MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile-Server 2025 R2

Bedienungsanleitung für Administratoren

milestone

Inhalt

Copyright, Marken und Verzichtserklärung ... **5**

Übersicht ... **6**

XProtect Mobile für Administrator/innen ... 6

Was ist neu? ... 7

Anforderungen und Hinweise ... **8**

Vor der Installation des XProtect Mobile-Servers ... 8

Anforderungen für das Einrichten von Benachrichtigungen ... 8

Anforderungen für das Einrichten von Smart Connect ... 9

Anforderungen für die Einrichtung der zweistufigen Verifikation für Benutzer ... 9

Anforderungen für das Einrichten von Video Push ... 9

Anforderungen für direktes Streaming ... 9

Voraussetzungen für das Teilen ... 10

Installation ... **11**

Installieren des XProtect Mobile-Servers ... 11

Konfiguration ... **14**

Einstellungen des mobilen Servers ... 14

Verbindungsdaten ... 14

Allgemein ... 15

Registerkarte Konnektivität ... 18

Registerkarte Serverstatus ... 20

Registerkarte Leistung ... 21

Registerkarte Untersuchungen ... 24

Registerkarte Video Push ... 26

Registerkarte Benachrichtigungen ... 27

Registerkarte Zweistufige Verifikation ... 28

Direktes Streaming ... 31

Adaptives Streaming ... 32

Datenverschlüsselung des mobilen Servers (Erklärung) ... 33

Aktivieren Sie die Verschlüsselung auf dem mobilen Server. ... 35

Milestone Federated Architecture und übergeordnete/untergeordnete Standorte ... 36

Smart Connect ... 37
Einrichten von Smart Connect ... 37
Aktivieren Sie die UPnP-Erkennungsfunktion in Ihrem Router ... 37
Aktivieren von Verbindungen im komplexen Netzwerk ... 38
Konfigurieren der Verbindungseinstellungen ... 38
Senden einer E-Mail-Nachricht an Benutzer ... 39
Benachrichtigungen ... 39
Konfigurieren von Push-Benachrichtigungen auf dem XProtect Mobile-Server ... 40
Aktivieren von Push-Benachrichtigungen für bestimmte oder alle Mobilgeräte ... 41
Deaktivieren des Sendens von Push-Benachrichtigungen an bestimmte oder alle Mobilgeräte ... 41
Ein oder alle registrierten Geräte aus der Liste der registrierten Geräte entfernen ... 41
Einrichten von Untersuchungen ... 42
Nutzung von Video Push für Videostreams ... 44
Einrichten von Video Push für Videostreams ... 44
Einen video push-Kanal für Video-Streaming hinzufügen ... 44
Einen Video-Push-Kanal bearbeiten ... 45
Einen video push-Kanal entfernen ... 46
Passwort ändern ... 46
Fügen Sie den Video Push-Treiber als Hardwaregerät auf dem Aufzeichnungsserver hinzu ... 46
Hinzufügen des video push-Treibergeräts zum video push-Kanal ... 48
Aktivieren Sie Audio für den vorhandenen Push-Videokanal ... 48
Einrichten von Benutzern für die zweistufige Verifikation über E-Mail ... 49
Informationen über den SMTP-Server eingeben ... 49
Den Verifizierungscode festlegen, der an Benutzer gesendet wird ... 49
Benutzern und Active Directory-Gruppen ein Verifizierungsverfahren zuweisen ... 50
Aktionen ... 50
Mobilgeräteverwaltung (MDM) ... 51
Konfiguration der Details des mobilen Servers auf der MDM-Plattform (Administratoren) ... 51
Einen Ausgang zur Verwendung im XProtect Mobile-Client und XProtect Web Client benennen ... 53
Externer IDP und XProtect Mobile ... 53
Konfigurieren des externen IDP-Logins für XProtect Web Client ... 54
Notfallalarme hinzufügen ... 54

Wartung **55**

Mobile Server Manager 55

Zugriff auf XProtect Web Client 55

Den Mobile Server-Dienst starten, anhalten oder neu starten 56

Passworteinstellungen für den Datenschutz ändern 56

Portnummern anzeigen/bearbeiten 57

Zugriff auf Protokolle und Untersuchungen 57

Untersuchungen-Ordner ändern 58

Status anzeigen 58

Lastausgleich für den mobilen Server verwenden 59

Mobilen Server zu einem anderen Host migrieren 60

Fehlerbehandlung **62**

Fehlerbehandlung XProtect Mobile 62

Anhänge **65**

Anhang A 65

Anhang B 68

Copyright, Marken und Verzichtserklärung

Copyright © 2025 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 für Administrator/innen

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.

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.

XProtect Mobile Server

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.

XProtect Mobile Plug-In

Das XProtect Mobile Plug-in ist Teil der XProtect Mobile Server Komponente. Mit dem XProtect Mobile Plug-in können Sie die mobilen Server in Ihrem VMS-System aufrufen und verwalten, und zwar über den Knoten **Server** in XProtect Management Client.

Sie installieren das XProtect Mobile Plug-in auf einen beliebigen Computer mit XProtect Management Client, von dem Sie die mobilen Server verwalten.

Mobile Server Manager

Nutzen Sie Mobile Server Manager, um Informationen über den Dienst zu erhalten, den Status des Mobile Server Dienstes zu überprüfen, Protokolle und Statusmeldungen aufzurufen und den Dienst zu starten und anzuhalten.

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

Was ist neu?

In XProtect Mobile Server 2023 R3

Verbindungsdaten:

- Prüfen Sie, ob der Mobile Server über das Internet erreichbar ist. Siehe Verbindungsdaten on page 14.

Alarme:

- Fügen Sie Notfallalarme hinzu, um die Benutzer über Alarme des höchsten Schweregrads im XProtect Mobile Client zu informieren. Siehe Notfallalarme hinzufügen on page 54.

In XProtect Mobile Server 2023 R2

Lesezeichen und Live-Video-Sharing:

- Für die gemeinsame Nutzung von Lesezeichen und Live-Video im XProtect Mobile Client müssen Sie die Verschlüsselung auf dem Management-Server aktivieren. Siehe Voraussetzungen für das Teilen on page 10.

Benachrichtigungen:

- Sie können Geräteregistrierungsdaten aus der VMS-Datenbank entfernen. Siehe Ein oder alle registrierten Geräte aus der Liste der registrierten Geräte entfernen on page 41.

In XProtect Mobile Server 2022 R3

Externe IDP:

- Sie können sich jetzt mit einem externen IDP bei XProtect Web Client und dem XProtect Mobile-Client anmelden. Siehe Externer IDP und XProtect Mobile on page 53

Mobilgeräteverwaltung (MDM):

- Der XProtect Mobile-Client unterstützt jetzt die Mobilgeräteverwaltung (MDM). Mit der Mobilgeräteverwaltung können Sie Geräte, Anwendungen und Daten über eine einheitliche Konsole verwalten und sichern. Weitere Informationen finden Sie unter Mobilgeräteverwaltung (MDM) on page 51

Push-Benachrichtigungen:

- Wenn Sie diese Funktion aktivieren, werden Sie durch eine Warnung darüber informiert, dass Ihr System möglicherweise nicht DSGVO-konform ist

In XProtect Mobile-Server 2022 R2

Benachrichtigungen:

- Standardmäßig sind die Benachrichtigungen deaktiviert.

Installation:

- Bei der Installation von Mobile Server können Sie eine Verbindung zum Überwachungssystem mit einem Basisbenutzer herstellen.

Anforderungen und Hinweise

Vor der Installation des XProtect Mobile-Servers

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

Milestone empfiehlt, dass Sie den XProtect Mobile-Server auf einem separaten Computer installieren. Bevor Sie die XProtect Mobile Server Komponente installieren und mit der Nutzung beginnen, stellen Sie Folgendes sicher:

- Sie haben die Kameras und Ansichten in XProtect Management Client eingerichtet.
- Der Computer des Mobilen Servers löst die Hostnamen der Computer auf, auf denen andere VMS-Serverkomponenten ausgeführt werden.
- Der Management-Server-Computer löst den Hostnamen des mobilen Server-Computers auf.
- Sie haben eine laufende VMS installiert.
- Sie haben mindestens einen VMS-Benutzer konfiguriert. Zur Verbindung mit dem Überwachungssystem erfordert die Rolle, zu der dieser Benutzer hinzugefügt wird, Berechtigungen für den Management-Server:
  - **Verbinden**
  - **Lesen**
  - **Bearbeiten**
- Wenn Sie ein Upgrade Ihres Systems durchführen, stellen Sie sicher, dass die Version des XProtect Mobile-Plug-ins mit der Version des Mobilen Servers übereinstimmt. Ihr System funktioniert ggf. nicht korrekt, wenn sich die Versionen des Plug-ins und der Mobilen Server unterscheiden.

