

MAKE THE  
WORLD SEE

# Milestone Systems

---

XProtect® Mobile-Server 2021 R1

Bedienungsanleitung für Administratoren



# Inhalt

|  |           |
|--|-----------|
| <b>Copyright, Marken und Verzichtserklärung</b>                              | <b>5</b>  |
| <b>Übersicht</b>   | <b>6</b>  |
| XProtect Mobile (erklärt)  | 6         |
| XProtect Mobile-Server (Erklärung)   | 6         |
| Produktvergleichstabelle   | 7         |
| <b>Anforderungen und Hinweise</b>  | <b>11</b> |
| Voraussetzungen für die Verwendung von XProtect Mobile                       | 11        |
| XProtect Mobile-Systemanforderungen  | 11        |
| Anforderungen für das Einrichten von Benachrichtigungen                      | 11        |
| Anforderungen für das Einrichten von Smart Connect                           | 12        |
| Anforderungen für die Einrichtung der zweistufigen Verifikation für Benutzer | 12        |
| Anforderungen für das Einrichten von Video Push                              | 12        |
| Anforderungen für direktes Streaming   | 12        |
| <b>Installation</b>  | <b>14</b> |
| XProtect Mobile-Server installieren  | 14        |
| <b>Konfiguration</b>   | <b>17</b> |
| Einstellungen des mobilen Servers  | 17        |
| Allgemein  | 17        |
| Registerkarte Konnektivität  | 20        |
| Registerkarte Serverstatus   | 22        |
| Registerkarte Leistung   | 23        |
| Registerkarte Untersuchungen   | 26        |
| Registerkarte Video Push   | 28        |
| Registerkarte Benachrichtigungen   | 29        |
| Registerkarte Zweistufige Verifikation                                       | 30        |
| Direktes Streaming (Erklärung)   | 33        |
| Adaptives Streaming (Erklärung)  | 34        |
| Sichere Kommunikation (Erläuterung)  | 35        |

- Verschlüsselung des Managementsservers (Erläuterung) .....36
- Verschlüsselung vom Management-Server zum Aufzeichnungsserver (Erläuterung) ..... 38
- Verschlüsselung zwischen dem Management Server und den Data Collector server (Erläuterung) .....39
- Verschlüsselung an alle Clients und Dienste, die Daten vom Aufzeichnungsserver abrufen (Erläuterung) .....40
- Datenverschlüsselung des mobilen Servers (Erläuterung) ..... 43
  - Anforderungen zur Verschlüsselung mobiler Server für Clients .....44
- Milestone Federated Architecture und den Master/Slave Servern (Erklärung) ..... 44
- Smart Connect (Erklärung) .....44
  - Einrichten von Smart Connect .....45
  - Aktivieren Sie die UPnP-Erkennungsfunktion in Ihrem Router .....45
  - Aktivieren von Verbindungen im komplexen Netzwerk .....45
  - Konfigurieren der Verbindungseinstellungen .....46
  - Senden einer E-Mail-Nachricht an Benutzer .....46
- Senden von Benachrichtigungen (Erklärung) ..... 47
  - Konfigurieren von Push-Benachrichtigungen auf dem XProtect Mobile-Server .....47
  - Aktivieren von Push-Benachrichtigungen für bestimmte oder alle Mobilgeräte .....48
  - Deaktivieren des Sendens von Push-Benachrichtigungen an bestimmte oder alle Mobilgeräte .....48
- Einrichten von Untersuchungen ..... 49
- Nutzung von Video Push für Videostreams (Erklärung) .....50
  - Einrichten von Video Push für Videostreams ..... 51
  - Einen video push-Kanal für Video-Streaming hinzufügen ..... 51
    - Einen Video-Push-Kanal bearbeiten ..... 52
    - Einen video push-Kanal entfernen .....52
    - Passwort ändern .....52
  - Den video push-Treiber als Gerät hinzufügen auf dem Recording Server ..... 53
  - Hinzufügen des video push-Treibergeräts zum video push-Kanal ..... 54
  - Aktivieren Sie Audio für den vorhandenen Push-Videokanal .....55
- Einrichten von Benutzern für die zweistufige Verifikation über E-Mail .....55
  - Informationen über den SMTP-Server eingeben ..... 56
  - Den Verifizierungscode festlegen, der an Benutzer gesendet wird ..... 56

|   |           |
|---|-----------|
| Benutzern und Active Directory-Gruppen eine Anmeldemethode zuweisen .....                                 | 56        |
| Aktionen (erklärt): .....   | 57        |
| Einen Ausgang zur Verwendung im XProtect Mobile-Client und XProtect Web Client benennen (Erklärung) ..... | 57        |
| <b>Wartung .....</b>  | <b>58</b> |
| Mobile Server Manager (erklärt) .....   | 58        |
| Zugriff auf XProtect Web Client .....   | 58        |
| Den Mobile Server-Dienst starten, anhalten oder neu starten .....   | 59        |
| Passworteinstellungen für den Datenschutz ändern .....  | 59        |
| Management-Server-Adresse eintragen/bearbeiten .....  | 60        |
| Portnummern anzeigen/bearbeiten .....   | 60        |
| Aktivieren Sie die Verschlüsselung auf dem mobilen Server. ....   | 60        |
| Zugriff auf Protokolle und Untersuchungen (erklärt) .....   | 62        |
| Untersuchungen-Ordner ändern .....  | 63        |
| Status anzeigen (Erklärung) .....   | 64        |
| <b>Fehlerbehandlung .....</b>   | <b>65</b> |
| Fehlerbehandlung XProtect Mobile .....  | 65        |

## Copyright, Marken und Verzichtserklärung

Copyright © 2021 Milestone Systems A/S

### 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

## XProtect Mobile (erklärt)

XProtect Mobile besteht aus fünf Komponenten:

- XProtect Mobile Client

Der Client XProtect Mobile ist eine mobile Überwachung-App, die Sie auf Ihrem Android- oder Apple-Gerät installieren und verwenden können. Sie können den XProtect Mobile-Client auf einer beliebigen Anzahl von Geräten installieren.

Weitere Informationen finden Sie im Benutzerhandbuch für den XProtect Mobile-Client, das Sie auf der Milestone Systems-Website (<https://www.milestone.com/support/help-yourself/manuals-and-guides/>) herunterladen können.

- XProtect Web Client

XProtect Web Client erlaubt Ihnen, Video live in Ihrem Web-Browser anzusehen, und Aufzeichnungen herunterzuladen. XProtect Web Client wird automatisch zusammen mit der Installation des XProtect Mobile-Servers installiert.

Für weitere Informationen laden Sie das XProtect Web Client Benutzerhandbuch von der Milestone Systems-Website (<https://www.milestone.com/support/help-yourself/manuals-and-guides/>) herunter.

- XProtect Mobile-Server
- XProtect Mobile Plug-in
- Mobile Server Manager

Der XProtect Mobile-Server, das XProtect Mobile-Plug-in und Mobile Server Manager werden in dieser Bedienungsanleitung erläutert.

## XProtect Mobile-Server (Erklärung)

Der XProtect Mobile-Server bearbeitet Anmeldungen am System vom XProtect Mobile-Client oder XProtect Web Client.

Ein XProtect Mobile-Server verteilt Videostreams von Aufzeichnungsservern an den XProtect Mobile-Client oder XProtect Web Client. Dies ermöglicht eine sichere Einrichtung, bei der die Aufzeichnungsserver nie mit dem Internet verbunden sind. Wenn ein XProtect Mobile-Server Videostreams von Aufzeichnungsservern empfängt, verwaltet er auch die komplexe Konvertierung von Codecs und Formaten, die das Streaming von Video auf das Mobilgerät erlauben.

Sie müssen den XProtect Mobile-Server auf allen Computern installieren, von denen aus Sie auf Aufzeichnungsserver zugreifen wollen. Wenn Sie den XProtect Mobile-Server installieren, melden Sie sich mit einem Konto an, das über Administratorrechte verfügt. Andernfalls können die Installation nicht erfolgreich abgeschlossen werden (siehe [XProtect Mobile-Server installieren auf Seite 14](#)).

Der XProtect Mobile-Server unterstützt direktes Streaming und adaptives Streaming im Live-Modus (nur für XProtect Expert und XProtect Corporate).

## Produktvergleichstabelle

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 Website Milestone (<https://www.milestonesys.com/solutions/platform/product-index/>).

Nachfolgend finden Sie eine Liste der Hauptunterschiede zwischen den Produkten:

| Name                              | XProtect Essential+ | XProtect Express+ | XProtect Professional+ | XProtect Expert       | XProtect Corporate      |
|-----------------------------------|---------------------|-------------------|------------------------|-----------------------|-------------------------|
| Standorte pro SLC                 | 1                   | 1                 | Mehrere Standorte      | Mehrere Standorte     | Mehrere Standorte       |
| Aufzeichnungsserver pro SLC       | 1                   | 1                 | Unbegrenzt             | Unbegrenzt            | Unbegrenzt              |
| Geräte pro Aufzeichnungsserver    | 8                   | 48                | Unbegrenzt             | Unbegrenzt            | Unbegrenzt              |
| Milestone Interconnect™           | -                   | Remote-System     | Remote-System          | Remote-System         | Zentraler/Remote-System |
| Milestone Federated Architecture™ | -                   | -                 | -                      | Remote-System         | Zentraler/Remote-System |
| Aufzeichnungsserver-Failover      | -                   | -                 | -                      | Cold- und Hot-Standby | Cold- und Hot-Standby   |

| Name  | XProtect Essential+         | XProtect Express+           | XProtect Professional+      | XProtect Expert                        | XProtect Corporate                     |
|---|-----------------------------|-----------------------------|-----------------------------|--|--|
| Fernzugriffsdienste   | -                           | -                           | -                           | -                                      | ✓                                      |
| Edge-Speicher-Unterstützung   | -                           | -                           | ✓                           | ✓                                      | ✓                                      |
| Mehrschichtige Videospeicherarchitektur   | Live-Datenbanken + 1 Archiv | Live-Datenbanken + 1 Archiv | Live-Datenbanken + 1 Archiv | Live-Datenbanken + unbegrenzte Archive | Live-Datenbanken + unbegrenzte Archive |
| SNMP-Benachrichtigung   | -                           | -                           | -                           | ✓                                      | ✓                                      |
| Zeitgesteuerte Benutzerzugriffsrechte   | -                           | -                           | -                           | -                                      | ✓                                      |
| Bildrate reduzieren (Ausdünnung)  | -                           | -                           | -                           | ✓                                      | ✓                                      |
| Videodatenverschlüsselung (Aufzeichnungsserver)                                       | -                           | -                           | -                           | ✓                                      | ✓                                      |
| Datenbanksignatur (Recording-Server)  | -                           | -                           | -                           | ✓                                      | ✓                                      |
| PTZ-Prioritätsstufen  | 1                           | 1                           | 3                           | 32000                                  | 32000                                  |
| Erweitertes PTZ (PTZ-Sitzung und Wachrundgang über XProtect Smart Client reservieren) | -                           | -                           | -                           | ✓                                      | ✓                                      |

| Name   | XProtect Essential+   | XProtect Express+     | XProtect Professional+ | XProtect Expert          | XProtect Corporate                                     |
|--|-----------------------|-----------------------|------------------------|--------------------------|--|
| Beweissicherung  | -                     | -                     | -                      | -                        | ✓  |
| Lesezeichenfunktion  | -                     | -                     | Nur manuell            | Manuell und regelbasiert | Manuell und regelbasiert                               |
| Live-Multi-streaming oder Multicasting, auch bekannt als adaptives Streaming | -                     | -                     | -                      | ✓                        | ✓  |
| Direktes Streaming   | -                     | -                     | -                      | ✓                        | ✓  |
| Gesamtsicherheit   | Client-Benutzerrechte | Client-Benutzerrechte | Client-Benutzerrechte  | Client-Benutzerrechte    | Client-Benutzerrechte/<br>Administrator-Benutzerrechte |
| XProtect Management Client-Profil  | -                     | -                     | -                      | -                        | ✓  |
| XProtect Smart Client-Profil   | -                     | -                     | 3                      | 3                        | Unbegrenzt   |
| XProtect Smart Wall  | -                     | -                     | -                      | Optional                 | ✓  |
| Systemmonitor  | -                     | -                     | -                      | ✓                        | ✓  |
| Smart Map  | -                     | -                     | -                      | ✓                        | ✓  |
| Zweistufige Verifizierung  | -                     | -                     | -                      | -                        | ✓  |

| Name  | XProtect Essential+ | XProtect Express+ | XProtect Professional+ | XProtect Expert | XProtect Corporate |
|---|---------------------|-------------------|------------------------|-----------------|--------------------|
| DLNA-Support  | -                   | ✓                 | ✓                      | ✓               | ✓                  |
| Privatsphärenausblendung  | -                   | ✓                 | ✓                      | ✓               | ✓                  |
| Gerätepasswortverwaltung  |                     |                   | ✓                      | ✓               | ✓                  |
| Verschlüsselter Export aus der Mediendatenbank (Mobilservers)               | ✓                   | ✓                 | ✓                      | ✓               | ✓                  |
| Digitale Signatur aus der Mediendatenbank exportierter Daten (Mobilservers) | ✓                   | ✓                 | ✓                      | ✓               | ✓                  |

## Anforderungen und Hinweise

### Voraussetzungen für die Verwendung von XProtect Mobile

Bevor Sie XProtect Mobile verwenden können, müssen folgende Voraussetzungen erfüllt sein:

- VMS muss installiert sowie für mindestens einen Benutzer konfiguriert sein und ausgeführt werden
- Im XProtect Smart Client müssen Kameras und Ansichten eingerichtet sein
- Ein mobiles Gerät mit Android oder iOS als Betriebssystem und mit Zugriff zu Google Play oder App Store, von wo aus Sie die XProtect Mobile Client-Anwendung herunterladen können
- Ein Webbrowser zum Ausführen von XProtect Web Client

Weitere Informationen zu den Anforderungen finden Sie unter [XProtect Mobile-Systemanforderungen auf Seite 11](#).

### XProtect Mobile-Systemanforderungen

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

- Die Anforderungen für den XProtect Mobile Client finden Sie, wenn Sie das Produktsymbol **XProtect Mobile** auswählen
- Um die Anforderungen für XProtect Web Client zu finden, wählen Sie das **XProtect Web Client** Produktsymbol aus
- Die Anforderungen für den XProtect Mobile Server finden Sie, wenn Sie das Symbol des bei Ihnen installierten XProtect Produktes auswählen
- Die Anforderungen für das XProtect Mobile-Plug-in sind folgende:
  - Eine laufende Management Client
  - Das Milestone-Plug-in ist installiert und in Ihr VMS integriert

### Anforderungen für das Einrichten von Benachrichtigungen

- Sie müssen mindestens einen Alarm mit mindestens einem Ereignis und einer Regel verknüpfen. Dies gilt nicht für Systembenachrichtigungen
- Vergewissern Sie sich, dass Ihre Milestone Care™-Vereinbarung mit Milestone Systems aktuell ist.
- Ihr System muss über Internetzugriff verfügen

Für weitere Informationen, siehe:

[Konfigurieren von Push-Benachrichtigungen auf dem XProtect Mobile-Server auf Seite 47](#)

[Registerkarte Benachrichtigungen auf Seite 29](#)

## Anforderungen für das Einrichten von Smart Connect

- Ihr XProtect Mobile-Server muss eine öffentliche IP-Adresse verwenden. Die Adresse kann statisch oder dynamisch sein, aber normalerweise ist es eine gute Idee, statische IP-Adressen zu verwenden.
- Sie müssen über eine gültige Lizenz für Smart Connect verfügen

## Anforderungen für die Einrichtung der zweistufigen Verifikation für Benutzer

- Sie haben einen SMTP-Server installiert
- Sie haben im Management Client im Knoten **Rollen** im Bereich **Standort-Navigation** Benutzer und Gruppen zu Ihrem XProtect-System hinzugefügt. Wählen Sie für die relevante Rolle die Registerkarte **Benutzer und Gruppen** aus
- Wenn Sie Ihr System von einer älteren Version von XProtect aktualisiert haben, müssen Sie den mobilen Server neu starten, damit die zweistufige Verifikation wirksam wird

Für weitere Informationen, siehe:

[Einrichten von Benutzern für die zweistufige Verifikation über E-Mail auf Seite 55](#)

[Registerkarte Zweistufige Verifikation auf Seite 30](#)

## Anforderungen für das Einrichten von Video Push

- Für jeden Kanal ist eine Gerätelizenz erforderlich
- Zur Aktivierung von Audio mit Push-Video:
  1. Laden Sie die Version Milestone XProtect Device Pack 10.3a oder später herunter und installieren Sie sie.
  2. Laden Sie XProtect Mobile Server Installer.exe 13.2a oder später herunter und installieren Sie es.
  3. Starten Sie den Recording Server-Dienst neu.

## Anforderungen für direktes Streaming

XProtect Mobile unterstützt Direct Streaming im Live-Modus (nur für XProtect Expert und XProtect Corporate).

### Anforderungen an die Kamerakonfiguration für direktes Streaming

Um Direct Streaming in XProtect Web Client und XProtect Mobile-Client zu verwenden, benötigen Sie die folgende Kamerakonfiguration:

- Die Kameras müssen (für alle Clients) das Codec H.264 unterstützen, oder das Codec H.265 (nur für den XProtect Mobile-Client)
- Es wird empfohlen, den Wert der **GOP-Größe** auf **1 Sekunde** zu setzen, und die **FPS-Einstellung** muss einen Wert haben, der höher ist als **10 FPS**

# Installation

## XProtect Mobile-Server installieren

Nach der Installation des XProtect Mobile-Servers können Sie XProtect Mobile-Client und XProtect Web Client mit Ihrem System verwenden. Um die Gesamtnutzung von Systemressourcen auf dem Computer zu reduzieren, auf dem der Management-Server ausgeführt wird, installieren Sie den XProtect Mobile-Server auf einem separaten Computer.

