird, bevor die 2 Minuten vergangen sind<br>• Wenn Sie einen Wert von **0** festlegen, wird jedes Mal eine E-Mailbenachrichtigung versendet, wenn das Benachrichtigungsprofil von einer Regel ausgelöst wird. Das kann unter Umständen dazu führen, dass sehr viele E-Mailbenachrichtigungen versendet werden. Wenn Sie also den Wert **0** verwenden, sollten Sie sich genau überlegen, ob Sie das Benachrichtigungsprofil bei Regeln verwenden möchten, die wahrscheinlich häufig ausgelöst werden |
| **Anzahl der Bilder** | Legen Sie die Höchstzahl der Standbilder fest, die Sie pro E-Mailbenachrichtigung des Benachrichtigungsprofils einbinden möchten. Standardmäßig sind es fünf Bilder. |
| **Zeit zwischen Bildern (ms)** | Legen Sie eine Zeit in Millisekunden fest, die zwischen den Aufnahmen der eingebundenen Bilder bestehen soll. Beispiel: Beim Standardwert von 500 Millisekunden werden die eingebundenen Bilder als Aufzeichnungen mit einem Bildabstand von einer halben Sekunde angezeigt. |
| **Zeit vor Ereignis (Sek.)** | Mit dieser Einstellung wird der Anfang der AVI-Datei festgelegt. Standardmäßig beginnt die Aufzeichnung auf der AVI-Datei 2 Sekunden vor Auslösen des Benachrichtigungsprofils. Sie können diesen Wert auf einen gewünschten Wert in Sekunden ändern. |
| **Zeit nach Ereignis (Sek.)** | Mit dieser Einstellung wird das Ende der AVI-Datei festgelegt. Standardmäßig endet die AVI-Datei 4 Sekunden nach Auslösen des Benachrichtigungsprofils. Sie können diesen Wert auf einen gewünschten Wert in Sekunden ändern. |
| **Bildrate** | Legen Sie die gewünschte Anzahl an Bildern pro Sekunde für die AVI-Datei fest. Der |

| Komponente | Voraussetzung |
|---|---|
| | Standardwert beträgt fünf Bilder pro Sekunde. Je größer die Bildrate, desto höher die Bildqualität und desto größer die AVI-Datei. |
| **Bilder in E-Mail einbetten** | Wenn ausgewählt (Standardeinstellung), werden Bilder in den Textteil der E-Mailbenachrichtigungen eingefügt. Wenn nicht ausgewählt, werden die Bilder den E-Mailbenachrichtigungen als angehängte Dateien beigefügt. |

## Ereignisübersicht

Wenn Sie eine ereignisbasierte Regel im **Regel verwalten**-Assistenten hinzufügen, können Sie unter einer Anzahl unterschiedlicher Ereignistypen wählen. Damit Sie einen guten Überblick erhalten, sind auswählbare Ereignisse nach folgenden Kriterien in Gruppen aufgelistet:

### Hardware:

Einige Hardwaregeräte können selbst Vorfälle erstellen, um z. B. Bewegung zu registrieren. Sie können diese Ereignisse verwenden, müssen sie jedoch erst auf der Hardware konfigurieren, bevor Sie diese im System nutzen können. Sie können die aufgelisteten Ereignisse möglicherweise nicht auf jeder Hardware nutzen, da nicht alle Kameratypen Manipulationen oder Temperaturveränderungen erkennen können.

### Hardware - Konfigurierbare Ereignisse:

Konfigurierbare Ereignisse von Hardware werden durch Gerätetreiber automatisch importiert. Dies bedeutet, dass sie von Hardware zu Hardware variieren und deswegen hier nicht dokumentiert sind. Konfigurierbare Ereignisse werden nicht ausgelöst, bis Sie diese dem System hinzugefügt und sie auf der Registerkarte **Ereignis** auf der Hardware konfiguriert haben. Für einige konfigurierbare Ereignisse müssen Sie sogar die Kamera (Hardware) an sich konfigurieren.

### Hardware - Voreingestellte Ereignisse:

| Ereignis | Beschreibung |
|---|---|
| **Kommunikationsfehler (Hardware)** | Tritt auf, wenn die Verbindung zur Hardware unterbrochen wird. |
| **Kommunikation gestartet (Hardware)** | Tritt auf, wenn die Verbindung zur Hardware hergestellt wurde. |
| **Kommunikation gestoppt (Hardware)** | Tritt auf, wenn die Verbindung zur Hardware beendet wurde. |

### Geräte - Konfigurierbare Ereignisse:

Konfigurierbare Ereignisse von Geräten werden durch Gerätetreiber automatisch importiert. Dies bedeutet, dass sie von Gerät zu Gerät variieren und deswegen hier nicht dokumentiert sind. Konfigurierbare Ereignisse werden nicht ausgelöst, bis Sie diese dem System hinzugefügt und sie auf der Registerkarte **Ereignis** auf einem Gerät konfiguriert haben.

### Geräte - Vordefinierte Ereignisse:

| Ereignis | Beschreibung |
|---|---|
| **Lesezeichenreferenz angefordert** | Hierzu kommt es, wenn in den Clients im Live-Modus ein Lesezeichen gesetzt wird. Außerdem eine Voraussetzung zum Anwenden der standardmäßigen Regel zur Aufzeichnung von Lesezeichen. |
| **Kommunikationsfehler (Gerät)** | Tritt auf, wenn die Verbindung zu einem Gerät unterbrochen wurde oder wenn ein Versuch unternommen wird, mit einem Gerät zu kommunizieren und dieser Versuch fehlschlägt. |
| **Kommunikation gestartet (Gerät)** | Tritt auf, wenn die Verbindung zu einem Gerät hergestellt wurde. |
| **Kommunikation gestoppt (Gerät)** | Tritt auf, wenn die Verbindung zu einem Gerät beendet wurde. |
| **Beweissicherung geändert** | Hierzu kommt es, wenn eine Beweissicherung für Geräte von einem Client-Benutzer oder über das MIP SDK geändert wird. |
| **Beweissicherung** | Hierzu kommt es, wenn eine Beweissicherung für Geräte von einem Client-Benutzer oder über das MIP SDK erstellt wird. |
| **Beweissicherung aufgehoben** | Hierzu kommt es, wenn eine Beweissicherung für Geräte von einem Client-Benutzer oder über das MIP SDK entfernt wird. |
| **Feed-Überlauf gestartet** | Feed-Überlauf (Medienüberlauf) tritt auf, wenn ein Aufzeichnungsserver empfangene Daten nicht so schnell verarbeiten kann, wie in der Konfiguration festgelegt wurde, und deswegen einige Aufzeichnungen verwerfen muss.<br>Wenn der Server einwandfrei funktioniert, wird der Feed-Überlauf |

| Ereignis | Beschreibung |
|---|---|
| | üblicherweise durch langsame Speicherungen verursacht. Sie können dieses Problem lösen, indem Sie entweder die Menge der zu speichernden Daten verringern oder die Leistung des Speichersystems verbessern. Verringern Sie die Menge der zu speichernden Daten, indem Sie Bildraten, Auflösung oder Bildqualität Ihrer Kameras senken. Dies kann allerdings die Aufzeichnungsqualität senken. Stattdessen können Sie aber auch die Leistung Ihres Speichersystems verbessern, indem Sie zusätzliche Festplatten installieren, um die Belastung zu verringern, oder indem Sie schnellere Festplatten oder Steuerungen installieren.<br>Sie können dieses Ereignis nutzen, um Aktionen auszulösen, durch die Sie das Problem umgehen, um beispielsweise die Aufzeichnungsbildrate zu senken. |
| **Feed-Überlauf gestoppt** | Hierzu kommt es, wenn ein Datenüberlauf (siehe Feed-Überlauf gestartet auf Seite 522) endet. |
| **Live-Client-Feed angefordert** | Tritt auf, wenn Client-Benutzer einen Live-Stream von einem Gerät anfordern.<br>Das Ereignis tritt auf Anfrage ein, auch wenn sich die Anfrage des Client-Benutzers später als erfolglos erweist, z. B. weil der Client-Benutzer nicht über die zum Einsehen des angeforderten Live-Feeds erforderlichen Berechtigungen verfügt oder weil der Feed aus irgendeinem Grund abgebrochen wird. |
| **Live Client-Feed beendet** | Tritt auf, wenn Client-Benutzer einen Live-Stream von einem Gerät nicht länger anfordern. |
| **Manuelle Aufzeichnung gestartet** | Tritt auf, wenn ein Client-Benutzer eine Aufzeichnung für eine Kamera startet.<br>Das Ereignis wird auch dann ausgelöst, wenn das Gerät bereits über Regelaktionen aufnimmt. |
| **Manuelle Aufzeichnung angehalten** | Tritt auf, wenn ein Client-Benutzer eine Aufzeichnung für eine Kamera anhält.<br>Wenn das Regelsystem ebenfalls eine Aufzeichnung gestartet hat, nimmt es weiterhin auf, sogar nachdem die manuelle Aufzeichnung angehalten wurde. |
| **Referenz für markierte Daten angefordert** | Hierzu kommt es, wenn eine Beweissicherung im Wiedergabemodus über die Clients  oder über das MIP SDK erstellt wird.<br>Es wird ein Ereignis erstellt, das Sie in Ihren Regeln verwenden können. |

| Ereignis | Beschreibung |
|---|---|
| **Bewegung gestartet** | Tritt auf, wenn das System Bewegungen auf Video erkennt, das es von einer Kamera erhält.<br><br>Für diesen Ereignistyp wird eine aktivierte Bewegungserkennung der Kamera im System benötigt, mit der das Ereignis verknüpft ist.<br><br>Neben der Bewegungserkennung durch das System können einige Kameras Bewegung selbstständig erkennen und das Ereignis **Bewegung gestartet (HW)** auslösen, doch dies hängt von der Konfiguration der Hardware der Kamera und vom System ab. Siehe auch Hardware – Konfigurierbare Ereignisse: auf Seite 521. |
| **Bewegung gestoppt** | Tritt auf, wenn Bewegung im empfangenen Video nicht mehr registriert werden kann. Siehe auch Bewegung gestartet auf Seite 524.<br><br>Für diesen Ereignistyp wird eine aktivierte Bewegungserkennung der Kamera im System benötigt, mit der das Ereignis verknüpft ist.<br><br>Neben der Bewegungserkennung durch das System können einige Kameras Bewegung selbstständig erkennen und das Ereignis „Bewegung gestoppt“ (HW) auslösen, doch dies hängt von der Konfiguration der Hardware der Kamera und vom System ab. Siehe auch Hardware – Konfigurierbare Ereignisse: auf Seite 521. |
| **Ausgang aktiviert** | Tritt auf, wenn ein externer Ausgangsport eines Geräts aktiviert wird.<br><br>Für diesen Ereignistyp muss mindestens ein Gerät in Ihrem System Ausgangsports unterstützen. |
| **Ausgang geändert** | Tritt auf, wenn der Status eines externen Ausgangsports eines Geräts verändert wird.<br><br>Für diesen Ereignistyp muss mindestens ein Gerät in Ihrem System Ausgangsports unterstützen. |
| **Ausgang deaktiviert** | Tritt auf, wenn ein externer Ausgangsport eines Geräts deaktiviert wird.<br><br>Für diesen Ereignistyp muss mindestens ein Gerät in Ihrem System Ausgangsports unterstützen. |
| **Manuelle PTZ-Sitzung gestartet** | Tritt auf, wenn eine manuell bediente PTZ-Sitzung auf einer Kamera gestartet wird (anders als eine PTZ-Sitzung, die auf planmäßigen Wachrundgängen basiert oder die automatisch durch ein Ereignis ausgelöst wird). |

| Ereignis | Beschreibung |
|---|---|
| | Für diesen Ereignistyp müssen die dem Ereignis zugeordneten Kameras PTZ-Kameras sein. |
| **Manuelle PTZ-Sitzung gestoppt** | Tritt auf, wenn eine manuell bediente PTZ-Sitzung auf einer Kamera gestoppt wird (anders als eine PTZ-Sitzung, die auf planmäßigen Wachrundgängen basiert oder die automatisch durch ein Ereignis ausgelöst wird).<br>Für diesen Ereignistyp müssen die dem Ereignis zugeordneten Kameras PTZ-Kameras sein. |
| **Aufzeichnung gestartet** | Tritt auf, wenn eine Aufzeichnung gestartet wird. Für das manuelle Starten von Aufzeichnungen gibt es ein separates Ereignis. |
| **Aufzeichnung angehalten** | Tritt auf, wenn eine Aufzeichnung angehalten wird. Für das manuelle Anhalten von Aufzeichnungen gibt es ein separates Ereignis. |
| **Einstellungen geändert** | Tritt auf, wenn die Einstellungen auf einem Gerät geändert wurden. |
| **Fehler beim Ändern der Einstellungen** | Tritt auf, wenn ein Versuch unternommen wird, die Einstellungen auf einem Gerät zu ändern und dieser Versuch fehlschlägt. |

Externe Ereignisse - Voreingestellte Ereignisse:

| Ereignis | Beschreibung |
|---|---|
| **Wiedergabe der Audionachricht anfordern** | Aktiviert, wenn das Abspielen von Audio-Nachrichten über das MIP SDK angefordert wird.<br>Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins (z. B. für die Integration mit externen Zutrittskontrollsystemen) für Ihr System entwickeln. |
| **Aufzeichnungsbeginn anfordern** | Wird aktiviert, wenn ein Aufzeichnungsstart über das MIP SDK angefordert wird.<br>Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins (z. B. für die Integration mit externen Zutrittskontrollsystemen) für Ihr System entwickeln. |

| Ereignis | Beschreibung |
|---|---|
| **Aufzeichnungsstopp anfordern** | Wird aktiviert, wenn ein Aufzeichnungsstopp über das MIP SDK angefordert wird.<br>Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins (z. B. für die Integration mit externen Zutrittskontrollsystemen) für Ihr System entwickeln. |

### Externe Ereignisse - Generische Ereignisse:

Generische Ereignisse ermöglichen es Ihnen, Aktionen im System auszulösen, indem einfache Zeichenketten über das IP-Netzwerk an das Videoverwaltungssystem gesendet werden. Der Zweck generischer Ereignisse besteht darin, so vielen externen Quellen wie möglich zu ermöglichen, mit dem System zu interagieren.

### Externe Ereignisse - Benutzerdefinierte Ereignisse:

Auch eine Anzahl an Ereignissen, die genau auf Ihr System zugeschnitten sind, könnte zur Auswahl stehen. Sie können benutzerdefinierte Ereignisse für Folgendes verwenden:

- Sie können Client-Benutzern ermöglichen, manuell Ereignisse auszulösen, während sie Live-Video in den Clients ansehen
- Zahllose andere Anwendungsmöglichkeiten. Sie können beispielsweise benutzerdefinierte Ereignisse erstellen, die auftreten, wenn ein bestimmter Datentyp von einem Gerät empfangen wird

  Siehe auch Benutzerdefinierte Ereignisse (Erklärung) auf Seite 85.

### Aufzeichnungsserver:

| Ereignis | Beschreibung |
|---|---|
| **Archiv verfügbar** | Hierzu kommt es, wenn ein Archiv für einen Aufzeichnungsserver wieder zur Verfügung steht, nachdem es zuvor nicht zur Verfügung stand. Siehe auch Archiv ist nicht verfügbar auf Seite 526. |
| **Archiv ist nicht verfügbar** | Tritt auf, wenn ein Archiv für einen Aufzeichnungsserver nicht mehr verfügbar ist, beispielsweise durch die Unterbrechung der Verbindung zu einem Archiv im Netzlaufwerk. In solchen Fällen können Sie keine Aufzeichnungen archivieren.<br>Sie können das Ereignis verwenden, um beispielsweise einen Alarm oder ein Benachrichtigungsprofil auszulösen, damit eine E-Mailbenachrichtigung |

| Ereignis | Beschreibung |
|---|---|
| | automatisch an das zuständige Personal in Ihrem Unternehmen gesendet wird. |
| **Archivierung nicht abgeschlossen** | Tritt ein, wenn ein Archiv für einen Aufzeichnungsserver den letzten Archivierungsgang noch nicht abgeschlossen hat, wenn der Start des nächsten Vorgangs geplant ist. |
| **Datenbank - Löschen von Aufzeichnungen vor Erreichen der festgelegten Speichergröße** | Tritt ein, wenn das Speicherzeitlimit vor dem Datenbankgrößenlimit erreicht ist. |
| **Datenbank - Löschen von Aufzeichnungen vor Erreichen der festgelegten Speicherzeit** | Tritt ein, wenn das Datenbankgrößenlimit vor dem Speicherzeitlimit erreicht ist. |
| **Datenbankfestplatte ist voll - automatische Archivierung** | Tritt ein, wenn eine Datenbankfestplatte voll ist. Eine Datenbankfestplatte ist voll, wenn nur noch weniger als 5 GB Speicherplatz auf der Festplatte vorhanden sind:<br>Wenn weniger als 5 GB Speicherplatz frei sind, werden immer die ältesten Daten in einer Datenbank automatisch archiviert (oder gelöscht, wenn kein nächstes Archiv festgelegt ist). |
| **Datenbankfestplatte ist voll - Löschen** | Tritt ein, wenn eine Datenbankfestplatte voll ist und weniger als 1 GB Speicherplatz frei ist. Daten werden gelöscht, auch wenn ein nächstes Archiv definiert ist. Eine Datenbank erfordert 250 MB an freiem Speicherplatz. Ist dieser Grenzwert erreicht (wenn Daten nicht schnell genug gelöscht werden), werden erst dann wieder Daten in die Datenbank geschrieben, wenn genügend Speicherplatz freigegeben wurde. Die tatsächliche Maximalgröße Ihrer Datenbank entspricht der Anzahl der angegebenen Gigabyte minus 5 GB. |
| **Datenbank ist voll - automatische Archivierung** | Tritt ein, wenn ein Archiv für einen Aufzeichnungsserver voll ist und automatisch in ein Archiv im Speicher archivieren muss. |
| **Datenbankreparatur** | Tritt ein, wenn eine Datenbank beschädigt ist. In diesem Fall versucht das |

| Ereignis | Beschreibung |
|---|---|
| | System automatisch, zwei Reparaturmethoden für die Datenbank durchzuführen: eine schnelle Reparatur und eine umfassende Reparatur. |
| **Datenbankspeicher verfügbar** | Hierzu kommt es, wenn ein Speichergerät für einen Aufzeichnungsserver wieder zur Verfügung steht, nachdem es zuvor nicht zur Verfügung stand. Siehe auch Datenbankspeicher nicht verfügbar auf Seite 528.<br><br>Sie können das Ereignis z. B. verwenden, um die Aufzeichnung zu starten, wenn sie durch das Ereignis **Datenbankspeicher nicht verfügbar** angehalten wurde. |
| **Datenbankspeicher nicht verfügbar** | Tritt ein, wenn ein Speicher für einen Aufzeichnungsserver nicht mehr verfügbar ist, z. B. durch die Unterbrechung der Verbindung zu einem Speicher im Netzwerklaufwerk. In solchen Fällen können Sie keine Aufzeichnungen archivieren.<br><br>Sie können das Ereignis z. B. verwenden, um die Aufzeichnung anzuhalten sowie einen Alarm oder ein Benachrichtigungsprofil auszulösen, damit eine E-Mailbenachrichtigung automatisch an das zuständige Personal in Ihrem Unternehmen gesendet wird. |
| **Fehler bei der verschlüsselten Failover-Kommunikation** | Hierzu kommt es bei einem SSL-Kommunikationsfehler zwischen dem Failover-Server und überwachten Aufzeichnungsservern. |
| **Failover gestartet** | Tritt ein, wenn ein Failover-Aufzeichnungsserver die Aufgabe eines Aufzeichnungsservers übernimmt. Siehe auch Failover-Server (Knoten). |
| **Failover angehalten** | Hierzu kommt es, wenn ein Aufzeichnungsserver wieder verfügbar ist und wieder von einem Failover-Aufzeichnungsserver übernehmen kann. |

### Systemmonitor-Ereignisse

Systemmonitorereignisse werden ausgelöst, wenn Schwellenwerte überschritten werden, die in dem Knoten **Systemmonitorschwellenwerte** konfiguriert wurden. Siehe auch Lassen Sie sich den aktuellen Zustand Ihrer Hardware anzeigen und beheben Sie ggf. Fehler auf Seite 317.

Diese Funktion erfordert, dass der Data Collector-Dienst ausgeführt wird.

Systemmonitor - Server:

| Ereignis | Beschreibung |
|---|---|
| **CPU-Auslastung - kritisch** | Tritt in, wenn die CPU-Auslastung den kritischen CPU-Schwellenwert überschreitet. |
| **CPU-Auslastung - normal** | Tritt in, wenn die CPU-Auslastung den Schwellenwert der Warn-CPU unterschreitet. |
| **CPU-Auslastung - Warnung** | Tritt ein, wenn die CPU-Auslastung den Schwellenwert der Warn-CPU überschreitet oder unter den kritischen CPU-Schwellenwert fällt. |
| **Rechenkapazitätauslastung - kritisch** | Tritt ein, wenn die Rechenkapazitätauslastung den kritischen Speicherschwellenwert überschreitet. |
| **Rechenkapazitätauslastung - normal** | Tritt ein, wenn die Rechenkapazitätauslastung unter den Schwellenwert für den Warnspeicher zurückfällt. |
| **Rechenkapazitätauslastung - Warnung** | Tritt ein, wenn die Rechenkapazitätauslastung den Schwellenwert für Warnspeicher überschreitet oder unter den Schwellenwert für die kritische Rechenkapazitätauslastung zurückfällt. |
| **NVIDIA Dekodierung kritisch** | Tritt ein, wenn die NVIDIA Dekodierung die kritische NVIDIA-Decodierungsschwelle überschreitet. |
| **NVIDIA Dekodierung normal** | Tritt ein, wenn die NVIDIA-Dekodierungsauslastung unter den Warn-NVIDIA-Dekodierungsschwellenwert fällt. |
| **NVIDIA Dekodierung Warnung** | Tritt ein, wenn die NVIDIA-Decodierungsverwendung den Warn-NVIDIA-Decodierschwellenwert überschreitet oder unter den kritischen NVIDIA-Decodierschwellenwert fällt. |
| **NVIDIA Speicherplatz kritisch** | Tritt ein, wenn die NVIDIA-Speicherbelegung den kritischen NVIDIA-Speichergrenzwert überschreitet. |
| **NVIDIA Speicherplatz normal** | Tritt auf, wenn die NVIDIA-Speicherbelegung unter den NVIDIA- |

| Ereignis | Beschreibung |
|---|---|
| | Warnschwellenwert für Warnungen zurückfällt. |
| **NVIDIA Speicherplatz Warnung** | Tritt auf, wenn die NVIDIA-Speicherauslastung den Warngrenzwert für NVIDIA-Speicher überschreitet oder unter den kritischen NVIDIA-Speicherschwellenwert fällt. |
| **NVIDIA Übertragung kritisch** | Tritt ein, wenn die NVIDIA-Übertragungsnutzung den kritischen NVIDIA-Übertragungs-Schwellenwert überschreitet. |
| **NVIDIA Übertragung normal** | Tritt ein, wenn die NVIDIA-Übertragungsnutzung unter den Warn-NVIDIA-Übertragungs-Schwellenwert fällt. |
| **NVIDIA Übertragung Warnung** | Tritt ein, wenn die NVIDIA-Übertragungsnutzung den Warn-NVIDIA-Übertragungs-Schwellenwert überschreitet oder unter den kritischen NVIDIA-Übertragungs-Schwellenwert fällt. |
| **Dienstverfügbarkeit - kritisch** | Tritt ein, wenn ein Serverdienst nicht mehr ausgeführt wird.<br>Für dieses Ereignis gibt es keine Schwellenwerte. |
| **Dienstverfügbarkeit - normal** | Tritt ein, wenn sich der Status eines Serverdiensts in ausführen ändert.<br>Für dieses Ereignis gibt es keine Schwellenwerte. |

### Systemmonitor - Kamera:

| Ereignis | Beschreibung |
|---|---|
| **Live-FPS- kritisch** | Tritt ein, wenn die Live-FPS-Rate unter den kritischen Live-FPS-Schwellenwert fällt. |
| **Live-FPS- normal** | Tritt ein, wenn die Live-FPS-Rate den Warngrenzwert für Live-FPS überschreitet. |
| **Live-FPS - Warnung** | Tritt ein, wenn die Live-FPS-Rate unter den Warnungs-FPS-Schwellenwert fällt oder den kritischen Live-FPS-Schwellenwert überschreitet. |

| Ereignis | Beschreibung |
|---|---|
| **Aufzeichnender FPS - kritisch** | Tritt ein, wenn die Aufzeichnungs-FPS-Rate unter den kritischen FPS-Schwellenwert für die Aufzeichnung fällt. |
| **Aufzeichnender FPS - normal** | Tritt ein, wenn die Aufzeichnungs-FPS-Rate den Schwellenwert für die Warnaufzeichnung überschreitet. |
| **Aufzeichnender FPS - Warnung** | Tritt ein, wenn die Aufzeichnungs-FPS-Rate unter den FPS-Schwellenwert für die Warnaufnahme fällt oder den Schwellenwert für die kritische Aufnahme-FPS überschreitet. |
| **Verwendeter Speicherplatz - kritisch** | Tritt ein, wenn der Speicherplatz für Aufnahmen einer bestimmten Kamera den kritischen Schwellenwert für den verwendeten Speicherplatz überschreitet. |
| **Verwendeter Speicherplatz - normal** | Tritt ein, wenn der Speicherplatz für Aufnahmen einer bestimmten Kamera unter den Schwellenwert für den Schwellenwert für Warnmeldungen zurückfällt. |
| **Verwendeter Speicherplatz - Warnung** | Tritt ein, wenn der für Aufnahmen einer bestimmten Kamera verwendete Speicher den Schwellenwert für den Schwellenwert für Warnmeldungen überschreitet oder unter den kritischen Schwellenwert für den verwendeten Speicherplatz zurückfällt. |

Systemmonitor - Festplatte:

| Ereignis | Beschreibung |
|---|---|
| **Freier Speicherplatz - kritisch** | Tritt ein, wenn die Speicherplatzbelegung den kritischen Schwellenwert für den freien Speicherplatz überschreitet. |
| **Freier Speicherplatz - normal** | Tritt ein, wenn die Speicherplatzbelegung unter den Schwellenwert für die Warnung über freien Speicherplatz fällt. |
| **Freier Speicherplatz - Warnung** | Tritt ein, wenn die Speicherplatzbelegung den Schwellenwert für den Schwellenwert für Warnspeicher überschreitet oder unter den Schwellenwert für kritischen freien Speicherplatz zurückfällt. |

### Systemmonitor - Speicher:

| Ereignis | Beschreibung |
|---|---|
| **Speicherzeit - kritisch** | Tritt ein, wenn das System vorhersagt, dass der Speicher schneller gefüllt wird als der Schwellenwert für die kritische Speicherzeit. Wenn beispielsweise Daten aus Videostreams den Speicher schneller füllen als erwartet. |
| **Speicherzeit - normal** | Tritt ein, wenn das System vorhersagt, dass der Speicher langsamer gefüllt wird als der Schwellenwert für die Warnungs-Speicherzeit. Zum Beispiel, wenn Daten aus Videostreams den Speicher mit der erwarteten Rate füllen. |
| **Speicherzeit - Warnung** | Tritt ein, wenn das System vorhersagt, dass der Speicher schneller gefüllt wird als der Schwellenwert für die Warnungs-Speicherzeit oder langsamer als der Schwellenwert für die kritische Speicherzeit. Wenn zum Beispiel Daten von Videostreams den Speicher schneller füllen als erwartet, weil mehr Bewegung von den Kameras erfasst wird, die für die Aufzeichnung von Bewegungen konfiguriert sind. |

### Andere:

| Ereignis | Beschreibung |
|---|---|
| **Automatische Lizenzaktivierung ist fehlgeschlagen** | Tritt ein, wenn automatische Lizenzaktivierung fehlschlägt.<br>Es gibt keine Schwellenwerte für dieses Ereignis. |
| **Planmäßige Passwortänderung gestartet** | Hierzu kommt es, wenn eine planmäßige Passwortänderung gestartet wird. |
| **Planmäßige Passwortänderung erfolgreich abgeschlossen** | Hierzu kommt es, wenn eine planmäßige Passwort-Änderung ohne Fehler abgeschlossen wird. |
| **Planmäßige Passwortänderung abgeschlossen, jedoch mit Fehlern** | Hierzu kommt es, wenn eine planmäßige Passwort-Änderung mit Fehlern abgeschlossen wird. |

### Ereignisse von XProtect Erweiterungen und -integrationen:

Ereignisse von XProtect Erweiterungen und -integrationen können im Regelsystem verwendet werden, zum Beispiel:

- Analyseereignisse können auch im Regelsystem verwendet werden

## Aktionen und Stoppaktionen

Der Assistent **Regel verwalten** bietet einige Aktionen und Stoppaktionen an, mit deren Hilfe Regeln erstellt werden können. Ihnen können mehr Aktionen zur Verfügung stehen, wenn Ihre Systeminstallation XProtect Erweiterungen oder anbieterspezifische Plug-ins nutzt. Zu den Aktionen jedes Typs werden ggf. entsprechende Stoppaktionen aufgeführt.