Anforderungen für das Einrichten von Benachrichtigungen

Zur Benachrichtigung der Benutzer, wenn es zu einem Zwischenfall kommt.

- Sie müssen mindestens einen Alarm mit mindestens einem Ereignis und einer Regel verknüpfen. Dies gilt nicht für Systembenachrichtigungen
- Sie haben eine aktuelle Milestone Care™ Vereinbarung mit Milestone Systems
- Ihr System muss über Internetzugriff verfügen

Für weitere Informationen, siehe:

Konfigurieren von Push-Benachrichtigungen auf dem XProtect Mobile-Server on page 40

Registerkarte Benachrichtigungen on page 27

Anforderungen für das Einrichten von Smart Connect

Zur Nutzung von Smart Connect und zur Bestätigung, dass Sie XProtect Mobile korrekt konfiguriert haben, benötigen Sie:

- Eine öffentliche IP-Adresse für Ihren XProtect Mobile Server. Die Adresse kann statisch oder dynamisch sein, aber normalerweise ist es eine gute Idee, statische IP-Adressen zu verwenden.
- Eine gültige Lizenz für Smart Connect
- Eine aktuelle Milestone Care™ Vereinbarung mit Milestone Systems

Anforderungen für die Einrichtung der zweistufigen Verifikation für Benutzer

So richten Sie Benutzer für die zweistufige Verifikation über E-Mail ein:

- Sie haben einen SMTP-Server installiert.
- Sie haben im XProtect im Knoten **Rollen** im Bereich **Standort-Navigation** Benutzer und Gruppen zu Ihrem Management Client-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 Mobile Server Dienst neu starten, damit die zweistufige Verifikation wirksam wird.

Für weitere Informationen, siehe:

Einrichten von Benutzern für die zweistufige Verifikation über E-Mail on page 49

Registerkarte Zweistufige Verifikation on page 28

Anforderungen für das Einrichten von Video Push

Um Video von der Kamera eines Mobilgeräts an das XProtect Überwachungssystem zu streamen, benötigen Sie Folgendes:

- Eine Gerätelizenz für jeden verwendeten Kanal.

Anforderungen für direktes Streaming

XProtect Mobile unterstützt das direkte Streaming im Live-Modus. Um Direct Streaming in XProtect Web Client und XProtect Mobile-Client zu verwenden, benötigen Sie die folgende Kamerakonfiguration:

- Die Kameras müssen die Codecs H.264 oder H.265 unterstützen.

  XProtect Web Client unterstützt nur H.264.

- 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

Voraussetzungen für das Teilen

Benutzer können Lesezeichen und Live-Videos teilen, während sie die XProtect Mobile Client-App verwenden. Diese Funktionalitäten sind verfügbar nachdem:

- Sie die Verschlüsselung auf dem Management-Server aktiviert haben.

Installation

Installieren des XProtect Mobile-Servers

Nach der Installation des XProtect Mobile-Servers können Sie den 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.

Herunterladen des XProtect Mobile-Server-Installationsprogramms

1. Geben Sie 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. Wählen Sie **Alle Sprachen** für das Installationsprogramm für den XProtect Mobile Server.

Installieren des XProtect Mobile-Servers

1. Führen Sie die heruntergeladene Datei aus. Wählen Sie dann **Ja** aus, um alle Warnungen zu bestätigen.
2. Wählen Sie die Sprache für das Installationsprogramm aus. Wählen Sie dann **Weiter** aus.
3. Lesen Sie und akzeptieren Sie die Lizenzvereinbarung. Wählen Sie dann **Weiter** aus.
4. 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

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

5. Nur für die benutzerdefinierte Installation: Wählen Sie die Komponenten aus, die Sie installiert haben möchten. Wählen Sie dann **Weiter** aus.
6. Wählen Sie das Dienstkonto für den mobilen Server aus. Wählen Sie dann **Weiter** aus.

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

7. Nur für die benutzerdefinierte Installation: Melden Sie sich mit einem bestehenden VMS-Benutzerkonto an, wenn Sie sich mit dem Überwachungssystem verbinden:
   - Das **Dienstkonto** ist das Konto, das Sie in Schritt 8 ausgewählt haben. Um eine Verbindung über dieses Konto herzustellen, stellen Sie sicher, dass das Dienstkonto Mitglied einer Domäne ist, auf die der Management-Server Zugriff hat
   - **Basisbenutzer**: Verwenden Sie einen Basisbenutzer, wenn das Dienstkonto kein Mitglied einer Domäne ist, auf die der Management-Server Zugriff hat

   > Um das Dienstkonto oder die Anmeldedaten für den Basisbenutzer später zu ändern oder zu bearbeiten, müssen Sie den Mobilen Server neu installieren.

   Klicken Sie auf **Fortfahren**.
8. Geben Sie in das Feld **Server-URL** die Adresse des primären Management-Servers ein.

   Nur für die benutzerdefinierte Installation: Geben Sie die Ports für die Kommunikation mit dem mobilen Server an. Wählen Sie dann **Weiter** aus. Bei einer typischen Installation erhalten die Verbindungsports die Standardportnummern 8081 für den HTTP-Port und 8082 für den HTTPS-Port).
9. 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**.
10. Geben Sie die Verschlüsselung für den mobilen Server an. Wählen Sie dann **Weiter** aus.

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.

Weitere Informationen zur Vorbereitung Ihres Systems für die sichere Kommunikation finden Sie unter:

- Datenverschlüsselung des mobilen Servers (Erklärung)
- Der Milestone Leitfaden zur Zertifizierung

Nach Abschluss der Installation können Sie außerdem von dem Taskleistensymbol Mobile Server Manager aus die Verschlüsselung aktivieren. (siehe Aktivieren Sie die Verschlüsselung auf dem mobilen Server. on page 35).

11. Wählen Sie den Datei-Speicherort und die Produktsprache aus und klicken Sie dann auf **Installieren**.

    Wenn die Installation abgeschlossen ist, wird eine Liste der erfolgreich installierten Komponenten angezeigt.

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 on page 15)
- Konfigurieren der Einstellungen für die Serververbindung (siehe Registerkarte Konnektivität on page 18)
- Einrichtung der Funktion Smart Connect (siehe Registerkarte Konnektivität on page 18)
- Den aktuellen Status des Servers sowie eine Liste der aktiven Benutzer finden Sie unter Registerkarte Serverstatus on page 20
- Sie können Leistungsparameter einrichten, um Direct Streaming und adaptives Streaming zu aktivieren, oder um Begrenzungen für transcodierte Videostreams festzulegen (siehe Registerkarte Leistung on page 21)
- Konfigurieren der Einstellungen für Untersuchungen (siehe Registerkarte Untersuchungen on page 24)
- Konfigurieren der Einstellungen für Push-Video (siehe Registerkarte Video Push on page 26)
- Angaben zur Einrichtung sowie zum Ein- und Ausschalten von Systembenachrichtigungen und Push-Benachrichtigungen finden Sie unter Registerkarte Benachrichtigungen on page 27
- Aktivieren und konfigurieren eines zusätzlichen Anmeldeschrittes für Benutzer (siehe Registerkarte Zweistufige Verifikation on page 28)

Verbindungsdaten

In den folgenden Tabellen werden die Status und Meldungen des mobilen Servers beschrieben, die für alle Registerkarten sichtbar sind.

Der Server ist über das Internet zugänglich

Farbe	Status	Beschreibung
Orange	Nicht zutreffend	Der mobile Server wurde nicht für den Zugriff von außerhalb des lokalen Netzwerks konfiguriert.

Farbe	Status	Beschreibung
Rot	Nein	Die XProtect Web Client und XProtect Mobile Client-Benutzer können nicht über das Internet mit dem mobilen Server verbunden werden.
Grün	Ja	Die XProtect Web Client und XProtect Mobile Client-Benutzer können über das Internet mit dem mobilen Server verbunden werden.