Der Management-Server verfügt über eine integrierte öffentliche Installations-Webseite. Von dieser Webseite können Administratoren und Endbenutzer die erforderlichen XProtect-Systemkomponenten vom Management-Server oder einem anderen Computer im System herunterladen und installieren.



XProtect Mobile Der Server wird automatisch installiert, wenn Sie die Option Einzelcomputer installieren.

Zum Installieren des XProtect Mobile-Servers:

1. Geben Sie die folgende URL in Ihren Browser ein: *http://[Management-Server-Adresse]/installation/admin*, wobei die [Management-Server-Adresse] die IP-Adresse oder der Hostname des Management-Servers ist.
2. Klicken Sie auf **Alle Sprachen**, um das XProtect Mobile-Server-Installationsprogramm aufzurufen.
3. Führen Sie die heruntergeladene Datei aus. Klicken Sie dann auf **Ja**, um alle Warnungen zu bestätigen. Das Entpacken beginnt.
4. Wählen Sie die Sprache für das Installationsprogramm aus. Klicken Sie dann auf **Weiter**.
5. Lesen Sie und akzeptieren Sie die Lizenzvereinbarung. Klicken Sie dann auf **Weiter**.
6. Wählen Sie den Installationstyp aus:
  - Klicken Sie auf **Typisch**, um den XProtect Mobile-Server und das Plug-in zu installieren.
  - Klicken Sie auf **Benutzerdefiniert**, um nur den Server oder nur das Plug-in zu installieren. Nur das Plug-in zu installieren ist z.B. nützlich, wenn Sie mit Management Client XProtect Mobile Server verwalten wollen, aber keinen XProtect Mobile Server auf dem betreffenden Computer brauchen



XProtect Mobile Läuft auf dem Computer Management Client zur Verwaltung von XProtect Mobile Servern in Management Client, ist das - Plug-in erforderlich.

7. Nur für die benutzerdefinierte Installation Wählen Sie die Komponenten aus, die Sie installiert haben möchten. Klicken Sie dann auf **Weiter**.

8. Wählen Sie das Dienstkonto für den mobilen Server aus. Klicken Sie dann auf **Weiter**.



Um die Anmeldedaten für das Dienstkonto später zu ändern oder zu bearbeiten, müssen Sie den Mobilserver neu installieren.

9. Geben Sie in das Feld **Server-URL** die Adresse des primären Management-Servers ein.
10. Nur für die benutzerdefinierte Installation Geben Sie die Ports für die Kommunikation mit dem mobilen Server an. Klicken Sie dann auf **Weiter**.



Bei einer typischen Installation erhalten die Verbindungsports die Standardportnummern 8081 für den HTTP-Port und 8082 für den HTTPS-Port).

11. 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**.

12. Geben Sie die Verschlüsselung für den mobilen Server an. Klicken Sie dann auf **Weiter**.

Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

- Zwischen den Mobile Servern und den Aufzeichnungsservern, Datensammlern und dem Management Server. Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.
- Zwischen den Mobile Servern und den Clients. Um die Verschlüsselung zwischen dem Mobile Server und den Clients zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.



Wenn Sie die Verschlüsselung nicht aktivieren, stehen bestimmte Funktionen auf manchen Clients nicht zur Verfügung. Weitere Informationen finden Sie unter [Anforderungen zur Verschlüsselung mobiler Server für Clients auf Seite 44](#).

Weitere Informationen zur Einrichtung der sicheren Kommunikation auf Ihrem System finden Sie unter [Datenverschlüsselung des mobilen Servers \(Erläuterung\) auf Seite 43](#) oder im Leitfaden zu Zertifikaten [Milestone](#).

Die Verschlüsselung können Sie auch nach Abschluss der Installation vom Mobile Server Manager-Taskleistensymbol Ihres Betriebssystems aktivieren (siehe [Aktivieren Sie die Verschlüsselung auf dem mobilen Server. auf Seite 60](#)).

13. Wählen Sie den Datei-Speicherort und die Produktsprache aus, und klicken Sie dann auf **Installieren**.
14. Wenn die Installation abgeschlossen ist, wird eine Liste der erfolgreich installierten Komponenten angezeigt. Klicken Sie dann auf **Schließen**.

Sie sind bereit für die Konfiguration von XProtect Mobile (siehe [Einstellungen des mobilen Servers auf Seite 17](#)).

# Konfiguration

## Einstellungen des mobilen Servers

In Management Client können Sie eine Liste der XProtect Mobile Servereinstellungen konfigurieren und bearbeiten. Auf diese Einstellungen haben Sie unten in der Werkzeugleiste der **Eigenschaften** des Mobile Servers Zugriff. Von dort können Sie:

- Aktivieren oder deaktivieren Sie die allgemeine Konfiguration der Servereigenschaften (siehe [Allgemein auf Seite 17](#))
- Konfigurieren der Einstellungen für die Serververbindung (siehe [Registerkarte Konnektivität auf Seite 20](#))
- Einrichtung der Funktion Smart Connect (siehe [Registerkarte Konnektivität auf Seite 20](#))
- Den aktuellen Status des Servers sowie eine Liste der aktiven Benutzer finden Sie unter [Registerkarte Serverstatus auf Seite 22](#)
- Sie können Leistungsparameter einrichten, um Direct Streaming und adaptives Streaming zu aktivieren, oder um Begrenzungen für transcodierte Videostreams festzulegen (siehe [Registerkarte Leistung auf Seite 23](#))
- Konfigurieren der Einstellungen für Untersuchungen (siehe [Registerkarte Untersuchungen auf Seite 26](#))
- Konfigurieren der Einstellungen für Push-Video (siehe [Registerkarte Video Push auf Seite 28](#))
- Angaben zur Einrichtung sowie zum Ein- und Ausschalten von Systembenachrichtigungen und Push-Benachrichtigungen finden Sie unter [Registerkarte Benachrichtigungen auf Seite 29](#)
- Aktivieren und konfigurieren eines zusätzlichen Anmeldeschrittes für Benutzer (siehe [Registerkarte Zweistufige Verifikation auf Seite 30](#))

## Allgemein

In den folgenden Tabellen werden die Einstellungen auf dieser Registerkarte beschrieben.

### Allgemein

| Name         | Beschreibung  |
|--------------|---|
| Servername   | Geben Sie den Namen des XProtect Mobile Servers ein.                      |
| Beschreibung | Geben Sie eine optionale Beschreibung für den XProtect Mobile-Server ein. |

| Name                  | Beschreibung   |
|-----------------------|--|
| <b>Mobile Server</b>  | Siehe den Namen des aktuell ausgewählten XProtect Mobile-Servers.  |
| <b>Anmeldemethode</b> | <p>Wählen Sie die Authentifizierungsmethode für die Anmeldung beim Server aus. Sie haben folgende Optionen:</p> <ul style="list-style-type: none"> <li>• <b>Automatisch</b></li> <li>• <b>Windows-Authentifizierung</b></li> <li>• <b>Basis-Authentifizierung</b></li> </ul> |

### Funktionen

Die folgende Tabelle beschreibt, wie die Verfügbarkeit der XProtect Mobile Funktionen gesteuert wird.

| Name   | Beschreibung  |
|--|---|
| <b>XProtect Web Client aktivieren</b>                | Aktivieren Sie den Zugriff auf XProtect Web Client. Diese Funktion ist standardmäßig aktiviert.   |
| <b>Aktivieren Sie die Ansicht "Alle Kameras"</b>     | Schließen Sie die Ansicht <b>Alle Kameras</b> mit ein. In dieser Ansicht werden alle Kameras angezeigt, die der betreffende Benutzer auf einem Aufzeichnungsserver sehen darf. Diese Funktion ist standardmäßig aktiviert.  |
| <b>Aktionen aktivieren (Ausgänge und Ereignisse)</b> | <p>Aktivieren Sie den Zugriff auf Aktionen in XProtect Mobile-Clients und XProtect Web Client. Diese Funktion ist standardmäßig aktiviert.</p> <p>Wenn Sie diese Funktion deaktivieren, können die Benutzer des Clients keine Ausgaben und Ereignisse sehen, selbst wenn diese korrekt konfiguriert sind.</p> |
| <b>Eingehendes Audiosignal aktivieren</b>            | Aktivieren Sie die Funktion für eingehenden Ton XProtect Web Client und XProtect Mobile Client. Diese Funktion ist standardmäßig aktiviert.   |
| <b>Push-to-talk aktivieren</b>                       | Push-to-Talk (PTT) Funktion in XProtect Web Client und XProtect Mobile Client aktivieren. Diese Funktion ist standardmäßig aktiviert.   |

| Name  | Beschreibung   |
|---|--|
| <b>Zugriff der integrierten Administrator-Rolle auf den XProtect Mobile-Server verweigern</b> | Aktivieren Sie diese Funktion, um Benutzern, die der integrierten Administratorrolle zugeordnet sind, den Zugriff auf Video über XProtect Mobile-Clients oder XProtect Web Client zu verweigern. |

### Protokolleinstellungen

Sie können die Protokolleinstellungen Informationen.

| Name                                  | Beschreibung   |
|---------------------------------------|--|
| <b>Speicherort der Protokolldatei</b> | Siehe Sie, wo das System Protokolldateien speichert.   |
| <b>Protokolle beibehalten für</b>     | Siehe die Anzahl an Tagen, für die Protokolle beibehalten werden. Die Standardeinstellung ist drei Tage. |

### Konfigurationsbackup

Wenn Ihr System über mehrere XProtect Mobile-Server verfügt, können Sie die Backup-Funktion verwenden, um aktuelle Einstellungen zu exportieren und diese auf anderen XProtect Mobile-Servern zu importieren.

| Name               | Beschreibung   |
|--------------------|--|
| <b>Importieren</b> | Importieren Sie eine XML-Datei mit einer neuen XProtect Mobile-Serverkonfiguration.                                  |
| <b>Exportieren</b> | Exportieren Sie Ihre XProtect Mobile-Serverkonfiguration. Ihr System speichert die Konfiguration in einer XML-Datei. |

## Registerkarte Konnektivität

Die Einstellungen auf der Registerkarte **Konnektivität** werden bei den folgenden Aufgaben verwendet:

- [Konfigurieren der Verbindungseinstellungen auf Seite 46](#)
- [Senden einer E-Mail-Nachricht an Benutzer auf Seite 46](#)
- [Aktivieren von Verbindungen im komplexen Netzwerk auf Seite 45](#)
- [Aktivieren Sie die UPnP-Erkennungsfunktion in Ihrem Router auf Seite 45](#)

Weitere Informationen finden Sie unter [Smart Connect \(Erklärung\) auf Seite 44](#).



Sie können konfigurieren, wie der XProtect Mobile Client und die XProtect Web Client Benutzer eine Verbindung zum XProtect Mobile Server herstellen, wenn Sie während der Installation den **Server Configurator** öffnen oder indem Sie nach der Installation mit der rechten Maustaste auf das Taskleistensymbol Mobile Server Manager klicken. Der Verbindungstyp kann entweder HTTPS oder HTTP sein. Weitere Informationen finden Sie unter [Aktivieren Sie die Verschlüsselung auf dem mobilen Server. auf Seite 60](#).

### Allgemein

| Name                                  | Beschreibung   |
|---------------------------------------|--|
| <b>Client-Timeout (HTTP)</b>          | Legen Sie mithilfe eines Timeline Areas fest, wie oft der XProtect Mobile-Client und XProtect Web Client dem XProtect Mobile-Server anzeigen müssen, dass sie betriebsbereit sind. Der Standardwert beträgt 30 Sekunden.<br><br>Milestone empfiehlt Ihnen, das Timeline Area nicht zu erhöhen. |
| <b>UPnP-Entdeckbarkeit aktivieren</b> | Dies macht den XProtect Mobile-Server durch UPnP-Protokolle im Netzwerk auffindbar.<br><br>Der XProtect Mobile-Client hat eine auf UPnP basierende Scanfunktionalität für das Finden von XProtect Mobile-Servern.  |
| <b>Portzuordnung aktivieren</b>       | Wenn der XProtect Mobile-Server hinter der Firewall installiert ist, ist Port Mapping im Router erforderlich, damit Clients vom Internet aus immer noch auf den Server zugreifen können.   |

| Name                            | Beschreibung   |
|---------------------------------|--|
|                                 | Mit der Option <b>Automatische Portzuordnung aktivieren</b> kann der XProtect Mobile Server diese Portzuordnung selbst vornehmen, vorausgesetzt, der Router ist dafür konfiguriert.                                    |
| <b>Smart Connect aktivieren</b> | Mit Smart Connect können Sie ohne Anmeldung mit einem Mobilgerät oder Tablet überprüfen, ob der XProtect Mobile-Server richtig konfiguriert wurde. Außerdem vereinfacht es den Verbindungsvorgang für Client-Benutzer. |

### Internetzugriff

| Name   | Beschreibung   |
|--|--|
| <b>Benutzerdefinierten Internetzugriff konfigurieren</b> | Wenn Sie die UPnP-Portzuordnung verwenden, um Verbindungen an eine bestimmte Verbindung weiterzuleiten, aktivieren Sie das Kontrollkästchen <b>Benutzerdefinierten Internetzugriff konfigurieren</b> .<br><br>Geben Sie dann die <b>IP-Adresse oder den Hostnamen</b> und den für die Verbindung zur verwendenden Port an. Dies können Sie z.B. tun, wenn Ihr Router kein UPnP unterstützt oder wenn Sie eine Routerkette haben. |
| <b>Standardadresse deaktivieren</b>                      | Deaktivieren Sie die standardmäßige IP-Adresse für die Verbindung mit dem mobilen Server nur mit einer bestimmten IP-Adresse oder hostname.  |
| <b>Auswählen, um die IP-Adresse dynamisch abzurufen</b>  | Wenn sich Ihre IP-Adressen häufig ändern, aktivieren Sie das Kontrollkästchen <b>Auswählen, um IP-Adresse dynamisch abzurufen</b> .  |
| <b>HTTP-Port</b>   | Geben Sie die Portnummer für die HTTP-Verbindung ein. Die standardmäßige Portnummer lautet 8081.   |
| <b>HTTPS-Port</b>  | Geben Sie die Portnummer für die HTTPS-Verbindung ein. Die standardmäßige Portnummer lautet 8082.  |
| <b>Server-Adressen</b>                                   | Listet alle IP-Adressen auf, die mit dem mobilen Server verbunden sind.  |

### Smart Connect-Benachrichtigung

| Name                         | Beschreibung  |
|------------------------------|---|
| <b>E-Mail-Einladung an</b>   | Geben Sie die E-Mail-Adresse des gewünschten Empfängers der Smart Connect-Benachrichtigung ein.   |
| <b>E-Mail-Sprache</b>        | Geben Sie die in der E-Mail verwendete Sprache an.  |
| <b>Smart Connect-Token</b>   | Ein eindeutiger Bezeichner, den Benutzer von Mobilgeräten verwenden können, um eine Verbindung zum XProtect Mobile-Server herzustellen. |
| <b>Link zu Smart Connect</b> | Ein Link, den Benutzer von Mobilgeräten verwenden können, um eine Verbindung zum XProtect Mobile-Server herzustellen.                   |

## Registerkarte Serverstatus

Sehen Sie sich die Statusdetails für den XProtect Mobile-Server an. Die Details sind schreibgeschützt:

| Name                             | Beschreibung   |
|----------------------------------|--|
| <b>Server ist aktiviert seit</b> | Zeigt das Datum und Uhrzeit des letzten Starts des XProtect Mobile-Servers.  |
| <b>CPU-Auslastung</b>            | Zeigt die aktuelle CPU-Auslastung auf dem mobilen Server an.   |
| <b>Externe Bandbreite</b>        | Zeigt die aktuell genutzte Bandbreite zwischen dem XProtect Mobile-Client oder XProtect Web Client und dem mobilen Server. |

## Aktive Benutzer

Sehen Sie sich die Statusdetails des XProtect Mobile-Client oder XProtect Web Client an, der/die aktuell mit dem XProtect Mobile-Server verbunden sind.

| Name                                   | Beschreibung   |
|--|--|
| <b>Benutzername</b>                    | Zeigt den Benutzernamen jedes XProtect Mobile-Client- oder XProtect Web Client-Benutzers an, der mit dem mobilen Server verbunden ist.   |
| <b>Status</b>                          | Zeigt die aktuelle Beziehung zwischen dem XProtect Mobile-Server und dem jeweiligen XProtect Mobile-Client oder XProtect Web Client-Benutzer an. Mögliche Statusmeldungen: <ul style="list-style-type: none"> <li>• <b>Verbunden:</b> Ein Anfangszustand, wenn die Clients und der Server Schlüssel und Verschlüsselungsinformationen austauschen</li> <li>• <b>Angemeldet:</b> Der XProtect Mobile-Client- oder XProtect Web Client-Benutzer ist im XProtect-System angemeldet</li> </ul> |
| <b>Video Bandbreitennutzung (kB/s)</b> | Zeigt die gesamte Bandbreite der Videostreams, die derzeit für jeden XProtect Mobile Client oder XProtect Web Client-Benutzer offen sind.  |
| <b>Audio Bandbreitennutzung (kB/s)</b> | Zeigt die gesamte Bandbreite der Audiostreams, die derzeit für jeden XProtect Web Client-Benutzer offen sind.  |
| <b>Transcodierte Videostreams</b>      | Zeigt die gesamte Bandbreite der transcodierten Videostreams, die derzeit für jeden XProtect Mobile Client oder XProtect Web Client-Benutzer offen sind.   |
| <b>Direkte Video-Streams</b>           | Zeigt die Gesamtzahl der Direct-Video-Streams, die derzeit für jeden XProtect Mobile-Client oder XProtect Web Client-Benutzer offen sind (nur für XProtect Expert und XProtect Corporate).   |
| <b>Transcodierte Audiostreams</b>      | Zeigt die Gesamtzahl der transcodierten Audiostreams, die derzeit für jeden XProtect Web Client-Benutzer offen sind.   |

