

MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile サーバー 2024 R1

システム管理者マニュアル



目次

著作権、商標、および免責条項	5
サポートされる VMS 製品とバージョン	6
概要	7
新機能	7
XProtect Mobile	8
要件と検討事項	9
XProtect Mobileサーバーをインストールする前に	9
通知設定の要件	9
スマートコネクト設定の要件	9
ユーザーの2要素認証設定の要件	10
ビデオプッシュ設定の要件	10
ダイレクトストリーミングの要件	10
共有を使用する要件	10
インストール	11
XProtect Mobileサーバーのインストール	11
設定	14
モバイルサーバーの設定	14
接続情報	14
一般タブ	15
接続タブ	18
[サーバーのステータス]タブ	20
パフォーマンスタブ	21
調査	24
ビデオプッシュタブ	26
通知タブ	27
要素認証タブ	28
直接ストリーミング	31
アダプティブストリーミング	31

モバイルサーバーデータの暗号化（説明付き）	32
モバイルサーバーで暗号化を有効にする	34
Milestone Federated Architectureと親/子サイト	35
スマートコネクト	35
スマートコネクトの設定	36
ルーターでUniversal Plug and Play検出を有効化する	36
複雑なネットワークでの接続を有効にする	36
接続の設定	37
Eメールメッセージをユーザーに送信する	37
通知	38
XProtect Mobileサーバーでプッシュ通知を設定	38
特定のモバイルデバイスまたはすべてのモバイルデバイスへのプッシュ通知の送信を有効化する	39
特定の、またはすべてのモバイルデバイスへのプッシュ通知の送信を停止する	39
登録済みデバイスリストから1つあるいはすべての登録済みデバイスを削除	39
調査の設定	40
ビデオプッシュを使用したビデオのストリーミング	42
ビデオをストリーミングするためのビデオプッシュの設定	42
ビデオをストリーミングするためのビデオプッシュチャンネルの追加	42
ビデオ プッシュチャンネルの編集	43
ビデオプッシュチャンネルの追加	43
パスワードの変更	43
レコーディングサーバーにハードウェアデバイスとしてビデオプッシュドライバを追加	44
ビデオプッシュドライバデバイスをビデオプッシュのためのチャンネルに追加	45
既存のビデオプッシュチャンネルで音声を有効にする	45
電子メールを使用して2要素認証のユーザーを設定する	46
SMTPサーバーに関する情報を入力します。	46
ユーザーに送信される認証コードを指定します。	46
ユーザーとActive Directoryグループへの認証方法の割り当て	47
アクション	47
モバイルデバイスの管理（MDM）	47

モバイルデバイスの管理プラットフォームでモバイルサーバーの詳細を設定する（システム管理者）	48
XProtect MobileクライアントおよびXProtect Web Clientで使用する出力に名前を付ける	49
外部IDPとXProtect Mobile	50
XProtect Web Clientの外部IDPログインを設定する	50
緊急アラートアラームの追加	50
メンテナンス	52
Mobile Server Manager	52
XProtect Web Clientへのアクセス	52
Mobile Serverサービスの起動、停止、再起動	53
データ保護パスワードの変更	53
ポート番号の表示/編集	54
ログへのアクセスおよび調査	54
調査フォルダーの変更	55
ステータスを表示	55
トラブルシューティング	57
XProtect Mobileトラブルシューティング	57
付録	60
付録A	60
付録B	63

著作権、商標、および免責条項

Copyright © 2024 Milestone Systems A/S

商標

XProtect は Milestone Systems A/S の登録商標です。

Microsoft および Windows は、Microsoft Corporation の登録商標です。App Store は Apple Inc. のサービスマークです。Android は Google Inc. の商標です。

本文書に記載されているその他の商標はすべて、該当する各所有者の商標です。

免責条項

本マニュアルは一般的な情報を提供するためのものであり、その作成には細心の注意が払われています。

この情報を使用することにより発生するリスクはすべて、使用者が負うものとします。また、ここに記載されている内容はいずれも、いかなる事柄も保証するものではありません。

Milestone Systems A/S は、事前の通知なしに変更を加える権利を有するものとします。

本書の例で使用されている人物および組織の名前はすべて架空のものです。実在する組織や人物に対する類似性は、それが現存しているかどうかにかかわらず、まったく偶然であり、意図的なものではありません。

この製品では、特定の規約が適用される可能性があるサードパーティー製ソフトウェアを使用することがあります。その場合、詳細はMilestoneシステムインストールフォルダーにあるファイル`3rd_party_software_terms_and_conditions.txt`をご参照ください。

サポートされる VMS 製品とバージョン

このマニュアルでは、次の XProtect VMS 製品でサポートされる機能について説明します。

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

Milestone は、XProtect VMS 製品の現行のバージョンと以前の 2 つのバージョンを使用して、本書に記載されている機能をテストします。

新しい機能が現在のリリースバージョンでのみサポートされており、以前のリリースバージョンではサポートされていない場合は、機能の説明にこれに関する情報が記載されます。

下記の販売が終了した XProtectVMS 製品でサポートされている XProtect クライアントと拡張機能のドキュメントは、Milestone ダウンロードページ (<https://www.milestonesys.com/downloads/>) にあります。

- XProtect Enterprise
- XProtect Professional
- XProtect Express
- XProtect Essential

概要

新機能

XProtect Mobile サーバー2023 R3

接続情報

- モバイルサーバーがインターネットからアクセス可能かどうかを確認します。[14ページの接続情報](#)をご参照ください。

アラーム

- 緊急アラートアラームを追加して、ユーザーがXProtect Mobileクライアントの最高重大度レベルのアラーム通知を受信できるようにします。[50ページの緊急アラートアラームの追加](#)をご参照ください。

XProtect Mobileサーバー2023 R2

ブックマークとライブビデオの共有

- XProtect Mobileクライアントでブックマークとライブビデオを共有するには、マネジメントサーバーで暗号化を有効にする必要があります。[10ページの共有を使用する要件](#)をご参照ください。

通知

- VMSデータベースからデバイス登録データを削除できます。[39ページの登録済みデバイスリストから1つあるいはすべての登録済みデバイスを削除](#)をご参照ください。

XProtect Mobileサーバー2022 R3

外部IDP

- 外部IDPを使用してXProtect Web ClientおよびXProtect Mobileクライアントにログインできるようになりました。[50ページの外部IDPとXProtect Mobile](#) を参照

モバイルデバイスの管理 (MDM)

- XProtect Mobileクライアントがモバイルデバイスの管理 (MDM) に対応しました。MDMを利用することで、デバイス、アプリ、データを1つの統合されたコンソールから管理および保護することができます。詳細については、[47ページのモバイルデバイスの管理 \(MDM\)](#) をご参照ください。

プッシュ通知

- この機能を有効にすると、システムがGDPRに準拠していない可能性があることを知らせる警告が表示されます。

XProtect Mobileサーバー2022 R2

通知

- 通知はデフォルトで無効です。

インストール

- Mobile Serverをインストールする際に、基本ユーザーとして監視システムに接続できます。

XProtect Mobile

XProtect Mobileは5つのコンポーネントから成り立っています。

XProtect Mobile クライアント

XProtect MobileクライアントはAndroidまたは Apple デバイスでインストールするモバイル サーヴェイランスアプリを使用できます。必要に応じてインストールしたXProtect Mobileクライアントの数だけ使うことができます。

XProtect Web Client

XProtect Web Clientでは、お使いのWebブラウザでライブ ビデオを閲覧でき、録画もダウンロードできます。XProtect Web Clientは、XProtect Mobileサーバーのインストール時に一緒に自動的にダウンロードされます。

XProtect Mobile サーバー

XProtect Mobileサーバーは、XProtect MobileクライアントまたはXProtect Web Clientからのシステムへのログインを処理する役割があります。

XProtect Mobileサーバーは、レコーディングサーバーから送られたビデオストリームをXProtect MobileクライアントまたはXProtect Web Clientに配信する役割を担います。これにより、レコーディングサーバーのインターネットへの接続を伴わない、安全なセットアップが可能です。XProtect Mobileサーバーがレコーディングサーバーからビデオストリームを受信すると、コーデックとフォーマットの複雑な変換を処理し、モバイルデバイス上でビデオストリーミングできます。

XProtect Mobile プラグイン

XProtect MobileプラグインはXProtectMobile Serverコンポーネントの一部です。このXProtect Mobileプラグインを使用すると、XProtect Management Clientの**Servers**ノードから、VMSシステム内のモバイルサーバーを表示および管理できます。

モバイルサーバーを管理するXProtect Management ClientコンピュータにXProtect Mobileプラグインをインストールします。

Mobile Server Manager

Mobile Server Managerを使用して、サービスに関する情報の取得、Mobile Serverサービスの状態の確認、ログやステータスメッセージの表示、サービスの開始と停止を行います。

XProtect MobileサーバーXProtect Mobileとプラグイン、およびにMobile Server Managerについては、このマニュアルで説明します。

要件と検討事項

XProtect Mobileサーバーをインストールする前に

さまざまな VMS アプリケーションおよびシステムコンポーネントのシステム要件についての情報は、Milestone ウェブサイト (<https://www.milestonesys.com/systemrequirements/>) をご覧ください。

MilestoneはXProtect Mobileサーバーを別のコンピュータにインストールすることを推奨しています。XProtectMobile Serverコンポーネントをインストールして使い始める前に、以下のことを確認してください。

- XProtect Management Clientでカメラとビューを設定済み。
- モバイルサーバーのコンピュータが、他のVMS サーバーコンポーネントを実行するコンピュータのホスト名を解決する。
- マネジメントサーバーのコンピュータがモバイルサーバーのコンピュータのホスト名を解決する。
- 稼働するVMSがインストールされている。
- 少なくとも1人のVMSユーザーを設定済み。監視システムに接続するには、このユーザーが追加された役割は、マネジメントサーバーの権限を必要とします。
 - 接続
 - 読み取り
 - 編集
- システムをアップグレードする場合は、XProtect Mobileプラグインのバージョンがモバイルサーバーのバージョンと一致していることをご確認ください。プラグインとモバイルサーバーのバージョンが異なる場合、システムが正常に機能しない可能性があります。

通知設定の要件

イベント発生時にユーザーに通知するには、以下が必要です。

- 1つ以上のアラームを1つ以上のイベントとルールに関連付ける必要があります。これはシステム通知では必要ありません。
- Milestone Care™との最新のMilestone Systems契約を締結していること。
- システムがインターネットに接続していること。

詳細については以下を参照：

[38ページのXProtect Mobileサーバーでプッシュ通知を設定](#)

[27ページの通知タブ](#)

スマートコネクト設定の要件

スマートコネクトを使用し、正しく設定されていることXProtect Mobileを確認するには、以下が必要です。

- XProtect MobileサーバーのパブリックIPアドレス。アドレスは静的または動的なものが可能ですが、一般的に静的IPアドレスを使用することをお勧めします。
- スマートコネクトの有効なライセンス
- Milestone Systemsとの最新のMilestone Care™契約の締結

ユーザーの2要素認証設定の要件

電子メールを使用して2要素認証の設定を行うには、以下をご確認ください。

- SMTPサーバーがインストールされていること。
- ユーザーおよびグループが**サイトナビゲーション**ペインの**役割**ノードのXProtectでManagement Clientシステムに追加されていること。関連する役割で、**ユーザーとグループ**タブを選択します。
- システムを以前のバージョンのXProtectからアップグレードした場合、2要素認証機能を有効にするには、Mobile Serverサービスを再起動する必要があります。

詳細については以下を参照：

[46ページの電子メールを使用して2要素認証のユーザーを設定する](#)

[28ページの要素認証タブ](#)

ビデオプッシュ設定の要件

モバイルデバイスのカメラからXProtect監視システムにビデオをストリーミングするには、以下が必要です。

- 使用する各チャンネルのデバイスライセンス。

ダイレクトストリーミングの要件

XProtect Mobileは、ライブモードでのダイレクトストリーミングに対応しています。XProtect Web ClientおよびXProtect Mobileクライアントでダイレクトストリーミングを使用するには、以下のカメラ設定が必要です。

- カメラがH.264またはH.265コーデックに対応している。



XProtect MobileクライアントはH.264のみに対応しています。

- **GOPサイズ**の値には**1秒**を設定し、**FPS**には**10 FPS**を上回る値を設定することが推奨されます。

共有を使用する要件

ユーザーは、XProtect Mobile クライアントアプリを使用中にブックマークやライブビデオを共有できます。これらの機能は以下の後に利用可能になります。

- マネジメントサーバーで暗号化が有効になっている。

インストール

XProtect Mobileサーバーのインストール

XProtect Mobileサーバーをインストールすると、XProtect MobileクライアントとXProtect Web Clientをシステムで使えるようになります。マネジメントサーバーを実行するコンピュータのシステムリソースの使用量を全体的に減らすには、個別のコンピュータ上にXProtect Mobileサーバーをインストールします。