Verbindung zu Server

Farbe	Nachricht	Beschreibung
Orange	**Ungültiges HTTPS-Zertifikat**	Das XProtect Mobile Plug-in erkennt das Zertifikat des mobilen Servers nicht.
Orange	**HTTP/HTTPS nicht erreichbar**	XProtect Management Client kann den mobilen Server nicht erreichen.
Rot	**HTTP/HTTPS nicht verbunden**	XProtect Management Client hat den mobilen Server erkannt, kann sich damit aber nicht verbinden.
Grün	**HTTP/HTTPS**	XProtect Management Client hat eine Verbindung mit dem mobilen Server aufgebaut.

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.
Mobile Server	Siehe den Namen des aktuell ausgewählten XProtect Mobile-Servers.

Funktionen

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

Name	Beschreibung
XProtect Web Client aktivieren	Aktivieren Sie den Zugriff auf XProtect Web Client. Diese Funktion ist standardmäßig aktiviert.
Aktivieren Sie die Ansicht Alle Kameras für den XProtect Mobile-Client	In dieser Ansicht werden alle Kameras angezeigt, die der betreffende Benutzer auf einem Aufzeichnungsserver sehen darf. Diese Funktion ist standardmäßig aktiviert.
Lesezeichen aktivieren	Aktivieren Sie die Lesezeichenfunktion, um Videosequenzen in XProtect Mobile Client und XProtect Web Client schnell finden zu können. Diese Funktion ist standardmäßig aktiviert.
Aktionen aktivieren (Ausgänge und Ereignisse)	Aktivieren Sie den Zugriff auf Aktionen in XProtect Mobile-Clients und XProtect Web Client. Diese Funktion ist standardmäßig aktiviert. Wenn Sie diese Funktion deaktivieren, können die Benutzer des Clients keine Ausgaben und Ereignisse sehen, selbst wenn diese korrekt konfiguriert sind.
Eingehendes Audiosignal aktivieren	Aktivieren Sie die Funktion für eingehenden Ton XProtect Web Client und XProtect Mobile Client. Diese Funktion ist standardmäßig aktiviert.

Name	Beschreibung
Push-to-talk aktivieren	Aktivieren Sie die Push-to-Talk-Funktion (PTT) in XProtect Web Client und XProtect Mobile im Client. Diese Funktion ist standardmäßig aktiviert.
Zugriff der integrierten Administrator-Rolle auf den XProtect Mobile-Server verweigern	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
Speicherort der Protokolldatei	Sehen Sie, wo das System Protokolldateien speichert.
Protokolle beibehalten für	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
Importieren	Importieren Sie eine XML-Datei mit einer neuen XProtect Mobile-Serverkonfiguration.
Exportieren	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 on page 38
- Senden einer E-Mail-Nachricht an Benutzer on page 39
- Aktivieren von Verbindungen im komplexen Netzwerk on page 38
- Aktivieren Sie die UPnP-Erkennungsfunktion in Ihrem Router on page 37

Weitere Informationen finden Sie unter Smart Connect on page 37.

> 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. on page 35.

Allgemein

Name	Beschreibung
Client-Zeitüberschreitung	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. Milestone empfiehlt Ihnen, das Timeline Area nicht zu erhöhen.
Aktivieren Sie UPnP-Auffindbarkeit	Dies macht den XProtect Mobile-Server durch UPnP-Protokolle im Netzwerk auffindbar. Der XProtect Mobile-Client hat eine auf UPnP basierende Scanfunktionalität für das Finden von XProtect Mobile-Servern.
Portzuordnung aktivieren	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 **Automatische Portzuordnung aktivieren** kann der XProtect Mobile Server diese Portzuordnung selbst vornehmen, vorausgesetzt, der Router ist dafür konfiguriert.
Smart Connect aktivieren	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
Benutzerdefinierten Internetzugriff konfigurieren	Geben Sie 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.
• **HTTP** • **HTTPS**	Wählen Sie den Verbindungstyp aus.
Auswählen, um die IP-Adresse dynamisch abzurufen	Aktivieren Sie das Kontrollkästchen, wenn sich Ihre IP-Adressen häufig ändern.
Verwenden Sie nur die konfigurierte URL-Adresse	Aktivieren Sie das Kontrollkästchen, um eine Verbindung zum mobilen Server nur mit einer benutzerdefinierten IP-Adresse oder einem Hostnamen herzustellen.
Server-Adressen	Listet alle URL-Adressen auf, die mit dem mobilen Server verbunden sind.

Smart Connect-Benachrichtigung

Name	Beschreibung
E-Mail-Einladung an	Geben Sie die E-Mail-Adresse des gewünschten Empfängers der Smart Connect-Benachrichtigung ein.
E-Mail-Sprache	Geben Sie die in der E-Mail verwendete Sprache an.
Smart Connect-Token	Ein eindeutiger Bezeichner, den Benutzer von Mobilgeräten verwenden können, um eine Verbindung zum XProtect Mobile-Server herzustellen.
Link zu Smart Connect	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
Server ist aktiviert seit	Zeigt das Datum und Uhrzeit des letzten Starts des XProtect Mobile-Servers.
CPU-Auslastung	Zeigt die aktuelle CPU-Auslastung auf dem mobilen Server an.
Externe Bandbreite	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
Benutzername	Zeigt den Benutzernamen jedes XProtect Mobile-Client- oder XProtect Web Client-Benutzers an, der mit dem mobilen Server verbunden ist.
Status	Zeigt die aktuelle Beziehung zwischen dem XProtect Mobile-Server und dem jeweiligen XProtect Mobile-Client oder XProtect Web Client-Benutzer an. Mögliche Statusmeldungen: • **Verbunden**: Ein Anfangszustand, wenn die Clients und der Server Schlüssel und Verschlüsselungsinformationen austauschen • **Angemeldet**: Der XProtect Mobile-Client- oder XProtect Web Client-Benutzer ist im XProtect-System angemeldet
Video Bandbreitennutzung (kB/s)	Zeigt die gesamte Bandbreite der Videostreams, die derzeit für jeden XProtect Mobile Client oder XProtect Web Client-Benutzer offen sind.
Audio Bandbreitennutzung (kB/s)	Zeigt die gesamte Bandbreite der Audiostreams, die derzeit für jeden XProtect Web Client-Benutzer offen sind.
Transcodierte Videostreams	Zeigt die gesamte Bandbreite der transcodierten Videostreams, die derzeit für jeden XProtect Mobile Client oder XProtect Web Client-Benutzer offen sind.
Direkte Video-Streams	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).
Transcodierte Audiostreams	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
Direktes Streaming aktivieren	Direktes Streaming aktivieren im XProtect Web Client und XProtect Mobile-Client (nur für XProtect Expert und XProtect Corporate). Diese Funktion ist standardmäßig aktiviert.
Adaptives Streaming aktivieren	Aktivieren Sie adaptives Streaming im XProtect Web Client und XProtect Mobile-Client (nur für XProtect Expert und XProtect Corporate). Diese Funktion ist standardmäßig aktiviert.
Streamingweisen	Wenn Sie die Funktion adaptives Streaming aktiviert haben, können Sie den Streamingmodus aus der Liste auswählen: • **Videoqualität optimieren (Standard)** - hierbei wird der Stream mit der geringsten verfügbaren Auflösung ausgewählt, die der geforderten Auflösung entspricht oder darüber liegt • **Leistung des Servers optimieren** - hierbei wird die geforderte Auflösung gesenkt und dann der Stream mit der geringsten verfügbaren Auflösung ausgewählt, die der reduzierten 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)

Beschränkungen für transcodierte Videostreams

Pegel 1

Bei **Pegel 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
Pegel 1	Aktivieren Sie das Kontrollkästchen, um die erste Begrenzungsstufe für die XProtect Mobile-Serverleistung zu aktivieren.
Max. FPS	Legen Sie einen Höchstwert für die maximale Anzahl von Bildern pro Sekunde (FPS) fest, die vom XProtect Mobile-Server an Clients gesendet werden soll.
Max. Bildauflösung	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 **Pegel 1** eine andere Begrenzungsstufe erzwingen möchten, können Sie stattdessen das Kontrollkästchen **Pegel 2** aktivieren. Der Wert der Einstellungen darf den auf der ersten Stufe festgelegten Wert nicht übersteigen. Wenn Sie für „Max. FPS“ auf **Pegel 1** beispielsweise 45 festlegen, können Sie für „Max. FPS“ auf **Pegel 2** maximal 44 festlegen.

