

MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile Server 2020 R1

Bedienungsanleitung für Administratoren



Inhalt

Copyright, Marken und Verzichtserklärung	5
Übersicht	6
XProtect Mobile (erklärt)	6
XProtect Mobile-Server (Erklärung)	6
Produktvergleichstabelle	7
Anforderungen und Hinweise	10
Voraussetzungen für die Verwendung von XProtect Mobile	10
XProtect Mobile-Systemanforderungen	10
Anforderungen für das Einrichten von Benachrichtigungen	10
Anforderungen für das Einrichten von Smart Connect	11
Anforderungen für die Einrichtung der zweistufigen Verifikation für Benutzer	11
Anforderungen für das Einrichten von Video Push	11
Anforderungen zur Verschlüsselung Mobiler Server für Clients	11
Installation	12
XProtect Mobile-Server installieren	12
Konfiguration	14
Einstellungen des mobilen Servers	14
Allgemein	14
Registerkarte Konnektivität	16
Registerkarte Serverstatus	17
Registerkarte Leistung	18
Registerkarte Untersuchungen	21
Registerkarte Video Push	22
Registerkarte Benachrichtigungen	23
Registerkarte Zweistufige Verifikation	24
Sichere Kommunikation (Erläuterung).	26
Verschlüsselung des Management-Servers (Erläuterung):	27
Verschlüsselung vom Management-Server zum Aufzeichnungsserver (Erläuterung)	29

Verschlüsselung an alle Clients und Dienste, die Daten vom Aufzeichnungsserver abrufen (Erläuterung)	30
Datenverschlüsselung des Mobilien Servers (Erläuterung)	32
Anforderungen zur Verschlüsselung Mobiler Server für Clients	33
Verschlüsselung aktivieren	33
Verschlüsselung zu Clients und Servern aktivieren	33
Die Verschlüsselung zum Management-Server aktivieren	35
Die Verschlüsselung vom Management-Server aus aktivieren	36
Aktivieren Sie die Verschlüsselung auf dem Mobilien Server.	39
Zertifikate bearbeiten	40
Milestone Federated Architecture und den Master/Slave Servern (Erklärung)	40
Smart Connect (Erklärung)	40
Einrichten von Smart Connect	41
Aktivieren Sie die UPnP-Erkennungsfunktion in Ihrem Router	41
Aktivieren von Verbindungen im komplexen Netzwerk	41
Konfigurieren der Verbindungseinstellungen	42
Senden einer E-Mail-Nachricht an Benutzer	42
Senden von Benachrichtigungen (Erklärung)	43
Konfigurieren von Push-Benachrichtigungen auf dem XProtect Mobile-Server	43
Aktivieren von Push-Benachrichtigungen für bestimmte oder alle Mobilgeräte	44
Deaktivieren des Sendens von Push-Benachrichtigungen an bestimmte oder alle Mobilgeräte	44
Einrichten von Untersuchungen	45
Nutzung von Video Push für Videostreams (Erklärung)	46
Einrichten von Video Push für Videostreams	46
Einen video push-Kanal für Video-Streaming hinzufügen	47
Einen video push-Kanal entfernen	47
Den video push-Treiber als Gerät auf dem hinzufügen Recording Server	47
Hinzufügen des video push-Treibergeräts zum video push-Kanal	48
Aktivieren Sie Audio für den vorhandenen Push-Videokanal	49
Einrichten von Benutzern für die zweistufige Verifikation über E-Mail	49
Informationen über den SMTP-Server eingeben	50

Den Verifizierungscode festlegen, der an Benutzer gesendet wird	50
Benutzern und Active Directory-Gruppen eine Anmeldemethode zuweisen	50
Aktionen (erklärt):	51
Einen Ausgang zur Verwendung im XProtect Mobile-Client und XProtect Web Client benennen (Erklärung)	51
Wartung	53
Mobile Server Manager (erklärt)	53
Zugriff auf XProtect Web Client	53
Den Mobile Server-Dienst starten, anhalten oder neu starten	54
Management-Server-Adresse eintragen/bearbeiten	54
Portnummern anzeigen/bearbeiten	55
Zertifikate bearbeiten	55
Zugriff auf Protokolle und Untersuchungen (erklärt)	55
Untersuchungen-Ordner ändern	56
Status anzeigen (Erklärung)	56
Fehlerbehandlung	58
Fehlerbehandlung XProtect Mobile	58

Copyright, Marken und Verzichtserklärung

Copyright © 2020 Milestone Systems A/S

Marken

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

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

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

Haftungsausschluss

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

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

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

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

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

Übersicht

XProtect Mobile (erklärt)

XProtect Mobile besteht aus fünf Komponenten:

- XProtect Mobile-Client

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

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

- XProtect Web Client

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

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

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

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

XProtect Mobile-Server (Erklärung)

XProtect Mobile-Server verwaltet Anmeldungen im System von XProtect Mobile-Client oder XProtect Web Client.

Ein XProtect Mobile-Server überträgt Videostreams von Aufzeichnungsservern an den XProtect Mobile-Client oder XProtect Web Client. Dadurch wird eine sichere Konfiguration geboten, da die Aufzeichnungsserver nie direkt 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 dem Mobilgerät ermöglichen.

Sie müssen die XProtect Mobile-Serverkomponente auf dem Computer installieren, über den Sie auf die Aufzeichnungsserver zugreifen möchten. Melden Sie sich bei der Installation des XProtect Mobile-Servers mit einem Konto an, das über Administratorrechte verfügt. Andernfalls kann die Installation nicht erfolgreich abgeschlossen werden.

Für weitere Informationen, siehe XProtect Mobile-Server installieren auf Seite 12

Produktvergleichstabelle

XProtect VMS beinhaltet die folgenden Produkte:

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

Die vollständige Funktionsliste finden Sie auf der Produktübersichtseite auf der Milestone-Website (<https://www.milestone.com/solutions/platform/product-index/>).

Nachfolgend finden Sie eine Liste der Hauptunterschiede zwischen den Produkten:

Name	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Standorte pro SLC	1	1	Mehrere Standorte	Mehrere Standorte	Mehrere Standorte
Aufzeichnungsserver pro SLC	1	1	Unbegrenzt	Unbegrenzt	Unbegrenzt
Geräte pro Aufzeichnungsserver	8	48	Unbegrenzt	Unbegrenzt	Unbegrenzt
Milestone Interconnect™	-	Remote-System	Remote-System	Remote-System	Zentraler/Remote-System
Milestone Federated Architecture™	-	-	-	Remote-System	Zentraler/Remote-System
Aufzeichnungsserver-Failover	-	-	-	Cold- und Hot-Standby	Cold- und Hot-Standby
Fernzugriffsdienste	-	-	-	-	✓
Edge-Speicher-Unterstützung	-	-	✓	✓	✓
Mehrschichtige Videospeicherarchitektur	Live-Datenbanke n + 1 Archiv	Live-Datenbanke n + 1 Archiv	Live-Datenbanke n + 1 Archiv	Live-Datenbanke n + unbegrenzte Archive	Live-Datenbanken + unbegrenzte Archive

Name	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
SNMP-Benachrichtigung	-	-	-	✓	✓
Zeitgesteuerte Benutzerzugriffsrechte	-	-	-	-	✓
Bildrate reduzieren (Ausdünnung)	-	-	-	✓	✓
Videodatenverschlüsselung (Aufzeichnungsserver)	-	-	-	✓	✓
Datenbanksignatur (Recording-Server)	-	-	-	✓	✓
PTZ-Prioritätsstufen	1	1	3	32000	32000
Erweitertes PTZ (PTZ-Sitzung und Wachrundgang über XProtect Smart Client reservieren)	-	-	-	✓	✓
Beweissicherung	-	-	-	-	✓
Lesezeichenfunktion	-	-	Nur manuell	Manuell und regelbasiert	Manuell und regelbasiert
Live-Multi-streaming oder Multicasting	-	-	-	✓	✓
Gesamtsicherheit	Client-Benutzerrechte	Client-Benutzerrechte	Client-Benutzerrechte	Client-Benutzerrechte	Client-Benutzerrechte/ Administrator-Benutzerrechte
XProtect Management Client-Profil	-	-	-	-	✓
XProtect Smart Client-Profil	-	-	3	3	Unbegrenzt
XProtect Smart Wall	-	-	-	Optional	✓
Systemmonitor	-	-	-	✓	✓

Name	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Smart Map	-	-	-	✓	✓
Zweistufige Verifizierung	-	-	-	-	✓
DLNA-Support	-	✓	✓	✓	✓
Privatsphärenausblendung	-	✓	✓	✓	✓
Gerätepasswortverwaltung			✓	✓	✓

Anforderungen und Hinweise

Voraussetzungen für die Verwendung von XProtect Mobile

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

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

Mehr über Anforderungen lesen Sie unter XProtect Mobile-Systemanforderungen auf Seite 10.

XProtect Mobile-Systemanforderungen

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

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

Anforderungen für das Einrichten von Benachrichtigungen

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

Für weitere Informationen, siehe:

Konfigurieren von Push-Benachrichtigungen auf dem XProtect Mobile-Server auf Seite 43

Registerkarte Benachrichtigungen auf Seite 23

Anforderungen für das Einrichten von Smart Connect

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

Anforderungen für die Einrichtung der zweistufigen Verifikation für Benutzer

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

Für weitere Informationen, siehe:

Einrichten von Benutzern für die zweistufige Verifikation über E-Mail auf Seite 49

Registerkarte Zweistufige Verifikation auf Seite 24

Anforderungen für das Einrichten von Video Push

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

Anforderungen zur Verschlüsselung Mobiler Server für Clients

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.

Wenn Sie zur Verschlüsselung des Mobilens Servers ein selbst signiertes Zertifikat auswählen, XProtect Mobile so kann der Client keine Verbindung zum Mobilens Server herstellen.

Installation

XProtect Mobile-Server installieren

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

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



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

Zum Installieren des XProtect Mobile-Servers:

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



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

7. Nur für die benutzerdefinierte Installation: Wählen Sie die Komponenten aus, die Sie installiert haben möchten. Klicken Sie dann auf **Weiter**.
8. Geben Sie die Verschlüsselung für den Mobilserver an. Klicken Sie dann auf **Weiter**.