## Registerkarte Leistung

Auf der Registerkarte **Leistung** können Sie die folgenden Einstellungen des XProtect Mobile-Servers vornehmen und dessen Leistung begrenzen:

**Video-Streaming-Einstellungen (nur für XProtect Expert und XProtect Corporate)**

| Name                                  | Beschreibung  |
|---------------------------------------|---|
| <b>Direktes Streaming aktivieren</b>  | Direktes Streaming aktivieren im XProtect Web Client und XProtect Mobile-Client (nur für XProtect Expert und XProtect Corporate). Diese Funktion ist standardmäßig aktiviert.   |
| <b>Adaptives Streaming aktivieren</b> | Aktivieren Sie adaptives Streaming im XProtect Web Client und XProtect Mobile-Client (nur für XProtect Expert und XProtect Corporate). Diese Funktion ist standardmäßig aktiviert.  |
| <b>Streamingweisen</b>                | <p>Wenn Sie die Funktion adaptives Streaming aktiviert haben, können Sie den Streamingmodus aus der Liste auswählen:</p> <ul style="list-style-type: none"> <li>• <b>Videoqualität optimieren (Standard)</b> - hierbei wird der Stream mit der geringsten verfügbaren Auflösung ausgewählt, die der geforderten Auflösung entspricht oder darüber liegt</li> <li>• <b>Leistung des Servers optimieren</b> - hierbei wird die geforderte Auflösung gesenkt und dann der Stream mit der geringsten verfügbaren Auflösung ausgewählt, die der reduzierten Auflösung entspricht oder darüber liegt</li> <li>• <b>Auflösung für geringe Bandbreiten optimieren</b> - hierbei wird der Stream mit der geringsten verfügbaren Auflösung ausgewählt (dies wird bei Verwendung von 3G oder instabilem Netz empfohlen)</li> </ul> |

**Beschränkungen für transcodierte Videostreams**

**Pegel 1**

Bei **Level 1** handelt es sich um die Standardbegrenzung auf dem XProtect Mobile-Server. Beschränkungen, die Sie hier einstellen, werden auf transcodierte Videostreams des XProtect Mobile stets angewendet.

| Name                      | Beschreibung   |
|---------------------------|--|
| <b>Pegel 1</b>            | Aktivieren Sie das Kontrollkästchen, um die erste Begrenzungsstufe für die XProtect Mobile-Serverleistung zu aktivieren.                               |
| <b>Max. FPS</b>           | Legen Sie einen Höchstwert für die maximale Anzahl von Bildern pro Sekunde (FPS) fest, die vom XProtect Mobile-Server an Clients gesendet werden soll. |
| <b>Max. Bildauflösung</b> | Legen Sie einen Höchstwert für die Bildauflösung fest, die beim Senden von Bildern vom XProtect Mobile-Server an Clients verwendet werden soll.        |

## Pegel 2

Wenn Sie statt der Standardbegrenzungsstufe auf **Level 1** eine andere Begrenzungsstufe erzwingen möchten, können Sie stattdessen das Kontrollkästchen **Level 2** aktivieren. Der Wert der Einstellungen darf den auf der ersten Stufe festgelegten Wert nicht übersteigen. Wenn Sie für „Max. FPS“ auf **Level 1** beispielsweise 45 festlegen, können Sie für „Max. FPS“ auf **Level 2** maximal 44 festlegen.

| Name                             | Beschreibung   |
|----------------------------------|--|
| <b>Pegel 2</b>                   | Aktivieren Sie das Kontrollkästchen, um die zweite Begrenzungsstufe für die XProtect Mobile-Serverleistung zu aktivieren.                              |
| <b>CPU-Schwellenwert</b>         | Legen Sie für die CPU-Auslastung auf dem XProtect Mobile-Server einen Schwellenwert fest, bevor das System Videostreambegrenzungen erzwingt.           |
| <b>Bandbreiten-Schwellenwert</b> | Legen Sie für die Bandbreitengrenze auf dem XProtect Mobile-Server einen Schwellenwert fest, bevor das System Videostreambegrenzungen erzwingt.        |
| <b>Max. FPS</b>                  | Legen Sie einen Höchstwert für die maximale Anzahl von Bildern pro Sekunde (FPS) fest, die vom XProtect Mobile-Server an Clients gesendet werden soll. |
| <b>Max. Bildauflösung</b>        | Legen Sie einen Höchstwert für die Bildauflösung fest, die beim Senden von Bildern vom XProtect Mobile-Server an Clients verwendet werden soll.        |

### Pegel 3

Sie können außerdem das Kontrollkästchen **Level 3** aktivieren, um eine dritte Begrenzungsstufe zu erstellen. Der Wert der Einstellungen darf den auf **Level 1** und **Level 2** festgelegten Wert nicht übersteigen. Wenn Sie für **Max. FPS** auf **Level 1** beispielsweise 45 und auf **Level 2** 32 festlegen, können Sie für **Max. FPS** auf **Level 3** maximal 31 festlegen.

| Name                             | Beschreibung  |
|----------------------------------|---|
| <b>Pegel 3</b>                   | Aktivieren Sie das Kontrollkästchen, um die dritte Begrenzungsstufe für die XProtect Mobile-Serverleistung zu aktivieren.                       |
| <b>CPU-Schwellenwert</b>         | Legen Sie für die CPU-Auslastung auf dem XProtect Mobile-Server einen Schwellenwert fest, bevor das System Videostreambegrenzungen erzwingt.    |
| <b>Bandbreiten-Schwellenwert</b> | Legen Sie für die Bandbreitengrenze auf dem XProtect Mobile-Server einen Schwellenwert fest, bevor das System Videostreambegrenzungen erzwingt. |
| <b>Max. FPS</b>                  | Legen Sie einen Höchstwert für die Anzahl Bilder pro Sekunde (FPS) fest, die vom XProtect Mobile-Server an Clients gesendet werden soll.        |
| <b>Max. Bildauflösung</b>        | Legen Sie einen Höchstwert für die Bildauflösung fest, die beim Senden von Bildern vom XProtect Mobile-Server an Clients verwendet werden soll. |



Das System wechselt nicht sofort von einer Stufe zur anderen. Wenn Ihr CPU- oder Bandbreitenschwellenwert weniger als fünf Prozent über oder unter der angegebenen Stufe liegt, wird die aktuelle Stufe beibehalten.

## Registerkarte Untersuchungen

### Untersuchungseinstellungen

Sie können Untersuchungen zulassen, damit die Benutzer mit dem XProtect Mobile Client oder XProtect Web Client:

- Auf Videoaufzeichnungen zugreifen können
- Zwischenfälle untersuchen können
- Videobeweise vorbereiten und herunterladen können

| Name  | Beschreibung   |
|---|--|
| <b>Untersuchungen ermöglichen</b>   | Aktivieren Sie dieses Kontrollkästchen, damit die Benutzer Untersuchungen erstellen können.  |
| <b>Untersuchungen-Ordner</b>  | Zeigt, wo Ihre Videoexporte auf Ihrer Festplatte gespeichert werden.   |
| <b>Untersuchungen anzeigen, die von anderen Benutzern durchgeführt werden</b> | Aktivieren Sie dieses Kontrollkästchen, um Benutzern den Zugriff auf Untersuchungen zu gewähren, die sie nicht selbst erstellt haben.  |
| <b>Aktivieren Sie die Größenbegrenzung des Untersuchungsordners</b>           | Aktivieren Sie dieses Kontrollkästchen, um die Größe des Untersuchungsordners zu begrenzen, und geben Sie die maximale Anzahl Megabyte an, die der Untersuchungsordner enthalten darf. Standardmäßig ist die Größe auf 2000 MB begrenzt.   |
| <b>Aktivieren Sie die Speicherdauer für Untersuchungen:</b>                   | Aktivieren Sie dieses Kontrollkästchen, um eine Speicherdauer für Untersuchungen festzulegen. Die Standardspeicherdauer beträgt sieben Tage.   |
| <b>Exportformate</b>  | <p>Aktivieren Sie das Kontrollkästchen für das Exportformat, das Sie verwenden möchten. Folgende Exportformate stehen zur Verfügung:</p> <ul style="list-style-type: none"> <li>• <b>AVI-Format</b></li> <li>• <b>XProtect-Format</b></li> <li>• <b>MKV-Format</b></li> </ul> <p>Die Kontrollkästchen sind standardmäßig leer.</p> |
| <b>Zeitstempel für AVI-Exporte einschließen</b>                               | Aktivieren Sie dieses Kontrollkästchen, um das Datum und die Uhrzeit für den Download der AVI-Datei anzuzeigen.  |
| <b>Codec für AVI-Exporte verwenden</b>  | Wählen Sie das Komprimierungsformat aus, das bei der Vorbereitung von AVI-Paketen zum Herunterladen verwendet wird.  |

| Name  | Beschreibung  |
|---|---|
|   | Die verfügbaren Codecs können je nach verwendetem Betriebssystem variieren. Wenn der gewünschte Codec nicht vorhanden ist, können sie ihn auf dem Computer installieren, auf dem der XProtect Mobile-Server ausgeführt wird. Anschließend wird er in der Liste angezeigt. |
| <b>Für AVI-Exporte verwendete Audio-Bitrate</b> | Wählen Sie aus der Liste die geeignete Audio-Bitrate aus, für den Fall, dass Audio in Ihrem Videoexport enthalten ist. Die Standardeinstellung ist 160000 Hz.   |

## Untersuchungen

| Name                        | Beschreibung   |
|-----------------------------|--|
| <b>Untersuchungen</b>       | Listet die Untersuchungen auf, die bisher im System konfiguriert wurden. Verwenden Sie die Schaltfläche <b>Löschen</b> oder <b>Alle löschen</b> , wenn Sie eine Untersuchung nicht mehr benötigen. Auf diese Weise können Sie wieder Speicherplatz auf dem Server freigeben.   |
| <b>Untersuchungsdetails</b> | Wenn Sie einzelne, für eine Untersuchung exportierte Videodateien löschen, die Untersuchung selbst aber behalten möchten, wählen Sie zuerst die Untersuchung in der Liste aus. Wählen Sie aus der Gruppe <b>Untersuchungsdetails</b> das Symbol "Löschen" rechts von den Feldern <b>XProtect</b> , <b>AVI</b> oder <b>MKV</b> für Exporte aus. |

## Registerkarte Video Push

Wenn Sie Video Push aktivieren, können Sie folgende Einstellungen vornehmen:

| Name              | Beschreibung                                       |
|-------------------|--|
| <b>Push-Video</b> | Aktivierung von Video Push auf dem mobilen Server. |

| Name              | Beschreibung  |
|-------------------|---|
| Anzahl der Kanäle | Zeigt die Anzahl der aktivierten Video Push-Kanäle in Ihrem XProtect-System an. |
| Kanal             | Zeigt die Nummer des entsprechenden Kanals an. Kann nicht bearbeitet werden.    |
| Port              | Die Portnummer des entsprechenden Video Push-Kanals.                            |
| MAC-Adresse       | Die MAC-Adresse des entsprechenden Video Push-Kanals.                           |
| Benutzername      | Geben Sie den Benutzernamen für den entsprechenden Video Push-Kanal ein.        |
| Kameraname        | Zeigt den Namen der Kamera an, wenn diese erkannt wurde.                        |

Wenn Sie alle erforderlichen Schritte abgeschlossen haben (siehe [Einrichten von Video Push für Videostreams auf Seite 51](#)), wählen Sie **Kameras suchen** aus, um die jeweilige Kamera zu suchen.

## Registerkarte Benachrichtigungen

Mithilfe der Registerkarte **Benachrichtigungen** können Sie Systembenachrichtigungen und Push-Benachrichtigungen aktivieren oder deaktivieren.

Wenn Sie Benachrichtigungen einschalten und einen oder mehrere Alarme oder Ereignisse konfiguriert haben, werden die Benutzer von XProtect Mobile benachrichtigt, wenn sich etwas ereignet. Wenn die App geöffnet ist, werden die Benachrichtigungen in XProtect Mobile auf dem Mobilgerät angezeigt. Mithilfe von Push-Benachrichtigungen werden Benutzer benachrichtigt, die XProtect Mobile nicht geöffnet haben. Diese Benachrichtigungen werden auf dem Mobilgerät angezeigt.

Für weitere Informationen, siehe: [Aktivieren von Push-Benachrichtigungen für bestimmte oder alle Mobilgeräte auf Seite 48](#)

In den folgenden Tabellen werden die Einstellungen auf dieser Registerkarte beschrieben.

| Name                                   | Beschreibung  |
|--|---|
| <b>Benachrichtigungen</b>              | Aktivieren Sie dieses Kontrollkästchen, um Benachrichtigungen zu aktivieren.  |
| <b>Geräteregistrierung beibehalten</b> | <p>Aktivieren Sie dieses Kontrollkästchen, um Informationen über die Geräte und Benutzer, die zu diesem Server eine Verbindung herstellen, zu speichern. Das System sendet Benachrichtigungen an diese Geräte.</p> <p>Wenn Sie dieses Kontrollkästchen deaktivieren, wird auch die Liste der Geräte deaktiviert. Wenn die Benutzer wieder Benachrichtigungen erhalten sollen, müssen Sie das Kontrollkästchen aktivieren und die Benutzer müssen erneut eine Verbindung zwischen ihren Geräten und dem Server herstellen.</p> |

### Registrierte Geräte

| Name              | Beschreibung  |
|-------------------|---|
| <b>Aktiviert</b>  | Aktivieren Sie dieses Kontrollkästchen, um Benachrichtigungen an das Gerät zu senden.   |
| <b>Gerätename</b> | <p>Liste der Mobilgeräte, die mit diesem Server verbunden sind.</p> <p>Sie können das Senden von Benachrichtigungen an bestimmte Geräte aktivieren oder deaktivieren, indem Sie das Kontrollkästchen <b>Aktiviert</b> aktivieren oder deaktivieren.</p> |
| <b>Benutzer</b>   | Name des Benutzers, der Benachrichtigungen empfängt.  |

## Registerkarte Zweistufige Verifikation



Verfügbare Funktionalität hängt vom verwendeten System ab. Weitere Informationen finden Sie unter <https://www.milestonesys.com/solutions/platform/product-index/>.

Verwenden Sie die Registerkarte **Zweistufige Verifikation**, um zusätzliche Anmeldeschritte für Benutzer folgender Systeme zu bestimmen und zu aktivieren:

- XProtect Mobile App auf ihren iOS- oder mobilen Android-Endgeräten
- XProtect Web Client

Die erste Art der Verifikation ist ein Passwort. Der erste Anmeldeschritt besteht in der Eingabe eines Passworts, der zweite Anmeldeschritt in der Eingabe eines Verifizierungscodes, den Benutzer nach Konfiguration in einer E-Mail erhalten.

Weitere Informationen finden Sie unter [Einrichten von Benutzern für die zweistufige Verifikation über E-Mail auf Seite 55](#).

In der folgenden Tabelle werden die Einstellungen auf dieser Registerkarte beschrieben.