Name	Beschreibung
Pegel 2	Aktivieren Sie das Kontrollkästchen, um die zweite Begrenzungsstufe für die XProtect Mobile-Serverleistung zu aktivieren.
CPU-Schwellenwert	Legen Sie für die CPU-Auslastung auf dem XProtect Mobile-Server einen Schwellenwert fest, bevor das System Videostreambegrenzungen erzwingt.
Bandbreiten-Schwellenwert	Legen Sie für die Bandbreitengrenze auf dem XProtect Mobile-Server einen Schwellenwert fest, bevor das System Videostreambegrenzungen erzwingt.
Max. FPS	Legen Sie einen Höchstwert für die maximale Anzahl von Bildern pro Sekunde (FPS) fest, die vom XProtect Mobile-Server an Clients gesendet werden soll.
Max. Bildauflösung	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 **Pegel 3** aktivieren, um eine dritte Begrenzungsstufe zu erstellen. Der Wert der Einstellungen darf den auf **Pegel 1** und **Pegel 2** festgelegten Wert nicht übersteigen. Wenn Sie für **Max. FPS** auf **Pegel 1** beispielsweise 45 und auf **Pegel 2** 32 festlegen, können Sie für **Max. FPS** auf **Pegel 3** maximal 31 festlegen.

Name	Beschreibung
Pegel 3	Aktivieren Sie das Kontrollkästchen, um die dritte Begrenzungsstufe für die XProtect Mobile-Serverleistung zu aktivieren.
CPU-Schwellenwert	Legen Sie für die CPU-Auslastung auf dem XProtect Mobile-Server einen Schwellenwert fest, bevor das System Videostreambegrenzungen erzwingt.
Bandbreiten-Schwellenwert	Legen Sie für die Bandbreitengrenze auf dem XProtect Mobile-Server einen Schwellenwert fest, bevor das System Videostreambegrenzungen erzwingt.
Max. FPS	Legen Sie einen Höchstwert für die Anzahl Bilder pro Sekunde (FPS) fest, die vom XProtect Mobile-Server an Clients gesendet werden soll.
Max. Bildauflösung	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
Untersuchungen ermöglichen	Aktivieren Sie dieses Kontrollkästchen, damit die Benutzer Untersuchungen erstellen können.
Untersuchungen-Ordner	Zeigt, wo Ihre Videoexporte auf Ihrer Festplatte gespeichert werden.
Untersuchungen anzeigen, die von anderen Benutzern durchgeführt werden	Aktivieren Sie dieses Kontrollkästchen, um Benutzern den Zugriff auf Untersuchungen zu gewähren, die sie nicht selbst erstellt haben.
Aktivieren Sie die Größenbegrenzung des Untersuchungsordners	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.
Aktivieren Sie die Speicherdauer für Untersuchungen:	Aktivieren Sie dieses Kontrollkästchen, um eine Speicherdauer für Untersuchungen festzulegen. Die Standardspeicherdauer beträgt sieben Tage.
Exportformate	Aktivieren Sie 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.
Zeitstempel für AVI-Exporte einschließen	Aktivieren Sie dieses Kontrollkästchen, um das Datum und die Uhrzeit für den Download der AVI-Datei anzuzeigen.
Codec für AVI-Exporte verwenden	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.
Für AVI-Exporte verwendete Audio-Bitrate	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
Untersuchungen	Listet die Untersuchungen auf, die bisher im System konfiguriert wurden. Verwenden Sie die Schaltfläche **Löschen** oder **Alle löschen**, wenn Sie eine Untersuchung nicht mehr benötigen. Auf diese Weise können Sie wieder Speicherplatz auf dem Server freigeben.
Untersuchungsdetails	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.

Registerkarte Video Push

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

Name	Beschreibung
Push-Video	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 on page 44), 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.

Die Benachrichtigungen sind standardmäßig deaktiviert.

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 on page 41

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

Name	Beschreibung
Benachrichtigungen	Aktivieren Sie dieses Kontrollkästchen, um Benachrichtigungen zu aktivieren.
Geräteregistrierung beibehalten	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. 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.

Registrierte Geräte

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

Registerkarte Zweistufige Verifikation

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

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 eine 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 on page 49.

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

Anbietereinstellungen > **E-Mail**

Name	Beschreibung
SMTP-Server	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.
SMTP-Server-Port	Geben Sie den Port des SMTP-Servers ein, der für den E-Mail-Versand verwendet werden soll. Die Standardportnummer lautet 25 ohne SSL und 465 mit SSL.
SSL verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn Ihr SMTP-Server SSL-Verschlüsselung unterstützt.
Benutzername	Geben Sie den Benutzernamen für die Anmeldung am SMTP-Server ein.
Passwort	Geben Sie das Passwort für die Anmeldung am SMTP-Server ein.
Sichere Passwortauthentifizierung (SPA) verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn Ihr SMTP-Server SPA unterstützt.
E-Mail-Adresse des Absenders	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	Geben Sie die Nachricht ein, die gesendet werden soll. Beispiel: Ihr Code lautet {0}. Wenn Sie die Variable {0} nicht angeben, wird der Code standardmäßig an das Textende angefügt.

Verifizierungscode-Einstellungen

Name	Beschreibung
Zeitüberschreitung bei Wiederverbindung (0–30 Minuten)	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. Diese Einstellung gilt nicht für XProtect Web Client.
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 Codeiengabeversuchen 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
	• **Lateinische Großbuchstaben (A-Z)** • **Lateinische Kleinbuchstaben (a-z)** • **Zahlen (0-9)** • **Sonderzeichen (!@#...)**

Benutzereinstellungen

Name	Beschreibung
Benutzer und Gruppen	Zeigt eine Liste der Benutzer und Gruppen an, die zum XProtect-System hinzugefügt wurden. Wenn eine Gruppe in Active Directory konfiguriert ist, bezieht der Mobile Server Informationen wie E-Mail-Adressen aus Active Directory. Windows-Gruppen unterstützen die zweistufige Verifikation nicht.
Verifizierungsverfahren	Wählen Sie für jeden Benutzer und jede Gruppe eine Verifikationseinstellung aus. Sie können auswählen zwischen: • **Keine Anmeldung**: der Benutzer kann sich nicht anmelden • **Keine zweistufige Verifikation**: der Benutzer muss Benutzername und Passwort eingeben • **E-Mail**: der Benutzer muss zusätzlich zu Benutzername und Passwort einen Prüfcode eingeben
Benutzerdetails	Geben Sie die E-Mail-Adresse ein, an die jedem Benutzer Codes geschickt werden.

Direktes Streaming

XProtect Mobile unterstützt das direkte Streaming im Live-Modus.

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. Der XProtect® Mobile-Client unterstützt auch die Verwendung des H.265-Codec. 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. Direktes Streaming erhöht auch die Leistung für dieselbe Hardware – bis zu fünfmal so viele gleichzeitige Videostreams im 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 on page 14).

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 on page 9)
- 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

XProtect Mobile unterstützt adaptives Streaming im Live-Modus.

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 können Sie die Funktion für Folgendes nutzen:

- Die Videoqualität zu optimieren - hierzu wird der Stream mit der geringsten verfügbaren Auflösung ausgewählt, die der geforderten Auflösung entspricht oder darüber liegt.
- Serverleistung optimieren - hierbei wird die geforderte Auflösung abgesenkt und dann der Stream mit der geringsten verfügbaren Auflösung ausgewählt, die der reduzierten Auflösung entspricht oder darüber liegt.

- Optimierung der Auflösung für geringe Bandbreiten - 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 on page 14).