Auf der Seite **Verschlüsselung für den Mobilien Server angeben** können Sie die Kommunikation zwischen dem mobilen Server und den Clients und Diensten sichern.



Wenn Sie die Verschlüsselung nicht aktivieren, stehen bestimmte Funktionen auf manchen Clients nicht zur Verfügung. Weitere Informationen finden Sie unter Anforderungen zur Verschlüsselung Mobiler Server für Clients auf Seite 33.

Wählen Sie von der Liste ein gültiges Zertifikat aus. Weitere Informationen zur Vorbereitung Ihres Systems für die sichere Kommunikation finden Sie unter Datenverschlüsselung des Mobilien Servers (Erläuterung) auf Seite 32 oder im Leitfaden *MilestoneZertifikate* (nur in englischer Sprache verfügbar).

Nach Abschluss der Installation können Sie die Verschlüsselung auch vom Taskleistensymbol Mobile Server Manager im Aufgabenbereich Ihres Betriebssystems aus aktivieren (s. Aktivieren Sie die Verschlüsselung auf dem Mobilien Server. auf Seite 39).

9. Wählen Sie das Dienstkonto für den Mobilien Server aus. Klicken Sie dann auf **Weiter**.



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

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



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

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

Sie sind jetzt bereit zur Konfiguration von XProtect Mobile (siehe Einstellungen des mobilen Servers auf Seite 14).

Konfiguration

Einstellungen des mobilen Servers

In Management Client können Sie eine Liste der XProtect Mobile-Servereinstellungen über Registerkarten unten in der Symbolleiste des Abschnitts **Eigenschaften** des mobilen Servers konfigurieren und bearbeiten. Von dort können Sie:

- Allgemeine Konfiguration der Serverfunktionen aktivieren oder deaktivieren (siehe Allgemein auf Seite 14)
- Konfigurieren Sie die Verbindungseinstellungen für den Server und richten Sie die Funktion Smart Connect ein (siehe die Registerkarte Registerkarte Konnektivität auf Seite 16)
- Aktuellen Status und aufgelistete aktive Benutzer anzeigen (siehe Registerkarte Serverstatus auf Seite 17)
- Leistungsparameter einrichten, zum Beispiel um Bilder in Normalgröße aktivieren oder Wiedergabe-Streams einzuschränken (siehe Registerkarte Leistung auf Seite 18)
- Untersuchungseinstellungen konfigurieren (siehe Registerkarte Untersuchungen auf Seite 21)
- Video push-Einstellungen konfigurieren (siehe Registerkarte Video Push auf Seite 22)
- System und Push-Benachrichtigungen einrichten, ein- und ausschalten (siehe Registerkarte Benachrichtigungen auf Seite 23)
- Zusätzliche Anmeldeschritte für Benutzer aktivieren und konfigurieren (siehe Registerkarte Registerkarte Zweistufige Verifikation auf Seite 24)

Allgemein

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

Allgemein

Name	Beschreibung
Servername	Geben Sie einen Namen für den XProtect Mobile-Servers ein.
Beschreibung	Geben Sie eine optionale Beschreibung für den XProtect Mobile-Server ein.
Mobiler Server	Siehe den Namen des aktuell ausgewählten XProtect Mobile-Servers.
Anmeldemethode	Wählen Sie die Authentifizierungsmethode für die Anmeldung beim Server aus. Sie haben folgende Optionen: <ul style="list-style-type: none"> • Automatisch • Windows-Authentifizierung • Basis-Authentifizierung

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.
Alle Kameraansichten aktivieren	Aktivierung der Ansicht Alle Kameras . In dieser Ansicht werden alle Kameras angezeigt, zu deren Ansicht ein Benutzer auf einem Aufzeichnungsserver berechtigt ist. 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, ist es Client-Benutzern nicht möglich, den Ausgang und Ereignisse zu sehen, auch wenn diese korrekt konfiguriert wurden.
Keyframes aktivieren	Keyframes werden nur gestreamt, wenn Benutzer auf Mobilgeräten oder in XProtect Web Client Video streamen. Dadurch wird weniger Bandbreite genutzt.
Eingehendes Audiosignal aktivieren	Eingehende Audiofunktion in XProtect Web Client und XProtect Mobile Client aktivieren. Diese Funktion ist standardmäßig aktiviert.
Push-to-talk aktivieren	Push-to-Talk (PTT) Funktion in XProtect Web Client und XProtect Mobile Client aktivieren. 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	Siehen 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 auf Seite 42
- Senden einer E-Mail-Nachricht an Benutzer auf Seite 42
- Aktivieren von Verbindungen im komplexen Netzwerk auf Seite 41
- Aktivieren Sie die UPnP-Erkennungsfunktion in Ihrem Router auf Seite 41

Weitere Informationen finden Sie unter Einrichten von Smart Connect auf Seite 41.

Allgemein

Name	Beschreibung
Verbindungstyp	Wählen Sie aus, wie XProtect Mobile-Client und XProtect Web Client-Benutzer eine Verbindung mit dem XProtect Mobile-Server aufbauen sollen. Sie haben die folgenden Optionen: Nur HTTP, HTTP und HTTPS oder nur HTTPS . Weitere Informationen finden Sie unter Anforderungen zur Verschlüsselung Mobiler Server für Clients auf Seite 33.
Client-Timeout (HTTP)	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.
UPnP-Entdeckbarkeit aktivieren	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 wurde, wird ein Port-Mapping im Router benötigt, damit Clients weiterhin aus dem Internetzugriff auf den Server haben. Die Option automatisches Port-Mapping aktivieren ermöglicht es dem XProtect Mobile-Server dieses Port-Mapping selbst durchzuführen, vorausgesetzt der Router ist dafür konfiguriert.

Name	Beschreibung
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	Wenn Sie die UPnP-Portzuordnung verwenden, um Verbindungen an eine spezifische Verbindung weiterzuleiten, aktivieren Sie das Kontrollkästchen Benutzerdefinierten Internetzugriff konfigurieren . Geben Sie dann die IP-Adresse oder den Hostnamen an und den Port, der für die Verbindung verwendet werden soll. Sie können dies beispielsweise tun, wenn Ihr Router UPnP nicht unterstützt oder Sie eine Kette von Routern haben.
Standardadresse deaktivieren	Deaktivieren Sie die standardmäßige IP-Adresse für die Verbindung mit dem mobilen Server nur mit einer bestimmten IP-Adresse oder hostname.
Auswählen, um die IP-Adresse dynamisch abzurufen	Wenn sich Ihre IP-Adressen häufig ändern, aktivieren Sie das Kontrollkästchen Auswählen, um IP-Adresse dynamisch abzurufen .
HTTP-Port	Geben Sie die Portnummer für die HTTP-Verbindung ein.
HTTPS-Port	Geben Sie die Portnummer für die HTTPS-Verbindung ein.
Server-Adressen	Listet alle IP-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 die Uhrzeit und das Datum, zu dem XProtect Mobile zum letzten Mal gestartet wurde.
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	<p>Zeigt die aktuelle Beziehung zwischen dem XProtect Mobile-Server und dem jeweiligen XProtect Mobile-Client oder XProtect Web Client-Benutzer an. Mögliche Statusmeldungen:</p> <ul style="list-style-type: none"> • 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 derzeit für jeden XProtect Mobile-Client oder XProtect Web Client-Benutzer offenen Videostreams an.
Audio Bandbreitennutzung (kB/s)	Zeigt die gesamte Bandbreite der derzeit für jeden XProtect Web Client-Benutzer offenen Audiostreams an.
Transcodierte Videostreams	Zeigt die gesamte Anzahl aktuell offener transkodierter Videostreams für jeden XProtect Mobile-Client oder XProtect Web Client-Benutzer an.
Transcodierte Audiostreams	Zeigt die gesamte Bandbreite der derzeit für jeden XProtect Web Client-Benutzer offenen Audiostreams an.

Registerkarte Leistung

Auf der Registerkarte **Leistung** können Sie für die Leistung des XProtect Mobile-Servers die folgenden Einschränkungen festlegen:

Einstellungen

Name	Beschreibung
Bilder in Originalgröße anzeigen	<p>Aktivieren, dass der XProtect Mobile-Server Bilder in Originalgröße an den XProtect Mobile-Client oder an XProtect Web Client sendet.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px; margin-top: 10px;">  <p>Die Anzeige von Bildern in Originalgröße erfordert mehr Bandbreite. Wird diese Option aktiviert, werden außerdem alle Regeln, die in den unten beschriebenen Einstellungen Stufen von Videostreambegrenzungen konfiguriert wurden, deaktiviert.</p> </div>
Wiedergabe-Streams einschränken	Wenn diese Option aktiviert ist, legt sie die maximale Anzahl von Videostreams im Untersuchungsmodus in XProtect Web Client fest.

Stufen von Videostreambegrenzungen

Pegel 1

Bei **Level 1** handelt es sich um die Standardbegrenzung auf dem XProtect Mobile-Server. Sofern Sie das Senden von Bildern in Originalgröße nicht aktiviert haben (siehe oben), werden alle Begrenzungen, die Sie hier festlegen, stets auf den Videostream von XProtect Mobile 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 **Level 1** eine andere Begrenzungsstufe erzwingen möchten, können Sie stattdessen das Kontrollkästchen **Level 2** aktivieren. Der Wert der Einstellungen darf den auf der ersten Stufe festgelegten Wert nicht übersteigen. Wenn Sie für „Max. FPS“ auf **Level 1** beispielsweise 45 festlegen, können Sie für „Max. FPS“ auf **Level 2** maximal 44 festlegen.

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

Name	Beschreibung
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.



Beachten Sie, dass bei der Aktivierung von **Bilder in Originalgröße anzeigen** auf der Registerkarte Allgemein keine **Leistung** sstufen angewendet werden.