### Der Assistent "Regel verwalten"

| Aktion | Beschreibung |
|---|---|
| **Aufzeichnung auf <Geräten> starten** | Starten der Aufzeichnung und Speichern der Daten von den ausgewählten Geräten in der Datenbank.<br><br>Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, Folgendes festzulegen:<br><br>Wann die Aufnahme beginnen soll. Das passiert entweder sofort oder ein paar Sekunden vor dem auslösenden Ereignis/Beginn des auslösenden Zeitintervalls; auf welchen Geräten die Aktion durchgeführt werden soll.<br><br>Für diesen Aktionstyp muss die Aufzeichnung auf den Geräten aktiviert sein, mit denen die Aktion verknüpft ist. Sie können Daten vor einem Ereignis oder Zeitintervall nur dann speichern, wenn Sie Voralarm-Puffer für die entsprechenden Geräte aktiviert haben. Die Aktivierung der Aufzeichnung und die Einstellungen für Voralarm-Puffer für ein Gerät erfolgen auf der Registerkarte **Aufzeichnung**.<br><br>**Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Aufzeichnung stoppen**.<br><br>Ohne diese Stopp-Aktion würde die Aufzeichnung potenziell für unbegrenzte Zeit weiterlaufen. Sie können |

| Aktion | Beschreibung |
|---|---|
| | auch weitere Stopp-Aktionen festlegen. |
| **Feed auf <Geräten> starten** | Starten des Datenfeeds von Geräten zum System. Wenn der Feed von einem Gerät gestartet wird, werden Daten vom Gerät zum System übertragen, sodass Sie diese je nach Datentyp anzeigen oder aufzeichnen können.<br><br>Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, festzulegen, auf welchen Geräten die Feeds gestartet werden sollen. Das System beinhaltet eine Standardregel, die sicherstellt, dass Feeds immer auf allen Kameras gestartet werden.<br><br>**Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Feed stoppen**.<br><br>Sie können auch weitere Stopp-Aktionen festlegen.<br><br>Durch die Verwendung der obligatorischen Stopp-Aktion **Feed stoppen** zum Stoppen des Feeds von einem Gerät werden keine Daten mehr vom Gerät zum System übertragen. Damit sind dann beispielsweise Live-Ansicht und Aufzeichnung von Videos nicht mehr möglich. Ein Gerät, für das Sie den Feed gestoppt haben, kann jedoch weiter mit dem Aufzeichnungsserver kommunizieren und Sie können den Feed über eine Regel wieder automatisch starten – anders, als wenn Sie das Gerät manuell deaktiviert haben.<br><br>⚠ Dieser Aktionstyp ermöglicht zwar Zugriff auf die Datenfeeds der ausgewählten Geräte, garantiert jedoch nicht, dass Daten aufgezeichnet werden, da Sie die Aufzeichnungseinstellungen separat festlegen müssen. |
| **Einstellen von <Smart Wall> auf** | Stellt XProtect Smart Wall auf eine ausgewählte |

| Aktion | Beschreibung |
|---|---|
| **<Voreinstellung>** | Voreinstellung ein. Legen Sie die Voreinstellung auf der Registerkarte **Smart Wall Voreinstellungen** fest.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **<Smart Wall>-<Bildschirm> auf Anzeigen von <Kameras> setzen** | Stellt einen bestimmten XProtect Smart Wall-Monitor auf die Anzeige von Live-Video von den ausgewählten Kameras an diesem Standort oder an einem untergeordneten Standort ein, der in Milestone Federated Architecture konfiguriert wurde.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **<Smart Wall>-<Bildschirm> auf Anzeigen von Text-<Nachrichte> setzen** | Stellt einen bestimmten XProtect Smart Wall-Monitor auf die Anzeige einer benutzerdefinierten Textnachricht mit bis zu 200 Zeichen ein.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **<Kameras> vom <Smart Wall>-Monitor <Bildschirm> entfernen** | Stoppen der Videoanzeige von einer bestimmten Kamera.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Live-Bildrate auf <Geräten> festlegen** | Legt die Bildrate für die Anzeige von Live-Video durch das System von den ausgewählten Kameras fest; sie ersetzt die Standardbildrate der Kameras. Die Einstellung erfolgt auf der Registerkarte **Einstellungen**.<br><br>Wenn Sie diesen Aktionstyp auswählen, fordert Sie der |

| Aktion | Beschreibung |
|---|---|
| | Assistent **Regel verwalten** dazu auf, die Bildrate und die Geräte dafür festzulegen. Überprüfen Sie stets, ob die angegebene Bildrate an den entsprechenden Kameras verfügbar ist.<br><br>**Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Standard-Live-Bildrate wiederherstellen**.<br><br>Ohne diese Stopp-Aktion würde die Standardbildrate potenziell nie wiederhergestellt werden. Sie können auch weitere Stopp-Aktionen festlegen. |
| **Aufzeichnungsbildrate auf <Geräten> festlegen** | Legt die Bildrate für das Speichern aufgezeichneter Videos von den ausgewählten Kameras in der Datenbank fest; sie ersetzt die Standardbildrate der Kameras.<br><br>Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, die Aufzeichnungsbildrate und die Kameras dafür festzulegen.<br><br>Sie können nur eine Aufzeichnungsbildrate für JPEG festlegen, einen Video-Codec, bei dem jedes Bild separat in ein JPEG-Bild komprimiert wird. Für diesen Aktionstyp muss auch die Aufzeichnung an den Kameras aktiviert sein, mit denen die Aktion verknüpft ist. Die Aktivierung der Aufzeichnung für eine Kamera erfolgt auf der Registerkarte **Aufzeichnung**. Die maximale Bildrate, die festgelegt werden kann, hängt von den entsprechenden Kameratypen und ihrer ausgewählten Bildauflösung ab.<br><br>**Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Standard-Aufzeichnungsbildrate wiederherstellen**.<br><br>Ohne diese Stopp-Aktion würde die Standard-Aufzeichnungsbildrate potenziell nie wiederhergestellt werden. Sie können auch weitere Stopp-Aktionen festlegen. |

| Aktion | Beschreibung |
|---|---|
| **Aufzeichnungsbildrate für alle Bilder bei MPEG-4/H.264/H.265 auf <Geräte> setzen** | Legt die Bildrate für das Speichern aufgezeichneter Videos von den ausgewählten Kameras in der Datenbank für die Aufzeichnung aller Bilder, nicht bloß von Keyframes, fest. Aktivieren Sie die Funktion zur Aufzeichnung nur der Keyframes auf der Registerkarte **Aufzeichnung**.<br><br>Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, auszuwählen, für welche Geräte die Aktion gelten soll.<br><br>Sie können für MPEG-4/H.264/H.265 nur die Keyframe-Aufzeichnung aktivieren. Für diesen Aktionstyp muss auch die Aufzeichnung an den Kameras aktiviert sein, mit denen die Aktion verknüpft ist. Die Aktivierung der Aufzeichnung für eine Kamera erfolgt auf der Registerkarte **Aufzeichnung**.<br><br>**Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen:<br>**Standard-Aufzeichnungsbildrate von Keyframes für MPEG-4/H.264/H.265 wiederherstellen**<br><br>Ohne diese Stopp-Aktion würde die Standardeinstellung potenziell nie wiederhergestellt werden. Sie können auch weitere Stopp-Aktionen festlegen. |
| **Wachrundgang auf <Gerät> unter Verwendung von <Profil> mit Priorität auf PTZ <Priorität> starten** | Startet PTZ-Wachrundgang für eine bestimmte PTZ-Kamera mit einer bestimmten Priorität gemäß einem bestimmten Wachrundgangprofil. Dies ist eine genaue Definition der Art und Weise, wie der Wachrundgang ausgeführt werden soll, einschließlich der Sequenz von Preset Positionen, Zeitsteuerungseinstellungen usw.<br><br>Wenn Sie Ihr System von einer älteren Systemversion aktualisiert haben, wurden die alten Werte (**Sehr niedrig**, **Niedrig**, **Mittel**, **Hoch** und **Sehr hoch**) folgendermaßen übersetzt:<br>• Sehr niedrig = 1.000<br>• Niedrig = 2.000 |

| Aktion | Beschreibung |
|---|---|
| | • Mittel = 3.000<br>• Hoch = 4.000<br>• Sehr hoch = 5.000<br><br>Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, ein Wachrundgangprofil auszuwählen. Sie können für ein Gerät jeweils nur ein Wachrundgangprofil auswählen.<br><br>Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, PTZ-Geräte sein.<br><br>Sie müssen mindestens ein Wachrundgangprofil für das/die Gerät(e) definieren. Auf der Registerkarte **Wachrundgang** können Sie Wachrundgangprofile für eine PTZ-Kamera definieren.<br><br>**Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen:<br>**Wachrundgang stoppen**<br><br>Ohne diese Stopp-Aktion würde der Wachrundgang potenziell nie aufhören. Sie können auch weitere Stopp-Aktionen festlegen. |
| **Wachrundgang für <Geräte> anhalten** | Hält den Wachrundgang an. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, die Geräte festzulegen, für die der Wachrundgang angehalten werden soll. |

| Aktion | Beschreibung |
|---|---|
| | Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, PTZ-Geräte sein.<br><br>Sie müssen mindestens ein Wachrundgangprofil für das/die Gerät(e) definieren. Auf der Registerkarte **Wachrundgang** können Sie Wachrundgangprofile für eine PTZ-Kamera definieren.<br><br>**Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Wachrundgang fortsetzen**<br><br>Ohne diese Stopp-Aktion würde der Wachrundgang potenziell für unbegrenzte Zeit angehalten bleiben. Sie können auch weitere Stopp-Aktionen festlegen. |
| **<Gerät> auf Position <Voreinstellung> mit Priorität auf PTZ <Priorität> verschieben** | Bewegt eine bestimmte Kamera in eine bestimmte Preset Position – jedoch immer gemäß Priorität. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, eine Preset-Position auszuwählen. Nur eine Preset-Position an einer Kamera kann ausgewählt werden. Es können nicht mehrere Preset-Positionen ausgewählt werden.<br><br>Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, PTZ-Geräte sein. |

| Aktion | Beschreibung |
|---|---|
| | Für diese Aktion müssen Sie mindestens eine Preset Position für diese Geräte definiert haben. Auf der Registerkarte **Voreinstellungen** können Sie Preset Positionen für eine PTZ-Kamera definieren.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Auf <Geräte> mit Priorität auf PTZ <Priorität> auf Standardvoreinstellung verschieben** | Verschiebt eine oder mehr Kameras in ihre jeweiligen Standard-Voreinstellungspositionen – jedoch immer gemäß Priorität. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, auszuwählen, für welche Geräte die Aktion gelten soll.<br><br>Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, PTZ-Geräte sein. Für diese Aktion müssen Sie mindestens eine Preset Position für diese Geräte definiert haben. Auf der Registerkarte **Voreinstellungen** können Sie Preset Positionen für eine PTZ-Kamera definieren.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Geräteausgang auf <Status> setzen** | Legt einen Ausgang auf einem Gerät auf einen bestimmten Status fest (aktiviert oder deaktiviert). Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel** |

| Aktion | Beschreibung |
|---|---|
| | **verwalten** dazu auf, den Status und die Geräte dafür festzulegen.<br><br>Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, jeweils mindestens einen externen Ausgang besitzen, der mit einem Ausgangsport verbunden ist.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Lesezeichen auf <Gerät> erstellen** | Erstellt ein Lesezeichen bei Live-Streaming oder Aufzeichnungen von einem bestimmten Gerät. Über Lesezeichen lassen sich bestimmte Ereignisse oder Zeitabschnitte einfach zurückverfolgen. Lesezeicheneinstellungen werden im Dialogfeld **Optionen** festgelegt. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, Lesezeichendetails festzulegen und Geräte auszuwählen.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Audio <Nachricht> auf <Gerät> mit <Priorität> Wiedergabe** | Gibt bei Auslösung durch ein Ereignis eine Audionachricht auf ausgewählten Geräten wieder. Bei den Geräten handelt es sich meistens um Lautsprecher oder Kameras.<br><br>Dieser Aktionstyp erfordert, dass Sie die Nachricht bei **Tools** > **Optionen** > Registerkarte **Audionachrichten** ins System hochgeladen haben.<br><br>Sie können mehrere Regeln für ein Ereignis erstellen und verschiedene Nachrichten an die Geräte senden, jedoch immer gemäß Priorität. Die Prioritäten, die die Sequenz festlegen, sind diejenigen, die auf der Registerkarte **Sprache** für die Regel und das Gerät für eine Rolle festgelegt sind: |

| Aktion | Beschreibung |
|---|---|
| | • Wenn eine Nachricht wiedergegeben wird und eine andere Nachricht mit derselben Priorität an denselben Lautsprecher gesendet wird, wird die erste Nachricht abgeschlossen, dann wird die zweite Nachricht wiedergegeben<br>• Wenn eine Nachricht wiedergegeben wird und eine andere Nachricht mit höherer Priorität an denselben Lautsprecher gesendet wird, wird die erste Nachricht unterbrochen und die zweite Nachricht sofort wiedergegeben |
| **Benachrichtigung senden an <Profil>** | Sendet eine Benachrichtigung mit einem bestimmten Benachrichtigungsprofil. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, ein Benachrichtigungsprofil sowie die Geräte auszuwählen, von denen Voralarm-Bilder enthalten sein sollen. Sie können nur ein einziges Benachrichtigungsprofil auswählen. Für ein einzelnes Benachrichtigungsprofil können jedoch mehrere Empfänger vorhanden sein.<br>Sie können auch mehrere Regeln für dasselbe Ereignis erstellen und für jedes der Benachrichtigungsprofile unterschiedliche Benachrichtigungen versenden. Um die Inhalte von Regeln zu kopieren und wiederzuverwenden, klicken Sie in der Liste **Regeln** mit der rechten Maustaste auf eine Regel.<br>Für diesen Aktionstyp müssen Sie mindestens ein Benachrichtigungsprofil definiert haben. Voralarm-Bilder sind nur enthalten, wenn Sie die Option **Bilder einschließen** für das entsprechende Benachrichtigungsprofil aktiviert haben.<br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Neuen <Protokolleintrag> vornehmen** | Generiert einen Eintrag im Regelprotokoll. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel** |

| Aktion | Beschreibung |
|---|---|
| | **verwalten** dazu auf, einen Text für den Protokolleintrag festzulegen. Beim Angeben des Protokolltexts können Sie in die Protokollnachricht Variablen einfügen, wie z. B. **$DeviceName$** oder **$EventName$**.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Plug-In auf <Geräten> starten** | Startet ein oder mehrere Plug-ins. Wenn Sie eine Aktion dieses Typs auswählen, fordert Sie der Assistent **Regel verwalten** auf, die erforderlichen Plug-ins auszuwählen und festzulegen, auf welchen Geräten diese gestartet werden sollen.<br><br>Für diesen Aktionstyp müssen ein oder mehrere Plug-ins auf Ihrem System installiert sein.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Plug-In auf <Geräten> stoppen** | Stoppt ein oder mehrere Plug-ins. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, erforderliche Plug-ins und die Geräte, auf denen die Plug-ins gestoppt werden sollen, festzulegen.<br><br>Für diesen Aktionstyp müssen ein oder mehrere Plug-ins auf Ihrem System installiert sein.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Neue Einstellungen auf <Geräte> anwenden** | Ändert die Geräteeinstellungen auf einem oder mehreren Geräten. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, die relevanten Geräte festzulegen, und Sie können die relevanten Einstellungen an diesen Geräten festlegen. |

| Aktion | Beschreibung |
|---|---|
| | Wenn Sie Einstellungen für mehrere Geräte festlegen, können Sie nur solche Einstellungen ändern, die für alle angegebenen Geräte verfügbar sind.<br><br>**Beispiel**: Sie legen fest, dass die Aktion mit Gerät 1 und Gerät 2 verknüpft sein soll. Gerät 1 hat die Einstellungen A, B und C, Gerät 2 die Einstellungen B, C und D. In diesem Fall können Sie nur die Einstellungen ändern, die für beide Geräte verfügbar sind, nämlich B und C.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Matrix auf Ansicht von <Geräte> setzen** | Zeigt Videoaufzeichnungen von den ausgewählten Kameras auf einem Computer, der Matrix-getriggerte Videoaufzeichnungen anzeigen kann, z.B. ein Computer, auf dem Sie XProtect Smart Client installiert haben.<br><br>Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, einen Matrix-Empfänger und ein oder mehrere Geräte festzulegen, deren Videobilder auf dem ausgewählten Matrix-Empfänger angezeigt werden sollen.<br><br>Mit diesem Aktionstyp können Sie jeweils immer nur einen Matrix-Empfänger auswählen. Wenn Sie wollen, dass Videobilder von den ausgewählten Geräten bei mehreren Matrix-Empfängern angezeigt werden, sollten Sie eine Regel für jeden benötigten Matrix-Empfänger erstellen oder die XProtect Smart Wall-Funktion verwenden. Um die Inhalte von Regeln zu kopieren und wiederzuverwenden, klicken Sie in der Liste **Regeln** mit der rechten Maustaste auf eine Regel. So müssen Sie nicht mehrere, beinahe identische Regeln von Grund auf neu erstellen. |

| Aktion | Beschreibung |
|---|---|
| | Im Rahmen der Konfiguration der Matrix-Empfänger selbst müssen Benutzer die Portnummer und das Passwort festlegen, die für die Matrix-Kommunikation benötigt werden. Vergewissern Sie sich, dass die Benutzer Zugriff auf diese Informationen haben. Die Benutzer müssen im Allgemeinen auch die IP-Adressen von zulässigen Hosts festlegen, von denen Befehle in Bezug auf die Anzeige Matrix-ausgelöster Videobilder akzeptiert werden. In diesem Fall müssen die Benutzer auch die IP-Adresse des Management-Servers sowie etwaige verwendete Router oder Firewalls kennen. |
| **SNMP-Trap senden** | Generiert eine kurze Nachricht, die Ereignisse bei ausgewählten Geräten protokolliert. Der Text von SNMP-Traps wird automatisch generiert und ist nicht anpassbar. Er kann den Quelltyp und den Namen des Geräts enthalten, bei dem das Ereignis aufgetreten ist.<br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Fernaufzeichnungen von <Geräten> abrufen und speichern** | Ruft Fernaufzeichnungen für einen angegebenen Zeitraum vor und nach dem auslösenden Ereignis von ausgewählten Geräten ab und speichert sie (die Geräte müssen lokale Aufzeichnung unterstützen).<br>Diese Regel ist unabhängig von der Einstellung der **Option zum automatischen Abruf von Fernaufzeichnungen, wenn Verbindung wiederhergestellt wurde**. |

| Aktion | Beschreibung |
|---|---|
| | **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Fernaufzeichnungen zwischen <Start- und Endzeit> von <Geräten> abrufen und speichern** | Ruft Fernaufzeichnungen in einem angegebenen Zeitraum von ausgewählten Geräten ab und speichert sie (die Geräte müssen lokale Aufzeichnung unterstützen).<br>Diese Regel ist unabhängig von der Einstellung der **Option zum automatischen Abruf von Fernaufzeichnungen, wenn Verbindung wiederhergestellt wurde**.<br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Angehängte Bilder speichern** | Sorgt dafür, dass ein Bild, das vom Ereignis „Bilder empfangen“ empfangen wird (per SMTP-E-Mail von einer Kamera gesendet) zur zukünftigen Verwendung gespeichert wird. In Zukunft können andere Ereignisse diese Aktion potenziell auch auslösen.<br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Archivierung auf <Archive> aktivieren** | Startet die Archivierung bei einem oder mehreren Archiven. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, relevante Archive auszuwählen.<br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Auf <Site> <benutzerdefiniertes Ereignis> auslösen** | Diese Aktion ist vorwiegend in der Milestone Federated Architecture relevant, Sie können sie jedoch auch in einer |

| Aktion | Beschreibung |
|---|---|
| | Konfiguration mit einem einzigen Standort verwenden. Mit dieser Regel lösen Sie ein benutzerdefiniertes Ereignis an einem Standort aus, üblicherweise einem Remote-System in einer föderalen Hierarchie.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **<Zugriffsanforderungsbenachrichtigung> anzeigen** | Gewährt Ihnen Zugriff auf Anforderungsnachrichten-Popup auf dem XProtect Smart Client-Bildschirm, wenn die Kriterien für das Auslösen von Ereignissen zusammen kommen. Milestone empfiehlt, dass Sie Zugriffskontrollereignisse als auslösende Ereignisse für diese Aktion anwenden, weil Zugriffs-Anforderungsnachrichten normalerweise zum Wirken an Zugriffskontroll-Befehlen und Kameras konfiguriert sind.<br><br>Für diesen Aktionstyp müssen ein oder mehrere Zutrittskontroll-Plug-ins auf Ihrem System installiert sein.<br><br>**Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden. |
| **Das Passwort auf Hardwaregeräten ändern** | Ändert das Passwort ausgewählter Hardwaregeräte in ein zufällig erzeugtes Passwort auf der Grundlage der Passwortanforderungen für das jeweilige Hardwaregerät. Eine Liste der unterstützten Hardwaregeräte finden Sie unter Hardware suchen.<br><br>Diese Aktion steht nur zur Verfügung, wenn Sie mithilfe des Regeltyps **Eine Aktion ausführen an einem <recurring time>** eine Regel dafür aufstellen. |

| Aktion | Beschreibung |
|---|---|
| | Für diese Maßnahme stehen die folgenden Ereignisse zur Verfügung:<br>• Planmäßige Passwortänderung gestartet auf Seite 532<br>• Planmäßige Passwortänderung erfolgreich abgeschlossen auf Seite 532<br>• Planmäßige Passwortänderung abgeschlossen, jedoch mit Fehlern auf Seite 532<br>Für Aktionen dieses Typs gibt es keine Stopp-Aktion.<br>Sie können den Fortgang dieser Aktion in dem Knoten **Aktuelle Aufgaben** ansehen. Weitere Informationen finden Sie unter Anzeige aktuell laufender Aufgaben auf Aufzeichnungsservern auf Seite 314.<br>Um die Ergebnisse der Aktion anzusehen - gehen Sie zu dem Knoten **Serverprotokolle** auf der Registerkarte **Systemprotokolle**. Weitere Informationen finden Sie unter Registerkarte „Serverprotokolle“ (Optionen) auf Seite 416.<br>Weitere Informationen finden Sie unter Systemprotokolle (Registerkarte). |

## Analyseereignisse testen (Eigenschaften)

Beim Test der Anforderungen eines Analyseereignisses erscheint ein Fenster, welches vier Bedingungen untersucht und mögliche Beschreibungen und Lösungen von Fehlern anbietet.

| Bedingung | Beschreibung | Fehlermeldungen und Lösungen |
|---|---|---|
| **Änderungen gespeichert** | Wenn das Ereignis neu ist, wird es gespeichert? Oder werden Änderungen am Ereignisnamen gespeichert? | **Speichern Sie die Änderungen vor dem Testen des Analyseereignisses**. Lösung/Erklärung: Speichern Sie die Änderungen. |

| Bedingung | Beschreibung | Fehlermeldungen und Lösungen |
|---|---|---|
| **Analyseereignisse aktiviert** | Wurde die Funktion Analyseereignis aktiviert? | **Analyseereignisse wurde nicht aktiviert**. Lösung/Erklärung: Aktivieren Sie die Funktion Analyseereignis. Um dies zu tun, klicken Sie auf **Tools** > **Optionen** > **Analyseereignisse** und wählen Sie das Kontrollkästchen **Aktiviert** aus. |
| **Adresse zugelassen** | Ist die IP-Adresse/der Hostname des Geräts, welche die Ereignisse sendet, dazu berechtigt (auf der Adressenliste für Analyseereignisse aufgeführt)? | **Der lokale Hostname muss in die Liste der zugelassenen Adressen für den Analyseereignis-Dienst hinzugefügt werden**. Lösung/Erklärung: Fügen Sie Ihr Gerät zur Liste der zugelassenen IP-Adressen oder Hostnamen für Analyseereignisse hinzu.<br>**Fehler beim Auflösen des lokalen Hostnamens**. Lösung/Erklärung: Die IP-Adresse oder Hostname des Geräts kann nicht gefunden werden oder ist ungültig. |
| **Analyseereignis senden** | War das Senden des Testereignisses an den Event Server erfolgreich? | Siehe Tabelle unten. |

Jeder Schritt ist entweder als fehlgeschlagen: ✗ oder erfolgreich markiert: ✓.

