

MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile Server 2020 R2

システム管理者 マニュアル



目次

Copyright、商標、および免責条項	5
概要	6
XProtect Mobile(説明付き)	6
XProtect Mobile サーバー(説明付き)	6
製品比較チャート	7
要件と注意事項	10
XProtect Mobileを使用するための要件	10
XProtect Mobile システム要件	10
通知設定の要件	10
スマートコネクト設定の要件	11
ユーザーの2要素認証設定の要件	11
ビデオプッシュ設定の要件	11
クライアントに対するモバイルサーバー暗号化の条件	11
ダイレクトストリーミングの要件	11
インストール	13
XProtect Mobileサーバーをインストール	13
設定	15
Mobileサーバーの設定	15
一般タブ	15
接続タブ	17
[サーバーステータス]タブ	19
パフォーマンスタブ	20
調査	23
ビデオプッシュタブ	24
通知タブ	25
要素認証タブ	26
ダイレクトストリーミング(説明付き)	29
アダプティブストリーミング(説明付き)	29

さらに情報が必要な時は 安全なコミュニケーション(説明付き)を参照。	30
サーバーの暗号化を管理(説明付き)	31
マネジメントサーバーからレコーディングサーバーへの通信を暗号化(説明付き)	32
マネジメントサーバーとData Collector Server間の暗号化(説明付き)	33
レコーディングサーバーからデータを取得しているクライアントとサーバーを暗号化(説明付き)	35
レコーディングサーバーデータ暗号化(説明付き)	36
クライアントに対するモバイルサーバー暗号化の条件	37
暗号化を有効化 (in English)	38
Enable encryption to and from the management server	38
Enable server encryption for recording servers or remote servers	39
Enable encryption to clients and servers	40
モバイルサーバー上で暗号化を有効化する	42
証明書の編集	42
Milestone Federated Architecture およびマスター/スレーブサーバー(説明付き)	43
スマートコネクト(説明付き)	43
Smart Connectの設定	43
ルーターでのUniversal Plug and Playの検出可能性を有効化	44
複雑なネットワークでの接続を有効にする	44
接続設定の構成	45
電子メールメッセージをユーザーに送信する	45
通知の送信(説明付き)	45
XProtect Mobileサーバーでプッシュ通知を設定	46
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	47
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	47
調査の設定	47
ビデオプッシュを使用したビデオのストリーミング(説明付き)	48
ビデオを流すための「ビデオ・プッシュ」の設定	49
ビデオプッシュ・チャンネルをストリーミングビデオに追加	49
ビデオプッシュチャンネルの追加	49
ビデオプッシュドライバーをハードウェアデバイスとしてに追加するRecording Server	49

ビデオオブッシュドライバデバイスをビデオオブッシュのためのチャンネルに追加します。	51
既存のビデオオブッシュチャンネルに対し音声の有効化する	51
ユーザーの電子メールによる2要素認証の設定を行います。	51
SMTPサーバーに関する情報を入力します。	52
ユーザーに送られてくる認証コードを指定します。	52
ユーザーとActive Directoryグループにログイン方法を割り当てます。	52
アクション(説明付き)	53
XProtect MobileクライアントおよびXProtect Web Clientで使用する出力の名前を決める(説明付き)	53
メンテナンス	54
Mobile Server Manager(説明付き)	54
XProtect Web Clientへのアクセス	54
Mobile Serverサービスの起動、停止、再起動	55
マネジメントサーバーのアドレスの入力/編集	55
ポート番号の表示/編集	55
証明書の編集	56
ログへのアクセスおよび調査(説明付き)	56
調査フォルダーを変更	56
ステータスの表示(説明付き)	57
トラブルシューティング	58
トラブルシューティングXProtect Mobile	58

Copyright、商標、および免責条項

Copyright © 2020 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

この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危険の責任はすべてその使用者にあるものとします。また、ここに記載されている内容はいずれも、いかなる事項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、特定の契約条件が適用される可能性があるサードパーティ製ソフトウェアを使用することがあります。その場合、詳細はお使いの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を参照してください。

概要

XProtect Mobile (説明付き)

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。XProtect Mobile任意の数のクライアントのインストールを使用できます。

詳細については、Milestone Systems Webサイト(<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>)からXProtect Mobileクライアントユーザーガイドをダウンロードしてください。

- XProtect Web Client

XProtect Web Client では、お使いのWebブラウザでライブビデオの閲覧ができ、また録画のダウンロードが可能です。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。

詳細については、XProtect Web Client Webサイト(<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>)からMilestone Systemsユーザーガイドをダウンロードしてください。

- XProtect Mobile サーバー
- XProtect Mobile プラグイン
- Mobile Server Manager

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

XProtect Mobile サーバー(説明付き)

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サーバーは、レコーディングサーバーへのアクセスに使用したい、すべてのサーバーにインストールする必要があります。XProtect Mobileサーバーをインストールする際には、管理者権限を持つアカウントを使用してログインします。それ以外の場合だと、インストールが正常に完了しません(「XProtect Mobileサーバーをインストールページ13をインストールする」を参照)。

XProtect Mobileサーバーは、ライブモードでのダイレクトストリーミングとアダプティブストリーミングに対応しています(XProtect ExpertおよびXProtect Corporateのみ)。

製品比較チャート

XProtect VMSには以下の製品が含まれます:

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

完全な機能リストは、Milestone Webサイト(<https://www.milestonesys.com/solutions/platform/product-index/>)の製品概要ページでご確認ください。

下記は各製品の主な違いのリストです。

名前	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
SLC(ソフトウェアライセンスコード)別の施設	1	1	[複数サイト]	[複数サイト]	[複数サイト]
SLCあたりのレコーディングサーバー	1	1	無制限	無制限	無制限
レコーディングサーバーあたりのハードウェアデバイス	8	48	無制限	無制限	無制限
Milestone Interconnect™	-	リモートサイト	リモートサイト	リモートサイト	中央/リモートサイト
Milestone Federated Architecture™	-	-	-	リモートサイト	中央/リモートサイト
フェールオーバーレコーディングサーバー	-	-	-	コールドスタンバイとホットスタンバイ	コールドスタンバイとホットスタンバイ
リモート接続サービス	-	-	-	-	✓

名前	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
エッジストレージサポート	-	-	✓	✓	✓
マルチステージビデオストレージ	ライブデータベース+ 1アーカイブ	ライブデータベース+ 1アーカイブ	ライブデータベース+ 1アーカイブ	ライブデータベース+ 無制限のアーカイブ	ライブデータベース+ 無制限のアーカイブ
SNMPトラップ(通知)	-	-	-	✓	✓
時間制限のあるユーザーアクセス権	-	-	-	-	✓
フレームレートの低減(調整)	-	-	-	✓	✓
ビデオデータ暗号化(レコーディングサーバー)	-	-	-	✓	✓
データベース署名(レコーディングサーバー)	-	-	-	✓	✓
PTZ優先レベル	1	1	3	32000	32000
拡張PTZ (PTZセッションとXProtect Smart Clientからのパトロールを予約)	-	-	-	✓	✓
エビデンスロック	-	-	-	-	✓
ブックマーク機能	-	-	手動のみ	手動およびルールベース	手動およびルールベース
ライブマルチストリーミングまたはマルチキャスト/アダプティブストリーミング	-	-	-	✓	✓

名前	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
ダイレクトストリーミング	-	-	-	✓	✓
セキュリティ全般	クライアントのユーザー権限	クライアントのユーザー権限	クライアントのユーザー権限	クライアントのユーザー権限	クライアントのユーザー権限/ 管理者のユーザー権限
XProtect Management Client のプロファイル	-	-	-	-	✓
XProtect Smart Client のプロファイル	-	-	3	3	無制限
XProtect Smart Wall	-	-	-	オプション	✓
システムモニター	-	-	-	✓	✓
スマートマップ	-	-	-	✓	✓
2要素認証	-	-	-	-	✓
DLNAサポート	-	✓	✓	✓	✓
プライバシーマスク	-	✓	✓	✓	✓
デバイスのパスワード管理			✓	✓	✓

要件と注意事項

XProtect Mobileを使用するための要件

XProtect Mobileの使用を開始する前に、次の項目が準備されていることを確認する必要があります。

- 1つ以上のユーザーでインストールおよび構成された実行中のVMS。
- XProtect Smart Clientで設定されたカメラとビュー。
- XProtect Mobile クライアントアプリケーションがダウンロードできるGoogle PlayまたはApp StoreへアクセスできるAndroidまたはiOSのモバイル デバイス
- 実行するWebブラウザXProtect Web Client

