JVC

ネットワークビデオレコーダー

型名 **VR-X8500**

Milestone XProtect VMS システム 管理者マニュアル

本書では、本システムの設定について、VR-X8500 取扱説明書（操作・設定編）に掲載されていない応用設定方法や Management Client の詳細な設定項目について説明しています。
本書は Milestone Systems A/S が作成した取扱説明書をオリジナルのまま掲載しており、すべての XProtect VMS 製品が対象となっています。
本機で採用している XProtect Express+ では対応していない機能に関する記載も含まれていますので、ご注意ください。

B5A-3749-00

目次

著作権、商標、および免責条項 22
概要 23
製品概要 23
メインシステムコンポーネント 23
マネジメントサーバー 23
レコーディングサーバー 24
イベントサーバー 24
ログサーバー 25
SQL Serverとデータベース 25
モバイルサーバー 25
Active Directory 25
Management Client (説明付き) 26
オプションのシステムコンポーネント 26
フェールオーバーレコーディングサーバー 26
フェールオーバーマネジメントサーバー 26
クライアント 26
XProtect Smart Client (説明付き) 26
XProtect Mobileクライアント(説明付き) 27
XProtect Web Client (説明付き) 28
分散型システム設定 29
アドオン製品 30
XProtect Access (説明付き) 30
XProtect LPR (説明付き) 31
XProtect Smart Wall (説明付き) 31
XProtect Transact (説明付き) 32
Milestone Open Network Bridge (説明付き) 33
XProtect DLNA Server (説明付き) 33

このシステムで使用するポート 33
製品比較チャート 46
ライセンス 49
ライセンス(説明付き) 49
ソフトウェアライセンスコードの変更 50
要件と注意事項 51
サマータイム(説明付き) 51
タイムサーバ(説明付き) 51
データベースのサイズを制限 52
Ipv6 および Ipv4 (説明付き) 52
Ipv6アドレスの書き方(説明付き) 54
URLでのIPv6アドレスの使用 54
仮想サーバー 55
複数のマネジメントサーバー(クラスタリング)(説明付き) 55
クラスタリングの要件 56
記録データベースを破損から守る 56
ハードディスク障害:ドライブの保護 56
Windowsタスクマネージャー:プロセスを終了する際は注意してください 57
停電:UPSを使用 57
SQLデータベーストランザクションログ(説明付き) 57
最低限のシステム要件 58
インストールを開始する前に 58
サーバーとネットワークの準備 58
Active Directoryの準備 59
インストール方法 59
SQL Serverエディションの決定 61
サービスアカウントを選択してください 62
Kerberos認証(説明付き) 62
ウィルススキャンの排除(説明付き) 64

FIPS 140-2準拠モードで実行するようにXProtect VMSを設定するにはどうすればよいですか? 65
FIPSが有効なシステムでXProtect VMSをインストールする前に 66
ソフトウェアライセンスコードを登録する 66
デバイスドライバー(説明付き) 66
オフラインインストールの要件 67
安全な通信(説明付き) 67
サーバーの暗号化を管理(説明付き) 68
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) 69
マネジメントサーバーとData Collector Server間の暗号化(説明付き) 71
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) 72
レコーディングサーバーデータ暗号化(説明付き) 74
クライアントに対するモバイルサーバー暗号化の条件 75
インストール 76
新しいXProtectシステムのインストール 76
XProtect Essential+をインストールする 76
システムのインストール - シングルコンピュータオプション 80
システムのインストール - カスタムオプション 84
新しいXProtectコンポーネントのインストール 88
Download Managerを介したインストール(説明付き) 88
Download Managerを介したレコーディングサーバーのインストール 89
Download Managerを介したフェールオーバーレコーディングサーバーのインストール 92
コマンドラインシェルを介したサイレントインストール(説明付き) 94
記録サーバーをサイレント・インストールします 95
XProtect Smart Clientサイレントインストール 96
ワークグループのインストール 98
クラスタへのインストール 98
Download Manager/ダウンロードWebページ 101
Download Managerのデフォルト設定 102
Download Managerの標準インストーラ(ユーザー) 104

Download Managerインストーラコンポーネントの追加/公開 104
Download Managerインストーラコンポーネントを非表示化/削除 105
Device Packのインストーラ- ダウンロードする必要があります 106
インストールログファイルとトラブルシューティング 107
設定 108
Management Clientをナビゲーション 108
ログイン概要 108
Management Clientウィンドウ概要 110
ペインの概要 113
メニュー概要 114
ファイルメニュー 114
編集メニュー 114
ビューメニュー 114
アクションメニュー 115
ツールメニュー 115
ヘルプメニュー 116
システムのオプションを設定 116
一般タブ(オプション) 116
サーバーログタブ(オプション) 118
メールサーバータブ(オプション) 119
AVI生成タブ(オプション) 120
ネットワークタブ(オプション) 121
ブックマークタブ(オプション) 121
ユーザー設定タブ(オプション) 122
カスタマーダッシュボードタブ(オプション) 122
エビデンスロックタブ(オプション) 122
音声メッセージタブ(オプション) 123
入退室管理設定タブ(オプション) 124
アナリティクスイベントタブ(オプション) 124

[アラームおよびイベント]タブ(オプション) 125
ジェネリックイベントタブ(オプション) 127
初期構成タスクリスト 129
サイトナビゲーションペインでのシステムの構成 130
サイトナビゲーション：基本 131
ライセンス情報 131
アクティベーションなしのデバイスの変更(説明付き) 133
アクティベーションなしのデバイスの変更数の計算方法 134
ライセンス概要の表示 135
自動ライセンスアクティベーション(説明付き) 135
自動ライセンスアクティベーションを有効にする 136
自動ライセンスアクティベーションを無効にする 136
ライセンスをオンラインでアクティベーション 136
ライセンスをオフラインでアクティベート 137
猶予期間が切れた後にライセンスをアクティベートする 137
追加ライセンスの取得 137
ライセンスとハードウェアデバイスの交換 138
サイト情報 138
サイト情報の編集 138
サイトナビゲーション：サーバーとハードウェア 139
サイトナビゲーション：サーバーとハードウェア：レコーディングサーバー 139
レコーディングサーバー(説明付き) 139
レコーディングサーバーを登録する 140
レコーディングサーバーの基本的な設定を変更または確認する 141
[レコーディングサーバーの設定]ウィンドウ 143
クライアントへの暗号化ステイタスを見る 144
レコーディングサーバーステータスアイコン 145
情報タブ(レコーディングサーバー) 146
インフォメーションタブ機能(レコーディングサーバー) 147

ストレージタブ(レコーディングサーバー) 148
ストレージとアーカイブ(説明) 149
レコーディングストレージが利用できない場合の動作を指定 152
新しいストレージの追加 154
ストレージでのアーカイブの作成 154
個別のデバイスまたはデバイスのグループをストレージに接続する 154
選択したストレージまたはアーカイブ設定の編集 155
エクスポートのデジタル署名を有効にします。 155
録画を暗号化する 156
アーカイブされた記録をバックアップする 158
アーカイブ構造(説明付き) 159
ストレージでのアーカイブの削除 160
ストレージの削除 161
アーカイブされていない記録をあるストレージから別のストレージへ移動する 161
ストレージおよび録画設定プロパティ 162
アーカイブ設定のプロパティ 163
フェールオーバータブ(レコーディングサーバー) 164
フェールオーバーレコーディングサーバーの割り当て 165
フェールオーバータブのプロパティ 166
マルチキャストタブ(レコーディングサーバー) 167
マルチキャスト(説明付き) 169
レコーディングサーバーのマルチキャストを有効にする 169
IPアドレス範囲の割り当て 170
データグラムオプションの指定 171
個々のカメラに対してマルチキャストを有効にする 171
ネットワークタブ(レコーディングサーバー) 171
パブリックアドレスを使用する理由 171
パブリックアドレスとポートの定義 172
ローカルIP範囲の割り当て 172

サイトナビゲーション：サーバーとハードウェア：フェールオーバーサーバー 172
フェールオーバーレコーディングサーバー(説明付き) 172
フェールオーバーの手順(説明付き) 174
フェールオーバーレコーディングサーバー機能(説明付き) 175
フェールオーバーレコーディングサーバーの設定と有効化 177
コールドスタンバイ用にフェールオーバーレコーディングサーバーをグループ化 178
レコーディングサーバーのステータスアイコンの読み方 178
マルチキャストタブ(フェールオーバーサーバー) 178
情報タブのプロパティ(フェールオーバーサーバー) 179
情報タブの機能(フェールオーバーグループ) 181
シーケンスタブのプロパティ(フェールオーバーグループ) 181
フェールオーバーレコーディングサーバーのサービス(説明付き) 181
フェールオーバーレコーディングサーバーで暗号化ステータスを表示 181
ステータスメッセージの表示 183
バージョン情報の表示 183
サイトナビゲーション：サーバーとハードウェア：ハードウェア 183
ハードウェア(説明付き) 183
ハードウェアの追加 183
ハードウェアの事前設定(説明付き) 185
ハードウェアの有効化/無効化 185
ハードウェアの編集 186
個々のデバイスの有効化/無効化 189
ハードウェアへの安全な接続設定する 190
ビデオエンコーダーでのPTZの有効化 190
ハードウェアの管理 191
情報タブ(ハードウェア) 191
設定タブ(ハードウェア) 192
PTZタブ(ビデオエンコーダー) 193
デバイスのパスワード管理(説明付き) 193

ハードウェアデバイスでのパスワード変更 194
デバイスファームウェアのアップデート(説明付き) 195
ハードウェアデバイスでのファームウェア更新 196
サイトナビゲーション：サーバーとハードウェア：リモートサーバーの管理 197
情報タブ(リモートサーバー) 197
設定タブ(リモートサーバー) 198
イベントタブ(リモートサーバー) 198
リモート取得タブ 198
サイトナビゲーション：デバイス：デバイスの使用 199
デバイス(説明付き) 199
カメラデバイス(説明付き) 200
マイクデバイス(説明付き) 200
スピーカーデバイス(説明付き) 201
メタデータデバイス(説明付き) 202
入力デバイス(説明付き) 203
手動で入力を有効にしてテストする 204
出力デバイス(説明付き) 204
手動で出力を有効にしてテストします。 205
デバイスグループ経由のデバイスの有効化/無効化 206
デバイスのステータスアイコン 206
サイトナビゲーション：デバイス：デバイスグループの操作 207
デバイスグループの追加 208
デバイスグループに含めるデバイスの指定 209
デバイスグループのすべてのデバイスに対する共通プロパティの指定 209
サイトナビゲーション：［デバイス］タブ 210
情報タブ(デバイス) 210
情報タブ(説明付き) 210
情報タブのプロパティ 211
設定タブ(デバイス) 212

設定タブ(説明付き) 212
カメラ設定(説明付き) 213
ストリームタブ(デバイス) 214
ストリームタブ(説明付き) 214
マルチストリーミング(説明付き) 215
ストリームの追加 216
録画タブ(デバイス) 217
[録画]タブ(説明付き) 217
記録の有効化と無効化 219
関連するデバイスで録画を有効にする 219
プレバッファ(説明付き) 219
プリバッファをサポートするデバイス 220
一時プレバッファ録画の保存 220
プリバッファの管理 220
手動記録の管理 221
レコーディングフレームレートを指定する 221
キーフレームレコーディングの有効化 222
ストレージ(説明付き) 222
デバイスをストレージ間で移動する 224
リモート録画(説明付き) 224
モーションタブ(デバイス) 224
モーションタブ(説明付き) 224
モーション検知の有効化と無効化 227
モーション検知設定の指定 227
ハードウェアアクセラレーション(説明付き) 227
手動感度の有効化 228
閾値の指定 229
キーフレーム設定の選択 229
画像処理間隔を選択 229

検出解像度の指定 230
スマート検索モーションデータの生成 230
領域の除外を指定 230
プリセットタブ(デバイス) 231
プリセットタブ(説明付き) 231
プリセット位置を追加する(タイプ1) 234
カメラからのプリセット位置を使用します(タイプ2) 236
デフォルトのプリセット位置の割り当て 236
プリセット位置を編集する(タイプ1のみ) 236
プリセット位置をテストする(タイプ2のみ) 238
プリセット位置のロック 238
プリセット位置をテストする(タイプ1のみ) 239
予約済みPTZセッション(解説済み) 239
PTZセッションのリリース 239
PTZセッションタイムアウトの指定 239
PTZセッションの優先度 240
パトロールタブ(デバイス) 241
パトロールタブ(説明付き) 241
パトロール設定の追加 243
パトロール設定でのプリセット位置の指定 243
各プリセット位置での時間を指定 244
旋回動作(PTZ)をカスタマイズ 244
終了位置の指定 245
手動パトロール(説明付き) 245
手動パトロールプロパティ 246
魚眼レンズタブ(デバイス) 246
魚眼レンズタブ(説明付き) 246
魚眼レンズサポートを有効/無効にする 247
魚眼レンズ設定の指定 247

イベントタブ(デバイス) 248
イベントタブ(説明付き) 248
イベントの追加 248
イベントプロパティの指定 249
イベントに複数のインスタンスを使用する 249
イベントタブ(プロパティ) 249
クライアントタブ(デバイス) 250
[クライアント]タブ(説明付き) 250
クライアントタブのプロパティ 251
プライバシーマスクタブ(デバイス) 252
プライバシーマスクタブ(説明付き) 252
プライバシーマスク(説明付き) 253
プライバシーマスクの有効化/無効化 256
プライバシーマスクを定義する 256
プライバシーマスクの除去権限をユーザーに与える 257
除去されたプライバシーマスクのタイムアウトを変更する 258
プライバシーマスク設定のレポートを作成します 259
プライバシーマスクタブ(プロパティ) 260
サイトナビゲーション：クライアント 262
クライアント(説明付き) 262
サイトナビゲーション：クライアント：Smart Wallの設定 262
XProtect Smart Wallライセンス 263
Smart Wallの構成 263
XProtect Smart Wallのユーザー権限を設定 265
Smart Wallプリセットのあるルールの使用(説明付き) 266
Smart Wallプロパティ 266
情報タブ(Smart Wallプロパティ) 266
プリセットタブ(Smart Wallプロパティ) 266
レイアウトタブ(Smart Wallプロパティ) 267

モニタープロパティ 268
情報タブ(モニタープロパティ) 268
プリセットタブ(モニタープロパティ) 269
サイトナビゲーション：クライアント：ビューグループ 270
ビューグループと役割(説明付き) 270
ビューグループの追加 270
サイトナビゲーション：クライアント：Smart Clientプロファイル 271
Smart Clientプロファイルの追加と構成 271
Smart Clientプロファイルのコピー 271
Smart Clientプロファイル、役割、時間プロファイルの作成と設定 272
簡易モードをデフォルトモードとして設定 272
オペレータが簡易モードと詳細モードで切り替えられないようにする 274
Smart Clientプロファイルのプロパティ 276
情報タブ(Smart Clientプロファイル) 276
全般タブ(Smart Clientプロファイル) 276
詳細タブ(Smart Clientプロファイル) 276
ライブタブ(Smart Clientプロファイル) 277
再生タブ(Smart Clientプロファイル) 277
設定タブ(Smart Clientプロファイル) 278
エクスポートタブ(Smart Clientプロファイル) 278
タイムラインタブ(Smart Clientプロファイル) 278
入退室管理タブ(Smart Clientプロファイル) 278
アラームマネージャータブ(Smart Clientプロファイル) 279
スマートマップタブ(Smart Clientプロファイル) 279
ビューレイアウトタブ(Smart Clientプロファイル) 280
サイトナビゲーション：クライアント：Management Clientプロファイル 280
Management Clientプロファイルの追加と構成 280
Management Clientプロファイルのコピー 281
Management Clientプロファイルのプロパティ 281

情報タブ(Management Clientプロファイル) 281
プロファイルタブ(Management Clientプロファイル) 282
サイトナビゲーション：クライアント：Matrixを設定中... 284
Matrix受信者の追加 285
ビデオをMatrixの受領者へ送信するためのルールを定義 285
複数のXProtect Smart Clientビューに同じビデオを送信 286
サイトナビゲーション：ルールとイベント 286
ルールおよびイベント(説明付き) 286
アクションおよびアクションの停止(説明付き) 288
イベント概要 298
ルール 309
ルール(説明付き) 309
デフォルトルール(説明付き) 310
ルールの複雑さ(説明付き) 312
ルールの検証(説明付き) 313
ルールの追加 314
ルールを編集、コピー、名前を変更する 315
ルールを無効/有効にする 315
定期スケジュール 316
時間プロファイル 316
時間プロファイルの指定 317
時間プロファイルの編集 319
日中時間プロファイル(説明付き) 319
日の長さの時間プロファイルの作成 320
日の長さの時間プロファイルのプロパティ 320
通知プロファイル 320
通知のプロファイル(説明付き) 320
通知のプロファイル作成の要件 321
通知プロファイルの追加 321