Fehlermeldungen und Lösungen für die Bedingung **Analyseereignis senden**:

| Fehlermeldung | Lösung |
|---|---|
| **Event Server nicht gefunden** | Nicht möglich den Event Server auf der Liste registrierter Dienste zu finden. |
| **Fehler beim Verbinden mit Event Server** | Nicht möglich mit dem Event Server über den angegeben Port zu verbinden. Der Fehler entsteht wahrscheinlich aufgrund von Netzwerkproblemen oder der Event Server-Dienst wurde gestoppt. |
| **Fehler beim Senden von Analyseereignis** | Die Verbindung zum Event Server wurde aufgebaut, aber das Ereignis kann nicht gesendet werden. Der Fehler entsteht wahrscheinlich aufgrund von |

| Fehlermeldung | Lösung |
|---|---|
| | Netzwerkproblemen (z. B. ein Timeout). |
| **Fehler beim Empfangen der Antwort vom Event Server** | Das Ereignis wurde zum Event Server gesendet, aber es gab keine Antwort. Der Fehler entsteht wahrscheinlich aufgrund von Netzwerkproblemen oder einem belegtem Port.<br>Sehen Sie sich das Event Server-Protokoll an, das normalerweise unter `ProgramData\Milestone\XProtect Event Server\Logs\` zu finden ist. |
| **Analyseereignis beim Event Server unbekannt** | Der Event Server-Dienst erkennt das Ereignis nicht. Der Fehler entsteht aufgrund des Ereignisses oder Änderungen am Ereignis wurden nicht gespeichert. |
| **Ungültiges Analyseereignis vom Event Server empfangen** | Das Format des Ereignisses ist nicht korrekt. |
| **Absender nicht vom Event Server autorisiert** | Höchstwahrscheinlich steht Ihre Anlage nicht auf der Liste der erlaubten IP-Adressen oder Hostnamen. |
| **Interner Fehler auf Event Server** | Fehler auf Event Server.<br>Sehen Sie sich das Event Server-Protokoll an, das normalerweise unter `ProgramData\Milestone\XProtect Event Server\Logs\` zu finden ist. |
| **Ungültige Antwort vom Event Server empfangen** | Die Antwort ist ungültig. Möglicherweise ist der Port belegt oder das Netzwerk hat Probleme.<br>Sehen Sie sich das Event Server-Protokoll an, das normalerweise unter `ProgramData\Milestone\XProtect Event Server\Logs\` zu finden ist. |
| **Unbekannte Antwort vom Event Server** | Die Antwort ist gültig, kann aber nicht verarbeitet werden. Der Fehler entsteht möglicherweise aufgrund von Netzwerkproblemen oder einem belegten Port.<br>Sehen Sie sich das Event Server-Protokoll an, das normalerweise unter `ProgramData\Milestone\XProtect Event Server\Logs\` zu finden ist. |
| **Unerwarteter Fehler** | Bitte kontaktieren Sie für weitere Hilfe den Milestone-Support. |

## Generische Ereignis- und Datenquellen (Eigenschaften)

Diese Funktion funktioniert nur, wenn Sie den XProtect Event Server installiert haben.

### Generisches Ereignis (Eigenschaften)

| Komponente | Voraussetzung |
|---|---|
| **Name** | Einmaliger Name für das generische Ereignis. Der Name muss einmalig unter allen Ereignistypen sein, wie z. B. benutzerdefinierte Ereignisse, Analyseereignisse und so weiter. |
| **Aktiviert** | Generische Ereignisse sind standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um das Ereignis zu deaktivieren. |
| **Ausdruck** | Ausdruck, nach dem das System bei der Analyse von Datenpaketen suchen soll. Sie können die folgenden Operatoren verwenden:<br>• `( )`: Wird verwendet, um sicherzustellen, dass verwandte Begriffe zusammen als logische Einheit verarbeitet werden. Sie können verwendet werden, um eine bestimmte Verarbeitungsreihenfolge in der Analyse zu erzwingen<br>**Beispiel**: Bei den Suchkriterien `(Benutzer001 ODER Tür053) UND Sonntag` werden zuerst die beiden Begriffe zwischen den Klammern verarbeitet, dann wird das Ergebnis mit dem letzten Teil des Strings kombiniert. Also sucht das System zuerst nach Paketen, die einen der beiden Begriffe `Benutzer001` oder `Tür053` beinhalten; dann wird überprüft, welche der Ergebnispakete zusätzlich den Begriff `Sonntag` enthalten.<br>• `UND`: Mit dem `UND`-Operator bestimmen Sie, dass die Begriffe auf beiden Seiten des `UND`-Operators vorhanden sein müssen<br>**Beispiel**: Die Suchkriterien `Benutzer001 UND Tür053 UND Sonntag` liefern nur dann ein Ergebnis, wenn die Begriffe `Benutzer001`, `Tür053` und `Sonntag` alle in Ihrem Ausdruck vorkommen. Es reicht nicht aus, wenn nur einer oder zwei der Begriffe darin vorkommen. Je mehr Begriffe Sie mit UND verbinden, desto weniger Ergebnisse erhalten Sie.<br>• `ODER`: Mit dem `ODER`-Operator bestimmen Sie, dass entweder der eine oder der andere Begriff vorhanden sein muss<br>**Beispiel**: Die Suchkriterien `"Benutzer001" ODER "Tür053" ODER "Sonntag"` liefern alle Ergebnisse, die entweder `Benutzer001`, `Tür053` oder `Sonntag` beinhalten. Je mehr Begriffe Sie mit `ODER` verbinden, desto mehr Ergebnisse erhalten Sie. |

| Komponente | Voraussetzung |
|---|---|
| **Ausdruckstyp** | Legt fest, wie genau das System beim Analysieren von erhaltenen Datenpaketen vorgehen soll. Es gibt die folgenden Optionen:<br>• **Suche**: Damit das Ereignis eintritt, muss das erhaltene Datenpaket den Text enthalten, der im Feld **Ausdruck** angegeben wurde, aber es darf auch noch weitere Inhalte haben<br><br>**Beispiel**: Wenn Sie bestimmt haben, dass das erhaltene Paket die Begriffe `Benutzer001` und `Tür053` enthalten soll, wird das Ereignis ausgelöst, wenn das empfangene Paket die Begriffe `Benutzer001` und `Tür053` und `Sonntag` enthält, da Ihre beiden gewünschten Begriffe im erhaltenen Paket enthalten sind<br>• **Übereinstimmung**: Damit das Ereignis eintritt, muss das erhaltene Datenpaket genau den Text enthalten, der im Feld **Ausdruck** angegeben wurde, und nichts anderes<br>• **Regulärer Ausdruck**:timmte Muster in den erhaltenen Datenpaketen angeben Damit das Ereignis eintritt, muss der Text, der im Feld **Ausdruck** angegeben wurde, bes<br>Wenn Sie von **Suche** oder **Übereinstimmung** auf **Regulärer Ausdruck** wechseln, wird der Text im Feld **Ausdruck** automatisch in einen regulären Ausdruck übersetzt. |
| **Priorität** | Die Priorität muss als Zahl zwischen 0 (höchste Priorität) und 999999 (niedrigste Priorität) angegeben werden.<br>Dasselbe Datenpaket kann auf unterschiedliche Ereignisse analysiert werden. Mit der Funktion des Zuweisens einer Priorität zu jedem Ereignis können Sie einstellen, welches Ereignis ausgelöst werden soll, wenn ein erhaltenes Paket mit den Kriterien von mehreren Ereignissen übereinstimmt.<br>Wenn das System ein TCP- und/oder UDP-Paket erhält, beginnt die Analyse des Pakets auf das Ereignis, das die höchste Priorität hat. Auf diese Weise wird nur das Ereignis mit der höchsten Priorität ausgelöst, wenn ein Paket mit den Kriterien von mehreren Ereignissen übereinstimmt. Wenn ein Paket mit den Kriterien von mehreren Ereignissen mit identischer Priorität übereinstimmt, z. B. zwei Ereignisse mit Priorität 999, werden alle Ereignisse dieser Priorität ausgelöst. |
| **Prüfen Sie, ob der Ausdruck mit dem Ereignis-String übereinstimmt** | Ein Ereignis-String, der mit dem Ausdruck abgeglichen werden soll, der im Feld **Ausdruck** eingegeben wurde. |

### Webhooks (Regeln und Ereignisknoten)

Im **Webhooks**-Knoten können Sie Webhook-Endpunkte erstellen, bearbeiten und löschen.

Beim Erstellen und Bearbeiten von Webhooks stehen folgende Felder zur Verfügung:

| Feld | Beschreibung |
|---|---|
| **Name** | Geben Sie einen eindeutigen Namen für den Webhook-Endpunkt ein.<br>Der Name für den Webhook darf nicht leer sein. |
| **Adresse** | Die URL des Webservers oder der Anwendung, an den/die Sie Ereignisdaten senden möchten. Wenn die URL des Webservers aktualisiert wird, müssen Sie den Webhook URL im Webhook-Knoten aktualisieren.<br>Durch die Verwendung HTTP über unsichere Netzwerke (wie offenes Internet) werden alle Ereignisse in Klartext dargestellt. |
| **Token** | Geben Sie ein Token ein, das verwendet wird, um die Kommunikation mit anderen Anwendungen zu sichern, indem Sie die Quelle des HTTP POST validieren.<br>Die Verwendung eines Tokens zur sicheren Kommunikation ist optional, wird jedoch empfohlen. |
| **API-Version** | Die Version des Webhook-Plugins und der API, die für die Webhook-Funktionalität verwendet werden. |

## Sicherheitsknoten

### Rollen (Sicherheitsknoten)

#### Registerkarte „Info“ (Rollen)

> Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Auf der Registerkarte **Info** eine Rolle können Sie folgende Einstellungen vornehmen:

| Name | Beschreibung |
|---|---|
| **Name** | Geben Sie einen Namen für die Rolle ein. |
| **Beschreibung** | Geben Sie eine Beschreibung für die Rolle ein. |
| **Management Client-Profil** | Wählen Sie ein Management Client-Profil zum Verknüpfen mit der Rolle aus.<br>Dies können Sie nicht auf die standardmäßige Rolle des **Administrators** anwenden.<br>  Erfordert Berechtigungen zur Verwaltung der Sicherheit auf dem Management-Server. |
| **Smart Client-Profil** | Wählen Sie ein Smart Client-Profil zum Verknüpfen mit der Rolle aus.<br>  Erfordert Berechtigungen zur Verwaltung der Sicherheit auf dem Management-Server. |
| **Standardzeitprofil** | Wählen Sie ein Standardzeitprofil zum Verknüpfen mit der Rolle aus.<br>Dies können Sie nicht auf die standardmäßige Rolle des **Administrators** anwenden. |
| **Beweissicherungsprofil** | Wählen Sie ein Beweissicherungsprofil zum Verknüpfen mit der Rolle aus. |
| **Smart Client Anmeldung innerhalb des Zeitprofils** | Wählen Sie ein Zeitprofil aus, über das sich der XProtect Smart Client-Benutzer anmelden darf, der mit dieser Rolle verknüpft ist.<br>Sollte der XProtect Smart Client-Benutzer angemeldet sein, wenn die Zeit abläuft, wird diese Person automatisch abgemeldet.<br>Dies können Sie nicht auf die standardmäßige Rolle des **Administrators** anwenden. |

| Name | Beschreibung |
|---|---|
| **Smart Client-Anmeldung erlauben** | Aktivieren Sie das Kontrollkästchen, um mit dieser Rolle verknüpften Benutzern zu erlauben, sich auf XProtect Smart Client anzumelden.<br>Der Zugriff auf Smart Client ist standardmäßig nicht erlaubt. Deaktivieren Sie das Kontrollkästchen, um den Zugriff auf XProtect Smart Client zu verweigern. |
| **XProtect Mobile-Client-Anmeldung erlauben** | Aktivieren Sie das Kontrollkästchen, um mit dieser Rolle verknüpften Benutzern zu erlauben, sich auf dem XProtect Mobile-Client anzumelden.<br>Der Zugriff auf XProtect Mobile-Client ist standardmäßig nicht erlaubt. Deaktivieren Sie das Kontrollkästchen, um den Zugriff auf den XProtect Mobile-Client zu verweigern. |
| **XProtect Web Client-Anmeldung erlauben** | Aktivieren Sie das Kontrollkästchen, um mit dieser Rolle verknüpften Benutzern zu erlauben, sich auf XProtect Web Client anzumelden.<br>Der Zugriff auf XProtect Web Client ist standardmäßig nicht erlaubt. Deaktivieren Sie das Kontrollkästchen, um den Zugriff auf XProtect Web Client zu verweigern. |
| **Anmelde-Autorisierung erforderlich** | Aktivieren Sie das Kontrollkästchen, um die Anmelde-Autorisierung mit der Rolle zu verknüpfen. Das bedeutet, dass XProtect Smart Client oder der Management Client nach einer zweiten Autorisierung fragt, meist durch einen Superuser oder Manager, wenn sich der Benutzer anmeldet.<br>Damit Administratoren Benutzer autorisieren können, konfigurieren Sie die Berechtigung **Benutzer autorisieren** für den Management Server auf der Registerkarte **Allgemeine Sicherheit**.<br>Dies können Sie nicht auf die standardmäßige Rolle des **Administrators** anwenden. |
| **Benutzer während PTZ-Sitzungen anonymisieren** | Aktivieren Sie das Kontrollkästchen, um die Namen der Benutzer auszublenden, die mit dieser Rolle verknüpft sind, wenn sie PTZ-Sitzungen regeln. |

### Benutzer und Gruppen-Registerkarte (Rollen)

Auf der Registerkarte **Benutzer und Gruppen**, weisen Sie Benutzern und Gruppen Rollen zu (siehe Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen auf Seite 309). Sie können Windows-Benutzer und Gruppen oder Basisbenutzer zuweisen (siehe Benutzer (Erklärung) auf Seite 66).

### Externer IDP (Rollen)

Auf der Registerkarte **externer IDP** können Sie bestehende Ansprüche anzeigen und neue Ansprüche zu Rollen hinzufügen.

| Name | Beschreibung |
|---|---|
| **Externer IDP** | Der Name des externen IDP. |
| **Name der Forderung** | Eine Variable, die im externen IDP festgelegt wird. |
| **Wert der Forderung** | Der Wert des Anspruchs, z. B. ein Gruppenname, anhand dessen dem Benutzer die entsprechende Rolle zugewiesen werden kann. |

### Registerkarte „Gesamtsicherheit“ (Rollen)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Auf der Registerkarte **Allgemeine Sicherheit** legen Sie die allgemeinen Berechtigungen für Rollen fest. Legen Sie für jede in Ihrem System verfügbare Komponente Zugriffsrechte für die Rollen fest, indem Sie **Zulassen** oder **Verweigern** einstellen. Wenn einer Rolle der Zugriff auf eine Komponente verwehrt wird, so ist die betreffende Komponente auf der Registerkarte **Gesamtsicherheit** für einen Benutzer in dieser Rolle nicht sichtbar.

Die Reigisterkarte **Globale Sicherheit** ist in der Gratis-XProtect Essential+ nicht verfügbar.

Sie können für XProtect Corporate mehr Zugriffsberechtigungen festlegen als bei den anderen XProtect VMS-Produkten. Dies liegt daran, dass Sie in XProtect Corporate nur differenzierte Administratorberechtigungen einrichten können, während Sie für eine Rolle, die XProtect Smart Client, XProtect Web Client oder XProtect Mobile Client verwendet, in allen Produkten allgemeine Berechtigungen einrichten können.

Die Gesamtsicherheitseinstellungen gelten nur für den aktuellen Standort.

Wenn Sie einen Benutzer mit mehr als einer Rolle verknüpfen und die Option **Verweigern** bei einer Sicherheitseinstellung für eine Rolle und für eine andere die Option **Zulassen** wählen, hat die Berechtigung **Verweigern** Vorrang vor der Berechtigung **Zulassen**.

Im Folgenden wird beschrieben, was mit jeder der Berechtigungen für die verschiedenen Systemkomponenten passiert, wenn Sie für die jeweilige Rolle die Option **Zulassen** wählen. Bei Verwendung von XProtect Corporate sehen Sie unter jeder Systemkomponente, welche Einstellungen **nur** für Ihr System verfügbar sind.

Für jede Systemkomponente oder -funktion kann der Gesamtsystemadministrator die Kontrollkästchen **Zulassen** oder **Verweigern** verwenden, um Sicherheitsberechtigungen für die Rolle einzurichten. Sicherheitsberechtigungen, die Sie hier einrichten, werden für die gesamte Systemkomponente oder -funktion eingerichtet. Wenn Sie z.B. das Kontrollkästchen **Verweigern** bei **Kameras** auswählen, sind für die Rolle keine der zum System hinzugefügten Kameras verfügbar. Wenn Sie dagegen das Kontrollkästchen **Zulassen** aktivieren, sind für die Rolle alle zum System hinzugefügten Kameras sichtbar. Die Auswahl von **Zulassen** oder **Verweigern** für Ihre Kameras bewirkt, dass die Kameraeinstellungen auf der Registerkarte **Gerät** Ihre Auswahl auf der Registerkarte **Gesamtsicherheit** übernehmen, sodass für die jeweilige Rolle entweder alle Kameras verfügbar oder nicht verfügbar sind.

Wenn Sie Sicherheitsberechtigungen für **einzelne** Kameras oder Ähnliches festlegen möchten, können Sie diese individuellen Berechtigungen nur dann auf der Registerkarte der betreffenden Systemkomponente oder -funktion einstellen, wenn Sie **keine Gesamtberechtigungen** für die Systemkomponente oder -funktion auf der Registerkarte **Gesamtsicherheit** festgelegt haben.

Die nachstehenden Beschreibungen gelten auch für die Berechtigungen, die Sie über den MIP SDK konfigurieren können.

Wenn Sie Ihre Basislizenz von XProtect Corporate auf eines der anderen Produkte umstellen möchten, achten Sie darauf, dass Sie alle Sicherheitsberechtigungen entfernen, die nur für XProtect Corporate zur Verfügung stehen. Wenn Sie diese Berechtigungen nicht entfernen, können Sie die Umstellung nicht abschließen.

### Managementserver

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Verbinden** | Dies ermöglicht es den Benutzern, sich mit Management Server zu verbinden.<br>Die Erlaubnis ist standardmäßig aktiviert.<br>Sie können die Erlaubnis für die Verbindung für Rollen für Wartungszwecke vorübergehend verweigern und dann den Zugriff auf das System erneut beantragen.<br>⚠ Diese Erlaubnis muss ausgewählt werden, um den Zugriff zum System zuzulassen. |
| **Lesen** | ⚠ Diese Berechtigung ist eine hochprivilegierte Verwaltungsberechtigung, die dem Benutzer umfangreiche Zugriffsrechte zum XProtect VMS gewährt, einschließlich des Zugriffs auf sensible Daten wie die im System konfigurierten Anmeldeinformationen.<br>Aktiviert den Zugriff auf eine Vielzahl verschiedener Funktionen, darunter:<br>• Anmelden mit dem Management Client<br>• Liste aktueller Aufgaben<br>• Server-Protokolle<br>Darüber hinaus ermöglicht es den Zugriff auf:<br>• Fernzugriffsdienste<br>• Smart Client Profile<br>• Management Client Profile<br>• Matrix<br>• Zeitprofile |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| | • Registrierte Server und Service Registration API<br><br>Diese Berechtigung erlaubt dem Client auch den Zugriff auf bestimmte sensible Informationen:<br><br>• Anmeldeinformationen für jeden konfigurierten externen Identity Provider<br>• Anmeldeinformationen, IP-Adressen und andere Informationen für alle Kameras im XProtect VMS<br>• Anmeldeinformationen für den konfigurierten Mailserver<br>• Anmeldeinformationen für jede konfigurierte Matrix<br>• Anmeldeinformationen, die für die Interconnect-Funktion konfiguriert sind<br>• Anmeldeinformationen, die für die Lizenzaktivierung konfiguriert sind<br><br>Mit dieser Berechtigung werden die Anmeldeinformationen der XProtect VMS-Benutzer nicht angezeigt. Dazu gehören Basisnutzer, Windows-Benutzer und Benutzer von externen IDPs. |
| **Bearbeiten** | Aktiviert die Berechtigung, bei einer Vielzahl verschiedener Funktionen Daten zu verändern, darunter:<br><br>• Optionen<br>• Lizenzverwaltung<br><br>Benutzer können außerdem das Folgende erstellen, löschen und bearbeiten:<br><br>• Fernzugriffsdienste<br>• Gerätegruppen<br>• Matrix<br>• Zeitprofile<br>• Benachrichtigungsprofile<br>• Registrierte Server |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| | Aktiviert die Berechtigung zur Konfiguration lokaler IP-Bereiche bei der Konfiguration des Netzwerks auf dem Aufzeichnungsserver. |
| **Systemmonitor** | Aktiviert die Berechtigung zur Einsichtnahme in die Daten des Systemmonitors. |
| **Status-API** | Aktiviert die Berechtigung zur Durchführung von Abfragen der Status-API auf dem Aufzeichnungsserver. D.h. die Rolle mit dieser aktiven Berechtigung kann den Status der Objekte auf dem Aufzeichnungsserver lesen. |
| **Hierarchie der föderalen Standorte verwalten** | Aktiviert die Berechtigung, den aktuellen Standort zu anderen Standorten in einer Verbundhierarchie hinzuzufügen und ihn davon trennen.<br>Wenn Sie diese Berechtigung nur für den untergeordneten Standort zulassen, kann der Benutzer dennoch den Standort vom übergeordneten Standort lösen. |
| **Sicherung von Konfiguration** | Aktiviert die Berechtigung, mit Hilfe der Sicherungs- und Wiederherstellungsfunktion des Systems Sicherungskopien der Systemkonfiguration zu erstellen. |
| **Benutzer autorisieren** | Aktiviert die Berechtigung, Benutzer zu autorisieren, wenn sie in XProtect Smart Client oder Management Client zu einer zweiten Anmeldung aufgefordert werden. Sie legen fest, ob für eine Rolle die Autorisierung für die Anmeldung auf der Registerkarte **Info** erforderlich ist. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung zur Verwaltung von Berechtigungen für den Management Server.<br>Benutzer können außerdem folgende Funktionsbereiche erstellen, löschen und bearbeiten: |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| | • Rollen<br>• Basisnutzer<br>• Smart Client Profile<br>• Management Client Profile |

**Aufzeichnungsserver**

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Bearbeiten** | Aktiviert die Berechtigung zum Bearbeiten von Eigenschaften auf den Aufzeichnungsservern, mit Ausnahme der Netzwerkkonfigurationseinstellungen, für deren Bearbeitung eine Berechtigung auf dem Management Server erforderlich ist. |
| **Löschen** | Aktiviert die Berechtigung, Aufzeichnungsserver zu löschen. Hierfür müssen Sie dem Benutzer auch Löschberechtigungen für Folgendes geben:<br>• Hardwaresicherheitsgruppe, wenn Sie Hardware zum Aufzeichnungsserver hinzugefügt haben<br>Wenn eines der Geräte auf dem Aufzeichnungsserver Beweissicherungen enthält, können Sie den Aufzeichnungsserver nur löschen, wenn er offline ist. |
| **Hardware verwalten** | Aktiviert die Berechtigung, auf Aufzeichnungsservern Hardware hinzuzufügen. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Speicher verwalten** | Aktiviert die Berechtigung, auf dem Aufzeichnungsserver Speichercontainer zu verwalten, d. h. Speichercontainer zu erstellen, zu löschen, zu verschieben und zu leeren. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung zur Verwaltung von Sicherheitsberechtigungen für Aufzeichnungsserver. |

### Failover-Server

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, in der Management Client auf Failover-Server zuzugreifen und diese einzusehen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in der Management Client Failover-Server zu erstellen, zu aktualisieren, zu löschen, zu verschieben und zu aktivieren oder zu deaktivieren. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen für die Failover-Server zu verwalten. |