要件に関する詳細は、XProtect Mobile システム要件 ページ10をご覧ください。

XProtect Mobile システム要件

各種コンポーネントの最低システム要件については、Milestone Webサイト (<https://www.milestonesys.com/systemrequirements/>) をご覧ください。

- XProtect Mobile クライアントのための要件を検索するには、**XProtect Mobile**製品 アイコンを選択してください
- XProtect Web Clientのための要件を確認するには、製品 アイコン**XProtect Web Client**を選択してください
- XProtect Mobileサーバーのための要件を検索するには、インストールしたXProtect製品のアイコンを選択してください
- XProtect Mobileプラグインの要件:
 - 実行中のManagement Client
 - Milestoneプラグインがインストールされ、VMSと統合します。

通知設定の要件

- 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 Systemsとの契約が最新であることMilestone Care™を確認します。
- インターネット接続があることを確認します

詳細については以下を参照：

XProtect Mobileサーバーでプッシュ通知を設定 ページ46でプッシュ通知を設定する

通知 タブページ25

スマートコネクト設定の要件

- XProtect Mobileサーバーは、パブリックIPアドレスを使用する必要があります。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が必要です

ユーザーの2要素認証設定の要件

- SMTPサーバーが設置されていること。
- 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XProtectのManagement Clientでシステムに追加されていること。関連する役割で、【ユーザーおよびグループ】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、モバイルサーバーを再起動して2要素認証機能を有効にしなければなりません。

詳細については以下を参照：

ユーザーの電子メールによる2要素認証の設定を行います。ページ51

要素認証 タブページ26

ビデオプッシュ設定の要件

- 各チャンネルは一つのハードウェアデバイスライセンスを必要とします
- ビデオプッシュで音声を有効にするには：
 1. Milestone XProtect Device Packのバージョン 10.3a以降をダウンロードしてインストールします。
 2. XProtect Mobile Server Installer.exeのバージョン13.2a以降をダウンロードしてインストールします。
 3. Recording Serverサービスを再起動します。

クライアントに対するモバイルサーバー暗号化の条件

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

モバイルサーバーの暗号化に自己証明を選択すると、XProtect Mobileクライアントはモバイルサーバーに接続できません。

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直接ストリーミングに対応しています(XProtect ExpertおよびXProtect Corporateのみ)。

直接ストリーミングのカメラ構成要件

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、以下のカメラ構成が必要となります。

- カメラがH.264コーデック(すべてのクライアント用) またはH.265コーデック(XProtectMobileクライアント専用)に対応している
- **【GOPサイズ】**の値には**1秒**を、そして**【FPS】**には**10 FPS**を上回る値を設定することが推奨されます。

インストール

XProtect Mobileサーバーをインストール

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、自分のシステムで使用できるようになります。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Webページがあります。このWeb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。



「ひとつのコンピュータ」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サーバーをインストールするには:

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. サーバー・インストーラーのすべての言語XProtect Mobileをクリックします。
3. ダウンロードしたファイルを実行します。すべての警告で【はい】をクリックします。解凍が開始します。
4. インストーラーの言語を選択してください。【続行】をクリックします。
5. 使用許諾契約を読み、同意します。【続行】をクリックします。
6. 安全に通信ができるよう、マネジメントサーバーへの接続に使用する証明書を選択します。
7. インストールの種類を選択:
 - 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】をクリックします。
 - 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、カスタムをクリックします。例えば、Management Clientを使ってXProtect Mobileサーバーをマネジメントしたいが、そのコンピュータ上でXProtect Mobileサーバーが不要な場合、プラグインのみをインストールすると便利です。



Management ClientでXProtect Mobileサーバーを管理するには、Management Clientを実行しているコンピュータ上でXProtect Mobileプラグインが必要です。

8. 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】をクリックします。
9. モバイルサーバーの暗号化を指定します。【続行】をクリックします。

【モバイルサーバーの暗号化を指定】ページでは、モバイルサーバーとクライアントサービスとの間で安全な通信を行うことができます。



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、クライアントに対するモバイルサーバー暗号化の条件ページ37をご参照ください。

リスト中の有効化された認証を選択。安全に通信できるシステムの確立に関する詳細については、レコーディングサーバー データ暗号化(説明付き) ページ36またはMilestone「*認証ガイド*」(英語版のみ)を参照してください。

また、インストールの完了後に、オペレーティングシステムのタスクバーにあるMobile Server Managerトレイアイコンを用いて暗号化を有効にすることもできます(「モバイルサーバー上で暗号化を有効化するページ42」を参照)。

10. 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】をクリックします。



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場合、モバイルサーバーの再インストールが必要となります。

11. [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。
12. 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】をクリックします。



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与えられます(HTTPポートが8081、HTTPSポートが8082)。

13. ファイルの場所と製品の言語を選択し、【インストール】をクリックします。
14. 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。【閉じる】をクリックします。

これでXProtect Mobileを構成する準備が整います(「モバイルサーバーの設定ページ15」を参照)。

設定

Mobileサーバーの設定

Management Client内のXProtect Mobileサーバー設定のリストを構成および編集は、モバイルサーバーの下部 ツールバーのプロパティセクションにあるタブから行えます。ここからは、次のことができます：

- サーバーの一般構成の有効化または無効化(一般 タブページ15を参照)
- サーバー接続設定を行って、スマートコネクト機能を設定する(「接続 タブページ17を参照)
- サーバー現在のステータスとアクティブなユーザーの表示([サーバーステータス]タブページ19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 ビデオストリーミングの制限を設定したりできます(「 パフォーマンスタブページ20を参照)
- 調査設定の構成 (調査 ページ23を参照)
- ビデオプッシュ設定の構成 (ビデオプッシュタブページ24を参照)
- システムとプッシュ通知の設定、およびオン、オフの切り替え(通知 タブページ25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(要素認証 タブページ26を参照)。

一般 タブ

次の表では、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。
ログイン方法	ユーザーがサーバーにログインするときに使用する認証方法を選択します。次から選択できます。 <ul style="list-style-type: none"> • 自動 • Windows認証 • 基本認証

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は有効になっています。
すべてのカメラビューを有効化	すべてのカメラビューを含めます。このビューには、ユーザーがレコーディングサーバーで表示できるすべてのカメラが表示されます。この機能はデフォルトでは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は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 クライアントのクライアントにおいて、インカム音声機能を可能にする。この機能はデフォルトでは有効になっています。
プッシュ・トゥークを使用可能にする	XProtect Web ClientとXProtect Mobile クライアントのクライアントにおいて、プッシュ・トゥーク(PTT)機能を可能にする。この昨日はデフォルトで使用可能です。
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。
ログの保持期間	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

接続タブの設定は次のタスクで使用できます。

- 接続設定の構成ページ45
- 電子メールメッセージをユーザーに送信するページ45
- 複雑なネットワークでの接続を有効にするページ44
- ルーターでのUniversal Plug and Playの検出可能性を有効化ページ44

詳細については、「スマートコネクト(説明付き) ページ43」を参照してください。

一般

名前	説明
接続タイプ	XProtect MobileクライアントおよびXProtect Web Clientユーザーの、XProtect Mobileサーバーへの接続の仕方を選択します。以下のオプションから選択できます。 HTTPのみ 、 HTTP および HTTPS 、または HTTPSのみ 。詳しくは、クライアントに対するモバイルサーバー暗号化の条件ページ37をご参照ください。
クライアントタイムアウト(HTTP)	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では、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	これによってXProtect MobileサーバーがUPnPプロトコルを用いてネットワーク上で発見可能にな

名前	説明
にする	ります。 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は、XProtect Mobileサーバーが、ルーターがそのために構成された場合は、サーバー自体でこのポートマッピングすることを可能にします。
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	UPnPポートマッピングを使用して、接続を特定の接続に向ける場合は、[カスタムインターネットアクセスの設定]チェックボックスを選択します。 IPアドレスまたはホスト名、そして接続に使われるポートを提供します。たとえば、ルーターがUPnPをサポートしない場合、またはルーターのチェーンがある場合は、これを実行できます。
デフォルトのアドレスをオフに設定	カスタムIPアドレスあるいはホスト名のみとモバイルサーバーのデフォルトIPアドレスの接続をオフに設定します。
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、IPアドレスを動的に取得するチェックボックスを選択します。
HTTPポート	HTTP接続のポート番号を入力します。
HTTPSポート	HTTPS接続のポート番号を入力します。
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IP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付と時刻が示されます。
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 Mobileクライアント、あるいはXProtect Web Client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： <ul style="list-style-type: none"> 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クライアントでのダイレクトストリーミングを有効にします。この機能はデフォルトでは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およびXProtect Mobileクライアントでのアダプティブストリーミングを有効にします。この機能はデフォルトでは有効になっています。
ストリーミングモード	<p>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。</p> <ul style="list-style-type: none"> 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