Datenverschlüsselung des mobilen Servers (Erklärung)

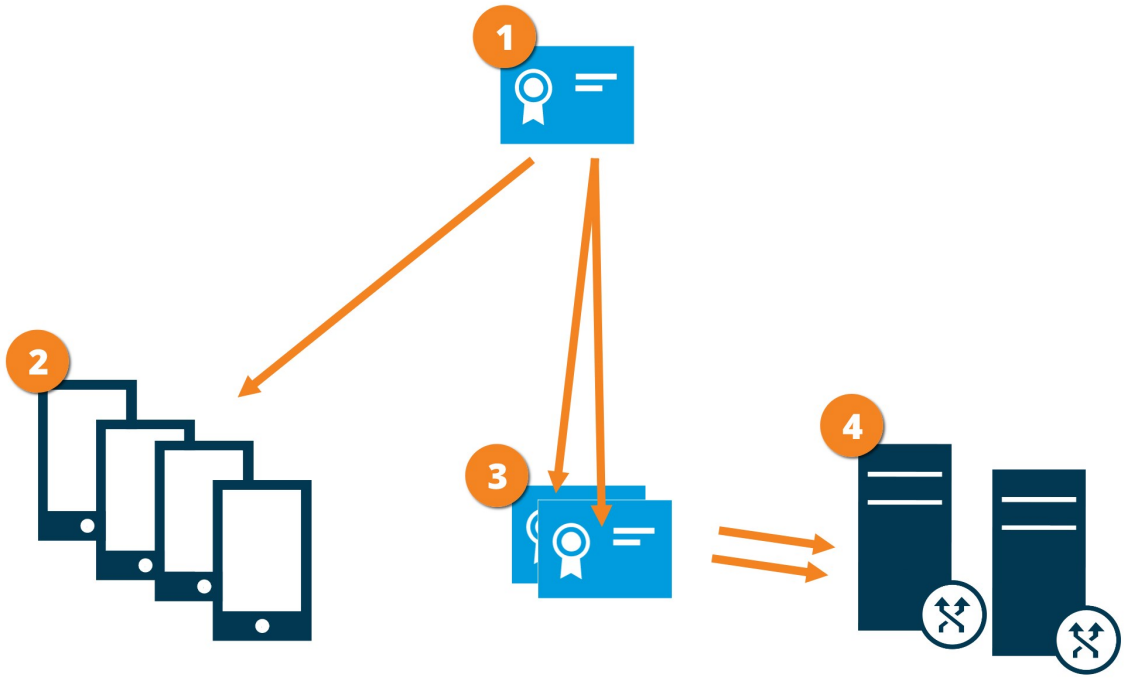
Aus Sicherheitsgründen empfiehlt Milestone, dass Sie bei der Verwaltung von Benutzerkonteneinstellungen zwischen dem Mobile Server und den Clients eine sichere Kommunikation verwenden.

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.

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.



❶ 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).

❷ 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

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

❹ 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.

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

Aktivieren Sie die Verschlüsselung auf dem mobilen Server.

Damit bei sicheren Verbindungen zwischen dem Mobile Server und Clients und Diensten ein HTTPS-Protokoll verwendet werden kann, müssen Sie auf dem Server ein gültiges Zertifikat anwenden. Das Zertifikat bestätigt, dass der Zertifikatsinhaber berechtigt ist, sichere Verbindungen herzustellen.

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

Wenn Sie die Verschlüsselung für eine Server-Gruppe konfigurieren, muss sie entweder mit Zertifikaten aktiviert werden, die zum selben CA-Zertifikat gehören, oder, wenn die Verschlüsselung deaktiviert ist, muss sie auf allen Computern in der Server-Gruppe deaktiviert werden.

Von einer ZS (Zertifizierungsstelle) ausgestellte Zertifikate verfügen über eine Zertifikatkette, deren Root das Root-Zertifikat der Zertifizierungsstelle ist. Wenn einem Gerät oder Browser dieses Zertifikat präsentiert wird, vergleicht es das Stammzertifikat mit den im Betriebssystem (Android, iOS, Windows usw.) vorinstallierten Stammzertifikaten. Ist das Stammzertifikat in der Liste der vorinstallierten Zertifikate enthalten, garantiert das Betriebssystem gegenüber dem Benutzer, dass die Verbindung ausreichend sicher ist. Diese Zertifikate werden für einen Domänennamen ausgestellt und sind nicht kostenlos erhältlich.

Schritte:

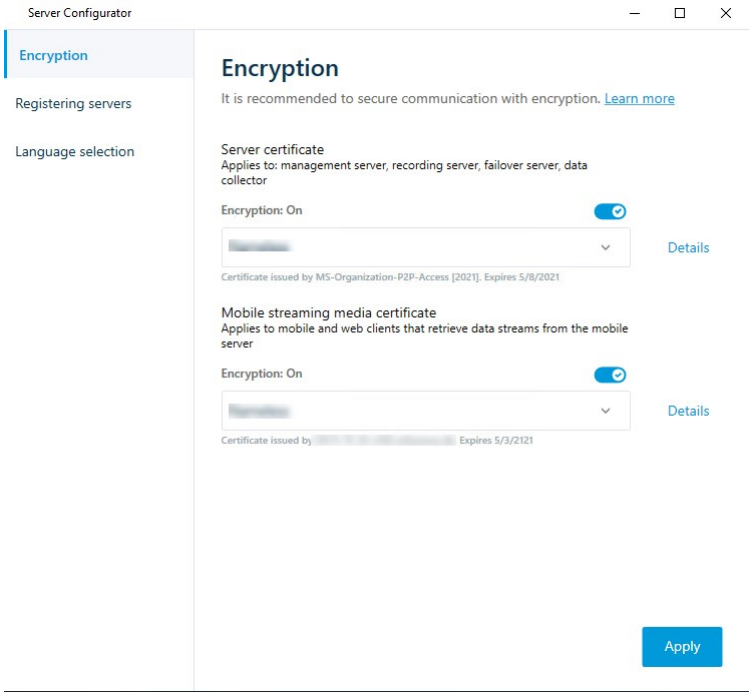
1. Öffnen Sie auf einem Computer mit installiertem mobilen Server die **Server Configurator** von:
   - Das Windows-Startmenü

   oder

   - Das Mobile Server Manager durch Klicken mit der rechten Maustaste auf das Symbol Mobile Server Manager auf der Taskleiste des Computers
2. Aktivieren Sie in der **Server Configurator**, unter **Zertifikat für mobile Streaming-Medien** die **Verschlüsselung**.
3. Klicken Sie auf **Zertifikat auswählen**, um eine Liste der eindeutigen Themennamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und die auf dem lokalen Computer im Windows Certificate Store installiert sind.
4. Wählen Sie ein Zertifikat für die Verschlüsselung der Kommunikation zwischen XProtect Mobile Client und XProtect Web Client mit dem Mobile Server aus.

Wählen Sie **Einzelheiten** aus, um die Angaben zum Windows Certificate Store zu dem ausgewählten Zertifikat anzuzeigen.

Der Benutzer des Dienstes Mobile Server hat Zugriff zum privaten Schlüssel erhalten. Diesem Zertifikat muss auf allen Clients vertraut werden.



5. Klicken Sie auf **Anwenden**.

Wenn Sie Zertifikate anwenden, wird der Mobile Server-Dienst neu gestartet.

Milestone Federated Architecture und übergeordnete/untergeordnete Standorte

Milestone Federated Architecture verbindet mehrere einzelne Standardsysteme zu einer föderalen Standorthierarchie mit über- und untergeordneten Standorten.

Um mit Ihrem XProtect Mobile oder XProtect Web Client Zugriff auf alle Standorte zu erhalten, installieren Sie den XProtect Mobile Server nur auf dem übergeordneten Standort.

Benutzer von XProtect Mobile Client oder XProtect Web Client müssen sich mit dem Management-Server am übergeordneten Standort verbinden.

Smart Connect

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:

.

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 on page 9

Registerkarte Konnektivität on page 18

Benachrichtigungen

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.

Die Benachrichtigungen sind standardmäßig deaktiviert.

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 on page 8 und Registerkarte Benachrichtigungen on page 27.

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. Lesen Sie die Warnung zu Ihren personenbezogenen Daten und wählen Sie **Ja** wenn Sie fortfahren möchten.
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**. Lesen Sie die Warnung zu Ihren personenbezogenen Daten und wählen Sie **Ja** wenn Sie fortfahren möchten

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.

Ein oder alle registrierten Geräte aus der Liste der registrierten Geräte entfernen

Wenn Sie die XProtect Mobile App deinstallieren oder das Gerät deaktivieren, können die Gerätedaten noch in der VMS-Datenbank gespeichert sein.