### Mobile Server

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, in der Management Client auf Mobil-Server zuzugreifen und diese einzusehen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in der Management Client Mobile-Server zu bearbeiten und zu löschen. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen für die Mobil-Server zu verwalten. |
| **Erstellen** | Aktiviert die Berechtigung, Mobil-Server zum System hinzuzufügen. |

**Hardware**

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Bearbeiten** | Aktiviert die Berechtigung, Eigenschaften von Hardware zu bearbeiten. |
| **Löschen** | Aktiviert die Berechtigung, Hardware zu löschen.<br>Wenn eines der Hardwaregeräte Beweissicherungen enthält, können Sie die Hardware nur löschen, wenn der Aufzeichnungsserver offline ist. |
| **Treiberbefehle** | Aktiviert die Berechtigung, spezielle Befehle an die Treiber zu senden und damit |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| | Funktionen und die Konfiguration auf dem Gerät selbst zu steuern.<br><br>Die Berechtigung für **Treiberbefehle** ist nur für speziell entwickelte MIP Plug-ins in den Clients vorgesehen. Es steuert keine Aufgaben, die Standardkonfiguration betreffend. |
| **Passwörter anzeigen** | Aktiviert die Berechtigung, sich im Dialogfeld **Hardware bearbeiten** Passwörter auf Hardware-Geräten anzeigen zu lassen. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen für die Hardware zu verwalten. |

**Kameras**

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, in den Clients und im Management Client Kamerageräte einzusehen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in der Management Client die Eigenschaften für Kameras zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Kameras. |
| **Live ansehen** | Aktiviert die Berechtigung, in den Clients und im Management Client Live-Video von Kameras anzusehen. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Eingeschränkte Live-Übertragung ansehen** | Ermöglicht die Anzeige von eingeschränkten Live-Videos von Kameras auf den Clients und dem Management Client. |
| **Wiedergabe** | Aktiviert die Berechtigung zur Wiedergabe von Videoaufzeichnungen von Kameras in allen Clients. |
| **Eingeschränkte Aufnahmen wiedergeben** | Ermöglicht die Berechtigung zur Wiedergabe von aufgezeichneten eingeschränkten Videos von Kameras auf allen Clients. |
| **Fernaufzeichnungen abrufen** | Aktiviert die Berechtigung zum Abrufen von Aufzeichnungen in den Clients von Kameras an entfernten Standorten oder von Edge-Speichern auf Kameras. |
| **Sequenzen lesen** | Aktiviert die Berechtigung zum Lesen der Sequenzinformationen, z. B. für die Wiedergabe von Videoaufzeichnungen in den Clients. |
| **intelligente Suche** | Aktiviert die Berechtigung zur Nutzung der intelligenten Suchfunktion in den Clients. |
| **Exportieren** | Aktiviert die Berechtigung, Aufzeichnungen von den Clients zu exportieren. |
| **Lesezeichen erstellen** | Aktiviert die Berechtigung, in Videoaufzeichnungen und Live-Videos auf den Clients Lesezeichen zu erstellen. |
| **Lesezeichen lesen** | Aktiviert die Berechtigung, in den Clients Lesezeichendetails zu suchen und zu lesen. |
| **Lesezeichen bearbeiten** | Aktiviert die Berechtigung, Lesezeichen in den Clients zu bearbeiten. |
| **Lesezeichen löschen** | Aktiviert die Berechtigung zum Löschen von Lesezeichen in den Clients. |
| **Beweissicherungen erstellen und erweitern** | Aktiviert die Berechtigung, Beweissicherungen in den Clients anzulegen und zu erweitern. |
| **Beweissicherungen lesen** | Aktiviert die Berechtigung, Beweissicherungen in den Clients zu durchsuchen und zu lesen. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Beweissicherungen löschen und reduzieren** | Aktiviert die Berechtigung, Beweissicherungen in den Clients zu löschen oder zu reduzieren. |
| **Live- und Wiedergabebeschränkungen erstellen und erweitern** | Ermöglicht die Berechtigung zum Erstellen und Erweitern von Einschränkungen in den Clients. |
| **Live- und Wiedergabebeschränkungen lesen** | Ermöglicht die Berechtigung zur Einsichtnahme in eine Liste der bestehenden Einschränkungen in den Clients. |
| **Live- und Wiedergabebeschränkungen löschen und reduzieren** | Ermöglicht die Berechtigung zum Löschen und Reduzieren von Einschränkungen in den Clients. |
| **Manuelle Aufzeichnung starten** | Aktiviert die Berechtigung, in den Clients manuelle Videoaufzeichnungen zu starten. |
| **Manuelle Aufzeichnung stoppen** | Aktiviert die Berechtigung, in den Clients manuelle Videoaufzeichnungen abzubrechen. |
| **AUX-Befehle** | Aktiviert die Berechtigung, auf der Kamera von den Clients aus Hilfsbefehle (AUX) zu verwenden.<br>**AUX-Befehle** bieten Benutzern z. B. die Möglichkeit, Wischer an Kameras zu steuern, die über einen Videoencoder verbunden sind. Mit Kameras verknüpfte Geräte, die über Hilfsanschlüsse verbunden sind, werden vom Client gesteuert. |
| **Manuelles PTZ** | Aktiviert die Berechtigung, auf PTZ-Kameras in den Clients und der Management Client PTZ-Funktionen zu verwenden. |
| **PTZ-Voreinstellungen oder Wachrundgangprofile aktivieren** | Aktiviert die Berechtigung, PTZ-Kameras an voreingestellte Positionen zu bewegen, Patrouillenprofile zu starten und zu stoppen und eine Patrouille auf den Clients und im Management Client zu unterbrechen.<br>Damit diese Rolle andere PTZ-Funktionen auf der Kamera nutzen kann, aktivieren Sie die Berechtigung für **Manuelles PTZ**. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **PTZ-Voreinstellungen oder Wachrundgangprofile verwalten** | Aktiviert die Berechtigung, PTZ-Voreinstellungen und Patrouillenprofilen auf PTZ-Kameras in den Clients und im Management Client hinzuzufügen, zu bearbeiten und zu löschen.<br>Damit diese Rolle andere PTZ-Funktionen auf der Kamera nutzen kann, aktivieren Sie die Berechtigung für **Manuelles PTZ**. |
| **PTZ-Voreinstellungen sperren/entsperren** | Aktiviert die Berechtigung, PTZ-Voreinstellungen im Management Client zu sperren und freizugeben. Ermöglicht oder verhindert, dass andere Benutzer Preset-Positionen in den Clients und im Management Client ändern können. |
| **PTZ-Sitzungen reservieren** | Aktiviert die Berechtigung, in den Clients und im Management Client PTZ-Kameras auf den reservierten PTZ-Sitzungsmodus zu stellen.<br>In einer reservierten PTZ-Sitzung können andere Benutzer mit einer höheren PTZ-Priorität nicht die Kontrolle übernehmen.<br>Damit diese Rolle andere PTZ-Funktionen auf der Kamera nutzen kann, aktivieren Sie die Berechtigung für **Manuelles PTZ**. |
| **PTZ-Sitzungen freigeben** | Aktiviert die Berechtigung, die PTZ-Sitzungen anderer Benutzer aus dem Management Client freizugeben.<br>Sie können Ihre eigenen PTZ-Sitzungen jederzeit ohne diese Berechtigung freigeben. |
| **Aufzeichnungen löschen** | Aktiviert die Berechtigung, über die Management Client gespeicherte Videoaufzeichnungen vom System zu löschen. |
| **Privatzonenmasken aufheben** | Aktiviert die Berechtigung, aus Datenschutzgründen verdeckte Bildbereiche in XProtect Smart Client vorübergehend freizulegen. Aktiviert auch die Berechtigung, anderen XProtect Smart Client-Nutzern zu erlauben, aus Datenschutzgründen verdeckte Bildbereiche freizulegen. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| | Die Aufhebung von Privatzonenmasken gilt nur für Privatzonenmasken, die im Management Client als aufhebbar konfiguriert sind. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, im Management Client Sicherheitsberechtigungen für die Kamera zu verwalten. |

### Mikrofone

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, sich Mikrofongeräte in den Clients und im Management Client anzeigen zu lassen. |
| **Bearbeiten** | Aktiviert die Berechtigung, Mikrofoneigenschaften in der Management Client zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Mikrofonen. |
| **Live abhören** | Aktiviert die Berechtigung, den Ton von Lautsprechern in den Clients und den Management Client live abzuhören. |
| **Eingeschränktes Live-Audio anhören** | Ermöglicht die Berechtigung, eingeschränkte Live-Audiosignale von den Lautsprechern der Clients und Management Clientzu hören. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Wiedergabe** | Aktiviert die Berechtigung, Tonaufzeichnungen von Mikrofonen in den Clients wiederzugeben. |
| **Eingeschränkte Aufnahmen wiedergeben** | Aktiviert die Berechtigung, eingeschränkte Tonaufzeichnungen von Mikrofonen in den Clients wiederzugeben. |
| **Fernaufzeichnungen abrufen** | Aktiviert die Berechtigung, in den Clients Aufnahmen von Mikrofonen an entfernten Standorten oder von Edge-Speichern auf Kameras abzurufen. |
| **Sequenzen lesen** | Aktiviert die Berechtigung, die Sequenzinformationen zu lesen, die sich z. B. auf die Registerkarte **Wiedergabe** in den Clients beziehen. |
| **Exportieren** | Aktiviert die Berechtigung, Aufzeichnungen von den Clients zu exportieren. |
| **Lesezeichen erstellen** | Aktiviert die Berechtigung, Lesezeichen in den Clients zu erstellen. |
| **Lesezeichen lesen** | Aktiviert die Berechtigung, in den Clients Lesezeichendetails zu suchen und zu lesen. |
| **Lesezeichen bearbeiten** | Aktiviert die Berechtigung, Lesezeichen in den Clients zu bearbeiten. |
| **Lesezeichen löschen** | Aktiviert die Berechtigung zum Löschen von Lesezeichen in den Clients. |
| **Beweissicherungen erstellen und erweitern** | Aktiviert die Berechtigung, Beweissicherungen in den Clients zu erstellen oder zu erweitern. |
| **Beweissicherungen lesen** | Aktiviert die Berechtigung, Einzelheiten zu Beweissicherungen in den Clients zu durchsuchen und zu lesen. |
| **Beweissicherungen löschen und reduzieren** | Aktiviert die Berechtigung, Beweissicherungen in den Clients zu löschen oder zu reduzieren. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Live- und Wiedergabebeschränkungen erstellen und erweitern** | Ermöglicht die Berechtigung des Erstellens und Erweiterns von Einschränkungen für Mikrofone auf den Clients. |
| **Live- und Wiedergabebeschränkungen lesen** | Aktiviert die Berechtigung, eine Liste der bestehenden Einschränkungen für Mikrofone in den Clients anzuzeigen. |
| **Live- und Wiedergabebeschränkungen löschen und reduzieren** | Ermöglicht die Berechtigung, Einschränkungen für Mikrofone auf den Clients zu löschen und zu reduzieren. |
| **Manuelle Aufzeichnung starten** | Aktiviert die Berechtigung, manuelle Tonaufzeichnungen in den Clients zu starten. |
| **Manuelle Aufzeichnung stoppen** | Aktiviert die Berechtigung, manuelle Tonaufzeichnungen in den Clients abzubrechen. |
| **Aufzeichnungen löschen** | Aktiviert die Berechtigung, gespeicherte Aufzeichnungen vom System zu löschen. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, in der Management Client Sicherheitsberechtigungen für Mikrofone zu verwalten. |

### Lautsprecher

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Lesen** | Aktiviert die Berechtigung, sich in den Clients und den Management Client Lautsprechergeräte anzeigen zu lassen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in der Management Client die Eigenschaften für Lautsprecher zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Lautsprechern. |
| **Live abhören** | Aktiviert die Berechtigung, den Ton von Lautsprechern in den Clients und den Management Client live abzuhören. |
| **Eingeschränktes Live-Audio anhören** | Ermöglicht die Berechtigung, eingeschränkte Live-Audiosignale von den Lautsprechern der Clients und Management Clientzu hören. |
| **Sprechen** | Aktiviert die Berechtigung, über die Lautsprecher in den Clients zu sprechen. |
| **Wiedergabe** | Aktiviert die Berechtigung, Tonaufzeichnungen von Lautsprechern in den Clients wiederzugeben. |
| **Eingeschränkte Aufnahmen wiedergeben** | Aktiviert die Berechtigung, Tonaufzeichnungen von Lautsprechern in den Clients wiederzugeben. |
| **Fernaufzeichnungen abrufen** | Aktiviert die Berechtigung zum Abrufen von Aufzeichnungen in den Clients von Lautsprechern an entfernten Standorten oder von Edge-Speichern auf Kameras. |
| **Sequenzen lesen** | Aktiviert die Berechtigung, Tonaufzeichnungen von Lautsprechern in den Clients mit Hilfe der Sequenzen-Funktion zu durchsuchen. |
| **Exportieren** | Aktiviert die Berechtigung, Tonaufzeichnungen von Lautsprechern in den Clients zu exportieren. |
| **Lesezeichen erstellen** | Aktiviert die Berechtigung, Lesezeichen in den Clients zu erstellen. |
| **Lesezeichen lesen** | Aktiviert die Berechtigung, in den Clients Lesezeichendetails |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| | zu suchen und zu lesen. |
| **Lesezeichen bearbeiten** | Aktiviert die Berechtigung, Lesezeichen in den Clients zu bearbeiten. |
| **Lesezeichen löschen** | Aktiviert die Berechtigung zum Löschen von Lesezeichen in den Clients. |
| **Beweissicherungen erstellen und erweitern** | Aktiviert die Berechtigung, Beweissicherungen zu erstellen oder zu erweitern, um Tonaufzeichnungen in den Clients zu schützen. |
| **Beweissicherungen lesen** | Aktiviert die Berechtigung, mit Beweissicherungen geschützte Tonaufzeichnungen in den Clients einzusehen. |
| **Beweissicherungen löschen und reduzieren** | Aktiviert die Berechtigung, Beweissicherungen auf geschützten Tonaufzeichnungen in den Clients zu löschen oder zu reduzieren. |
| **Live- und Wiedergabebeschränkungen erstellen und erweitern** | Ermöglicht das Erstellen und Erweitern von Einschränkungen für Sprecher in den Clients. |
| **Live- und Wiedergabebeschränkungen lesen** | Ermöglicht die Einsichtnahme in eine Liste der bestehenden Einschränkungen für Sprecher in den Clients. |
| **Live- und Wiedergabebeschränkungen löschen und reduzieren** | Ermöglicht die Berechtigung zum Löschen und Reduzieren von Einschränkungen für Sprecher in den Clients. |
| **Manuelle Aufzeichnung starten** | Aktiviert die Berechtigung, manuelle Tonaufzeichnungen in den Clients zu starten. |
| **Manuelle Aufzeichnung stoppen** | Aktiviert die Berechtigung, manuelle Tonaufzeichnungen in den Clients abzubrechen. |
| **Aufzeichnungen löschen** | Aktiviert die Berechtigung, gespeicherte Aufzeichnungen vom System zu löschen. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Sicherheit verwalten** | Aktiviert die Berechtigung, im Management Client Sicherheitsberechtigungen für Lautsprecher zu verwalten. |

**Metadaten**

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, in den Clients Metadaten zu empfangen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in der Management Client die Eigenschaften von Metadaten zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Metadatengeräten. |
| **Live** | Aktiviert die Berechtigung, in den Clients Live-Metadaten von Metadatengeräten zu empfangen. |
| **Eingeschränkte Live-Übertragung ansehen** | Ermöglicht die Berechtigung, eingeschränkte Live-Metadaten von Metadatengeräten in den Clients zu empfangen. |
| **Wiedergabe** | Aktiviert die Berechtigung, von Metadatengeräten aufgezeichnete Daten in den Clients wiederzugeben. |
| **Eingeschränkte Aufnahmen wiedergeben** | Ermöglicht die Wiedergabe von eingeschränkten aufgezeichneten Daten von Metadatengeräten auf den Clients. |
| **Fernaufzeichnungen abrufen** | Aktiviert die Berechtigung, in den Clients Aufnahmen von |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| | Metadatengeräten an entfernten Standorten oder von Edge-Speichern auf Kameras abzurufen. |
| **Sequenzen lesen** | Aktiviert die Berechtigung, die Sequenzinformationen zu lesen, die sich z. B. auf die Registerkarte **Wiedergabe** in den Clients beziehen. |
| **Exportieren** | Aktiviert die Berechtigung, Aufzeichnungen in den Clients zu exportieren. |
| **Beweissicherungen erstellen und erweitern** | Aktiviert die Berechtigung, in den Clients Beweissicherungen zu erstellen. |
| **Beweissicherungen lesen** | Aktiviert die Berechtigung, sich Beweissicherungen in den Clients anzeigen zu lassen. |
| **Beweissicherungen löschen und reduzieren** | Aktiviert die Berechtigung, Beweissicherungen in den Clients zu löschen oder zu reduzieren. |
| **Live- und Wiedergabebeschränkungen erstellen und erweitern** | Ermöglicht die Erstellung und Erweiterung von Einschränkungen für Metadaten in den Clients. |
| **Live- und Wiedergabebeschränkungen lesen** | Ermöglicht die Einsichtnahme in eine Liste der bestehenden Einschränkungen für Metadaten in den Clients. |
| **Live- und Wiedergabebeschränkungen löschen und reduzieren** | Ermöglicht die Berechtigung, Metadaten in den Clients zu löschen und Einschränkungen zu reduzieren. |
| **Manuelle Aufzeichnung starten** | Aktiviert die Berechtigung, die manuelle Aufzeichnung von Metadaten in den Clients zu starten. |
| **Manuelle Aufzeichnung stoppen** | Aktiviert die Berechtigung, die manuelle Aufzeichnung von Metadaten in den Clients abzubrechen. |
| **Aufzeichnungen löschen** | Aktiviert die Berechtigung, gespeicherte Aufzeichnungen vom System zu löschen. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Sicherheit verwalten** | Aktiviert die Berechtigung, im Management Client Sicherheitsberechtigungen für Metadaten zu verwalten. |

### Eingang

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, in den Clients und im Management Client Eingabegeräte einzusehen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in der Management Client die Eigenschaften für Eingabegeräte zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Eingabegeräten. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, in der Management Client Sicherheitsberechtigungen für Eingabegeräte zu verwalten. |

### Ausgang

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, sich in den Clients Ausgabegeräte anzeigen zu lassen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in der Management Client die Eigenschaften für Ausgabegeräte zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Ausgabegeräten. |
| **Aktivieren** | Aktiviert die Berechtigung, Ausgänge in den Clients zu aktivieren. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung zur Verwaltung von Sicherheitsberechtigungen in Management Client für Ausgabegeräte. |

### Smart Wall

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitsberechtigungen in XProtect Management Client. |
| **Lesen** | Aktiviert die Berechtigung zum Betrachten einer Videowand in XProtect Smart Client. |
| **Bearbeiten** | Aktiviert die Berechtigung zum Bearbeiten von Eigenschaften für die Smart Wall Definition in XProtect Management Client. |
| **Löschen** | Aktiviert die Berechtigung zum Löschen vorhandener Smart Wall Definitionen in XProtect Management Client. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Bedienen** | Aktiviert die Berechtigung zum Aktivieren und Ändern von Smart Wall Definitionen, z. B. zum Ändern und Aktivieren von Voreinstellungen oder zum Anwenden von Kameras auf Ansichten in XProtect Smart Client und in XProtect Management Client.<br><br>Sie können **Betrieb** mit Zeitprofilen verknüpfen, die festlegen, wann die Benutzerberechtigung gilt. |
| **Smart Wall Erstellen** | Aktiviert die Berechtigung zum Erstellen neuer Smart Wall Definitionen in XProtect Management Client. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitsberechtigungen in XProtect Management Client für die Smart Wall Definition. |
| **Wiedergabe** | Aktiviert die Berechtigung zur Wiedergabe aufgezeichneter Daten von einer Videowand in XProtect Smart Client.<br><br>Sie können die **Wiedergabe** mit Zeitprofilen verknüpfen, die festlegen, wann die Benutzerberechtigung gilt. |

### Ansichtsgruppen

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, sich in den Clients und im Management |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| | Client Ansichtsgruppen anzeigen zu lassen. Ansichtsgruppen werden im Management Client erstellt. |
| **Bearbeiten** | Aktiviert die Berechtigung, an den Ansichtsgruppen in der Management Client Eigenschaften zu bearbeiten. |
| **Löschen** | Aktiviert die Berechtigung, Ansichtsgruppen in der Management Client zu löschen. |
| **Bedienen** | Aktiviert die Berechtigung, in XProtect Smart Client Ansichtsgruppen in zu verwenden, d. h. Untergruppen und Ansichten zu erstellen und zu löschen. |
| **Ansichtsgruppe erstellen** | Aktiviert die Berechtigung, in der Management Client Ansichtsgruppen zu erstellen. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, in der Management Client Sicherheitsberechtigungen für Ansichtsgruppen zu verwalten. |

**Benutzerdefinierte Ereignisse**

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, sich in den Clients benutzerdefinierte Ereignisse anzeigen zu lassen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in Management Client Eigenschaften bei benutzerdefinierten Ereignissen zu bearbeiten. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Löschen** | Aktiviert die Berechtigung, in den Management Client benutzerdefinierte Ereignisse zu löschen. |
| **Auslöser** | Aktiviert die Berechtigung, in den Clients benutzerdefinierte Ereignisse auszulösen. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, in der Management Client Sicherheitsberechtigungen für benutzerdefinierte Ereignisse zu verwalten. |
| **Benutzerdefiniertes Ereignis erstellen** | Aktiviert die Berechtigung, in den Management Client neue benutzerdefinierte Ereignisse zu erstellen. |

### Analyseereignisse

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, in den Management Client Analyseereignisse einzusehen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in Management Client Eigenschaften bei Analyseereignisse zu bearbeiten. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, in der Management Client Sicherheitsberechtigungen für Analyseereignisse zu verwalten. |

### Generische Ereignisse

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, in den Clients und im Management Client allgemeine Ereignisse einzusehen. |
| **Bearbeiten** | Aktiviert die Berechtigung, in Management Client Eigenschaften bei allgemeinen Ereignissen zu bearbeiten. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, in der Management Client Sicherheitsberechtigungen für allgemeine Ereignisse zu verwalten. |

**Matrix**

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, Videos von den Clients auszuwählen an den Matrix-Empfänger zu senden. |
| **Bearbeiten** | Aktiviert die Berechtigung, in der Matrix die Eigenschaften für eine Management Client zu bearbeiten. |
| **Löschen** | Aktiviert die Berechtigung, in der Matrix eine Management Client zu löschen. |
| **Matrix Erstellen** | Aktiviert die Berechtigung, in der Matrix eine neue Management Client zu erstellen. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen im Management Client für alle Matrix zu verwalten. |

### Regeln

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, bestehende Regeln in der Management Client einzusehen. |
| **Bearbeiten** | Aktiviert die Berechtigung, Eigenschaften für Regeln zu bearbeiten und das Regelverhalten in der Management Client festzulegen.<br>Erfordert außerdem, dass der Benutzer auf alle von der Regel betroffenen Geräte Schreibzugriff hat. |
| **Löschen** | Aktiviert die Berechtigung, Regeln aus dem Management Client zu löschen.<br>Erfordert außerdem, dass der Benutzer auf alle von der Regel betroffenen Geräte Schreibzugriff hat. |
| **Regel erstellen** | Aktiviert die Berechtigung, in der Management Client neue Regeln zu erstellen.<br>Erfordert außerdem, dass der Benutzer auf alle von der Regel betroffenen Geräte Schreibzugriff hat. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, im Management Client Sicherheitsberechtigungen für alle Regeln zu verwalten. |

### Sites

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, in der Management Client andere Standorte einzusehen. Verbundene Standorte sind über die Milestone Federated Architecture verbunden.<br>Zur Bearbeitung von Eigenschaften benötigen Sie auf dem Management-Server Bearbeitungsberechtigungen für jeden Standort. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung zur Verwaltung von Sicherheitsberechtigungen an allen Standorten. |

### Systemmonitor

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, sich die Systemmonitore in XProtect Smart Client anzeigen zu lassen. |
| **Bearbeiten** | Aktiviert die Berechtigung, die Eigenschaften von Systemmonitoren in der Management Client zu bearbeiten. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, im Management Client Sicherheitsberechtigungen für alle Systemmonitore zu verwalten. |

### Metadatensuche

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Aktiviert die Berechtigung, sich die Funktion **Metadatennutzung** im Management Client und die zugehörigen Einstellungen anzeigen zu lassen, aber nicht die Berechtigung, die Einstellungen zu ändern. |
| **Konfiguration der Metadatensuche bearbeiten** | Aktiviert die Berechtigung, Metadaten-Suchkategorien, z. B. Metadaten für Personen oder Fahrzeuge, im Management Client zu aktivieren oder zu deaktivieren. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen für die Suche in Metadaten zu verwalten. |

### Suchen

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Öffentliche Suchen lesen** | Aktiviert die Berechtigung, sich gespeicherte öffentliche Suchvorgänge in XProtect Smart Client anzeigen zu lassen und diese zu öffnen. |
| **Öffentliche Suchen erstellen** | Aktiviert die Berechtigung, neu konfigurierte Suchen als öffentliche Suchen in XProtect Smart Client zu speichern. |
| **Öffentliche Suchen** | Aktiviert die Berechtigung, Einzelheiten zu oder die Konfiguration von |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **bearbeiten** | gespeicherten öffentlichen Suchen in XProtect Smart Client zu bearbeiten, z. B. den Namen, die Beschreibung, die Kameras und die Suchkategorien. |
| **Öffentliche Suchen löschen** | Aktiviert die Berechtigung, gespeicherte öffentliche Suchen zu löschen. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen in der Management Client für die Suche zu verwalten. |