**Anbiereinstellungen > E-Mail**

| Name   | Beschreibung  |
|--|---|
| <b>SMTP-Server</b>                                       | Geben Sie die IP-Adresse oder den Hostnamen des SMTP-Servers (Simple Mail Transfer Protocol) ein, der für den Versand der E-Mails für die zweistufige Verifikation verwendet werden soll. |
| <b>SMTP-Server-Port</b>                                  | Geben Sie den Port des SMTP-Servers ein, der für den E-Mail-Versand verwendet werden soll.<br><br>Die Standardportnummer lautet 25 ohne SSL und 465 mit SSL.                              |
| <b>SSL verwenden</b>                                     | Aktivieren Sie dieses Kontrollkästchen, wenn Ihr SMTP-Server SSL-Verschlüsselung unterstützt.   |
| <b>Benutzername</b>                                      | Geben Sie den Benutzernamen für die Anmeldung am SMTP-Server ein.   |
| <b>Passwort</b>  | Geben Sie das Passwort für die Anmeldung am SMTP-Server ein.  |
| <b>Sichere Passwortauthentifizierung (SPA) verwenden</b> | Aktivieren Sie dieses Kontrollkästchen, wenn Ihr SMTP-Server SPA unterstützt.   |
| <b>E-Mail-Adresse des Absenders</b>                      | Geben Sie die E-Mail-Adresse für den Versand der Verifizierungscodes ein.   |

| Name           | Beschreibung   |
|----------------|--|
| E-Mail-Betreff | Geben Sie einen Betreff für die E-Mail ein. Beispiel: Ihr Code für die zweistufige Verifizierung.  |
| E-Mail-Text    | <p>Geben Sie die Nachricht ein, die gesendet werden soll. Beispiel: Ihr Code lautet {0}.</p> <div style="border: 1px solid #0070C0; padding: 5px; background-color: #D9E1F2;">  Wenn Sie die Variable {0} nicht angeben, wird der Code standardmäßig an das Textende angefügt.                 </div> |

### Verifizierungscode-Einstellungen

| Name   | Beschreibung  |
|--|---|
| Zeitüberschreitung bei Wiederverbindung (0-30 Minuten) | <p>Geben Sie den Zeitraum an, innerhalb dem XProtect Mobile-Clientbenutzer ihre Anmeldung nicht erneut verifizieren müssen, zum Beispiel bei einer Trennung der Netzwerkverbindung. Der Standardzeitraum ist drei Minuten.</p> <p>Diese Einstellung gilt nicht für XProtect Web Client.</p> |
| Code läuft ab nach (1-10 Minuten)                      | Geben Sie eine Gültigkeitsdauer für den Verifizierungscode nach Empfang durch den Benutzer an. Nach diesem Zeitraum wird der Code ungültig, und der Benutzer muss einen neuen Code anfordern. Der Standardzeitraum ist fünf Minuten.  |
| Code-Eingabeversuche (1-10 Versuche)                   | Legen Sie die maximale Anzahl von Codeeingabeversuchen fest, bevor der bereitgestellte Code seine Gültigkeit verliert. Die Standardanzahl ist drei.   |
| Codelänge (4-6 Zeichen)                                | Geben Sie die Länge des Codes ein. Die Standardzeichenlänge beträgt sechs.  |
| Codezusammensetzung                                    | Geben Sie an, wie komplex der vom System generierte Code sein soll. Sie können auswählen zwischen:  |

| Name | Beschreibung  |
|------|---|
|      | <ul style="list-style-type: none"> <li>• Lateinische Großbuchstaben (A-Z)</li> <li>• Lateinische Kleinbuchstaben (a-z)</li> <li>• Zahlen (0-9)</li> <li>• Sonderzeichen (!@#...)</li> </ul> |

### Benutzereinstellungen

| Name                           | Beschreibung  |
|--------------------------------|---|
| <b>Benutzer und Gruppen</b>    | <p>Zeigt eine Liste der Benutzer und Gruppen an, die zum XProtect-System hinzugefügt wurden.</p> <p>Wenn eine Gruppe in Active Directory konfiguriert ist, bezieht der Mobile Server Informationen wie E-Mail-Adressen aus Active Directory.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #0070c0;">  <p>Windows-Gruppen unterstützen die zweistufige Verifikation nicht.</p> </div> |
| <b>Verifizierungsverfahren</b> | <p>Wählen Sie für jeden Benutzer und jede Gruppe eine Verifikationseinstellung aus. Sie können auswählen zwischen:</p> <ul style="list-style-type: none"> <li>• <b>Keine Anmeldung:</b> der Benutzer kann sich nicht anmelden</li> <li>• <b>Keine zweistufige Verifikation:</b> der Benutzer muss Benutzername und Passwort eingeben</li> <li>• <b>E-Mail:</b> der Benutzer muss zusätzlich zu Benutzername und Passwort einen Prüfcode eingeben</li> </ul>   |
| <b>Benutzerdetails</b>         | <p>Geben Sie die E-Mail-Adresse ein, an die jedem Benutzer Codes geschickt werden.</p>  |

## Direktes Streaming (Erklärung)

XProtect Mobile unterstützt das direkte Streaming im Live-Modus (nur für XProtect Expert und XProtect Corporate).

Direct Streaming ist eine Video-Streaming-Technologie, bei der Videoaufzeichnungen von einem XProtect-System auf Clients direkt im Codec H.264 übertragen werden, das von den meisten modernen IP-Kameras unterstützt wird. Für Direct Streaming ist kein Transcoding erforderlich, so dass das XProtect-System teilweise entlastet wird.

Die Direct-Streaming-Technologie steht im Gegensatz zur Einstellung für Transcoding in XProtect, bei dem ein XProtect-System Videoaufzeichnungen von dem Codec, welches die Kamera verwendet, in JPEG-Dateien umwandelt. Die Aktivierung dieser Funktion führt zu einer geringeren CPU-Auslastung bei gleicher Konfiguration der Kameras und Videostreams. Direct Streaming erhöht auch die Leistung für dieselbe Hardware – bis zu fünfmal so viele gleichzeitige Videostreams Vergleich zum Transcoding.

Sie können auch mit der Funktion Direct Streaming Videoaufzeichnungen von Kameras direkt zum XProtect Mobile Client übertragen, die das Codec H.265 unterstützen.

In Management Client können Sie Direct Streaming für Clients aktivieren oder deaktivieren (siehe [Einstellungen des mobilen Servers auf Seite 17](#)).

#### **Der Videostream geht vom Direct Streaming zum Transcoding zurück, wenn:**

- Die Funktion Direct Streaming wurde in Management Client deaktiviert, oder die Anforderungen wurden nicht erfüllt (siehe [Anforderungen für direktes Streaming auf Seite 12](#))
- Das Codec der Streamingkamera unterscheidet sich von H.264 (für alle Clients) oder H.265 (nur für den XProtect Mobile-Client)
- Das Video kann mehr als 10 Sekunden lang nicht abgespielt werden
- Die Bildrate der Streamingkamera ist auf **einen** Frame pro Sekunde (1 FPS) eingestellt
- Die Verbindung zum Server oder mit der Kamera wurde unterbrochen
- Sie verwenden bei Live Videos die Funktion zur und Unkenntlichmachung geschützter Inhalte

## **Adaptives Streaming (Erklärung)**

XProtect Mobile unterstützt adaptives Streaming im Live-Modus (nur für XProtect Expert und XProtect Corporate).

Adaptives Streaming ist nützlich, wenn Sie mehrere Live-Videostreams in derselben Kameraansicht betrachten. Die Funktion optimiert die Leistung des XProtect Mobile-Servers und verbessert die Dekodierfähigkeit und -leistung von Geräten, auf denen XProtect Mobile-Client und XProtect Web Client laufen.

Um adaptives Streaming zu nutzen, müssen in Ihren Kameras mehrere Streams mit unterschiedlicher Auflösung definiert sein. In diesem Fall erlaubt Ihnen die Funktion:

- Die Videoqualität zu optimieren - hierzu wird der Stream mit der geringsten verfügbaren Auflösung ausgewählt, die der geforderten Auflösung entspricht oder darüber liegt
- Auflösung für geringe Bandbreiten optimieren - hierbei wird der Stream mit der geringsten verfügbaren

Auflösung ausgewählt (dies wird bei Verwendung von 3G oder instabilem Netz empfohlen)

- Auflösung für geringe Bandbreiten optimieren - hierbei wird der Stream mit der geringsten verfügbaren Auflösung ausgewählt (dies wird bei Verwendung von 3G oder instabilem Netz empfohlen)



Beim Zoomen ist der geforderte Live-Videostream stets derjenige mit der höchsten verfügbaren Auflösung.



Die Nutzung der Bandbreite wird oft gesenkt, wenn die Auflösung der angeforderten Streams reduziert wird. Die Ausnutzung der Bandbreite ist außerdem abhängig von weiteren Einstellungen in der Konfiguration der angegebenen Streams.

Sie können adaptives Streaming aktivieren oder deaktivieren und Ihren bevorzugten Streamingmodus für die Funktion auf der Registerkarte **Leistung** der Einstellungen für den Mobile Server in Management Client einstellen (siehe [Einstellungen des mobilen Servers auf Seite 17](#)).

## Sichere Kommunikation (Erläuterung).

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 die sichere Kommunikation dadurch hergestellt, dass SSL/TLS mit asymmetrischer Verschlüsselung (RSA) verwendet wird.

Das SSL/TLS-Protokoll verwendet zwei Schlüssel—einer privat, einer öffentlich—zur Authentifizierung, Sicherung und Verwaltung sicherer Verbindungen.

Eine Zertifizierungsstelle (Certificate Authority (CA)) kann Web-Diensten auf Servern mithilfe eines CA-Zertifikates Zertifikate ausstellen. 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. Client und Server können jetzt mit den öffentlichen und privaten Serverzertifikaten einen geheimen Schlüssel austauschen und somit eine sichere SSL/TLS-Verbindung herstellen.

Weitere Informationen zu TLS finden Sie unter [https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)



Zertifikate haben ein Verfalldatum. XProtect VMS gibt Ihnen keine Wawrnung, 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

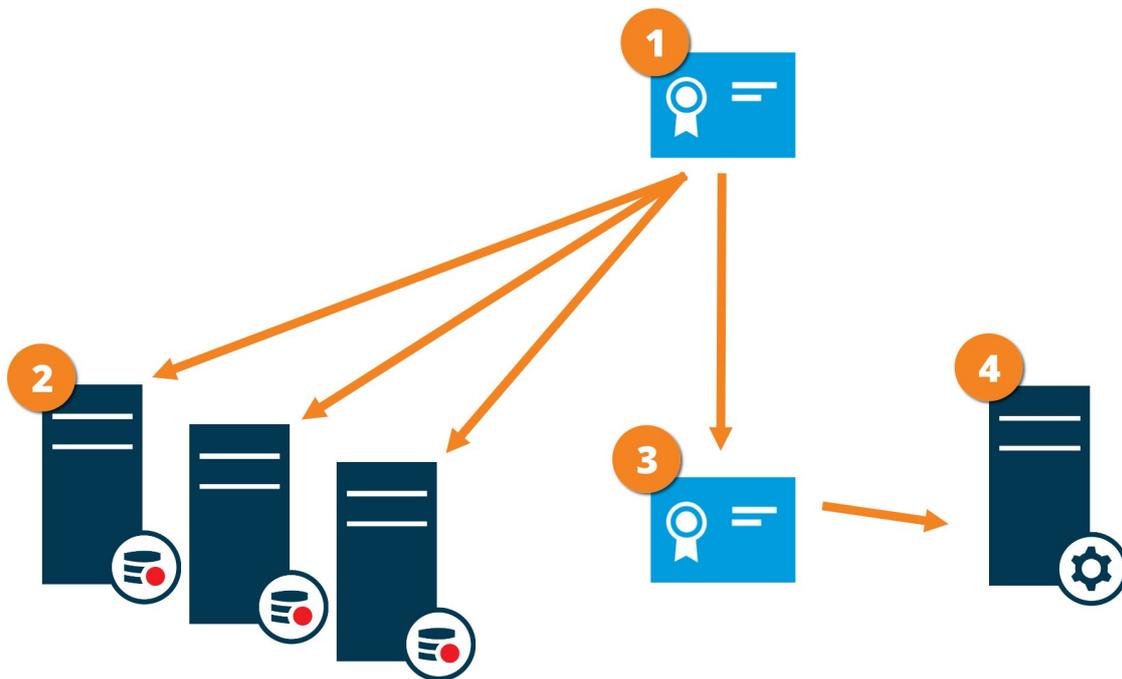
Um die Zertifikate zu erneuern, folgen Sie den Schritten in dieser Anleitung, wie Sie es bereits getan haben, als Sie Zertifikate erstellt haben.

## Verschlüsselung des Managementervers (Erläuterung)

Sie können die wechselseitige Verbindung zwischen dem Managementserver und dem Aufzeichnungsserver verschlüsseln. Wenn Sie die Verschlüsselung auf dem Managementserver aktivieren, so gilt diese für die Verbindungen von allen Aufzeichnungsservern, die eine Verbindung zum Managementserver herstellen. Wenn Sie die Verschlüsselung auf dem Managementserver aktivieren, müssen Sie auch auf allen Aufzeichnungsservern die Verschlüsselung aktivieren. Bevor Sie die Verschlüsselung aktivieren, müssen Sie auf dem Managementserver und auf allen Aufzeichnungsservern Sicherheitszertifikate installieren.

### Verteilung von Zertifikaten für Managementserver

Die Grafik illustriert das zugrundeliegende Konzept dafür, wie Zertifikate signiert werden, wie ihnen vertraut wird, und wie diese in XProtect VMS verteilt werden, um die Kommunikation zum Managementserver zu sichern.



- 1 Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl das Thema/der Eigentümer (Managementserver) vertraut, als auch die Partei, die das Zertifikat überprüft (Aufzeichnungsserver)
- 2 Dem CA-Zertifikat muss auf allen Aufzeichnungsservern vertraut werden. Auf diese Weise können die Aufzeichnungsserver die Gültigkeit der von der CA ausgegebenen Zertifikate überprüfen.
- 3 Das CS-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen dem Managementserver und den Aufzeichnungsservern
- 4 Das CA-Zertifikat muss auf dem Computer installiert werden, auf dem der Managementserver läuft

Anforderungen für das private Zertifikat des Managementsservers:

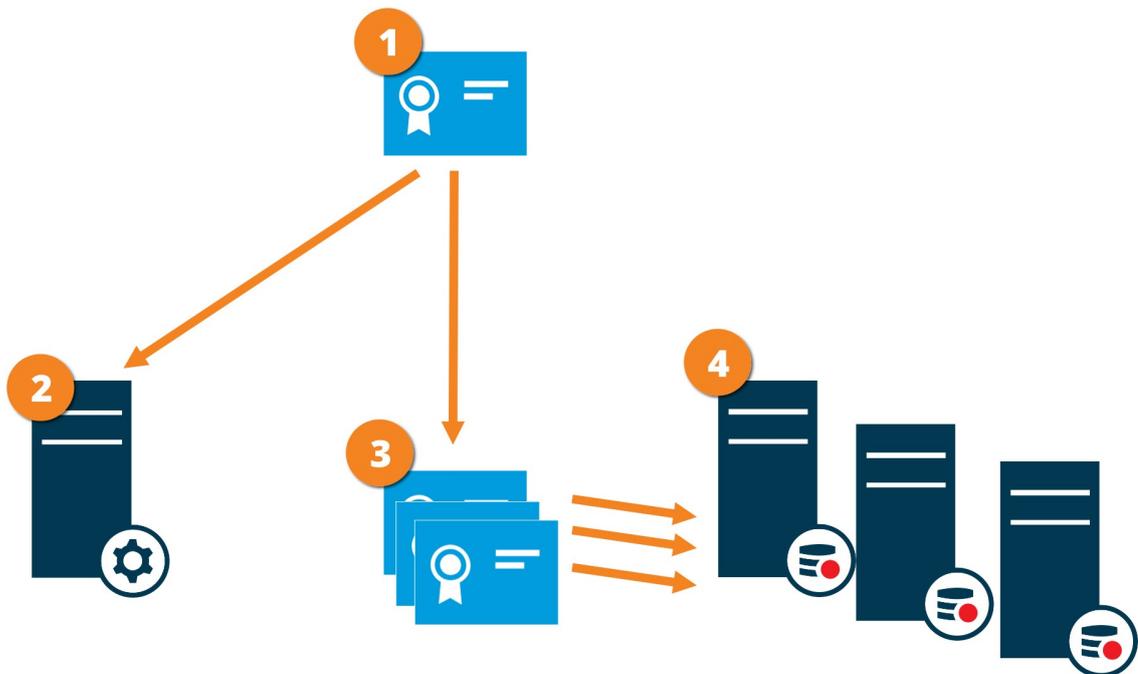
- Wird dem Aufzeichnungsserver ausgestellt, damit der Hostname des Aufzeichnungsservers im Namen des Zertifikates enthalten ist, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, an die das Zertifikat ausgegeben wird
- Wird auf dem Managementserver selbst vertraut, indem dem CA-Zertifikat vertraut wird, das zur Ausstellung des Zertifikates für den Aufzeichnungsserver verwendet wurde.
- Ihm wird auf allen Aufzeichnungsservern vertraut, die mit dem Managementserver verbunden sind, indem dem CA-Zertifikat vertraut wird, das zur Ausstellung des Zertifikates für den Aufzeichnungsserver verwendet wurde.

## Verschlüsselung vom Management-Server zum Aufzeichnungsserver (Erläuterung)

Sie können die wechselseitige Verbindung zwischen dem Managementserver und dem Aufzeichnungsserver verschlüsseln. Wenn Sie die Verschlüsselung auf dem Managementserver aktivieren, so gilt diese für die Verbindungen von allen Aufzeichnungsservern, die eine Verbindung zum Managementserver herstellen. Die Verschlüsselung dieser Kommunikation muss nach den Einstellungen für die Verschlüsselung auf dem Management-Server erfolgen. Wenn also die Verschlüsselung auf dem Managementserver aktiviert ist, muss sie auch auf den Aufzeichnungsservern aktiviert sein und umgekehrt. Bevor Sie die Verschlüsselung aktivieren, müssen Sie auf dem Management-Server und auf allen Aufzeichnungsservern Sicherheitszertifikate installieren, einschließlich der Failover-Aufzeichnungsserver.

### Verteilung von Zertifikaten

Die Grafik illustriert das zugrundeliegende Konzept dafür, wie Zertifikate signiert werden, wie ihnen vertraut wird, und wie diese in XProtect VMS verteilt werden, um die Kommunikation vom Managementserver zu sichern.



- 1** Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl Thema/Eigentümer (Aufzeichnungsserver) vertraut, als auch die Partei, die das Zertifikat überprüft (Management-Server)
- 2** Dem öffentlichen CA-Zertifikat muss auf dem Management-Server vertraut werden. So kann der Aufzeichnungsserver die Gültigkeit der von der CA ausgegebenen Zertifikate überprüfen.
- 3** Das CA-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen den Aufzeichnungsservern und dem Managementserver

4 Das CA-Zertifikat muss auf den Computern installiert werden, auf denen die Aufzeichnungsserver laufen

Anforderungen für das Zertifikat des privaten Aufzeichnungsservers:

- Es wird dem Aufzeichnungsserver ausgestellt, damit der Hostname des Aufzeichnungsservers im Zertifikat enthalten ist, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, an die das Zertifikat ausgegeben wird
- Ihm wird auf dem Managementserver vertraut, indem dem CA-Zertifikat vertraut wird, das bei der Ausstellung des Zertifikates für den Aufzeichnungsserver verwendet wurde.