名前	説明
	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負荷について閾値を設定します。
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閾値を設定します。
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負荷について閾値を設定します。
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閾値を設定します。
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または帯域の閾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

調査を有効化すると、XProtect MobileクライアントあるいはXProtect Web Clientを使用して、録画されたビデオにアクセスし、インシデントを調査し、エビデンスビデオを準備およびダウンロードすることができます。

名前	説明
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。
調査フォルダーのサイズを制限する:	調査フォルダーが含むことができる最大メガバイト数を入力します。デフォルトサイズは2000MBです。
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。

名前	説明
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。
エクスポートが失敗したときにデータを保持または削除する (MKVおよびAVI)	調査でダウンロード用に正常に準備されていないデータを保持するか、削除するかを選択します。

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 [データベース]、[AVI]、[MKV]フィールドの右にある削除アイコンをクリックします。

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(「ビデオを流すための「ビデオ・プッシュ」の設定 ページ49」を参照)、[カメラの検索]を選択して関連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。

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は、XProtect Mobileはイベントが発生したときに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参照: 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 ページ47

次の表では、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。詳細については、
「<https://www.milestonesys.com/solutions/platform/product-index/>」を参照してください。

[2要素認証]タブから、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、および指定します。

- iOS またはAndroid モバイル デバイス上の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。もう一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、ユーザーの電子メールによる2要素認証の設定を行います。ページ51を参照してください。

次の表では、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。

名前	説明
	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。
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。 <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  {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。 </div>

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ない期間を指定します。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。

名前	説明
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。
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	システムによって課されるコードの複雑度を指定します。次の中から選択できます。 <ul style="list-style-type: none"> • 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	<p>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。</p> <p>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。</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;">  Windowsグループは2要素認証をサポートしていません。 </div>
検証方法	<p>各ユーザーまたはグループの認証設定を選択します。次の中から選択できます。</p> <ul style="list-style-type: none"> • 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。

ダイレクトストリーミング(説明付き)

XProtect Mobile はライブモードでの直接ストリーミングに対応しています(XProtect ExpertおよびXProtect Corporateのみ)。

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ディングは不要なため、XProtectにかかる負荷の一部が軽減されます。

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のトランスコーディング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。ダイレクトストリーミングはまた、同一のハードウェアのパフォーマンスも向上させます(トランスコーディングと比較して最大で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可能です。

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(「Mobileサーバーの設定ページ15」を参照)。

ビデオストリームは以下が発生すると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ません(「ダイレクトストリーミングの要件ページ11」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(1FPS)に設定されている
- サーバーまたはカメラとの接続が失われている
- 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(説明付き)

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(XProtect ExpertおよびXProtect Corporateのみ)。

アダプティブストリーミングは、カメラの同一ビューで複数のライブビデオストリームを視聴する場合に便利です。この機能により、XProtect Mobileサーバーのパフォーマンスが最適化され、XProtect Web Clientを実行しているデバイスのデコーディング能力とパフォーマンスが向上します。

アダプティブストリーミングを活用するためには、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、この機能によって以下が可能となります。

- ビデオ画質の最適化 - 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

のと同様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)



ズーム中に要求される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(「Mobileサーバーの設定ページ15」を参照)。

さらに情報が必要な時は **安全なコミュニケーション(説明付き)** を参照。

ハイパーテキスト転送プロトコルセキュア(HTTPS)は、ハイパーテキスト転送プロトコル(HTTP)をコンピュータネットワークで安全に通信するために強化したものです。HTTPSでは、通信プロトコルはトランスポートレイヤーセキュリティ(TLS)、または、それ以前の手段であるセキュアソケットレイヤー(SSL)を使用して暗号化されています。

XProtect VMSでは、非対称鍵暗号を伴うSSL/TLS(RSA)を使用することで安全な通信が確立されます。

SSL/TLS プロトコルは、秘密鍵1つと公開鍵1つのペアを使用し、安全な接続を認証し、確実にし、管理します。

認証管理者(CA)は、CA証明書を使ってサーバー上のWebサービスに証明書を発行します。証明書には、秘密鍵と公開鍵の2種類のキーが含まれています。公開鍵は、パブリック証明書をインストールすることにより、Webサービスのクライアント(サービスクライアント)にインストールされます。秘密鍵はサーバー証明書の署名に使用するもので、サーバーにインストールする必要があります。サービスクライアントがWebサービスを呼び出すときは、必ずWebサービスが公開鍵を含むサーバー証明書をクライアントに送信します。サービスクライアントは、すでにインストールされたパブリックCA証明書を使用し、サーバー証明書を検証します。これで、クライアントとサーバーはパブリック及びプライベートサーバー証明書を使用して秘密鍵を交換することができます。よって安全なSSL/TLS通信が確立します。

TLSの詳細については、https://en.wikipedia.org/wiki/Transport_Layer_Securityを参照してください

認証は期限付きです。XProtect VMS は、認証が期限を迎える時も警告しません。証明書の有効期限が切れると

- クライアントは、期限の切れた証明書を持つレコーディングサーバーを信頼できず、通信ができなくなります。。



- レコーディングサーバーは、期限の切れた証明書を持つマネージメントサーバーを信頼できず、通信ができなくなります。。

- モバイルサーバーは、期限の切れた証明書を持つモバイルサーバーを信頼できず、通信ができなくなります。。

証明書の更新は、証明書を作成したときの要領で、本ガイドのステップに従ってください。

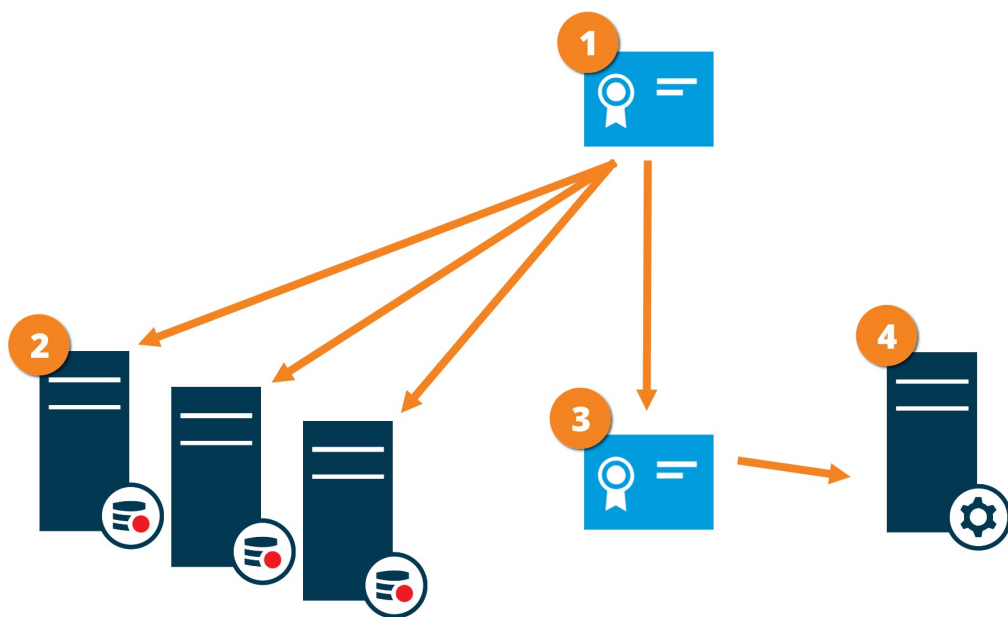
同じサブジェクト名で認証を更新してWindows Certificate Storeに追加すると、サーバーは自動的に新しい認証を獲得します。これにより、たくさんのレコーディングサーバーがレコーディングサーバー毎にサービスの再起動なしで、また認証を再度選択する必要がなく、認証を更新するのが簡単になります。

サーバーの暗号化を管理(説明付き)

マネージメントサーバーとレコーディングサーバー間の双方向接続を暗号化することができます。マネージメントサーバー上の暗号化を有効にした場合、そのマネージメントサーバーに接続するすべてのレコーディングサーバーからの接続に適用されます。マネージメントサーバーの暗号化を有効にした場合、すべてのレコーディングサーバーでも暗号化を有効にする必要があります。暗号化を有効化する前に、マネージメントサーバーとすべてのレコーディングサーバーにセキュリティ証明書をインストールしてください。