Eメール通知をトリガーするルールを使用する 323
通知プロファイル(プロパティ) 323
ユーザー定義イベント 325
ユーザー定義のイベント(説明付き) 325
ユーザー定義イベントの追加 326
ユーザー定義イベントの名前変更 327
アナリティクスイベント 327
アナリティクスイベント(説明付き) 327
アナリティクスイベントの追加と編集 327
アナリティクスイベントのテスト 328
アナリティクスイベントをテストする(プロパティ) 329
アナリティクスイベント設定の編集 331
ジェネリックイベント 331
ジェネリックイベント(説明付き) 331
ジェネリックイベントの追加 331
ジェネリックイベント(プロパティ) 332
ジェネリックイベントデータソース(プロパティ) 334
サイトナビゲーション：セキュリティ 335
役割(説明付き) 336
役割の権利(説明付き) 336
ユーザー(説明付き) 337
役割の追加および管理 338
役割のコピー、名前の変更、削除 339
ユーザーおよびグループの役割からの削除、役割への割り当て 339
有効な役割の表示 340
役割の設定 341
情報タブ(役割) 341
ユーザーおよびグループタブ(役割) 342
セキュリティ全般タブ(役割) 343

デバイスタブ(役割) 366
PTZタブ(役割) 372
通話タブ(役割) 373
リモート録画タブ(役割) 374
Smart Wallタブ(役割) 374
外部イベントタブ(役割) 374
ビューグループタブ(役割) 375
サーバータブ(役割) 375
Matrixタブ(役割) 376
アラームタブ(役割) 376
入退室管理タブ(役割) 377
LPRタブ(役割) 377
MIPタブ(役割) 378
基本ユーザー(説明付き) 378
基本ユーザーの作成 378
サイトナビゲーション：システムダッシュボード 378
システムダッシュボード(説明付き) 378
システムモニター(説明付き) 379
ダッシュボードのカスタマイズ 380
システムモニターの詳細(説明付き) 381
システムモニターしきい値(説明付き) 382
システムモニターしきい値の設定 384
エビデンスロック(説明付き) 385
現在のタスク(説明付き) 387
設定レポート(説明付き) 387
設定レポートの追加 388
設定レポートの詳細 388
サイトナビゲーション：サーバーログ 388
ログ(説明付き) 388

フィルターログ 389
ログのエクスポート 390
ログを録画するため、2018 R2およびそれ以前のコンポーネントを許可します 391
システムログ(プロパティ) 392
監査ログ(プロパティ) 392
ルールによってトリガーされるログ(プロパティ) 393
サイトナビゲーション：メタデータの使用 394
メタデータとは？ 394
メタデータ検索(説明付き) 394
メタデータ検索の要件 394
XProtect Smart Clientでメタデータ検索カテゴリおよび検索フィルターを表示/非表示にする 394
サイトナビゲーション：アラーム 395
アラーム(説明付き) 395
アラーム設定(説明付き) 397
アラーム定義 397
アラームの追加 398
アラーム定義(プロパティ) 399
アラームデータ設定 401
音声の設定 403
暗号化を有効にする 404
管理サーバーとの間で暗号化を有効にする 404
レコーディングサーバーまたはリモートサーバーのサーバー暗号化を有効にする 405
クライアントとサーバーに対して暗号化を有効にする 407
モバイルサーバーで暗号化を有効にする 409
クライアントへの暗号化ステイタスを見る 411
Milestone Federated Architectureの設定 412
フェデレーテッドサイトを実行するためのシステムの設定 416
サイトを階層に追加 417
階層に含むことを許可 418

サイトプロパティの設定 418
サイト階層の更新 419
階層の他のサイトへのログイン 419
階層からのサイトの分離 420
フェデレーテッドサイトのプロパティ 420
一般タブ 420
親サイトタブ 421
Milestone Interconnectの設定 421
Milestone InterconnectまたはMilestone Federated Architectureの選択(説明付き) 422
Milestone Interconnectおよびラインセンス 422
Milestone Interconnect(説明付き) 422
Milestone Interconnectの設定(説明付き) 424
リモートサイトを中央Milestone Interconnectサイトに追加 425
ユーザー権限の割り当て 426
リモートサイトのハードウェアの更新 426
リモートシステムにリモートデスクトップを接続 427
リモートサイトのカメラからの直接再生を可能にする 427
リモートサイトのカメラからリモート録画を取得する 427
リモートサイトからのイベントに応答するように中央サイトを構成する 428
リモート接続サービスの設定 429
One-Clickカメラ接続のSTS環境をインストール 430
STSの追加/編集 430
新しいAxis One-Clickカメラの登録 431
Axis One-Clickカメラの接続プロパティ 431
スマートマップを設定する 432
背景地図(説明付き) 432
Google MapsまたはBing MapsのAPIキーの取得 433
Google Maps 433
Bing Maps 433

Management ClientでBing MapsまたはGoogle Mapsを有効化 434
XProtect Smart ClientでBing MapsまたはGoogle Mapsを有効化 434
OpenStreetMapタイルサーバーの指定 435
キャッシュされたスマートマップファイル(説明付き) 435
スマートマップの編集を有効にする 436
スマートマップ上のカメラの編集を有効にする 437
カメラの位置、方向、視野、および深度を設定する(スマートマップ) 437
Milestone Federated Architectureとともにスマートマップを設定する。 439
メンテナンス 441
システム設定のバックアップおよび復元 441
システム設定のバックアップおよび復元について 441
共有バックフォルダーの選択 442
システム設定の手動バックアップ 442
システム設定の復元(手動バックアップから) 442
システム設定パスワード(説明付き) 443
システム設定パスワードの詳細 444
システム構成パスワードの設定変更 444
システム設定パスワードの設定入力(回復) 445
システム設定の手動バックアップについて(説明付き) 445
イベントサーバー構成のバックアップと復元について(説明付き) 446
システム設定のスケジュールされたバックアップと復元(説明付き) 446
スケジュールされたバックアップによるシステム設定のバックアップ 447
システム設定の復元(スケジュールされたバックアップから) 447
ログサーバーのSQLデータベースのバックアップ 448
バックアップ/復元の失敗と問題のシナリオについて(説明付き) 448
マネジメントサーバーの移動 448
マネジメントサーバーの利用不可(説明付き) 449
システム設定の移動 450
レコーディングサーバーの交換 450

ハードウェアの移動 451
ハードウェアの移動(ウィザード) 452
ハードウェアの交換 455
SQL Serverとデータベースの管理 458
SQL Serverとデータベースアドレスの変更(説明付き) 458
ログサーバーのSQL Serverとデータベースを変更 459
マネジメントサーバーとイベントサーバーのSQLアドレスを変更 459
サーバーサービスの管理 460
サーバーマネージャーのトレーアイコン(説明付き) 460
マネジメントサーバーサービスの開始または停止 462
レコーディングサーバーサービスの開始または停止 462
マネジメントサーバーまたはレコーディングサーバーのステータスメッセージの表示 463
暗号化の管理 - 方法:Server Configurator 463
イベントサーバーサービスの開始、停止、再開 464
イベントサーバーサービスの停止 465
Event ServerまたはMIPログの表示 465
登録済みサービスの管理 467
登録済みサービスの追加と編集 467
ネットワーク設定の管理 467
登録済みサービスのプロパティ 468
デバイスドライバの削除(説明付き) 468
レコーディングサーバーの削除 469
レコーディングサーバーでのすべてのハードウェアの削除 469
トラブルシューティング 470
問題:SQL Serverとデータベースのアドレスを変更するとデータベースにアクセスできなくなる 470
問題:ポートの競合が原因でレコーディングサーバーを起動できない 470
問題:レコーディングサーバーが、マネジメントサーバークラスタノードを切り替える際にオフラインになる 471
アップグレード 472
アップグレード(説明付き) 472

アップグレード要件 473
FIPS 140-2準拠モードで実行するようXProtect VMSをアップグレードする 474
アップグレードの推奨手順 475
ワークグループ設定内でのアップグレード 477
クラスタでのアップグレード 478

著作権、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

製品概要

XProtect VMS製品は多種多様なインストール用に設計された監視カメラ管理ソフトウェアです。お店を破壊行為から守りたい場合も複数の施設を管理したい場合も、XProtectがあれば可能です。このソリューションはすべてのデバイス、サーバー、およびユーザーを集中管理し、スケジュールとイベントによる非常に柔軟なルールシステムを提供します。

このシステムは、以下の主要な要素で構成されています。

- **Management Server**は、インストールの中心で、複数のサーバーで構成されています。
- 1つまたは複数の**Recording Server**
- **XProtect Management Client**の、1つ以上のインストール
- **XProtect Download Manager**
- **XProtect® Smart Client**の、1つ以上のインストール
- **XProtect Web Client**の1つ以上の使用および/または必要に応じて**XProtect Mobile**クライアントのインストール

また、このシステムには、監視システムの任意のカメラからXProtect Smart Clientをインストールした任意のコンピュータにビデオを配信表示することができる、統合的なMatrix機能があります。

システムは仮想サーバーまたは複数の物理的なサーバーに分散型設定でインストールできます。ページ29の分散型システム設定も参照してください。

さらに、このシステムには、XProtect Smart Clientからエビデンスビデオをエクスポートする際に、スタンドアロンのXProtect® Smart Client - Player を含めることも可能です。XProtect Smart Client - Playerを使うと、エビデンスビデオの受信者(警察官、内部/外部捜査官など)は、ソフトウェアをコンピュータにインストールしなくてもエクスポートされた録画を閲覧および再生することができます。

最も多機能な製品をインストールすれば(ページ46の製品比較チャートを参照)、ご利用中のシステムで無制限の数のカメラ、サーバー、およびユーザーを、必要に応じて複数のサイトで使用できます。IPv4に加えて、IPv6も処理できます。

メインシステムコンポーネント

マネジメントサーバー

マネジメントサーバーは監視カメラ管理ソフトウェアシステムの中心となるコンポーネントです。SQLデータベース内の監視システムの構成は、SQL Serverマネジメントサーバーコンピュータ本体、またはネットワーク上の別のSQL Serverに保存されます。また、ユーザーの認証、ユーザー権限、ルールシステムなども処理します。システムパフォーマンスを改善するために、複数のマネジメントサーバーを1つのMilestone Federated Architecture™として実行することができます。マネジメントサーバーはサービスと実行されるものであり、通常は専用サーバーにインストールされます。

ユーザーは初期認証のためにマネジメントサーバーに接続し、それからたとえばビデオ録画のためにレコーディングサーバーへと透過的に接続できます。

レコーディングサーバー

レコーディングサーバーは、ネットワークカメラやビデオエンコーダーと通信して、取得された音声および動画を記録した上で、ライブおよび記録された音声および動画へのアクセスをクライアントに提供します。また、レコーディングサーバーは、Milestone Interconnectテクノロジーを使って他のMilestone製品との通信も行います。

デバイスドライバー

- ネットワークカメラとビデオエンコーダーとの通信は、各デバイス専用に開発されたデバイスドライバー、または同じメーカーからの類似した複数のデバイス用のデバイスドライバーを通して行われます
- 2018 R1のリリースから、デバイスドライバーは2つのDevice Packに分けられます：より新しいドライバーを持つレギュラーDevice Packと、古いバージョンのドライバーを持つレガシーDevice Packです
- レギュラーDevice Packは、レコーディングサーバーをインストールする時に自動的にインストールされます。その後、新しいバージョンのDevice Packをダウンロード、およびインストールすることで、ドライバーを更新できます
- レガシーDevice Packは、システムがレギュラーDevice Packをインストール済みの場合のみ、インストールすることが可能です。前のバージョンが既にシステムにインストールされている場合は、レガシーDevice Packからのドライバーは、自動的にインストールされます。これはソフトウェアダウンロードページ（https://www.milestonesys.com/downloads/）から手動でダウンロードおよびインストールが可能です。

メディアデータベース

- 取得された音声および動画データは、レコーディングサーバーに保存されます。このカスタムメードの高パフォーマンスデータベースは、音声および動画データの録画と保管用に最適化されています。
- メディアデータベースは、多段階アーカイブ、ビデオ調整、暗号化、および録画への電子署名の追加など、さまざまな独自の機能をサポートしています

イベントサーバー

イベントサーバーは、イベント、アラーム、マップ、およびサードパーティ統合に関連するさまざまなタスクをMIP SDKを通じて処理します。

イベント

- すべてのシステムイベントがイベントサーバーに統合されるため、システムイベントを活用して統合を実行するパートナーは、場所とインターフェースを一元化できます
- また、イベントサーバーは、ジェネリックイベントまたはアナリティクスイベントインターフェースを通してシステムにイベントを送信するためのサードパーティアクセスを提供します

アラーム

- イベントサーバーは、アラーム機能、アラームロジック、アラーム状態をホストし、アラームデータベースを処理します。アラームデータベースは、マネジメントサーバーが使用するものと同じSQLデータベースに保存されます

マップ

- イベントサーバーは、XProtect Smart Clientで設定および使用されているマップもホストします

MIP SDK

- 最後に、システムイベントへのアクセスに使用する、サードパーティ製のプラグインをイベントサーバーにインストールすることができます

ログサーバー

ログサーバーには、SQLデータベース内でシステム全体に対して発せられたすべてのログメッセージが保存されます。このログメッセージSQLデータベースは、マネジメントサーバーのシステム構成SQLデータベースと同じSQL Serverか、または個別のSQL Serverに実装することができます。ログサーバーは通常、マネジメントサーバーと同じサーバーにインストールされますが、マネジメント/ログサーバーのパフォーマンス向上のため別のサーバーにインストールにインストールすることも可能です。

SQL Serverとデータベース

マネジメントサーバー、イベントサーバー、ログサーバーには、単一または複数のSQL ServerインストールのSQLデータベースに存在するシステム構成、アラーム、イベント/ログメッセージなどが保存されます。マネジメントサーバーとイベントサーバーは同じSQLデータベースを共有しますが、ログサーバーは独自のSQLデータベースを使用します。システムインストーラには、Microsoft SQL Server Express(SQL Serverの無料版)が含まれています。

Milestoneでは、大規模なシステムまたはSQLデータベースを行き来するトランザクションが多いシステムについては、ネットワーク上の専用コンピュータと、他の目的では使用されていない専用ハードディスクドライブでSQL ServerのMicrosoft® SQL Server® StandardまたはMicrosoft® SQL Server® Enterpriseエディションを使用するよう推奨しています。専用ドライブにSQL Serverをインストールすることで、全体的なシステムパフォーマンスが上がります。

モバイルサーバー

モバイルサーバーはXProtect MobileクライアントおよびXProtect Web Clientユーザーがシステムにアクセスできるようにします。

これら2種のクライアントのシステムゲートウェイとして機能するほか、オリジナルカメラのビデオストリームでは多くの場合、クライアントユーザーの帯域幅には大きすぎるため、モバイルサーバーはビデオのトランスコード(再エンコード)も行うことができます。

分散またはカスタムインストールを実行している場合、Milestoneは、モバイルサーバーを専用サーバーにインストールすることを推奨します。

Active Directory

Active Directoryは、Windowsドメインのネットワーク向けにMicrosoftが実装した分散型ディレクトリサービスです。これは、ほとんどのWindows Serverオペレーティングシステムに搭載されています。このサービスは、ユーザーやアプリケーションがアクセスできるネットワーク上のリソースを識別します。

Active Directoryがインストールされている場合は、Active DirectoryからWindowsユーザーを追加できますが、Active Directoryを使用せずに基本ユーザーを追加することもできます。基本ユーザーについては、特定のシステム制限があります。

Management Client (説明付き)

システムの設定や日常的な管理のための多機能マネジメントクライアントです。複数の言語で用意されています。

通常は、監視システムの管理者のワークステーションか同等の場所にインストールされます。

Management Clientの詳細については、ページ108のManagement Clientをナビゲーションを参照してください。

オプションのシステムコンポーネント

次のコンポーネントは使用する必須はありませんが、別の目的を達成するために追加できるコンポーネントです。

フェールオーバー 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は、レコーディングサーバーで障害が起こった場合、レコーディングタスクを引き継ぎます。