マネジメントサーバーには、ビルトインの公開インストールウェブページがあります。このウェブページでは、システム管理者およびエンドユーザーが、マネジメントサーバーまたは他のすべてのシステムのコンピュータから必要なXProtectシステムコンポーネントをダウンロードしてインストールできます。



「シングルコンピュータ」オプションをインストールすると、XProtect Mobileサーバーは自動でインストールされます。

XProtect Mobileサーバーインストーラをダウンロードします

1. ブラウザに次のURLを入力します: `http:// [マネジメントサーバーアドレス] /installation/admin` [マネジメントサーバーアドレス] は、マネジメントサーバーのIPアドレスまたはホスト名です。
2. XProtect Mobileサーバーインストーラ向けに**すべての言語**を選択します。

XProtect Mobileサーバーのインストール

1. ダウンロードしたファイルを実行します。すべての警告に対して**はい**をクリックします。
2. インストーラの言語を選択します。**続行**を選択します。
3. 使用許諾契約を読み、同意します。**続行**を選択します。
4. インストールのタイプを選択します。
 - XProtect Mobileサーバーとプラグインをインストールするには、**標準**を選択します。
 - サーバーのみ、またはプラグインのみをインストールするには、**カスタム**を選択します。例えば、Management Clientを使ってXProtect Mobileサーバーを管理したいが、コンピュータ上でXProtect Mobileサーバーが不要な場合は、プラグインのみをインストールすると便利です。



XProtect MobileManagement ClientでXProtect Mobileサーバーを管理するには、Management Clientを実行するコンピュータ上にプラグインが必要です。

5. カスタムインストールのみ：インストールしたいコンポーネントを選択します。**続行**を選択します。

6. モバイルサーバーのサービスアカウントを選択します。**続行**を選択します。



後の段階でサービスアカウント資格情報を変更または編集するには、モバイルサーバーを再インストールする必要があります。

7. カスタムインストールのみ：監視システムに接続するには、既存のVMSユーザーアカウントでログインします。

- **サービスアカウント**は、手順8で選択したアカウントです。このアカウントを使用して接続するには、サービスアカウントがマネジメントサーバーがアクセスできるドメインのメンバーになっていることを確認します。
- **基本ユーザー**：サービスアカウントがマネジメントサーバーがアクセスできるドメインのメンバーになっていない場合は、基本ユーザーを使用します。



後の段階でサービスアカウントまたは基本ユーザーの資格情報を変更または編集するには、モバイルサーバーを再インストールする必要があります。

続行をクリックします。

8. **サーバーURL**フィールドに、プライマリマネジメントサーバーのアドレスを入力します。

カスタムインストールのみ：モバイルサーバーと通信する接続ポートを指定します。**続行**を選択します。通常のインストールでは、通信ポートにはデフォルトのポート番号が割り当てられます（HTTP ポートは8081、HTTPSポートは8082）。

9. **モバイルサーバーのデータ保護パスワードを割り当て**ページで、パスワードを入力して調査を暗号化します。システムを復元する場合や、追加のモバイルサーバーを使用してシステムを拡張する場合、モバイルサーバーのデータにアクセスするため、システム管理者はこのパスワードを入力する必要があります。



このパスワードを保存し、安全に保管してください。この指示に従わない場合、モバイルサーバーのデータを復元する機能が損なわれる可能性があります。

調査をパスワードで保護したくない場合は、**モバイルサーバーのデータ保護パスワードを使用しないことを選択し、調査が暗号化されないことを理解しました**を選択します。

[**続行**] をクリックします。

10. モバイルサーバーの暗号化を指定します。**続行**を選択します。

暗号化を選択ページでは、以下の通信フローを保護できます。

- モバイルサーバーとレコーディングサーバー、データコレクター、マネジメントサーバー間。内部通信フローの暗号化を有効にするには、**サーバー証明書**セクションで証明書を選択します
- モバイルサーバーとクライアント間。モバイルサーバーからデータストリームを取得するモバイルサーバーとクライアント間の暗号化を有効にするには、**ストリーミングメディア証明書**セクションで証明書を選択します



暗号化を有効にしないと、クライアントでいくつかの機能が利用できなくなります。
詳しくは、[クライアントのモバイルサーバー暗号化要件](#)をご参照ください。

システムで安全な通信を確立する方法の詳細については、以下を参照してください：

- [レコーディングサーバーのデータの暗号化（説明付き）](#)
- [証明書に関するMilestoneガイド](#)

オペレーティングシステムのタスクバーにあるMobileServerManagerトレイアイコンからインストールを完了した後に、暗号化を有効にすることもできます（[34ページのモバイルサーバーで暗号化を有効にする](#)を参照）。

11. ファイルの場所と製品の言語を選択し、**インストール**を選択します。

インストールが完了すると、インストールされたコンポーネントのリストが表示されます。

設定

モバイルサーバーの設定

ManagementClientでは、XProtectMobileサーバー設定のリストを作成して編集できます。この設定には、モバイルサーバーの**プロパティ**セクションの最下部にあるツールバーでアクセスできます。ここからは、次のことができます：

- サーバー機能の一般構成の有効化または無効化（[15ページの一般タブ](#)を参照）
- サーバー接続設定を行う（[18ページの接続タブ](#)を参照）
- スマートコネクト機能を設定する（[18ページの接続タブ](#)を参照）
- サーバーの現在のステータスとアクティブなユーザーの一覧を表示（[20ページの\[サーバーのステータス\]タブ](#)を参照）
- パフォーマンスパラメーターを設定することで、ダイレクトストリーミングまたはアダプティブストリーミングを有効にしたり、トランスコード化したビデオストリーミングの制限を設定したりできます（[21ページのパフォーマンスタブ](#)を参照）
- 調査設定の構成（[24ページの調査](#)を参照）
- ビデオプッシュ設定の構成（[26ページのビデオプッシュタブ](#)を参照）
- システム通知とプッシュ通知の設定、およびオン、オフの切り替え（[27ページの通知タブ](#)を参照）
- ユーザー向けの追加ログインステップの有効化および設定（[28ページの要素認証タブ](#)を参照）

接続情報

以下の表は、すべてのタブで表示されるモバイルサーバーのステータスとメッセージについて説明しています。

サーバーにはインターネット経由でアクセスできます。

色	ステータス	説明
オレンジ色	N/A	モバイルサーバーはローカルネットワーク外からアクセスできるように設定されていません。

色	ステータス	説明
赤	いいえ	XProtect Web ClientおよびXProtect Mobileのクライアントユーザーはインターネットからモバイルサーバーに接続できません。
緑	はい	XProtect Web ClientとXProtect Mobileクライアントユーザーはインターネットからモバイルサーバーに接続できます。

サーバーへの接続

色	メッセージ	説明
オレンジ色	HTTPSの無効な証明書	XProtect Mobileプラグインがモバイルサーバーの証明書を認識しません。
オレンジ色	HTTP/HTTPS*（アクセス不能）	XProtect Management Clientがモバイルサーバーにアクセスできません。
赤	HTTP/HTTPS（未接続）	XProtect Management Clientがモバイルサーバーを検出しましたが、接続できません。
緑	HTTP/HTTPS	XProtect Management Clientがモバイルサーバーとの接続を確立しました。

一般タブ

以下の表で、このタブの設定について説明します。

一般

名前	説明
サーバー名	XProtect Mobileサーバーの名前を入力します。
説明	オプションで、XProtect Mobileサーバーの説明を入力します。
モバイルサーバー	現在選択中のXProtect Mobileサーバーの名前を確認します。

機能

XProtect Mobileの機能をどのように管理するかについて下表に記します。

名前	説明
XProtect Web Clientを有効化	XProtect Web Clientへのアクセスを有効にします。この機能はデフォルトで有効になっています。
XProtect Mobileクライアントの、「すべて」のカメラビューを有効にします	このビューには、レコーディングサーバーでユーザーが閲覧できるカメラがすべて表示されます。この機能はデフォルトで有効になっています。
ブックマークを有効にする	ブックマーク機能を有効にして、XProtect MobileクライアントとXProtect Web Clientでビデオシーケンスをすばやく見つけます。この機能はデフォルトで有効になっています。
アクションを有効（出力およびイベント）	XProtect MobileクライアントおよびXProtect Web Clientでアクションへのアクセスを有効にします。この機能はデフォルトで有効になっています。 この機能を無効にすると、クライアントユーザーは出力とイベントを（たとえこれらが適切に構成されていても）表示することはできません。
インカム音声を使用可能にする	XProtect Web ClientとXProtect Mobileクライアントで受信音声機能を有効にします。この機能はデフォルトで有効になっています。

名前	説明
プッシュ・トゥ・トークを有効にする	XProtect Web ClientとXProtect Mobileクライアントで、プッシュ・トゥ・トーク（PTT）機能を有効にします。この機能はデフォルトで有効になっています。
XProtect Mobileサーバーへの組み込みシステム管理者役割アクセスを拒否	組み込まれたシステム管理者役割に割り当てられたユーザーがXProtect MobileクライアントあるいはXProtect Web Clientのビデオにアクセスすることの除外を有効にします。

ログ設定

ログ設定情報を見ることができます。

名前	説明
ログファイルの場所	システムがログファイルを保存する場所を指定します。
ログの保存期間	ログを保持する日数を確認します。デフォルトは30日です。

設定のバックアップ

システムに複数のXProtect Mobileサーバーがある場合、バックアップ機能を使って既存の設定をエクスポートし、その他のXProtect Mobileサーバーにそれらをインポートします。

名前	説明
インポート	新規XProtect Mobileサーバー構成でXMLファイルをインポートします。
エクスポート	XProtect Mobileサーバー構成をエクスポートします。システムは、構成をXMLファイルに保存しています。

接続タブ

接続タブの設定は以下のタスクで使用できます。

- [37ページの接続の設定](#)
- [37ページのEメールメッセージをユーザーに送信する](#)
- [36ページの複雑なネットワークでの接続を有効にする](#)
- [36ページのルーターでUniversal Plug and Play検出を有効化する](#)

詳細については、[35ページのスマートコネクト](#)をご参照ください。



インストール中、**XProtect Mobile**を開いた際にXProtect Web ClientクライアントとXProtect MobileユーザーがServer Configuratorサーバーに接続する方法を設定できます。インストール後にMobile Server Managerトレイアイコンを右クリックすることも可能です。接続タイプはHTTPSまたはHTTPのいずれかになります。詳細については、[34ページのモバイルサーバーで暗号化を有効にする](#)をご参照ください。

一般

名前	説明
クライアントタイムアウト	XProtect MobileクライアントおよびXProtect Web Clientが、自らが実行中であることをXProtect Mobileサーバーに表示すべき時間枠を設定します。デフォルト値は30秒です。 Milestoneは、この時間枠を長くしないことを推奨しています。
UPnP-検出を有効に設定	これによってXProtect MobileUPnPプロトコルを用いてネットワーク上でサーバーを見つけることができます。 XProtect Mobileクライアントは、UPnPに基づいてXProtect Mobileサーバーを見つけるためのスキャン機能を有しています。
自動ポートマッピングを有効にする	XProtect Mobileサーバーがファイアウォールの後方にインストールされている場合、クライアントが引き続きインターネットからサーバーにアクセスできるよう、ルーターにポートマッピングが必要となります。 自動ポートマッピングを有効にするオプション を選択すると、XProtect Mobileサーバー自体がポートマッピングを実行できます。ただし、ルーターがこれに対応できるよう設

名前	説明
	定されていないではありません。
Smart Connect を有効にする	Smart Connectは検証を行うためにモバイル機器やタブレットにログインせずに、XProtect Mobileサーバーが正しく設定されたことを確認できるようにします。また、クライアントのユーザーの接続プロセスを簡易化します。

インターネットアクセス

名前	説明
カスタムインターネットアクセスの構成	IPアドレスまたはホスト名 と、接続に使われるポート番号を提供します。たとえば、ルーターがUPnPをサポートしない場合や、ルーターのチェーンがある場合に、これを実行できます。
• HTTP • HTTPS	接続のタイプを選択します。
選択するとIPアドレスを自動的に取得します	IPアドレスが頻繁に変更される場合は、チェックボックスをオンにします。
校正されたURLアドレスのみを使用する	カスタム指定のIPアドレスまたはホスト名のみを使用してモバイルサーバーに接続するには、チェックボックスを選択します。
サーバーアドレス	モバイルサーバーと接続されているすべてのURLアドレスをリストアップします。

Smart Connect通知

名前	説明
招待を電子メールで送信する:	Smart Connect通知の受信者の電子メールアドレスを入力します。
電子メール言語	電子メールで使用する言語を指定します。
Smart Connect トークン	モバイルデバイスのユーザーがXProtect Mobileサーバーに接続するために使用できる固有の識別子。
Smart Connectへのリンク	モバイルデバイスのユーザーがXProtect Mobileサーバーに接続するために使用できるリンク。