## Verschlüsselung zwischen dem Management Server und den Data Collector server (Erläuterung)

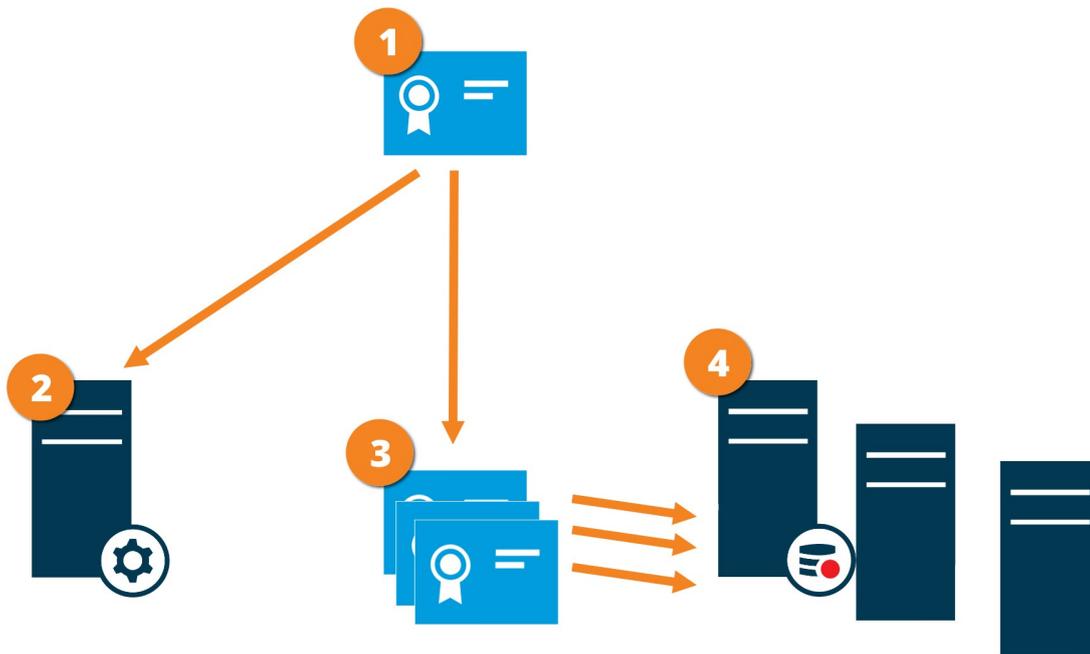
Sie können die wechselseitige Verbindung zwischen dem Managementserver und dem davon abhängigen Data Collector verschlüsseln, wenn Sie einen Remote Server des folgenden Typs haben:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

Wenn Sie die Verschlüsselung auf dem Managementserver aktivieren, so gilt diese für die Verbindungen von allen Data Collector-Servern, die eine Verbindung zum Managementserver herstellen. Die Verschlüsselung dieser Kommunikation muss nach den Einstellungen für die Verschlüsselung auf dem Management-Server erfolgen. Wenn also die Verschlüsselung auf dem Managementserver aktiviert ist, muss sie auch auf den Data Collector-Servern aktiviert sein, die mit jedem der Remote Server verbunden sind, und umgekehrt. Bevor Sie die Verschlüsselung aktivieren, müssen Sie auf dem Managementserver und auf allen Data Collector-Servern, die mit Remote Servern verknüpft sind, Sicherheitszertifikate installieren.

### Verteilung von Zertifikaten

Die Grafik illustriert das zugrundeliegende Konzept dafür, wie Zertifikate signiert werden, wie ihnen vertraut wird, und wie diese in XProtect VMS verteilt werden, um die Kommunikation vom Managementserver zu sichern.



- 1 Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl Thema/Eigentümer (Datensammlerserver) vertrauen als auch die Partei, die das Zertifikat überprüft (Management Server)
- 2 Dem öffentlichen CA-Zertifikat muss auf dem Management-Server vertraut werden. So kann der Aufzeichnungsserver die Gültigkeit der von der CA ausgegebenen Zertifikate überprüfen.
- 3 Das CA-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen den Datensammlungsservern und dem Managementserver
- 4 Das CA-Zertifikat muss auf den Computern installiert werden, auf denen die Datensammlerserver laufen

Anforderungen für das Zertifikat des privaten Datensammlerserver:

- Es wird dem Server ausgestellt, damit der Hostname des Datensammlerservers im Zertifikat enthalten ist, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, denen das Zertifikat ausgestellt wird
- Ihm wird auf dem Managementserver vertraut, indem dem CA-Zertifikat vertraut wird, das bei der Ausstellung des Zertifikates für den Datensammlungsserver verwendet wurde.

## Verschlüsselung an alle Clients und Dienste, die Daten vom Aufzeichnungsserver abrufen (Erläuterung)

Wenn Sie auf einem Aufzeichnungsserver die Verschlüsselung aktivieren, wird die Kommunikation aller Clients, Server und Integrationen verschlüsselt, die Datenstreams vom Aufzeichnungsserver abrufen. Diese werden in diesem Dokument als 'Clients' bezeichnet:

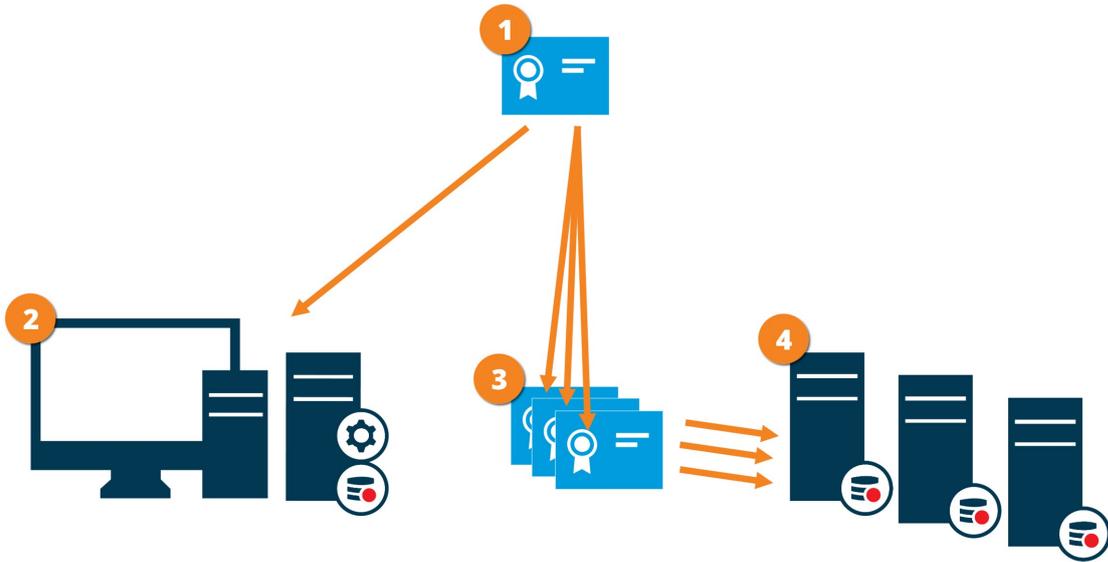
- XProtect Smart Client
- Management Client
- Management Server (für Systemmonitor und für Bilder und AVI-Videoclips in email notifications)
- XProtect Mobile Server
- XProtect Event Server
- XProtect LPR
- Milestone Open Network Bridge
- XProtect DLNA Server
- Seiten, die Datenstreams vom Aufzeichnungsserver abrufen durch Milestone Interconnect
- Manche der MIP SDK Integrationen von Drittanbietern



Für Lösungen, die mit MIP SDK 2018 R3 oder früher gebaut wurden, die auf Aufzeichnungsserver zugreifen: Wenn die Integrationen mithilfe von MIP SDK Bibliotheken erfolgen, müssen sie mit MIP SDK 2019 R1 wieder aufgebaut werden; wenn die Integrationen direkt mit den Aufzeichnungsserver-APIs kommunizieren, ohne MIP SDK Bibliotheken zu verwenden, müssen die Integratoren selbst HTTPS-Support hinzufügen.

### **Verteilung von Zertifikaten**

Die Grafik illustriert das zugrundeliegende Konzept dafür, wie Zertifikate signiert werden, wie ihnen vertraut wird, und wie diese in XProtect VMS verteilt werden, um die Kommunikation zum Aufzeichnungsserver zu sichern.



- 1** Ein CA fungiert als vertrauenswürdiger Dritter, dem sowohl Thema/Eigentümer (Aufzeichnungsserver) vertrauen, als auch die Partei, die das Zertifikat überprüft (alle Clients)
- 2** Dem öffentlichen CA-Zertifikat muss auf allen Clientcomputern vertraut werden. So können die Clients die Gültigkeit der von der CA ausgegebenen Zertifikate überprüfen
- 3** Das CA-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen den Aufzeichnungsservern und allen Clients und Diensten
- 4** Das CA-Zertifikat muss auf den Computern installiert werden, auf denen die Aufzeichnungsserver laufen

Anforderungen für das Zertifikat des privaten Aufzeichnungsservers:

- Es wird dem Aufzeichnungsserver ausgestellt, damit der Hostname des Aufzeichnungsservers im Zertifikat enthalten ist, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, an die das Zertifikat ausgegeben wird
- Ihm wird von allen Computern vertraut, die Dienste ausführen, die Datenstreams von Aufzeichnungsservern abrufen, indem sie dem CA-Zertifikat vertrauen, das bei der Aufstellung des Aufzeichnungsserverzertifikates verwendet wurde
- Das Dienstkonto, auf dem der Aufzeichnungsserver läuft, muss Zugriff zum privaten Schlüssel des Zertifikates auf dem Aufzeichnungsserver haben.



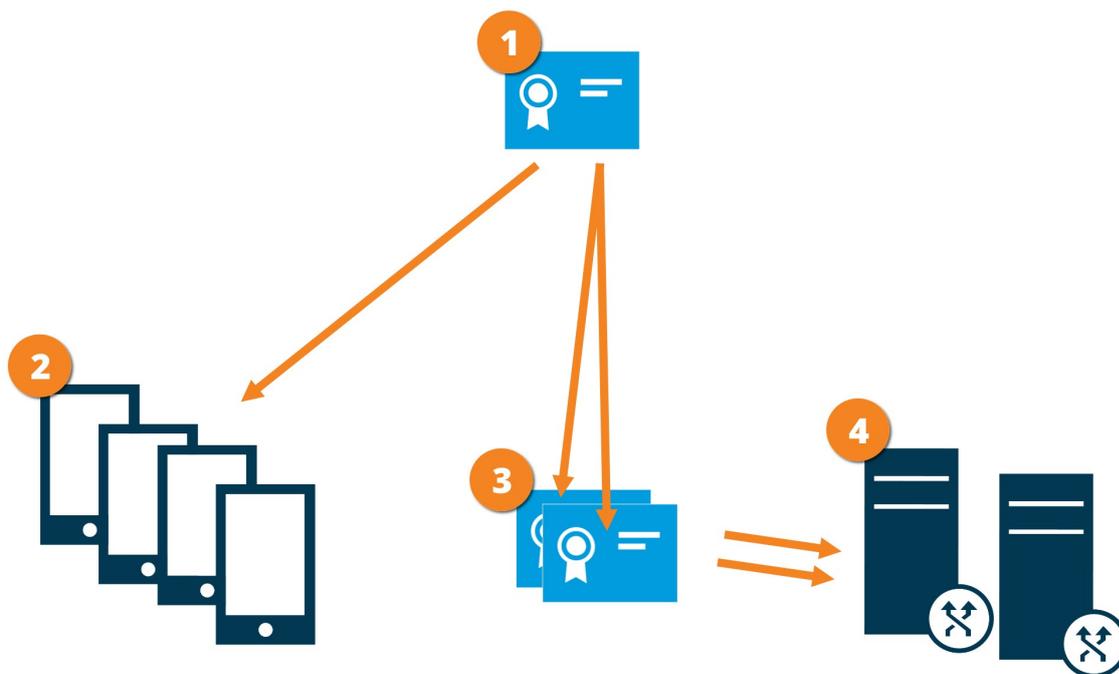
Wenn Sie auf den Aufzeichnungsservern die Verschlüsselung aktivieren, und Ihr System verwendet Failover-Aufzeichnungsserver, so empfiehlt Milestone, dass Sie die Failover-Aufzeichnungsserver ebenfalls dafür vorbereiten, dass sie eine Verschlüsselung verwenden.

## Datenverschlüsselung des mobilen Servers (Erläuterung)

In XProtect VMS wird die Verschlüsselung für jeden mobilen Server aktiviert oder deaktiviert. Wenn Sie die Verschlüsselung auf einem mobilen Server aktivieren, so können Sie sich aussuchen, ob Sie die verschlüsselte Kommunikation mit allen Clients, Diensten und Integrationen verwenden wollen, die Datenstreams abrufen.

### Verteilung von Zertifikaten für mobile Server

Die Grafik illustriert das zugrundeliegende Konzept dafür, wie Zertifikate signiert werden, wie ihnen vertraut wird, und wie diese in XProtect VMS verteilt werden, um die Kommunikation mit dem mobilen Server zu sichern.



- 1 Eine CA fungiert als vertrauenswürdiger Dritter, dem sowohl das Thema/der Eigentümer (mobiler Server) vertraut, als auch die Partei, die das Zertifikat überprüft (alle Clients).
- 2 Dem öffentlichen CA-Zertifikat muss auf allen Clientcomputern vertraut werden. Auf diese Weise können die Clients die Gültigkeit der von der CA ausgegebenen Zertifikate überprüfen

3 Das CA-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen dem Mobile Server und den Clients und Diensten

4 Das CA-Zertifikat muss auf dem Computer installiert werden, auf dem der mobile Server läuft

#### **Anforderungen für das CA-Zertifikat:**

- Der Hostname des mobilen Servers muss im Zertifikates enthalten sein, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, an die das Zertifikat ausgegeben wird
- Dem Zertifikat muss von allen Computern vertraut werden, die Dienste ausführen, die Datenstreams vom mobilen Server abrufen
- Das Dienstkonto, auf dem der Aufzeichnungsserver läuft, muss Zugriff zum privaten Schlüssel des CA-Zertifikates haben.

#### **Anforderungen zur Verschlüsselung mobiler Server für Clients**

Aus Sicherheitsgründen empfiehlt Milestone, dass Sie bei der Verwaltung von Benutzerkonteneinstellungen zwischen dem Mobile Server und den Clients eine sichere Kommunikation verwenden.

Wenn Sie die Verschlüsselung nicht aktivieren und keine HTTP-Verbindung verwenden, so steht die Push-to-Talk-Funktion in XProtect Web Client später nicht zur Verfügung.

## **Milestone Federated Architecture und den Master/Slave Servern (Erklärung)**

Wenn Ihr System Unterstützung für Milestone Federated Architecture oder Server in einer Master/Slave-Konfiguration bietet, können Sie mithilfe Ihres XProtect Mobile-Clients oder XProtect Web Client auf diese Server zugreifen. Verwenden Sie diese Funktionalität, um Zugriff auf alle Kameras auf allen Slave-Servern zu erhalten, indem Sie sich beim Master-Server anmelden.

In einer Milestone Federated Architecture-Konfiguration erhalten Sie über den zentralen Standort Zugriff auf untergeordnete Standorte. Installieren Sie den XProtect Mobile-Server nur auf dem zentralen Standort.

Wenn sich Benutzer des XProtect Mobile-Clients oder XProtect Web Client bei einem Server anmelden, um alle Kameras auf allen Servern in Ihrem System anzuzeigen, müssen sie dafür eine Verbindung zur IP-Adresse des Master-Servers herstellen. Damit die Kameras im XProtect Mobile-Client oder XProtect Web Client angezeigt werden, müssen Benutzer für alle Server im System über Administratorrechte verfügen.

## **Smart Connect (Erklärung)**

Mit Smart Connect können Sie ohne Anmeldung mit einem Mobilgerät oder Tablet überprüfen, ob der XProtect Mobile-Server richtig konfiguriert wurde. Außerdem vereinfacht es den Verbindungsvorgang für die XProtect Mobile-Client- und XProtect Web Client-Benutzer.

Dieses Feature setzt voraus, dass Ihr XProtect Mobile-Server eine öffentliche IP-Adresse verwendet und Ihr System über eine Lizenz für ein Milestone Care Plus-Abonnementpaket verfügt.

Das System zeigt im Management Client sofort an, wenn die Konfiguration der Remoteverbindung erfolgreich war, und bestätigt, dass der XProtect Mobile-Server über das Internet erreichbar ist.

Mit Smart Connect kann der XProtect Mobile-Server nahtlos zwischen internen und externen IP-Adressen umschalten und von jedem Ort aus eine Verbindung zum XProtect Mobile-Server herstellen.

Um Kunden die Einrichtung von Mobile Clients zu erleichtern, können Sie direkt über den Management Client eine E-Mail an den Endbenutzer senden. Die E-Mail enthält einen Link, der den Server direkt zu XProtect Mobile hinzufügt. Die Einrichtung wird erledigt, ohne dass Netzwerkadressen oder Ports angegeben werden müssen.

## Einrichten von Smart Connect

Um die Smart-Connect-Funktion einzurichten, gehen Sie wie folgt vor:

1. Erweitern Sie in Management Client im Navigationsbereich das Feld **Server** und wählen Sie **Mobile Server** aus.
2. Wählen Sie den mobilen Server aus und klicken Sie auf die Registerkarte **Konnektivität**.
3. Aktivieren Sie die UPnP-Erkennungsfunktion Ihres Routers.
4. Konfigurieren Sie die Verbindungseinstellungen.
5. Senden Sie eine E-Mail-Nachricht an die Benutzer.
6. Aktivieren Sie Verbindungen im komplexen Netzwerk.