フェールオーバーレコーディングサーバーは2つのモードで操作されます。

- コールドスタンバイ - 複数のレコーディングサーバーをモニター
- ホットスタンドバイ - 単一のレコーディングサーバーをモニター

コールドフェールオーバーモードとホットスタンバイモードとの違いは、コールドスタンバイモードではフェールオーバー レコーディング サーバーはどのサーバーを引き継ぐか不明であり、このためレコーディングサーバーに故障が発生するまで開始できないということです。ホットスタンバイモードでは、フェールオーバー時間が大幅に短くなります。これはフェールオーバー レコーディングサーバーがどのレコーディングサーバーを引き継ぐかをすでに知っているためで、カメラ接続という最終手順を除けば、設定およびスタートアップを完全にあらかじめロードできるためです。

フェールオーバーマネジメントサーバー

マネジメントサーバーのフェールオーバーサポートは、MicrosoftWindowsClusterにマネジメントサーバーをインストールすることで実現できます。クラスタでは、最初のサーバーで障害が起こった場合、マネジメントサーバー機能を他のサーバーが引き継ぎます。

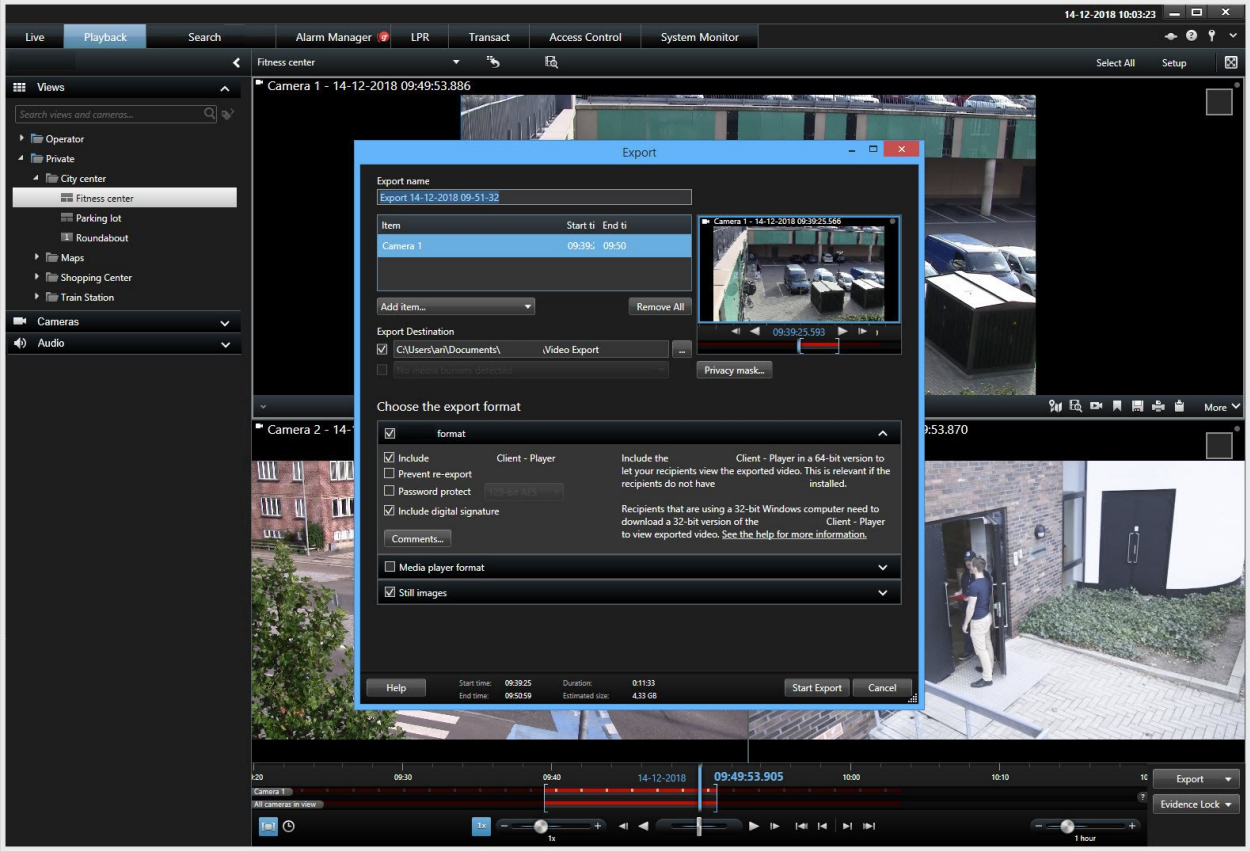
クライアント

システムのオペレータが使用する各種クライアントの紹介。

XProtect Smart Client (説明付き)

XProtect Smart Clientは、IP監視カメラの管理に役立つよう設計されたデスクトップ アプリケーションです。ライブおよび録画ビデオへのアクセス、カメラおよび接続済みセキュリティデバイスの即時コントロール、録画とメタデータの詳細検索能力をユーザーに与えることにより、セキュリティインストールに対する直感的なコントロールを提供します。

XProtect Smart Clientは適応力の高いユーザーインターフェースを、複数の言語で使用できます。各オペレータの作業に応じて最適化し、特定のスキルや権限レベルに応じて調節が可能です。



ライトやダークのテーマを選択することで、特定の任務環境のためにビューをカスタマイズすることをインターフェイスが許可します。また、作業用に最適化されたタブや、統合ビデオタイムラインによって、監視の操作が簡単になります。

MIP SDKを使用すると、さまざまなタイプのセキュリティおよびビジネスシステム、ビデオ分析アプリケーションを統合し、XProtect Smart Clientを介して管理できます。

XProtect Smart Clientはオペレーターのコンピュータにインストールされなければなりません。サーヴェイランスシステム管理者はManagement Clientを通じて、サーヴェイランスシステムへのアクセスを管理します。クライアントが表示する録画データは、XProtectシステムイメージサーバーのサービスによって配信されます。サービスは、監視システムサーバーのバックグランドで実行されます。別個のハードウェアは不要です。

XProtect Mobileクライアント(説明付き)

XProtect Mobileクライアントは、モバイル監視ソリューションで、XProtectシステムの他の部分と密接に統合されます。Androidタブレットまたはスマートフォン、あるいはApple®タブレット、スマートフォン、もしくはポータブル音楽プレーヤーで実行され、カメラへのアクセス権限を与え、管理 クライアントに設定された他の機能を表示します。

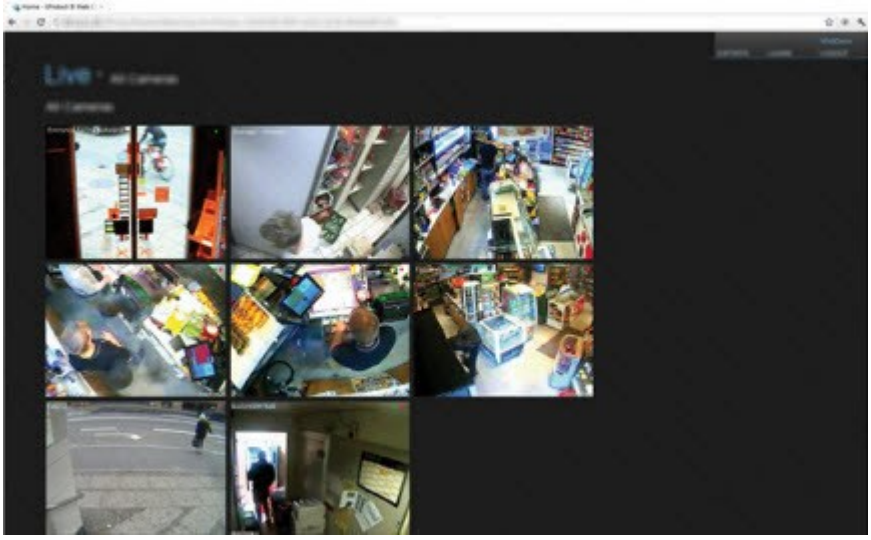
XProtect Mobileクライアントを使用して、複数のカメラのライブビューの確認および録画されたビデオの再生を行ったり、パン/チルト/ズーム(PTZ)カメラの制御や、出力やイベントを実行することができます。また、ビデオ配信機能を使用して、使用しているモバイルデバイスのビデオをXProtectシステムに送信します。

システムでXProtect Mobileクライアントを使用したい場合は、XProtect Mobileサーバーを追加して、XProtect Mobileクライアントと使用しているシステムの間での接続を確立する必要があります。XProtect Mobileサーバーが設定されたら、Google PlayまたはApp Storeから無料のXProtect Mobileをダウンロードし、XProtect Mobileの使用を開始します。

ビデオをXProtectシステムにプッシュ配信するデバイスごとに必要なデバイスライセンスは1つです。

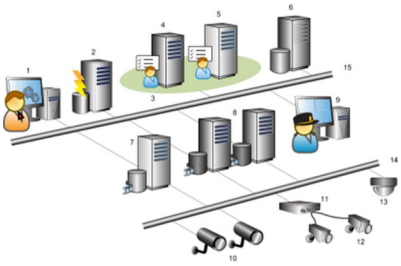
XProtect Web Client (説明付き)

XProtect Web ClientはWebベースのクライアントアプリケーションで、ビデオを表示、再生、共有できます。ライブビデオの表示、録画ビデオの再生、エビデンスの印刷やエクスポートなど、最も頻繁に使用される監視機能に瞬時にアクセスできます。どの機能にアクセスできるかは、Management Clientで設定した個々のユーザー権限によって異なります。



XProtect Web Clientへのアクセスを有効にするには、XProtect Mobileサーバーをインストールして、XProtect Web Clientと、使用しているシステムの間での接続を確立する必要があります。XProtect Web Client自体はインストールを必要とせず、大半のインターネットブラウザで動作します。XProtect Mobileサーバーを設定したら、インターネットアクセスが可能なコンピュータやタブレットで、どこからでも(適切な外部/インターネットアドレス、ユーザー名およびパスワードが分かっていることが必要) XProtectシステムを監視することができます。

分散型システム設定



分散型システム設定の例。カメラおよびレコーディングサーバーの数と、接続できるクライアントの数は、必要なだけ増やすことができます。

凡例：

1. Management Client(s)
2. イベントサーバー
3. Microsoft Cluster
4. マネジメントサーバー
5. フェールオーバーマネジメントサーバー
6. SQL Serverを備えたサーバー

7. フェールオーバーレコーディングサーバー
8. レコーディングサーバー
9. XProtect Smart Client(s)
10. IPビデオカメラ
11. ビデオエンコーダ
12. アナログカメラ
13. PTZ IPカメラ
14. カメラのネットワーク
15. サーバーのネットワーク

アドオン製品

Milestoneは、追加機能を提供するため、完全にXProtectを統合したアドオン製品を開発しました。アドオン製品へのアクセスは、ソフトウェアライセンスコード(SLC)によって制御されます。

XProtect Access (説明付き)

> XProtect Accessを使用する場合、XProtectシステムでこの機能の使用を許可する基本ライセンスを購入しておく必要があります。また、制御する各ドア用の入退室管理ドアライセンスも必要です。

> XProtect Accessに対するベンダー固有のプラグインが存在するベンダーからの入退室管理システムで、XProtect Accessを使用することができます。

入退室管理統合機能には、XProtectとお客様の入退室管理システムを簡単に統合できる新機能が含まれています。特長：

- XProtect Smart Client内の複数の入退室管理システムを操作できる共通のユーザーインターフェース。
- 入退室管理システムをより素早く強力に統合
- オペレータ向けに追加された機能(以下を参照)。

XProtect Smart Clientでは、オペレータは以下の機能を使用できます。

- アクセスポイントでのイベントのライブ監視
- オペレータによるアクセスリクエストの受理
- マップの統合

- 入退室管理イベントのアラーム定義
- アクセスポイントでのイベントの調査
- ドアの状態の一元化された概要とコントロール
- カードホルダー情報と管理

監査ログは、XProtect Smart Clientからの入退室管理システムで各ユーザーが実行するコマンドを記録します。

統合を開始するには、XProtect Access基本ライセンス以外にも、ベンダー特有の統合プラグインがイベントサーバーにインストールされている必要があります。。

XProtect LPR (説明付き)

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 LPRは、ビデオベースのコンテンツ分析(VCA)および、監視システムやXProtect Smart Clientでインタラクティブに利用できる車両のナンバープレート認識を提供します。

プレートの文字を読み取るために、XProtect LPRは、特殊なカメラ設定による画像の光学的文字認識を使用します。

ナンバープレート認識(LPR)を、録画やイベントベースの出力の起動などの他の監視機能と組み合わせることもできます。

XProtect LPRでのイベントの例：

- 特定の品質での監視システムによる録画のトリガー
- アラームの有効化
- ポジティブ/ネガティブなナンバープレート一致リストとの照合
- ゲートを開く
- ライトを点灯
- インシデントのビデオを、特定のセキュリティスタッフメンバーのコンピュータ画面へプッシュ
- 携帯電話へのテキストメッセージ送信

イベントで、XProtect Smart Clientのアラームを有効にできます。

XProtect Smart Wall (説明付き)

> 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 Smart Wallは高度なアドオンツールです。組織で特有のセキュリティ要件を満たすことのできるビデオウォールを作成できるようになります。Smart Wallは、VMS[1]システム内のすべてのビデオデータの概要を提供します。概要は複数のオペレータ間で共有できます。

XProtect Smart Wallでは、オペレータはXProtect Smart Clientで利用できるほぼすべてのコンテンツタイプ(ビデオ、画像、テキスト、アラーム、スマートマップなど)を共有できます。

最初に、XProtect Management Clientでシステム管理者がXProtect Smart Wallを構成します。これにはSmart Wallのレイアウトとカメラを各種モニターに分散する方法をコントロールするプリセットが含まれます。XProtect Smart Clientでオペレータは、各種プリセットを適用することでSmart Wallに表示する内容を変更できます。表示の変更は、自動的にプリセットを変更させる機能を持つ「ルール」を用いて制御することもできます。

Smart Wall概要では、オペレータは簡単なドラッグ&ドロップ操作で特定のコンテンツまたはビュー全体をSmart Wallモニターに追加できます。

XProtect Transact (説明付き)

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 Transactは、MilestoneのIPビデオ監視ソリューションへのアドオンです。

XProtect Transactは実行中のトランザクションを監視し、過去のトランザクションを調査するためのツールです。トランザクションは、詐欺を証明したり、犯人のエビデンスを提示したりするためなどに、トランザクションを監視するデジタル監視動画にリンクしています。トランザクションラインと動画画像の間には1対1の関係があります。

トランザクションデータは、さまざまなタイプのトランザクションソースから発生します。一般的には、POSシステムやATMなどです。

[1]「ビデオマネジメントソフトウェア」の短縮形

Milestone Open Network Bridge (説明付き)

ONVIFは、IPビデオ製品監視が安全かつ基準に沿って機能するためのオープンでグローバルなフォーラムです。その目的は、ビデオデータの交換を容易にすることです。例えば、警察、監視センター、あるいは同様な機関がIPベースの監視システムで流れたライブまた記録ビデオに迅速にアクセスできます。

Milestone Systemsは、この目的を支援したいと考え、Milestone Open Network Bridgeを開発しました。Milestone Open Network BridgeはMilestoneオープンプラットホームの一部であり、Milestoneの動画管理ソフトウェア製品からからライブまた録音されたビデオを取得させるためのONVIFの部分をサポートするインターフェースを提供しています。

このドキュメントは次の内容です。

- ONVIF基準と参考マテリアルへのリンクに関する情報
- XProtect VMS製品におけるMilestone Open Network Bridgeのインストールと構成方法
- 様々なタイプのONVIFクライアントがXProtect VMS製品からライブまた録画ビデオをストリームする方法の例

XProtect DLNA Server (説明付き)

DLNA(Digital Living Network Alliance) はマルチメディアデバイスの接続基準です。電子デバイスの製造者はさまざまなベンダーやデバイスの間で相互運用ができるように、そして音声やビデオ、写真などのマルチメディアコンテンツを配信できるように、自社製品のDLNA認定を受けます。