マネージメントサーバーの証明書配布

図では、証明書が署名され、信頼され、XProtect VMSで配布されて安全にマネージメントサーバーとの通信が行えるという基本コンセプトを表しています。



- ❶ CA証明者は信頼されたサードパーティのように機能し、サブジェクト/オーナー(マネージメントサーバー)側と、証明書を認証する側(レコーディングサーバー)の双方によって信頼されたものとなります。
- ❷ CA証明書はすべてのレコーディングサーバー上で信頼されている必要があります。このようにして、レコーディングサーバーはCAによる認証の信頼性を確認します。
- ❸ CA証明書は、マネージメントサーバーとレコーディングサーバー間で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、マネージメントサーバーが実行され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。

プライベートマネージメントサーバー証明書の要件:

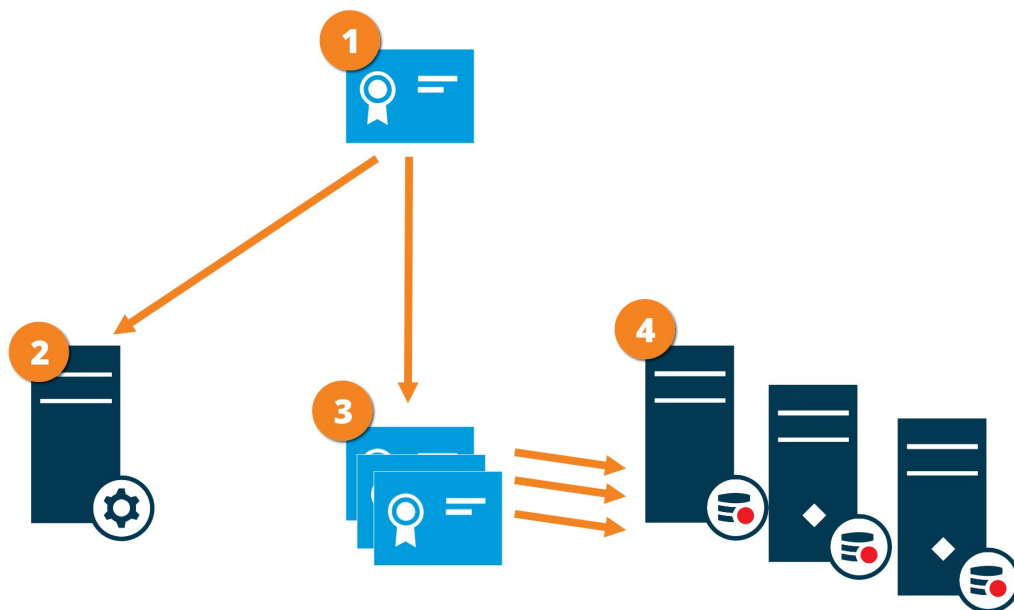
- 認証名にマネージメントサーバーのホスト名が含まれるか、DNS認証される名前リストの中にサブジェクト(オーナー)としてマネージメントサーバーに発行されます。
- マネージメントサーバー証明書の発行に使用されたCA証明書が信頼されていることから、これがマネージメントサーバーでも信頼されていること。
- マネージメントサーバー証明書の発行に使用されたCA証明書を信用することによって、マネージメントサーバーに接続するすべてのレコーディングサーバーで信用されていること

マネージメントサーバーからレコーディングサーバーへの通信を暗号化(説明付き)

マネージメントサーバーとレコーディングサーバー間の双方向接続を暗号化することができます。マネージメントサーバー上の暗号化を有効にした場合、そのマネージメントサーバーに接続するすべてのレコーディングサーバーからの接続に適用されます。この通信の暗号化は、マネージメントサーバーの暗号化設定に従う必要があります。そのため、マネージメントサーバーの暗号化が有効になっている場合、これをレコーディングサーバーでも有効にしなくてはならず、逆もまた同様です。暗号化を有効にする前に、マネージメントサーバーと全レコーディングサーバー(フェールオーバーレコーディングサーバーを含む)にセキュリティ証明書をインストールする必要があります。

証明書の配布

図では、証明書が署名され、信頼され、XProtect VMSで配布されて安全にマネージメントサーバーからの通信が行えるという基本コンセプトを表しています。



- ❶ CA証明書は信頼されたサードパーティのように機能し、サブジェクト所有者(レコーディングサーバー)側と、証明書を認証する側(マネージメントサーバー)の双方によって信頼されているとみなされます。
- ❷ CA認証はマネージメントサーバーで信頼されている必要があります。このように、マネージメントサーバーはCAによる認証の信頼性を確認します。
- ❸ CA証明書は、レコーディングサーバーとマネージメントサーバー間で安全な接続を確立するために使用されます。
- ❹ CA認証は、レコーディングサーバーが実行されるコンピュータにインストールする必要があります。

プライベートレコーディングサーバー認証のための要件:

- 認証名にレコーディングサーバーのホスト名が含まれるか、DNS認証される名前リストの中にサブジェクト(オーナー)としてレコーディングサーバーに発行されます。
- レコーディングサーバー証明書の発行に使用されたCA証明書を信用することによって、マネージメントサーバーで信用されていること

マネージメントサーバーとData Collector Server間の暗号化(説明付き)

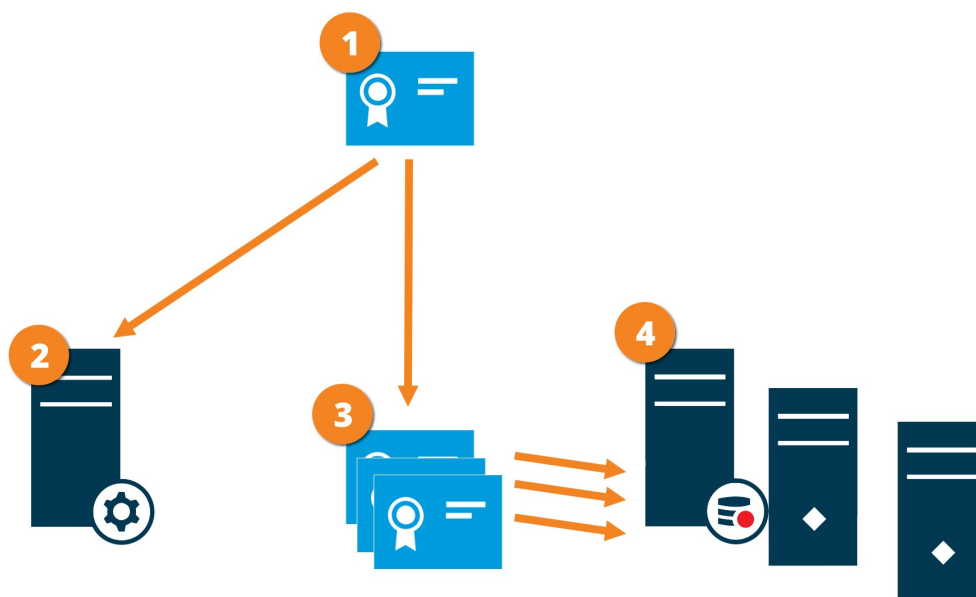
以下のタイプの外部サーバーがある場合、マネージメントサーバーと関連付けられているData Collector 間の双方向接続を暗号化できます。

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

マネジメントサーバー上で暗号化を有効にする場合、マネジメントサーバーに接続するすべてのData Collectorサーバーからの接続にも暗号化の有効化が適用されます。この通信の暗号化は、マネジメントサーバーの暗号化設定に従う必要があります。したがって、マネジメントサーバーの暗号化を有効にすると、各外部サーバーに関連付けられているData Collectorサーバーでも暗号化が有効になり、逆もまた同様となります。暗号化を有効化する前に、必ずマネジメントサーバーに加え、外部サーバーに関連付けられているすべてのData Collectorサーバーにセキュリティ証明書をインストールしてください。

証明書の配布

図では、証明書が署名され、信頼され、XProtect VMSで配布されて安全にマネージメントサーバーからの通信が行えるという基本コンセプトを表しています。



- 1 CA証明書は、サブジェクト/所有者側(データコレクタサーバー)と証明書を認証する側(マネジメントサーバー)両方によって信頼されている信頼されたサードパーティとして機能します
- 2 CA認証はマネジメントサーバーで信頼されている必要があります。このように、マネジメントサーバーはCAによる認証の信頼性を確認します。
- 3 CA証明書は、データコレクタサーバーとマネジメントサーバー間の安全な接続を確立するために使用されます
- 4 CA証明書は必ずデータコレクタサーバーを実行するコンピュータにインストールしてください

プライベートデータコレクタサーバー証明書の要件:

- サブジェクト(所有者)として証明書にデータコレクタサーバーのホスト名を含めるか、証明書が発行されるDNS名のリスト内を含める形で証明書にデータコレクタサーバーのホスト名を含めるため、データコレクタサーバーに発行されること
- データコレクタサーバー証明書の発行に使用されたCA証明書を信頼することによって、マネジメントサーバーで信頼されていること

レコーディングサーバーからデータを取得しているクライアントとサーバーを暗号化(説明付き)

レコーディングサーバーを暗号化可能にする場合、すべてのクライアント、サーバー、ならびにレコーディングサーバーからデータストリームを受け取るインテグレーションは暗号化されます。この文書では「クライアント」と呼んでいます:

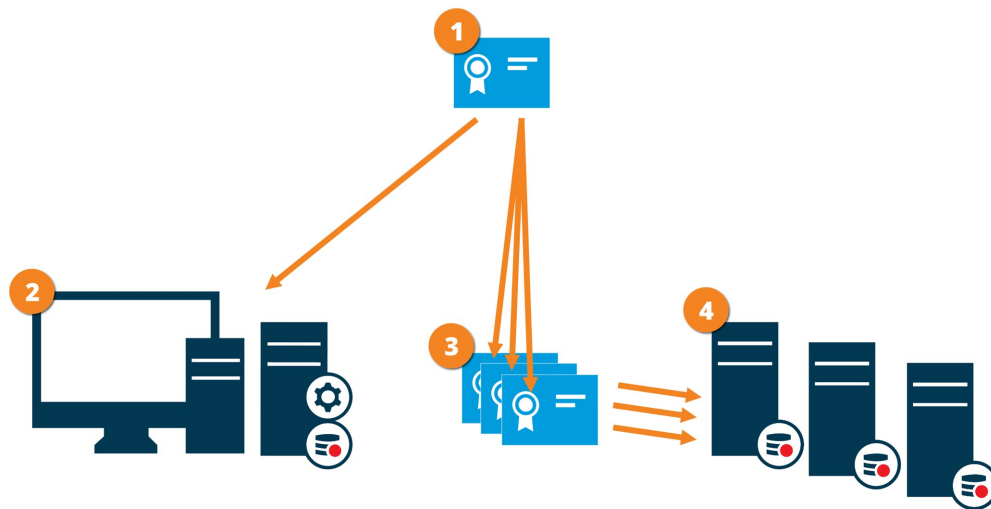
- XProtect Smart Client
- Management Client
- Management Server(eメール通知によるシステムモニター向け、とイメージとAVIビデオクリップ向け)
- XProtect Mobile Server
- XProtect Event Server
- XProtect LPR
- ONVIF Bridge
- XProtect DLNA Server
- を通してレコーディングサーバーからデータストリームを取得するサイトMilestone Interconnect
- サードパーティMIP SDKインテグレーション



レコーディングサーバーにアクセスする、MIP SDK 2018 R3、および以前のバージョンで構築したソリューション: MIP SDKライブラリを用いて統合が行われた場合、MIP SDK 2019 R1でこれらを再構築する必要があります。統合においてMIP SDKライブラリを使用せずにRecording Server APIと直接通信が行われる場合、インテグレータはご自身でHTTPSサポートを追加する必要があります。

証明書の配布

図では、証明書が署名され、信頼され、XProtect VMSで配布されて安全にレコーディングサーバーとの通信が行えるという基本コンセプトを表しています。



- ❶ CA証明書は信頼されたサードパーティのように機能し、サブジェクト/所有者(レコーディングサーバー)側と、証明書を認証する側(全クライアント)の双方によって信頼されているとみなされます。
- ❷ CA認証は全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による認証の信頼性を確認します。
- ❸ CA証明書は、レコーディングサーバーと全クライアント/サービス間で安全な接続を確立するために使用されます。
- ❹ CA認証は、レコーディングサーバーが実行されるコンピュータにインストールする必要があります。

プライベートレコーディングサーバー認証のための要件:

- 認証名にレコーディングサーバーのホスト名が含まれるか、DNS認証される名前の中のリストの中にサブジェクト(オーナー)としてレコーディングサーバーに発行されます。
- レコーディングサーバー認証の発行に使用されたCA認証を信頼することによって、レコーディング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コンピュータで信頼されています
- レコーディングサーバーを実行するサービスアカウントは、レコーディングサーバー上のプライベート認証キーへアクセスします。



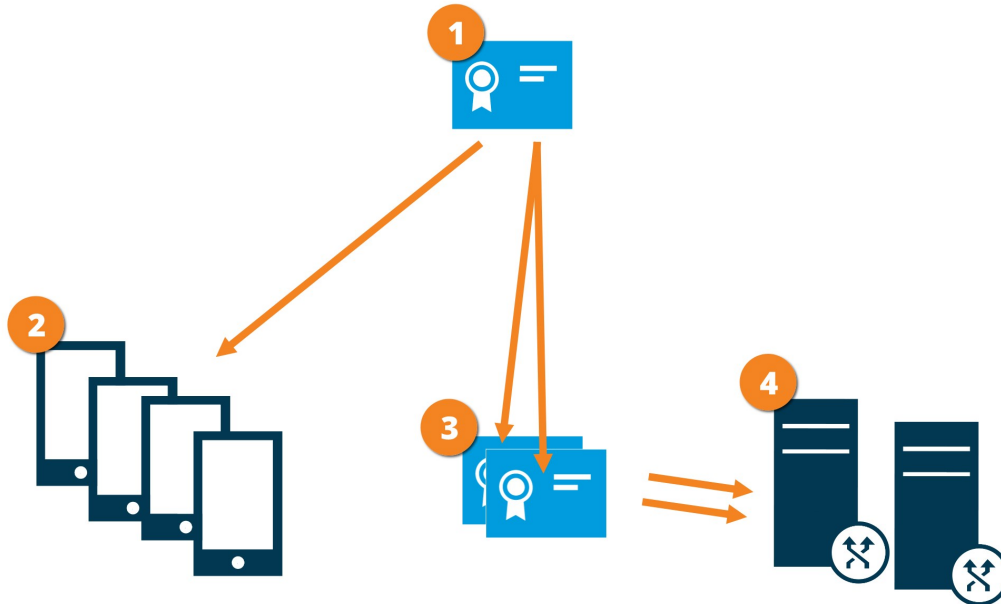
レコーディングサーバーの暗号化が有効化されており、システムがフェールオーバーレコーディングサーバーを適用している場合は、Milestone はフェールオーバーレコーディングサーバーも暗号化する準備をすることをお勧めします。

レコーディングサーバーデータ暗号化(説明付き)

XProtect VMS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き、クライアント、サービス、データストリームを取得するインテグレーションすべてのコミュニケーションを暗号化することができます。

モバイルサーバーの証明書配布

図では、証明書が署名され、信頼され、XProtect VMS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表しています。



- ① CAは信頼されたサードパーティのように振る舞い、サブジェクト/オーナー(モバイルサーバー)双方によって、また、認証確認する(全クライアント)側によって信頼されます。
- ② CA認証は全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による認証の信頼性を確認します。
- ③ CA認証は、モバイルサーバーとクライアントと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。
- ④ CA認証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してください。

CA認証のための要件:

- モバイルサーバーのホスト名は、サブジェクト/オーナーとして、またはDNS認証される名前のリストの中にある認証名に含まれる必要があります
- 認証証明書は、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認証の秘密鍵へアクセスします

クライアントに対するモバイルサーバー暗号化の条件

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

モバイルサーバーの暗号化に自己証明を選択すると、XProtect Mobileクライアントはモバイルサーバーに接続できません。

暗号化を有効化 (in English)

Enable encryption to and from the management server

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see [サーバーの暗号化を管理\(説明付き\)ページ31](#).

Prerequisites:

- A server authentication certificate is trusted on the computer that hosts the management server

First, enable encryption on the management server.