Die VMS entfernt die Geräteregistrierungsdaten, wenn:

- Sie einen Benutzer aus dem System entfernen.
- Milestone Care Plus wurde für mehr als 180 Tage nicht erneuert.

Es gibt jedoch Szenarien, in denen die Geräteregistrierungsdaten nicht automatisch entfernt werden.

Sie müssen ein oder alle registrierten Geräte manuell entfernen, wenn:

- Ein Benutzer hat sein Telefon verloren.
- Sie möchten den mobilen Server vollständig deinstallieren und seine Daten entfernen.
- Ein Benutzer hat aufgehört, die XProtect Mobile Client-App oder die Benachrichtigungen zu verwenden.
- Sie haben eine Active Directory (AD)-Gruppe zu einer VMS-Rolle hinzugefügt und die Berechtigungen für einen Benutzer haben sich geändert. Wenn Sie eine AD-Gruppe hinzufügen, sieht der VMS die Benutzer in dieser Rolle nicht. Wenn Sie einen Benutzer aus einer AD-Gruppe entfernen oder dem Benutzer die Verwendung des mobilen Servers untersagen, müssen Sie auch das Gerät des Benutzers manuell aus der Liste entfernen.

So entfernen Sie ein registriertes Gerät:

1. Wählen Sie im Management Client den mobilen Server aus und klicken Sie auf die Registerkarte **Benachrichtigungen**.
2. Gehen Sie wie folgt vor:
    - Für einzelne Geräte wählen Sie das Gerät aus und wählen dann **Entfernen**.
    - Für alle Geräte wählen Sie **Alle entfernen**.

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

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 on page 26 und Anforderungen für das Einrichten von Video Push on page 9.

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.

Fügen Sie den Video Push-Treiber als Hardwaregerät auf dem Aufzeichnungsserver hinzu

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 den Video-Push-Treiber ein:
   - Benutzername: Lassen Sie das Feld leer, um den Standardbenutzernamen zu verwenden.
   - Passwort: Geben Sie das **Milestone** - Passwort ein, das vom System erzeugt wird. Wenn Sie das Passwort beim Hinzufügen des Video Push-Kanals auf dem Mobile Server geändert haben, geben Sie das von Ihnen bevorzugte Passwort ein. 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 on page 9), 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 im Bereich **Eigenschaften** auf die Registerkarte **Client**.
   Weitere Informationen finden Sie auf der Registerkarte Client (Rollen).
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. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/xprotect-comparison/).

Mit der zweistufigen Verifikation auf dem -Server können Sie einen zusätzlichen Anmeldeschritt für Benutzer des XProtect Mobile XProtect Web Client-Clients oder XProtect Mobilefestlegen. 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 on page 49.
2. Den Verifizierungscode festlegen, der an Benutzer gesendet wird on page 49.
3. Benutzern und Active Directory-Gruppen ein Verifizierungsverfahren zuweisen on page 50.

Siehe auch Anforderungen für die Einrichtung der zweistufigen Verifikation für Benutzer on page 9 und Registerkarte Zweistufige Verifikation on page 28.

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 **Anbietereinstellungen** 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.

Weitere Informationen finden Sie unter Registerkarte Zweistufige Verifikation on page 28.

Den Verifizierungscode festlegen, der an Benutzer gesendet wird

So legen Sie die Komplexität des Verifizierungscodes 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 Codeiengabeversuchen 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 on page 28.

Benutzern und Active Directory-Gruppen ein Verifizierungsverfahren 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 **Verifizierungsmethode** eine Verifizierungsmethode für die einzelnen Benutzer oder Gruppen aus.
2. Geben Sie in das Feld **Benutzerdetails** 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 on page 28.

Aktionen

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 on page 15.

Mobilgeräteverwaltung (MDM)

Mobilgeräteverwaltung (Mobile Device Management, MDM) ist eine Software, die Mobilgeräte sichert, überwacht, verwaltet und unterstützt, die von Anwendern, Dienstleistern und Unternehmen eingesetzt werden.

MDM-Lösungen umfassen typischerweise eine Serverkomponente, die die Verwaltungsbefehle an die Mobilgeräte sendet, und eine Client-Komponente, die auf dem verwalteten Gerät läuft und die Managementbefehle empfängt und umsetzt.

Sie können den XProtect Mobile-Client verteilen und benutzerdefinierte Richtlinien zu den Geräten in Ihrem Unternehmen hinzufügen.

Um die MDM-Funktionalität auf einem mobilen Gerät zu nutzen, müssen Sie die Daten des mobilen Servers auf der MDM-Softwareplattform konfigurieren. Die Daten des mobilen Servers umfassen den Servernamen, die Serveradresse, den Server-Port und das Verbindungstypprotokoll.

Wenn Sie die Daten eines bereits hinzugefügten mobilen Servers aktualisiert haben, muss der Anwender diesen Server manuell aus der Liste **Server** löschen und die XProtect Mobile App neu starten.

Konfiguration der Details des mobilen Servers auf der MDM-Plattform (Administratoren)

Um den XProtect Mobile-Client über eine MDM-Plattform an mobile Geräte zu übertragen und zu verwalten, müssen Sie die Serverdetails hinzufügen. Weitere Informationen zur Konfiguration finden Sie in der Dokumentation zu Ihrer MDM-Software.

Wenn Sie keine der obligatorischen Serverangaben eingegeben haben oder falsche Angaben gemacht haben, wird der mobile Server nicht zur XProtect Mobile-App hinzugefügt.

Für Android-Benutzer

Sie können die Serverdaten in der Benutzeroberfläche Ihrer MDM-Plattform angeben. Sie haben die Möglichkeit, eine verwaltete Konfigurationsdatei mit den Serverdaten hochzuladen.

Serverdaten:

- **Servername** – (Obligatorisch) Geben Sie den Servernamen ein
- **Serveradresse** – (Obligatorisch) Geben Sie die Serveradresse ein
- **Server-Port** – (Obligatorisch) Geben Sie die Portnummer des Servers ein
- **Verbindungsprotokolltyp** – Aktivieren Sie diese Option, wenn Sie eine HTTPS-Verbindung verwenden. Deaktivieren Sie diese Option, wenn Sie eine HTTP-Verbindung verwenden. Standardmäßig ist die HTTPS-Verbindung aktiviert

Hochladen der Datei auf Ihre MDM-Plattform:

1. Am Ende dieses Handbuchs, in Anhang A, finden Sie die verwaltete Konfigurationsvorlage für Android-Geräte. Kopieren Sie den Inhalt.
2. Öffnen Sie einen Texteditor Ihrer Wahl und fügen Sie den Inhalt ein.
3. Geben Sie die Serverdaten in den Feldern **android:description** an.
4. Speichern Sie die Datei als .XML.
5. Öffnen Sie Ihre MDM-Plattform und laden Sie die verwaltete Konfigurationsdatei hoch.

Für iOS-Benutzer

Um iOS-Geräte über eine MDM-Plattform zu verwalten, müssen Sie die Verbindungsdetails in der verwalteten Konfigurationsdatei angeben.

1. Am Ende dieses Handbuchs, in Anhang B, finden Sie die verwaltete Konfigurationsvorlage für iOS-Geräte. Kopieren Sie den Inhalt.
2. Öffnen Sie einen Texteditor Ihrer Wahl und fügen Sie den Inhalt ein.
3. Geben Sie die Serverdaten an:
    - **versionConfig** – (Obligatorisch) Geben Sie die Standardversion der App-Konfiguration ein **1.0.0**
    - **serverNameConfig** – (Obligatorisch) Geben Sie den Servernamen ein
    - **serverAddressConfig** – (Obligatorisch) Geben Sie die Serveradresse ein
    - **serverPortConfig** – (Obligatorisch) Geben Sie die Portnummer des Servers ein
    - **serverConnectionProtocolTypeConfig** – Der Standardverbindungstyp ist **HTTPS**; um eine nicht sichere Verbindung zu verwenden, geben Sie **HTTP** ein
4. Speichern Sie die Datei als .XML.
5. Öffnen Sie Ihre MDM-Plattform und laden Sie die verwaltete Konfigurationsdatei hoch.