一般表示やテレビの内容はDLNA認定を受けており、ネットワークに接続されています。メディアコンテンツのネットワークをスキャンしたり、デバイスに接続したり、メディアストリームが組み込みメディアプレーヤーにリスエストしたりできます。XProtect DLNA Serverは特定のDLNA認定デバイスで検出でき、選択されたカメラからメディアプレーヤー付きDLNA認定デバイスにライブでビデオストリームを配信できます。

> DLNAデバイスには、1～10秒のライブビデオ遅延があります。これはデバイスのバッファサイズが異なることによって引き起こされます。

XProtect DLNA ServerはXProtectシステムと同じネットワークに接続されている必要があり、DLNAデバイスはXProtect DLNA Serverと同じネットワークに接続されている必要があります。

このシステムで使用するポート

これらが必要とするXProtectコンポーネントとポートのすべてを以下に記します。ファイアウォールが不必要なトラフィックのみをブロックするなど、システムが使用するポートを指定する必要があります。これらのポートのみを有効にします。リストにはローカルプロセスで使用するポートも含んでいます。

次の2つのグループに調整されています。

- サーバーコンポーネント(サービス) は特定ポートのサービスを提供しますので、これらポートについてのクライアントの要求を聞く必要があります。よって、これらのポートは着信 / 送信接続のためWindowsファイアウォールで開いておく必要があります。
- クライアントコンポーネント(クライアント) はサーバーコンポーネントの特定ポートに接続を開始します。よって、これらのポートは発信接続のために開く必要があります。発信接続は一般的に、デフォルトでWindowsファイアウォールで開かれています。

何も言及されていない場合は、サーバーコンポーネントのポートは着信接続のために開き、クライアントコンポーネントのポートは発信接続のために開く必要があります。

サーバーのコンポーネントは他のサーバー コンポーネントに対してクライアントのように機能する点に留意してください。この文書では明示的に記載されていません。

ポート番号はデフォルト番号ですが、変更できます。Management Clientで構成できないポートを変更する必要がある場合は、Milestoneサポートまでお問い合わせください。

サーバーコンポーネント(着信接続)

次の各セクションでは特定サービスで開く必要あるポートを記載しています。特定コンピュータで開けておく必要があるポートを見つけるためには、このコンピュータで実行しているすべてのサービスを考慮する必要があります。

マネジメントサーバーサービスと関連プロセス

ポート番号	プロトコル	プロセス	接続元	目的
80	HTTP	IIS	すべてのXProtectコンポーネント マネジメントサーバーサービスとレコーディングサーバーサービス	認証や構成などの主な通信 IDPによるレコーディング サーバーと管理サーバーの登録。
443	HTTPS	IIS	XProtect Smart Clientおよび Management Client	基本ユーザーの認証。
6473	TCP	マネジメントサーバーサービス	Management Server Manager トレイアイコン、ローカル接続のみ。	状況の表示とサービスの管理。
8080	TCP	マネジメントサーバー	ローカル接続のみ。	サーバー上の内部プロセス間の通信。
9000	HTTP	マネジメントサーバー	レコーディングサーバーサービス	サーバー間の内部コミュニケーション用Webサービスです。

ポート番号	プロトコル	プロセス	接続元	目的
12345	TCP	マネジメントサーバーサービス	XProtect Smart Client	システムとMatrix受信者の間の通信。 Management Clientのポート番号は変更できます。
12974	TCP	マネジメントサーバーサービス	Windows SNMPサービス	SNMP拡張エージェントとの通信。 システムがSNMPを適用しない場合でも、他の目的でこのポートを使用しないでください。 XProtect 2014 システム以前のポート番号は6475でした。 XProtect 2019 R2システム以前のポート番号は7475でした。

SQL Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
1433	TCP	SQL Server	マネジメントサーバーサービス	構成の保存と取得。
1433	TCP	SQL Server	イベントサーバーサービス	イベントの保存と取得
1433	TCP	SQL Server	ログサーバーサービス	ログエントリの保存と取得。

Data Collectorサービス

ポート番号	プロトコル	プロセス	接続元	目的
7609	HTTP	IIS	マネジメントサーバーコンピューター上：他の全サーバー上のData Collectorサービス。 その他のコンピューター上：マネジメントサーバー上のData Collectorサービス。	システムモニター。

イベントサーバーサービス

ポート番号	プロトコル	プロセス	接続元	目的
1234	TCP/UDP	イベントサーバーサービス	XProtectシステムにジェネリックイベントを送信するサーバーすべて。	外部システムまたはデバイスからのジェネリックイベントをリスンします。 関連のデータソースが有効な場合のみ。
1235	TCP	イベントサーバーサービス	XProtectシステムにジェネリックイベントを送信するサーバーすべて。	外部システムまたはデバイスからのジェネリックイベントをリスンします。 関連のデータソースが有効な場合のみ。
9090	TCP	イベントサーバーサービス	XProtectシステムにアナリティクスイベントを送信するすべてのシステムまたはデバイス。	外部システムまたはデバイスからのアナリティクスイベントをリスンします。 アナリティクスイベント機能が有効な場合のみ関連。
22331	TCP	イベントサーバーサービス	XProtect Smart Client および Management Client	構成、イベント、アラーム、およびマップデータ。
22333	TCP	イベントサーバーサービス	MIPプラグインおよびアプリケーション。	MIP メッセージング。

レコーディングサーバーサービス

ポート番号	プロトコル	プロセス	接続元	目的
25	SMTP	レコーディ	カメラ、エンコーダー、および I/O デバイ	デバイスからのイベントメッセージをリスンします。 このポートはデフォルトでは無効になってい

ポート番号	プロトコル	プロセス	接続元	目的
		ングサーバーサービス	ス。	ます。
5210	TCP	レコーディングサーバーサービス	フェールオーバーレコーディング サーバー。	フェールオーバー レコーディング サーバーが実行された後のデータベースの統合。
5432	TCP	レコーディングサーバーサービス	カメラ、エンコーダー、および I/O デバイス。	デバイスからのイベントメッセージをリスンします。 このポートはデフォルトでは無効になっています。
7563	TCP	レコーディングサーバーサービス	XProtect Smart Client, Management Client	ビデオおよび音声ストリーム、PTZ コマンドの取得。
8966	TCP	レコーディング	Recording Server Manager トレイアイコン、ローカル接続	状況の表示とサービスの管理。

ポート番号	プロトコル	プロセス	接続元	目的
		サーバーサービス	のみ。	
9001	HTTP	レコーディングサーバーサービス	マネジメントサーバー	サーバー間の内部コミュニケーション用Webサービスです。 複数のレコーディングサーバーインスタンスが使用されている場合は、それぞれのインスタンスに独自のポートが必要です。追加ポートは9002、9003、などとなります。
11000	TCP	レコーディングサーバーサービス	フェールオーバーレコーディングサーバー	レコーディングサーバーのステータスのポーリング。
12975	TCP	レコーディングサーバーサービス	Windows SNMP サービス	SNMP拡張エージェントとの通信。 システムがSNMPを適用しない場合でも、他の目的でこのポートを使用しないでください。 XProtect 2014システム以前では、ポート番号は6474でした。 XProtect 2019 R2システム以前のポート番号は7474でした。
65101	UDP	レコーディング	ローカル接続のみ	ドライバーからのイベント通知をリスンします。

ポート番号	プロトコル	プロセス	接続元	目的
		サーバーサービス		

上記のレコーディングサーバーサービスに加えて、レコーディングサーバーはカメラ、NVR、リモート相互接続サイト(Milestone Interconnect ICP)への送信接続も設定します。

フェールオーバーサーバーサービスと**Failover Recording Server**サービス

ポート番号	プロトコル	プロセス	接続元	目的
25	SMTP	Failover Recording Serverサービス	カメラ、エンコーダー、およびI/Oデバイス。	デバイスからのイベントメッセージをリスンします。 このポートはデフォルトでは無効になっています。
5210	TCP	Failover Recording Serverサービス	フェールオーバー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が実行された後のデータベースの統合。
5432	TCP	Failover Recording Serverサービス	カメラ、エンコーダー、およびI/Oデバイス。	デバイスからのイベントメッセージをリスンします。 このポートはデフォルトでは無効になっています。
7474	TCP	Failover Recording Serverサービス	Windows SNMPサービス	SNMP拡張エージェントとの通信。 システムがSNMPを適用しない場合でも、他の目的でこのポートを使用しないでください。

ポート番号	プロトコル	プロセス	接続元	目的
7563	TCP	Failover Recording Serverサービス	XProtect Smart Client	ビデオおよび音声ストリーム、PTZ コマンドの取得。
8844	UDP	Failover Recording Serverサービス	ローカル接続のみ。	2つのサーバーの間の通信。
8966	TCP	Failover Recording Serverサービス	Failover Recording Server Managerトレイアイコン、ローカル接続のみ。	状況の表示とサービスの管理。
8967	TCP	フェールオーバーサーバーサービス	Failover Server Managerトレイアイコン、ローカル接続のみ。	状況の表示とサービスの管理。
8990	TCP	フェールオーバーサーバーサービス	マネジメントサーバーサービス	フェールオーバーサーバーサービスのステータスをモニター。
9001	HTTP	フェールオーバーサーバーサービス	マネジメントサーバー	サーバー間の内部コミュニケーション用Webサービスです。

上記のフェールオーバーサーバー / Failover Recording Serverサービスへの受信接続に加えて、フェールオーバーサーバー / Failover Recording Server サービスは、通常のレコーダー、カメラ、ビデオプッシュ向けに送信接続を確立します。

ログサーバーサービス

ポート番号	プロトコル	プロセス	接続元	目的
22337	HTTP	ログサーバーサービス	XProtectおよびレコーディングサーバーを除く、すべてのManagement Clientコンポーネント。	ログサーバーの書き込み、読み取り、構成を行います。

モバイルサーバーサービス

ポート番号	プロトコル	プロセス	接続元	目的
8000	TCP	モバイルサーバーサービス	Mobile Server Managerトレイアイコン、ローカル接続のみ。	SysTrayアプリケーション。
8081	HTTP	モバイルサーバーサービス	Mobileクライアント、Webクライアント、およびManagement Client。	ビデオや音声などデータストリームの送信。
8082	HTTPS	モバイルサーバーサービス	MobileクライアントおよびWebクライアント。	ビデオや音声などデータストリームの送信。
40001 - 40099	HTTP	モバイルサーバーサービス	レコーディングサーバーサービス	モバイルサーバービデオプッシュ。 このポート範囲はデフォルトでは無効になっています。

LPRサーバーサービス

ポート番号	プロトコル	プロセス	接続元	目的
22334	TCP	LPRサーバーサービス	イベントサーバー	認証されたナンバープレートとサーバー状況の取得。 接続するためには、イベントサーバーにはLPRプラグインがインストールされている必要があります。
22334	TCP	LPRサーバーサービス	LPR Server Managerトレイアイコン、ローカル接続のみ。	SysTrayアプリケーション

Milestone Open Network Bridgeサービス

ポート番号	プロトコル	プロセス	接続元	目的
580	TCP	Milestone Open Network Bridgeサービス	ONVIFクライアント	ビデオストリーム構成の認証と要求
554	RTSP	RTSPサービス	ONVIFクライアント	ONVIFクライアントへの要求ビデオのストリーミング。

XProtect DLNA Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
9100	HTTP	DLNAサーバーサービス	DLNAデバイス	デバイス検出およびDLNAチャネル構成の提供。ビデオストリームの要求。
9200	HTTP	DLNAサーバーサービス	DLNAデバイス	DLNAデバイスへの要求ビデオのストリーミング。

XProtect Screen Recorderサービス

ポート番号	プロトコル	プロセス	接続元	目的
52111	TCP	XProtect Screen Recorder	レコーディングサーバーサービス	モニターからビデオの提供。録画サーバー上にカメラと同じように表示され、機能します。 Management Clientのポート番号は変更できます。

サーバーコンポーネント(送信接続)

マネジメントサーバーサービス

ポート番号	プロトコル	接続先	目的
443	HTTPS	ライセンス管理サービスをホストするライセンスサーバー。コミュニケーションは https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx を通じて行われます。	ライセンスのアクティベーション

サーバー サービス

ポート番号	プロトコル	接続先	目的
80	HTTP	レコーディング サーバーとフェールオーバー レコーディング サーバー	ビデオと音声の認証、構成、およびデータストリーム。
443	HTTPS	レコーディング サーバーとフェールオーバー レコーディング サーバー	ビデオと音声の認証、構成、およびデータストリーム。
554	RTSP	レコーディング サーバーとフェールオーバー レコーディング サーバー	ビデオと音声のデータストリーム。
11000	TCP	フェールオーバーレコーディングサーバー	レコーディングサーバーのステータスのポーリング。
40001 – 40099	HTTP	モバイル サーバー サービス	モバイル サーバー ビデオプッシュ。 このポート範囲はデフォルトでは無効になっています。

フェールオーバーサーバーサービスとFailover Recording Serverサービス

ポート番号	プロトコル	接続先	目的
11000	TCP	フェールオーバーレコーディングサーバー	レコーディングサーバーのステータスのポーリング。

イベントサーバーサービス

ポート番号	プロトコル	接続先	目的
443	HTTPS	Milestone Customer Dashboard 経由 https://service.milestonesys.com/	XProtectシステムからMilestone Customer Dashboardへステータス、イベント、エラーメッセージを送信。

ログサーバーサービス

ポート番号	プロトコル	接続先	目的
443	HTTP	ログサーバー	メッセージをログサーバーに転送します。

カメラ、エンコーダー、I/Oデバイス(着信接続)

ポート番号	プロトコル	接続元	目的
80	TCP	レコーディングサーバーとフェールオーバーレコーディングサーバー	ビデオと音声の認証、構成、およびデータストリーム。
443	HTTPS	レコーディングサーバーとフェールオーバーレコーディングサーバー	ビデオと音声の認証、構成、およびデータストリーム。
554	RTSP	レコーディングサーバーとフェールオーバーレコーディングサーバー	ビデオと音声のデータストリーム。

カメラ、エンコーダー、I/Oデバイス(送信接続)

ポート番号	プロトコル	接続先	目的
25	SMTP	レコーディングサーバーとフェールオーバーレ	イベント通知の送信(使用され

ポート番号	プロトコル	接続先	目的
		コーディング サーバー	ていません)
5432	TCP	レコーディング サーバーとフェールオーバー レコーディング サーバー	イベント通知の送信。 このポートはデフォルトでは無効になっています。
22337	HTTP	ログサーバー	メッセージをログサーバーに転送します。

発信接続が確立できるカメラは数種のモデルのみです。

クライアントコンポーネント(発信接続)

XProtect Smart Client、**XProtect Management Client**、**XProtect Mobile**サーバー

ポート番号	プロトコル	接続先	目的
80	HTTP	マネジメントサーバーサービス	認証
443	HTTPS	マネジメントサーバーサービス	基本ユーザーの認証。
7563	TCP	レコーディングサーバーサービス	ビデオおよび音声ストリーム、PTZ コマンドの取得。
22331	TCP	イベントサーバーサービス	アラーム。

XProtect Web Client、**XProtect Mobile** クライアント

ポート番号	プロトコル	接続先	目的
8081	HTTP	XProtect Mobileサーバー	ビデオおよび音声ストリームの取得。
8082	HTTPS	XProtect Mobileサーバー	ビデオおよび音声ストリームの取得。

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(ソフトウエ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ティング / アダプティブストリーミング	-	-	-	✓	✓
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	クライアントのユーザー	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/

名前	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
	権限	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			✓	✓	✓

ライセンス

ライセンス(説明付き)

XProtect Essential+システムをダウンロードして登録すれば、システムを作動させ、8種のデバイスライセンスを無料で使用できます。自動ライセンスアクティベーションに対応しているため、ハードウエアはシステムに追加するだけで起動します。このトピックの残りの部分と他のライセンス関連のトピックは、より上位のXProtect製品にアップグレードする場合にのみお読みください(ページ50のソフトウェアライセンスコードの変更を参照)。

ソフトウェアとライセンスを購入すると、次のものを受け取ります。

- 注文確認書
- ソフトウェアライセンスファイルは、.lic拡張子とSLC (ソフトウェアライセンスコード)に基づく名前が付いています。

SLCは注文確認書にも記載され、次のようにハイフンで区切られた数字と文字から構成されています。

- 製品バージョン2014以前:xxx-xxxx-xxxx
- 製品バージョン2016以降:xxx-xxx-xxx-xx-xxxxxx

貴方が購入したVMS製品とライセンスについての全情報は、ソフトウエア・ライセンス・ファイルで見られます。Milestone貴方のSLC情報とソフトウエア・ライセンスの写しを、再度見られるように安全に場所に保存することをお勧めします。ナビゲーションツリーで、[基本]>[ライセンス情報]を選択すると、SLCも確認することができます。My Milestoneユーザーアカウントの作成、リセラーへのサポート問い合わせ、システムを変更する必要がある場合などには、ソフトウェアライセンスファイルまたはSLCが必要になる場合があります。