Steps:

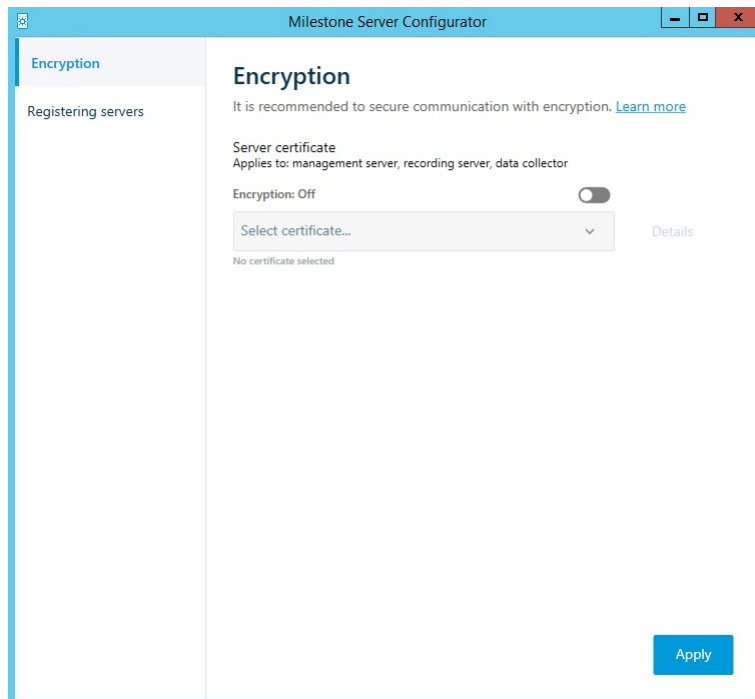
1. On the computer that runs the management server, right-click the Management Server Manager icon in the notification area and select **Server Configurator**.

The **Server Configurator** window appears. The options in this window depend on what servers are installed on the computer.

2. Under **Server certificate**, turn on encryption and select the certificate to encrypt communication between the recording server, management server and data collector server.

When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.

To complete the enabling of encryption, the next step is to update the encryption settings on each recording server and each server with a data collector (Event Server, Log Server, LPR Server, and Mobile Server). For more information, see [Enable server encryption for recording servers or remote servers](#) ページ39.

Enable server encryption for recording servers or remote servers

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see [マネジメントサーバーからレコーディングサーバーへの通信を暗号化\(説明付き\)](#) ページ32 and [マネジメントサーバーとData Collector Server間の暗号化\(説明付き\)](#) ページ33.

Prerequisites:

- You have enabled encryption on the management server, see [暗号化を有効化 \(in English\)](#) ページ38

Steps:

- On each computer that runs a recording server or remote server with a data collector, open the **Server Configurator** from the Windows startup menu.

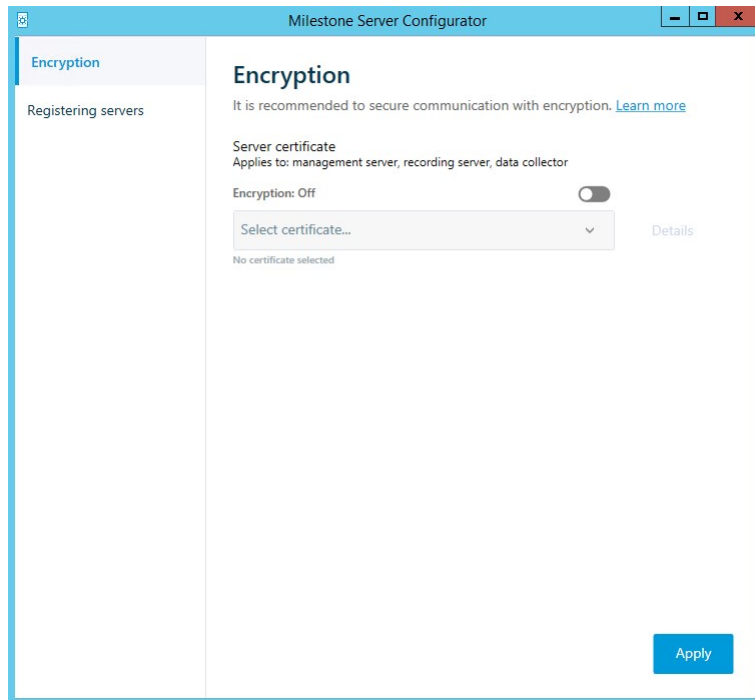
The options in this window depend on what servers are installed on the computer.

2. In the **Server Configurator**, under **Server certificate**, turn on encryption and select the certificate to encrypt communication between the recording server, management server and data collector server.

When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

The recording server service user has been given access to the private key. It is required that this certificate is trusted on all clients.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.



When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

Enable encryption to clients and servers

You can encrypt connections from the recording server to clients and servers that stream data from the recording server. For more information, see [レコーディングサーバーからデータを取得しているクライアントとサーバーを暗号化\(説明付き\) ページ35](#).

Prerequisites:

- The server authentication certificate to be used is trusted on all computers running services that retrieve

data streams from the recording server

- XProtect Smart Client and all services that retrieve data streams from the recording server must be version 2019 R1 or later
- Some third-party solutions created using MIP SDK versions earlier than 2019 R1 may need to be updated

Steps:

1. On each computer that runs a recording server or remote server with a data collector, open the **Server Configurator** from the Windows startup menu.

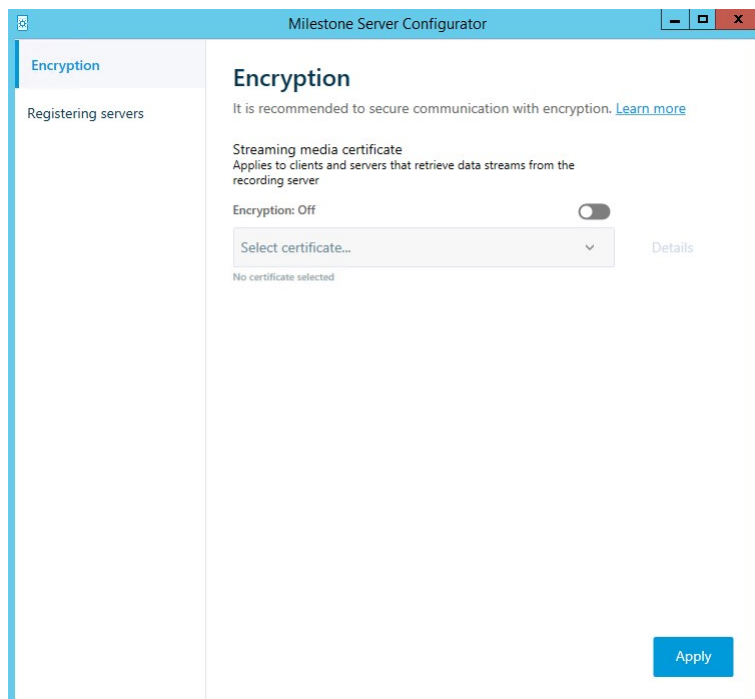
The options in this window depend on what servers are installed on the computer.

2. In the **Server Configurator**, under **Streaming media certificate**, turn on encryption and select the certificate to encrypt communication between the clients and servers that retrieve data streams from the recording server.

When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

The recording server service user has been given access to the private key. It is required that this certificate is trusted on all clients.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.



When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

To verify if the recording server uses encryption, see View encryption status to clients.


モバイルサーバー上で暗号化を有効化する

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、証明書所有者が接続を確立することを承認されていることを裏付けます。詳細については、「レコーディングサーバーデータ暗号化(説明付き) ページ36」と「クライアントに対するモバイルサーバー暗号化の条件ページ37」を参照してください。



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。


モバイルサーバーのインストール後に暗号化を有効にするには:

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、OSのタスクバーのMobile Server Managerトレイアイコンを右クリックし、**【証明書の編集】**を選択します。
2. **【モバイルサーバーからデータストリームを取得している全てのクライアントとサービスを暗号化する】**のチェックボックスを選択します。
3. 有効な証明書を選択するには、 をクリックします。Windowsのセキュリティのダイアログボックスが開きます。
4. 適用したい証明書を選択します。
5. **OK** をクリックします。

証明書の編集

安全な接続に使用している証明書の有効期限が切れた場合は、モバイルサーバーが実行しているコンピュータにインストールされている別の証明書を選択することができます。

証明書の変更方法:

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、OSのタスクバーのMobile Server Manager トレイアイコンを右クリックし、**【証明書編集】**を選択します。
2. 有効な認証を選択するには、 をクリックします。Windowsのセキュリティのダイアログボックスが開きます。
3. 適用したい証明書を選択します。
4. **OK** をクリックします。

メッセージが、証明書がインストールされていることとMobile Serverサービスが変更を適用するために再起動したことを通知します。

Milestone Federated Architecture およびマスター/スレーブサーバー(説明付き)

システムがマスター/スレーブ設定でMilestone Federated Architectureあるいはサーバーをサポートする場合は、XProtect Mobile クライアントあるいはXProtect Web Clientを使用してこのようなサーバーにアクセスできます。この機能を使用して、マスターサーバーにログインし、すべてのスレーブサーバー上のすべてのカメラへのアクセスを取得します。