Registerkarte Untersuchungen

Untersuchungseinstellungen

Sie können Untersuchungen aktivieren, sodass für Sie tätige Personen den XProtect Mobile-Client oder XProtect Web Client verwenden können, um auf Videoaufzeichnungen zuzugreifen, Vorfälle zu untersuchen und Videobeweise vorzubereiten und herunterladen zu können.

Name	Beschreibung
Untersuchungen-Ordner	Zeigt, wo Ihre Videoexportie auf Ihrer Festplatte gespeichert werden.
Größe des Untersuchungen-Ordners beschränken auf	Geben Sie die maximale Speichergröße des Untersuchungen-Ordners in Megabyte an. Die Standardgröße beträgt 2.000 MB.
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.
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. 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.

Name	Beschreibung
Daten beibehalten oder löschen, wenn Exportvorgänge fehlschlagen (MKV und AVI)	Wählen Sie aus, ob Daten, deren Vorbereitung zum Herunterladen fehlgeschlagen ist, aufbewahrt oder gelöscht werden sollen.

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. Klicken Sie dann in der Gruppe Untersuchungsdetails auf das Löschen-Symbol rechts neben den Feldern Datenbank , AVI oder MKV für Exporte.

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.
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 Einrichten von Video Push für Videostreams auf Seite 46 (siehe Einrichten von Video Push für Videostreams) abgeschlossen haben, klicken Sie auf **Kameras suchen**, um nach der entsprechenden Kamera zu suchen.

Registerkarte Benachrichtigungen

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

Wenn Sie die Benachrichtigungen aktivieren und mindestens einen Alarm und ein Ereignis konfiguriert haben, benachrichtigt XProtect Mobile die Benutzer, wenn ein Ereignis eintritt. Wenn die App geöffnet ist, werden die Benachrichtigungen in XProtect Mobile auf dem Mobilgerät angezeigt. Mithilfe von Push-Benachrichtigungen werden Benutzer benachrichtigt, die XProtect Mobile nicht geöffnet haben. Diese Benachrichtigungen werden auf dem Mobilgerät angezeigt.

Für weitere Informationen, siehe: Aktivieren von Push-Benachrichtigungen für bestimmte oder alle Mobilgeräte auf Seite 44

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. Weitere Informationen finden Sie unter <https://www.milestonesys.com/solutions/platform/product-index/>.

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

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


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

Für weitere Informationen siehe Einrichten von Benutzern für die zweistufige Verifikation über E-Mail auf Seite 49.

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

Anbiitereinstellungen > 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. Standardmäßig wird der Port 25 (ohne SSL) bzw. 465 (mit SSL) verwendet.
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 Verifizierungscode ein.
E-Mail-Betreff	Geben Sie einen Betreff für die E-Mail ein. Beispiel: Ihr Code für die zweistufige Verifizierung.

Name	Beschreibung
E-Mail-Text	<p>Geben Sie die Nachricht ein, die gesendet werden soll. Beispiel: Ihr Code lautet {0}.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  <p>Wenn Sie die Variable {0} nicht angeben, wird der Code standardmäßig an das Textende angefügt.</p> </div>

Verifizierungscode-Einstellungen

Name	Beschreibung
Zeitüberschreitung bei Wiederverbindung (0-30 Minuten)	<p>Geben Sie den Zeitraum an, innerhalb dem XProtect Mobile-Clientbenutzer ihre Anmeldung nicht erneut verifizieren müssen, zum Beispiel bei einer Trennung der Netzwerkverbindung. Der Standardzeitraum ist drei Minuten.</p> <p>Diese Einstellung gilt nicht für XProtect Web Client.</p>
Code läuft ab nach (1-10 Minuten)	<p>Geben Sie eine Gültigkeitsdauer für den Verifizierungscode nach Empfang durch den Benutzer an. Nach Ablauf dieser Zeit verliert der Code seine Gültigkeit und der Benutzer muss einen neuen Code beantragen. Der Standardzeitraum ist fünf Minuten.</p>
Code-Eingabeversuche (1-10 Versuche)	<p>Legen Sie die maximale Anzahl von Codeeingabeversuchen fest, bevor der bereitgestellte Code seine Gültigkeit verliert. Die Standardanzahl ist drei.</p>
Codelänge (4-6 Zeichen)	<p>Geben Sie die Länge des Codes ein. Die Standardzeichenlänge beträgt sechs.</p>
Codezusammensetzung	<p>Geben Sie an, wie komplex der vom System generierte Code sein soll. Sie können auswählen zwischen:</p> <ul style="list-style-type: none"> • Lateinische Großbuchstaben (A-Z) • Lateinische Kleinbuchstaben (a-z) • Zahlen (0-9) • Sonderzeichen (!@#...)

Benutzereinstellungen

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

Sichere Kommunikation (Erläuterung).

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

In XProtect VMS wird die sichere Kommunikation mithilfe von SSL/TLS mit asymmetrischer Verschlüsselung (RSA) hergestellt.

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

Eine Zertifizierungsstelle (Certificate Authority (CA)) kann Web-Diensten auf Servern mithilfe eines CA-Zertifikates Zertifikate ausstellen. Dieses Zertifikat enthält zwei Schlüssel, einen privaten und einen öffentlichen. Der öffentliche Schlüssel wird auf den Clients eines Web-Dienstes (Dienst-Clients) installiert, indem ein öffentliches Zertifikat installiert wird. Der private Schlüssel dient dazu, Serverzertifikate zu signieren, die auf dem Server installiert werden müssen. Jedes Mal, wenn ein Dienst-Client den Web-Dienst anruft, sendet der Web-Dienst das Serverzertifikat, einschließlich des öffentlichen Schlüssels, an den Client. Der Dienst-Client kann das Serverzertifikat mithilfe des bereits installierten, öffentlichen CA-Zertifikates überprüfen. Der Client und der Server können nun das öffentliche und private Serverzertifikat zum Austausch eines geheimen Schlüssels verwenden und somit eine sichere SSL/TLS-Verbindung herstellen.

Weitere Informationen zu TLS finden Sie unter https://en.wikipedia.org/wiki/Transport_Layer_Security

Zertifikate haben ein Verfalldatum. XProtect VMS gibt Ihnen keine Wawrnung, wenn das Zertifikat in Kürze abläuft. Wenn ein Zertifikat abläuft:

- Die Clients vertrauen dann nicht mehr dem Aufzeichnungsserver mit dem abgelaufenen Zertifikat und können daher auch nicht mehr mit ihm kommunizieren.
- Die Aufzeichnungsserver vertrauen dann nicht mehr dem Management-Server mit dem abgelaufenen Zertifikat und können daher auch nicht mehr mit ihm kommunizieren.
- Die mobilen Geräte vertrauen dann nicht mehr dem Mobilien Server mit dem abgelaufenen Zertifikat und können daher auch nicht mehr mit ihm kommunizieren.



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

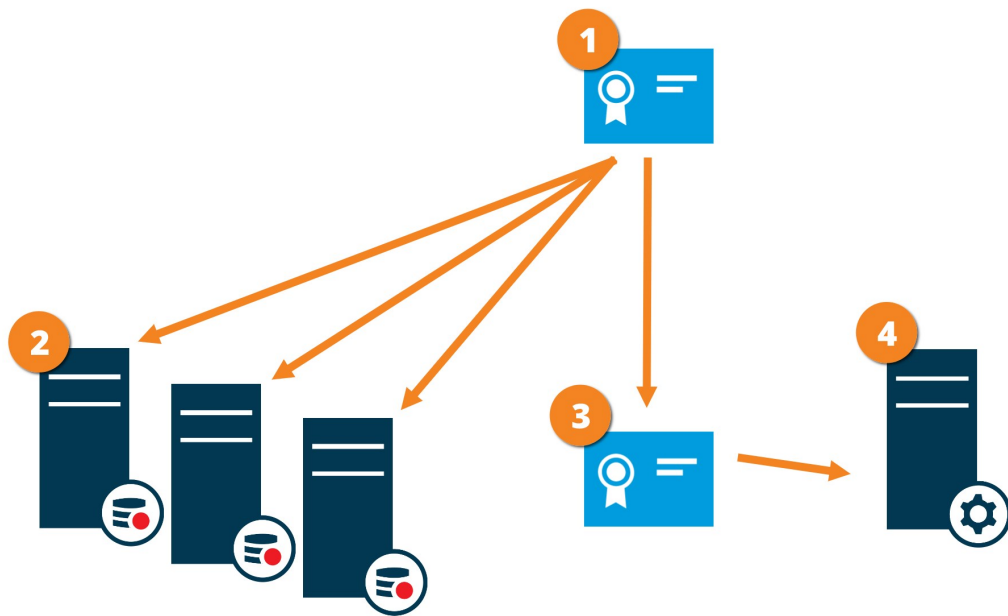
Wenn Sie ein Zertifikat mit demselben Themennamen erneuern und es zum Windows Certificate Store hinzufügen, so übernehmen die Server automatisch das neue Zertifikat. Dies erleichtert das Erneuern für viele Server, ohne dass das Zertifikat für jeden Aufzeichnungsserver erneut ausgewählt werden muss und ohne den Dienst neu starten zu müssen.

Verschlüsselung des Management-Servers (Erläuterung):

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

Verteilung von Zertifikaten für Management-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 zum Management-Server zu sichern.