## Aktivieren Sie die UPnP-Erkennungsfunktion in Ihrem Router

Um das Verbinden von Mobilgeräten mit XProtect Mobile-Servern zu vereinfachen, können Sie die Funktion Universal Plug and Play (UPnP) in Ihrem Router aktivieren. Mit UPnP kann der XProtect Mobile-Server Port Forwarding automatisch konfigurieren. Sie können die Portweiterleitung aber auch manuell über die Weboberfläche Ihres Routers einrichten. Der Einrichtungsvorgang kann sich von Router zu Router unterscheiden. Wenn Sie Hilfe bei der Einrichtung der Portweiterleitung für Ihren Router benötigen, ziehen Sie die Dokumentation für das jeweilige Gerät zu Rate.



Der XProtect Mobile Server-Dienst überprüft alle fünf Minuten, ob der Server für Benutzer im Internet verfügbar ist. Der Status wird in der oberen linken Ecke im Bereich

**Eigenschaften** angezeigt:

Server accessible through internet: 

## Aktivieren von Verbindungen im komplexen Netzwerk

Wenn Sie ein komplexes Netzwerk haben, in dem benutzerdefinierte Einstellungen vorliegen, können Sie die Informationen angeben, die Benutzer für die Verbindung benötigen.

Nehmen Sie auf der Registerkarte **Verbindungen** in der Gruppe **Internetzugriff** folgende Eingaben vor:

- Wenn Sie die UPnP-Portzuordnung verwenden, um Verbindungen an eine bestimmte Verbindung weiterzuleiten, aktivieren Sie das Kontrollkästchen **Benutzerdefinierten Internetzugriff konfigurieren**. Geben Sie dann die **IP-Adresse oder den Hostnamen** und den für die Verbindung zur verwendenden Port an. Dies können Sie z.B. tun, wenn Ihr Router kein UPnP unterstützt oder wenn Sie eine Routerkette haben
- Wenn sich Ihre IP-Adressen häufig ändern, aktivieren Sie das Kontrollkästchen **Aktivieren, um IP-Adresse dynamisch abzurufen**

## Konfigurieren der Verbindungseinstellungen

1. Erweitern Sie in Management Client im Navigationsbereich das Feld **Server** und wählen Sie **Mobile Server** aus.
2. Wählen Sie den Server aus und klicken Sie auf die Registerkarte **Konnektivität**.
3. Verwenden Sie die Optionen in der Gruppe **Allgemein**, um folgende Angaben zu machen:
  - Um XProtect Mobile Client und XProtect Web Client Benutzern die Verbindungsherstellung zwischen Mobilgeräten und XProtect Mobile-Servern zu erleichtern, markieren Sie das Kontrollkästchen **Smart Connect aktivieren**.
  - Legen Sie mithilfe eines Timeline Areas fest, wie oft der XProtect Mobile-Client und XProtect Web Client dem mobilen Server anzeigen müssen, dass sie betriebsbereit sind.
  - Um die XProtect Mobile-Server im Netzwerk mittels des UPnP Protokolle sichtbar zu machen, markieren Sie das Kontrollkästchen **UPnP-Entdeckbarkeit aktivieren**
  - Um zu aktivieren, dass der XProtect Mobile-Server die Portzuordnung selbst vornimmt, wenn der Router dafür konfiguriert ist, markieren Sie das Kontrollkästchen **Automatische Portzuordnung aktivieren**

## Senden einer E-Mail-Nachricht an Benutzer

Um Kunden die Einrichtung von XProtect Mobile Client und XProtect Web Client zu erleichtern, können Sie direkt über den Management Client eine E-Mail an den Endbenutzer senden. Die E-Mail enthält einen Link, der den Server direkt zu XProtect Mobile hinzufügt. Die Einrichtung wird erledigt, ohne dass Netzwerkadressen oder Ports angegeben werden müssen.

1. Geben Sie im Feld **E-Mail-Einladung an** die E-Mail-Adresse des Empfängers der Smart-Connect-Benachrichtigung ein und wählen Sie eine Sprache aus.
2. Gehen Sie anschließend wie folgt vor:
  - Klicken Sie auf **Senden**, um die Nachricht zu versenden
  - Kopieren Sie die Informationen in das Messaging-Programm, das Sie verwenden

Für weitere Informationen, siehe:

[Anforderungen für das Einrichten von Smart Connect auf Seite 12](#)

[Registerkarte Konnektivität auf Seite 20](#)

## Senden von Benachrichtigungen (Erklärung)

Sie können einstellen, dass XProtect Mobile Benutzer über Ereignisse benachrichtigt, z. B. wenn ein Alarm ausgelöst wird oder ein Fehler mit einem Gerät oder Server auftritt. Benachrichtigungen werden immer zugestellt, auch wenn die App nicht ausgeführt wird. Wenn XProtect Mobile auf dem Mobilgerät geöffnet ist, wird die Benachrichtigung in der App zugestellt. Auch Systembenachrichtigungen werden zugestellt, wenn die App nicht ausgeführt wird. Benutzer können festlegen, welche Benachrichtigungsarten sie erhalten möchten. Dabei hat ein Benutzer z. B. folgende Auswahlmöglichkeiten:

- Alle Alarme
- Nur Alarme, die dem Benutzer zugeordnet sind
- Nur Systemalarme

Diese werden z. B. ausgelöst, wenn ein Server offline oder wieder online geschaltet wird.

Um Benutzer zu benachrichtigen, die XProtect Mobile nicht geöffnet haben, können Sie sogenannte Push-Benachrichtigungen verwenden. Push-Benachrichtigungen werden an das Mobilegerät gesendet und eignen sich sehr gut dafür, die Benutzer unterwegs zu informieren.

### Verwenden von Push-Benachrichtigungen



Zur Nutzung von Push-Benachrichtigungen muss Ihr System über Internetzugriff verfügen.

Push-Benachrichtigungen verwenden Clouddienste von Apple, Microsoft und Google:

- Apple Push Notification-Service (APN)
- Microsoft Azure Notification Hub
- Google Cloud Messaging Push Notification-Dienst

Ihr System darf in einem bestimmten Zeitabschnitt nur eine begrenzte Anzahl von Benachrichtigungen versenden. Wenn Ihr System diesen Grenzwert überschreitet, kann es im nächsten Zeitabschnitt nur alle 15 Minuten eine Benachrichtigung versenden. Die Benachrichtigung enthält dann eine Zusammenfassung der Ereignisse, die in diesen 15 Minuten aufgetreten sind. Nach dem nächsten Zeitabschnitt wird diese Beschränkung wieder aufgehoben.

Siehe auch [Anforderungen für das Einrichten von Benachrichtigungen auf Seite 11](#) und [Registerkarte Benachrichtigungen auf Seite 29](#).

## Konfigurieren von Push-Benachrichtigungen auf dem XProtect Mobile-Server

So konfigurieren Sie Push-Benachrichtigungen:

1. Wählen Sie im Management Client den mobilen Server aus und klicken Sie auf die Registerkarte **Benachrichtigungen**.
2. Aktivieren Sie das Kontrollkästchen **Benachrichtigungen**, damit Benachrichtigungen an alle Mobilgeräte gesendet werden, die eine Verbindung zum Server herstellen.
3. Aktivieren Sie das Kontrollkästchen **Geräteregistrierung beibehalten**, um Informationen über die Benutzer und Mobilgeräte zu speichern, die eine Verbindung zum Server herstellen.



Der Server sendet Benachrichtigungen nur an die Mobilgeräte in dieser Liste. Wenn Sie das Kontrollkästchen **Geräteregistrierung beibehalten** deaktivieren und die Änderung speichern, wird die Liste vom System gelöscht. Um anschließend erneut Push-Benachrichtigungen zu erhalten, müssen Benutzer eine erneute Verbindung mit ihrem Gerät herstellen.

## Aktivieren von Push-Benachrichtigungen für bestimmte oder alle Mobilgeräte

Um zu aktivieren, dass XProtect Mobile Benutzer per Push-Nachricht an bestimmte oder alle Mobilgeräte benachrichtigt werden, wenn ein Ereignis eintritt:

1. Wählen Sie im Management Client den mobilen Server aus und klicken Sie auf die Registerkarte **Benachrichtigungen**.
2. Gehen Sie wie folgt vor:
  - Wählen Sie für Einzelgeräte das Kontrollkästchen **Aktiviert** für jedes Mobilgerät aus, das in der Tabelle **Angemeldete Geräte** aufgelistet ist
  - Für alle Mobilgeräte aktivieren Sie das Kontrollkästchen **Benachrichtigungen**

## Deaktivieren des Sendens von Push-Benachrichtigungen an bestimmte oder alle Mobilgeräte

Sie haben mehrere Möglichkeiten, um das Versenden von Push-Benachrichtigungen an bestimmte oder alle Mobilgeräte zu deaktivieren.

1. Wählen Sie im Management Client den mobilen Server aus und klicken Sie auf die Registerkarte **Benachrichtigungen**.
2. Gehen Sie wie folgt vor:
  - Um die Funktion für einzelne Geräte zu beenden, müssen Sie das Kontrollkästchen **Aktiviert** für jedes Mobilgerät einzeln deaktivieren. Der Benutzer kann mit einem anderen Gerät eine Verbindung zum XProtect Mobile-Server herstellen.
  - Um die Funktion für alle Geräte zu beenden, müssen Sie das Kontrollkästchen **Benachrichtigungen** deaktivieren

Wenn Sie die Push-Funktion vorübergehend für alle Geräte beenden möchten, deaktivieren Sie das Kontrollkästchen **Geräteregistrierung beibehalten** und speichern Sie die Änderung. Das System sendet wieder Benachrichtigungen, wenn sich die Benutzer neu verbinden.

## Einrichten von Untersuchungen

Richten Sie Untersuchungen ein, damit die Benutzer mit XProtect Web Client oder XProtect Mobile auf Videoaufzeichnungen zugreifen und Zwischenfälle untersuchen können, sowie um Videobeweise vorbereiten und herunterladen zu können.

Folgen Sie diesen Schritten, um Untersuchungen einzurichten:

1. Klicken Sie in Management Client auf den mobilen Server und klicken Sie dann auf die Registerkarte **Untersuchungen**.
2. Aktivieren Sie das Kontrollkästchen **Untersuchungen zulassen**. Dieses Kontrollkästchen ist standardmäßig ausgewählt.
3. Geben Sie im Feld **Untersuchungen-Ordner** einen Speicherort für die Videos an, die für die Untersuchung verwendet werden sollen.
4. Optional: Wenn Sie möchten, dass Benutzer auf von anderen Benutzern erstellte Untersuchungen zugreifen können, aktivieren Sie das Kontrollkästchen **Untersuchungen anzeigen, die von anderen Benutzern durchgeführt werden** aus. Wenn das Kontrollkästchen nicht ausgewählt ist, können Benutzer nur ihre eigenen Untersuchungen sehen.
5. Aktivieren Sie dieses Kontrollkästchen **Größe des Untersuchungsordners begrenzen**, um die maximale Anzahl Megabyte anzugeben, die der Untersuchungsordner enthalten darf.
6. Aktivieren Sie das Kontrollkästchen **Speicherdauer für Untersuchungen aktivieren**, um eine Speicherdauer für Untersuchungen festzulegen. Die Standardspeicherdauer beträgt sieben Tage.
7. Aktivieren Sie unter **Exportformate** das Kontrollkästchen für das Exportformat, das Sie verwenden möchten. Folgende Exportformate stehen zur Verfügung:
  - **AVI-Format**
  - **XProtect Format**
  - **MKV-Format**



Die Kontrollkästchen sind standardmäßig leer.

8. (Optional) Um das Datum und die Uhrzeit mit festzuhalten, an dem das Video heruntergeladen wurde, aktivieren Sie das Kontrollkästchen **Zeitstempel für AVI-Exporte mit einschließen**.

9. Wählen Sie im Feld **Codec für AVI-Exporte verwenden** das Komprimierungsformat für die Downloadvorbereitung von AVI-Paketen aus.



Abhängig vom Betriebssystem, das Sie verwenden, enthält die Liste unterschiedliche Codecs. Wenn in der Liste der von Ihnen gesuchte Codec fehlt, können sie ihn auf dem Computer installieren, auf dem Management Client ausgeführt wird. Danach wird er in der Liste angezeigt.



Codecs können verschiedene Komprimierungsraten verwenden, die Einfluss auf die Videoqualität haben. Höhere Komprimierungsraten sparen Speicherplatz, reduzieren dafür aber die Qualität. Niedrigere Kompressionsraten belegen mehr Speicherplatz und belasten das Netzwerk stärker, liefern aber eine höhere Qualität. Am besten informieren Sie sich über die einzelnen Codecs, bevor Sie sich für einen entscheiden.

10. Wählen Sie aus der Liste **Verwendete Bitrate für AVI-Exporte** die entsprechende Audio-Bitrate aus, wenn Audio in Ihrem Videoexport enthalten ist. Die Standardeinstellung ist 160000 Hz.



Damit Benutzer Untersuchungen speichern können, müssen Sie ihnen die **Exportieren**-Berechtigung zuweisen.

### Bereinigen von Untersuchungen

Untersuchungen oder Videoexporte, die Sie nicht mehr benötigen, können Sie auf Wunsch löschen. Auf diese Weise können Sie wieder Speicherplatz auf dem Server freigeben.

- Um eine Untersuchung und alle exportierten Videos zu löschen, die dafür erstellt wurden, wählen Sie auf der Liste die Untersuchung aus und klicken Sie dann auf **Löschen**
- Wenn Sie einzelne, für eine Untersuchung exportierte Videodateien löschen, die Untersuchung selbst aber behalten möchten, wählen Sie zuerst die Untersuchung in der Liste aus. Wählen Sie aus der Gruppe **Untersuchungsdetails** das Symbol **Löschen** rechts von den Feldern **XProtect**, **AVI** oder **MKV** für Exporte aus

## Nutzung von Video Push für Videostreams (Erklärung)

Sie können Push-Video einrichten, so dass die Benutzer andere über eine Situation auf dem Laufenden halten oder ein Video aufzeichnen können, um dieses später zu untersuchen, indem sie Videos von der Kamera ihres mobilen Enderätes auf Ihr XProtect Überwachungssystem streamen. Der Videostream beinhaltet ggf. auch Audio.

Siehe auch [Registerkarte Video Push auf Seite 28](#) und [Anforderungen für das Einrichten von Video Push auf Seite 12](#).

## Einrichten von Video Push für Videostreams

Damit Benutzer Video von ihren Mobilgeräten an das XProtect-System streamen können, müssen Sie Video Push auf dem XProtect Mobile-Server einrichten.

Führen Sie in der Management Client die folgenden Schritte in der angegebenen Reihenfolge aus:

1. Markieren Sie auf der Registerkarte **Video Push** das Kontrollkästchen **Video Push**, um die Funktion zu aktivieren.
2. Fügen Sie einen video push-Kanal für Video-Streaming hinzu.
3. Fügen Sie den Video-Push-Treiber als Hardwaregerät auf dem Recording Server hinzu. Der Treiber simuliert ein Kameragerät, um das Videostreaming an Recording Server zu ermöglichen.
4. Fügen Sie das Video Push-Treibergerät zum video push Kanal hinzu.

## Einen video push-Kanal für Video-Streaming hinzufügen

So fügen Sie einen Kanal hinzu:

1. Wählen Sie im Navigationsbereich **Mobile Server** aus, und wählen Sie dann den Mobile Server aus.
2. Aktivieren Sie auf der Registerkarte **Video Push** das Kontrollkästchen **Video Push**.
3. Klicken Sie unter **Kanal-Mapping** unten links in der Ecke auf **Hinzufügen**, um einen Video-Push-Kanal hinzuzufügen.
4. Geben Sie in die Dialogbox, die dann erscheint, den Benutzernamen für das Benutzerkonto ein (das unter **Rollen** hinzugefügt wird), das den Kanal benutzen soll. Dieses Benutzerkonto muss Zugriff auf den XProtect Mobile-Server und den Aufzeichnungsserver erhalten (auf der Registerkarte **Gesamtsicherheit**.)



Um Video Push zu verwenden, müssen sich Benutzer mit dem Benutzernamen und Passwort für dieses Konto über ihr Mobilgerät bei XProtect Mobile anmelden.



Wenn Sie auf dem Mobile Server einen neuen Video-Push-Kanal hinzufügen, erzeugt das System die Portnummer und die MAC-Adresse des Kanals, die verwendet werden, wenn der Kanal als Hardwaregerät auf dem Aufzeichnungsserver hinzugefügt wird. Das System erzeugt außerdem das Passwort, das für die Verbindung des Recording Server mit dem Mobile Server verwendet wird. Das Standardpasswort ist **Milestone**.

5. Notieren Sie sich die Portnummer. Sie werden diese benötigen, wenn Sie den Video Push-Treiber als

Gerät auf dem Aufzeichnungsserver hinzufügen.

6. Klicken Sie auf **OK**, die Dialogbox zu dem Video-Push-Kanal zu schließen.
7. Um den Kanal zu speichern, klicken Sie links oben in der Ecke des Navigationsfensters auf **Speichern**.

### Einen Video-Push-Kanal bearbeiten

Sie können die Konfigurationsdetails eines Video-Push-Kanals, den Sie hinzugefügt haben, bearbeiten:

1. Wählen Sie unter **Kanal-Mapping** den zu bearbeitenden Kanal aus, und klicken Sie dann auf **Bearbeiten**.
2. Wenn Sie die Bearbeitung abgeschlossen haben, klicken Sie auf **OK**, um die Dialogbox zu dem Video-Push-Kanal zu schließen.
3. Um Bearbeitung des Kanals zu speichern, klicken Sie links oben in der Ecke des Navigationsfensters auf **Speichern**.