Milestone Federated Architecture設定では、中央サイト経由で子サイトへのアクセスを取得します。XProtect Mobileサーバーは中央サイトにのみインストールします。

これは、XProtect Mobile クライアントあるいはXProtect Web Clientのユーザーがサーバーにログインして、システムのすべてのサーバーからカメラを表示する場合、マスターサーバーのIPアドレスに接続する必要があるということです。XProtect Mobile クライアントあるいはXProtect Web Clientでカメラを表示するには、ユーザーはシステムのすべてのサーバーでシステム管理者権限が必要です。

スマートコネクト(説明付き)

スマートコネクトは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せずに、XProtect Mobileが正しく構成されたことを確認できるようにします。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易化します。

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いること、システムがMilestone Care Plus購読パッケージのライセンスを受けている必要があります。

Management Clientリモート接続の設定がうまく行われた場合、即座にシステムからフィードバックが送られ、XProtect Mobileサーバーはインターネットからアクセスできます。

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簡単にするために、Management Client内からエンドユーザーに直接Eメールを送れます。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。

Smart Connect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で、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。
3. ルーターでのUniversal Plug and Playの検出可能性を有効にします。
4. 接続を設定する。
5. 電子メールメッセージをユーザーに送信する。
6. 複雑なネットワークでの接続を有効にする。

ルーターでのUniversal Plug and Playの検出可能性を有効化

モバイルデバイスをXProtect Mobileサーバーに簡単に接続するには、ルーターでUniversal Plug and Play (UPnP)を有効にするという方法があります。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、Web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わからな場合は、そのデバイスのマニュアルを参照してください。



5分ごとに、XProtect Mobile Server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。状態は、[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コネクティビティタブで、次の項目を指定します。

- UPnPポートマッピングを使用して、接続を特定の接続に向ける場合は、[カスタムインターネットアクセスの設定]チェックボックスを選択します。IPアドレスまたはホスト名、そして接続に使われるポートを提供します。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は、これを実行できます
- IPアドレスが頻繁に変更される場合は、チェックするとIPアドレスを動的に取得するチェックボックスを選択します

接続設定の構成

1. Management Clientで、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、次の項目を指定します：
 - XProtect MobileクライアントとXProtect Web Clientユーザーが簡単に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
 - 接続タイプフィールドで使用するプロトコルを指定します
 - 安全な接続をオンにする前に、デジタル証明書の知識があることを確認してください。XProtect Mobileサーバーで証明書を追加する方法については、証明書の編集ページ42を参照してください。
 - 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モバイルサーバーに表示すべき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** 発見性を有効にする 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。

電子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の設定を簡単にするために、Management Client内からエンドユーザーに直接Eメールを送れます。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。

1. 招待を電子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電子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。
 - 使用する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：

スマートコネクト設定の要件ページ11

接続タブページ17

通知の送信(説明付き)

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、XProtectMobile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えます。プッシュ通知はモバイルデバイスに配信され、移動中のユーザーが最新情報を常に得られるようにするための優れた方法です。

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。

「通知設定の要件 ページ10」と「通知 タブ ページ25」も参照してください。

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。
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

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。

調査の設定

調査を設定し、XProtect Web ClientあるいはXProtect Mobileを使用して、録画されたビデオにアクセスし、インシデントを調査し、エビデンスビデオを準備およびダウンロードできるようにします。

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. 有効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. 調査フォルダーのサイズを制限するフィールドで、調査フォルダーが含められる最大メガバイト数を入力します。
5. 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。
6. 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。

7. **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に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。

8. 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ルストから、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。
9. エクスポートが失敗した場合のデータを保持または削除する(**MKV**および**AVI**)フィールドで、不完全な可能性もあるが、正常にダウンロードされたデータを、保持するか削除するかどうかを指定します。



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、調査用に作成されたすべてのビデオエクスポートを削除するには、リストの調査を選択し、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、エクスポート用のデータベース、**AVI**、または**MKV**フィールドの右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(説明付き)

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監視システムに動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、動画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。

「ビデオプッシュタブページ24」および「ビデオプッシュ設定の要件ページ11」も参照してください。

ビデオを流すための「ビデオ・プッシュ」の設定

ユーザーが携帯デバイスからXProtectシステムにビデオを流すには、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次の手順で設定が可能です。

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. ビデオプッシュチャンネルをストリーミングビデオに追加。
3. ビデオプッシュドライバーをハードウェアデバイスとして追加するRecording Server。このドライバーはカメラデバイスに影響して、Recording Serverにビデオを流すことができます。
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。

ビデオプッシュ・チャンネルをストリーミングビデオに追加

チャンネルを追加するためには、次のステップを踏んで下さい。

1. ナビゲーションペインで、【モバイルサーバー】を選んでから、モバイルサーバーを選択します。
2. 「ビデオ・プッシュ」のタブ上で、「ビデオ・プッシュ」を選択しボックス内をチェチェックして下さい。
3. 右下の【追加】をクリックして、チャンネルマッピングにビデオプッシュチャンネルを追加します。
4. チャンネルを使用するには、ユーザーアカウントのユーザー名(役割の下に追加されたもの)を入れて下さい。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。

5. ポート・ナンバーを書き留めておいて下さい。それは、記録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」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・ボックスを閉じて、チャンネルを保存します。

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：

- 削除するチャンネルを選択し、右下の【削除】をクリックします。

ビデオプッシュドライバーをハードウェアデバイスとして追加するRecording Server

1. ナビゲーションの窓で、「記録サーバー」をクリックして下さい。
2. ビデオを流したいサーバーを右クリックして、【ハードウェアの追加】をクリックして、【ハードウェアの追加】ウィザードを開きます。

3. ハードウェア探知方法として【手動】を選択し、【次へ】をクリックして下さい。
4. カメラのログイン資格情報を入力します。
 - ユーザ名には、出荷時設定またはカメラに指定されたユーザー名を入力します。
 - パスワードの場合: 入力 **Milestone**、ついで次へをクリックします



これはハードウェアのための資格情報で、ユーザーのものではありません。資格情報はチャンネルのためのユーザー名とは関係ありません。

5. ドライバーズリストで**Milestone**を展開し、「ビデオ・プッシュ・ドライバー」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。



このシステムは「ビデオ・プッシュ・ドライバー」デバイスのためにMACアドレスを作成しています。このアドレスを使用することをお勧めします。そのアドレスは、「ビデオ・プッシュ・ドライバー」デバイスに問題が生じた時だけ、あるいは例えば新しいアドレスとポートナンバーを追加する必要があるときだけ変更して下さい。

6. 「アドレス」欄で、XProtect MobileサーバーにインストールされているコンピューターのIPアドレスを入れて下さい。
7. 「ポート」欄で、ビデオを流すために作成したチャンネル用のポートナンバーを入れて下さい。ポートナンバー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」内で、「ビデオ・プッシュ・ドライバー」を選択し、「次へ」をクリックして下さい。
9. システムが新しいハードウェアを探知したら、「次へ」をクリックして下さい。
10. 「ハードウェア名テンプレート」欄で、ハードウェアのモデルとそのIPアドレスを表示するか、またはモデルだけかを決めて下さい。
11. 関係するデバイスが作動するかどうかは、「作動可」チェックボックスを選択して決めて下さい。「ビデオ・プッシュ・ドライバー」の関連デバイスは、作動不可でも、追加することができます。後で、作動可にできます。



ビデオを流す際にロケーション情報を使いたい場合は、「メタデータ・ポート」を作動させる必要があります。



ビデオをストリームするとき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のマイクを有効にしてください。

12. 左にある関連デバイスの既定グループを選択するか、あるいは【グループ追加】フィールドの特定グループを選択して下さい。一つのグループにデバイスを追加すれば、同時にすべてのデバイスを設定したり、あるいはデバイスの入れ替えが簡単にできます。


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します。

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するには、以下の手順に従ってください。

1. 「サイト・ナビゲーション」で、「携帯サーバー」をクリックしてから、「ビデオ・プッシュ」タブをクリックして下さい。
2. 「カメラを見つける」をクリックして下さい。成功すると、カメラ名欄に、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. あなたの構成を保存して下さい。

既存のビデオプッシュチャンネルに対し音声の有効化する

ビデオプッシュで音声を有効にする要件を満たした後(ビデオプッシュ設定の要件ページ11参照)、Management Clientでは:

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、「Video Push Driver」フォルダーを展開してからビデオプッシュに該当するマイクを右クリックします。
3. [有効化]を選択してマイクを有効化します。
4. 同じフォルダー内で、ビデオプッシュに該当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([クライアントタブのプロパティ]参照)。
6. [該当するマイク]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のフォルダーを展開しビデオプッシュに該当するマイクを選択します。
8. **OK** をクリックします。