- ❶ Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl das Thema/der Eigentümer (Management-Server) vertraut, als auch die Partei, die das Zertifikat überprüft (Aufzeichnungsserver)
- ❷ Dem CA-Zertifikat muss auf allen Aufzeichnungsservern vertraut werden. So überprüfen die Aufzeichnungsserver die Gültigkeit der von der CA ausgegebenen Zertifikate
- ❸ Das CA-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen dem Management-Server und den Aufzeichnungsservern
- ❹ Das CA-Zertifikat muss auf dem Computer installiert werden, auf dem der Management-Server läuft

Anforderungen für das private Zertifikat des Management-Servers:

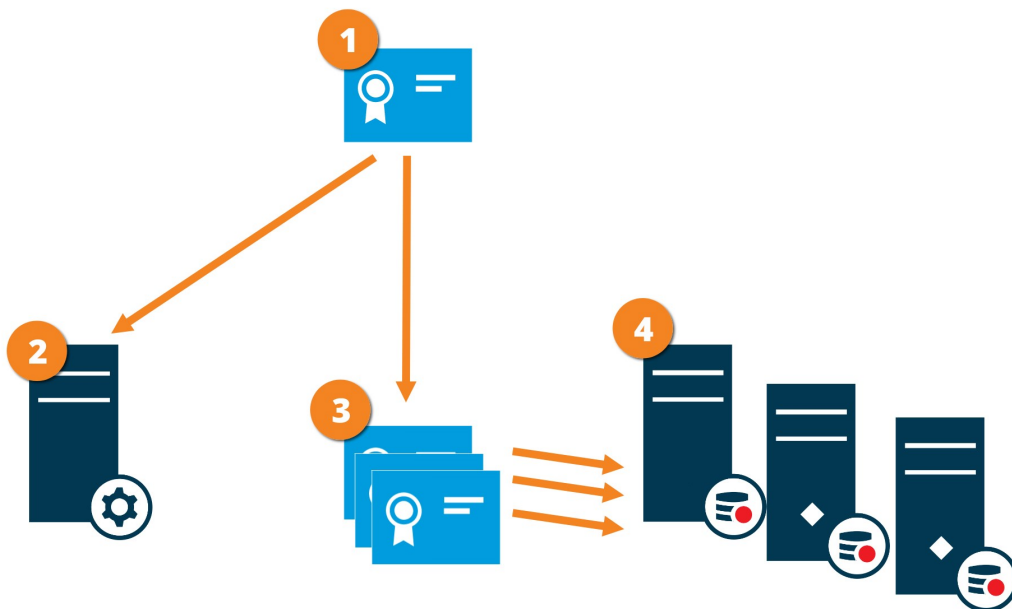
- Wird dem Management-Server ausgestellt, damit der Hostname des Management-Servers im Namen des Zertifikates enthalten ist, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, an die das Zertifikat ausgegeben wird
- Wird auf dem Management-Server selbst vertraut, indem dem CA-Zertifikat vertraut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

Verschlüsselung vom Management-Server zum Aufzeichnungsserver (Erläuterung)

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

Verteilung von Zertifikaten

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



- ❶ Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl Thema/Eigentümer (Aufzeichnungsserver) vertraut, als auch die Partei, die das Zertifikat überprüft (Management-Server)
- ❷ Dem öffentlichen CA-Zertifikat muss auf dem Management-Server vertraut werden. So überprüft der Management-Server die Gültigkeit der von der CA ausgegebenen Zertifikate
- ❸ Das CA-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen den Aufzeichnungsservern und dem Management-Server
- ❹ Das CA-Zertifikat muss auf den Computern installiert werden, auf denen die Aufzeichnungsserver laufen

Anforderungen für das Zertifikat des privaten Aufzeichnungsservers:

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

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

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

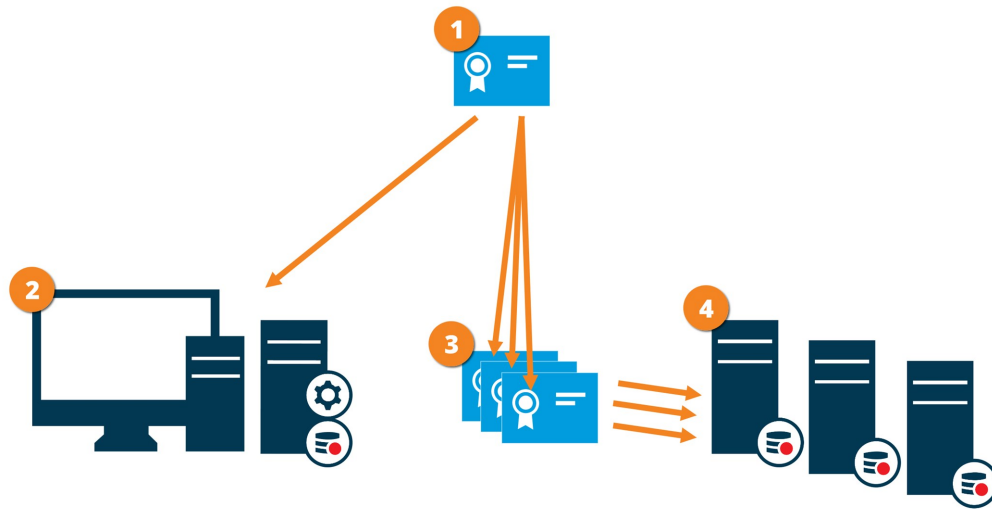
- XProtect Smart Client
- Management Client
- Management Server (für Systemmonitor und für Bilder und AVI-Videoclips in email notifications)
- XProtect Mobile-Server
- XProtect Event Server
- XProtect LPR
- ONVIF Bridge
- XProtect DLNA Server
- Seiten, die Datenstreams vom Aufzeichnungsserver abrufen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



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

Verteilung von Zertifikaten

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



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

Anforderungen für das Zertifikat des privaten Aufzeichnungsservers:

- Es wird dem Aufzeichnungsserver ausgestellt, damit der Hostname des Aufzeichnungsservers im Zertifikat enthalten ist, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, an die das Zertifikat ausgegeben wird
- Vertrauenswürdig für alle Computer, auf denen Dienste laufen, die Datenstreams vom Aufzeichnungsserver abrufen, vorzugsweise dadurch, dass sie dem CA-Zertifikat vertrauen, das zur Ausgabe des Zertifikates des Aufzeichnungsservers verwendet wurde
- Das Dienstkonto, auf dem der Aufzeichnungsserver läuft, muss Zugriff zum privaten Schlüssel des Zertifikates auf dem Aufzeichnungsserver haben.



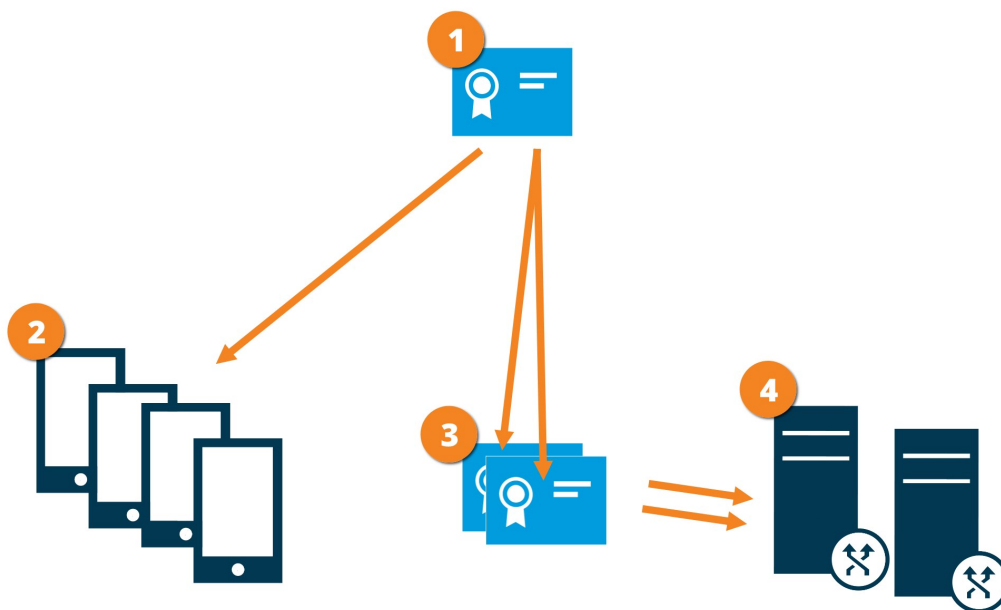
Wenn Sie auf den Aufzeichnungsservern die Verschlüsselung aktivieren, und Ihr System verwendet Failover-Aufzeichnungsserver, so empfiehlt Milestone, dass Sie die Failover-Aufzeichnungsserver ebenfalls dafür vorbereiten, dass sie eine Verschlüsselung verwenden.

Datenverschlüsselung des Mobilien Servers (Erläuterung)

In XProtect VMS wird die Verschlüsselung für jeden Mobilien Server aktiviert oder deaktiviert. Wenn Sie die Verschlüsselung auf einem Mobilien 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 Mobilien Server zu sichern.



- 1 Eine CA fungiert als vertrauenswürdiger Dritter, dem sowohl das Thema/der Eigentümer (Mobiler Server) vertraut, als auch die Partei, die das Zertifikat überprüft (alle Clients).
- 2 Dem öffentlichen CA-Zertifikat muss auf allen Clientcomputern vertraut werden. So überprüfen die Clients die Gültigkeit der von der CA ausgegebenen Zertifikate
- 3 Das CA-Zertifikat dient zur sicheren Verbindung zwischen dem Mobilien Server und Clients und Diensten
- 4 Das CA-Zertifikat muss auf dem Computer installiert werden, auf dem der Mobile Server läuft

Anforderungen für das CA-Zertifikat:

- Der Hostname des Mobilens 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 Mobilens Server abrufen
- Das Dienstkonto, auf dem der Mobile Server läuft, muss Zugriff zum privaten Schlüssel des CA-Zertifikates haben.

Anforderungen zur Verschlüsselung Mobiler Server für Clients

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.

Wenn Sie zur Verschlüsselung des Mobilens Servers ein selbst signiertes Zertifikat auswählen, XProtect Mobile so kann der Client keine Verbindung zum Mobilens Server herstellen.