Einen Ausgang zur Verwendung im XProtect Mobile-Client und XProtect Web Client benennen

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.

Für weitere Informationen siehe Ausgang.

Externer IDP und XProtect Mobile

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

Sie können sich in XProtect Web Client oder dem XProtect Mobile-Client über einen externen IDP mit XProtect 2022 R3 und höher anmelden.

Um sich mit einem externen IDP bei XProtect Web Client oder dem XProtect Mobile-Client anzumelden, müssen Sie eine HTTPS-Verbindung verwenden.

Bevor Sie einen externen IDP-Login für XProtect Web Client und den XProtect Mobile-Client konfigurieren, stellen Sie sicher, dass Sie Folgendes getan haben:

- Fügen Sie einen externen IDP hinzu und konfigurieren Sie ihn
- Registrierte Ansprüche
- Ansprüche auf Rollen abgebildet

Weitere Informationen finden Sie im Administratorhandbuch für XProtect VMS.

Um sich bei XProtect Web Client über einen externen IDP anzumelden, benötigen Sie eine zusätzliche Konfiguration. Siehe Konfigurieren des externen IDP-Logins für XProtect Web Client on page 54.

Konfigurieren des externen IDP-Logins für XProtect Web Client

Die Option zur Anmeldung über einen externen IDP an XProtect Web Client ist nur für HTTPS Verbindungen verfügbar.

1. Wählen Sie in Management Client **Extras** > **Optionen** und öffnen Sie die Registerkarte **externer IDP**.
2. Wählen Sie im Abschnitt **Umleitungs-URIs für Webclients** die Option **Hinzufügen**.
3. Geben Sie die Adressen für XProtect Web Client im Format `https://[address]:[port number]/index.html` ein:
    - Geben Sie als Adresse den Hostnamen oder die IP-Adresse des Computers ein, auf dem der mobile Server läuft
    - Geben Sie als Portnummer den Port ein, den XProtect Web Client für die Kommunikation mit dem mobilen Server verwendet. Für HTTPS-Verbindungen lautet die Standard-Portnummer 8082

Notfallalarme hinzufügen

Wenn eine potenzielle Gefahr erkannt wurde, können XProtect Mobile Client-Benutzer mit dem Notfallalarm Alarmbenachrichtigungen der höchsten Dringlichkeitsstufe erhalten, die Alarmdetails einsehen und sofort handeln. Ein Notfallalarm ist ein Alarmtyp, den Sie in XProtect Management Client definieren.

Damit dies funktioniert, sind Push-Benachrichtigungen erforderlich. Push-Benachrichtigungen sind nur verfügbar, wenn Sie eine Milestone Care Plus-Lizenz erworben haben.

Diese Funktion steht nur bei bestimmten XProtect VMS-Produkten zur Verfügung. Die vollständige Liste der Funktionen finden Sie auf der Produktübersichtsseite auf der Milestone Website (https://www.milestonesys.com/products/software/xprotect-comparison/).

Zum Hinzufügen eines solchen Alarms müssen Sie:

1. Eine neue Alarmkategorie mit Stufe 99 hinzufügen, und zwar in **Alarme** > **Alarmdateneinstellungen**. Sie können so viele Kategorien mit Stufe 99 erstellen, wie Sie benötigen.
2. Fügen Sie eine Alarmdefinition mit dieser Kategorie hinzu.

Wartung

Mobile Server Manager

Beim Mobile Server Manager handelt es sich um eine Taskleisten-gesteuerte Funktion, die mit dem Mobilen 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 on page 55
- Den Mobile Server-Dienst starten, anhalten oder neu starten on page 56
- Passworteinstellungen für den Datenschutz ändern on page 56
- Portnummern anzeigen/bearbeiten on page 57
- Aktivieren Sie die Verschlüsselung auf dem mobilen Server. on page 35 mithilfe des **Server Configurator**
- Öffnen Sie die heutige Protokolldateien (siehe Zugriff auf Protokolle und Untersuchungen on page 57)
- Öffnen Sie den Protokollordner (siehe Zugriff auf Protokolle und Untersuchungen on page 57)
- Öffnen Sie den Ordner mit den Untersuchungen (siehe Zugriff auf Protokolle und Untersuchungen on page 57)
- Untersuchungen-Ordner ändern on page 58
- Siehe XProtect Mobile Server Status (siehe Status anzeigen on page 58)

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 Internetbrowser (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 Porteinstellungen 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.

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**.

Zugriff auf Protokolle und Untersuchungen

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

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

Lastausgleich für den mobilen Server verwenden

Als zusätzliche Sicherheitsmaßnahme verwendet XProtect Mobile bei der Kommunikation zwischen dem Server und der mobilen App IDs. Wenn sich ein Benutzer zum ersten Mal über die XProtect Mobile-App mit einem mobilen Server verbindet, wird die Server-ID des mobilen Servers auf das Gerät des Benutzers kopiert. Bei jedem Versuch, eine Verbindung zu einem mobilen Server herzustellen, werden die Server-IDs mit den ursprünglich erhaltenen IDs verglichen.

Standardmäßig hat jeder Server eine eindeutige Server-ID. Um einer Lastausgleichsgruppe einen mobilen Server hinzuzufügen, müssen Sie dafür sorgen, dass die ID des mobilen Servers mit der von den anderen mobilen Servern in der Gruppe verwendeten IDs übereinstimmt.

Auf einem Host in der Lastausgleichsgruppe

So kopieren Sie die Server-IDs von einem Host:

1. Gehen Sie zu `C:\ProgramFiles\Milestone\Milestone Mobile Server` und kopieren Sie die Datei **VideoOS.MobileServer.Service.exe.config**.
2. Fügen Sie die Datei auf Ihrem Desktop ein und öffnen Sie sie mit einem beliebigen Textverarbeitungsprogramm.

3. Durchsuchen Sie die Datei nach dem `ServerSettings`-Tag. Es sieht wie folgt aus:

```
<ServerSetings>
 <Identification>
  <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
  <add key="ServiceIdS" value="10353810-803F-4880-BC22-417B37F1A1C8">
  <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
 </Identification>
---
</ServerSettings>
```

4. Kopieren Sie die Werte für **ServiceID** und **ReportedServiceID**.

Auf den anderen Hosts, die zu der Gruppe gehören

Auf einem Host, der zur Lastausgleichsgruppe gehört:

1. Gehen Sie zu `C:\ProgramFiles\Milestone\Milestone Mobile Server` und öffnen Sie die Datei **VideoOS.MobileServer.Service.exe.config** mit einem beliebigen Textverarbeitungsprogramm.
2. Durchsuchen Sie die Datei nach dem `ServerSettings`-Tag und ersetzen Sie die Werte für **ServiceID** und **ReportedServiceID** durch die Werte aus der ursprünglichen Konfigurationsdatei.
3. Starten Sie den Mobile Server-Dienst neu, damit die Änderungen angewendet werden.
4. Bitten Sie die XProtect Mobile-Client-Benutzer, den mobilen Server erneut hinzuzufügen.

Wiederholen Sie die Schritte auf allen Hosts, die zur Lastausgleichsgruppe gehören.

Mobilen Server zu einem anderen Host migrieren

Als zusätzliche Sicherheitsmaßnahme verwendet XProtect Mobile bei der Kommunikation zwischen dem Server und der mobilen App IDs. Wenn sich ein Benutzer zum ersten Mal über die XProtect Mobile-App mit einem mobilen Server verbindet, wird die Server-ID des mobilen Servers auf das Gerät des Benutzers kopiert. Immer, wenn die App versucht, eine Verbindung zu einem mobilen Server herzustellen, vergleicht sie die Server-IDs mit den ursprünglichen IDs. Wenn die Server-IDs nicht übereinstimmen, schlägt die Verbindung fehl.

Wenn Sie den mobilen Server zu einem anderen Host migrieren und die ursprüngliche Adresse beibehalten, müssen Sie auch die Server-ID des alten Servers beibehalten.

Auf dem alten Host

Erledigen Sie Folgendes, bevor Sie zu Ihrem mobilen Server migrieren:

1. Gehen Sie zu `C:\ProgramFiles\Milestone\Milestone Mobile Server`, kopieren Sie die Datei **VideoOS.MobileServer.Service.exe.config** und öffnen Sie sie mit einem beliebigen Textverarbeitungsprogramm.