ユーザーの電子メールによる2要素認証の設定を行います。



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。詳細については、「<https://www.milestonesys.com/solutions/platform/product-index/>」を参照してください。

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しなければなりません。

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にて、以下の手順に従ってください。

1. SMTPサーバーに関する情報を入力します。ページ52。
2. ユーザーに送られてくる認証コードを指定します。ページ52。
3. ユーザーとActive Directoryグループにログイン方法を割り当てます。ページ52。

「ユーザーの2要素認証設定の要件ページ11」と「要素認証 タブページ26」も参照してください。

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]**を選んでから、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の、電子メールタブで、SMTPサーバーに関する情報を入力した後、ログイン時および2次ログインで設定する電子メールを指定します。それぞれのパラメータの詳細については、「要素認証 タブページ26」を参照してください。

詳細については、「要素認証 タブページ26」を参照してください。

ユーザーに送られてく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:

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、例えばネットワーク切断の際に再確認なしに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. システムによって課されるコードの複雑度を指定します。

詳細については、「要素認証 タブページ26」を参照してください。

ユーザーとActive Directoryグループにログイン方法を割り当てます。

[ユーザー設定]セクションの、**[2段階認証]**タブに、XProtectシステムに追加したユーザーおよびグループのリストが表示されます。

1. **[ログイン方法]**列で、各ユーザーまたはグループの検証方法を選択します。
2. 詳細フィールドで、各ユーザーの電子メールアドレス等の配信の詳細を追加します。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際、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. あなたの構成を保存して下さい。

電子メールによる2要素認証のユーザー設定手順を完了しました。

詳細については、「要素認証 タブページ26」を参照してください。

アクション(説明付き)

XProtect Mobile クライアント内またはXProtect Web Client内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。

詳細は、一般タブページ15を参照してください。

XProtect Mobile クライアントおよびXProtect Web Clientで使用する出力の名前を決める(説明付き)

アクションが現行のカメラで正しく表示されるためには、カメラと同じ名前を出力グループにつける必要があります。

例:

「AXIS P3301, P3304 - 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で、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)にて、同じ名前を入力する必要があります。

【説明】フィールドにて、「AXIS P3301,P3304 - 10.100.50.110 - Camera 1 - Light switch」のように詳細説明を追加することができます。



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、出力デバイス(説明付き)を参照してください。

メンテナンス

Mobile Server Manager (説明付き)

Mobile Server Manager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 Server Manager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。

- XProtect Web Clientへのアクセスページ54
- Mobile Serverサービスの起動、停止、再起動ページ55
- マネジメントサーバーのアドレスの入力/編集ページ55
- ポート番号の表示/編集ページ55
- 証明書の編集ページ42
- 今日のログファイルを開く(ログへのアクセスおよび調査(説明付き) ページ56を参照)
- ログフォルダーを開く(ログへのアクセスおよび調査(説明付き) ページ56を参照)
- オープン調査フォルダー(ログへのアクセスおよび調査(説明付き) ページ56を参照)
- 調査フォルダーを変更ページ56
- XProtect Mobile Server ステータス(ステータスの表示(説明付き) ページ57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、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その他のすべてのコンピュータからアクセスできます。

1. Management ClientでXProtect Mobile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、通知エリアのMobile Server Managerトレイアイコンを右クリックし、**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(Internet Explorer、Mozilla Firefox、Google Chrome、Safari)を開きます。

- 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)。

スタンダード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て、**http://127.2.3.4:8081**とタイプします。安全に確立されたHTTPS接続を使用するには、**https://127.2.3.4:8082**とタイプします。これで、XProtect Web Clientを使用できます。

- 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 Mobile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 Web Client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、Mobile Server Managerアイコンを右クリックし、**Mobile Server**サービスの起動、**Mobile Server**サービスの停止、または**Mobile Server**サービスの再起動を選択します

マネジメントサーバーのアドレスの入力/編集

- Mobile Server Managerアイコンを右クリックし、[マネジメントサーバーのアドレス]を選択します。
- [サーバーURL]フィールドに、サーバーのURLアドレスを入力します。
- OK** をクリックします。


ポート番号の表示/編集

- 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。
- 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。
- OK** をクリックします。

証明書編集

安全な接続に使用している証明書の有効期限が切れた場合は、モバイルサーバーが実行しているコンピュータにインストールされている別の証明書を選択することができます。

証明書の変更方法:

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、OSのタスクバーのMobile Server Manager トレイアイコンを右クリックし、**[証明書の編集]**を選択します。
2. 有効な認証を選択するには、 をクリックします。Windowsのセキュリティのダイアログボックスが開きます。
3. 適用したい証明書を選択します。
4. **OK** をクリックします。

メッセージが、証明書がインストールされていることとMobile Serverサービスが変更を適用するために再起動したことを通知します。

ログへのアクセスおよび調査(説明付き)

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先のフォルダーを開くことができます。

これら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



お使いのシステムからXProtect Mobileをアンインストールする場合、そのログファイルは削除されません。適切な権限があるシステム管理者は、後でこれらのログファイルにアクセスしたり、必要でなくなった場合に削除を決定したりできます。ログファイルのデフォルトでの場所は、**[プログラムデータ]**フォルダーです。ログファイルのデフォルトでの場所を変更する場合、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。

調査フォルダーを変更

調査のデフォルトでの場所は、「プログラムデータ」フォルダーです。調査フォルダーのデフォルトのロケーションを変更する場合、既存の調査が新しいロケーションに自動的にコピーされることも、削除されることもありません。お使いのハードディスク上で調査エクスポートを保存するロケーションを変更するには。

1. Mobile Server Managerアイコンを右クリックし、調査フォルダーの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. 既存のフォルダーの閲覧、あるいは新しいフォルダーを作成するには、フォルダーフィールドの隣の、現在のロケーションが表示されている場所にて、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、現在のロケーションに保管されている既存の調査に適応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 既存の調査を新しいフォルダーに移動します
- 

もし既存の調査を新しいフォルダーに移動させない場合、それを閲覧することはできません。
- 削除: 既存の調査を削除します
 - なにもしない 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、それらは表示できなくなります。
4. **[適応]** をクリックし、> クリック**OK**。

ステータスの表示(説明付き)

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。
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

トラブルシューティング XProtect Mobile

接続

1. なぜ**XProtect Mobile**クライアントから自分のレコーディング/**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サーバーが、XProtectシステムが実行されているサーバーに、または専用サーバーにインストールされていなければなりません。また、XProtectビデオ管理設定において、関連するXProtect Mobile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/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について詳しくは、「構成」のセクション(Mobileサーバーの設定ページ15)を参照してください。

2. 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。なぜでしょうか？

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、TCPとUDP通信を手動で有効にする必要があります。

3. **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、Verisignとった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製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

1. **XProtect Mobile**クライアントでビデオを視聴する際に、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、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。**XProtect Smart Client**ユーザーマニュアルを参照してください(弊社のウェブサイト(<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>) からダウンロード可能)。

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。

2. オフィスのWiFiを介して自宅からXProtectビデオ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？

自宅のインターネットの帯域幅をお調べください。家庭用インターネット接続ではたいいてい、ダウンロード/アップロード帯域幅が異なります(通常は20 Mbit/2 Mbitなど記述)。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ビデオ管理システムではビデオをXProtect Mobile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。XProtect Mobileクライアントのネットワークのダウンロード速度が良好ながらも、複数の場所において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ことで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テッドデコーディング

1. 私が所有しているプロセッサはハードウェアアクセラレーテッドデコーディングに対応していますか？

ハードウェアアクセラレーテッドデコーディングには、Intelから販売されている比較的新しいプロセッサのみ対応しています。お持ち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/Search/FeatureFilter?productType=processors/>)を参照してください。

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。

お持ちの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テッド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(「ステータスの表示(説明付き) ページ57」を参照)。

2. 私が使用している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テッド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Intelウェブサイトに記載されている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。これらのドライバーは、Windowsアップデートでは入手できません。

モバイルサーバーが仮想環境にインストールされている場合、ハードウェアアクセラレーテッドデコーディングには対応しません。

3. どうすればモバイルサーバーでのハードウェアアクセラレーション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テッド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テッド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：

1. VideoOS.MobileServer.Service.exe.configを探します。パスは通常以下ようになっています：
C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config
2. 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。



helpfeedback@milestone.dk

Milestoneについて

Milestone Systems はオープンプラットフォームの監視カメラ管理ソフトウェア (Video Management Software: 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Milestoneの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。