Verschlüsselung aktivieren

Verschlüsselung zu Clients und Servern aktivieren

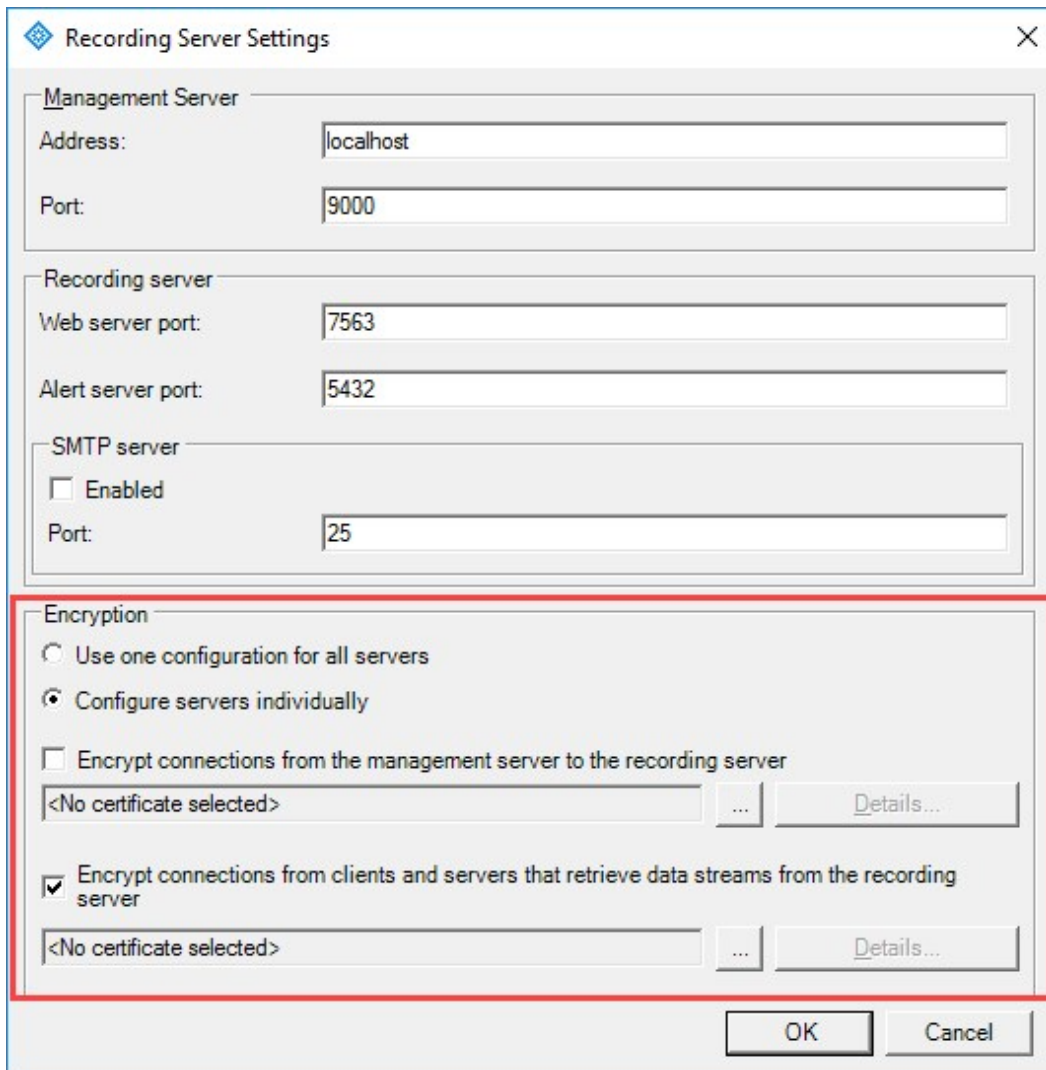
Sie können Verbindungen vom Aufzeichnungsserver an Clients und Dienste verschlüsseln, die Daten vom Aufzeichnungsserver streamen. Weitere Informationen finden Sie unter Sichere Kommunikation (Erläuterung). auf Seite 26.

Anforderungen:

- Einem Serverauthentifizierungszertifikat wird von allen Computern vertraut, die Dienste ausführen, die Datenstreams vom Aufzeichnungsserver abrufen
- XProtect Smart Client und alle Dienste, die Datenströme vom Aufzeichnungsserver beziehen, müssen auf Version 2019 R1 oder einer spätere Version aktualisiert werden
- Manche der Lösungen von Drittanbietern, die mit Hilfe von Versionen von MIP SDK erstellt wurden, die vor der Version 2019 R1 lagen, müssen ggf. aktualisiert werden

Schritte:

1. Klicken Sie auf dem Computer, auf dem der Aufzeichnungsserver läuft, mit der rechten Maustaste auf das Symbol Recording Server Manager im Benachrichtigungsbereich.
2. Wählen Sie **Recording Server Service anhalten** aus.
3. Klicken Sie erneut rechts auf das Symbol Recording Server Manager und wählen Sie **Einstellungen ändern**.
Das Fenster **Recording Server-Einstellungen** wird angezeigt.
4. Geben sie unten die Verschlüsselungseinstellungen für den Aufzeichnungsserver ein:



- **Die Verschlüsselung gilt für alle Clients und Dienste, die Datenstreams vom Aufzeichnungsserver abrufen:** Bevor sie die Verschlüsselung aktivieren, lesen Sie bitte die in diesem Thema aufgeführten Anforderungen
- Wählen Sie ein Zertifikat aus: Enthält eine Liste der eindeutigen Themennamen von Zertifikaten, die auf dem lokalen Computer im Windows Certificate Store installiert sind, der einen privaten Schlüssel hat.
Der Benutzer des Aufzeichnungsserverdienstes hat Zugang zum privaten Schlüssel erhalten. Diesem Zertifikat muss auf allen Clients vertraut werden.
- **Einzelheiten:** Klicken sie, um die Angaben zum Windows Certificate Store zu dem ausgewählten Zertifikat anzuzeigen

5. Klicken Sie auf **OK**.
6. Zum erneuten Starten des Dienstes Recording Server klicken Sie bitte rechts auf das Symbol **Recording Server** und wählen Sie **Dienst Recording Server starten**.



Das Anhalten des Dienstes Recording Server bedeutet, dass Sie keine Live-Videoaufnahmen machen und anschauen können, während Sie die Basiskonfiguration des Aufzeichnungsservers überprüfen oder ändern.

Um zu überprüfen, ob der Aufzeichnungsserver eine Verschlüsselung verwendet, s. Verschlüsselungsstatus anzeigen.

Die Verschlüsselung zum Management-Server aktivieren

Sie können die wechselseitige Verbindung zwischen dem Management-Server und dem Aufzeichnungsserver verschlüsseln. Wenn Ihr System mehrere Aufzeichnungsserver hat, müssen Sie die Verschlüsselung auf allen Aufzeichnungsservern aktivieren. Weitere Informationen finden Sie unter Sichere Kommunikation (Erläuterung) auf Seite 26.

Anforderungen:

- Einem Server-Authentifizierungszertifikat wird auf allen Aufzeichnungsservern vertraut
- Für alle Aufzeichnungsserver muss ein Upgrade auf die Version 2019 R1 oder später vorgenommen werden

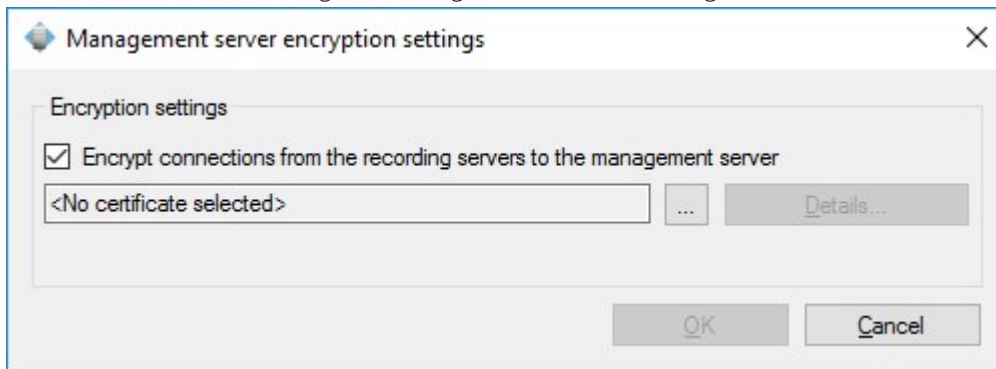
Zunächst aktivieren Sie die Verschlüsselung auf dem Management-Server.

Schritte:

1. Klicken Sie auf dem Computer, auf dem der Management-Server läuft, rechts auf das Symbol Management Server Manager im Benachrichtigungsbereich.
2. Wählen Sie Management Server **Service** aus.
3. Klicken Sie erneut rechts auf das Symbol Management Server Manager und wählen Sie **Einstellungen ändern**.

Das Fenster **Verschlüsselungseinstellungen für den Management-Server** erscheint.

4. Geben Sie die Verschlüsselungseinstellungen für den Aufzeichnungsserver ein:



- **Verbindungen von den Aufzeichnungsservern zum Management-Server verschlüsseln:** Bevor sie die Verschlüsselung aktivieren, lesen Sie bitte die in diesem Thema aufgeführten Anforderungen
- Wählen Sie ein Zertifikat aus: Enthält eine Liste der eindeutigen Themennamen von Zertifikaten, die auf dem lokalen Computer im Windows Certificate Store installiert sind, der über einen privaten Schlüssel verfügt, und dem CA-Zertifikat muss auf dem Management-Server vertraut werden.
- **Einzelheiten:** Klicken sie, um die Angaben zum Windows Certificate Store zu dem ausgewählten Zertifikat anzuzeigen

5. Klicken Sie auf **OK**.

6. Zum erneuten Starten des Dienstes Management Server klicken Sie bitte rechts auf das Symbol Management Server Manager und wählen Sie **Dienst Management Server starten**.

Um die Aktivierung der Verschlüsselung zu vervollständigen, ist der nächste Schritt die Aktualisierung der Verschlüsselungseinstellungen auf jedem Aufzeichnungsserver. Weitere Informationen finden Sie unter Die Verschlüsselung vom Management-Server aus aktivieren auf Seite 36.