### Alarme

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Management** | Aktiviert die Berechtigung, Alarme in der Smart Client zu verwalten. Zum Beispiel, das Ändern der Prioritäten von Alarmen, das erneute Zuweisen von Alarmen an andere Benutzer, die Bestätigung von Alarmen, die Änderung des Alarmstatus von mehreren Alarmen (zum Beispiel von **Neu** zu **Zugewiesen**). Zum Bearbeiten der Alarmeinstellungen benötigen Sie die Berechtigung **Alarmeinstellungen verwalten**.<br>Die Registerkarte **Alarme und Ereignisse** im Dialogfeld **Optionen** wird nur angezeigt, wenn Sie diese Berechtigung erteilen. |
| **Ansicht** | Ermöglicht die Berechtigung zum Aufrufen der Registerkarte **Alarm-Manager** in XProtect Smart Client und Abrufen von Alarmen und Alarmeinstellungen über die API. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| | Zum Aufrufen der Alarme in XProtect Smart Client müssen Sie die Berechtigung **Ansicht** für mindestens eine Alarmdefinition aktivieren. Sie rufen standardmäßig Alarme von Drittanbieter-Lösungen auf. |
| **Alarme deaktivieren** | Aktiviert die Berechtigung, Alarme zu deaktivieren. |
| **Benachrichtigungen empfangen** | Aktiviert die Berechtigung, Benachrichtigungen über Alarme in XProtect Mobile Clients und XProtect Web Client zu empfangen. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen für Alarme zu verwalten. |
| **Alarmeinstellungen verwalten** | Aktiviert die Berechtigung, Alarmdefinitionen, -zustände, -kategorien, -töne sowie die Alarm- und Ereignisspeicherung zu bearbeiten. Zum Bearbeiten der Alarmeinstellungen benötigen Sie die Berechtigung **Verwalten**. |

**Alarmdefinitionen**

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Ansicht** | Aktiviert die Berechtigung, Alarmdefinitionen, -zustände, -kategorien, -töne sowie die Alarm- und Ereignisspeicherung aufzurufen. |
| **Schreiben** | Aktiviert die Berechtigung **Ansicht**. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen für Alarmdefinitionen zu verwalten. |

**Server-Protokolle**

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Systemprotokolleinträge lesen** | Aktiviert die Berechtigung, Systemprotokolleinträge zu sehen. |
| **Auditprotokolleinträge lesen** | Aktiviert die Berechtigung, Auditprotokolleinträge zu sehen. |
| **Von Regeln ausgelöste Protokolleinträge lesen** | Aktiviert die Berechtigung, von Regeln ausgelöste Protokolleinträge zu sehen. |
| **Protokollkonfiguration lesen** | Aktiviert die Berechtigung, Protokolleinstellungen in **Extras** > **Optionen** > **Server Logs** zu lesen. |
| **Aktualisierung der Protokollkonfiguration** | Aktiviert die Berechtigung, Protokolleinstellungen in **Extras** > **Optionen** > **Server Logs** zu ändern. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen für Alarme zu verwalten. |

### Zutrittskontrolle

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Bearbeiten** | Aktiviert die Berechtigung, die Eigenschaften für die Zugangskontrollsysteme in der Management Client zu bearbeiten. |
| **Zutrittskontrolle verwenden** | Ermöglicht dem Benutzer, alle auf die Zutrittskontrolle bezogenen Funktionen in den Clients zu verwenden. |
| **Karteninhaberliste anzeigen** | Hiermit kann sich der Benutzer auf der Registerkarte **Zugangskontrolle** die Liste der Kartenbesitzer in den Clients anzeigen lassen. |
| **Benachrichtigungen empfangen** | Erlaubt es dem Benutzer Benachrichtigungen über Zutrittsanforderungen in den Clients zu erhalten. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung, Sicherheitsberechtigungen für alle Zugangskontrollsysteme zu verwalten. |

**Nummernschilderkennung (LPR)**

Wenn Ihr System mit XProtect LPR läuft, geben Sie dem Benutzer bitte die folgenden Berechtigungen:

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **LPR verwenden** | Erlaubt dem Benutzer die Verwendung aller Nummernschilderkennungsfunktionen in den Clients. |
| **Übereinstimmungslisten verwalten** | Erlaubt die Berechtigung im Management Client Übereinstimmungslisten hinzuzufügen, zu importieren, zu ändern, zu exportieren und zu löschen. |
| **Übereinstimmungslisten lesen** | Erlaubt die Einsichtnahme in die Übereinstimmungslisten. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung zur Verwaltung von Sicherheitsberechtigungen in Management Client zur Festlegung aller Transaktionen. |

**Transaktionsquellen**

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Ermöglicht die Berechtigung zum Anzeigen von Eigenschaften für die Transaktionsquellen in der Management Client. |
| **Bearbeiten** | Ermöglicht die Berechtigung zum Bearbeiten von Eigenschaften für die Transaktionsquellen in der Management Client. |
| **Löschen** | Ermöglicht die Berechtigung zum Löschen von Transaktionsquellen in der Management Client. |
| **Erstellen** | Ermöglicht die Berechtigung zum Erstellen neuer Transaktionsquellen in der Management Client. |
| **Sicherheit verwalten** | Ermöglicht die Berechtigung zur Verwaltung von Sicherheitsberechtigungen in Management Client für alle Transaktionsquellen. |

**Transaktionsdefinition**

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Vollständige Kontrolle** | Aktiviert die Berechtigung zur Verwaltung aller Sicherheitseinträge in diesem Teil des Systems. |
| **Lesen** | Ermöglicht die Berechtigung zum Anzeigen von Eigenschaften für die Transaktionsdefinitionen in der Management Client. |
| **Bearbeiten** | Ermöglicht die Berechtigung zum Bearbeiten von Eigenschaften für die Transaktionsdefinitionen in der Management Client. |
| **Löschen** | Ermöglicht die Berechtigung zum Löschen von Transaktionsdefinitionen in der Management Client. |
| **Erstellen** | Ermöglicht die Berechtigung zum Erstellen von Transaktionsdefinitionen in der Management Client. |
| **Sicherheit verwalten** | Aktiviert die Berechtigung zur Verwaltung von Sicherheitsberechtigungen in Management Client zur Festlegung aller Transaktionen. |

**MIP-Plug-ins**

Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins für Ihr System entwickeln, z. B. für die Integration in externe Zutrittskontrollsysteme oder ähnliche Funktionen.

Registerkarte „Geräte“ (Rollen)

Verfügbare Funktionalität hängt vom verwendeten System ab. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/product-index/).

Auf der Registerkarte **Geräte** können Sie bestimmen, welche Funktionen die Benutzer/Gruppen mit der ausgewählten Rolle für jedes Gerät (z. B. eine Kamera) oder jede Gerätegruppe im XProtect Smart Client verwenden können.

Denken Sie daran, die Einstellungen bei jedem Gerät zu wiederholen. Sie können auch eine Gerätegruppe auswählen und die Rollenberechtigungen für alle Geräte in der Gruppe in einem Schritt festlegen.

Sie können auch die Kontrollkästchen mit den Quadraten aktivieren oder deaktivieren. Beachten Sie jedoch, dass Ihre Auswahl dann für **alle** Geräte in der Gerätegruppe gilt. Alternativ können Sie auch die einzelnen Geräte in der Gerätegruppe auswählen, um zu prüfen, für welche Geräte genau die jeweilige Berechtigung gilt.

Auf Kameras bezogene Berechtigungen

Legen Sie die folgenden Berechtigungen für Kameraeräte fest:

| Name | Beschreibung |
|---|---|
| **Lesen** | Die ausgewählten Kameras sind in den Clients sichtbar. |
| **Live ansehen** | Ermöglicht es, Live-Videos von den ausgewählten Kameras in den Clients zu sehen.<br>Für XProtect Smart Client ist es erforderlich, dass der Rolle die Berechtigung gegeben wurde, sich die Registerkarte **Live** der Kunden anzeigen zu lassen. Diese Erlaubnis wird als Teil der Anwendungsgenehmigungen erteilt. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Eingeschränkte Live-Übertragung ansehen** | Ermöglicht die Live-Ansicht von eingeschränkten Videos der ausgewählten Kamera(s) in den Clients. |

| Name | Beschreibung |
|---|---|
| | Für XProtect Smart Client ist es erforderlich, dass der Rolle die Berechtigung gegeben wurde, sich die Registerkarte **Live** der Kunden anzeigen zu lassen. Diese Erlaubnis wird als Teil der Anwendungsgenehmigungen erteilt. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Wiedergabe > Innerhalb des Zeitprofils** | Ermöglicht es, aufgezeichnete Videos von den ausgewählten Kameras in den Clients wiederzugeben. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Wiedergabe > Wiedergabe beschränken auf** | Ermöglicht es, aufgezeichnete Videos von den ausgewählten Kameras in den Clients wiederzugeben. Bestimmen Sie eine Wiedergabebeschränkung oder wenden Sie keine Beschränkungen an. |
| **Eingeschränkte Aufnahmen wiedergeben** | Ermöglicht die Wiedergabe von aufgezeichneten, eingeschränkten Videos der ausgewählten Kamera(s) in den Clients. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Sequenzen lesen** | Ermöglicht es, die Sequenzinformationen, z. B. bezüglich des Sequenz Explorers, in den Clients zu lesen. |
| **intelligente Suche** | Ermöglicht es dem Benutzer, die Smart Search-Funktion in den Clients zu verwenden. |
| **Exportieren** | Ermöglicht es dem Benutzer, Aufzeichnungen von den Clients zu exportieren. |
| **Manuelle Aufzeichnung starten** | Ermöglicht es, eine manuelle Aufzeichnung der Videos von den ausgewählten Kameras in den Clients zu starten. |
| **Manuelle Aufzeichnung stoppen** | Ermöglicht es, eine manuelle Aufzeichnung der Videos von den ausgewählten Kameras in den Clients zu stoppen. |
| **Lesezeichen lesen** | Ermöglicht es, Lesezeichendetails in den Clients zu suchen und zu lesen. |

| Name | Beschreibung |
|---|---|
| **Lesezeichen bearbeiten** | Ermöglicht es, Lesezeichen in den Clients zu bearbeiten. |
| **Lesezeichen erstellen** | Ermöglicht es, Lesezeichen in den Clients hinzuzufügen. |
| **Lesezeichen löschen** | Ermöglicht es, Lesezeichen in den Clients zu löschen. |
| **AUX-Befehle** | Ermöglicht es Hilfsbefehle von den Clients zu verwenden. |
| **Beweissicherungen erstellen und erweitern** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Hinzufügen der Kameras zu neuen oder bestehenden Beweissicherungen<br>• Erweitern der Ablaufzeit für bestehende Beweissicherungen<br>• Erweitern des geschützten Intervalls für bestehende Beweissicherungen<br>Erfordert Benutzerberechtigungen für alle in der Beweissicherung enthaltenen Geräte. |
| **Beweissicherungen löschen und reduzieren** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Entfernen der Kamera aus bestehenden Beweissicherungen<br>• Löschen von bestehenden Beweissicherungen<br>• Verkürzen der Ablaufzeit für bestehende Beweissicherungen<br>• Verkürzen des geschützten Intervalls für bestehende Beweissicherungen<br>Erfordert Benutzerberechtigungen für alle in der Beweissicherung enthaltenen Geräte. |
| **Beweissicherungen lesen** | Ermöglicht es dem Client-Benutzer, nach Beweissicherungsdetails zu suchen und sie zu lesen. |
| **Live- und** | Gibt dem Client-Benutzer folgende Möglichkeiten: |

| Name | Beschreibung |
|---|---|
| **Wiedergabebeschränkungen erstellen und erweitern** | • Eine Live-Einschränkung für die Kamera erstellen<br>• Eine Wiedergabebeschränkung für die Kameraaufzeichnungen erstellen<br>• Hinzufügen einer neuen Kamera zu einer Live- oder Wiedergabebeschränkung<br>• Verlängern der Sperrfrist der Kameraaufzeichnungen<br>Erfordert Benutzerrechte für alle in der Einschränkung enthaltenen Geräte. |
| **Live- und Wiedergabebeschränkungen lesen** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Liste der bestehenden Live- und Wiedergabebeschränkungen für die Kamera anzeigen<br>• Filtern und Durchsuchen der Liste der Live- und Wiedergabebeschränkungen der Kamera |
| **Live- und Wiedergabebeschränkungen löschen und reduzieren** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Eine Live-Einschränkung für die Kamera aufheben<br>• Eine Wiedergabebeschränkung für die Kameraaufzeichnungen aufheben<br>• Reduzieren der Sperrfrist der Kameraaufzeichnungen<br>• Die Einstellungen für die Live- oder Wiedergabebeschränkung ändern<br>Erfordert Benutzerrechte für alle in der Einschränkung enthaltenen Geräte. |

Auf Mikrofone bezogene Berechtigungen

Legen Sie die folgenden Berechtigungen für Mikrofongeräte fest:

| Name | Beschreibung |
|---|---|
| **Lesen** | Die ausgewählten Mikrofone sind in den Clients sichtbar. |
| **Live abhören** | Ermöglicht es, Live-Audio von den ausgewählten Mikrofonen in den Clients zu hören.<br>Für XProtect Smart Client ist es erforderlich, dass der Rolle die Berechtigung gegeben wurde, sich die Registerkarte **Live** der Kunden anzeigen zu lassen. Diese Erlaubnis wird als Teil der Anwendungsgenehmigungen erteilt. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Eingeschränktes Live-Audio anhören** | Ermöglicht das Abhören von eingeschränkten Live-Videos von dem/den ausgewählten Mikrofon(en) der Clients.<br>Für XProtect Smart Client ist es erforderlich, dass der Rolle die Berechtigung gegeben wurde, sich die Registerkarte **Live** der Kunden anzeigen zu lassen. Diese Erlaubnis wird als Teil der Anwendungsgenehmigungen erteilt. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Wiedergabe > Innerhalb des Zeitprofils** | Ermöglicht es, aufgezeichnetes Audio von den ausgewählten Mikrofonen in den Clients wiederzugeben. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Wiedergabe > Wiedergabe beschränken auf** | Ermöglicht es, aufgezeichnetes Audio von den ausgewählten Mikrofonen in den Clients wiederzugeben. Bestimmen Sie eine Wiedergabebeschränkung oder wenden Sie keine Beschränkungen an. |
| **Eingeschränkte Aufnahmen wiedergeben** | Ermöglicht die Wiedergabe von aufgezeichneten eingeschränkten Audiodaten von dem/den ausgewählten Mikrofon(en) in den Clients. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Sequenzen lesen** | Ermöglicht es, die Sequenzinformationen, z. B. bezüglich des Sequenz Explorers, in den Clients zu lesen. |
| **Exportieren** | Ermöglicht es dem Benutzer, Aufzeichnungen von den Clients zu exportieren. |

| Name | Beschreibung |
|---|---|
| **Manuelle Aufzeichnung starten** | Ermöglicht es, eine manuelle Aufzeichnung vom Audio der ausgewählten Mikrofone in den Clients zu starten. |
| **Manuelle Aufzeichnung stoppen** | Ermöglicht es, eine manuelle Aufzeichnung vom Audio der ausgewählten Mikrofone in den Clients zu stoppen. |
| **Lesezeichen lesen** | Ermöglicht es, Lesezeichendetails in den Clients zu suchen und zu lesen. |
| **Lesezeichen bearbeiten** | Ermöglicht es, Lesezeichen in den Clients zu bearbeiten. |
| **Lesezeichen erstellen** | Ermöglicht es, Lesezeichen in den Clients hinzuzufügen. |
| **Lesezeichen löschen** | Ermöglicht es, Lesezeichen in den Clients zu löschen. |
| **Beweissicherungen erstellen und erweitern** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Hinzufügen des Mikrofons zu neuen oder bestehenden Beweissicherungen<br>• Erweitern der Ablaufzeit für bestehende Beweissicherungen<br>• Erweitern des geschützten Intervalls für bestehende Beweissicherungen<br>Erfordert Benutzerberechtigungen für alle in der Beweissicherung enthaltenen Geräte. |
| **Beweissicherungen löschen und reduzieren** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Entfernen des Mikrofons aus bestehenden Beweissicherungen<br>• Löschen von bestehenden Beweissicherungen<br>• Verkürzen der Ablaufzeit für bestehende Beweissicherungen<br>• Verkürzen des geschützten Intervalls für bestehende Beweissicherungen |

| Name | Beschreibung |
|---|---|
| | Erfordert Benutzerberechtigungen für alle in der Beweissicherung enthaltenen Geräte. |
| **Beweissicherungen lesen** | Ermöglicht es dem Client-Benutzer, nach Beweissicherungsdetails zu suchen und sie zu lesen. |
| **Live- und Wiedergabebeschränkungen erstellen und erweitern** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Eine Live-Einschränkung für das Mikrofon erstellen<br>• Eine Wiedergabebeschränkung für die Audioaufzeichnungen erstellen<br>• Hinzufügen eines neuen Mikrofons zu einer Live- oder Wiedergabebeschränkung<br>• Verlängern der Sperrfrist der Audioaufzeichnungen<br>Erfordert Benutzerrechte für alle in der Einschränkung enthaltenen Geräte. |
| **Live- und Wiedergabebeschränkungen lesen** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Eine Liste der bestehenden Live- und Wiedergabebeschränkungen für das Mikrofon anzeigen<br>• Filtern und Durchsuchen der Liste der Live- und Wiedergabebeschränkungen am Mikrofon |
| **Live- und Wiedergabebeschränkungen löschen und reduzieren** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Eine Live-Einschränkung für das Mikrofon aufheben<br>• Eine Wiedergabebeschränkung für die Audioaufzeichnungen aufheben<br>• Reduzieren der Sperrfrist der Audioaufzeichnungen<br>• Die Einstellungen für die Live- oder Wiedergabebeschränkung ändern |

| Name | Beschreibung |
|---|---|
| | Erfordert Benutzerrechte für alle in der Einschränkung enthaltenen Geräte. |

Auf Lautsprecher bezogene Berechtigungen

Legen Sie die folgenden Berechtigungen für Lautsprechergeräte fest:

| Name | Beschreibung |
|---|---|
| **Lesen** | Die ausgewählten Lautsprecher sind in den Clients sichtbar. |
| **Live abhören** | Ermöglicht es, Live-Audio von den ausgewählten Lautsprechern in den Clients zu hören.<br>Für XProtect Smart Client ist es erforderlich, dass der Rolle die Berechtigung gegeben wurde, sich die Registerkarte **Live** der Kunden anzeigen zu lassen. Diese Erlaubnis wird als Teil der Anwendungsgenehmigungen erteilt. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Eingeschränktes Live-Audio anhören** | Ermöglicht das Abhören von eingeschränkten Live-Videos von dem/den ausgewählten Lautsprecher(n) der Clients.<br>Für XProtect Smart Client ist es erforderlich, dass der Rolle die Berechtigung gegeben wurde, sich die Registerkarte **Live** der Kunden anzeigen zu lassen. Diese Erlaubnis wird als Teil der Anwendungsgenehmigungen erteilt. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Wiedergabe > Innerhalb des Zeitprofils** | Ermöglicht es, aufgezeichnetes Audio von den ausgewählten Lautsprechern in den Clients wiederzugeben. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Wiedergabe > Wiedergabe beschränken auf** | Ermöglicht es, aufgezeichnetes Audio von den ausgewählten Lautsprechern in den Clients wiederzugeben. Bestimmen Sie eine Wiedergabebeschränkung oder wenden Sie keine Beschränkungen |

| Name | Beschreibung |
|---|---|
| | an. |
| **Eingeschränkte Aufnahmen wiedergeben** | Ermöglicht es, aufgezeichnetes Audio von dem/den ausgewählten Lautsprecher(n) in den Clients wiederzugeben. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Sequenzen lesen** | Ermöglicht es, die Sequenzinformationen, z. B. bezüglich des Sequenz Explorers, in den Clients zu lesen. |
| **Exportieren** | Ermöglicht es dem Benutzer, Aufzeichnungen von den Clients zu exportieren. |
| **Manuelle Aufzeichnung starten** | Ermöglicht es, eine manuelle Aufzeichnung vom Audio der ausgewählten Lautsprecher in den Clients zu starten. |
| **Manuelle Aufzeichnung stoppen** | Ermöglicht es, eine manuelle Aufzeichnung vom Audio der ausgewählten Lautsprecher in den Clients zu stoppen. |
| **Lesezeichen lesen** | Ermöglicht es, Lesezeichendetails in den Clients zu suchen und zu lesen. |
| **Lesezeichen bearbeiten** | Ermöglicht es, Lesezeichen in den Clients zu bearbeiten. |
| **Lesezeichen erstellen** | Ermöglicht es, Lesezeichen in den Clients hinzuzufügen. |
| **Lesezeichen löschen** | Ermöglicht es, Lesezeichen in den Clients zu löschen. |
| **Beweissicherungen erstellen und erweitern** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Hinzufügen der Lautsprecher zu neuen oder bestehenden Beweissicherungen<br>• Erweitern der Ablaufzeit für bestehende Beweissicherungen<br>• Erweitern des geschützten Intervalls für bestehende Beweissicherungen |

| Name | Beschreibung |
|---|---|
| |  Erfordert Benutzerberechtigungen für alle in der Beweissicherung enthaltenen Geräte. |
| **Beweissicherungen löschen und reduzieren** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Entfernen der Lautsprecher aus bestehenden Beweissicherungen<br>• Löschen von bestehenden Beweissicherungen<br>• Verkürzen der Ablaufzeit für bestehende Beweissicherungen<br>• Verkürzen des geschützten Intervalls für bestehende Beweissicherungen<br>  Erfordert Benutzerberechtigungen für alle in der Beweissicherung enthaltenen Geräte. |
| **Beweissicherungen lesen** | Ermöglicht es dem Client-Benutzer, nach Beweissicherungsdetails zu suchen und sie zu lesen. |
| **Live- und Wiedergabebeschränkungen erstellen und erweitern** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Eine Live-Einschränkung für die Lautsprecher erstellen<br>• Eine Wiedergabebeschränkung für die Audioaufzeichnungen erstellen<br>• Hinzufügen eines neuen Mikrofons zu einer Live- oder Wiedergabebeschränkung<br>• Verlängern der Sperrfrist der Audioaufzeichnungen<br>  Erfordert Benutzerrechte für alle in der Einschränkung enthaltenen Geräte. |
| **Live- und Wiedergabebeschränkungen** | Gibt dem Client-Benutzer folgende Möglichkeiten: |

| Name | Beschreibung |
|---|---|
| **lesen** | • Liste der bestehenden Live- und Wiedergabebeschränkungen für die Lautsprecher anzeigen<br>• Filtern und Durchsuchen der Liste der Live- und Wiedergabebeschränkungen auf den Lautsprechern |
| **Live- und Wiedergabebeschränkungen löschen und reduzieren** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Eine Live-Einschränkung für die Lautsprecher aufheben<br>• Eine Wiedergabebeschränkung für die Audioaufzeichnungen aufheben<br>• Reduzieren der Sperrfrist der Audioaufzeichnungen<br>• Die Einstellungen für die Live- oder Wiedergabebeschränkung ändern<br>  Erfordert Benutzerrechte für alle in der Einschränkung enthaltenen Geräte. |

### Auf Metadaten bezogene Berechtigungen

Legen Sie die folgenden Berechtigungen für Metadatengeräte fest:

| Name | Beschreibung |
|---|---|
| **Lesen** | Aktiviert die Berechtigung, Metadatengeräte zu sehen und Daten davon in den Clients abzurufen. |
| **Bearbeiten** | Aktiviert die Berechtigung, die Eigenschaften von Metadaten zu bearbeiten. Damit können die Nutzer außerdem Metadatengeräte im Management Client und über das MIP SDK aktivieren oder deaktivieren. |
| **Live ansehen** | Aktiviert die Berechtigung, sich in den Clients Live-Metadaten von Kameras anzeigen zu lassen. |

| Name | Beschreibung |
|---|---|
| | Für XProtect Smart Client ist es erforderlich, dass der Rolle die Berechtigung gegeben wurde, sich die Registerkarte **Live** der Kunden anzeigen zu lassen. Diese Erlaubnis wird als Teil der Anwendungsgenehmigungen erteilt. |
| **Live-Einschränkung anzeigen** | Aktiviert die Berechtigung, eingeschränkte Live-Metadaten von Kameras in den Clients anzuzeigen.<br>Für XProtect Smart Client ist es erforderlich, dass der Rolle die Berechtigung gegeben wurde, sich die Registerkarte **Live** der Kunden anzeigen zu lassen. Diese Erlaubnis wird als Teil der Anwendungsgenehmigungen erteilt. |
| **Wiedergabe** | Aktiviert die Berechtigung, von Metadatengeräten aufgezeichnete Daten in den Clients wiederzugeben. |
| **Eingeschränkte Aufnahmen wiedergeben** | Ermöglicht die Wiedergabe von aufgezeichneten Daten von Geräten mit eingeschränkten Metadaten auf den Clients. |
| **Sequenzen lesen** | Aktiviert die Berechtigung, die Sequenzenfunktion beim Durchsuchen von aufgezeichneten Daten aus Metadatengeräten in den Clients zu verwenden. |
| **Exportieren** | Aktiviert die Berechtigung, Tonaufzeichnungen von Metadatengeräten in den Clients zu exportieren. |
| **Beweissicherungen erstellen und erweitern** | Aktiviert die Berechtigung, Beweissicherungen für Metadaten in den Clients zu erstellen und zu erweitern. |
| **Beweissicherungen lesen** | Aktiviert die Berechtigung, Beweissicherungen von Metadaten in den Clients einzusehen. |
| **Beweissicherungen löschen und reduzieren** | Aktiviert die Berechtigung, Beweissicherungen von Metadaten in den Clients zu löschen oder zu reduzieren. |
| **Manuelle Aufzeichnung starten** | Aktiviert die Berechtigung, die manuelle Aufzeichnung von Metadaten in den Clients zu starten. |

| Name | Beschreibung |
|---|---|
| **Manuelle Aufzeichnung stoppen** | Aktiviert die Berechtigung, die manuelle Aufzeichnung von Metadaten in den Clients abzubrechen. |
| **Live- und Wiedergabebeschränkungen erstellen und erweitern** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Erstellen einer Live-Einschränkung für das Metadatengerät<br>• Erstellen einer Wiedergabebeschränkung für das Metadatengerät<br>• Hinzufügen neuer Metadaten zu einer Live- oder Wiedergabebeschränkung<br>• Verlängern der Sperrfrist des Metadatengeräts<br>Erfordert Benutzerrechte für alle in der Einschränkung enthaltenen Geräte. |
| **Live- und Wiedergabebeschränkungen lesen** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Eine Liste der bestehenden Live- und Wiedergabebeschränkungen auf dem Metadatengerät anzeigen<br>• Filtern und Durchsuchen der Liste der Live- und Wiedergabebeschränkungen auf dem Metadatengerät |
| **Live- und Wiedergabebeschränkungen löschen und reduzieren** | Gibt dem Client-Benutzer folgende Möglichkeiten:<br>• Aufhebung einer Live-Beschränkung für das Metadatengerät<br>• Aufhebung einer Wiedergabebeschränkung auf dem Metadatengerät<br>• Verkürzung der Sperrfrist für das Metadatengerät<br>• Die Einstellungen für die Live- oder Wiedergabebeschränkung ändern<br>Erfordert Benutzerrechte für alle in der Einschränkung enthaltenen Geräte. |

### Auf Eingaben bezogene Berechtigungen

Legen Sie die folgenden Berechtigungen für Eingabegeräte fest:

| Name | Beschreibung |
|---|---|
| **Lesen** | Der/die ausgewählte/n Eingang/Eingänge ist/sind in den Clients sichtbar. |

### Auf Ausgaben bezogene Berechtigungen

Legen Sie die folgenden Berechtigungen für Ausgabegeräte fest:

| Name | Beschreibung |
|---|---|
| **Lesen** | Die ausgewählten Ausgänge sind in den Clients sichtbar. Wenn sichtbar, ist der Ausgang auf einer Liste in den Clients auswählbar. |
| **Aktivieren** | Die ausgewählten Ausgänge können vom Management Client und den Clients aktiviert werden. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |

## PTZ-Registerkarte (Rollen)

Berechtigungen für Schwenk-Neige-Zoom-Kameras (PTZ) legen Sie auf der Registerkarte **PTZ** fest. Sie bestimmen die Funktionen, die Benutzer/Gruppen in den Clients verwenden können. Auswählen können Sie einzelne PTZ-Kameras oder Gerätegruppen, die PTZ-Kameras enthalten.