[サーバーのステータス]タブ

XProtect Mobileサーバーにおけるステータスの詳細を見る。詳細は読み取り専用です：

名前	説明
サーバー有効化日	XProtect Mobileサーバーが前回起動したときの日時を示します。
CPU使用率	サーバーでの現在のCPU使用状況を示します。
外部帯域幅	現在のXProtect MobileクライアントあるいはXProtect Web Clientとモバイルサーバーの間の帯域幅を示します。

アクティブなユーザー

XProtect Mobileサーバーと現在接続されているXProtect Web Clientクライアント、あるいはXProtect Mobileサーバーのステータスの詳細を見ます。

名前	説明
ユーザー名	モバイルサーバーと接続されているXProtect Mobileクライアント、あるいはXProtect Web Clientユーザーのそれぞれのユーザー名を表示します。
ステータス	XProtect Mobileサーバーと、対象となるXProtect Mobile クライアント、あるいはXProtect Web Clientユーザーの間の現在の関係を表示します。考えられる状態： ● 接続済み：クライアントとサーバーがキーと暗号化資格情報を交換する時の最初のステータス ● ログイン：XProtect Mobileクライアント、あるいはXProtect Web ClientユーザーはXProtectシステムにログインしています。
ビデオ帯域幅使用状況(kB/秒)	各XProtect MobileクライアントまたはXProtect Web Clientユーザーに対して現在開かれている、ビデオストリームの帯域幅の合計が表示されます。
音声帯域幅使用状況(kB/秒)	各XProtect Web Clientユーザーに対して現在開かれている、音声ストリームの帯域幅の合計が表示されます。
トランスコードされたビデオストリーム	各XProtect MobileクライアントまたはXProtect Web Clientユーザーに対して現在開かれている、トランスコード化ビデオストリームの総数が表示されます。
ダイレクトビデオストリーム	各XProtect MobileクライアントまたはXProtect Web Clientユーザーに対して現在開かれている、ダイレクトビデオストリームの総数が表示されます（XProtect ExpertおよびXProtect Corporateのみ）。
トランスコードされた音声ストリーム	各XProtect Web Clientユーザーに対して現在開かれている、トランスコード化音声ストリームの総数が表示されます。

パフォーマンスタブ

「パフォーマンス」タブでは、XProtect Mobileサーバーのパフォーマンスに対して以下の設定と制限を設けることができます。

ビデオストリーミング設定（XProtect ExpertおよびXProtect Corporate専用）

名前	説明
直接ストリーミングを有効化	XProtect Web ClientおよびXProtect Mobileクライアントでの直接ストリーミングを有効にします（XProtect ExpertおよびXProtect Corporateのみ）。この機能はデフォルトで有効になっています。
アダプティブストリーミングの有効化	XProtect Web ClientとXProtect Mobileクライアントでアダプティブストリーミングを有効にします（XProtect ExpertとXProtect Corporateの場合のみ）。この機能はデフォルトで有効になっています。
ストリーミングモード	アダプティブストリーミング機能を有効にすると、ストリーミングモードのタイプをリストから選択できるようになります。 ● ビデオ画質の最適化（デフォルト） - 利用可能なもっとも低い解像度（要求したものと同等またはそれ以上の解像度）を持つストリームが選択されます ● サーバーパフォーマンスの最適化 - 要求された解像度を低下させた後、使用可能なもっとも低い解像度（低下したものと同等またはそれ以上の解像度）を持つストリームが選択されます ● 低帯域幅用に解像度を最適化 - 利用可能なもっとも低い解像度を持つストリームが選択されます（3Gまたは不安定なネットワークを使用している場合に推奨）

トランスコード化ビデオストリームの制限

レベル1

レベル1は、XProtect Mobileサーバーにデフォルトで設定される制限です。ここで設定した制限は、常にXProtect Mobileのトランスコード化ビデオストリームに適用されます。

名前	説明
レベル1	チェックボックスを選択すると、XProtect Mobileサーバーのパフォーマンスに第一レベルの制限が適用されます。
最大FPS	XProtect Mobileサーバーからクライアントへの送信のフレーム数/秒(FPS)の最大数について制限を設定します。
最大画像解像度	XProtect Mobileサーバーからクライアントへ送信される画像の解像度について制限を設定します。

レベル2

レベル1でデフォルトである制限とは異なるレベルの制限を強制したい場合は、代わりに**レベル2**のチェックボックスを選択します。最初のレベルで設定したレベルより高い設定はできません。たとえば、**レベル1**で最大FPSを45に設定すると、**レベル2**では、最大FPSは44以下にしか設定できません。

名前	説明
レベル2	チェックボックスを選択すると、XProtect Mobileサーバーのパフォーマンスに第二レベルの制限が適用されます。
CPUしきい値	システムがビデオストリームの制限を強制する前に、XProtect MobileサーバーのCPU負荷についてしきい値を設定します。
帯域幅しきい値	システムがビデオストリームの制限を強制する前に、XProtect Mobileサーバーの帯域負荷についてしきい値を設定します。
最大FPS	XProtect Mobileサーバーからクライアントへの送信のフレーム数/秒(FPS)の最大数について制限を設定します。
最大画像解像度	XProtect Mobileサーバーからクライアントへ送信される画像の解像度について制限を設定します。

レベル3

また、**レベル3**チェックボックスを選択して、制限に関する第三レベルを作成することもできます。**レベル1**および**レベル2**で設定したレベルより高い設定はできません。たとえば、**レベル1**で**最大FPS**を45に、**レベル2**で32に設定すると、**レベル3**では**最大FPS**は31以下にしか設定できません。

名前	説明
レベル3	チェックボックスを選択すると、XProtect Mobileサーバーのパフォーマンスに第一レベルの制限が適用されます。
CPUしきい値	システムがビデオストリームの制限を強制する前に、XProtect MobileサーバーのCPU負荷についてしきい値を設定します。
帯域幅しきい値	システムがビデオストリームの制限を強制する前に、XProtect Mobileサーバーの帯域負荷についてしきい値を設定します。
最大FPS	XProtect Mobileサーバーからクライアントへの送信のフレーム数/秒(FPS)について制限を設定します。
最大画像解像度	XProtect Mobileサーバーからクライアントへ送信される画像の解像度について制限を設定します。



システムは、あるレベルから別のレベルへすぐに切り替わることはありません。CPUまたは帯域のしきい値の変動が指定されたレベルから5パーセント未満であれば、現在のレベルを使用し続けます。

調査

調査設定

他の人がXProtect MobileクライアントやXProtect Web Clientを使用して以下を実行できるように調査を有効にすることができます。

- 録画ビデオにアクセスする
- インシデントを調査する
- ビデオエビデンスを準備してダウンロードする

名前	説明
調査を有効にする	このチェックボックスを選択すると、ユーザーは調査を作成できます。
調査フォルダー	ビデオがハードドライブのどこにエクスポートされ保存されたかを表示します。
他のユーザーの調査を表示する	このチェックボックスを選択すると、ユーザーが自分が作成していない調査にアクセスできます。
調査フォルダーのサイズ制限を有効にします	このチェックボックスを選択すると、調査フォルダーのサイズ制限を設定し、調査フォルダーに含めることのできる最大メガバイト数を入力できます。デフォルトのサイズは2000 MBです。
調査の保存期間を有効に設定	このチェックボックスを選択すると、調査の保存期間を設定できます。初期設定の保存期間は7日間です。
エクスポートフォーマット	使用したいエクスポートフォーマットのチェックボックスを選択してください。以下のエクスポートフォーマットを利用できます。 • AVIフォーマット • XProtectフォーマット • MKVフォーマット デフォルトでチェックボックスは選択されていません。
AVIエクスポートのタイムスタンプを含む	このチェックボックスを選択すると、AVIファイルがダウンロードされた日時が含まれます。
AVIエクスポートで使用されたコーデック	ダウンロード用のAVIパッケージを準備するときに使用する圧縮形式を選択します。 選択するコーデックは、オペレーティングシステムによって異なる場合があります。必要なコーデックが表示されない場合は、XProtect Mobileサーバーが稼働しているコンピュータにインストールすると、リストに追加されます。
AVIのエクスポートに使用された音声のビット	エクスポートするビデオに音声が含まれている場合は、リストから適切な音声ビットレートを選択します。デフォルトは160000 Hzです。

調査

名前	説明
調査	システムにて現在までに設定されている調査をリストアップする。調査のこれ以上の続行を希望しない場合は、 削除 あるいは すべて削除 ボタンを使用します。例えば、サーバーでより多くのディスク領域が使用できるようにする場合には、これは非常に便利です。
詳細	調査用にエクスポートされた個別のビデオファイルを削除しながらその調査を保持するには、リストで調査を選択します。 調査の詳細 グループで、エクスポート用の XProtect 、 AVI 、または MKV フィールドの右にある削除アイコンを選択します。

ビデオプッシュタブ

ビデオ配信を有効にする場合、以下の設定を指定します。

名前	説明
ビデオプッシュ	モバイルサーバーでビデオ配信を有効にします。
チャンネル数	XProtectシステムで有効なビデオ配信チャンネルの数が表示されます。
チャンネル	関連するチャンネルのチャンネル数が表示されます。編集不可。
ポート	関連するビデオ配信チャンネルのポート番号。
MACアドレス	関連するビデオ配信チャンネルのMACアドレス。
ユーザー名	関連するビデオ配信チャンネルに関連するユーザー名を入力します。
カメラ名	カメラが特定されている場合、カメラの名前が表示されます。

必要なステップが完了したら（[42ページのビデオをストリーミングするためのビデオプッシュの設定](#)を参照）、**カメラの検索**を選択して該当するカメラを検索します。

通知タブ

[通知]タブを使用して、システム通知とプッシュ通知をオン/オフにします。

デフォルトでは、通知は無効になります。

通知をオンにし、1つ以上のアラームとイベントが構成されている場合、XProtect Mobileはイベントが発生するとユーザーに通知します。アプリが開くと、モバイルデバイスのXProtect Mobileで通知が配信されます。プッシュ通知はXProtect Mobileを開いていないユーザーに通知します。これらの通知はモバイルデバイスに配信されます。

詳細については以下をご参照ください。 [39ページの特定のモバイルデバイスまたはすべてのモバイルデバイスへのプッシュ通知の送信を有効化する](#)

以下の表で、このタブの設定について説明します。

名前	説明
通知	このチェックボックスを選択すると、通知がオンになります。
デバイス登録の管理	このチェックボックスを選択すると、このサーバーに接続するデバイスとユーザーの情報を保存します。これらのデバイスに通知を送信します。 このチェックボックスをオフにする場合、デバイスのリストもクリアされます。ユーザーがもう一度通知の受信を開始する前に、チェックボックスを選択し、ユーザーはもう一度デバイスをサーバーに接続する必要があります。

登録されたデバイス

名前	説明
有効	このチェックボックスを選択すると、デバイスへの通知送信を開始します。
デバイス名	このサーバーに接続されているモバイルデバイスのリスト。 特定のデバイスへの送信を開始または停止するには、[有効]チェックボックスをオンまたはオフにします。
ユーザー	通知を受け取るユーザーの名前

要素認証タブ



使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (<https://www.milestonesys.com/products/software/product-index/>) の製品概要ページにあります。

[2段階認証]タブを使用して、以下のユーザーにおける追加のログインステップを有効にして指定します。

- iOS またはAndroid モバイル デバイスのXProtect Mobileアプリ
- XProtect Web Client

認証の最初のタイプはパスワードです。もう1つのタイプは認証コードで、これらを電子メールでユーザーに送信するように設定できます。

詳細については、[46ページの電子メールを使用して2要素認証のユーザーを設定する](#)をご参照ください。

以下の表で、このタブの設定について説明します。

プロバイダー設定>電子メール

名前	説明
SMTPサーバー	2要素認証電子メールの簡易メール転送プロトコル（SMTP）サーバーのIPアドレスまたはホスト名を入力します。
SMTPサーバーポート	電子メールを送信するSMTPサーバーのポートを指定します。 デフォルトのポート番号は、SSLを使用しない場合は25、SSLを使用する場合は465です。
SSLを使用	SMTPサーバーがSSL暗号化をサポートしている場合は、このチェックボックスを選択します。
ユーザー名	SMTPサーバーにログインするユーザー名を指定します。
パスワード	SMTPサーバーにログインするパスワードを指定します。

名前	説明
セキュリティで保護されたパスワード認証 (SPA) の使用	SMTPサーバーがSPAをサポートしている場合は、このチェックボックスを選択します。
送信者の電子メールアドレス	認証コードを送信する電子メールアドレスを指定します。
電子メールの件名	電子メールの件名を指定します。例：2要素認証コード。
電子メールテキスト	送信するメッセージを入力します。例：あなたのコードは{0}です。  {0} 変数の入力を忘れた場合、コードはデフォルトでテキストの最後に追加されます。

検証コード設定

名前	説明
再接続タイムアウト (0～30分)	たとえば、ネットワークが切断された場合、XProtect Mobileクライアントユーザーがログインを再確認する必要がある期間を指定します。デフォルトの期間は3分間です。 この設定はXProtect Web Clientには適応されません。
コードは (1～10分) 後に有効期限が切れます	ユーザーが受け取った認証コードを使用できる期間を指定します。この期間の後はコードが無効となるため、ユーザーは新しいコードを要求する必要があります。デフォルトの期間は5分間です。
コード入力試行 (1～10回試行)	提供されたコードが無効になるまでの、コード入力試行最大回数を指定します。デフォルトの回数は3回です。

名前	説明
コード長（4～6文字）	コードの文字数を指定します。デフォルトの長さは6文字です。
コードの構成	システムが生成するコードの複雑度を指定します。以下から選択できます。 • アルファベット大文字 (A-Z) • ラテン語の小文字(a～z) • 数字 (0～9) • 特殊文字 (!@#...)