Wenn Sie die Portnummer und die MAC-Adresse eines Video-Push-Kanals bearbeiten, achten Sie darauf, auch die Konfigurationsdetails zu dem Video-Push-Kanal, den Sie zuvor auf dem Aufzeichnungsserver hinzugefügt haben, durch die neuen Informationen zu ersetzen. Andernfalls wird die Verbindung zwischen dem Recording Server und dem Mobile Server unterbrochen.

### Einen video push-Kanal entfernen

Kanäle, die Sie nicht mehr benötigen, können entfernt werden:

1. Wählen Sie unter **Kanal-Mapping** den zu entfernenden Kanal aus, und klicken Sie dann auf **Entfernen**.
2. Um die Änderungen zu speichern, klicken Sie links oben in der Ecke des Navigationsfensters auf **Speichern**.

### Passwort ändern

Sie können das automatisch erzeugte Passwort, das für die Verbindung zwischen dem Recording Server und dem Mobile Server verwendet wird, ändern:

1. Klicken Sie unter **Kanal-Mapping** unten rechts in der Ecke auf **Passwort ändern**.
2. Geben Sie in das Dialogfeld **Video-Push-Passwort ändern** das neue Passwort in das erste Feld ein, wiederholen Sie das neue Passwort dann im zweiten Feld und klicken Sie dann auf **OK**.
3. Um die Änderungen zu speichern, klicken Sie links oben in der Ecke des Navigationsfensters auf **Speichern**.



Wenn Sie das Passwort für den Video-Push-Kanal ändern, wird die Änderung auf alle Video-Push-Kanäle angewendet, die bereits aufgeführt sind oder in Zukunft hinzugefügt werden. Auch wenn Sie alle vorhandenen Video-Push-Kanäle von der Liste löschen, bleibt das neue Passwort aktiv und wird auf zukünftige Kanäle angewendet.



Nach dem Abspeichern der Änderungen werden alle vorhandenen Video-Push-Kanäle abgeschaltet, da die Verbindung zwischen dem Recording Server und dem Mobile Server unterbrochen ist. Um diese Verbindung wiederherzustellen, müssen Sie den Assistenten **Hardware ersetzen** ausführen, indem Sie mit der rechten Maustaste auf die Registerkarte **Aufzeichnungsserver** klicken und dann das neue Passwort für den Video-Push-Treiber eingeben, den Sie als Hardwaregerät auf dem Recording Server hinzugefügt haben.

## Den video push-Treiber als Gerät hinzufügen auf dem Recording Server

1. Klicken Sie im Navigationsbereich auf **Aufzeichnungsserver**.
2. Klicken Sie mit der rechten Maustaste auf den Server, an den Sie einen Videostream senden möchten, und klicken Sie dann auf **Hardware hinzufügen**, um den Assistenten **Hardware hinzufügen** zu öffnen.
3. Wählen Sie die Hardware-Erkennungsmethode **Manuell** aus und klicken Sie auf **Weiter**.
4. Geben Sie die Anmeldedaten für die Kamera ein:
  - Benutzername: Geben Sie die werkseitig eingestellten Standardwerte bzw. den auf der Kamera angegebenen Benutzernamen ein
  - Passwort: Geben Sie das **Milestone** - Passwort ein, das vom System erzeugt wird, oder, wenn Sie es beim Hinzufügen des Video-Push-Kanals auf dem Mobile Server geändert haben, geben Sie das von Ihnen bevorzugte Passwort ein, und klicken Sie dann auf **Weiter**



Diese Anmeldedaten gelten für die jeweilige Hardware, nicht für den Benutzer. Die Anmeldedaten sind nicht mit dem Benutzerkonto verknüpft, das für den Zugriff auf den Video-Push-Kanal verwendet wird.

5. Erweitern Sie in der Liste der Treiber **Milestone**, wählen Sie das Kontrollkästchen **Video Push-Treiber** aus und klicken Sie auf **Weiter**.
6. Geben Sie in das Feld **Adresse** die IP-Adresse des Computers ein, auf dem der XProtect Mobile Server installiert ist.



Es wird empfohlen, die vom System erzeugte MAC-Adresse zu verwenden. Diese sollten Sie nur ändern, wenn Sie Probleme mit dem Video-Push-Treibergerät haben, oder wenn Sie z.B. die Portnummer und die MAC-Adresse des Video-Push-Kanals auf dem Mobile Server bearbeitet haben.

7. Geben Sie im Feld **Port** die Portnummer des von Ihnen zum Streamen von Video erstellten Kanals ein. Die Portnummer wurde bei der Erstellung des Kanals zugewiesen.
8. Wählen Sie in der Spalte **Hardwaremodell Video Push-Treiber** aus und klicken Sie auf **Weiter**.
9. Wenn das System die neue Hardware erkannt hat, klicken Sie auf **Weiter**.
10. Geben Sie im Feld **Vorlage für die Hardwarebezeichnung** an, ob entweder das Modell der Hardware und die IP-Adresse angezeigt werden soll, oder nur das Modell.
11. Geben Sie an, ob zugehörige Geräte aktiviert werden sollen, indem Sie das Kontrollkästchen **Aktiviert** aktivieren. Sie können zugehörige Geräte zur Liste für den **Video Push-Treiber** hinzufügen, auch wenn sie nicht aktiviert sind. Sie können diese zu einem späteren Zeitpunkt aktivieren.



Wenn Sie beim Streamen von Video Standortinformationen verwenden möchten, müssen Sie den Port **Metadaten** aktivieren.



Wenn Sie während eines Videostreams Audio abspielen wollen, müssen Sie das Mikrofon aktivieren, das zu der Kamera gehört, von der Sie Video streamen.

12. Wählen Sie auf der linken Seite die Standardgruppen für die zugehörigen Geräte aus oder wählen Sie im Feld **Zur Gruppe hinzufügen** eine bestimmte Gruppe aus. Wenn Sie einer Gruppe Geräte hinzufügen, vereinfacht das möglicherweise die Übernahme von Einstellungen für alle Geräte bzw. das Ersetzen von Geräten.

## Hinzufügen des video push-Treibergeräts zum video push-Kanal

Um das Video Push-Treibergerät zum Video Push-Kanal hinzuzufügen, befolgen Sie diese Schritte:

1. Klicken Sie im Bereich **Standort-Navigation** auf **Mobile Server** und dann auf die Registerkarte **Video Push**.
2. Klicken Sie auf **Kameras suchen**. Bei erfolgreicher Suche wird der Name der Video Push-Treiberkamera im Feld **Kameraname** angezeigt.
3. Speichern Sie Ihre Konfiguration.

## Aktivieren Sie Audio für den vorhandenen Push-Videokanal

Wenn Sie die Anforderungen für die Aktivierung des Tons in Push-Video erfüllt haben (siehe [Anforderungen für das Einrichten von Video Push auf Seite 12](#)), in Management Client:

1. Erweitern Sie im Bereich **Standort-Navigation** den Knoten **Server** und klicken sie dann auf **Aufzeichnungsserver**.
2. Wählen Sie im Bereich "Übersicht" den entsprechenden Aufzeichnungsserver-Ordner, erweitern Sie dann den Ordner **Video Push Driver** und klicken Sie mit der rechten Maustaste auf das Mikrofon für Push-Video.
3. Wählen Sie **Aktivieren** aus, um das Mikrofon zu aktivieren.
4. Wählen Sie im selben Ordner die Kamera für Push-Video aus.
5. Klicken Sie in dem Fensterbereich **Eigenschaften** auf die Registerkarte **Client** (siehe [Registerkarte 'Client' \(Geräte\)](#)).
6. Klicken Sie auf der rechten Seite des Feldes **Zugeordnetes Mikrofon** auf . Es öffnet sich die Dialogbox **Ausgewähltes Gerät**.
7. Erweitern Sie auf der Registerkarte **Aufzeichnungsserver** den Aufzeichnungsserver-Ordner und wählen Sie das Mikrofon für Push-Video aus.
8. Klicken Sie auf **OK**.

## Einrichten von Benutzern für die zweistufige Verifikation über E-Mail



Verfügbare Funktionalität hängt vom verwendeten System ab. Weitere Informationen finden Sie unter <https://www.milestonesys.com/solutions/platform/product-index/>.

Mit der zweistufigen Verifikation auf dem XProtect Mobile-Server können Sie einen zusätzlichen Anmeldeschritt für Benutzer des XProtect Mobile-Clients oder XProtect Web Client festlegen. Zusätzlich zum üblichen Benutzernamen und Passwort muss der Benutzer einen Verifizierungscode eingeben, der per E-Mail zugestellt wird.

Die zweistufige Verifikation verbessert die Sicherheit Ihres Überwachungssystems.

Führen Sie in Management Client die folgenden Schritte aus:

1. [Informationen über den SMTP-Server eingeben auf Seite 56](#).
2. [Den Verifizierungscode festlegen, der an Benutzer gesendet wird auf Seite 56](#).
3. [Benutzern und Active Directory-Gruppen eine Anmeldemethode zuweisen auf Seite 56](#).

Siehe auch [Anforderungen für die Einrichtung der zweistufigen Verifikation für Benutzer auf Seite 12](#) und [Registerkarte Zweistufige Verifikation auf Seite 30](#).

## Informationen über den SMTP-Server eingeben

Der Anbieter benötigt folgende Informationen über den SMTP-Server:

1. Wählen Sie im Navigationsbereich **Mobile Server** aus und dann den entsprechenden mobilen Server.
2. Aktivieren Sie auf der Registerkarte **Zweistufige Verifikation** das Kontrollkästchen **Zweistufige Verifizierung aktivieren**.
3. Geben Sie unter **Anbiereinstellungen** auf der Registerkarte **E-Mail** Informationen über Ihren SMTP-Server ein und wählen Sie die E-Mail aus, die Client-Benutzern angezeigt werden soll, wenn sie sich anmelden und für den zweiten Anmeldeschritt konfiguriert werden. Einzelheiten zu jedem der Parameter finden Sie unter [Registerkarte Zweistufige Verifikation auf Seite 30](#).

Weitere Informationen finden Sie unter [Registerkarte Zweistufige Verifikation auf Seite 30](#).

## Den Verifizierungscode festlegen, der an Benutzer gesendet wird

So legen Sie die Komplexität des Verifizierungscode fest:

1. Geben Sie auf der Registerkarte **Zweistufige Verifikation** im Abschnitt **Verifizierungscode-Einstellungen** den Zeitraum an, innerhalb dem XProtect Mobile-Client-Benutzer ihre Anmeldung nicht erneut verifizieren müssen, zum Beispiel bei einer Trennung der Netzwerkverbindung. Der Standardzeitraum ist drei Minuten.
2. Geben Sie eine Gültigkeitsdauer für den Verifizierungscode nach Empfang durch den Benutzer an. Nach diesem Zeitraum wird der Code ungültig, und der Benutzer muss einen neuen Code anfordern. Der Standardzeitraum ist fünf Minuten.
3. Legen Sie die maximale Anzahl von Codeeingabeversuchen fest, bevor der bereitgestellte Code seine Gültigkeit verliert. Die Standardanzahl ist drei.
4. Geben Sie die Länge des Codes ein. Die Standardzeichenlänge beträgt sechs.
5. Geben Sie an, wie komplex der vom System generierte Code sein soll.

Weitere Informationen finden Sie unter [Registerkarte Zweistufige Verifikation auf Seite 30](#).

## Benutzern und Active Directory-Gruppen eine Anmeldemethode zuweisen

Auf der Liste **Zweistufige Verifikation** im Abschnitt **Benutzereinstellungen** wird die Liste der zu Ihrem XProtect-System hinzugefügten Benutzer und Gruppen angezeigt.

1. Wählen Sie in der Spalte **Anmeldemethode** eine Verifizierungsmethode für die einzelnen Benutzer oder Gruppen aus.
2. Geben Sie in das Feld **Einzelheiten** die Einzelheiten zur Lieferung ein, wie z.B. die E-Mail-Adressen der einzelnen Benutzer. Das nächste Mal, wenn sich der Benutzer bei XProtect Web Client oder der XProtect Mobile-App anmeldet, wird die zweite Anmeldeabfrage angezeigt.

3. Wenn eine Gruppe in Active Directory konfiguriert ist, bezieht der XProtect Mobile-Server Informationen wie E-Mail-Adressen aus Active Directory.



Windows-Gruppen unterstützen die zweistufige Verifikation nicht.

4. Speichern Sie Ihre Konfiguration.

Damit sind die Schritte zur Konfiguration Ihrer Benutzer für die zweistufige Verifikation über E-Mail abgeschlossen.

Weitere Informationen finden Sie unter [Registerkarte Zweistufige Verifikation auf Seite 30](#).

## Aktionen (erklärt):

Sie können die Verfügbarkeit der Registerkarte **Aktionen** im XProtect Mobile-Client oder XProtect Web Client verwalten, indem Sie die Option **Aktionen** auf der Registerkarte **Allgemein** aktivieren oder deaktivieren. **Aktionen** sind standardmäßig aktiviert und alle verfügbaren Aktionen für die verbundenen Geräte werden hier angezeigt.

Weitere Informationen finden Sie unter [Allgemein auf Seite 17](#).

## Einen Ausgang zur Verwendung im XProtect Mobile-Client und XProtect Web Client benennen (Erklärung)

Um zu erreichen, dass Maßnahmen zusammen mit der aktuellen Kamera korrekt angezeigt werden, müssen Sie eine Ausgabegruppe erstellen, die den gleichen Namen hat wie die Kamera.

### Beispiel:

Wenn Sie eine Ausgabegruppe mit Ausgaben erstellen, die mit der Kamera verbunden sind und die die Bezeichnung "AXIS P3301 - 10.100.50.110 - Kamera 1" haben, müssen Sie in das Feld **Name** den gleichen Namen eingeben (unter den **Angaben zur Gerätegruppe**).

In dem Feld **Beschreibung** können Sie eine weitere Beschreibung eingeben, z.B. "AXIS P3301 - 10.100.50.110 - Kamera 1 - Lichtschalter".



Wenn Sie sich nicht an diese Namenskonventionen halten, werden in der Aktionsliste für die Ansicht der entsprechenden Kamera keine Aktionen angezeigt. Die Aktionen werden dann in der Liste sonstiger Aktionen auf der Registerkarte **Aktionen** angezeigt.

Weitere Informationen finden Sie unter [Ausgabegeräte \(Erklärung\)](#).

## Wartung

### Mobile Server Manager (erklärt)

Beim Mobile Server Manager handelt es sich um eine Taskleisten-gesteuerte Funktion, die mit dem Mobilien Server verbunden ist. Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol Mobile Server Manager im Benachrichtigungsbereich. Dann öffnet sich ein Menü, von dem aus Sie Zugriff auf die Funktionen des Mobile Servers haben.

Sie können:

- [Zugriff auf XProtect Web Client auf Seite 58](#)
- [Den Mobile Server-Dienst starten, anhalten oder neu starten auf Seite 59](#)
- [Passworteinstellungen für den Datenschutz ändern auf Seite 59](#)
- [Management-Server-Adresse eintragen/bearbeiten auf Seite 60](#)
- [Portnummern anzeigen/bearbeiten auf Seite 60](#)
- [Aktivieren Sie die Verschlüsselung auf dem mobilen Server. auf Seite 60 mithilfe des \*\*Server Configurator\*\*](#)
- [Öffnen Sie die heutige Protokolldateien \(siehe \[Zugriff auf Protokolle und Untersuchungen \\(erklärt\\) auf Seite 62\]\(#\)\)](#)
- [Öffnen Sie den Protokollordner \(siehe \[Zugriff auf Protokolle und Untersuchungen \\(erklärt\\) auf Seite 62\]\(#\)\)](#)
- [Öffnen Sie den Ordner mit den Untersuchungen \(siehe \[Zugriff auf Protokolle und Untersuchungen \\(erklärt\\) auf Seite 62\]\(#\)\)](#)
- [Untersuchungen-Ordner ändern auf Seite 63](#)
- [Siehe XProtect Mobile Server Status \(siehe \[Status anzeigen \\(Erklärung\\) auf Seite 64\]\(#\)\)](#)

### Zugriff auf XProtect Web Client

Wenn Sie auf Ihrem Computer einen XProtect Mobile Server installiert haben, können Sie mit dem XProtect Web Client auf Ihre Kameras und Ansichten zugreifen. Da Sie XProtect Web Client nicht installieren müssen, können Sie von dem Computer aus darauf zugreifen, auf dem Sie den XProtect Mobile Server installiert haben, oder auf jedem anderen Computer, den Sie zu diesem Zweck verwenden wollen.

1. Richten Sie den XProtect Mobile-Server in Management Client ein.
2. Wenn Sie den Computer benutzen, auf dem ein XProtect Mobile-Server installiert ist, klicken Sie mit der rechten Maustaste auf das Mobile Server Manager-Taskleistensymbol und wählen Sie **Öffnen XProtect Web Client**.
3. Wenn Sie nicht den Computer verwenden, auf dem ein XProtect Mobile-Server installiert ist, können Sie von einem Browser aus darauf zugreifen. Fahren Sie mit Schritt 4 fort.

4. Öffnen Sie einen Internet-Browser (Microsoft Edge, Mozilla Firefox, Google Chrome oder Safari).
5. Geben Sie die externe IP-Adresse ein, d. h. die externe Adresse und die Portnummer des Servers, auf dem der XProtect Mobile-Server läuft.

Beispiel: Der XProtect Mobile-Server ist auf einem Server mit der IP-Adresse 127.2.3.4 installiert und so konfiguriert, dass er HTTP-Verbindungen über den Port 8081 und HTTPS-Verbindungen über den Port 8082 akzeptiert (diese Porteeinstellungen sind die Standardeinstellungen des Installationsprogramms).