まず、Webサイト(https://www.milestonesys.com/downloads/) からソフトウェアをダウンロードします。ソフトウェアのインストール(ページ76の新しいXProtectシステムのインストールを参照)中に、ソフトウェアライセンスファイルが求められます。

インストールが完了し、ライセンスをアクティベートすると、同じSLCのインストールすべてのライセンス概要を表示できます。[基本] > [ライセンス情報]ページを選択してください。

少なくとも2つのライセンスを購入しています。

基本ライセンス: 少なくとも、XProtect製品のいずれか1つの基本ライセンスをお持ちです。XProtectアドオン製品には1つ以上の基本ライセンスをお持ちの場合もあります。

ハードウェアデバイスライセンス: XProtectシステムに追加するすべてのハードウェアデバイスには、デバイスライセンスが必要です。カメラに接続されたスピーカー、マイク、または入出力デバイスのデバイスライセンスは不要です。複数のカメラをビデオエンコーダーに接続している場合でも、必要なハードウェアデバイスライセンスはビデオエンコーダーIPアドレスにつき1つだけです。ビデオエンコーダーには1つ以上のIPアドレスがある場合があります。

詳細については、Milestone Webサイト(https://www.milestonesys.com/supported-devices/) で、サポートされるハードウェア一覧を参照してください。XProtect Mobileでビデオプッシュ機能を使用する場合は、システムにビデオをプッシュするモバイルデバイスまたはタブレットごとに1つのデバイスライセンスも必要です。もし、デバイスライセンスが不足している場合は、あまり重要でないハードウエアを無効にする(ページ185のハードウェアの有効化/無効化を参照)ことにより、新しいハードウェアデバイスを代わりに実行できます。

お使いの監視システムがMilestone Interconnectを使用したより大きいシステム階層の中央サイトである場合は、リモートサイトのハードウェアデバイスからビデオを見るするために、Milestone Interconnectカメラライセンスが必要です。XProtect Corporateのみが中央サイトとして動作できます。

ほとんどのXProtectアドオン製品には追加のライセンスタイプが必要です。ソフトウェアライセンスファイルには、アドオン製品のライセンスの情報も含まれています。一部のアドオン製品には、個別のソフトウェアライセンスファイルがあります。

ソフトウェアライセンスコードの変更

第一期の最中に一時ソフトウェアライセンスコード(SLC) でインストールを実行した場合、またはより上位のXProtect製品にアップグレードした場合、新しいソフトウェアライセンスファイルを受け取った際に、アンインストールまたは再インストールなしにSLCを変更することができます。

これはマネジメントサーバーでローカルに行う必要があります。でこれを実行することはできませんManagement Client。

1. マネジメントサーバーで、タスクバーの通知エリアへ移動します。

2. マネジメントサーバーアイコンを右クリックし、ライセンスの変更を選択します。
3. ライセンスのインポートをクリックします。
4. 次に、この目的で保存したソフトウェアライセンスファイルを選択します。完了すると、ライセンスの[ライセンスのインポート]ボタンのすぐ下に、選択したソフトウェアライセンスファイルの場所が追加されます。
5. OKをクリックします。SLCを登録する準備ができました。ページ66のソフトウェアライセンスコードを登録するを参照してください。

要件と注意事項

サマータイム(説明付き)

夏時間 (DST) は、夕方の日照時間を長く、朝の日照時間を短くするために、時計を進める制度です。DSTの使用は、国/地域によって異なります。

監視システムでの作業では、本質的に時間が重要であるため、システムがどのようにDSTに対応するかを知っておくことが重要です。

> ⚠ DST期間中、またはDST期間の録画がある場合は、DST設定を変更しないでください。

春:標準時間からDSTへ切り替える

標準時間からDSTへの変更は、時計を1時間進めるのであまり問題ではありません。

例:

時計は02:00(標準時間)から03:00(DST)へと進められるので、その日は23時間となります。その場合、その朝の02:00から03:00の間にデータはありません。その日にはその時間は存在しなかったためです。

秋:DSTから標準時間へ切り替える

秋にDSTから標準時間へ切り替えるとき、時計を1時間戻します。

例:

時計は02:00(DST)から01:00(標準時間)に戻されるので、その日は25時間となります。この場合、01:59:59になると、その後すぐに01:00:00に戻ります。システムが応答しなかった場合、基本的にはその時間を再録画します。たとえば、最初の01:30は、2回目の01:30によって上書きされます。

この問題が発生しないようにするために、システム時刻が5分以上変更された場合、現在のビデオがアーカイブされます。クライアントでは01:00時間の最初の発生を直接表示できませんが、データは録画され、安全です。XProtect Smart Clientでこのビデオを参照するには、アーカイブされたデータベースを直接開きます。

タイムサーバ(説明付き)

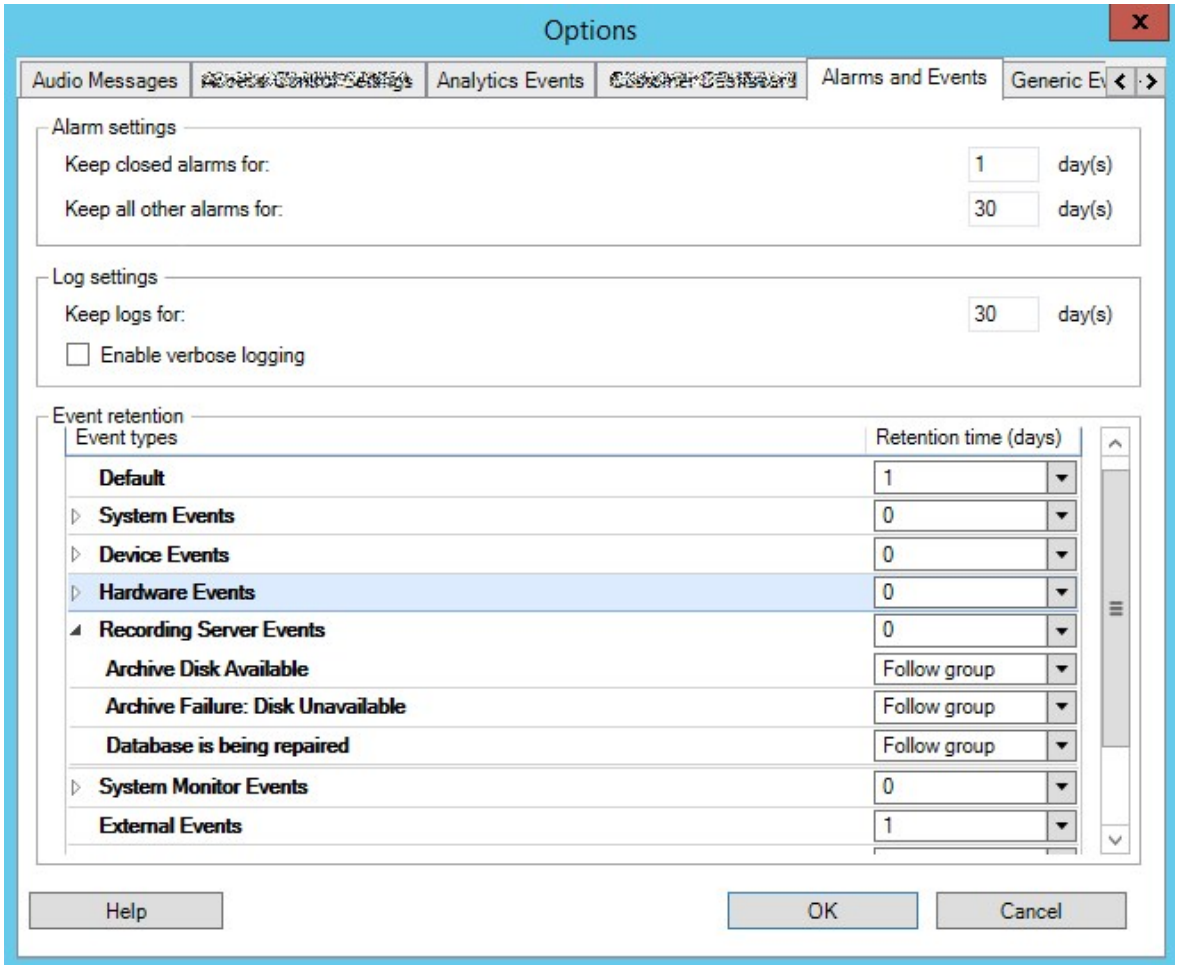
システムが画像を受信すると、ただちにタイムスタンプが付けられます。カメラは別個のユニットであり、別個のタイミングデバイスを持っているので、カメラの時刻と使用しているシステムの時刻が完全に一致していないことがあります。これが混乱の原因になる場合があります。カメラがタイムスタンプをサポートしている場合、Milestoneでは、一貫性のある同期を行うために、タイムサーバーによってカメラとシステムの時刻を自動同期することを推奨しています。

タイムサーバーの構成に関する詳細は、MicrosoftのWebサイト(https://www.microsoft.com/)で「タイムサーバー」、「タイムサービス」、または類似のトピックを検索してください。

データベースのサイズを制限

SQLデータベース(「ページ25のSQL Serverとデータベース」を参照) のサイズが、システムのパフォーマンスに影響が及ぶほど増大するのを防ぐため、各種イベントとアラームを何日間データベースに保存するかを指定できます。

1. [ツール] メニューを開きます。
2. [オプション] > [アラームとイベント] タブをクリックします。



3. 必要な設定を行います。詳細については、「ページ125の[アラームおよびイベント]タブ(オプション) 」を参照してください。

Ipv6 および Ipv4 (説明付き)

システムでは、IPv6とIPv4がサポートされています。XProtect Smart Clientでも同様 。

IPv6はインターネットプロトコル(IP)の最新バージョンです。インターネットプロトコルは、形式とIPアドレスの使用を決定します。IPv6は、依然としてより広く使用されているIPバージョンIPv4と共存しています。IPv6は、IPv4のアドレス枯渇を解決するために開発されました。IPv4アドレスは32ビット長であるのに対し、IPv6アドレスは128ビットの長さです。

つまりインターネットのアドレス帳の一意アドレスの数が43億から340澗(10の34乗)へ増えたという意味です。増大係数は79000 (10の27乗)。? (10の27乗)。増大係数は79000? (10の27乗)大係数は79000? (10の27乗)。

ますます多くの組織が、ネットワークにIPv6を実装しています。たとえば、すべての米国連邦機関のインフラストラクチャは、IPv6準拠である必要があります。このマニュアルに記載されている例および図は、現在も最も一般的に使用されているIPバージョンである、IPv4の使用を反映しています。IPv6も同様に問題なく動作します。

Ipv6 でのシステムの使用 (説明付き)

システムでIPv6を使用する場合は、次の条件が適用されます。

サーバー

サーバーでは、IPv4に加えて、IPv6もよく使用されます。ただし、システム内の1つのサーバーのみ(例：マネジメントサーバー、レコーディングサーバー) で特定のIPバージョンが必要とされる場合、システム内のすべての他のサーバーが、同じIPバージョンを使用して通信しなければなりません。

例：システム内のすべてのサーバー(1つを除く) は、IPv4とIPv6の両方を使用できます。例外は、IPv6のみ使用できるサーバーです。これは、すべてのサーバーがIPv6を使用して相互に通信する必要があることを意味します。

デバイス

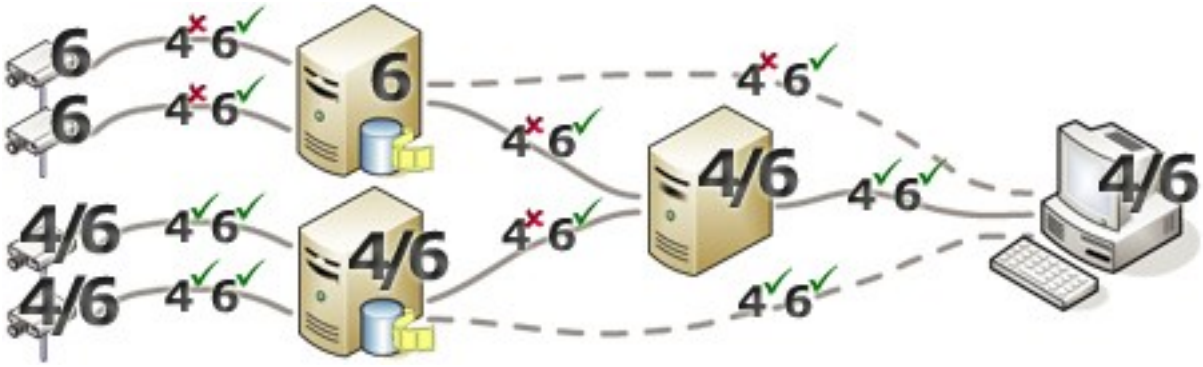
ネットワーク設備と対象のレコーディングサーバーでもデバイスのIPバージョンがサポートされていれば、サーバー通信で使用されているIPバージョンとは異なるIPバージョンのデバイス(カメラ、入力、出力、マイク、スピーカー) を使用できます。下記の図も参照してください。

クライアント

お使いのシステムがIPv6を使用している場合、ユーザーはXProtect Smart Clientを使用して接続する必要があります。XProtect Smart Clientは、IPv4だけではなくIPv6もサポートします。

システム内の1つ以上のサーバーがIPv6だけしか使用できない場合は、XProtect Smart Clientユーザーは、他のサーバーとの通信にIPv6を使用しなければなりません。このようなケースでは、XProtect Smart Clientのインストールは厳密には最初の認証のためにマネジメントサーバーに接続し、その後録画にアクセスするために必要なレコーディングサーバーに接続することに注意してください。

ただし、ネットワーク設備で異なるIPバージョン間の通信がサポートされており、コンピュータ上にIPv6プロトコルがインストールされている場合、XProtect Smart ClientユーザーはIPv6ネットワーク上にある必要はありません。図も参照してください。クライアントコンピュータにIPv6をインストールするには、コマンドプロンプトを開き、「*Ipv6 install*」と入力して[ENTER]を押します。
図例



例：システム内の1つのサーバーが、IPv6のみを使用しているため、そのサーバーとのすべての通信で、IPv6を使用する必要があります。ただし、そのサーバーはシステム内のすべての他のサーバー間の通信に使用されるIPバージョンも決定します。

との互換性なしMatrix Monitor

IPv6を使用している場合、お使いのシステムでMatrix Monitorアプリケーションを使用できません。XProtect Smart ClientのMatrix機能は影響を受けません。

Ipv6アドレスの書き方(説明付き)

IPv6のアドレスは通常、4つの16進数から成るブロック8つで記述され、各ブロックがコロンで分離されています。

例：*2001:0B80:0000:0000:0000:0F80:3FA8:18AB*

アドレスは、ブロック内の先頭のゼロを削除することで、短縮できます。4桁のブロックの一部は、ゼロのみで構成されている場合もあることに注意してください。0000ブロックなどの番号が連続している場合、そのアドレスは、0000ブロックを2つのコロンに置き換えることによって短縮できます(アドレス内にそのような2つのコロンが1つだけである場合)。

例：

例：*2001:0B80:0000:0000:0000:0F80:3FA8:18AB*は、次のように短縮できます。

2001:B80:0000:0000:0000:F80:3FA8:18AB 先頭のゼロを削除した場合、または

*2001:0B80::0F80:3FA8:18AB*0000ブロックを削除した場合、または

*2001:B80::F80:3FA8:18AB*先頭のゼロと0000ブロックを削除した場合。

URLでのIPv6アドレスの使用

IPv6アドレスにはコロンが含まれます。ただし、コロンはまた、他の種類のネットワークアドレス指定構文でも使用されます。たとえば、IPv4は、IPアドレスとポート番号の両方がURLで使用された場合、コロンを使用して分離します。IPv6は、この原理を継承しました。したがって、混乱を避けるために、IPv6アドレスがURL内で使用される場合にIPv6アドレスを角括弧で囲みます。

Ipv6アドレスを持つURLの例：*http:// [2001:0B80:0000:0000:0000:0F80:3FA8:18AB]*、つまり、これは次のように短縮できます。例：*http:// [2001:B80::F80:3FA8:18AB]*

Ipv6アドレスとポート番号を持つURLの例：*http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234*、つまり、これは次のように短縮できます。例：*http://[2001:B80::F80:3FA8:18AB]:1234*

IPv6の詳細については、IANA Webサイト(https://www.iana.org/numbers/) などを参照してください。IANA(Internet Assigned Numbers Authority、インターネットで利用されるアドレス資源の管理機関) は、IPアドレス指定の世界的な調整を行う組織です。

仮想サーバー

システム コンポーネントバーチャルWindows® サーバー上でVMware® やMicrosoft® Hyper-V®.