ユーザー設定

名前	説明
ユーザーおよびグループ	XProtectシステムに追加されたユーザーおよびグループを一覧表示します。 グループがActive Directoryで構成されている場合、モバイルサーバーはActive Directoryからの電子メールアドレスなどの詳細情報を使用します。  Windowsグループは2要素認証をサポートしていません。
検証方法	各ユーザーまたはグループの認証設定を選択します。以下から選択できます。 • ログインなし：ユーザーはログインできません。 • 2要素認証なし：ユーザーはユーザー名とパスワードを入力しなければなりません。 • 電子メール：ユーザーはユーザー名とパスワードに加えて認証コードを入力しなければなりません
ユーザー詳細	各ユーザーがコードを受け取る電子メールアドレスを入力します。

直接ストリーミング

XProtect Mobileは、ライブモードでのダイレクトストリーミングに対応しています。

ダイレクトストリーミングは、H.264コーデック形式のビデオをXProtectシステムからクライアントに直接転送するためのビデオストリーミング技術です。これは、多くの新型IPカメラでサポートされています。ダイレクトストリーミングにはトランスコードは不要なため、XProtectにかかる負荷がいくらか軽減されます。

ダイレクトストリーミング技術は、（XProtectシステムにより、ビデオがカメラで使用されるコーデックからJPEGファイルへとデコードされる）XProtectのトランスコード設定とは対照的です。この機能を有効にすると、カメラとビデオストリーミングの設定を変更することなくCPU使用率が軽減します。さらにダイレクトストリーミングは、同一のハードウェアのパフォーマンスも向上させます（トランスコードと比較して最大で5倍の量のビデオストリーミングが可能）。

ダイレクトストリーミング機能を使用して、H.265コーデックに対応しているカメラからビデオを直接XProtect Mobileクライアントに転送することもできます。

Management Clientでは、クライアント向けのダイレクトストリーミングを有効または無効にできます（[14ページのモバイルサーバーの設定](#)を参照）。

ビデオストリームは、以下の場合にダイレクトストリーミングからトランスコーディングにフォールバックします。

- ダイレクトストリーミング機能がManagement Clientで無効にされたか、要件が満たされていない（[10ページのダイレクトストリーミングの要件](#)を参照）。
- ストリーミングカメラのコーデックがH.264またはH.265ではありません（XProtect Mobileクライアントのみ）
- ビデオを10秒間以上にわたって再生できない
- ストリーミングカメラのフレームレートが秒あたり1フレーム（1 FPS）に設定されている
- サーバーとの接続、またはカメラとの接続が失われました
- ライブビデオ中にプライバシーマスク機能を使用している

アダプティブストリーミング

XProtect Mobileは、ライブモードでのアダプティブストリーミングに対応しています。

アダプティブストリーミングは、同じカメラのビューで複数のライブビデオストリームを閲覧する場合に便利です。この機能はXProtect Mobileサーバーのパフォーマンスを最適化し、XProtect MobileクライアントとXProtect Web Clientを実行しているデバイスのデコード性能とパフォーマンスを改善します。

アダプティブストリーミングを活用するには、カメラに解像度の異なる複数のストリームを設定する必要があります。この場合、この機能では以下のことができます。

- ビデオ画質の最適化 - 利用可能な最も低い解像度（要求したものと同等またはそれ以上の解像度）を持つストリームが選択されます。
- サーバーパフォーマンスの最適化 - 要求された解像度を低下させた後、使用可能な最も低い解像度（低下したものと同等またはそれ以上の解像度）を持つストリームが選択されます。
- 低帯域幅用に解像度を最適化 - 利用可能な最も低い解像度を持つストリームが選択されます（3Gまたは不安定なネットワークを使用している場合に推奨）。



ズーム中に要求されるライブビデオストリームは、常に利用可能なもっとも高い解像度を持つものとなります。



帯域幅の使用はたいいてい、要求したストリームの解像度が下げられるのに併せて減少します。帯域幅の使用は、定義したストリーム構成の他の設定にも依存します。

アダプティブストリーミングの有効化/無効化、またはこの機能における優先ストリーミングモードの設定は、Management Clientのモバイルサーバー設定の**パフォーマンス**タブで行えます（[14ページのモバイルサーバーの設定](#)を参照）。

モバイルサーバーデータの暗号化（説明付き）

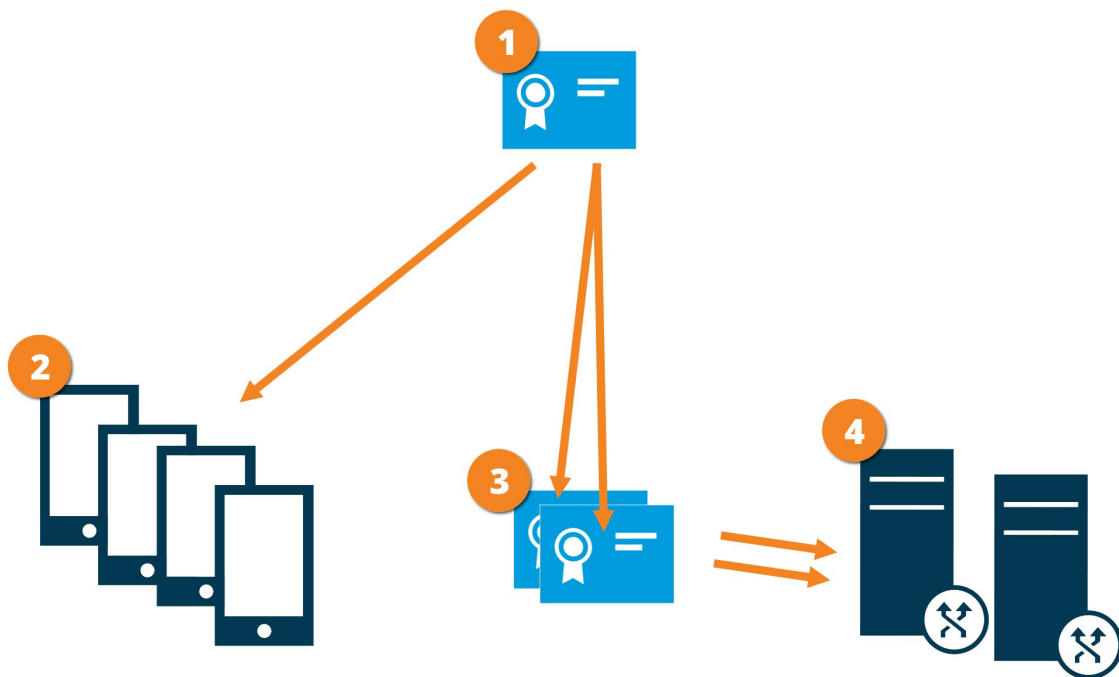
セキュリティ上の理由から、Milestoneは、ユーザーアカウントの設定を管理する際、モバイルサーバーとクライアント間で安全な通信を使用するよう推奨しています。

暗号化せずにHTTP通信を使用する場合は、XProtect Web Clientのプッシュ・トゥ・トーク機能は使用できません。

XProtectVMS では、暗号化はモバイルサーバーごとに有効化または無効化されます。モバイルサーバーで暗号化を有効にすると、クライアント、サービス、データストリームを取得する統合すべてとの通信を暗号化するか選択することができます。

モバイルサーバーの証明書配布

この図は、証明書が署名、信頼され、XProtectVMS で配布されて安全にモバイルサーバーとの通信が行えるという基本コンセプトを示しています。



❶ CA証明書は信頼されたサードパーティーのように機能し、サブジェクト/所有者（モバイルサーバー）と証明書を
確認する側（すべてのクライアント）双方に信頼されます。

❷ CA証明書はすべてのクライアント上で信頼されている必要があります。このようにして、クライアントはCAが発
行する証明書の有効性を確認します

❸ CA証明書は、モバイルサーバーとクライアントおよびサービス間の安全な接続を確立するために使用されます

❹ CA証明書はモバイルサーバーを実行しているコンピュータにインストールする必要があります

CA証明書の要件

- モバイルサーバーのホスト名は、サブジェクト/所有者として証明書に含まれているか、証明書発行対象の
DNSの名前リストに含まれていなくてはなりません
- 証明書は、モバイルサーバーからデータストリームを取得するサービスを実行しているすべてのデバイスで
信頼される必要があります
- モバイルサーバーを実行するサービスアカウントは、CA証明書のプライベートキーへのアクセス権限が必要
です

詳細については、[XProtect VMS システムの保護方法に関する証明書ガイド](#)を参照してください。

モバイルサーバーで暗号化を有効にする

HTTPSプロトコルを使用して、モバイルサーバーとクライアント間の安全な接続を確立する場合、サーバー上で有効な証明書を適用する必要があります。この証明書は、証明書所有者が安全な接続を確立する権限を持っていることを裏付けるものです。

詳細については、[XProtect VMS システムの保護方法に関する証明書ガイド](#)を参照してください。



サーバーグループの暗号化を設定する場合は、同じ CA 証明書に属する証明書で有効にする必要があります。暗号化が無効な場合は、サーバーグループのあらゆるコンピュータで無効にしなくてはなりません。



CA（証明書システム管理者）によって発行される証明書は証明書チェーンを持っており、このチェーンのルートにはCAルート証明書があります。デバイスまたはブラウザがこの証明書をみるとき、これはそのルート証明書とOS上にあらかじめインストールされているもの（Android、iOS、Windowsなど）とを比較します。ルート証明書があらかじめインストールされている証明書リストのなかにある場合は、サーバーへの接続が十分に安全であることをOSがユーザーに保証します。これらの証明書はドメイン名に対して発行され、無料です。

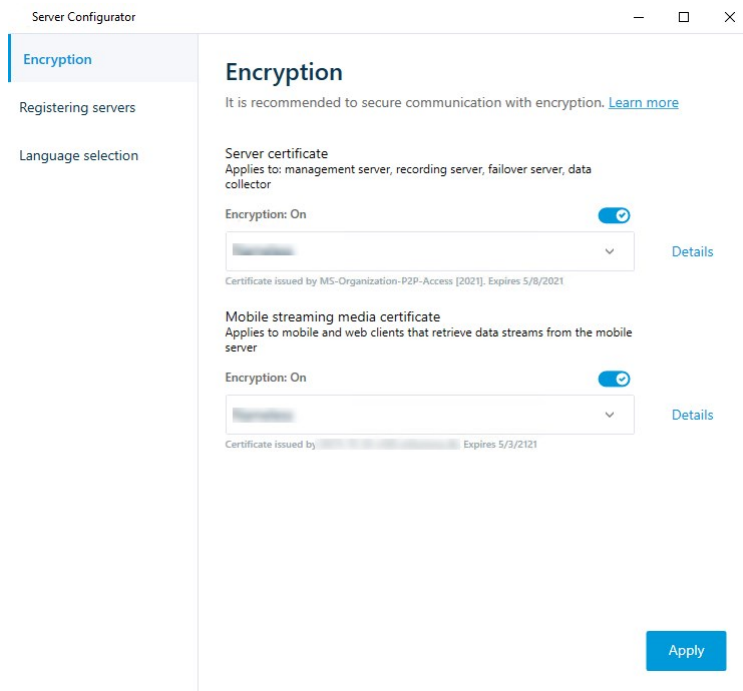
手順：

1. モバイル サーバーがインストールされているコンピュータで、以下から**Server Configurator**を開きます：
 - Windows のスタート メニューまたは
 - Mobile Server Managerコンピュータのタスクバーで Mobile Server Manager アイコンを右クリック
2. **Server Configurator**の[モバイル ストリーミング メディア証明書]で[暗号化]をオンにします。
3. [証明書を選択] をクリックすると、プライベートキーを持つ、Windows 証明書ストアでローカルコンピュータにインストールされている証明書の一意のサブジェクト名のリストが開きます。
4. XProtect MobileクライアントおよびXProtect Web Clientとモバイル サーバーとの通信を暗号化するための証明書を選択します。