Die Verschlüsselung vom Management-Server aus aktivieren

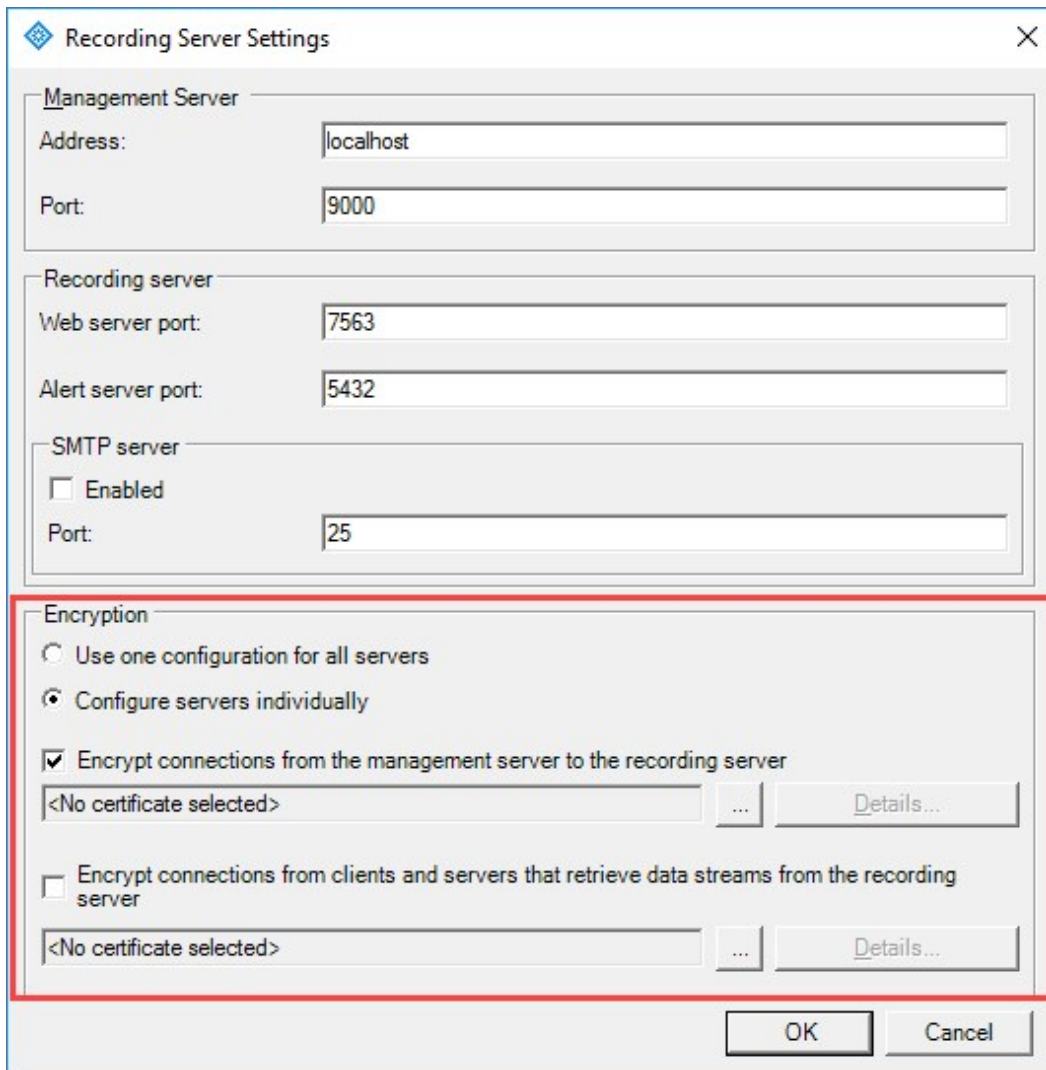
Sie können die wechselseitige Verbindung zwischen dem Management-Server und dem Aufzeichnungsserver verschlüsseln. Wenn Ihr System mehrere Aufzeichnungsserver hat, müssen Sie die Verschlüsselung auf allen Aufzeichnungsservern aktivieren. Weitere Informationen finden Sie unter Sichere Kommunikation (Erläuterung) auf Seite 26.

Anforderungen:

- Einem Server-Authentifizierungszertifikat wird auf dem Management-Server vertraut
- Für alle Aufzeichnungsserver muss ein Upgrade auf die Version 2019 R1 oder später vorgenommen werden
- Sie haben die Verschlüsselung auf dem Management-Server aktiviert, s. Die Verschlüsselung zum Management-Server aktivieren auf Seite 35

Schritte:

1. Klicken Sie auf dem Computer, auf dem der Aufzeichnungsserver läuft, mit der rechten Maustaste auf das Symbol Recording Server Manager im Benachrichtigungsbereich.
2. Wählen Sie **DienstRecording Server anhalten** aus.
3. Klicken Sie erneut rechts auf das Symbol Recording Server Manager und wählen Sie **Einstellungen ändern**.
Das Fenster **Recording Server-Einstellungen** wird angezeigt.
4. Geben sie unten die Verschlüsselungseinstellungen für den Aufzeichnungsserver ein:



- **Verbindungen vom Aufzeichnungsserver zum Management-Server verschlüsseln:** Bevor sie die Verschlüsselung aktivieren, lesen Sie bitte die in diesem Thema aufgeführten Anforderungen
 - Sie können die Option **Eine Konfiguration für alle Server verwenden** auswählen, wenn Sie auf allen Servern dasselbe Zertifikat verwenden.
 - Wählen Sie ein Zertifikat aus: Enthält eine Liste der eindeutigen Themennamen von Zertifikaten, die auf dem lokalen Computer im Windows Certificate Store installiert sind, der einen privaten Schlüssel hat.
 - **Einzelheiten:** Klicken sie, um die Angaben zum Windows Certificate Store zu dem ausgewählten Zertifikat anzuzeigen
5. Klicken Sie auf **OK**.
 6. Geben Sie in die Dialogbox **Auf dem Management-Server registrieren** die Adresse des Management-Servers ein, mit dem der Aufzeichnungsserver eine Verbindung herstellen soll, und klicken Sie dann auf **OK**. Die Nummer des Standardports ist 443.

7. Geben Sie den Benutzernamen und das Passwort eines Systemadministrators von XProtect ein und klicken Sie auf **OK**.
8. Zum erneuten Starten des Dienstes Recording Server klicken Sie bitte rechts auf das Symbol **Recording Server** und wählen Sie **Dienst Recording Server starten**.



Das Anhalten des Dienstes Recording Server bedeutet, dass Sie keine Live-Videoaufnahmen machen und anschauen können, während Sie die Basiskonfiguration des Aufzeichnungsservers überprüfen oder ändern.


Aktivieren Sie die Verschlüsselung auf dem Mobilien Server.

Wenn Sie für die Verbindung zwischen einem Mobilien Server und den Clients und Diensten ein sicheres HTTPS-Protokoll verwenden möchten, müssen Sie auf dem Server ein gültiges Zertifikat installieren. Das Zertifikat bestätigt, dass der Zertifikatsinhaber berechtigt ist, sichere Verbindungen herzustellen. Weitere Informationen finden Sie unter Datenverschlüsselung des Mobilien Servers (Erläuterung) auf Seite 32 und Anforderungen zur Verschlüsselung Mobiler Server für Clients auf Seite 33.



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.


Zu Aktivierung der Verschlüsselung nach der Installation des Mobilien Servers:

1. Klicken Sie auf einem Computer, auf dem ein Mobiler Server installiert ist, mit der rechten Maustaste auf das Mobile Server Manager-Symbol in der Taskleiste des Betriebssystems und wählen Sie **Zertifikat bearbeiten** aus.
2. Wählen Sie das Kontrollkästchen **Verschlüsselung gilt für alle Clients und Dienste, die Datenstreams vom Mobilien Server abrufen**.
3. Zur Auswahl eines gültigen Zertifikates klicken Sie auf . Es öffnet sich ein Kasten mit dem Windows-Sicherheitsdialog.
4. Wählen Sie das Zertifikat aus, das Sie anwenden möchten.
5. Klicken Sie auf **OK**.

Zertifikate bearbeiten

Falls das Zertifikat, das Sie für die sichere Verbindung verwenden, abgelaufen ist, können Sie ein anderes auf dem Computer installiertes Zertifikat auswählen, auf dem der Mobile Server läuft.

Ändern Sie ein Zertifikat:

1. Klicken Sie auf einem Computer, auf dem ein Mobiler Server installiert ist, mit der rechten Maustaste auf das Mobile Server Manager-Symbol in der Taskleiste des Betriebssystems und wählen Sie **Zertifikat bearbeiten** aus.
2. Zur Auswahl eines gültigen Zertifikates klicken Sie auf . Es öffnet sich ein Kasten mit dem Windows-Sicherheitsdialog.
3. Wählen Sie das Zertifikat aus, das Sie anwenden möchten.
4. Klicken Sie auf **OK**.

Eine Mitteilung informiert Sie darüber, dass das Zertifikat installiert wurde und dass der Mobile Server-Dienst neu gestartet wurde, um die Änderung anzuwenden.

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

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

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

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

Smart Connect (Erklärung)

Mit Smart Connect können Sie ohne Anmeldung mit einem Mobilgerät oder Tablet überprüfen, ob XProtect Mobile 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. Mithilfe von UPnP kann der XProtect Mobile-Server die Portweiterleitung automatisch konfigurieren. Sie können die Portweiterleitung aber auch manuell über die Weboberfläche Ihres Routers einrichten. Der Einrichtungsvorgang kann sich von Router zu Router unterscheiden. Wenn Sie Hilfe bei der Einrichtung der Portweiterleitung für Ihren Router benötigen, ziehen Sie die Dokumentation für das jeweilige Gerät zu Rate.