仮想化は、多くの場合ハードウェアリソースの利用を向上させるために使用されています。通常、ハードウェアのホストサーバーで実行される仮想サーバーでは、同時に仮想サーバーに大きな負荷を与えることはありません。ただし、レコーディングサーバーは、すべてのカメラやビデオストリーミングを録画します。これにより、CPU、メモリ、ネットワーク、およびストレージシステムに高い負荷がかかります。そのため、仮想サーバーで実行した場合も、多くの場合は利用できるリソースをすべて使用してしまうので、仮想化の通常のメリットの大部分は活かされなくなってしまいます。

仮想環境で実行する場合、デフォルト設定を変更した上で、仮想サーバーに割り当てられるのと同じ量のメモリをハードウェアホストが持ち、レコーディングサーバーを実行している仮想サーバーが十分なCPUと記憶を割り当てられていることが重要です。設定によって異なりますが、通常、レコーディングサーバーには2～4 GBのメモリが必要です。もうひとつの問題は、ネットワークアダプタの割り当てとハードディスクのパフォーマンスです。レコーディングサーバーを実行している仮想サーバーのホストサーバーに、物理的ネットワークアダプタを割り当てるとします。これによって、ネットワークアダプタが他の仮想サーバーへのトラフィックで過負荷にならないようにすることが簡単に実現できます。ネットワークアダプタを複数の仮想サーバーで使用すると、設定された量の画像を取得および録画していないレコーディングサーバーに、ネットワークトラフィックが流入してしまいます。

複数のマネジメントサーバー(クラスタリング) (説明付き)

Management Serverは、サーバーのクラスタ内の複数のサーバーにインストールできます。これにより、システムのダウンタイムがほとんどなくなります。クラスタ内のサーバーに障害が発生すると、クラスタにある別のサーバーが、マネジメントサーバーを実行している障害のあるサーバーの仕事を自動的に引き継ぎます。マネジメントサーバーサービスを切り替えて、クラスタ内の他のサーバーで実行する自動プロセスには、最長で30秒かかります。

監視の設定毎に有効なマネジメントサーバーを1つしか持てませんが、障害の場合に他のマネジメントサーバーが代わりに使われるように設定できます。

> 許可されているフェールオーバーの回数は、6時間で2回に限られています。これを超えると、マネジメントサーバーサービスはクラスタリングサービスによって自動的に起動されることはなくなります。許可されるフェールオーバーの回数は、必要に応じて変更できます。

クラスタリングの要件

- Microsoft Windows Server 2012以降がインストールされている2台のマシン。以下を確認してください:
  - クラスタノードとして追加したいすべてのサーバーによって、同じWindows Serverバージョンが実行されている
  - クラスタノードとして追加したいすべてのサーバーが、同じドメインに加えられている
  - ローカル管理者としてWindowsアカウントにログインするアクセス権限を持っている

  Microsoft Windows Serverのクラスターについては、「フェールオーバー クラスターhttps://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster」を参照してください。

- Microsoft SQL Serverのインストール

  外部SQL Serverおよびサーバー クラスター外でインストールされているデータベース、または、サーバー クラスター内の内部SQL Serverサービス(クラスター化)(内部SQL Serverサービスの作成ではMicrosoft® SQL Server® StandardまたはMicrosoft® SQL Server® Enterpriseエディションを使用する必要があり、クラスター化されたSQL Serverとして機能)のいずれか。

  > 管理サーバーをデータベースに接続する際は、システムの設定に応じて、現在のシステム設定のパスワードを提供するよう求められることがあります。ページ443のシステム設定パスワード(説明付き)を参照してください。

記録データベースを破損から守る

カメラデータベースが破損する可能性があります。このような問題を解決するために、いくつかのデータベース修理オプションが存在します。しかしMilestoneは、カメラデータベースが破損していないことを確認する手順を実行することをお勧めします。

ハードディスク障害:ドライブの保護

ハードディスクドライブは機械装置であり、外的な要因に対して脆弱です。以下は、ハードディスクドライブを傷つけ、カメラデータベースの破損を引き起こす可能性がある外部要因の例です。

- 振動(監視システムサーバーとその周囲が安定していることを確認してください)
- 高温(サーバーが適切に換気されていることを確認してください)
- 強力な磁場(避けてください)
- 停電(必ず無停止電源装置(UPS)を使用してください)
- 静電気(ハードディスクドライブを取り扱う場合には、必ずご自身を接地してください)
- 火災、水など(回避)

Windowsタスクマネージャー: プロセスを終了する際は注意してください

Windowsタスクマネージャで作業するときには、監視システムに影響を与えるプロセスを終了させないように注意してください。Windowsタスクマネージャで[プロセスの終了]をクリックして、アプリケーションまたはシステムサービスを終了すると、プロセスには、終了される前にその状態またはデータを保存する機会が与えられません。その結果として、カメラデータベースが破損する可能性があります。

Windowsタスクマネージャは通常、プロセスを終了しようとすると警告を表示します。プロセスを終了しても監視システムに影響がないことに確信が持てない場合は、警告メッセージでプロセスを終了するか尋ねられた場合にいいえをクリックします。

停電:UPSを使用

データベースが破損する最大の原因として、ファイルが保存されず、オペレーティングシステムが適切に終了されずに、レコーディングサーバーが突然にシャットダウンすることが挙げられます。これは、停電、または誰かが誤ってサーバーの電源コードを抜いてしまった場合などに発生することがあります。

レコーディングサーバーが突然シャットダウンしないように保護するための最善の方法は、各レコーディングサーバーにUPS(無停電電源装置)を備え付けることです。

UPSは、電池駆動の第2電源として動作して、電源異常が発生した場合に、開いているファイルを保存して安全にシステムの電源を切るために必要な電源を提供します。UPSの仕様はさまざまですが、多数のUPSには、開いているファイルの自動保存、システム管理者へのアラート発行などを行うソフトウェアが含まれています。

組織の環境に適した種類のUPSを選択することは、個別のプロセスです。ニーズを評価する際には、停電時にUPSが提供する必要のある実行時間を考慮に入れてください。開いているファイルを保存し、オペレーティングシステムを正しくシャットダウンするには、数分かかる場合があります。

SQLデータベーストランザクションログ(説明付き)

変更がSQLデータベースに書き込まれるたびに、SQLデータベースによってこの変更が自身のトランザクションログに記録されます。

トランザクションログを使用すれば、Microsoft® SQL Server Management Studioを介してSQLデータベースに加えられた変更をロールバックし、元に戻すことができます。デフォルトでは、SQLデータベースには自身のデータベースログが無期限に保管されます。つまり、トランザクションログのエントリ数は時間とともに増えていきます。トランザクションログはデフォルトでシステムドライブに配置されており、そのサイズが増え続けることでWindowsが正常に実行されなくなるおそれがあります。

このような状況を避けるため、トランザクションログを定期的にフラッシュするようお勧めします。フラッシュを行ってもトランザクションログファイルが小さくなることはありませんが、その内容がクリーンアップされることから、制御不能な事態にまで拡大することを防ぐことができます。お使いのVMSシステムによってトランザクションログがフラッシュされることはありません。SQL Serverでは、トランザクションログを複数の方法でフラッシュできます Microsoftサポートページ(https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017)にアクセスし、「*トランザクションログの切り捨て*」の項目を探してください。

最低限のシステム要件

各種システム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。

インストールを開始する前に

Milestoneでは、実際のインストールを開始する前に、次のセクションに記載の要件を確認するように推奨しています。

サーバーとネットワークの準備

オペレーティングシステム

すべてのサーバーにMicrosoft Windowsオペレーティングシステムのクリーンインストールがあり、すべてのサーバーにすべての最新のWindows更新がインストールされていることを確認します。

各種システム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。

Microsoft® .NET Framework

すべてのサーバーにMicrosoft .NET Framework 4.7以降がインストールされていることを確認します。

ネットワーク

すべてのシステムコンポーネントに固定IPアドレスを割り当てるか、カメラにDHCP予約を作成します。十分な帯域幅がネットワークで使用可能であることを保証するために、システムにより帯域幅が消費される方法とタイミングを理解する必要があります。ネットワークに対する主要な負荷には次の3つの要素があります。

- カメラビデオストリーム
- ビデオを表示するクライアント
- 録画されたビデオのアーカイブ

レコーディングサーバーはカメラからビデオストリームを取得し、これがネットワークに対する固定的な負荷になります。ビデオを表示するクライアントはネットワーク帯域幅を消費します。クライアントビューのコンテンツに変更がない場合は、負荷は一定です。ビューコンテンツ、ビデオ検索、または再生の変更により、負荷が動的になります。

録画したビデオのアーカイブはオプションの機能で、コンピュータの内部ストレージシステムに十分なスペースがない場合に、システムがネットワークストレジに録画を移動します。これは定義する必要があるスケジュールされたジョブです。一般的には、ネットワークドライブにアーカイブし、ネットワークに対するスケジュールされた動的な負荷にします。

ネットワークには、このようなトラフィックのピークに対応するための帯域幅ヘッドルームが必要です。これにより、システムの応答性と一般的なユーザー経験が改善されます。

Active Directoryの準備

Active Directoryサービスによってユーザーをシステムに追加する場合は、Active Directoryがインストールされており、ドメインコントローラーとして機能するサーバーをネットワークで使用できなくてはなりません。

ユーザーとグループ管理を簡単に行うには、Milestoneシステムをインストールする前に、Microsoftアクティブディレクトリ®をインストールし、設定することを[1]お勧めしますXProtect。システムをインストールしてから、マネジメントサーバーをActive Directoryに追加すると、マネジメントサーバーを再インストールして、Active Directoryで定義した新しいWindowsユーザーにユーザーを置き換えなければならなくなります。

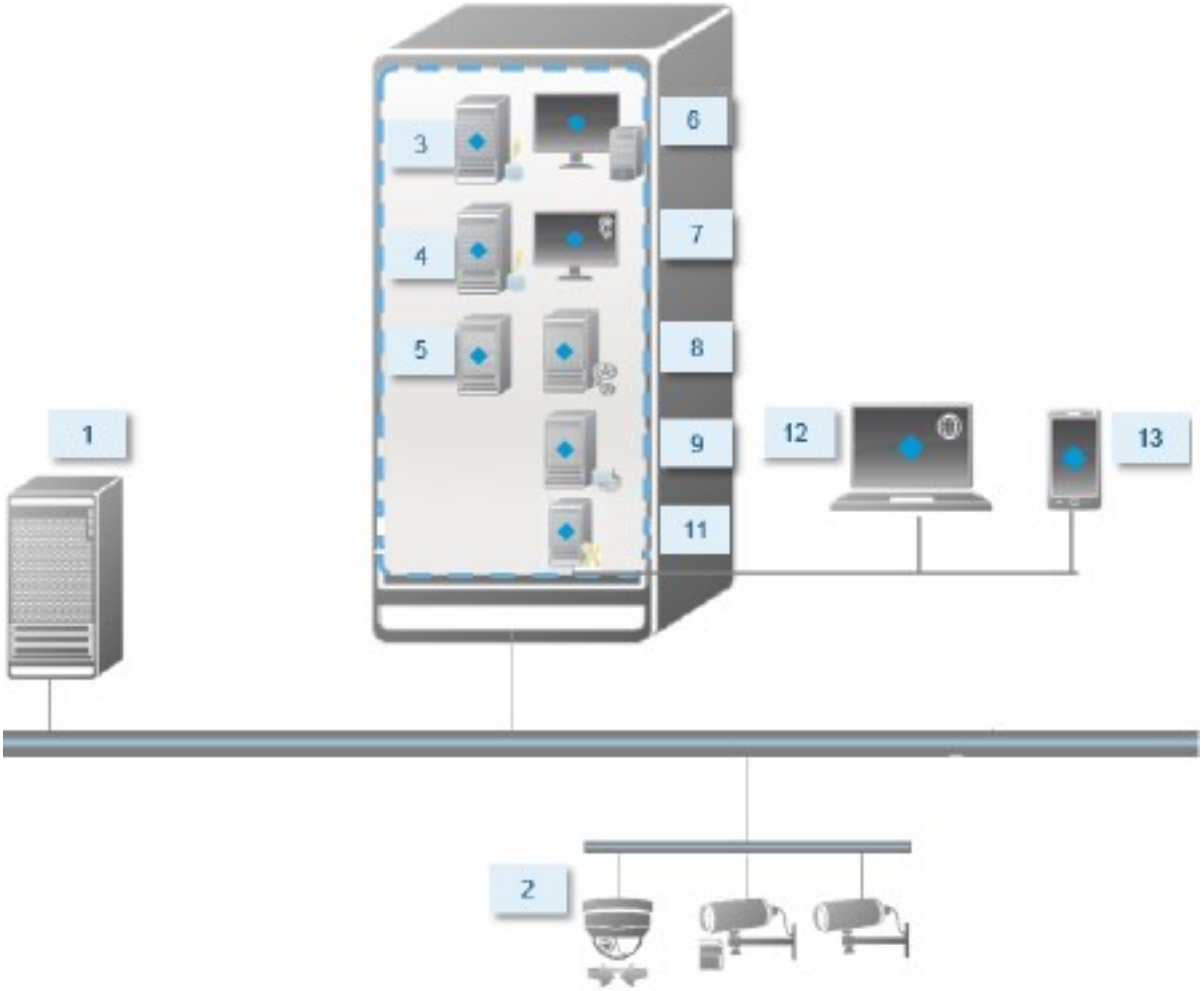
基本ユーザーはMilestone Federated Architectureシステムでサポートされていないため、Milestone Federated Architectureを使用することを計画している場合は、Active Directoryサービス経由でWindowsユーザーを追加する必要があります。Active Directoryをインストールしない場合は、インストールの際にページ98のワークグループのインストールの手順に従ってください。

インストール方法

インストールウィザードでは、使用するインストール方法を決定する必要があります。組織のニーズに基づいて選択してください。ただし、通常は、システムを購入した時点でインストール方法は既に決定されています。

オプション	説明
1つのコンピュータ	現在のコンピュータに、すべてのサーバー/クライアントコンポーネントと、SQL Serverがインストールされます。 インストールが完了すれば、ウィザードを介してシステムを設定できる場合があります。続行することに同意した後、レコーディングサーバーによってハードウェアのネットワークがスキャンされ、どのハードウェアをシステムに追加するかを選択できるようになります。設定ウィザードに追加できるハードウェアデバイスの最大数は、お持ちの基本ライセンスに応じて異なります。また、カメラがビュー内であらかじめ構成され、デフォルトのオペレータの役割が作成されます。インストールが終了するとXProtect Smart Clientが開き、システムを使用する準備が整います。
カスタム:	マネジメントサーバーは常にシステムコンポーネントリストで選択され、常にインストールされますが、現在のコンピュータに何をインストールするか(他のサーバーコンポーネントやクライアントコンポーネントなど)は自由に選択できます。 デフォルトでは、レコーディングサーバーはコンポーネントリスト内で選択されていませんが、これは変更可能です。未選択のコンポーネントを後から他のコンピュータにインストールすることもできます。