Legen Sie die folgenden Berechtigungen für PTZ fest:

| Name | Beschreibung |
|---|---|
| **Manuelles PTZ** | Bestimmt, ob die ausgewählte Rolle PTZ-Funktionen verwenden und einen Wachrundgang an der ausgewählten Kamera anhalten kann.<br>Legen Sie ein Zeitprofil fest, wählen Sie **Immer** oder behalten Sie den Standardwert bei, der dem Standardzeitprofil folgt, das auf der Registerkarte **Info** für diese Rolle festgelegt wurde. |

| Name | Beschreibung |
|---|---|
| **PTZ-Voreinstellungen oder Wachrundgangprofile aktivieren** | Legt fest, ob die ausgewählte Rolle die ausgewählte Kamera zu Preset-Positionen bewegen, Wachrundgangprofile starten und stoppen sowie einen Wachrundgang anhalten kann.<br>Legen Sie ein Zeitprofil fest, wählen Sie **Immer** oder behalten Sie den Standardwert bei, der dem Standardzeitprofil folgt, das auf der Registerkarte **Info** für diese Rolle festgelegt wurde.<br>Damit diese Rolle andere PTZ-Funktionen auf der Kamera nutzen kann, aktivieren Sie die Berechtigung für **Manuelles PTZ**. |
| **PTZ-Priorität** | Legt die Priorität der PTZ-Kameras fest. Wenn mehrere Benutzer an einem Überwachungssystem dieselbe PTZ-Kamera zur selben Zeit steuern möchten, können Konflikte auftreten.<br>Sie können solche Situationen vermeiden, indem Sie eine Priorität für die Verwendung der ausgewählten PTZ-Kameras nach Benutzern/Gruppen mit der ausgewählten Rolle bestimmen. Bestimmen Sie eine Priorität zwischen 1 und 32.000, wobei 1 die niedrigste Priorität bedeutet. Die Standardpriorität liegt bei 3.000. Die Rolle mit dem höchsten Prioritätswert kann die PTZ-Kameras steuern. |
| **PTZ-Voreinstellungen oder Wachrundgangprofile verwalten** | Legt die Berechtigung zum Hinzufügen, Bearbeiten und Löschen von PTZ-Voreinstellungen und Überwachungsprofilen für die ausgewählte Kamera sowohl in der Management Client als auch in der XProtect Smart Client fest.<br>Damit diese Rolle andere PTZ-Funktionen auf der Kamera nutzen kann, aktivieren Sie die Berechtigung für **Manuelles PTZ**. |
| **PTZ-Voreinstellungen sperren/entsperren** | Bestimmt, ob die Rolle Preset-Positionen für die ausgewählte Kamera sperren und entsperren kann. |
| **PTZ-Sitzungen reservieren** | Bestimmt die Berechtigung, die ausgewählte Kamera in den reservierten PTZ-Sitzungsmodus zu versetzen.<br>In einer reservierten PTZ-Sitzung können andere Benutzer oder Wachrundgangsitzungen mit einer höheren PTZ-Priorität nicht die Kontrolle übernehmen.<br>Damit diese Rolle andere PTZ-Funktionen auf der Kamera nutzen kann, |

| Name | Beschreibung |
|---|---|
| | aktivieren Sie die Berechtigung für **Manuelles PTZ**. |
| **PTZ-Sitzungen freigeben** | Bestimmt, ob die ausgewählte Rolle die PTZ-Sitzungen von anderen Benutzern freigeben kann mit Management Client.<br>Sie können Ihre eigenen PTZ-Sitzungen jederzeit ohne diese Berechtigung freigeben. |

### Registerkarte „Sprache“ (Rollen)

Nur relevant, wenn Sie Lautsprecher auf Ihrem System verwenden. Legen Sie die folgenden Berechtigungen für Lautsprecher fest:

| Name | Beschreibung |
|---|---|
| **Sprechen** | Bestimmen Sie, ob Benutzer über die ausgewählten Lautsprecher sprechen dürfen. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei. |
| **Sprechpriorität** | Wenn mehrere Client-Benutzer über dieselben Lautsprecher zur selben Zeit sprechen möchten, können Konflikte auftreten.<br>Lösen Sie das Problem, indem Sie eine Priorität für die Nutzung der ausgewählten Lautsprecher durch Benutzer/Gruppen mit der ausgewählten Rolle festlegen. Legen Sie eine Priorität von **Sehr niedrig** bis **Sehr hoch** fest. Die Rolle mit der höchsten Priorität darf den Lautsprecher vor den anderen Rollen verwenden.<br>Wenn zwei Benutzer mit der gleichen Rolle zur selben Zeit sprechen möchten, gilt das Windhundprinzip. |

### Registerkarte „Fernaufzeichnungen“ (Rollen)

Legen Sie die folgenden Berechtigungen für Fernaufzeichnungen fest:

| Name | Beschreibung |
|---|---|
| **Fernaufzeichnungen abrufen** | Aktiviert die Berechtigung, Aufzeichnungen in den Clients von Kameras, Mikrofonen, Lautsprechern und Metadatengeräten an entfernten Standorten oder von Edge-Speichern an Kameras abzurufen. |

### Smart Wall Registerkarte (Rollen)

Mit Hilfe von Rollen können Sie Ihren Client-Benutzern entsprechende Benutzerberechtigungen für Smart Wall erteilen:

| Name | Beschreibung |
|---|---|
| **Lesen** | Gestattet Benutzern die Anzeige der ausgewählten Smart Wall in XProtect Smart Client. |
| **Bearbeiten** | Ermöglicht es Benutzern, die ausgewählte Smart Wall im Management Client zu bearbeiten. |
| **Löschen** | Ermöglicht es Benutzern, die ausgewählte Smart Wall im Management Client zu löschen. |
| **Bedienen** | Gestattet Benutzern die Anwendung von Layouts auf die ausgewählte Smart Wall in XProtect Smart Client und die Aktivierung von Voreinstellungen. |
| **Wiedergabe** | Gestattet Benutzern die Wiedergabe von aufgezeichneten Daten aus dem ausgewählten Smart Wall in XProtect Smart Client. |

### Registerkarte „Externes Ereignis“ (Rollen)

Geben Sie die folgenden Berechtigungen für externe Ereignisse an:

| Name | Beschreibung |
|---|---|
| **Lesen** | Ermöglicht es Benutzern nach dem ausgewählten externen Systemereignis in den Clients und im Management Client zu suchen und dieses anzusehen. |
| **Bearbeiten** | Ermöglicht es Nutzern, das ausgewählte externe Systemereignis im Management Client zu bearbeiten. |
| **Löschen** | Ermöglicht es Nutzern, das ausgewählte externe Systemereignis im Management Client zu löschen. |
| **Auslöser** | Ermöglicht es Nutzern, das ausgewählte externe Systemereignis in den Clients auszulösen. |

### Registerkarte „Ansichtsgruppe“ (Rollen)

Auf der Registerkarte **Ansichtsgruppe** bestimmen Sie, welche Ansichtsgruppen die Benutzer und Benutzergruppen mit der ausgewählten Rolle in den Clients verwenden können.

Geben Sie die folgenden Berechtigungen für Ansichtsgruppen an:

| Name | Beschreibung |
|---|---|
| **Lesen** | Aktiviert die Berechtigung, sich in den Clients und im Management Client Ansichtsgruppen anzeigen zu lassen. Ansichtsgruppen werden im Management Client erstellt. |
| **Bearbeiten** | Aktiviert die Berechtigung, an Ansichtsgruppen in der Management Client Eigenschaften zu bearbeiten. |
| **Löschen** | Aktiviert die Berechtigung, Ansichtsgruppen in der Management Client zu löschen. |
| **Bedienen** | Aktiviert die Berechtigung, in XProtect Smart Client Ansichtsgruppen in zu verwenden, d. h. Untergruppen und Ansichten zu erstellen und zu löschen. |

### Registerkarte „Server“ (Rollen)

Die Angabe von Rollenberechtigungen auf der Registerkarte **Server** ist nur relevant, wenn Ihr System in einem Milestone Federated Architecture Setup arbeitet.

| Name | Beschreibung |
|---|---|
| **Sites** | Aktiviert die Berechtigung, die ausgewählte Seite in der Management Client zu sehen. Verbundene Standorte sind über die Milestone Federated Architecture verbunden.<br><br>Zur Bearbeitung von Eigenschaften benötigen Sie auf dem Management-Server Bearbeitungsberechtigungen für jeden Standort. |

Weitere Informationen dazu finden Sie unter Konfigurieren von Milestone Federated Architecture auf Seite 98.

### Matrix Registerkarte (Rollen)

Wenn Sie in Ihrem System Matrix-Empfänger konfiguriert haben, können Sie ggf. Matrix Rollenberechtigungen konfigurieren. Von einem Client können Sie Videos an ausgewählte Matrix-Empfänger senden. Wählen Sie die Benutzer, die diese empfangen können, auf der Registerkarte Matrix.

Die folgenden Berechtigungen stehen zur Verfügung:

| Name | Beschreibung |
|---|---|
| **Lesen** | Bestimmen Sie, ob Benutzer und Gruppen mit der ausgewählten Rolle Videos auswählen und an die Matrix-Empfänger der Clients senden können. |

### Registerkarte „Alarme“ (Rollen)

Wenn Sie in Ihrer Systemeinrichtung Alarme verwenden, um einen zentralen Überblick und Kontrolle über Ihre Installation (ggf. einschließlich anderer XProtect Server) zu ermöglichen, können Sie auf der Registerkarte **Alarme** die Alarmberechtigungen für Benutzer und Gruppen mit der ausgewählten Rolle festlegen, die sie haben sollen, z. B. wie Alarme in den Clients behandelt werden sollen.

Unter **Alarme** legen Sie die Berechtigungen für Alarme fest:

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Management** | Aktiviert die Berechtigung, Alarme in der Smart Client zu verwalten. Zum Beispiel, das Ändern der Prioritäten von Alarmen, das erneute Zuweisen von Alarmen an andere Benutzer, die Bestätigung von Alarmen, die Änderung des Alarmstatus von mehreren Alarmen (zum Beispiel von **Neu** zu **Zugewiesen**). Zum Bearbeiten der Alarmeinstellungen benötigen Sie die Berechtigung **Alarmeinstellungen verwalten**.<br><br>Die Registerkarte **Alarme und Ereignisse** im Dialogfeld **Optionen** wird nur angezeigt, wenn Sie diese Berechtigung erteilen. |
| **Ansicht** | Ermöglicht die Berechtigung zum Aufrufen der Registerkarte **Alarm-Manager** in XProtect Smart Client und Abrufen von Alarmen und Alarmeinstellungen über die API.<br><br>Zum Aufrufen der Alarme in XProtect Smart Client müssen Sie die Berechtigung **Ansicht** für mindestens eine Alarmdefinition aktivieren. Sie rufen standardmäßig Alarme von Drittanbieter-Lösungen auf. |
| **Alarme deaktivieren** | Aktiviert die Berechtigung, Alarme zu deaktivieren. |

| Sicherheitserlaubnis | Beschreibung |
|---|---|
| **Benachrichtigungen empfangen** | Aktiviert die Berechtigung, Benachrichtigungen über Alarme in XProtect Mobile Clients und XProtect Web Client zu empfangen. |
| **Alarmeinstellungen verwalten** | Aktiviert die Berechtigung, Alarmdefinitionen, -zustände, -kategorien, -töne sowie die Alarm- und Ereignisspeicherung zu bearbeiten. Zum Bearbeiten der Alarmeinstellungen benötigen Sie die Berechtigung **Verwalten**. |

Unter **Alarmdefinitionen** legen Sie die Berechtigungen für eine spezifische Alarmdefinition fest:

| Name | Beschreibung |
|---|---|
| **Ansicht** | Aktiviert die Berechtigung, Alarmdefinitionen, -zustände, -kategorien, -töne sowie die Alarm- und Ereignisspeicherung aufzurufen. |
| **Schreiben** | Aktiviert die Berechtigung **Ansicht**. |

### Registerkarte „Zutrittskontrolle“ (Rollen)

Wenn Sie Basisnutzer, Windows-Benutzer oder -Gruppen hinzufügen oder bearbeiten, können Sie Zutrittskontrolleinstellungen bestimmen:

| Name | Beschreibung |
|---|---|
| **Zutrittskontrolle verwenden** | Ermöglicht dem Benutzer, alle auf die Zutrittskontrolle bezogenen Funktionen in den Clients zu verwenden. |
| **Karteninhaberliste anzeigen** | Hiermit kann sich der Benutzer auf der Registerkarte **Zugangskontrolle** die Liste der Kartenbesitzer in den Clients anzeigen lassen. |
| **Benachrichtigungen empfangen** | Erlaubt es dem Benutzer Benachrichtigungen über Zutrittsanforderungen in den Clients zu erhalten. |

### Registerkarte „LPR“ (Rollen)

Wenn Ihr System mit XProtect LPR läuft, geben Sie für die Benutzer die folgenden Berechtigungen an:

| Name | Beschreibung |
|---|---|
| **LPR verwenden** | Aktiviert die Berechtigung, in den Clients beliebige Nummernschilderkennungsfunktionen zu nutzen. |
| **Übereinstimmungslisten verwalten** | Erlaubt die Berechtigung im Management Client Übereinstimmungslisten hinzuzufügen, zu importieren, zu ändern, zu exportieren und zu löschen. |
| **Übereinstimmungslisten lesen** | Erlaubt die Berechtigung zur Einsichtnahme in Übereinstimmungslisten. |

### Registerkarte Vorfälle (Rollen)

Falls Sie XProtect Incident Manager haben, können Sie die folgenden Berechtigungen für Ihre Rollen angeben.

Um einer Management Client-Administratorrolle die Berechtigung zu erteilen, Vorfalleigenschaften zu verwalten oder anzuzeigen, wählen Sie den Knoten **Vorfalleigenschaften** aus.

Um einem Anwender von XProtect Smart Client die Berechtigung zu erteilen, Ihre definierten Vorfalleigenschaften einzusehen, wählen Sie **Vorfalleigenschaften** und erteilen Sie die Berechtigung **Ansicht**. Um einem Anwender allgemeine Berechtigungen zu erteilen, **Vorfallprojekte** zu verwalten oder einzusehen, wählen Sie den Knoten Vorfallprojekt aus. Erweitern Sie den Knoten **Vorfallprojekt** und wählen Sie einen oder mehrere Unterknoten aus, um Berechtigungen für diese zusätzlichen Funktionen oder Fähigkeiten zu erteilen.

| Name | Beschreibung |
|---|---|
| **Management** | Berechtigung zum Verwalten (Anzeigen, Erstellen, Bearbeiten und Löschen) von Einstellungen und Eigenschaften im Zusammenhang mit einer Funktion oder zur Anzeige eines Benutzeroberflächenelements, das vom ausgewählten Knoten entweder in Management Client oder XProtect Smart Client dargestellt wird. |
| **Ansicht** | Berechtigung zum Anzeigen (aber nicht zum Erstellen, Bearbeiten und Löschen) der Einstellungen und Eigenschaften im Zusammenhang mit einer Funktion oder zur Anzeige eines Benutzeroberflächenelements, das vom ausgewählten Knoten entweder in Management Client oder XProtect Smart Client dargestellt wird. |

### MIP Registerkarte (Rollen)

Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins für Ihr System entwickeln, z. B. für die Integration in externe Zutrittskontrollsysteme oder ähnliche Funktionen. Plug-ins von Drittanbietern haben ihre eigenen Einstellungen auf den einzelnen Registerkarten.

Die Einstellungen, die Sie ändern, hängen vom tatsächlichen Plug-in ab. Auf der Registerkarte **MIP** finden Sie die benutzerdefinierten Einstellungen für die Plug-ins.

## Basisnutzer (Sicherheitsknoten)

In Milestone XProtect VMSgibt es zwei Arten von Benutzerkonten:  Basisnutzer und Windows Nutzer.

Basisnutzer sind Benutzerkonten, die Sie in Milestone XProtect VMS erstellen. Es handelt sich um ein dediziertes Systembenutzerkonto mit einem grundlegenden Benutzernamen und einem Passwort für die Authentifizierung des einzelnen Nutzers.

Windows Nutzer sind Benutzerkonten, die Sie über Microsofts Active Directoryhinzufügen.

Es gibt einige Unterschiede zwischen Basisnutzern und Windows Nutzern:

- Basisnutzer authentifizieren sich durch einen Benutzernamen und ein Passwort und bestehen speziell für ein System/Standort. Beachten Sie, dass selbst wenn ein Basisnutzer, der an einem föderalen Standort erstellt wurde, denselben Namen und dasselbe Passwort hat wie ein Basisnutzer an einem anderen föderalen Standort, der Basisnutzer nur Zugang zu dem Standort hat, an dem er erstellt wurde.
- Windows Nutzer authentifizieren sich auf Basis ihrer Windows Anmeldung und sind auf einen bestimmten Computer beschränkt.

# System-Dashboard-Knoten

## System-Dashboard-Knoten

Unter dem Knoten **System Dashboard** finden Sie verschiedene Funktionen zur Überwachung Ihres Systems und seiner verschiedenen Systemkomponenten.

| Name | Beschreibung |
|---|---|
| **Aktuelle Aufgabe** | Erhalten Sie eine Übersicht über alle laufenden Aufgaben auf einem ausgewählten Aufzeichnungsserver. |
| **Systemmonitor** | Überwachen Sie den Status Ihrer Server und Kameras mittels der von Ihnen festgelegten Parameter. |

| Name | Beschreibung |
|---|---|
| **Schwellenwerte des Systemmonitors** | Stellen Sie Schwellenwerte für überwachte Parameter auf dem Server ein und überwachen Sie Kacheln, die im Systemmonitor verwendet werden. |
| **Beweissicherung** | Erhalten Sie eine Übersicht über alle geschützten Daten im System. |
| **Konfigurationsberichte** | Drucken Sie einen Bericht mit Ihrer Systemkonfiguration aus. Sie können entscheiden, was in den Bericht aufgenommen wird. |

## Aktuelle Aufgaben (System-Dashboardknoten)

Das Fenster **Aktuelle Aufgaben** zeigt eine Übersicht über laufende Aufgaben für den ausgewählten Aufzeichnungsserver. Wenn Sie eine Aufgabe ausgelöst haben, die über längere Zeit im Hintergrund läuft, können Sie das Fenster **Aktuelle Aufgaben** öffnen, um zu sehen, welche Fortschritte die Aufgabe macht. Beispiele für langwierige Aufgaben, die vom Benutzer ausgelöst werden können, sind Firmware-Updates und das Verschieben von Hardware. Dort finden Sie Informationen zur Anfangszeit, zur geschätzten Endzeit und zum Fortschritt der Aufgabe.

Die Angaben in dem Fenster **Aktuelle Aufgaben** werden nicht dynamisch aktualisiert, sondern zeigen eine Momentaufnahme der aktuellen Aufgaben in dem Augenblick, wo Sie das Fenster öffnen. Wenn Sie das Fenster schon länger geöffnet haben, aktualisieren Sie die Informationen, indem Sie auf die Schaltfläche **Aktualisieren** in der unteren rechten Ecke des Fensters klicken.

## System-Monitor (der Knoten "System Dashboard")

Die Funktion **System-Monitor** gibt Ihnen einen schnellen, visuellen Überblick über den aktuellen Zustand der Server und Kameras in Ihrem System.

### Das Fenster Systemmonitor-Dashboard

#### Kacheln

Der obere Teil des Fensters **System-Monitor-Dashboard** zeigt farbige Kacheln, die den Zustand der Serverhardware und der Kamerahardware Ihres Systems darstellen.

Die Kacheln ändern ihren Zustand und damit ihre Farbe je nach den im Knoten **System-Monitor-Schwellenwerte** eingestellten Schwellenwerten. Weitere Informationen finden Sie unter System-Monitor-Schwellenwerte (der Knoten "System Dashboard") auf Seite 614. Die Schwellenwerte werden so festgelegt, dass die Farben der Kacheln folgende Bedeutung haben:

| Kachelfarbe | Beschreibung |
|---|---|
| **Grün** | **Normaler** Status. Alles läuft normal. |
| **Gelb** | **Warnstatus**. Mindestens ein üÜberwachungsparameter liegt über dem Schwellenwert für den Zustand **Normal**. |
| **Rot** | **Kritischer** Status. Mindestens ein überwachter Parameter liegt über dem Schwellenwert für den **normalen** Status und dem **Warnstatus**. |

Hardwareliste mit Überwachungsparametern

Wenn Sie auf eine Kachel klicken, können Sie den Zustand jedes ausgewählten Überwachungparameters für jede Hardware sehen, die durch eine Kachel im unteren Teil des Fensters **System-Monitor-Dashboard** dargestellt wird.


*Beispiel: Die LIVE-FPS-Überwachungsparameter einer Kamera haben den Zustand "Warnung" erreicht.*

### Dashboard-Fenster anpassen

Wählen Sie in der oberen rechten Ecke des Fensters **Anpassen**, um das Fenster **Dashboard anpassen** zu öffnen.

Im Fenster **Dashboard anpassen** können Sie auswählen, welche Kachel Sie erstellen, bearbeiten oder löschen wollen. Beim Erstellen oder Bearbeiten von Kacheln können Sie auswählen, welche Hardware und welche Überwachungsparameter Sie auf der Kachel überwachen wollen.

### Das Fenster "Details"

Wenn Sie eine Kachel auswählen und dann aus der Hardwareliste mit Überwachungsparametern die Schaltfläche **Details** rechts von einer Kamera oder einem Server auswählen, können Sie sich - je nach der ausgewählten Hardware - Systeminformationen anzeigen lassen und Berichte erstellen über:

| Hardware | Informationen |
|---|---|
| **Managementserver** | Zeigt Daten zu:<br>• CPU-Auslastung<br>• Verfügbare Rechenkapazität |

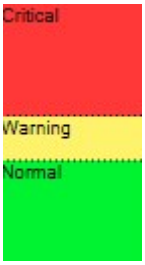
| Hardware | Informationen |
|---|---|
| | Wählen Sie **Verlauf** aus, um den Verlauf der Zustände Ihrer Hardware zu sehen und einen Bericht zu den o.g. Daten zu erstellen. |
| **Aufzeichnungsserver** | Zeigt Daten zu:<br>• CPU-Auslastung<br>• Verfügbare Rechenkapazität<br>• Datenträger<br>• Speicher<br>• Netzwerk<br>• Kameras<br>Wählen Sie **Verlauf** aus, um den Verlauf der Zustände Ihrer Hardware zu sehen und einen Bericht zu den o.g. Daten zu erstellen. |
| **Failover-Aufzeichnungsserver** | Zeigt Daten zu:<br>• CPU-Auslastung<br>• Verfügbare Rechenkapazität<br>• Überwachte Aufzeichnungsserver<br>Wählen Sie **Verlauf** aus, um den Verlauf der Zustände Ihrer Hardware zu sehen und einen Bericht zu den o.g. Daten zu erstellen. |
| **Log-Server, Ereignisserver usw.** | Zeigt Daten zu<br>• CPU-Auslastung<br>• Verfügbare Rechenkapazität<br>Wählen Sie **Verlauf** aus, um den Verlauf der Zustände Ihrer Hardware zu sehen und einen Bericht zu den o.g. Daten zu erstellen. |
| **Kameras** | Zeigt Daten zu: |

| Hardware | Informationen |
|---|---|
| | • Speicher<br>• Belegter Speicherplatz<br>• Live-FPS (Standard)<br>• Aufzeichnungs-FPS<br>• Live-Videoformat<br>• Aufzeichnungs-Videoformat<br>• Mediendaten empfangen (Kbit/s)<br>• Verfügbare Rechenkapazität<br>Wählen Sie den Namen der Kamera aus, um deren Zustandsverlauf zu sehen und einen Bericht zu erstellen zu:<br>• Von Kamera empfangene Daten<br>• Auslastung des Kameradatenträgers |

Wenn Sie auf die Details des Systemmonitors von einem Server-Betriebssystem aus zugreifen, könnten Sie eine Meldung bezüglich **Internet Explorer erweiterte Sicherheitskonfiguration** bekommen. Folgen Sie den Anweisungen, um die Seite **System Monitor** zu den **Vertrauenswürdigen Seiten der Zone** hinzuzufügen, bevor Sie fortfahren.