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

Eigenschaften angezeigt:

Server accessible through internet: 

Aktivieren von Verbindungen im komplexen Netzwerk

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

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

- Wenn Sie die UPnP-Portzuordnung verwenden, um Verbindungen an eine bestimmte Verbindung weiterzuleiten, aktivieren Sie das Kontrollkästchen **Benutzerdefinierten Internetzugriff konfigurieren**. Geben Sie dann die **IP-Adresse oder den Hostnamen** an und den Port, der für die Verbindung verwendet

werden soll. Sie können dies beispielsweise tun, wenn Ihr Router UPnP nicht unterstützt oder Sie eine Kette von Routern 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**.
 - Im Feld **Verbindungstyp** geben Sie das zu verwendende Protokoll an
 - Bevor Sie sichere Verbindungen aktivieren, müssen Sie sich mit der Funktionsweise von digitalen Zertifikaten vertraut machen. Informationen zum Hinzufügen eines Zertifikats im XProtect Mobile-Server finden Sie unter Zertifikate bearbeiten auf Seite 40
 - Legen Sie mithilfe eines Timeline Areas fest, wie oft der XProtect Mobile-Client und XProtect Web Client dem mobilen Server anzeigen müssen, dass sie betriebsbereit sind.
 - Um die XProtect Mobile-Server im Netzwerk mittels des UPnP Protokolle sichtbar zu machen, markieren Sie das Kontrollkästchen **UPnP-Entdeckbarkeit aktivieren**
 - Um zu aktivieren, dass der XProtect Mobile-Server die Portzuordnung selbst vornimmt, wenn der Router dafür konfiguriert ist, markieren Sie das Kontrollkästchen **Automatische Portzuordnung aktivieren**

Senden einer E-Mail-Nachricht an Benutzer

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

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

Für weitere Informationen, siehe:

Anforderungen für das Einrichten von Smart Connect auf Seite 11

Registerkarte Konnektivität auf Seite 16

Senden von Benachrichtigungen (Erklärung)

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

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

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

Um Benutzer zu benachrichtigen, die XProtect Mobile nicht geöffnet haben, können Sie sogenannte Push-Benachrichtigungen verwenden. Push-Benachrichtigungen werden an das Mobilgerät gesendet und sind optimal dafür geeignet, mobile Benutzer auf dem Laufenden zu halten.

Verwenden von Push-Benachrichtigungen



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

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

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

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

Siehe auch Anforderungen für das Einrichten von Benachrichtigungen auf Seite 10 und die Registerkarte Registerkarte Benachrichtigungen auf Seite 23.

Konfigurieren von Push-Benachrichtigungen auf dem XProtect Mobile-Server

So konfigurieren Sie Push-Benachrichtigungen:

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



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

Aktivieren von Push-Benachrichtigungen für bestimmte oder alle Mobilgeräte

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

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

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

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

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

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

Einrichten von Untersuchungen

Richten Sie Untersuchungen ein, damit für Sie tätige Personen mit XProtect Web Client oder XProtect Mobile auf Videoaufzeichnungen zugreifen, Tatbestände untersuchen und Videobeweisbilder vorbereiten und herunterladen 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. Wählen Sie das Kontrollkästchen **Aktiviert** aus. 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. Geben Sie im Feld **Größe des Untersuchungsordners beschränken auf** die maximale Größe in Megabyte für die im Untersuchungsordner gespeicherten Inhalte an.
5. 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.
6. Optional: Sie können auch das Datum und die Uhrzeit eines Videodownloads protokollieren. Wählen Sie dazu das Kontrollkästchen **Zeitstempel für AVI-Exporte einschließen** aus.
7. 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.

- 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.
- Geben Sie im Feld **Daten beibehalten oder löschen, wenn Exportvorgänge fehlschlagen (MKV und AVI)** an, ob heruntergeladene Daten – auch bei Unvollständigkeit – entweder gespeichert oder gelöscht werden sollen.



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.

- Zum Löschen einer Untersuchung und aller dafür erstellten Videoexporte wählen Sie die Untersuchung in der Liste aus und klicken 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. Klicken Sie dann in der Gruppe **Untersuchungsdetails** auf das **Löschen**-Symbol rechts neben den Feldern **Datenbank**, **AVI** oder **MKV** für Exporte.

Nutzung von Video Push für Videostreams (Erklärung)

Sie können Video Push einrichten, damit Benutzer Video von der Kamera ihres Mobilgeräts an Ihr XProtect-Überwachungssystem streamen können, um andere Benutzer über eine Situation auf dem Laufenden zu halten oder Video zur späteren Überprüfung aufzuzeichnen. Der Videostream beinhaltet ggf. auch Audio.

Siehe auch die Registerkarte Registerkarte Video Push auf Seite 22 und Anforderungen für das Einrichten von Video Push auf Seite 11.

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:

- Markieren Sie auf der Registerkarte **Video Push** das Kontrollkästchen **Video Push**, um die Funktion zu aktivieren.
- Fügen Sie einen video push-Kanal für Video-Streaming hinzu.
- Fügen Sie den video push-Treiber als Gerät auf dem Recording Server hinzu. Der Treiber simuliert ein Kameragerät, um das Videostreaming an Recording Server zu ermöglichen.
- 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 dann den mobilen Server.
2. Aktivieren Sie auf der Registerkarte **Video Push** das Kontrollkästchen **Video Push**.
3. Klicken Sie in der rechten unteren Ecke auf **Hinzufügen**, um unter **Kanalzuordnung** einen Video-Push-Kanal hinzuzufügen.
4. Geben Sie den Benutzernamen des Benutzerkontos (hinzugefügt unter **Rollen**) ein, das den Kanal verwenden wird. 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.

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**, um das Dialogfeld „Video Push-Kanal“ zu schließen und den Kanal zu speichern.

Einen video push-Kanal entfernen

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

- Wählen Sie den zu entfernenden Kanal aus und klicken Sie dann in der unteren rechten Ecke auf **Entfernen**

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

1. Klicken Sie im Navigationsbereich auf **Aufzeichnungsserver**.
2. Klicken Sie mit der rechten Maustaste auf den Server, an den Sie einen Videostream senden möchten, und klicken Sie dann auf **Hardware hinzufügen**, um den Assistenten **Hardware hinzufügen** zu öffnen.
3. Wählen Sie die Hardware-Erkennungsmethode **Manuell** aus und klicken Sie auf **Weiter**.
4. Geben Sie die Anmeldeinformationen für die Kamera ein:
 - Geben Sie als Benutzernamen den werksseitigen Standardwert oder den in der Kamera angegebenen Benutzernamen ein
 - Passwort: Geben Sie **Milestone** ein und klicken Sie auf **Weiter**



Hierbei handelt es sich um die Anmeldeinformationen für die Hardware, nicht für den Benutzer. Diese haben keinen Bezug zum Benutzernamen für den Kanal.

- Erweitern Sie in der Liste der Treiber **Milestone**, wählen Sie das Kontrollkästchen **Video Push-Treiber** aus und klicken Sie auf **Weiter**.



Das System generiert eine MAC-Adresse für das Video Push-Treibergerät. Wir empfehlen Ihnen, diese Adresse zu verwenden. Sie sollten sie nur bei Problemen mit dem Video Push-Treibergerät ändern, oder z.B. wenn Sie eine neue Adresse und Portnummer hinzufügen müssen.

- Geben Sie im Feld **Adresse** die IP-Adresse des Computers ein, auf dem XProtect Mobile-Server installiert ist.
- 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.
- Wählen Sie in der Spalte **Hardwaremodell Video Push-Treiber** aus und klicken Sie auf **Weiter**.
- Wenn das System die neue Hardware erkannt hat, klicken Sie auf **Weiter**.
- Legen Sie im Feld **Vorlage für Hardware-Namen** fest, ob das Hardwaremodell und die IP-Adresse oder nur das Modell angezeigt werden soll.
- 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.

- 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:

- Klicken Sie im Bereich **Standort-Navigation** auf **Mobile Server** und dann auf die Registerkarte **Video Push**.
- 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

Sobald Sie die Anforderungen zur Aktivierung von Push-Video erfüllt haben (siehe Anforderungen für das Einrichten von Video Push auf Seite 11), in Management Client:

1. Erweitern Sie im Bereich **Standort-Navigation** den Knoten **Server** und klicken sie dann auf **Aufzeichnungsserver**.
2. Wählen Sie in dem Fenster Übersicht das entsprechende Verzeichnis für den Aufzeichnungsserver aus und erweitern Sie dann das Verzeichnis **Treiber für Push-Video** 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 Verzeichnis die Kamera für Video Push.
5. Klicken Sie in dem Fenster **Eigenschaften** auf die Registerkarte **Client** (siehe Eigenschaften der Registerkarte Client).
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** das Verzeichnis Aufzeichnungsserver und wählen Sie das Mikrofon für Push-Video aus.
8. Klicken Sie auf **OK**.

Einrichten von Benutzern für die zweistufige Verifikation über E-Mail



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

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

Die zweistufige Verifikation verbessert die Sicherheit Ihres Überwachungssystems.

Führen Sie in Management Client die folgenden Schritte aus:

1. Informationen über den SMTP-Server eingeben auf Seite 50.
2. Den Verifizierungscode festlegen, der an Benutzer gesendet wird auf Seite 50.
3. Benutzern und Active Directory-Gruppen eine Anmeldemethode zuweisen auf Seite 50.

Siehe auch Anforderungen für die Einrichtung der zweistufigen Verifikation für Benutzer auf Seite 11 und die Registerkarte Registerkarte Zweistufige Verifikation auf Seite 24.

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 Einzelheiten zu den einzelnen Parametern siehe die Registerkarte Registerkarte Zweistufige Verifikation auf Seite 24.

Weitere Einzelheiten siehe die Registerkarte Registerkarte Zweistufige Verifikation auf Seite 24.

Den Verifizierungscode festlegen, der an Benutzer gesendet wird

So legen Sie die Komplexität des Verifizierungscode fest:

1. Geben Sie auf der Registerkarte **Zweistufige Verifikation** im Abschnitt **Verifizierungscode-Einstellungen** den Zeitraum an, innerhalb dem XProtect Mobile-Client-Benutzer ihre Anmeldung nicht erneut verifizieren müssen, zum Beispiel bei einer Trennung der Netzwerkverbindung. Der Standardzeitraum ist drei Minuten.
2. Geben Sie eine Gültigkeitsdauer für den Verifizierungscode nach Empfang durch den Benutzer an. Nach Ablauf dieser Zeit verliert der Code seine Gültigkeit und der Benutzer muss einen neuen Code anfordern. Der Standardzeitraum ist fünf Minuten.
3. Legen Sie die maximale Anzahl von Codeingabeversuchen 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 Einzelheiten siehe die Registerkarte Registerkarte Zweistufige Verifikation auf Seite 24.