シングルコンピュータのインストール

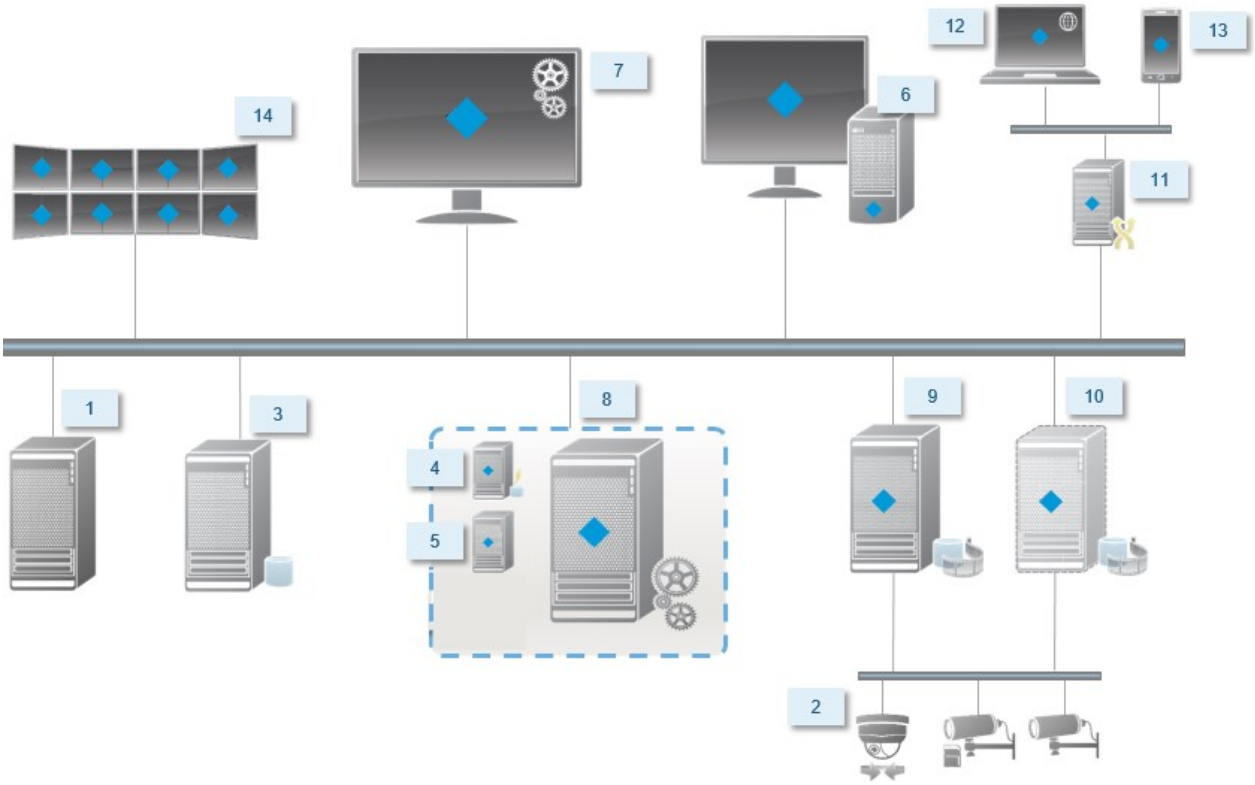


標準システムコンポーネント:

1. **Active Directory**
2. デバイス
3. **SQL Server**を備えたサーバー
4. イベントサーバー
5. ログサーバー
6. **XProtect Smart Client**
7. **Management Client**
8. マネジメントサーバー

9. レコーディングサーバー
10. フェールオーバーレコーディングサーバー
11. XProtect Mobileサーバー
12. XProtect Web Client
13. XProtect Mobileクライアント
14. XProtect Smart ClientとXProtect Smart Wall

カスタムインストール - 分散型システムコンポーネントの例



SQL Serverエディションの決定

Microsoft® SQL Server® ExpressはSQL Serverの無料版であり、インストールと使用に向けた準備が他のSQL Serverエディションよりも簡単です。単一のコンピュータへのインストール中には、SQL Serverがすでにコンピュータにインストールされていない限り、Microsoft SQL Server Expressがインストールされます。

XProtect VMSインストールにMicrosoft SQL Server Expressバージョン2019が含まれています。一部のWindowsオペレーティングシステムは、このSQL Serverエディションに対応してません。XProtect VMSをインストールする前に、お使いのオペレーティングシステムがSQL Server 2019に対応していることを確認してください。オペレーティングシステムがこのSQL Serverエディ

ションに対応していない場合は、XProtect VMSインストールを開始する前に、対応しているSQL Serverのエディションをインストールします。サポートされているSQL Serverエディションの詳細については、https://www.milestonesys.com/systemrequirements/を参照してください。

Milestoneでは、大規模なシステムまたはSQLデータベースを行き来するトランザクションが多いシステムについては、ネットワーク上の専用コンピュータと、他の目的では使用されていない専用ハードディスクドライブでSQL ServerのMicrosoft® SQL Server® StandardまたはMicrosoft® SQL Server® Enterpriseエディションを使用するよう推奨しています。専用ドライブにSQL Serverをインストールすることで、全体的なシステムパフォーマンスが上がります。

サービスアカウントを選択してください

インストールの一部として、このコンピュータでMilestoneサービスを実行するためのアカウントを指定する必要があります。ログインユーザーには関係なく、サービスは常にこのアカウントで実行されます。アカウントにすべての必要なユーザー権限があることを確認してください。たとえば、タスクを実行するための適切な権限、ネットワーク共有フォルダーへの適切なネットワークおよびファイルアクセスなどです。

定義済みのアカウントまたはユーザーアカウントのいずれかを選択できます。システムをインストールする環境に応じて、判断してください。

ドメイン環境

ドメイン環境：

- Milestoneは、ビルトインのNetwork Serviceアカウントを使用することをお勧めします。

  システムを複数のコンピュータに拡張する必要がある場合でも、使いやすいアカウントです。

- ドメインユーザーアカウントも使用できますが、構成が多少困難になる可能性があります。

ワークグループ環境

ワークグループ環境では、Milestoneは、すべての必要な権限があるローカルユーザーアカウントを使用することをお勧めします。通常は、これは管理者アカウントです。

> 複数のコンピュータにシステムコンポーネントをインストールする場合は、選択したユーザーアカウントがインストールされたすべてのコンピュータに、同じ名前、パスワード、アクセス権で存在する必要があります。

Kerberos認証(説明付き)

Kerberosはチケットベースのネットワーク認証プロトコルです。クライアント/サーバまたはサーバ/サーバ・アプリケーションのための強固な認証を提供するように設計されています。

古いMicrosoft NT LAN(NTLM)認証プロトコルの代替としてKerberos認証を使用します。

Kerberos認証は相互認証、つまりクライアントがサービスを、サービスがクライアントを認証する必要があります。この方法では、パスワードを公開せずに、クライアントXProtectからXProtectサーバーへ、より確実に認証できます。

Active Directory内にサービス・プリンシパル名(SPN)を登録することで、XProtect VMSで相互認証が可能になります。SPNは、XProtect Serverサービスのようなエンティティを一意に識別するエイリアスです。相互認証を使用するすべてのサービスでは、クライアントがネットワーク上のサービスを識別できるように、SPNを登録する必要があります。正しく登録されたSPNがなければ、相互認証を行えません。

以下の表で、Milestoneサービスおよび対応登録する必要がある対応ポート番号を一覧表示します:

サービス	ポート番号
マネジメントサーバー - IIS	80 - 構成可能
マネジメントサーバー - 内部	8080
レコーディングサーバー - Data Collector一	7609
フェールオーバーサーバー	8990
イベントサーバー	22331
LPRサーバー	22334

アクティブ・ディレクトリに登録する必要があるサービスの数は、現在のインストール状況に依存します。Data Collectorは、マネジメントサーバー、レコーディングサーバー、イベントサーバーまたはフェールオーバーサーバーサービスのインストール時に自動的にインストールされます。

サービスを走らせるユーザーのために、2つのSPNsを登録する必要があります。:1つはホスト名で、もう1つは全権限を与えられたドメイン名で。

ネットワーク・ユーザー・サービス・アカウントの下でサービスを実行している場合は、このサービスを実行しているコンピュータごとに2つのSPNを登録する必要があります。

これはMilestoneSPN命名スキーム:

```
VideoOS/[DNS ホスト名]:[ポート]
VideoOS/[完全修飾ドメイン名]:[ポート]
```

以下は、次の詳細で、コンピュータ上で実行されるレコーディングサーバーサービスのSPNの例です。

```
ホスト名:Record-Server1
ドメイン:Surveillance.com
```

登録するSPN:

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

ウィルススキャンの排除(説明付き)

他のデータベースソフトウェアの場合と同様に、XProtectソフトウェアを実行しているコンピュータにアンチウイルスプログラムがインストールされている場合は、特定のファイルのタイプやフォルダ、ならびに特定のネットワーク通信を除外することが重要になります。このような例外を設定しておかないと、ウイルススキャンで大量のシステムリソースが消費されてしまいます。さらに、スキャンプロセスによってファイルが一時的にロックされ、その結果として録画プロセスが破損したり、データベースが破損する可能性もあります。

ウイルススキャンを実行する必要がある場合、録画データベースを含んでいるレコーディングサーバーのフォルダー(デフォルトではc:\mediadatabase\、ならびにすべてのサブフォルダー)はスキャンしないでください。また、アーカイブ保存ディレクトリでもウイルススキャンは実行しないでください。

以下を除外に追加してください。

- ファイルのタイプ:.blk、.idx、.pic
- フォルダーおよびサブフォルダー:
  - C:\Program Files\Milestone または C:\Program Files (x86)\Milestone
  - C:\ProgramData\Milestone\MIPSDK
  - C:\ProgramData\Milestone\XProtect Mobile Server\Logs
  - C:\ProgramData\Milestone\XProtect Data Collector Server\Logs
  - C:\ProgramData\Milestone\XProtect Event Server\Logs
  - C:\ProgramData\Milestone\XProtect Log Server
  - C:\ProgramData\Milestone\XProtect Management Server\Logs
  - C:\ProgramData\Milestone\XProtect Recording Server\Logs
  - C:\ProgramData\Milestone\XProtect Report Web Server\Logs

- 以下のTCPポートでのネットワークスキャンを除外：

製品	TCPポート
XProtect VMS	80、8080、7563、25、21、9993
XProtect Mobile	8081

または

- 以下のプロセスのネットワークスキャンを除外：

製品	プロセス
XProtect VMS	VideoOS.Recorder.Service.exe、VideoOS.Server.Service.exe、VideoOS.Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe

組織によってはウイルススキャンに関する厳密な方針があるかもしれませんが、上記の場所やファイルをウイルススキャンから除外することが重要です。

FIPS 140-2準拠モードで実行するようにXProtect VMSを設定するにはどうすればよいですか?

FIPS 140-2の操作モードでXProtect VMSを実行するには以下を行う必要があります。

- FIPS 140-2の認定操作モードでWindowsオペレーティングシステムを実行します。FIPSの有効化の詳細については、Microsoftサイトを参照してください。
- FIPSが有効になったWindowsオペレーティングシステムで、スタンドアロンサードパーティ統合を実行できることを確認
- 操作のFIPS 140-2準拠モードを確保できるような方法でデバイスに接続
- メディアデータベースのデータがFIPS 140-2準拠暗号で暗号化されていることを確認

  これを行うには、メディアデータベースアップグレードツールを実行します。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、強化ガイドのFIPS 140-2準拠セクションを参照してください。

FIPSが有効なシステムでXProtect VMSをインストールする前に

新しいXProtect VMSのインストールは、FIPSが有効になっているコンピュータで実行できますが、WindowsオペレーティングシステムでFIPSが有効な場合はXProtect VMSをアップグレードできません。

アップグレードする場合は、インストールする前に、VMSに含まれているすべてのコンピュータでWindows FIPSセキュリティポリシーを無効にしてください。この中にはSQLサーバーをホストしているコンピュータも含まれます。

XProtect VMSインストーラーはFIPSセキュリティポリシーを確認し、FIPSが有効であれば、インストールの開始を防ぎます。

ただし、XProtect VMSバージョン2020 R3以降にアップグレードしている場合は、FIPSを無効にする必要はありません。

XProtect VMSのコンポーネントをすべてのコンピュータにインストールして、FIPS向けにシステムを準備した後、VMSのすべてのコンピュータのWindowsでFIPSセキュリティポリシーを有効にできます。

FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、強化ガイドのFIPS 140-2準拠セクションを参照してください。

ソフトウェアライセンスコードを登録する

インストールする前に、Milestoneから受け取ったソフトウェアライセンスファイルの名前と場所を把握しておく必要があります。

XProtect Essential+の無料版をインストールできます。無料版はXProtect VMSの機能やカメラの数が限られています。インストールのためにはインターネットに接続してくださいXProtect Essential+。

ソフトウェアライセンスコード(SLC)は注文確認書に記載されています。ソフトウェアライセンスファイル名はSCLに基づいています。

Milestoneは、インストール前にSLCをWebサイト(https://online.milestonesys.com/) に登録することをお勧めします。代理店により登録済みの場合もあります。

デバイスドライバー(説明付き)

お使いのシステムでは、ビデオデバイスドライバーを使用して、レコーディングサーバーに接続したカメラデバイスを制御および通信しています。システムの各レコーディングサーバーに、デバイスドライバーをインストールする必要があります。

2018 R1のリリースから、デバイスドライバーは2つのDevice Packに分けられます：より新しいドライバーを持つレギュラーDevice Packと、古いバージョンのドライバーを持つレガシーDevice Packです。

レギュラーDevice Packは、レコーディングサーバーをインストールする時に自動的にインストールされます。その後、新しいバージョンのDevice Packをダウンロード、およびインストールすることで、ドライバーを更新できます。Milestoneではデバイスドライバーの新規バージョンを定期的に公開しており、当社Webサイト上のダウンロードページ(https://www.milestonesys.com/downloads/) でデバイスパックとしてご利用いただけます。Device Packを更新するときには、インストール済みのバージョンに最新バージョンを上書きインストールできます。

レガシーDevice Packは、システムがレギュラーDevice Packをインストール済みの場合のみ、インストールすることが可能です。前のバージョンが既にシステムにインストールされている場合は、レガシーDevice Packからのドライバーは、自動的にインストールされます。これはソフトウェアダウンロードページ(https://www.milestonesys.com/downloads/) から手動でダウンロードおよびインストールが可能です。

インストールする前にレコーディングサーバーサービスを停止します。停止しなければ、コンピュータを再起動する必要があります。

最高のパフォーマンスを維持するために、常に最新バージョンのデバイスドライバーをご使用ください。

オフラインインストールの要件

オフラインであるサーバーにシステムをインストールする場合、以下が必要となります。

- `Milestone XProtect VMS製品2020 R3システムInstaller.exe`ファイル
- XProtectシステムのソフトウェアライセンスファイル(SLC) 。
- 必須の.NETバージョン(https://www.milestonesys.com/systemrequirements/) を含むOSインストールメディア。

安全な通信(説明付き)

ハイパーテキスト トランスファー プロトコル セキュア (HTTPS) は、ハイパーテキスト トランスファー プロトコル (HTTP) をコンピューター 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は、秘密キー1つと公開キー1つのペアを使用し、安全なコネクションを認証して安全な接続を管理します。

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、秘密キーと公開キーの2種類のキーが含まれています。公開キーは、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。秘密キー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、必ずWebサービスが公開キー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公開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キーを交換することができ、安全なSSL/TLS通信を確立できます。

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、認証の期限が近づいても警告しません。証明書の有効期限が切れた場合:

- クライアントは、証明書の有効期限が切れたレコーディング サーバーを信頼しないため、通信できません
- レコーディング サーバーは、証明書の有効期限が切れた管理サーバーを信頼しないため、通信できません
- モバイル機器は、証明書の有効期限が切れたモバイル サーバーを信頼しないため、通信できません