## System-Monitor-Schwellenwerte (der Knoten "System Dashboard")

Mit den Schwellenwerten für den Systemmonitor können Sie die Schwellenwerte festlegen und anpassen, wann Kacheln auf dem **System Monitor Dashboard** visuell anzeigen sollen, dass Ihre Systemhardware ihren Zustand ändert. Zdie CPU Auslastung eines Servers zum Beispiel von normal (grün) in den Verhandlungszustand (gelb) oder von einem Planungszustand (gelb) in einem kritischen Zustand (rot).




*Beispielschwellenwerte zwischen den drei Zuständen*

Sie können die Schwellenwerte für Server, Kameras, Festplatten und Speicher ändern, und alle Schwellenwerte haben einige Schaltflächen und Einstellungen gemeinsam.

**Gemeinsame Elemente der Benutzeroberfläche**

| Schaltflächen und Einstellungen | Beschreibung | Einheit |
|---|---|---|
| **Berechnungsintervall** | Die Verbindung zu Ihren verschiedenen Hardwaregeräten fällt oft kurzzeitig aus. Wenn Sie ein Berechnungsintervall von 0 Sekunden vorgeben, lösen alle diese kurzzeitigen Ausfälle Alarm wegen Änderungen des Hardwarezustands aus. Daher sollten Sie ein Berechnungsintervall vorgeben, das eine gewisse Länge hat.<br><br>Wenn Sie ein Berechnungsintervall von einer (1) Minute angeben, so erhalten Sie nur dann einen Alarm, wenn der Durchschnittswert für die gesamte Minute über dem Schwellenwert liegt. Bei korrekt eingestelltem Berechnungsintervall erhalten Sie keinen falsch positiven Alarm, sondern nur solche wegen länger anhaltender Probleme z.B. mit der CPU-Auslastung oder Speichernutzung.<br><br>Informationen dazu, wie Sie die Zahlenwerte der Berechnungsintervalle ändern können, finden Sie unter Schwellenwerte dafür bearbeiten, wann sich Hardwarezustände ändern sollen auf Seite 320. | Sek. |
| **Erweitert** | Wenn Sie die Schaltfläche **Erweitert** auswählen, können Sie die Schwellenwerte und Berechnungsintervalle für einzelne Server, Kameras, Festplatten und Speichergeräte festlegen. Weitere Informationen finden Sie weiter unten. | - |
| **Regel erstellen** | Sie können Ereignisse aus dem **System-Monitor** und Regeln zum Auslösen von Maßnahmen kombinieren, z.B. wenn die CPU-Auslastung eines Servers kritisch ist oder eine Festplatte nicht mehr genügend Speicherplatz hat.<br><br>Weitere Informationen finden Sie unter Regeln und Ereignisse (Erklärung) auf Seite 82 und Regeln hinzufügen auf Seite 293. | - |

**Serverschwellenwerte**

| Schwellenwert | Beschreibung | Einheit |
|---|---|---|
| **CPU-Auslastung** | Schwellenwerte für die CPU-Nutzung auf den von Ihnen überwachten Servern. | % |
| **Verfügbare Rechenkapazität** | Schwellenwerte für das auf den von Ihnen überwachten Servern genutzte RAM. | MB |
| **NVIDIA-Dekodierung** | Schwellenwerte für die Nutzung der NVIDIA-Dekodierung auf den von Ihnen überwachten Servern. | % |
| **NVIDIA-Speicher** | Schwellenwerte für das auf den von Ihnen überwachten Servern genutzte NVIDIA-RAM. | % |
| **NVIDIA-Rendering** | Schwellenwerte für die Nutzung des NVIDIA-Renderings auf den von Ihnen überwachten Servern. | % |

**Kameraschwellenwerte**

| Schwellenwert | Beschreibung | Einheit |
|---|---|---|
| **Live-FPS** | Schwellenwerte für die FPS der bei der Anzeige von Live-Video auf den von Ihnen überwachten Kameras verwendeten Kameras. | % |
| **Aufzeichnungs-FPS** | Schwellenwerte für die FPS der Videoaufzeichnungen auf den von Ihnen überwachten Kameras verwendeten Kameras. | % |
| **Verwendeter Speicherplatz** | Schwellenwerte für den von den von Ihnen überwachten Kameras verwendeten Speicherplatz. | GB |

**Schwellenwerte für Festplatten**

| Schwellenwert | Beschreibung | Einheit |
|---|---|---|
| **Freier Speicherplatz** | Schwellenwerte für den verfügbaren Speicherplatz auf den von Ihnen überwachten Festplatten. | GB |

**Schwellenwerte für Speicher**

| Schwellenwert | Beschreibung | Einheit |
|---|---|---|
| **Speicherzeit** | Schwellenwert, der eine Prognose dafür anzeigt, wann in Ihrem Speicher kein Platz mehr vorhanden sein wird. Der angezeigte Betriebszustand basiert auf Ihrer Systemeinrichtung und wird zweimal täglich aktualisiert. | Tage |

## Beweismittelsicherung (System-Dashboard-Knoten)

**Beweismittelsicherung** unter dem Knoten **System Dashboard** zeigt eine Übersicht über alle geschützten Daten im aktuellen Überwachungssystem.

Für alle Beweismittelsicherungen stehen die folgenden Metadaten zur Verfügung:

- Beginn und Enddatum der geschützten Daten
- Der Benutzer, der die Beweise gesichert hat
- Wenn Beweise nicht länger gesichert sind
- Wo die Daten gespeichert sind
- Die Größer jeder Beweissicherung

Alle im Fenster **Beweismittelsicherung** gezeigten Informationen stellen Momentaufnahmen dar. Drücken Sie F5, um zu aktualisieren.

## Konfigurationsberichte (System-Dashboardknoten)

Beim Installieren und Konfigurieren Ihres VMS-Systems treffen Sie zahlreiche Auswahlen, die Sie ggf. dokumentieren wollen. Im Lauf der Zeit ist es auch schwer, sich an alle Einstellungen zu erinnern, die Sie seit der Installation und Erstkonfiguration geändert haben - oder auch nur in den letzten zwei Monaten. Darum können Sie einen Bericht mit allen Ihren Konfigurationsseinstellungen ausdrucken.

Die folgenden Einstellungen stehen zur Verfügung, wenn Sie Konfigurationsberichte erstellen und ausdrucken:

| Name | Beschreibung |
|---|---|
| **Berichte** | Eine Liste mit Elementen, die in einen Konfigurationsbericht aufgenommen werden kann. |
| **Alle auswählen** | Fügt alle Elemente auf der Liste der **Berichte** zum Konfigurationsbericht hinzu. |
| **Alle abwählen** | Entfernt alle Elemente auf der Liste der **Berichte** aus dem Konfigurationsbericht. |
| **Front Page** | Passen Sie die Front Page des Berichts an. |
| **Formatierung** | Formatieren Sie den Bericht. |
| **Sensible Daten auslassen** | Entfernt personenbezogene Daten, wie Benutzernamen, E-Mail-Adressen und sensible Daten sonstiger Art aus dem Konfigurationsbericht und macht diesen somit DSGVO-konform.<br>Informationen zum Lizenzeigentümer werden stets vom Bericht ausgeschlossen. |
| **Exportieren** | Wählen Sie einen Speicherort für den Bericht aus und erstellen Sie ihn als PDF-Datei. |

# Der Knoten "Serverprotokolle"

## Der Knoten "Serverprotokolle"

### Systemprotokolle (Registerkarte)

Jede Zeile in einem Protokoll stellt einen Protokolleintrag dar. Jeder Protokolleintrag enthält einige Informationsfelder:

| Name | Beschreibung |
|---|---|
| **Protokollstufe** | Info, Warnung oder Fehler. |

| Name | Beschreibung |
|---|---|
| **Lokalzeit** | Zeitstempel in der Ortszeit des Servers Ihres Systems. |
| **Nachrichtentext** | Die Identifikationsnummer für den protokollierten Vorfall. |
| **Kategorie** | Der Typ des protokollierten Vorfalls. |
| **Quelltyp** | Der Gerätetyp, auf dem sich der protokollierte Vorfall ereignet hat, beispielsweise ein Server oder Gerät. |
| **Quellname** | Name des Ausrüstungsgegenstands, auf dem sich der protokollierte Vorfall ereignet hat. |
| **Ereignistyp** | Der Ereignistyp, den der protokollierte Vorfall repräsentiert. |

### Auditprotokolle (Registerkarte)

Jede Zeile in einem Protokoll stellt einen Protokolleintrag dar. Jeder Protokolleintrag enthält einige Informationsfelder:

| Name | Beschreibung |
|---|---|
| **Lokalzeit** | Zeitstempel in der Ortszeit des Servers Ihres Systems. |
| **Nachrichtentext** | Zeigt eine Beschreibung des protokollierten Vorfalls an. |
| **Berechtigung** | Die Informationen darüber, ob die Remote Nutzeraktion erlaubt (genehmigt) war oder nicht. |
| **Kategorie** | Der Typ des protokollierten Vorfalls. |
| **Quelltyp** | Der Gerätetyp, auf dem sich der protokollierte Vorfall ereignet hat, beispielsweise ein Server oder Gerät. |
| **Quellname** | Name des Ausrüstungsgegenstands, auf dem sich der protokollierte Vorfall ereignet hat. |

| Name | Beschreibung |
|---|---|
| **Benutzer** | Der Benutzername des Remote Nutzers, der den protokollierten Vorfall verursacht hat. |
| **Benutzerstandort** | Die IP-Adresse oder der Hostname des Computers, mit dem der Remote Nutzer den protokollierten Vorfall verursacht hat. |

### Durch Regel ausgelöste Protokolle (Registerkarte)

Jede Zeile in einem Protokoll stellt einen Protokolleintrag dar. Jeder Protokolleintrag enthält einige Informationsfelder:

| Name | Beschreibung |
|---|---|
| **Lokalzeit** | Zeitstempel in der Ortszeit des Servers Ihres Systems. |
| **Nachrichtentext** | Zeigt eine Beschreibung des protokollierten Vorfalls an. |
| **Kategorie** | Der Typ des protokollierten Vorfalls. |
| **Quelltyp** | Der Gerätetyp, auf dem sich der protokollierte Vorfall ereignet hat, beispielsweise ein Server oder Gerät. |
| **Quellname** | Name des Ausrüstungsgegenstands, auf dem sich der protokollierte Vorfall ereignet hat. |
| **Ereignistyp** | Der Ereignistyp, den der protokollierte Vorfall repräsentiert. |
| **Regelname** | Name der Regel, die den Protokolleintrag ausgelöst hat. |
| **Dienstname** | Name des Dienstes, auf dem sich der protokollierte Vorfall ereignet hat. |

# Metadaten-Knoten

## Metadaten und Metadatensuche

Um Metadaten-Geräte zu verwalten und zu konfigurieren siehe Suchkategorien und Suchfilter für Metadaten anzeigen auf Seite 322.

### Was sind Metadaten?

Metadaten sind Daten zu Daten, z. B. Daten, die das Videobild, den Inhalt, Objekte im Bild oder den Ort beschreiben, an dem das Bild aufgezeichnet wurde.

Metadaten können erzeugt werden von:

- Das Gerät, das selbst die Daten liefert, z. B. eine Kamera, die Videoaufzeichnungen liefert
- Einem Drittsystem oder Integration über einen generischen Metadatentreiber

### Metadatensuche

Eine Metadatensuche ist jede Suche nach Videoaufzeichnungen in XProtect Smart Client, bei der Suchkategorien und Suchfilter verwendet werden, die sich auf Metadaten beziehen.

Die Standardsuchkategorien für Milestone Metadaten sind:

- Speicherort:Die Benutzer können Geokoordinaten und einen Suchradius von diesen Koordinaten aus festlegen.
- Personen: Die Benutzer können nach Geschlecht, ungefährer Größe und Alter suchen und sich die Ergebnisse mit Gesichtern anzeigen lassen.
- Fahrzeuge:Benutzer können nach Fahrzeugfarbe, Geschwindigkeit und Typ sowie nach einem bestimmten Nummernschild suchen.

### Suchanforderungen für Metadaten

Um Suchergebnisse zu erhalten, müssen Sie einen der folgenden Schritte ausführen:

- Mindestens ein Gerät in Ihrem Videoüberwachungssystem, das Videoaufzeichnungen analysieren kann und das korrekt konfiguriert ist
- Ein Videoverarbeitungsdienst in Ihrem Videoüberwachungssystem, der Metadaten erzeugt

In beiden Fällen müssen die Metadaten das erforderliche Metadatenformat haben.

Weitere Informationen finden Sie in der -Dokumentation zur Integration der Metadatensuche.

# Zugangskontrollknoten

## Zutrittskontrolleigenschaften

### Registerkarte „Allgemeine Einstellungen“ (Zutrittskontrolle)

| Name | Beschreibung |
|---|---|
| **Aktivieren** | Systeme sind standardmäßig aktiviert, d. h. sie sind in XProtect Smart Client für Benutzer mit ausreichenden Berechtigungen sichtbar und das XProtect System empfängt Ereignisse aus der Zutrittskontrolle.<br>Sie können ein System beispielsweise während der Wartung deaktivieren, um unnötige Alarme zu vermeiden. |
| **Name** | Der Name der Zutrittskontrollintegration, wie in der Management-Anwendung und den Clients angezeigt. Sie können den bestehenden Namen mit einem Neuen überschreiben. |
| **Beschreibung** | Geben Sie eine Beschreibung für die Zutrittskontrollintegration ein. Dies ist optional. |
| **Integrations-Plug-in** | Zeigt den Typ des Zutrittskontrollsystems an, welches während der initialen Integration ausgewählt wurde. |
| **Letzte Konfiguration aktualisieren** | Zeigt Datum und Zeit der letzten Konfiguration, die vom Zutrittskontrollsystem importiert wurde. |
| **Konfiguration aktualisieren** | Klicken Sie auf die Schaltfläche, wenn Sie die im Zutrittskontrollsystem in XProtect vorgenommene Konfigurationsänderungen anzeigen lassen wollen (zum Beispiel wenn Sie eine Tür hinzugefügt oder entfernt haben).<br>Eine Zusammenfassung der Konfigurationsänderungen des Zutrittskontrollsystems erscheint. Überprüfen Sie die Liste, um sicherzustellen, dass Ihr Zutrittskontrollsystem korrekt widergespiegelt wird, bevor Sie die neue Konfiguration anwenden. |
| **Anwenderanmeldung erforderlich** | Aktivieren Sie eine zusätzliche Anmeldung für die Client-Benutzer, wenn das Zugangskontrollsystem differenzierte Benutzerberechtigungen unterstützt. Wenn sie diese Option aktivieren, steht Ihnen das Zutrittskontrollsystem im XProtect Mobile-Client nicht zur Verfügung.<br>Diese Option ist nur sichtbar, wenn das Integrations-Plug-in differenzierte Benutzerberechtigungen unterstützt. |

Die Bezeichnung und der Inhalt der folgenden Felder wurde aus dem Integrations-Plug-in importiert. Unten finden Sie einige Beispiele typischer Felder:

| Name | Beschreibung |
|---|---|
| **Adresse** | Geben Sie die Adresse des Hostservers des integrierten Zutrittskontrollsystems ein. |
| **Port** | Bestimmen Sie die Portnummer auf dem Server, der mit dem Zutrittskontrollsystem verbunden ist. |
| **Benutzername** | Geben sie den Namen des Benutzers ein, wie im Zutrittskontrollsystem festgelegt, der als Administrator des integrierten Systems in XProtect fungieren soll. |
| **Passwort** | Bestimmen Sie das Passwort des Benutzers. |

### Registerkarte „Türen und zugehörige Kameras“ (Zutrittskontrolle)

Diese Registerkarte stellt Zuordnungen zwischen Zutrittspunkten von Türen und Kameras, Mikrofonen oder Lautsprechern her. Sie können Kameras als Teil des Integrationsassistenten verknüpfen, eine spätere Änderung ist aber jederzeit möglich. Zuordnungen zu Mikrofonen und Lautsprechern sind durch die zugehörigen Mikrofone und Lautersprecher an der Kamera eingeschlossen.

| Name | Beschreibung |
|---|---|
| **Türen** | Listet die verfügbaren Zutrittspunkte der Türen auf, die im Zutrittskontrollsystem festgelegt sind; nach Türen gruppiert.<br><br>Zur einfacheren Navigation der relevanten Türen, können Sie mittels einer Dropdown-Liste oberhalb der Türen in Ihrem Zutrittskontrollsystem filtern.<br><br>**Aktiviert**: Lizenzierte Türen sind standardmäßig aktiviert. Sie können eine Tür deaktivieren, um eine Lizenz freizugeben.<br><br>**Lizenz**: Zeigt, falls eine Tür lizenziert ist oder ob die Lizenz abgelaufen ist. Das Feld ist leer, wenn die Tür deaktiviert ist.<br><br>**Entfernen**: Klicken Sie auf **Entfernen**, um eine Kamera aus einem Zutrittspunkt zu entfernen. Wenn Sie alle Kameras entfernen, wird das Kontrollkästchen für zugehörige Kameras automatisch abgewählt. |

| Name | Beschreibung |
|---|---|
| **Kameras** | Listet alle im XProtect-System konfigurierten Kameras auf.<br>Wählen Sie eine Kamera von der Liste aus und ziehen Sie diese per Drag & Drop zum gewünschten Zutrittspunkt, um den Zutrittspunkt mit der Kamera zu verknüpfen. |

### Registerkarte Zutrittskontrollereignisse (Zutrittskontrolle)

Ereigniskategorien erlauben es Ihnen, Ereignisse zu gruppieren. Die Konfiguration von Ereigniskategorien betrifft das Verhalten der Zutrittskontrolle im XProtect-System und erlaubt es Ihnen beispielsweise einen Alarm einzustellen, der einen einzelnen Alarm in mehreren Ereignistypen auslöst.

| Name | Beschreibung |
|---|---|
| **Zutrittskontrollereignis** | Listet die Zutrittskontrollereignisse auf, die vom Zutrittskontrollsystem importiert wurden. Das Integrations-Plug-in steuert die standardmäßige Aktivierung und Deaktivierung von Ereignissen. Sie können Ereignisse jederzeit nach der Integration deaktivieren oder aktivieren.<br>Sobald ein Ereignis aktiviert ist, wird es in der XProtect Ereignisdatenbank gespeichert und steht beispielsweise dem Filtern im XProtect Smart Client zur Verfügung. |
| **Quelltyp** | Zeigt die Zutrittskontrolleinheit, die das Zutrittskontrollereignis auslösen kann. |
| **Ereigniskategorie** | Weisen Sie keine, eine oder mehrere Ereigniskategorien den Zutrittskontrollereignissen zu. Das System ordnet automatisch zugehörige Ereigniskategorien zu den Ereignissen während der Integration zu. Dies aktiviert ein Standard-Setup im XProtect-System. Sie können die Zuordnung zu jeder Zeit ändern.<br>Integrierte Ereigniskategorien sind:<br>• Zutritt verweigert<br>• Zutritt gewährt<br>• Zutrittsanforderung<br>• Alarm |

| Name | Beschreibung |
|---|---|
| | • Fehler<br>• Warnung<br>Ereignisse und Ereigniskategorien, die vom Integrations-Plug-in festgelegt werden, erscheinen ebenfalls, allerdings können Sie auch Ihre eigenen Ereigniskategorien festlegen; siehe **Benutzerdefinierte Kategorien**.<br>Wenn Sie die Ereigniskategorien in XProtect Corporate ändern, stellen Sie sicher, dass die bestehenden Zutrittskontrollregeln weiterhin funktionieren. |
| **Benutzerdefinierte Kategorien** | Erlaubt es Ihnen benutzerdefinierte Ereigniskategorien zu erstellen, zu ändern oder zu löschen.<br>Sie können Ereigniskategorien erstellen, wenn die integrierten Kategorien nicht Ihren Anforderungen entsprechen, bspw. in Verbindung mit der Festlegung von auslösenden Ereignissen für Zutrittskontrollaktionen.<br>Die Kategorien werden global für alle Integrationssystem zum XProtect-System hinzugefügt. Sie erlauben die Einrichtung von systemübergreifender Steuerung, z. B. bei Alarmdefinitionen.<br>Wenn Sie eine benutzerdefinierte Ereigniskategorie löschen, erhalten Sie eine Warnung, falls diese von einer Integration verwendet wird. Sollten Sie diese dennoch löschen, funktionieren keine der Konfigurationen in dieser Kategorie (z. B. Zutrittskontrollaktionen) mehr. |

### Registerkarte „Zutrittsanforderungsbenachrichtigung“ (Zutrittskontrolle)

Sie können Zutrittsanforderungsbenachrichtigungen festlegen, die auf der XProtect Smart Client-Anzeige erscheinen sollen, wenn ein Ereignis auftritt.

| Name | Beschreibung |
|---|---|
| **Name** | Geben Sie einen Namen für die Zutrittsanforderungsbenachrichtigung ein. |

| Name | Beschreibung |
|---|---|
| **Zutrittsanforderungsbenachrichtigung hinzufügen** | Klicken Sie, um Zutrittsanforderungsbenachrichtigungen hinzufügen und festzulegen.<br><br>Um eine Benachrichtigung zu löschen, klicken Sie rechts auf das **X**.<br><br>  Wenn ein Benutzer von XProtect Smart Client sich in den übergeordneten Standort in einer Milestone Federated Architecture-Hierarchie einloggt, erscheinen Zutrittsanforderungsbenachrichtigungen des untergeordneten Standorts ebenfalls in XProtect Smart Client. |
| **Details der Zutrittsanforderungsbenachrichtigung** | Bestimmt, welche Kameras, Mikrofone oder Lautsprecher in den Zutrittsanforderungsbenachrichtigungen erscheint, wenn ein gewisses Ereignis auslöst. Bestimmt auch den Alarmton wenn die Benachrichtigung aufpoppt. |
| **Befehl hinzufügen** | Wählen Sie aus, welche Befehle als Schaltflächen im Dialogfenster der Zutrittsanforderungsbenachrichtigung in XProtect Smart Client zur Verfügung stehen sollen.<br><br>Zugehörige Zutrittsanfragebefehle:<br>• Aktiviert alle Befehle in Bezug auf Zutrittsanforderungsoperationen, die in der Quelleinheit verfügbar sind. Zum Beispiel, **Tür öffnen**<br><br>Alle zugehörigen Befehle:<br>• Aktiviert alle Befehle in der Quelleinheit<br><br>Zutrittskontrollbefehl:<br>• Aktiviert einen ausgewählten Zutrittskontrollbefehl<br><br>Systembefehl:<br>• Aktiviert ein Befehl, der im XProtect-System voreingestellt ist<br><br>Um einen Befehl zu löschen, klicken Sie rechts auf das **X**. |

### Registerkarte „Karteninhaber“ (Zutrittskontrolle)

Verwenden Sie die Registerkarte **Kartenhalter**, um Informationen über Karteninhaber im Zutrittskontrollsystem zu überprüfen.

| Name | Beschreibung |
|---|---|
| **Karteninhaber suchen** | Geben Sie die Buchstaben des Namens eines Karteninhabers ein und, sofern dieser existiert, erscheint er in der Liste. |
| **Name** | Listet die Namen der Karteninhaber auf, die aus dem Zutrittskontrollsystem abgerufen wurden. |
| **Typ** | Listet den Karteninhabertypen auf, zum Beispiel:<br>• Mitarbeiter<br>• Wache<br>• Gast |

Wenn Ihr Zutrittskontrollsystem das Hinzufügen/Löschen von Bildern im XProtect-System unterstützt, können Sie den Karteninhaber Bilder hinzufügen. Dies ist besonders nützlich, wenn Ihr Zutrittskontrollsystem keine Bilder der Karteninhaber einschließt.

| Name | Beschreibung |
|---|---|
| **Bild auswählen** | Legen Sie den Dateipfad für ein Bild des Karteninhabers fest. Diese Schaltfläche ist nicht sichtbar, wenn das Zutrittskontrollsystem die Bilder verwaltet.<br>Erlaubte Dateiformate sind: .bmp, .png, und .jpg.<br>Bilder werden an die maximale Ansichtsgröße angepasst.<br>Milestone empfiehlt, dass Sie ein quadratisches Bild verwenden. |
| **Bild löschen** | Klicken Sie, um das Bild zu löschen. Wenn das Zutrittskontrollsystem ein Bild hatte, wird dieses Bild nach der Löschung angezeigt. |

# Vorfallknoten

## Vorfalleigenschaften (Vorfallknoten)

Die folgenden Informationen beschreiben Einstellungen in Bezug auf XProtect Incident Manager.

Alle Vorfalleigenschaft für Ihre XProtect Smart Client-Anwender werden auf diesen Registerkarten festgelegt:

- Typen
- Status
- Kategorien
- Kategorie 1-5

Alle Vorfalleigenschaften haben die folgenden Einstellungen:

| Name | Beschreibung |
|---|---|
| **Name** | Die Namen von Vorfalleigenschaften müssen nicht eindeutig sein. Es ist jedoch in vielen Situationen von Vorteil, einmalige und selbsterklärende Namen zu verwenden. |
| **Beschreibung** | Eine weitere Erklärung der festgelegten Vorfalleigenschaft. Wenn Sie z. B. eine Kategorie namens *Standort* erstellt haben, könnte die Beschreibung lauten *Wo hat sich der Vorfall ereignet?* |

# Transaktionsknoten

## Transaktionsquellen (der Knoten "Transaktion")

Die folgende Tabelle beschreibt die Eigenschaften für Transaktionsquellen.