2. Durchsuchen Sie die Datei nach dem `ServerSettings`-Tag. Es sieht wie folgt aus:

```
<ServerSetings>
 <Identification>
  <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
  <add key="ServiceIdS" value="10353810-803F-4880-BC22-417B37F1A1C8">
  <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
 </Identification>
---
</ServerSettings>
```

3. Kopieren Sie die Werte für **ServiceID** und **ReportedServiceID**.

Sie können Ihren mobilen Server jetzt migrieren.

Auf dem neuen Host

Gehen Sie nach der Installation und Konfiguration des mobilen Servers auf dem neuen Host wie folgt vor:

1. Gehen Sie zu `C:\ProgramFiles\Milestone\Milestone Mobile Server` und öffnen Sie die Datei **VideoOS.MobileServer.Service.exe.config** mit einem beliebigen Textverarbeitungsprogramm.
2. Durchsuchen Sie die Datei nach dem `ServerSettings`-Tag und ersetzen Sie die Werte für **ServiceID** und **ReportedServiceID** durch die Werte aus der ursprünglichen Konfigurationsdatei.
3. Starten Sie den Mobile Server-Dienst neu, damit die Änderungen angewendet werden.
4. Bitten Sie die XProtect Mobile-Client-Benutzer, den mobilen Server erneut hinzuzufügen.

Fehlerbehandlung

Fehlerbehandlung XProtect Mobile

Verbindungen

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 on page 14).

Das Serveradressenfeld muss einen gültigen Hostnamen enthalten, wenn es auf das iOS Gerät angewendet wird. Gültige Hostnamen können die ASCII-Buchstaben „a“ bis „z“ (Groß- und Kleinschreibung werden unterschieden), die Ziffern „0“ bis „9“, Punkte und Bindestriche („-“) enthalten.

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.

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.

Ich habe die Adresse des mobilen Servers nicht geändert, aber die Benutzer des XProtect Mobile-Client können keine Verbindung mehr dazu herstellen. Warum?

Die XProtect Mobile-Clients stellenüber eine eindeutige Service-ID eine Verbindung zum mobilen Server her. Selbst wenn der Hostname und die IP-Adresse des Computers mit dem mobilen Server unverändert bleiben, stimmt die Service-ID unter Umständen nicht mit der für die Clients gespeicherten ID überein. Das ist zum Beispiel in folgenden Situationen der Fall:

- Sie haben Ihren Computer zurückgesetzt und den mobilen Server neu installiert.
- Sie haben den mobilen Server auf einen anderen Computer verschoben, aber die ursprüngliche Konfiguration beibehalten.

Sie können wie folgt vorgehen, um die Verbindung wiederherzustellen:

- Aktualisieren Sie die Service-ID auf dem neuen mobilen Server, damit sie der Service-ID aus der vorherigen Konfiguration entspricht. Siehe https://developer.milestonesys.com/s/article/unable-to-establish-connection-to-XProtect-Mobile-Server-using-Android-iOS-client.
- Bitten Sie die Benutzer des XProtect Mobile-Client, sich neu mit dem mobilen Server zu verbinden.

Bildqualität

Warum ist die Bildqualität manchmal so schlecht, wenn ich mir Videoaufzeichnungen im XProtect Mobile-Client anschaue?

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.

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

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://www.intel.com/content/www/us/en/ark/featurefilter.html?productType=873&0_QuickSyncVideo=True), 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 on page 58).

Unterstützt mein Betriebssystem die hardwarebeschleunigte Dekodierung?

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

Achten Sie darauf, dass auf Ihrem System die aktuellen Grafiktreiber installiert sind. Diese Treiber sind nicht über das Windows-Update erhältlich.

Wie deaktiviere ich die hardwarebeschleunigte Dekodierung auf dem Mobilen Server? (Erweitert)

- Wenn der Prozessor auf dem Mobilen 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 Dateiendung .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.

Benachrichtigungen

Ich habe keine Änderungen in der Benachrichtigungskonfiguration vorgenommen, aber die registrierten Geräte erhalten keine Benachrichtigungen mehr. Warum?

Wenn Sie Ihre Lizenz aktualisiert haben oder Ihr Milestone Care Abo erneuert haben, müssten Sie den Mobile Server Dienst neu starten.

Anhänge

Anhang A

Verwaltete Konfigurationsvorlage für Android

```
<?xml version="1.0" encoding="utf-8"?>

<restrictions xmlns:android="http://schemas.android.com/apk/res/android">

    <restriction
        android:defaultValue="1.0.0"
        android:description="The current version of the app configuration"
        android:key="version_config"
        android:restrictionType="hidden"
        android:title="Version" />

    <restriction
```

```
        android:description="(Mandatory) Enter the server name."
        android:key="server_name_config"
        android:restrictionType="string"
        android:title="Server name" />

    <restriction
        android:description="(Mandatory) Enter the server address."
        android:key="server_address_config"
        android:restrictionType="string"
        android:title="Server address" />

    <restriction
        android:description="(Mandatory) Enter the server port."
```

```
        android:key="server_port_config"

        android:restrictionType="integer"

        android:title="Server port" />


    <restriction

        android:description="Enable when you use an HTTPS connection. Disable when
you use an HTTP connection."

        android:key="server_secure_connection_config"

        android:restrictionType="bool"

        android:title="Connection protocol type"

        android:defaultValue="true"/>


</restrictions>
```

Anhang B

Verwaltete Konfigurationsvorlage für iOS

```
<managedAppConfiguration>
    <version>1</version>
    <bundleId>com.milestonesys.XProtect</bundleId>
    <dict>
        <string keyName="versionConfig">
            <defaultValue>
                <value>1.0.0</value>
            </defaultValue>
        </string>
        <string keyName="serverNameConfig">
        </string>
        <string keyName="serverAddressConfig">
        </string>
```

```
        <string keyName="serverPortConfig">
        </string>
        <string keyName="serverConnectionProtocolTypeConfig">
            <defaultValue>
                <value>HTTPS</value>
            </defaultValue>
        </string>
    </dict>
    <presentation defaultLocale="en-US">
        <field keyName="versionConfig" type="input">
            <label>
                <language value="en-US">Version</language>
            </label>
            <description>
```

```
                <language value="en-US">The current version of the app
configuration</language>

            </description>

        </field>

    <fieldGroup>

        <name>

            <language value="en-US">Mobile server</language>

        </name>

        <field keyName="serverNameConfig" type="input">

            <label>

                <language value="en-US">Server name</language>

            </label>

            <description>

                <language value="en-US">(Mandatory) Enter the server
name.</language>
```

```
            </description>
        </field>
        <field keyName="serverAddressConfig" type="input">
            <label>
                <language value="en-US">Server address</language>
            </label>
            <description>
                <language value="en-US">(Mandatory) Enter the server
address.</language>
            </description>
        </field>
        <field keyName="serverPortConfig" type="input">
            <label>
                <language value="en-US">Server port</language>
```

```
            </label>

            <description>

                <language value="en-US">(Mandatory) Enter the server
port.</language>

            </description>

        </field>

        <field keyName="serverConnectionProtocolTypeConfig" type="input">

            <label>

                <language value="en-US">Connection protocol type</language>

            </label>

            <description>

                <language value="en-US">To specify the connection protocol type,
enter HTTPS or HTTP.</language>

            </description>

        </field>
```

```
    </fieldGroup>

    </presentation>

</managedAppConfiguration>
```

helpfeedback@milestone.dk

Info über Milestone

Milestone Systems ist ein weltweit führender Anbieter von Open-Platform-Videomanagementsoftware – Technologie, die Unternehmen hilft für Sicherheit zu sorgen, Ressourcen zu schützen und die Wirtschaftlichkeit zu erhöhen. Milestone Systems ist die Basis einer Open Platform Community, die die Zusammenarbeit und Innovation bei der Entwicklung und dem Einsatz von Netzwerkvideotechnologie vorantreibt und für zuverlässige, individuell anpassbare Lösungen sorgt, die sich an über 150.000 Standorten auf der ganzen Welt bewährt haben. Milestone Systems wurde 1998 gegründet und ist ein eigenständiges Unternehmen der Canon Group. Weitere Informationen erhalten Sie unter https://www.milestonesys.com/.