[詳細] を選択すると、選択した証明書の Windows 証明書ストア情報が表示されます。

Mobile Serverサービス ユーザーには秘密キーへのアクセスが付与されています。この証明書はあらゆるクラ

クライアントで信頼される必要があります。



5. [適用] をクリックします。



証明書を適用すると、Mobile Serverサービスが再起動します。

Milestone Federated Architectureと親/子サイト

Milestone Federated Architectureは、複数の別個のシステムを親/子サイトのフェデレーテッドサイト階層にリンクします。

XProtect MobileまたはXProtect Web Clientですべてのサイトにアクセスするには、親サイトにのみXProtect Mobileサーバーをインストールします。

XProtect MobileまたはXProtect Web Clientクライアントのユーザーは、親サイトのマネジメントサーバーに接続する必要があります。

スマートコネクト

スマートコネクトを利用すると、検証を行うためにモバイルデバイスやタブレットにログインしなくても、XProtect Mobileが正しく設定されたことを確認できます。また、XProtect MobileクライアントとXProtect Web Clientユーザーの接続プロセスを簡素化します。

この機能では、XProtect MobileサーバーがパブリックIPアドレスを使用しており、システムにMilestone Care Plusサブスクリプションパッケージのライセンスが付与されている必要があります。

リモート接続の設定が成功した場合、即座にシステムからManagement Clientにフィードバックが送られ、XProtect Mobileサーバーがインターネットからアクセスできることを確認します。

スマートコネクトはXProtect Mobileサーバーが内部および外部のIPアドレス間をシームレスに切り替え、どこからでもXProtect Mobileに接続できるようにします。

顧客のモバイルクライアントの設定を容易にするために、Management Client内からエンドユーザーに直接Eメールを送信できます。Eメールにはサーバーを直接にXProtect Mobile追加するリンクが含まれています。これでネットワークアドレスやポートを入力する必要なしに設定が完了します。

スマートコネクトの設定

スマートコネクト機能を設定するには、次の手順に従います。

1. Management Clientのナビゲーションペインで、**サーバー**を展開し、**モバイルサーバー**を選択します。
2. モバイルサーバーを選択し、**接続**タブをクリックします。
3. ルーターでUniversal Plug and Play検出を有効にします。
4. 接続を設定します。
5. Eメールメッセージをユーザーに送信します。
6. 複雑なネットワークでの接続を有効にします。

ルーターでUniversal Plug and Play検出を有効化する

モバイルデバイスをXProtect Mobileサーバーに容易に接続できるよう、ルーターでUniversal Plug and Play (UPnP) を有効にできます。UPnPにより、XProtect Mobileサーバーはポート転送を自動的に構成できます。ただし、ウェブインターフェイスを使用すると、ルーターでポート転送を手動で設定できます。ルーターによっては、ポートマッピングの設定手順が異なる場合があります。ルーターでポート転送を設定する方法が分からない場合は、デバイスのマニュアルをご参照ください。



5分ごとに、XProtectMobileServerサービスは、インターネットのユーザーがサーバーを使用できることを検証します。ステータスは、**プロパティ**ペインの左上に表示されます：

Server accessible through internet: ●。

複雑なネットワークでの接続を有効にする

カスタム設定がある複雑なネットワークの場合、ユーザーが接続に必要な情報を入力できます。

インターネットアクセスグループの**接続**タブで、以下を指定します。

- UPnPポートマッピングを使用して接続を特定の接続にリダイレクトするには、**カスタムインターネットアクセスを設定**チェックボックスを選択します。次に、**IPアドレスまたはホスト名**と、接続に使われるポートを入力します。例えば、ルーターがUPnPをサポートしない場合、またはルーターのチェーンがある場合に、この設定を行います
- IPアドレスが頻繁に変更される場合は、**チェックしてIPアドレスを動的に取得**チェックボックスを選択します

接続の設定

1. Management Clientのナビゲーションペインで、**サーバー**を展開し、**モバイルサーバー**を選択します。
2. サーバーを選択し、**接続**タブをクリックします。
3. **全般**グループのオプションを使用して、以下を指定します。
 - XProtect MobileクライアントとXProtect Web Clientユーザーが容易にXProtect Mobileサーバーに接続できるようにするには、**スマートコネクトを有効にする**チェックボックスを選択します
 - XProtect MobileクライアントおよびXProtect Web Clientが稼働中であることをモバイルサーバーに示す頻度の時間枠を設定します。
 - UPnPプロトコルを使用したネットワーク上でXProtect Mobileサーバーを検出できるようにするには、**UPnP検出を有効にする**チェックボックスを選択します
 - ルーターがその仕様で構成されている際にXProtect Mobileサーバーがポートマッピングを自ら実行できるようにするには、**自動ポートマッピングを有効にする**チェックボックスを選択します。

Eメールメッセージをユーザーに送信する

XProtect MobileクライアントとXProtect Web Clientの設定を容易にするために、Management Client内からエンドユーザーに直接Eメールを送信できます。Eメールにはサーバーを直接XProtect Mobileに追加するリンクが含まれています。これでネットワークアドレスやポートを入力する必要なしに設定が完了します。

1. **招待をEメールで送信する**フィールドに、スマートコネクト通知の受信者のEメールアドレスを入力し、言語を指定します。
2. 次に、以下のいずれか1つを実行します。
 - メッセージを送信するには、**送信**をクリックします。
 - メッセージングプログラムに情報をコピーします。

詳細については以下を参照：

[9ページのスマートコネクト設定の要件](#)

[18ページの接続タブ](#)

通知

XProtect Mobileを有効にして、アラームトリガーやデバイスまたはサーバーで問題が発生した場合など、イベントが発生したときにユーザーに通知できます。

アプリが実行されているかどうかに関わらず、通知は常に配信されます。XProtect Mobileがモバイルデバイスで開くと、通知が配信されます。システム通知は、アプリが実行されていない場合でも配信されます。ユーザーは受信する通知のタイプを指定できます。たとえば、次の状態の通知を受信することを選択できます。

- すべてのアラーム
- 割り当てられたアラームのみ
- システム関連のアラームのみ

これらは、サーバーがオフラインになったとき、またはオンラインに戻ったとき場合があります。

また、プッシュ通知を使用すると、XProtect Mobileを開いていないユーザーにも通知できます。これらはプッシュ通知といいます。プッシュ通知はモバイルデバイスに配信されます。これは、移動中のユーザーが常に最新情報を得られる優れた方法です。

デフォルトでは、通知は無効になります。

プッシュ通知の使用



プッシュ通知をしようするには、システムがインターネットにアクセスできる必要があります。

プッシュ通知はApple、Microsoft、Googleからクラウドサービスを使用します。

- Apple Push Notificationサービス (APN)
- Microsoft Azure通知ハブ
- Google Cloud Messaging Push Notificationサービス

システムが特定の期間に送信できる通知数は制限されています。この制限を超過すると、次の期間中に15分ごとに1件の通知のみを送信できます。通知には、15分間に発生したイベントの概要が含まれます。次の期間の後、制限は削除されます。

[9ページの通知設定の要件](#)と[27ページの通知タブ](#)もご参照ください。

XProtect Mobileサーバーでプッシュ通知を設定

プッシュ通知を設定するには、次の手順に従います。

1. Management Clientでモバイルサーバーを選択してから、**通知**タブをクリックします。
2. サーバーに接続するすべてのモバイルデバイスに通知を送信するには、**[通知]**チェックボックスを選択します。個人データに関する警告を読み、続行する場合は**はい**を選択します。
3. サーバーに接続するユーザーとモバイルデバイスの情報を保存するには、**[デバイス登録の管理]**チェックボックスを選択します。



サーバーはリストのモバイルデバイスにのみ通知を送信します。**[デバイス登録の管理]**チェックボックスをオフにし、変更を保存すると、リストが消去されます。もう一度プッシュ通知を受信するには、デバイスを再接続する必要があります。

特定のモバイルデバイスまたはすべてのモバイルデバイスへのプッシュ通知の送信を有効化する

XProtect Mobileを有効化するには、特定またはすべてのモバイル デバイスにプッシュ通知を送信することによってイベントが発生したときにユーザーに通知します。

1. Management Clientでモバイルサーバーを選択してから、**通知**タブをクリックします。
2. 以下のいずれか1つを実行します。
 - 個々のデバイスの場合は、**[登録済みデバイス]**テーブルにリストアップされている、各モバイルデバイスのチェックボックスの**[有効化]**を選択します
 - すべてのモバイルデバイスでは、**通知**チェックボックスを選択します。個人データに関する警告を読み、続行する場合は**はい**を選択します

特定の、またはすべてのモバイルデバイスへのプッシュ通知の送信を停止する

特定の、またはすべてのモバイルデバイスへのプッシュ通知の送信を停止するには、複数の方法があります。

1. Management Clientでモバイルサーバーを選択してから、**通知**タブをクリックします。
2. 以下のいずれか1つを実行します。
 - 個別のデバイスで、各モバイルデバイスの**[有効]**チェックボックスをオフにします。ユーザーは別のデバイスを使用して、XProtect Mobileサーバーに接続できます。
 - すべてのデバイスの**[通知]**チェックボックスをオフにします。

すべてのデバイスを一時的に停止するには、**[デバイス登録の管理]**チェックボックスをオフにし、変更を保存します。ユーザーが再接続した後に、もう一度通知が送信されます。

登録済みデバイスリストから1つあるいはすべての登録済みデバイスを削除

XProtect Mobileアプリをアンインストール、あるいはデバイスを無効にする際に、デバイスのデータがVMSデータベースに残っている場合があります。

VMSは以下の場合にデバイス登録データを削除します。

- システムからユーザーを削除している。
- Milestone Care Plusが180日以上更新されていない。

ただし、デバイス登録データが自動的に削除されない場合もあります。

以下の場合、1つあるいはすべての登録済みデバイスを手動で削除する必要があります。

- ユーザーが自分の電話を失くした。
- モバイルサーバーを完全にアンインストールし、データを削除してください。
- ユーザーがXProtect Mobile クライアントアプリまたは通知の使用を止めている。
- VMSの役割にActive Directory(AD)グループを追加して、ユーザーの権限を変更している。ADグループを追加する場合、VMSはその役割でユーザーを確認しません。ADグループからユーザーを削除したり、モバイルサーバーの使用を制限する場合は、リストからユーザーのデバイスを手動で削除する必要もあります。

登録済みデバイスを削除するには、以下のことを行います。

1. Management Clientでモバイルサーバーを選択してから、**通知**タブをクリックします。
2. 以下のいずれか1つを実行します。
 - 個々のデバイスの場合、デバイスを選択、次に**削除**を選択します。
 - すべてのデバイスの場合、**全削除**を選択します。

調査の設定

XProtect Web ClientあるいはXProtect Mobileを使用して録画ビデオへのアクセスとインシデントの調査を行い、ビデオエビデンスを準備してダウンロードできるように調査を設定します。

調査を設定するには、次の手順に従います。

1. Management Clientでは、モバイルサーバーをクリックしてから、**調査**タブをクリックします。
2. **[調査を有効にする]**チェックボックスを選択します。デフォルトでは、チェックボックスが選択されています。
3. **調査フォルダー**フィールドで、調査のビデオを保存する場所を指定します。
4. オプション：ユーザーが他のユーザーが作成する調査にアクセスできるようにするには、**他のユーザーが作成した調査を表示する**チェックボックスを選択します。このチェックボックスを選択しない場合、ユーザーは自分の調査のみを表示できます。
5. **調査フォルダーのサイズ制限を有効にする**チェックボックスを選択し、調査フォルダーに含めることのできる最大メガバイト数を設定します。
6. **調査の保存期間を有効に設定**チェックボックスを選択すると、調査の保存期間を設定できます。デフォルトで保存期間は7日間に設定されています。

7. **エクスポートフォーマット**で、使用したいエクスポートフォーマットのチェックボックスを選択してください。以下のエクスポートフォーマットを利用できます。

- **AVIフォーマット**
- **XProtectフォーマット**
- **MKVフォーマット**



デフォルトでチェックボックスは選択されていません。

8. (オプション) ビデオがダウンロードされた日時を含めるには、**AVIエクスポートのタイムスタンプを含める**チェックボックスを選択します。
9. **AVIエクスポートで使用されたコーデック**フィールドで、ダウンロード用にAVIパッケージを準備するとき使用する圧縮形式を選択します。



リストのコーデックは、オペレーティングシステムによって異なる場合があります。使用するコーデックが表示されない場合は、Management Clientが実行されているコンピュータにインストールすると、このリストに表示されます。



また、コーデックは異なる圧縮率を使用することがあり、動画品質に影響する場合があります。高圧縮率によりストレージ要件が減りますが、画質が低下する可能性があります。低圧縮率はストレージとネットワーク容量が増えますが、画質が上がります。選択する前にコーデックを調査することをお勧めします。