Weitere Informationen dazu, wie eine Quelle hinzugefügt wird, finden Sie unter Transaktionsquelle hinzufügen (Assistent).

Transaktionsquellen (Eigenschaften)

| Name | Beschreibung |
|---|---|
| **Aktivieren** | Wenn Sie die Transaktionsquelle deaktivieren möchten, deaktivieren Sie dieses Kontrollkästchen. Der Stream der Transaktionsdaten wird angehalten, aber die bereits importierten Daten bleiben im Event Server. Sie können Transaktionen einer deaktivierten Transaktionsquelle während der Speicherzeit in XProtect Smart Client weiterhin aufrufen.<br><br>Auch eine deaktivierte Transaktionsquelle erfordert eine Transaktionsquellenlizenz. |
| **Name** | Wenn Sie den Namen ändern möchten, geben Sie hier einen neuen Namen ein. |
| **Konnektor** | Sie können den ausgewählten Anschluss, den Sie beim Erstellen der Transaktionsquelle ausgewählt haben, nicht ändern. Für die Auswahl eines anderen Anschlusses müssen Sie eine neue Transaktionsquelle erstellen und im Assistenten den gewünschten Anschluss auswählen. |
| **Transaktionsdefinition** | Sie können eine andere Transaktionsdefinition auswählen, die festlegt, wie die empfangenen Transaktionsdaten in Transaktionen und Transaktionszeilen umgewandelt werden sollen. Dazu wird unter anderem Folgendes definiert:<br>• Beginn und Ende einer Transaktion.<br>• Wie Transaktionen in XProtect Smart Client angezeigt werden |
| **Speicherzeit** | Geben Sie in Tagen an, wie lange die Transaktionsdaten auf dem Event Server gespeichert bleiben. Standardmäßig beträgt die Speicherzeit 30 Tage. Nach dem Verstreichen der Speicherzeit werden die Daten automatisch gelöscht. Dadurch soll vermieden werden, dass die Speicherkapazität der Datenbank überschritten wird.<br><br>Der Mindestwert beträgt 1 Tag, der maximale Wert 1.000 Tage. |
| **TCP-Client-Konnektor** | Wenn Sie **TCP-Client-Konnektor** ausgewählt haben, legen Sie diese Einstellungen fest:<br>• **Hostname**: Geben Sie den Hostnamen des TCP-Servers ein, welcher der Transaktionsquelle zugeordnet wurde |

| Name | Beschreibung |
|---|---|
| | • **Port**: Geben Sie den Portnamen des TCP-Servers ein, welcher der Transaktionsquelle zugeordnet wurde |
| **Konnektor für seriellen Port** | Wenn Sie **Konnektor für seriellen Port** ausgewählt haben, legen Sie diese Einstellungen fest und stellen Sie sicher, dass sie mit den Einstellungen der Transaktionsquelle übereinstimmen:<br>• **Serieller Port**: Wählen Sie den COM-Port aus<br>• **Baudrate**: Geben Sie die Anzahl der pro Sekunde übertragenen Bits an<br>• **Parität**: Geben Sie die Methode zur Erkennung von Fehlern in den Übertragungen an. Standardmäßig ist **Keine** ausgewählt<br>• **Datenbits**: Geben Sie die Anzahl an Bits ein, die für die Darstellung eines Datenzeichens verwendet wird<br>• **Stopp-Bits**: Geben Sie die Anzahl an Bits ein, die anzeigen, wann ein Byte übertragen wurde. Die meisten Geräte benötigen 1 Bit<br>• **Handshake**: Geben Sie die Handshake-Methode an, die das Kommunikationsprotokoll zwischen der Transaktionsquelle und dem Event Server bestimmt |

## Transaktionsdefinitionen (der Knoten "Transaktion")

Die folgende Tabelle beschreibt die Eigenschaften für Definitionen, die für die Transaktionsquellen zu verwenden sind.

Weitere Informationen dazu, wie Transaktionsdefinitionen erstellt und hinzugefügt werden, finden Sie unter Transaktionsdefinitionen erstellen und hinzufügen.

### Transaktionsdefinitionen (Eigenschaften)

| Name | Beschreibung |
|---|---|
| **Name** | Geben Sie einen Namen ein. |
| **Verschlüsselung** | Wählen Sie den Zeichensatz aus, der von der Transaktionsquelle verwendet wird, zum Beispiel der Registrierkasse. Auf diese Weise wird XProtect Transact |

| Name | Beschreibung |
|---|---|
| | dabei unterstützt, die Transaktionsdaten in verständlichen Text zu konvertieren, mit dem Sie die Definition konfigurieren können.<br>Wenn Sie die falsche Kodierung auswählen, ist der angezeigte Text möglicherweise nicht verwertbar. |
| **Datenerfassung starten** | Erfassen Sie Transaktionsdaten von der angeschlossenen Transaktionsquelle. Sie können die Daten verwenden, um eine Transaktionsdefinition zu konfigurieren.<br>Warten Sie, bis mindestens eine, idealerweise mehrere Transaktionen abgeschlossen wurden. |
| **Datenerfassung stoppen** | Wenn Sie genügend Daten für die Konfiguration der Definition erfasst haben, klicken Sie auf diese Schaltfläche. |
| **Aus Datei laden** | Wenn Sie Daten aus einer bereits vorhandenen Datei importieren möchten, klicken Sie auf diese Schaltfläche. In der Regel handelt es sich dabei um eine Datei, die Sie zuvor im Format .capture erstellt haben. Sie kann jedoch auch ein anderes Format besitzen. Wichtig dabei ist, dass die Kodierung der Importdatei mit der Kodierung übereinstimmt, die für die aktuelle Definition ausgewählt wurde. |
| **In Datei speichern** | Wenn Sie die erfassten Rohdaten in eine Datei speichern möchten, klicken Sie auf diese Schaltfläche. Sie können sie später wiederverwenden. |
| **Übereinstimmungstyp** | Wählen Sie in den für die Suche nach dem Start- und dem Stopmuster in den gesammelten Rohdaten zu verwendenden Match-Typ:<br>• Genaue Übereinstimmung verwenden: Die Suche findet Zeichenfolgen, die genau das enthalten, was Sie in den Feldern **Start-Muster** und **Stop-Muster** eingegeben haben |

| Name | Beschreibung |
|---|---|
| | • Platzhalter verwenden: Die Suche findet Zeichenfolgen, die das enthalten, was Sie in den Feldern **Start-Muster** und **Stop-Muster** in Kombination mit einem Platzhaltersymbol (*, #, ?) eingegeben haben<br>* entspricht einer beliebigen Anzahl an Zeichen. Wenn Sie zum Beispiel „Start Tra*tion“ eingegeben haben, ermittelt die Suche Zeichenfolgen, die „Start Transaktion“ enthalten.<br># entspricht genau 1 Ziffer. Wenn Sie zum Beispiel „# Wassermelone“ eingegeben haben, ermittelt die Suche Zeichenfolgen, die zum Beispiel „1 Wassermelone“ enthalten. ?<br>Entspricht genau 1 Zeichen. Sie können zum Beispiel den Suchbegriff „Start Trans?ktion“ verwenden, um Zeichenfolgen zu ermitteln, die „Start Transaktion“ enthalten<br>• Regulären Ausdruck verwenden: Verwenden Sie diesen Typ, um Zeichenfolgen zu identifizieren, die spezifische Schreibweisen oder Konventionen enthalten, wie zum Beispiel ein Datumsformat oder eine Kreditkartennummer. Weitere Informationen finden Sie auf der Microsoft-Website (https://docs.microsoft.com/dotnet/standard/base-types/regular-expression-language-quick-reference/). |
| **Rohdaten** | Zeichenfolgen mit Transaktionsdaten aus der verbundenen Transaktionsquelle werden in dieser Lösung angezeigt. |
| **Start-Muster** | Geben Sie ein Start-Muster an, um anzugeben, wo eine Transaktion beginnt. Der Anfang und das Ende von Transaktionen wird im Feld **Vorschau** durch horizontale Linien dargestellt. Auf diese Weise behalten Benutzer einen besseren Überblick über die einzelnen Transaktionen. |
| **Stop-Muster** | Geben Sie ein Stop-Muster an, um anzugeben, wo eine Transaktion endet. Ein Stop-Muster ist nicht zwingend erforderlich, ist jedoch hilfreich, wenn die erhaltenen Daten unter den eigentlichen Transaktionen auch irrelevante Informationen enthalten, wie z.B. Angaben zu den Öffnungszeiten oder Sonderangebote.<br>Wenn Sie kein Stop-Muster angeben, so wird das Ende des Empfangs dadurch definiert, wo der nächste Empfang beginnt. Der Anfang wird dadurch vorgegeben, was in das Feld **Start-Muster** eingegeben wird. |

| Name | Beschreibung |
|---|---|
| **Filter hinzufügen** | Mithilfe der Schaltfläche **Filter hinzufügen** können Sie Zeichen angeben, die in XProtect Smart Client ausgelassen oder durch andere Zeichen bzw. einen Zeilenumbruch ersetzt werden sollen.<br>Das Ersetzen von Zeichen ist dann nützlich, wenn die Zeichenfolge der Transaktionsquelle Steuerzeichen enthält, die nicht zum Drucken verwendet werden. Zeilenumbrüche hinzuzufügen ist notwendig, damit die Quittungen in XProtect Smart Client so aussehen, wie die Originalquittungen. |
| **Filtertext** | Zeigt die Zeichen an, die aktuell im Abschnitt **Rohdaten** ausgewählt sind. Wenn Sie wissen, dass Sie bestimmte Zeichen weglassen oder ersetzen möchten, diese jedoch nicht in der gesamten Zeichenfolge der Rohdaten enthalten sind, können Sie die Zeichen manuell in das Feld **Zeichen** eingeben.<br>Wenn es sich bei diesem Zeichen um ein Steuerzeichen handelt, müssen Sie den hexadezimalen Byte-Wert eingeben. Verwenden Sie dieses Format für den Byte-Wert: {XX} und {XX,XX,...}, wenn ein Zeichen aus mehreren Bytes besteht. |
| **Aktion** | Für jeden Filter, den Sie hinzufügen, sollten Sie angeben, wie mit den ausgewählten Zeichen umgegangen werden soll:<br>• Auslassen: Die ausgewählten Zeichen werden herausgefiltert<br>• Ersetzen: Die ausgewählten Zeichen werden durch die von Ihnen angegebenen Zeichen ersetzt<br>• Zeilenumbruch hinzufügen: Die ausgewählten Zeichen werden durch einen Zeilenumbruch ersetzt |
| **Substitution** | Geben Sie den Text ein, durch den die ausgewählten Zeichen ersetzt werden sollen. Dies ist nur relevant, wenn Sie die Aktion **Ersetzen** ausgewählt haben. |
| **Entfernen Sie Steuerzeichen, die nicht als Filtertext definiert sind** | Entfernen Sie nicht druckbare Zeichen, die nach dem Hinzufügen von Filtern noch nicht entfernt wurden.<br>In dem Fenster **Rohdaten**, im Abschnitt **Vorschau**, können Sie sehen, wie sich die Zeichenfolgen für die Transaktionsdaten ändern, wenn Sie diese Einstellung vornehmen bzw. deaktivieren. |
| **Vorschau** | Mithilfe des Abschnitts **Vorschau** können Sie überprüfen, ob Sie unerwünschte Zeichen ermittelt und herausgefiltert haben. Die hier angezeigte Ausgabe entspricht dem Aussehen eines echten Belegs in XProtect Smart Client. |

# Alarmknoten

## Alarmdefinitionen (Alarmknoten)

Wenn Ihr System auf Ihrem System ein Ereignis registriert, können Sie das System so konfigurieren, dass es einen Alarm im XProtect Smart Client erstellt. Sie müssen Alarme definieren, bevor Sie diese verwenden können und Alarme werden auf Basis der Ereignisse definiert, die auf Ihren Systemservern registriert werden. Sie können auch benutzerdefinierte Ereignisse verwenden, um Alarme auszulösen und dasselbe Ereignis verwenden, um mehrere verschiedene Alarme auszulösen.

### Alarmdefinitionseinstellungen:

| Name | Beschreibung |
|---|---|
| **Aktivieren** | Standardmäßig ist die Alarmdefinition aktiviert. Wählen Sie das Kontrollkästchen ab, um dies zu deaktivieren. |
| **Name** | Alarmnamen müssen nicht einmalig sein, aber die Verwendung von einmaligen und selbsterklärenden Alarmnamen bietet in vielen Situationen Vorteile. |
| **Anweisungen** | Geben Sie einen beschreibenden Text zu dem Alarm ein und wie das Problem, das den Alarm verursacht hat, zu lösen ist.<br>Der Text erscheint im XProtect Smart Client, wenn der Benutzer den Alarm behandelt. |
| **Auslösendes Ereignis** | Wählen Sie die Ereignisnachricht, die angezeigt werden soll, wenn der Alarm ausgelöst wird. Wählen Sie aus zwei Auswahllisten:<br>• Die erste Menüoption: Wählen Sie den Ereignistyp, z. B. Analyseereignis und Systemereignisse<br>• Die zweite Menüoption: Wählen Sie die speziell zu verwendende Ereignisnachricht aus. Die verfügbaren Nachrichten werden durch den Ereignistyp bestimmt, den Sie im ersten Dropdown-Menü ausgewählt haben |
| **Quellen** | Wählen Sie die Quellen, aus denen die Ereignisse stammen. Abgesehen von Kameras oder sonstigen Geräten, kann es sich bei den Quellen auch um plug-in-definierte Quellen handeln, z. B. VCA  und MIP. Die Optionen hängen vom Ereignistyp ab, den Sie ausgewählt haben. |

Alarmauslöser:

| Name | Beschreibung |
|---|---|
| **Zeitprofil** | Wählen Sie die Optionsschaltfläche **Zeitprofil** aus, um das Zeitintervall zu bestimmen, während dem die Alarmdefinition aktiv ist. Es wird nur das Zeitprofil auf der Liste angezeigt, das Sie unter dem Knoten **Regeln und Ereignisse** definiert haben. Wenn keines definiert wurde, ist nur die Option **Immer** verfügbar. |
| **Ereignisgesteuert** | Wenn Sie möchten, dass der Alarm auf einem Ereignis basiert, wählen Sie diese Optionsschaltfläche. Legen Sie nach dem Auswählen das Start- und Stoppereignis fest. Sie können für Kameras, Videoserver und -eingänge festgelegte Hardware-Ereignisse auswählen. Siehe auch Ereignisübersicht. Auch globale/manuelle Vorfalldefinitionen können verwendet werden. Siehe auch Benutzerdefinierte Ereignisse (Erklärung). |

Anwenderaktion erforderlich:

| Name | Beschreibung |
|---|---|
| **Zeitgrenze** | Wählen Sie eine Zeitgrenze, vor der eine Aktion des Anwenders erforderlich ist. Der Standardwert ist 1 Minute. Die Zeitgrenze ist erst aktiv, wenn Sie im Dropdown-Menü **Ausgelöste Ereignisse** ein Ereignis angehängt haben. |
| **Ausgelöste Ereignisse** | Wählen Sie aus, welche Ereignisse ausgelöst werden sollen, wenn die Zeitgrenze überschritten wurde. |

Karten:

| Name | Beschreibung |
|---|---|
| **Alarm-Manager-Ansicht** | Weisen Sie dem Alarm entweder eine Smart Map oder eine Karte zu, wenn der Alarm in XProtect Smart Client > **Alarm Manager** aufgeführt ist. |

| Name | Beschreibung |
|---|---|
| | Smart Map zeigt Alarme an, wenn diese von einem Gerät ausgelöst werden und wenn das Gerät zu der Smart Map hinzugefügt wird. |

Andere:

| Name | Beschreibung |
|---|---|
| **Zugehörige Kameras** | Wählen Sie bis zu 15 Kameras aus, die in die Alarmdefinition eingeschlossen werden, auch wenn diese Kameras den Alarm nicht selbst auslösen. Das kann relevant sein, wenn Sie z. B. eine externe Ereignisnachricht (wie z. B. eine Tür, die geöffnet wird) als Quelle Ihres Alarms ausgewählt haben. Wenn Sie eine oder mehrere Kameras in der Nähe der Tür definieren, können Sie die Kameraaufzeichnungen des Vorfalls an den Alarm anhängen. |
| **Anfänglicher Eigentümer des Alarms** | Auswahl eines standardmäßig verantwortlichen Benutzers für den Alarm. |
| **Anfängliche Alarmpriorität** | Wählen Sie eine Priorität für den Alarm aus. Verwenden Sie diese Prioritäten in XProtect Smart Client, um die Wichtigkeit eines Alarms zu festzulegen. |
| **Alarmkategorie** | Wählen Sie für den Alarm eine Alarmkategorie aus, z. B. **Fehlalarm** oder **Untersuchung erforderlich**. |
| **Durch Alarm ausgelöste Ereignisse** | Definieren Sie ein Ereignis, das der Alarm in XProtect Smart Client auslösen kann. |
| **Alarm automatisch schließen** | Aktivieren Sie dieses Kontrollkästchen, wenn ein bestimmtes Ereignis den Alarm automatisch anhalten soll. Nicht alle |

| Name | Beschreibung |
|---|---|
| | Ereignisse können Alarme auslösen. Deaktivieren Sie das Kontrollkästchen, um den neuen Alarm am Anfang zu deaktivieren. |
| **Administratoren zuzuordnende Alarme** | Wählen Sie das Kontrollkästchen aus, um Benutzern mit Administratorrolle in die Liste **Zugewiesen zu** aufzunehmen.<br>Die Liste **Zugeordnet zu** befindet sich in den Alarmdetails auf der Registerkarte **Alarm Manager** in XProtect Smart Client.<br>Deaktivieren Sie das Kontrollkästchen, um Benutzer mit Administratorrolle aus der Liste **Zugewiesen zu** herauszufiltern, um die Liste zu kürzen. |

## Alarmdateneinstellungen (Alarmknoten)

Legen Sie beim Konfigurieren der Alarmdateneinstellungen Folgendes fest:

### Registerkarte „Alarm-Datenstufen“

**Prioritäten**

| Name | Beschreibung |
|---|---|
| **Stufe** | Fügen Sie neue Prioritäten mit frei wählbaren Stufenzahlen hinzu oder verwenden/bearbeiten Sie die standardmäßigen Prioritätsstufen (Zahl 1, 2 oder 3). Diese Prioritätsstufen werden zur Konfiguration der Einstellung **Anfängliche Alarmpriorität** verwendet. |
| **Name** | Geben Sie einen Namen für die Entität ein. Sie können beliebig viele erstellen. |
| **Ton** | Wählen Sie den Ton, der mit dem Alarm verknüpft werden soll. Verwenden Sie einen der Standardtöne oder fügen Sie weitere unter **Toneinstellungen** hinzu. |
| **Ton wiederholen** | Entscheiden Sie, ob der Ton nur einmal oder wiederholt abgespielt werden soll, bis der Benutzer in XProtect Smart Client in der Alarmliste auf den Alarm klickt. |

| Name | Beschreibung |
|---|---|
| **Aktivieren Sie die Desktop-Benachrichtigungen** | Für jede Alarmpriorität können Sie die Desktop-Benachrichtigungen aktivieren oder deaktivieren. Wenn Sie ein XProtect VMS verwenden, das Smart Client-Profile unterstützt, müssen Sie auf den erforderlichen Smart Client Profilen auch die Benachrichtigungen aktivieren. Siehe Registerkarte Alarm-Manager (Smart Client-Profile) auf Seite 509. |

### Zustände

| Name | Beschreibung |
|---|---|
| **Stufe** | Zusätzlich zu den standardmäßigen Zustandsstufen (Zahlen **1**, **4**, **9** und **11**, die nicht bearbeitet oder wiederverwendet werden können) können Sie neue Zustände mit frei wählbaren Stufenzahlen hinzufügen. Diese Zustandsstufen sind nur auf der *Alarmliste* von XProtect Smart Client sichtbar. |

### Kategorien

| Name | Beschreibung |
|---|---|
| **Stufe** | Fügen Sie neue Kategorien mit frei wählbaren Stufenzahlen hinzu. Diese Kategoriestufen werden zur Konfiguration der Einstellung **Anfängliche Alarmkategorie** verwendet.<br>  Stufe 99 ist für den Notfallalarm im XProtect Mobile Client reserviert. |
| **Name** | Geben Sie einen Namen für die Entität ein. Sie können beliebig viele erstellen. |

**Konfiguration der Alarmliste-Registerkarte**

| Name | Beschreibung |
|---|---|
| **Verfügbare Spalten** | Verwenden Sie >, um auszuwählen, welche Spalten in der *Alarmliste* von XProtect Smart Client verfügbar sein sollen. Verwenden Sie < zum Aufheben der Auswahl. Danach sollte **Ausgewählte Spalten** die einzuschließenden Elemente enthalten. |

Registerkarte „Gründe für das Schließen“

| Name | Beschreibung |
|---|---|
| **Aktivieren** | Auswählen, um zu aktivieren, dass allen Alarmen ein Schließungsgrund zugewiesen werden muss, bevor sie geschlossen werden können. |
| **Grund** | Fügen Sie Schließungsgründe hinzu, zwischen denen der Benutzer beim Schließen von Alarmen wählen kann. Diese könnten z. B. sein: *Unbefugter Zutritt aufgeklärt* oder *Fehlalarm*. Sie können beliebig viele erstellen. |

## Audioeinstellungen (Alarmknoten)

Legen Sie beim Konfigurieren der Toneinstellungen Folgendes fest:

| Name | Beschreibung |
|---|---|
| **Töne** | Wählen Sie den Ton, der mit dem Alarm verknüpft werden soll. Die Tonliste enthält einige standardmäßige Windows-Sounds. Sie können auch neue Töne hinzufügen (.wav oder .mp3). |
| **Hinzufügen** | Töne hinzufügen. Suchen Sie in den Audiodateien und laden Sie eine oder mehrere .wav- oder .mp3-Dateien hoch. |
| **Entfernen** | Entfernen Sie einen ausgewählten Ton von der Liste der manuell hinzugefügten Töne. Standardtöne können nicht entfernt werden. |
| **Test** | Testen Sie den Ton. Wählen Sie den Ton auf der Liste. Der Ton wird einmal abgespielt. |

# Hierarchie der föderalen Sites

## Eigenschaften für einen föderalen Standort

Dieser Abschnitt beschreibt die Registerkarte **Allgemein** und die Registerkarte **Mutterseite**.

### Allgemein

Sie können einige der Informationen zum Standort, an dem Sie gerade angemeldet sind, ändern.

| Name | Beschreibung |
|---|---|
| **Name** | Geben Sie den Namen des Standorts ein. |
| **Beschreibung** | Geben Sie eine Standortbeschreibung ein. |
| **URLs** | Verwenden Sie die Liste, um URL(s) für diesen Standort hinzuzufügen und zu entfernen und um anzugeben, ob diese extern sind oder nicht. Externe Adressen können außerhalb des lokalen Netzwerks aufgerufen werden. |
| **Version** | Die Versionsnummer des Management-Servers des Standorts. |
| **Dienstkonto** | Das Dienstkonto, unter dem der Management-Server ausgeführt wird. |
| **Zeitpunkt der letzten Synchronisierung** | Zeit und Datum der letzten Synchronisierung der Hierarchie. |
| **Status der letzten Synchronisierung** | Der Status der letzten Synchronisierung der Hierarchie. Der Status kann entweder **Erfolgreich** oder **Fehlgeschlagen** sein. |

### Registerkarte „Übergeordneter Standort“

In dieser Registerkarte werden Informationen zum übergeordneten Standort des Standorts angezeigt, an dem Sie gerade angemeldet sind. Diese Registerkarte ist nicht sichtbar, wenn Ihr Standort über keinen übergeordneten Standort verfügt.

| Name | Beschreibung |
|---|---|
| **Name** | Zeigt den Namen des übergeordneten Standorts an. |
| **Beschreibung** | Zeigt eine Beschreibung des übergeordneten Standorts an (optional). |
| **URLs** | Listet URL(s) für diesen übergeordneten Standort auf und gibt an, ob sie extern oder intern sind. Externe Adressen können außerhalb des lokalen Netzwerks aufgerufen werden. |
| **Version** | Die Versionsnummer des Management-Servers des Standorts. |
| **Dienstkonto** | Das Dienstkonto, unter dem der Management-Server ausgeführt wird. |
| **Zeitpunkt der letzten Synchronisierung** | Zeit und Datum der letzten Synchronisierung der Hierarchie. |
| **Status der letzten Synchronisierung** | Der Status der letzten Synchronisierung der Hierarchie. Der Status kann entweder **Erfolgreich** oder **Fehlgeschlagen** sein. |

helpfeedback@milestone.dk

Info über Milestone

Milestone Systems ist ein weltweit führender Anbieter von Open-Platform-Videomanagementsoftware – Technologie, die Unternehmen hilft für Sicherheit zu sorgen, Ressourcen zu schützen und die Wirtschaftlichkeit zu erhöhen. Milestone Systems ist die Basis einer Open Platform Community, die die Zusammenarbeit und Innovation bei der Entwicklung und dem Einsatz von Netzwerkvideotechnologie vorantreibt und für zuverlässige, individuell anpassbare Lösungen sorgt, die sich an über 150.000 Standorten auf der ganzen Welt bewährt haben. Milestone Systems wurde 1998 gegründet und ist ein eigenständiges Unternehmen der Canon Group. Weitere Informationen erhalten Sie unter https://www.milestonesys.com/.