Geben Sie in die Adresszeile Ihres Browsers ein **http://127.2.3.4:8081**, wenn Sie eine Standard-HTTP-Verbindung verwenden wollen, oder **https://127.2.3.4:8082**, um eine sichere HTTPS-Verbindung zu nutzen. Sie können XProtect Web Client nun verwenden.

6. Fügen Sie die Adresse in Ihrem Browser als Lesezeichen hinzu, damit Sie zukünftig ganz leicht auf XProtect Web Client zugreifen können. Falls Sie XProtect Web Client auf dem lokalen Computer verwenden, auf dem Sie den XProtect Mobile-Server installiert haben, können Sie auch die vom Installationsprogramm erstellte Verknüpfung auf dem Desktop verwenden. Klicken Sie auf die Verknüpfung, um Ihren Standardbrowser zu starten und XProtect Web Client zu öffnen.



Sie müssen den Cache des Internetbrowsers, in dem XProtect Web Client ausgeführt wird, löschen, bevor Sie eine neue Version von XProtect Web Client verwenden können. Die Systemadministratoren müssen ihre XProtect Web Client-Benutzer bitten, den Browsercache nach der Aktualisierung zu löschen, oder diese Aktion per Fernzugriff erzwingen (diese Aktion kann innerhalb einer Domäne nur im Internet Explorer ausgeführt werden).

## Den Mobile Server-Dienst starten, anhalten oder neu starten

Falls nötig, können Sie den Mobile Server-Dienst über Mobile Server Manager starten, anhalten und neu starten.

- Um eine dieser Aufgaben durchzuführen, klicken Sie mit der rechten Maustaste auf das Mobile Server Manager-Symbol und wählen Sie **Mobile Server-Dienst starten**, **Mobile Server-Dienst anhalten** oder **Mobile Server-Dienst neu starten** aus.

## Passworteinstellungen für den Datenschutz ändern

Das Datenschutzpasswortes für den Mobile Server dient zum Verschlüsseln von Untersuchungen. 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.

Zum Ändern des Passwortes für den Datenschutz auf dem Mobile Server:

1. Klicken Sie mit der rechten Maustaste auf das Symbol Mobile Server Manager und wählen Sie **Passworteinstellungen für den Datenschutz ändern**. Ein Dialogfeld wird angezeigt.
2. Geben Sie in das Feld **Neues Passwort** Ihr neues Passwort ein.

3. Geben Sie das neue Passwort in das Feld **Neues Passwort bestätigen** ein.
4. (Optional) Wenn Sie kein Passwort zum Schutz Ihrer Untersuchungen festlegen möchten, 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**.
5. Klicken Sie auf **OK**.



Dieses Passwort müssen Sie sicher aufbewahren. Andernfalls können die Daten auf dem Mobile Server evtl. nicht wiederhergestellt werden.

## Management-Server-Adresse eintragen/bearbeiten

1. Klicken Sie dort mit der rechten Maustaste auf das Symbol Mobile Server Manager und wählen Sie dann **Management-Server-Adresse** aus.
2. Geben Sie in das Feld **Server-URL** die URL-Adresse des Servers ein.
3. Klicken Sie auf **OK**.

## Portnummern anzeigen/bearbeiten

1. Klicken Sie mit der rechten Maustaste auf das Mobile Server Manager-Symbol des mobilen Server Managers, und wählen Sie die Option **Portnummern anzeigen/bearbeiten** aus.
2. Um die Portnummern zu bearbeiten, geben Sie die jeweilige Portnummer ein. Sie können für HTTP-Verbindungen eine Standardportnummer oder eine sichere Portnummer für HTTPS-Verbindungen, oder beide, angeben.
3. Klicken Sie auf **OK**.

## 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 unter [Datenverschlüsselung des mobilen Servers \(Erläuterung\) auf Seite 43](#) und [Anforderungen zur Verschlüsselung mobiler Server für Clients auf Seite 44](#).



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 Domännennamen 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

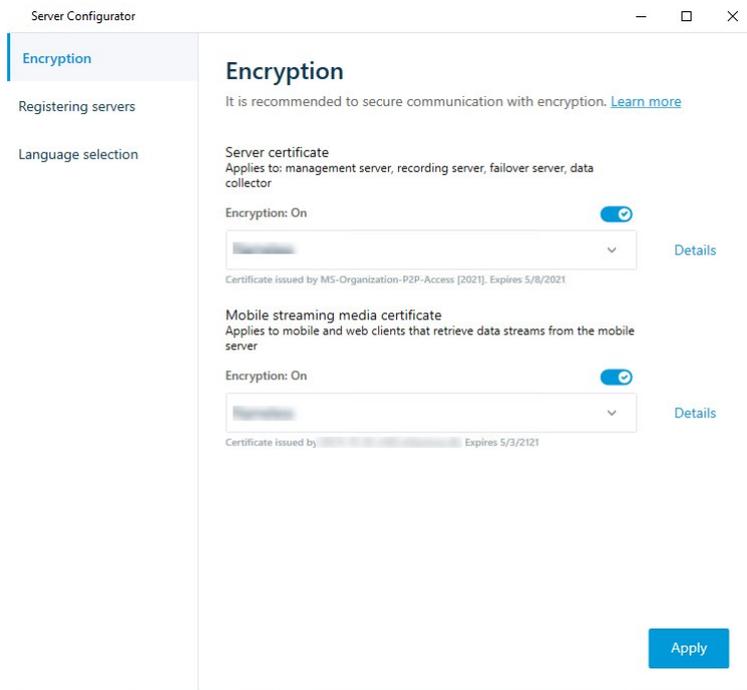
- Das Mobile Server Manager durch Klicken mit der rechten Maustaste auf das Symbol Mobile Server Manager auf der Taskleiste des Computers

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.

## Zugriff auf Protokolle und Untersuchungen (erklärt)

Mithilfe des Mobile Server Manager können Sie rasch auf die Protokolldatei des aktuellen Tages zugreifen und die Ordner öffnen, in dem die Protokolldateien und in dem die Untersuchungen gespeichert sind.

Zum Öffnen von einer dieser Dateien, klicken Sie mit der rechten Maustaste auf das Mobile Server Manager-Symbol und wählen Sie:

- **Heutige Protokolldatei öffnen**
- **Protokollordner öffnen**
- **Den Untersuchungen-Ordner öffnen**

Auditprotokolle werden für jede Maßnahme erstellt, die nicht bereits durch Management Server oder Recording Server protokolliert wird.

Die folgenden Maßnahmen werden stets protokolliert (selbst wenn die erweiterte Auditprotokollierung nicht aktiviert ist):

- Gesamte Verwaltung (diese Auditprotokollmeldungen enthalten den alten und den neuen Wert)
- Alle Maßnahmen zur Erstellung, Bearbeitung oder Löschung von Untersuchungen sowie die Vorbereitung und das Herunterladen exportierter Materialien, die Änderung relevanter Teile der Konfiguration. Das Auditprotokoll enthält Einzelheiten dazu, was getan wurde.



Video-Push-Streaming wird nur protokolliert, wenn die Auditprotokollierung aktiviert ist.



Wenn Sie den XProtect Mobile-Server von Ihrem System deinstallieren, werden die zugehörigen Protokolldateien nicht gelöscht. Administratoren mit den entsprechenden Benutzerberechtigungen können später auf diese Protokolldateien zugreifen, oder sie löschen, wenn sie nicht mehr gebraucht werden. Standardspeicherort der Protokolldateien ist der Ordner **ProgramData**. Wenn Sie den Standardspeicherort für Protokolldateien ändern, werden vorhandene Protokolle nicht an den neuen Speicherort kopiert und auch nicht gelöscht.

## Untersuchungen-Ordner ändern

Standardspeicherort für Untersuchungen ist der Ordner **ProgramData**. Wenn Sie den Standardspeicherort für den Untersuchungsordner ändern, werden vorhandene Untersuchungen nicht automatisch an den neuen Speicherort kopiert und auch nicht gelöscht. So ändern Sie den Ort wo die Untersuchungen-Exporte auf Ihrer Festplatte gespeichert werden:

1. Klicken Sie mit der rechten Maustaste auf das Mobile Server Manager-Symbol und wählen Sie **Untersuchungen-Ordner ändern**.

Das Fenster **Untersuchungen-Speicherort** Fenster wird geöffnet.

2. Klicken Sie neben dem **Ordner**-Feld, das die aktuelle Position anzeigt, auf das Ordner-Symbol, um nach einem vorhandenen Ordner zu suchen oder einen neuen Ordner zu erstellen > Auf **OK** klicken.

3. Wählen Sie aus der Liste mit **Alten Untersuchungen**, wählen Sie die Aktion, die Sie auf die vorhandene Untersuchung anwenden möchten, welche am aktuellen Speicherort gespeichert ist. Die Optionen sind:

- **Verschieben:** Bewegt vorhandene Untersuchungen zum neuen Ordner



Wenn Sie die vorhandenen Untersuchungen nicht zum neuen Ordner bewegen, werden Sie sie nicht länger sehen können.

- **Löschen:** Löscht die vorhandenen Untersuchungen
- **Nichts tun:** Die vorhandenen Untersuchungen verbleiben am aktuellen Ordnerspeicherort. Sie können diese nicht mehr sehen, nachdem Sie den Standardspeicherort des Untersuchungen-Ordners geändert haben.

4. Klicken Sie auf **Anwenden** > klicken Sie auf **OK**.

## Status anzeigen (Erklärung)

Klicken Sie mit der rechten Maustaste auf das Mobile Server Manager-Symbol und wählen Sie **Status anzeigen** aus oder doppelklicken Sie auf das Mobile Server Manager-Symbol, um ein Fenster zu öffnen, das den Status des XProtect Mobile-Servers anzeigt. Die folgenden Informationen werden angezeigt:

| Name                              | Beschreibung   |
|-----------------------------------|--|
| <b>Server in Betrieb seit</b>     | Datum und Uhrzeit des letzten Starts des XProtect Mobile-Servers.                            |
| <b>Verbundene Benutzer</b>        | Anzahl der Benutzer, die aktuell mit dem XProtect Mobile-Server verbunden sind.              |
| <b>Hardware-Dekodierung</b>       | Zeigt an, ob auf dem XProtect Mobile-Server die hardwarebeschleunigte Dekodierung aktiv ist. |
| <b>CPU-Auslastung</b>             | Gibt an, wie viel Prozent der CPU aktuell vom XProtect Mobile-Server ausgelastet sind.       |
| <b>Verlauf der CPU-Auslastung</b> | Grafik, die den Verlauf der CPU-Auslastung durch den XProtect Mobile-Server darstellt.       |

# Fehlerbehandlung

## Fehlerbehandlung XProtect Mobile

### Verbindungen

1. **Warum kann ich keine Verbindung von meinem XProtect Mobile-Client zu meinen Aufnahmen/meinem XProtect Mobile Server herstellen?**

Um eine Verbindung zu Ihren Aufzeichnungen herzustellen, muss der XProtect Mobile Server auf dem Server installiert sein, auf dem Ihr XProtect System läuft, oder alternativ auf einem eigenen Server. Die relevanten XProtect Mobile Einstellungen in der Einrichtung Ihres XProtect Video-Managements sind ebenfalls erforderlich. Diese werden als Plug-ins oder als Teil einer Produktinstallation oder einer Erweiterung installiert. Einzelheiten dazu, wie Sie den XProtect Mobile Server erhalten und wie die XProtect Mobile Einstellungen für den Client in Ihr XProtect System integriert werden, finden Sie im Abschnitt zur Konfiguration (siehe [Einstellungen des mobilen Servers auf Seite 17](#)).

2. **Ich habe gerade meine Firewall eingeschaltet, und jetzt kann ich kein mobiles Gerät mit meinem Server verbinden. Warum nicht?**

Wenn bei der Installation des XProtect Mobile Servers Ihre Firewall abgeschaltet wurde, müssen Sie die TCP- und UDP-Kommunikation manuell aktivieren.

3. **Wie kann ich die Sicherheitswarnung vermeiden, wenn ich mein System XProtect Web Client über eine HTTPS-Verbindung betreibe?**

Diese Warnung erscheint, weil die Angaben zur Serveradresse in dem Zertifikat nicht korrekt sind. Die Verbindung ist verschlüsselt.

Das selbstsignierte Zertifikat im XProtect Mobile-Server muss durch Ihr eigenes Zertifikat ersetzt werden, das mit der Serveradresse übereinstimmt, die für die Verbindung mit dem XProtect Mobile-Server verwendet wird. Diese Zertifikate können von offiziellen Zertifizierungsstellen erhalten werden, z.B. Verisign. Zu weiteren Einzelheiten wenden Sie sich an die ausgewählte Zertifizierungsstelle. XProtect Mobile Server verwendet kein Microsoft IIS. Das heisst, dass die Anweisungen zum Erzeugen von Certificate Signing Request (CSR)-Dateien durch die Zeichnungsberechtigung mithilfe von IIS für den XProtect Mobile Server nicht gelten. Sie müssen eine CSR-Datei mithilfe von Befehlszeilenzertifikattools oder sonstigen, ähnlichen Drittanwendungen von Hand erstellen. Dieses Verfahren sollte nur von Systemadministratoren oder fortgeschrittenen Anwendern durchgeführt werden.

## Bildqualität

1. **Warum ist die Bildqualität manchmal so schlecht, wenn ich mir Videoaufzeichnungen im XProtect Mobile-Client anschau?**

Der XProtect Mobile-Server stellt die Bildqualität je nach verfügbarer Bandbreite zwischen Server und Client automatisch ein. Wenn die Bildqualität, die Sie erhalten, geringer ist als im XProtect® Smart Client, verfügen Sie u.U. über zu wenig Bandbreite um durch den XProtect Mobile Client Bilder in voller Auflösung zu erhalten. Grund dafür kann entweder eine zu geringe Bandbreite vom Server im Upstream sein, oder zu wenig Bandbreite im Downstream auf dem Client. Weitere Informationen finden Sie im [Benutzerhandbuch für XProtect Smart Client](#).

Wenn Sie sich in einer Zone mit gemischter WLAN-Bandbreite befinden, verbessert sich ggf. die Bildqualität, wenn Sie in eine Zone mit besserer Bandbreite kommen.

2. **Warum ist die Bildqualität zu schlecht, wenn ich von zuhause über WLAN eine Verbindung zu meinem XProtect Video Management System im Büro herstelle?**

Prüfen Sie die Bandbreite Ihrer Internetverbindung zuhause. Viele private Internetanschlüsse haben eine unterschiedlich große Bandbreite für Download und Upload. Dies wird oft z.B. als 20 Mbit/2 Mbit beschrieben. Dies liegt daran, dass Heimanwender selten große Datenmengen in das Internet hochladen müssen, dagegen aber umfangreiche Daten konsumieren. Das XProtect Video Management System muss Video zum XProtect Mobile-Client senden, und wird dabei durch die Uploadgeschwindigkeit Ihrer Internetverbindung eingeschränkt. Wenn die Bildqualität an mehreren Standorten gleich schlecht ist, an denen die Downloadgeschwindigkeit des XProtect Mobile Client-Netzwerks gut ist, lässt sich das Problem u.U. dadurch lösen, dass die Upload-Geschwindigkeit Ihrer Internetverbindung zuhause erhöht wird.

## Hardwarebeschleunigte Decodierung

1. **Unterstützt mein Prozessor die hardwarebeschleunigte Dekodierung?**

Nur die neueren Prozessoren von Intel unterstützen die hardwarebeschleunigte Decodierung. Schauen Sie auf der Internetseite von Intel nach (<https://ark.intel.com/Search/FeatureFilter?productType=processors/>), ob Ihr Prozessor unterstützt wird.

Achten Sie in dem Menü darauf, dass **Technologien > Intel Quick Sync Video** auf **Ja** steht.

Wenn Ihr Prozessor unterstützt wird, ist die hardwarebeschleunigte Dekodierung standardmäßig aktiviert. Den aktuellen Status sehen Sie unter **Status anzeigen** im Mobile Server Manager (siehe [Status anzeigen \(Erklärung\) auf Seite 64](#)).

## 2. Unterstützt mein Betriebssystem die hardwarebeschleunigte Dekodierung?

Alle Betriebssysteme, die von XProtect unterstützt werden, unterstützen auch die Hardwarebeschleunigung.

Achten Sie darauf, dass Sie auf Ihrem System die neuesten Grafiktreiber von der Internetseite von Intel installiert haben. Diese Treiber sind nicht über das Windows-Update erhältlich.

Die hardwarebeschleunigte Decodierung wird nicht unterstützt, wenn der Mobile Server in einer virtuellen Umgebung installiert ist.

## 3. Wie deaktiviere ich die hardwarebeschleunigte Dekodierung auf dem Mobilien Server? (Erweitert)

Wenn der Prozessor auf dem Mobilien Server die hardwarebeschleunigte Dekodierung unterstützt, ist sie standardmäßig aktiviert. Gehen Sie wie folgt vor, um die hardwarebeschleunigte Dekodierung abzuschalten:

1. Suchen Sie die Datei VideoOS.MobileServer.Service.exe config. Der Pfad lautet üblicherweise:  
C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config.
2. Öffnen Sie die Datei in Notepad oder in einem ähnlichen Texteditor. Legen Sie ggf. Notepad als Standardanwendung für Dateien mit der Dateierdung .config fest.
3. Suchen Sie das Feld <add key="HardwareDecodingMode" value="Auto" />.
4. Ersetzen Sie den Wert "Auto" durch "Off".
5. Speichern und schließen Sie die Datei.



[helpfeedback@milestone.dk](mailto:helpfeedback@milestone.dk)

#### 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/>.