10. エクスポートするビデオに音声が含まれている場合は、**AVI エクスポートに使用された音声ビットレート**リストから、適切な音声ビットレートを選択します。デフォルトは160000 Hzです。



ユーザーが調査を保存できるようにするには、**エクスポート**権限をユーザーに割り当てたセキュリティ役割に付与する必要があります。

調査のクリーンアップ

保持する必要がない調査またはビデオエクスポートがある場合は、削除できます。たとえば、サーバーでより多くのディスク領域が使用できるようにする場合には、これが便利です。

- 調査と、その調査のために作成されたビデオエクスポートをすべて削除するには、リストで調査を選択してから**削除**をクリックします。
- 調査用にエクスポートされた個別のビデオファイルを削除しながらその調査を保持するには、リストで調査を選択します。**調査の詳細**グループで、エクスポート用の**XProtect**、**AVI**、または**MKV**フィールドの右側にある**削除**アイコンをクリックします。

ビデオプッシュを使用したビデオのストリーミング

ビデオプッシュを設定すると、ユーザーはモバイルデバイスのカメラからXProtect監視システムに録画をストリーミングし、常に状況に関する通知を受信するか、ビデオを録画して後から調査できます。ビデオストリームには音声もついている場合があります。

[26ページのビデオプッシュタブ](#)と[10ページのビデオプッシュ設定の要件](#)もご参照ください。

ビデオをストリーミングするためのビデオプッシュの設定

ユーザーがモバイルデバイスからXProtectシステムにビデオをストリーミングするには、XProtect Mobileサーバーでビデオプッシュを設定する必要があります。

Management Clientで、以下の手順で設定します。

1. **ビデオプッシュ**タブで、**ビデオプッシュ**チェックボックスを選択して、この機能を有効にします。
2. ビデオをストリーミングするためのビデオプッシュチャンネルを追加します。
3. ビデオプッシュドライバーをRecording Serverのハードウェアデバイスとして追加します。このドライバーはカメラデバイスをシミュレーションして、Recording Serverにビデオをストリーミングできるようにします。
4. ビデオプッシュドライバーデバイスをビデオプッシュのためのチャンネルに追加します。

ビデオをストリーミングするためのビデオプッシュチャンネルの追加

チャンネルを追加するには、以下の手順に従います。

1. ナビゲーションペインで**モバイル サーバー**を選択し、モバイルサーバーを選択します。
2. **ビデオプッシュ**タブで、**ビデオプッシュ**チェックボックスを選択します。
3. **チャンネルマッピング**の左下で**追加**をクリックし、ビデオ プッシュチャンネルを追加します。
4. 表示されたダイアログボックスで、チャンネルを使用するユーザーアカウントのユーザー名を入力します（**役割**で追加）。このユーザーアカウントによるXProtect Mobileサーバーとレコーディングサーバーへのアクセスを**セキュリティ全般**タブで許可する必要があります。



ビデオプッシュを使用するには、このアカウントのユーザー名とパスワードを使用して、モバイルデバイスでXProtect Mobileにログインする必要があります。



新しいビデオ プッシュチャンネルを追加すると、レコーディング サーバーでハードウェア デバイスとしてチャンネルを追加する際に使われるポート番号とMACアドレスが生成されます。また、Recording ServerとMobile Serverの接続で使用されるパスワードも生成されます。デフォルトのパスワードは、**Milestone**です。

5. ポート番号をメモしておきます。レコーディングサーバーにハードウェアデバイスとしてビデオプッシュドライバを追加する時に必要です。
6. **OK**をクリックして、ビデオ プッシュチャンネルダイアログを閉じます。
7. チャンネルを保存するには、ナビゲーション ペインの左上で**保存**をクリックします。

ビデオ プッシュチャンネルの編集

追加したビデオ プッシュチャンネルの設定詳細は編集できます。

1. **チャンネルマッピング**で編集するチャンネルを選択し、**編集**をクリックします。
2. 編集を終了したら、**OK**をクリックしてビデオ プッシュチャンネルダイアログボックスを閉じます。
3. 編集内容を保存するには、ナビゲーション ペインの左上で**保存**をクリックします。



ビデオ プッシュチャンネルのポート番号とMACアドレスを編集する場合は、レコーディングサーバーで以前に追加したビデオプッシュチャンネル設定の詳細も必ず新しい情報に置き換えてください。これを行わなければ、Recording ServerとMobile Serverの接続が失われます。

ビデオプッシュチャンネルの追加

不要になったチャンネルは削除できます。

1. **チャンネルマッピング**で削除するチャンネルを選択し、**削除**をクリックします。
2. 変更を保存するには、ナビゲーション ペインの左上で**保存**をクリックします。

パスワードの変更

自動的に生成され、Recording ServerとMobile Serverの接続で使用するパスワードは変更可能です。

1. **チャンネルマッピング**の右下で**パスワードの変更**をクリックします。
2. **ビデオプッシュのパスワード変更**ダイアログボックスで、最初のフィールドに新しいパスワードを入力し、2番目のフィールドにも新しいパスワードを繰り返し入植し、**OK**をクリックします。
3. 変更を保存するには、ナビゲーション ペインの左上で**保存**をクリックします。



ビデオ プッシュチャンネルのパスワードを変更すると、すでにリストに含まれているビデオプッシュチャンネル、または将来、追加されるビデオ プッシュチャンネルすべてに変更が適用されます。既存のビデオ プッシュチャンネルをすべてリストから削除する場合でも、新しいパスワードは有効なままで、将来のチャンネルに適用されます。



Recording ServerとMobile Serverの接続が失われるため、変更を保存した後、既存のビデオプッシュチャンネルはすべて機能しなくなります。この接続を回復するには、ナビゲーションペインで**レコーディングサーバー**タブを右クリックして**ハードウェア交換**ウィザードを実行し、Recording Serverでハードウェアデバイスとして追加したビデオプッシュドライバの新しいパスワードを入力します。

レコーディングサーバーにハードウェアデバイスとしてビデオプッシュドライバを追加

1. ナビゲーションペインで**レコーディングサーバー**をクリックします。
2. ビデオをストリーミングしたいサーバーを右クリックして**ハードウェアを追加**をクリックし、**ハードウェアを追加**ウィザードを開きます。
3. ハードウェア検知方法として**手動**を選択し、**次へ**をクリックします。
4. ビデオプッシュドライバのログイン資格情報を入力します。
 - ユーザー名：デフォルトのユーザー名を使用する場合は、このフィールドを空白のままにします。
 - パスワード：**Milestone**を入力します - システムによって生成されるパスワードです。モバイルサーバーでビデオプッシュチャンネルを追加した際にパスワードを変更した場合は、使用したいパスワードを入力します。**次へ**をクリックします。



これはユーザーではなく、ハードウェアの資格情報です。資格情報は、ビデオプッシュチャンネルへのアクセスで使用するユーザーアカウントには関係していません。

5. ドライバのリストで**Milestone**を展開し、**ビデオプッシュドライバ**のチェックボックスを選択してから**次へ**をクリックします。
6. **アドレス**フィールドには、XProtect MobileサーバーがインストールされているコンピュータのIPアドレスを入力します。



システムの生成したMACアドレスを使用するようお勧めします。ビデオプッシュドライバで問題が発生した場合、またはモバイルサーバーでビデオプッシュチャンネルのポート番号とMACアドレスを編集した場合などにのみ変更します。

7. **ポート**フィールドで、ビデオのストリーミングのために作成したチャンネルのポート番号を入力します。ポート番号はチャンネルを作成した時に割り当てられています。
8. **ハードウェアモデル**列で、**ビデオプッシュドライバ**を選択し、**次へ**をクリックします。
9. システムが新しいハードウェアを検知したら、**次へ**をクリックします。

10. **ハードウェア名テンプレート**フィールドで、ハードウェアのモデルとそのIPアドレスを表示するか、モデルのみを表示するかを指定します。
11. 関連デバイスを有効にするかどうかは、**有効にする**チェックボックスを選択して指定します。有効にしない場合でも、**ビデオプッシュドライバー**のリストに関連デバイスを追加できます。後で有効にすることもできます。



ビデオをストリーミングする際にロケーション情報を使用したい場合は、**メタデータ**ポートを有効にする必要があります。



ビデオをストリーミングする際に音声を再生したい場合は、ビデオストリーミングに使うカメラに関連付けられているマイクを有効にする必要があります。

12. 左側で該当するデバイスのデフォルトのグループを選択するか、**グループに追加**フィールドで特定のグループを選択します。1つのグループにデバイスを追加すると、同時にすべてのデバイスに設定を適用したり、デバイスの入れ替えをすることが容易にできます。

ビデオプッシュドライバーデバイスをビデオプッシュのためのチャンネルに追加

ビデオプッシュドライバーデバイスをビデオプッシュのためのチャンネルに追加するには、以下の手順に従います。

1. **サイトナビゲーション**ペインで、**モバイルサーバー**をクリックし、**ビデオプッシュ**タブをクリックします。
2. **カメラを検索**をクリックします。成功すると、**カメラ名**フィールドに、ビデオプッシュドライバー カメラの名前が表示されます。
3. 設定を保存します。

既存のビデオプッシュチャンネルで音声を有効にする

ビデオプッシュで音声を有効にするための要件を満たした後（[10ページのビデオプッシュ設定の要件](#)を参照）、Management Clientで以下を実行します。

1. **サイトナビゲーション**ペインで**サーバーノード**を展開し、**レコーディングサーバー**をクリックします。
2. 概要ペインで該当するレコーディングサーバーのフォルダーを選択し、**ビデオプッシュドライバー**フォルダーを展開して、ビデオプッシュに関連するマイクを右クリックします。
3. **有効にする**を選択してマイクを有効にします。
4. 同じフォルダー内で、ビデオプッシュに関連するカメラを選択します。
5. **プロパティ**ペインで、**クライアント**タブをクリックします。
詳細については、[クライアントタブ（デバイス）](#)を参照してください。

6. **関連マイク**フィールドの右側にある  をクリックします。**選択したデバイス**ダイアログボックスが開きます。
7. **レコーディングサーバー**タブで、レコーディングサーバーフォルダーを展開し、ビデオプッシュに関連するマイクを選択します。
8. **[OK]** をクリックします。

電子メールを使用して2要素認証のユーザーを設定する



使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (<https://www.milestonesys.com/products/software/product-index/>) の製品概要ページにあります。

XProtect MobileクライアントまたはXProtect Web Clientのユーザーに追加のログイン手順を課すには、XProtect Mobileサーバー上で2要素認証の設定を行います。標準のユーザー名とパスワードに加えて、ユーザーは電子メールで送信される認証コードを入力する必要があります。

2要素認証により監視システムの保護レベルが高まります。

Management Clientで以下の手順に従ってください。

1. [46ページ](#)のSMTPサーバーに関する情報を入力します。。
2. [46ページ](#)のユーザーに送信される認証コードを指定します。。
3. [47ページ](#)のユーザーとActive Directoryグループへの認証方法の割り当て。

[10ページ](#)のユーザーの2要素認証設定の要件と[28ページ](#)の要素認証タブもご参照ください。

SMTPサーバーに関する情報を入力します。

プロバイダーはSMTPサーバーに関する情報を使用します。

1. ナビゲーションペインで**モバイルサーバー**を選択し、該当するモバイルサーバーを選択します。
2. **2要素認証**タブで、**2要素認証を有効にする** チェックボックスを選択します。
3. **プロバイダー設定**の下で**電子メール**タブで、SMTPサーバーに関連する情報を入力し、ログイン時 および2次ログインで設定する電子メールアドレスを指定します。

詳細については、[28ページ](#)の**要素認証タブ**をご参照ください。

ユーザーに送信される認証コードを指定します。

認証コードの複雑度を指定するには、以下を実行します。

1. **認証コード設定** セクションの**2要素認証**タブで、XProtect Mobileクライアントユーザーが、ネットワーク切断の際などに再確認する必要なくログインできる期間を指定します。デフォルトの期間は3分間です。
2. ユーザーが受け取った認証コードを使用できる期間を指定します。この期間終了後はコードが無効となるため、ユーザーは新しいコードを要求する必要があります。デフォルトの期間は5分間です。
3. 提供されたコードが無効になるまでの、コード入力試行最大回数を指定します。デフォルトの回数は3回です。
4. コードの文字数を指定します。デフォルトの長さは6文字です。
5. システムが生成するコードの複雑度を指定します。

詳細については、[28ページの要素認証タブ](#)をご参照ください。

ユーザーとActive Directoryグループへの認証方法の割り当て

ユーザー設定セクションの**2要素認証**タブに、XProtectシステムに追加されたユーザーとグループのリストが表示されます。

1. **認証方法**列で、各ユーザーまたはグループの認証方法を選択します。
2. **ユーザー詳細**フィールドで、各ユーザーの電子メールアドレスなど、コード送信に関する詳細を追加します。次回、ユーザーがXProtect Web ClientまたはXProtect Mobileアプリにログインすると、セカンダリログインが求められます。
3. グループがActive Directoryで構成されている場合、XProtect MobileサーバーはActive Directoryからの電子メールアドレスなどの詳細情報を使用します。