Benutzern und Active Directory-Gruppen eine Anmeldemethode zuweisen

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

1. Wählen Sie in der Spalte **Anmeldemethode** eine Verifizierungsmethode für die einzelnen Benutzer oder Gruppen aus.
2. Machen Sie im Feld **Details** Angaben zur E-Mail-Zustellung; geben Sie Beispiel die E-Mail-Adressen einzelner Benutzer ein. 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 Einzelheiten siehe die Registerkarte Registerkarte Zweistufige Verifikation auf Seite 24.

Aktionen (erklärt):

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

Weitere Informationen finden Sie auf der Allgemein auf Seite 14.

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

Um Aktionen mit der aktuellen Kamera richtig anzuzeigen, müssen Sie eine Ausgangsgruppe erstellen, die denselben Namen wie die Kamera hat.

Beispiel:

Beim Erstellen einer Ausgang-Gruppe mit Ausgängen an einer Kamera mit der Bezeichnung „AXIS P3301, P3304 – 10,100.50.110 – Kamera 1“ müssen Sie den gleichen Namen in das Feld **Name** eingeben (unter **Gerätegruppendaten**).

Sie können zu dem Titel im entsprechenden Feld eine **Beschreibung** hinzufügen, z. B. „AXIS P3301,P3304 - 10.100.50.110 - Kamera 1 - Lichtschalter“.



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

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

Wartung

Mobile Server Manager (erklärt)

Beim Mobile Server Manager handelt es sich um eine Taskleisten-gesteuerte Funktion, die mit dem Mobilien Server verbunden ist. Per Rechtsklick auf das Mobile Server Manager-Symbol im Benachrichtigungsbereich wird ein Menü geöffnet, in dem Sie auf die Mobile Server-Funktion zugreifen können.

Sie können:

- Zugriff auf XProtect Web Client auf Seite 53
- Den Mobile Server-Dienst starten, anhalten oder neu starten auf Seite 54
- Management-Server-Adresse eintragen/bearbeiten auf Seite 54
- Portnummern anzeigen/bearbeiten auf Seite 55
- Zertifikate bearbeiten auf Seite 40
- Öffnen Sie die heutige Protokolldatei (siehe Zugriff auf Protokolle und Untersuchungen (erklärt) auf Seite 55)
- Öffnen Sie den Protokollordner (siehe Zugriff auf Protokolle und Untersuchungen (erklärt) auf Seite 55)
- Öffnen Sie den Untersuchungsordner (siehe Zugriff auf Protokolle und Untersuchungen (erklärt) auf Seite 55)
- Untersuchungen-Ordner ändern auf Seite 56
- Siehe XProtect Mobile-Server Status (siehe Status anzeigen (Erklärung) auf Seite 56)

Zugriff auf XProtect Web Client

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

1. Richten Sie den XProtect Mobile-Server in Management Client ein.
2. Wenn Sie den Computer verwenden, auf dem der XProtect Mobile-Server installiert ist, können Sie mit der rechten Maustaste auf das Mobile Server Manager-Symbol im Benachrichtigungsbereich klicken und **Öffnen XProtect Web Client** auswählen.
3. Wenn Sie nicht den Rechner verwenden, auf dem der XProtect Mobile-Server installiert ist, können Sie über einen Browser zugreifen. Fahren Sie mit Schritt 4 fort.
4. Öffnen Sie einen Internetbrowser (Internet Explorer, 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 nutzen wollen, oder **https://127.2.3.4:8082** wenn Sie eine sichere HTTPS-Verbindung nutzen wollen. 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.

Management-Server-Adresse eintragen/bearbeiten

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


Portnummern anzeigen/bearbeiten

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

Zertifikate bearbeiten

Falls das Zertifikat, das Sie für die sichere Verbindung verwenden, abgelaufen ist, können Sie ein anderes auf dem Computer installiertes Zertifikat auswählen, auf dem der Mobile Server läuft.

Ändern Sie ein Zertifikat:

1. Klicken Sie auf einem Computer, auf dem ein Mobiler Server installiert ist, mit der rechten Maustaste auf das Mobile Server Manager-Symbol in der Taskleiste des Betriebssystems und wählen Sie **Zertifikat bearbeiten** aus.
2. Zur Auswahl eines gültigen Zertifikates klicken Sie auf . Es öffnet sich ein Kasten mit dem Windows-Sicherheitsdialog.
3. Wählen Sie das Zertifikat aus, das Sie anwenden möchten.
4. Klicken Sie auf **OK**.

Eine Mitteilung informiert Sie darüber, dass das Zertifikat installiert wurde und dass der Mobile Server-Dienst neu gestartet wurde, um die Änderung anzuwenden.

Zugriff auf Protokolle und Untersuchungen (erklärt)

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

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

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



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

Untersuchungen-Ordner ändern

Standardspeicherort für Untersuchungen ist der Ordner **ProgramData**. Wenn Sie den standardmäßigen Ort des Untersuchungen-Ordners ändern, werden vorhandene Untersuchungen nicht automatisch an den neuen Standort kopiert, noch werden sie gelöscht. So ändern Sie den Ort wo die Untersuchungen-Exporte auf Ihrer Festplatte gespeichert werden:

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

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

2. Klicken Sie neben dem **Ordner**-Feld, das die aktuelle Position anzeigt, auf das Ordner-Symbol, um nach einem vorhandenen Ordner zu suchen oder einen neuen Ordner zu erstellen > Auf **OK** klicken.
3. Wählen Sie aus der Liste mit **Alten Untersuchungen**, wählen Sie die Aktion, die Sie auf die vorhandene Untersuchung anwenden möchten, welche am aktuellen Speicherort gespeichert ist. Die Optionen sind:
 - **Verschieben**: Bewegt vorhandene Untersuchungen zum neuen Ordner



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

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

Status anzeigen (Erklärung)

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

Name	Beschreibung
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.

Fehlerbehandlung

Fehlerbehandlung XProtect Mobile

Verbindungen

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

Um eine Verbindung zu Ihren Aufzeichnungen herzustellen, muss der XProtect Mobile-Server auf demjenigen Server installiert sein, auf dem auch 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 sind entweder als Plugins oder als Teil einer Produktinstallation oder eines Upgrade installiert. Einzelheiten dazu, wie Sie den XProtect Mobile-Server erhalten und wie die Einstellungen für den XProtect Mobile-Client in Ihr XProtect-System integriert werden finden Sie im Abschnitt Konfiguration (siehe Einstellungen des mobilen Servers auf Seite 14).

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

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

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

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

Das selbstsignierte Zertifikat im XProtect Mobile-Server muss durch Ihr eigenes Zertifikat ersetzt werden, das mit der Serveradresse übereinstimmt, die für die Verbindung mit dem XProtect Mobile-Server verwendet wird. Diese Zertifikate können von offiziellen Zertifizierungsstellen erhalten werden, z.B. Verisign. Zu weiteren Einzelheiten wenden Sie sich an die ausgewählte Zertifizierungsstelle.

XProtect Mobile Server verwendet kein Microsoft IIS. Das bedeutet, dass die von der Zertifizierungsstelle mithilfe von IIS zur Erzeugung der Dateien des Certificate Signing Requests (CSR) gegebenen Anweisungen für den XProtect Mobile-Server nicht gelten. Sie müssen die CSR-Datei mithilfe von Befehlszeilenzertifizierungstools oder sonstigen Drittanwendungen manuell erstellen. Dieses Verfahren sollte nur von Systemadministratoren oder fortgeschrittenen Anwendern durchgeführt werden.

Bildqualität

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

Der XProtect Mobile-Server stellt die Bildqualität je nach verfügbarer Bandbreite zwischen Server und Client automatisch ein. Wenn die Bildqualität geringer ist, als im XProtect® Smart Client, haben Sie u.U. zu wenig Bandbreite, um durch den XProtect Mobile-Client die volle Bildauflösung zu erhalten. Grund dafür kann entweder eine zu geringe Bandbreite vom Server im Upstream sein, oder zu wenig Bandbreite im Downstream auf dem Client. Siehe das **XProtect Smart Client Benutzerhandbuch**, das Sie von unserer Website (<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>) herunterladen können.

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

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

Prüfen Sie die Bandbreite Ihrer Internetverbindung zuhause. Viele private Internetverbindungen haben unterschiedliche Bandbreiten im Upload und Download, was oft z.B. als 20 Mbit/2 Mbit angegeben wird. 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 verschiedenen Standorten, an denen die Download-Geschwindigkeit des Netzwerks des XProtect Mobile-Clients gut ist, gleichbleibend niedrig ist, kann das Problem evtl. dadurch gelöst werden, dass Sie die Uploadgeschwindigkeit Ihrer Internetverbindung zuhause erhöhen.

Hardwarebeschleunigte Dekodierung

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

Nur neuere Prozessoren von Intel unterstützen die hardwarebeschleunigte Dekodierung. Schauen Sie auf der Intel-Website (<https://ark.intel.com/Search/FeatureFilter?productType=processors/>) nach, 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 finden Sie unter **Status anzeigen** im Mobile Server Manager (siehe Status anzeigen (Erklärung) auf Seite 56).

2. **Unterstützt mein Betriebssystem die hardwarebeschleunigte Dekodierung?**

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

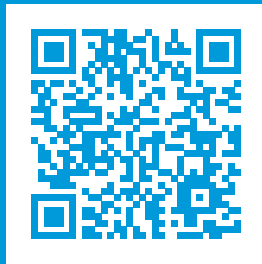
Achten Sie darauf, dass Sie auf Ihrem System die neuesten Grafiktreiber von der Internetseite von Intel installiert haben. Diese Treiber sind nicht über das Windows-Update erhältlich.

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

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

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

1. Suchen Sie die Datei VideoOS.MobileServer.Service.exe config. Der Pfad lautet üblicherweise:
C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config.
2. Öffnen Sie die Datei in Notepad oder in einem ähnlichen Texteditor. Legen Sie ggf. Notepad als Standardanwendung für Dateien mit der 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.



helpfeedback@milestone.dk

Über Milestone

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