Windowsグループは2要素認証をサポートしていません。

4. 設定を保存します。

電子メールによる2要素認証のユーザー設定手順が完了しました。

詳細については、[28ページの要素認証タブ](#)をご参照ください。

アクション

XProtect MobileクライアントまたはXProtect Web Clientの**アクション**タブの有効性は、**一般**タブでアクションを有効化、または無効化することで管理できます。**アクション**はデフォルトで有効であり、接続されたデバイスのすべての使用可能なアクションがここに表示されます。

詳細については、[15ページの一般タブ](#)をご参照ください。

モバイルデバイスの管理 (MDM)

モバイルデバイス管理 (MDM) は、携帯電話事業者、サービスプロバイダー、企業などに導入されているモバイルデバイスを保護、監視、管理、サポートするソフトウェアです。

一般にMDMソリューションは、モバイルデバイスに管理コマンドを送信するサーバーコンポーネントと、管理対象デバイス上で動作し、管理コマンドを受信して実行されるクライアントコンポーネントから構成されます。

組織内のデバイスにXProtect Mobileクライアントを分散し、カスタムポリシーを追加することができます。



モバイルデバイスでMDM機能を利用するには、MDMソフトウェアプラットフォームでモバイルサーバーの設定を行う必要があります。モバイルサーバーの詳細情報は、サーバー名、サーバーアドレス、サーバーのポート、接続タイププロトコルなどです。



追加済みのモバイルサーバーの詳細を更新済みの場合は、オペレータはそのサーバーを**サーバー**リストから手動で削除し、XProtect Mobileアプリを再起動する必要があります。

モバイルデバイスの管理プラットフォームでモバイルサーバーの詳細を設定する（システム管理者）

XProtect Mobileクライアントをモバイルデバイスの管理プラットフォームからモバイルデバイスに配布・管理するためには、サーバーの詳細を追加する必要があります。設定の詳細については、モバイルデバイスの管理ソフトのマニュアルをご参照ください。



必須サーバーの詳細が入力されていない場合、または誤った情報を入力した場合、モバイルサーバーはXProtect Mobileアプリに追加されません。

Androidユーザーの場合

サーバーの詳細は、モバイルデバイスの管理プラットフォームのユーザーインターフェイスで指定できます。サーバーの詳細情報を含む管理対象の設定ファイルをアップロードするオプションがあります。

サーバー詳細：

- **サーバー名** - （必須）サーバー名を入力します
- **サーバーアドレス** - （必須）サーバーアドレスを入力します
- **サーバーポート** - （必須）サーバーポート番号を入力します
- **接続プロトコルのタイプ** - HTTPS接続を使用する際に有効にします。HTTP接続の場合は無効にします。デフォルトで、HTTPS接続は有効になっています

モバイルデバイスの管理プラットフォームにファイルをアップロードするには、以下の手順を行います。

1. 本マニュアル巻末の付録Aにある、Androidデバイス向けの管理対象の設定テンプレートを見つけます。内容をコピーします。
2. テキストエディタを開き、内容を貼り付けます。

3. **android:description**フィールドのサーバー詳細を指定します。
4. .XMLファイルとして保存します。
5. モバイルデバイスの管理プラットフォームを開き、管理対象の設定ファイルをアップロードします。

iOSユーザーの場合

モバイルデバイスの管理プラットフォームからiOSデバイスを管理するには、管理対象の設定ファイルに接続の詳細を指定する必要があります。

1. 本マニュアル巻末の付録Bにある、iOSデバイス向けの管理対象の設定テンプレートを見つけます。内容をコピーします。
2. テキストエディタを開き、内容を貼り付けます。
3. 以下のようにサーバーの詳細を指定します。
 - **versionConfig** - (必須) アプリ設定**1.0.0**のデフォルトバージョンを入力します
 - **serverNameConfig** - (必須) サーバー名を入力します
 - **serverAddressConfig** - (必須) サーバーアドレスを入力します
 - **serverPortConfig** - (必須) サーバーポート番号を入力します
 - **serverConnectionProtocolTypeConfig** - デフォルトの接続タイプは**HTTPS**で、保護されていない接続を使用する場合は**HTTP**を入力します
4. .XMLファイルとして保存します。
5. モバイルデバイスの管理プラットフォームを開き、管理対象の設定ファイルをアップロードします。

XProtect MobileクライアントおよびXProtect Web Clientで使用する出力に名前を付ける

現行のカメラでアクションを正しく表示するには、出力グループにカメラと同じ名前を付ける必要があります。

例：

「AXIS P3301 - 10.100.50.110 - Camera 1」という名前のカメラに接続されている出力を使って出力グループを作成する場合、**名前**フィールド（**デバイスグループ情報**の下）で同じ名前を入力する必要があります。

説明フィールドで、「AXIS P3301 - 10.100.50.110 - Camera 1 - Light switch」のように詳細な説明を追加できます。



これらの命名規則に従わない場合、アクションは関連付けられたカメラのビューのアクションリストで使用できません。代わりに、アクションは**アクションタブ**の他のアクションのリストに表示されます。

詳細については、[出力](#)を参照してください。

外部IDPとXProtect Mobile

IDPはIdentity Providerの頭字語です。外部IDPは、ユーザーID情報を保存および管理し、他のシステムにユーザー認証サービスを提供できる外部アプリケーションおよびサービスです。外部IDPはXProtectVMSに関連付けることができます。

XProtect Web Client 2022 R3以降では、外部IDPを使用してXProtect MobileまたはXProtectクライアントにログインできます。



XProtect Web ClientおよびXProtect Mobileのクライアントに外部IDPでログインするには、HTTPS接続を使用する必要があります。

XProtectWebClientおよびXProtectMobileのクライアントの外部IDPログインを設定する前に、以下を確認してください。

- 外部IDPが設定されている
- クレームが登録されている
- クレームが役割へマッピングされている

詳細については、[XProtectVMS管理者マニュアル](#)を参照してください。

外部IDP経由でXProtect Web Clientにログインするには、追加の設定が必要です。[50ページのXProtect Web Clientの外部IDPログインを設定する](#)をご参照ください。

XProtect Web Clientの外部IDPログインを設定する

XProtect Web Clientに外部IDP経由でログインするオプションは、HTTPS接続時のみ利用可能です。

1. Management Clientで、**ツール>オプション**を選択し、**外部IDP**タブを開きます。
2. **ウェブクライアントのリダイレクトURI**セクションで**追加**を選択します。
3. XProtect Web Clientのアドレスを**https://[address]:[port number]/index.html**の形式で入力します。
 - アドレスには、モバイルサーバーが動作しているコンピュータのホスト名またはIPアドレスを入力します
 - ポート番号には、XProtect Web Clientがモバイルサーバーと通信するために使用するポートを入力します。HTTPS接続の場合、デフォルトのポート番号は8082です

緊急アラートアラームの追加

潜在的な危険が検知された場合、緊急アラートによりXProtect Mobileクライアントのユーザーは最重要レベルのアラーム通知の受信や、アラーム詳細が表示でき、迅速な対応が可能になります。緊急アラートは、XProtect Management Clientで定義するタイプのアラームです。



この機能が動作するには、プッシュ通知が必要です。プッシュ通知は、Milestone Care Plus ライセンスを購入した場合にのみ利用できます。



この機能は、特定のXProtect VMS 製品でのみ使用できます。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (<https://www.milestonesys.com/products/software/product-index/>) の製品概要ページにあります。

このアラームを追加するには、以下を行う必要があります。

1. **アラーム>アラームデータ設定**で、レベル99の新しいアラームカテゴリを追加します。レベル99のカテゴリは、必要なだけ作成することができます。
2. このカテゴリでアラーム定義を追加します。

メンテナンス

Mobile Server Manager

MobileServerManagerは、モバイルサーバーに接続されるトレイコントロール機能です。通知エリアでMobile ServerManagerトレイアイコンを右クリックすると、モバイルサーバーに簡単にアクセスできるメニューが開きます。

次の操作に従ってください。

- [52ページのXProtect Web Clientへのアクセス](#)
- [53ページのMobile Serverサービスの起動、停止、再起動](#)
- [53ページのデータ保護パスワードの変更](#)
- [54ページのポート番号の表示/編集](#)
- [34ページのモバイルサーバーで暗号化を有効にする（Server Configuratorを使用）](#)
- 今日ログファイルを開く（[54ページのログへのアクセスおよび調査](#)を参照）
- ログフォルダーを開く（[54ページのログへのアクセスおよび調査](#)を参照）
- 調査フォルダーを開く（[54ページのログへのアクセスおよび調査](#)を参照）
- [55ページの調査フォルダーの変更](#)
- XProtect Mobile Serverのステータスを参照（[55ページのステータスを表示](#)を参照）

XProtect Web Clientへのアクセス

XProtect Mobileサーバーがコンピュータにインストールされている場合は、XProtect Web Clientを使用してカメラとビューにアクセスできます。XProtect Web Clientをインストールする必要はないため、XProtect Mobileサーバーをインストールしたコンピュータまたはこの目的で使用する他のすべてのコンピュータからアクセスできます。

1. XProtect MobileでManagement Clientサーバーを設定します。
2. XProtect Mobileサーバーがインストールされているコンピュータを使用している場合は、通知エリアのMobile Server Managerトレイアイコンを右クリックして**XProtect Web Clientを開く**を選択します。
3. XProtect Mobileサーバーがインストールされているコンピュータを使用しない場合は、ブラウザからアクセスできます。このプロセスで手順4を続行します。
4. インターネットブラウザ(Microsoft Edge、Mozilla Firefox、Google Chrome、またはSafari)を開きます。

5. 外部IPアドレスを入力します。これは、XProtect Mobileサーバーが実行されているサーバーの外部アドレスとポート番号です。

例：XProtect MobileサーバーがIPアドレス127.2.3.4のサーバーにインストールされ、ポート8081でHTTP接続を許可し、ポート8082でHTTPS接続を許可するように設定されます（インストーラのデフォルト設定）。

標準HTTP接続をご希望の場合は、お使いのブラウザのアドレスバーに**http://127.2.3.4:8081**と入力します。安全に確立されたHTTPS接続を**https://127.2.3.4:8082**使用するにはと入力してください。これで、XProtect Web Clientを使用できます。

6. 今後、XProtect Web Clientに簡単にアクセスできるように、アドレスをブラウザのブックマークに追加します。XProtect Web ClientサーバーをインストールしたローカルコンピュータでXProtect Mobileを使用する場合は、インストーラで作成されたデスクトップショートカットも使用できます。ショートカットをクリックしてデフォルトのブラウザを起動し、XProtect Web Clientを開きます。



XProtect Web Clientの新しいバージョンを使用するには、XProtect Web Clientを実行しているインターネットブラウザのキャッシュをクリアする必要があります。システム管理者は、アップグレードの際にXProtect Web Clientユーザーにブラウザのキャッシュのクリアを依頼するか、このアクションをリモートで強制的に実行する必要があります（このアクションを実行できるのは、ドメイン内のInternet Explorerだけです）。

Mobile Serverサービスの起動、停止、再起動

必要に応じてMobile ServerサービスをMobile Server Managerから起動、停止、再起動できます。

- これらのタスクのいずれかを実行するには、MobileServerManagerアイコンを右クリックし、**MobileServerサービスの起動**、**MobileServerサービスの停止**、または**MobileServerサービスの再起動**を選択します

データ保護パスワードの変更

モバイルサーバーのデータ保護パスワードは、調査を暗号化するために使われます。システムを復元する場合や、追加のモバイルサーバーを使用してシステムを拡張する場合、モバイルサーバーのデータにアクセスするため、システム管理者はこのパスワードを入力する必要があります。

モバイルサーバーのデータ保護パスワードを変更するには、以下を実行します。

1. Mobile Server Managerアイコンを右クリックして、**データ保護パスワードの設定を変更**を選択します。ダイアログボックスが表示されます。
2. **新しいパスワード**フィールドに新しいパスワードを入力します。
3. **新しいパスワードを再入力**フィールドに新しいパスワードを再入力します。
4. （オプション）調査をパスワードで保護したくない場合は、**モバイルサーバーのデータ保護パスワードを使用しないことを選択し、調査が暗号化されないことを理解しました**を選択します。
5. [OK] をクリックします。



このパスワードを保存し、安全に保管してください。この指示に従わない場合、モバイルサーバーのデータを復元する機能が損なわれる可能性があります。

ポート番号の表示/編集

1. Mobile Server Managerアイコンを右クリックして、**ポート番号の表示/編集**を選択します。
2. ポート番号を編集するには、関連するポート番号を入力します。標準ポート番号(HTTP接続用)および/または安全なポート番号(HTTPS接続用)を指定できます。
3. [OK] をクリックします。

ログへのアクセスおよび調査

Mobile Server Managerにより、その日のログファイルにアクセスし、ログファイルが保存されているフォルダーを開き、調査が保存されているフォルダーを開くことができます。

そのいずれかを開くには、Mobile Server Managerアイコンを右クリックし、以下から選択します。

- **今日のログファイルを開く**
- **ログフォルダーを開く**
- **調査フォルダーを開く**

Management ServerまたはRecording Serverによって記録されていないアクションすべてに対して監査ログが作成されます。

以下のアクションは常に記録されます（拡張監査ログが有効になっていない場合も同様です）。

- すべての管理作業（この監査ログメッセージには以前の値と新しい値が含まれます）
- 調査の作成、編集または削除に関するすべてのアクション、エクスポートされた資料の準備とダウンロード、関連する設定の変更。監査ログには、操作に関する詳細が含まれます。



ビデオプッシュストリーミングは、拡張監査ログが有効になっている場合にのみ記録されます。



システムからXProtect Mobileをアンインストールしても、ログファイルは削除されません。適切なユーザー権限のあるシステム管理者は、後でログファイルにアクセスしたり、不要になれば削除したりできます。ログファイルのデフォルトの場所は、**ProgramData**フォルダーです。ログファイルのデフォルトの場所を変更しても、既存のログは新しい場所へコピーされず、削除もされません。

調査フォルダーの変更

デフォルトでは、調査の場所は、**ProgramData**フォルダーです。調査フォルダーのデフォルトの場所を変更しても、既存の調査は新しい場所に自動的にコピーされず、削除されることもありません。ハードディスク上で調査エクスポートを保存場所を変更するには、以下を実行します。

1. Mobile Server Managerアイコンを右クリックし、**調査フォルダーを変更**をクリックします。

調査ロケーションウィンドウが開きます。

2. 既存のフォルダーを参照する、または新規フォルダーを作成するには、現在の場所が表示されている**フォルダー**フィールドの横でフォルダーアイコンをクリックし、**OK**をクリックします。
3. **以前の調査**リストから、現在の場所に保存されている既存の調査に適用したいアクションを選択します。オプションは以下のとおりです。

- **移動**：既存の調査を新規フォルダーに移動します



既存の調査を新規フォルダーに移動しない場合、閲覧できなくなります。

- **削除**：既存の調査を削除します
- **何もしない**：既存の調査は現在のフォルダーの場所に残ります。調査フォルダーのデフォルトの場所を変更した後は、それらは表示されなくなります。

4. **適用**をクリックし、>**OK**をクリックします。

ステータスを表示

Mobile Server Managerアイコンを右クリックし、**ステータスの表示**を選択するか、Mobile Server Managerアイコンをダブルクリックしてウィンドウを開き、XProtect Mobileサーバーのステータスを確認します。以下の情報を表示できます。

名前	説明
サーバー実行日	XProtect Mobileサーバーが前回起動されたときの日付と時刻。
接続済みユーザー	現在XProtect Mobileサーバーに接続されているユーザーの数。
ハードウェアのデコード	XProtect Mobileサーバーでハードウェアアクセラレーションによるデコードが実行中かどうかを示します。

名前	説明
CPU使用率	現在XProtect Mobileサーバーが使用しているCPUの%。
CPU使用履歴	XProtect MobileサーバーによるCPU使用の履歴を詳しく示すグラフ。

トラブルシューティング

XProtect Mobileトラブルシューティング

接続

なぜXProtect Mobileクライアントから自分の録画/XProtect Mobileサーバーに接続できないのでしょうか？

録画コンテンツに接続するには、XProtect Mobileシステムを実行するサーバー、または専用サーバーにXProtectサーバーがインストールされていなければなりません。また、XProtect Mobileビデオ管理設定において、関連するXProtect設定も必要となります。これらはプラグインとして、または製品インストールやアップグレードの一環としてインストールされます。XProtect Mobileサーバーを取得する方法、およびXProtect Mobileクライアント関連の設定をXProtectシステムに統合する方法の詳細については、設定セクション（[14ページのモバイルサーバーの設定](#)）をご参照ください。

サーバーアドレスフィールドには、iOSデバイスに適用される有効なホスト名が含まれていなければなりません。有効なホスト名には、ASCII文字「a」～「z」（大文字と小文字は区別されません）、数字「0」～「9」、ドット、ハイフン（「-」）を含めることができます。

ファイアウォールをオンにしましたが、モバイルデバイスをサーバーに接続できません。なぜですか？

XProtect Mobileサーバーのインストール時にファイアウォールをオフにしていた場合は、TCPとUDP通信を手動で有効にする必要があります。

HTTPS接続を介してXProtectWebClientを実行する際に、セキュリティ警告を避けるにはどうすればよいのでしょうか？

警告は、証明書のサーバーアドレス情報が誤っていることが原因で発せられます。接続は暗号化されたままとなります。

XProtect Mobileサーバー内の自己署名証明書を、XProtect Mobileサーバーとの接続に使用するサーバーアドレスと一致している独自の証明書に置き換える必要があります。これらの証明書は、ベリサインなどの公式の証明書署名機関を介して取得します。詳細については、該当する署名機関にお問い合わせください。

XProtect MobileサーバーではMicrosoft IISは使用されません。つまり、署名機関によるIISを用いた証明書署名要求（CSR）ファイルの生成に関する説明は、XProtect Mobileサーバーには適用されません。CSRファイルは、コマンドライン証明書ツール、または類似したサードパーティーの他のアプリケーションを使用して手動で作成する必要があります。このプロセスは、システム管理者および上級ユーザー以外は実行しないでください。

画質

XProtect Mobileクライアントでビデオを閲覧する際に、画質が良くないのはなぜでしょうか？

XProtect Mobileサーバーには、サーバーとクライアント間で利用できる帯域幅に応じて、自動的に画質を調整する機能があります。XProtect® Smart Clientよりも画質が悪い場合は、帯域幅が小さすぎるためにXProtect Mobileクライアントでフル解像度の画像を表示できないという状況が考えられます。その原因として、サーバーからの上流帯域幅が小さすぎるか、またはクライアントの下流帯域幅が小さすぎる可能性があります。詳細については、[XProtect Smart Clientユーザーマニュアル](#)を参照してください。

ワイヤレス帯域幅が混在しているエリアでは、帯域幅の良いエリアに入った時点で画質が改善することに気付くかもしれません。

オフィスのWiFiを介して自宅からXProtect監視カメラ管理システムに接続すると、画質が悪くなるのはなぜでしょうか？

ご自宅のインターネットの帯域幅を調べてください。多くの家庭用インターネット接続では、ダウンロード/アップロード帯域幅が異なります（通常は20Mbit/2Mbitなど）。これは、ホームユーザーは大量のデータをダウンロードすることはあっても、インターネットにアップロードすることはほとんどないためです。XProtect監視カメラ管理システムではビデオをXProtectMobileクライアントに送信する必要があり、そのプロセスは接続のアップロード速度に大きく依存します。XProtectMobileクライアントのネットワークのダウンロード速度は良好でも、複数の場所で常に画質が低い場合は、自宅のインターネット接続のアップロード速度を高めると問題が解決する可能性があります。

ハードウェアアクセラレーションによるデコーディング

私のプロセッサは、ハードウェアアクセラレーションによるデコーディングに対応していますか？

Intelから販売されている比較的新しいプロセッサのみが、ハードウェアアクセラレーションによるデコーディングに対応しています。あなたのプロセッサが対応しているかどうかは、Intelのウェブサイト

(https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&0_QuickSyncVideo=True) をご参照ください。

メニューで**テクノロジー>Intel Quick Sync Video**が**はい**に設定されていることを確認してください。

プロセッサが対応している場合、ハードウェアアクセラレーションによるデコーディングはデフォルトで有効になります。現在のステータスは、Mobile Server Managerの**ステータスを表示**で確認できます（[55ページのステータスを表示](#)を参照）。

私のオペレーティングシステムは、ハードウェアアクセラレーションによるデコーディングに対応していますか？

XProtectがサポートしているオペレーティングシステムは、いずれもハードウェアアクセラレーションに対応しています。

必ず最新のグラフィックドライバーをシステムにインストールしてください。このドライバーは、Windowsアップデートでは入手できません。

どうすればモバイルサーバーでハードウェアアクセラレーションによるデコーディングを無効にできますか？（上級）

- モバイルサーバーのプロセッサがハードウェアアクセラレーションによるデコーディングに対応している場合、これはデフォルトで有効になります。ハードウェアアクセラレーションによるデコーディングをオフにするには、以下の手順に従います。
 - ファイル VideoOS.MobileServer.Service.exe.configを検索します。パスは通常、以下のようになっています。C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config。
 - このファイルをメモ帳などのテキストエディターで開きます。必要に応じて、.configファイルタイプをメモ帳に関連付けます。

3. `<add key="HardwareDecodingMode" value="Auto" />`フィールドを探します。
4. 「Auto」値を「Off」に置き換えます。
5. ファイルを保存して閉じます。

通知

通知設定を変更していないのに、登録したデバイスが通知を受け取らなくなりました。なぜですか？

ライセンスを更新した場合、またはMilestone Careサブスクリプションを更新した場合は、Mobile Serverサービスを再起動する必要があります。

付録

付録A

Android向けのマネージド設定テンプレート

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

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

```
<restriction
```

```
    android:defaultValue="1.0.0"
```

```
    android:description="The current version of the app configuration"
```

```
    android:key="version_config"
```

```
    android:restrictionType="hidden"
```

```
    android:title="Version" />
```

```
<restriction
```

```
android:description="(Mandatory) Enter the server name."
```

```
android:key="server_name_config"
```

```
android:restrictionType="string"
```

```
android:title="Server name" />
```

```
<restriction
```

```
android:description="(Mandatory) Enter the server address."
```

```
android:key="server_address_config"
```

```
android:restrictionType="string"
```

```
android:title="Server address" />
```

```
<restriction
```

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

```
android:key="server_port_config"
```

```
android:restrictionType="integer"
```

```
android:title="Server port" />
```

```
<restriction
```

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

```
    android:key="server_secure_connection_config"
```

```
    android:restrictionType="bool"
```

```
    android:title="Connection protocol type"
```

```
    android:defaultValue="true" />
```

```
</restrictions>
```

付録B

iOSのマネージド型設定テンプレート

```
<managedAppConfiguration>
```

```
<version>1</version>
```

```
<bundleId>com.milestonesys.XProtect</bundleId>
```

```
<dict>
```

```
<string keyName="versionConfig">
```

```
<defaultValue>
```

```
<value>1.0.0</value>
```

```
</defaultValue>
```

```
</string>
```

```
<string keyName="serverNameConfig">
```

```
</string>
```

```
<string keyName="serverAddressConfig">
```

```
</string>
```

```
<string keyName="serverPortConfig">
```

```
</string>
```

```
<string keyName="serverConnectionProtocolTypeConfig">
```

```
<defaultValue>
```

```
<value>HTTPS</value>
```

```
</defaultValue>
```

```
</string>
```

```
</dict>
```

```
<presentation defaultLocale="en-US">
```

```
<field keyName="versionConfig" type="input">
```

```
<label>
```

```
<language value="en-US">Version</language>
```

```
</label>
```

```
<description>
```



```

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

```

```

    </description>

```

```

</field>

```

```

<fieldGroup>

```

```

    <name>

```

```

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

```

```

    </name>

```

```

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

```

```

    <label>

```

```

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

```

```

    </label>

```

```

    <description>

```

```

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

```

```
</description>
```

```
</field>
```

```
<field keyName="serverAddressConfig" type="input">
```

```
<label>
```

```
<language value="en-US">Server address</language>
```

```
</label>
```

```
<description>
```

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

```
</description>
```

```
</field>
```

```
<field keyName="serverPortConfig" type="input">
```

```
<label>
```

```
<language value="en-US">Server port</language>
```

```
</label>
```

```
<description>
```

```

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

```

```
</description>
```

```
</field>
```

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

```
<label>
```

```

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

```

```
</label>
```

```
<description>
```

```

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

```

```
</description>
```

```
</field>
```

```
</fieldGroup>
```

```
</presentation>
```

```
</managedAppConfiguration>
```



helpfeedback@milestone.dk

Milestone について

Milestone Systems はオープンプラットフォームのビデオ管理ソフトウェア（VMS）の世界有数のプロバイダーです。お客様の安全の確保、資産の保護を通してビジネス効率の向上に役立つテクノロジーを提供しています。Milestone Systems は、世界の 15 万以上のサイトで実証された高い信頼性と拡張性を持つソリューションにより、ネットワークビデオ技術の開発と利用におけるコラボレーションとイノベーションを促進するオープンプラットフォームコミュニティを形成しています。Milestone Systems は、1998 年創業、Canon Group 傘下の独立企業です。詳しくは、<https://www.milestonesys.com/>をご覧ください。