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。

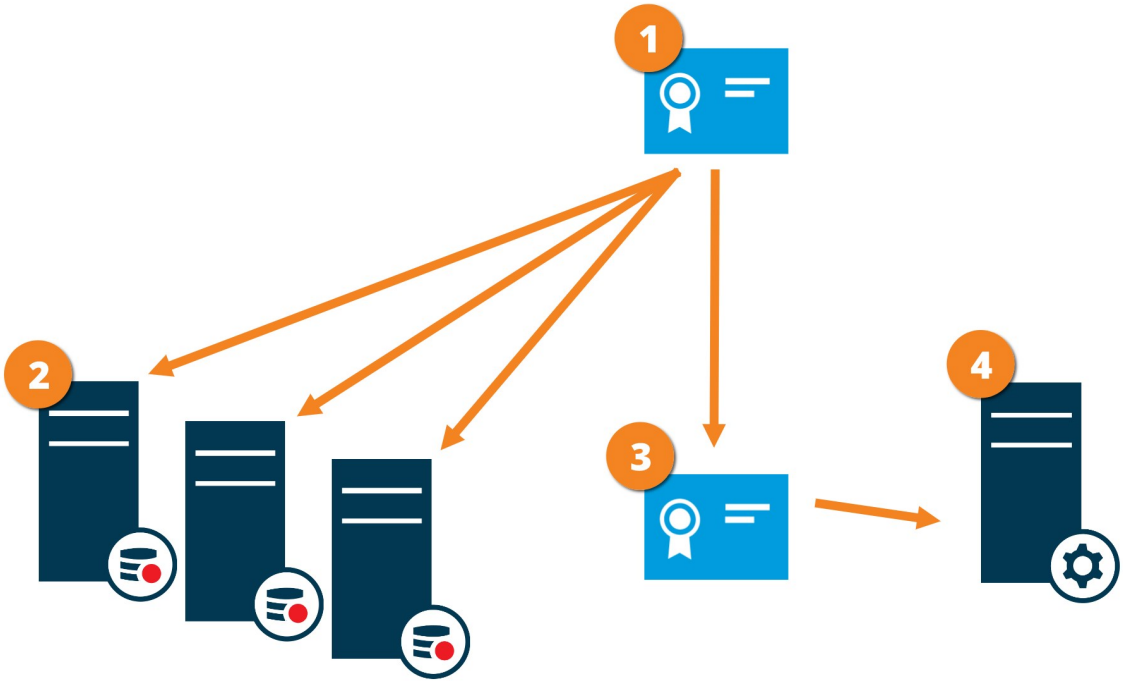
同じサブジェクト名で認証を更新してWindows証明書ストアに追加すると、サーバーは自動的に新しい認証を獲得します。これにより、多数のレコーディング サーバーで証明書を更新しやすくなります。レコーディング サーバーごとにサービスを再起動したり、証明書を再度選択する必要はありません。

サーバーの暗号化を管理(説明付き)

管理サーバーとレコーティング サーバー間の双方向接続を暗号化できます。管理サーバー上の暗号化を有効にすると、その管理サーバーに接続するすべてのレコーティング サーバーからの接続に適用されます。管理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、管理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証明書をインストールしてください。

管理サーバーの証明書配布

この図は、証明書が署名され、信頼され、XProtect VMSで配布されて安全に管理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。



❶CA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 (管理サーバー) と、証明書を認証する側 (レコーディング サーバー) の双方に信頼されます。

❷CA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による証明書の信頼性を確認します。

❸CA証明書は、管理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。

❹CA証明書は、管理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。

プライベート管理サーバー証明書の要件:

- 認証名に管理サーバーのホスト名が含まれるか、DNS認証される名前のリストの中にサブジェクト(所有者) として管理サーバーに発行されます。
- 管理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、これが管理サーバーでも信頼されていること。
- 管理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、管理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

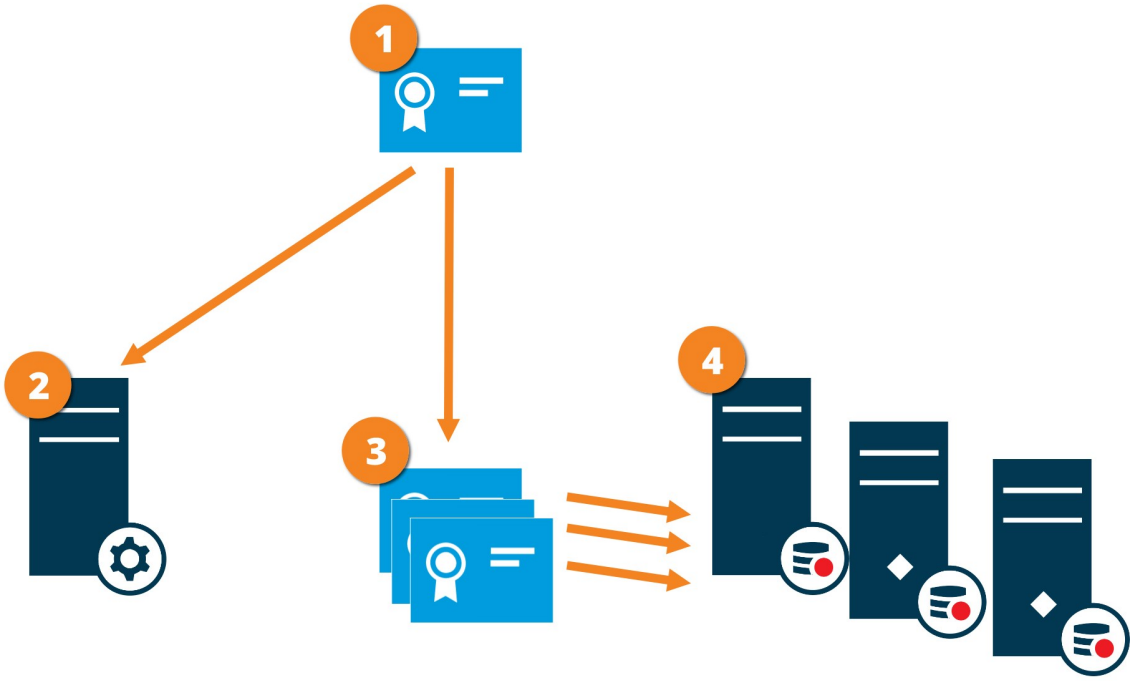
マネジメントサーバーからレコーディングサーバーへの通信を暗号化(説明付き)

マネージメントサーバーとレコーテ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テ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。このようして、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)

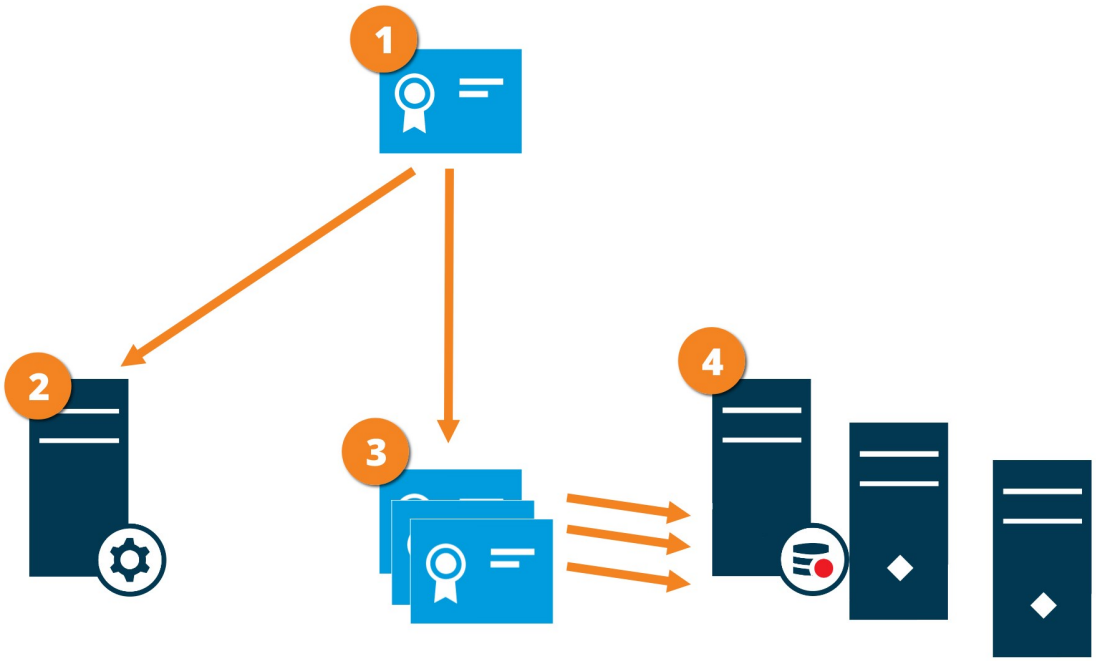
以下のタイプのリモートサーバーがある場合は、管理サーバーとData Collector関連サーバー間の双方向接続を暗号化できます。

- レコーディングサーバー
- イベントサーバー
- ログサーバー
- LPRサーバー
- モバイルサーバー

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。管理サーバーの暗号化が有効になっている場合は、これを各リモートサーバーに関連のあるData Collector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。暗号化を有効化する前に、管理サーバーと、リモートサーバーに関連しているすべてのData Collectorサーバーで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、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

❷ 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。このようして、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、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

❹ 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名のリスト内に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)

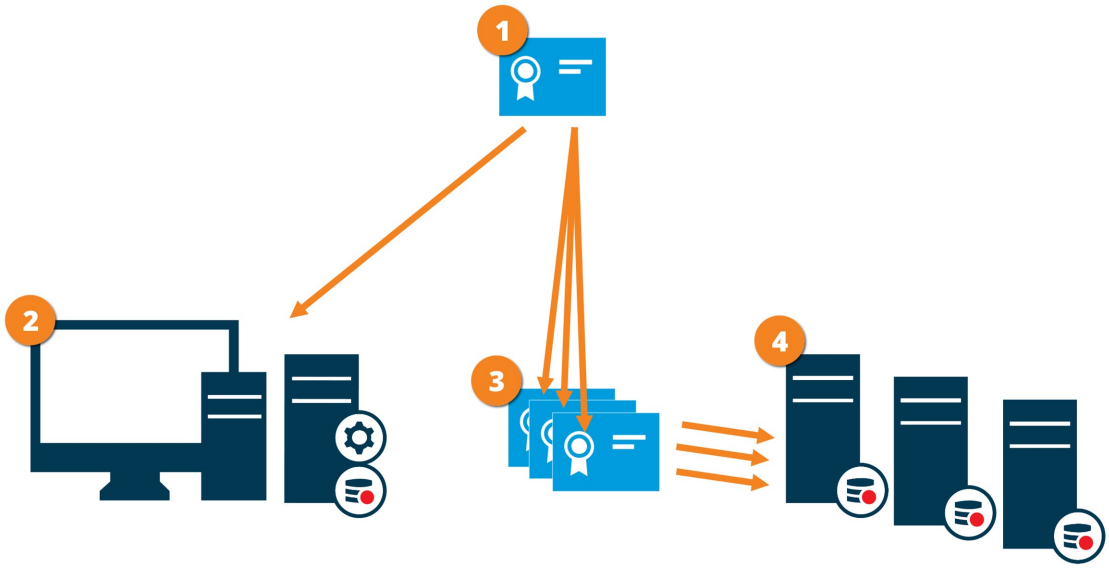
レコーディングサーバーを暗号化可能にする場合、すべてのクライアント、サーバー、ならびにレコーディングサーバーからデータストリームを受け取るインテグレーションは暗号化されます。この文書では「クライアント」と呼んでいます:

- XProtect Smart Client
- Management Client
- マネジメントサーバー(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サーバー
- XProtect Event Server
- XProtect LPR
- Milestone Open Network 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。

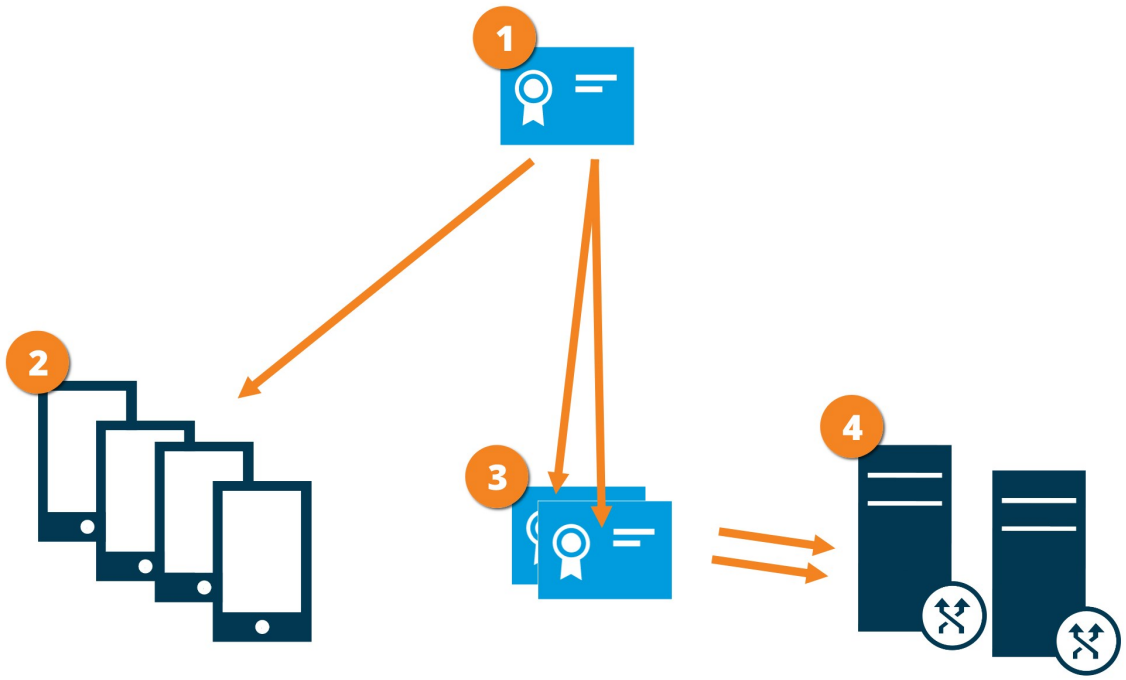
レコーディングサーバーの暗号化が有効化されており、システムがフェールオーバーレコーディングサーバーを適用している場合は、Milestone はフェールオーバー レコーディングサーバー も暗号化する準備をすることをお勧めします。

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際、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。



❶CA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 (モバイル サーバー) と証明書を確認する側 (クライアントすべて) 双方に信頼されます。

❷CA認証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による証明書の信頼性を確認します。

❸CA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。

❹CA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してください。

CA認証要件:

- 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、またはDNS認証される名前リストの認証名に含まれていなくてはなりません
- 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認証の秘密キーへのアクセス権限が必要です

クライアントに対するモバイルサーバー暗号化の条件

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

インストール

新しいXProtectシステムのインストール

XProtect Essential+をインストールする

XProtect Essential+の無料版をインストールできます。無料版はXProtect VMSの機能やカメラの数が限られています。インストールのためにはインターネットに接続してくださいXProtect Essential+。

このバージョンは、シングルコンピュータインストールオプションを使用して1台のコンピュータにインストールされます。シングルコンピュータオプションは、現在のコンピュータにすべてのサーバーコンポーネントとクライアントコンポーネントをインストールします。

> Milestoneでは、インストールの前に以下のセクションを注意して読むようお勧めしています:ページ58のインストールを開始する前に。

> FIPSインストールでは、Windowsオペレーティングシステムで FIPSが有効になっている場合、XProtect VMSをアップグレードできません。インストールする前に、VMSに含まれているすべてのコンピューターでWindows FIPSセキュリティポリシーを無効にします(SQLサーバーをホストしているコンピューターも含まれます)。ただし、XProtect VMSバージョン2020 R3以降にアップグレードしている場合は、FIPSを無効にする必要はありません。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、強化ガイドのFIPS 140-2準拠セクションを参照してください。

初期インストールの後、設定ウィザードを続けることができます。ハードウエアと構成に応じて、レコーディングサーバーがネットワーク上のハードウエアをスキャンします。その後、どのハードウェアデバイスをシステムに追加するか選択できます。カメラはビューに事前構成されており、マイクやスピーカーといったその他デバイスは、オプションで有効にできます。また、ユーザーにオペレーターの役割、あるいはシステム管理者の役割を持たせてシステムに加えることも可能です。インストールが終了するとXProtect Smart Clientが開き、システムを使用する準備が整います。

インストールウィザードを閉じると、XProtect Management Clientが開き、ハードウェアデバイスやユーザーのシステムへの追加といった手動設定が可能になります。

> 以前のバージョンの製品からアップグレードすると、システムはハードウェアのスキャン、または新しいビューとユーザーのプロファイル作成を行いません。

1. ソフトウェアをインターネット (https://www.milestonesys.com/downloads/) からダウンロードし、`Milestone XProtect VMS製品2020 R3システムInstaller.exe`ファイルを実行します。
2. インストール ファイルが展開されます。セキュリティ設定によって、1つまたは複数のWindows®セキュリティ警告が表示されます。これらを許可すると、展開が続行されます。
3. 完了すると、**Milestone XProtect VMS**インストール ウィザードが表示されます。
   1. インストール中に言語を選択します(これは、インストール後にシステムによって使用される言語ではありません。これは後の段階で選択します) 。続行をクリックします。
   2. *Milestone使用許諾契約*を読みます。使用許諾契約の条項に同意しますチェックボックスを選択して、続行をクリックします。
   3. **XProtect Essential+**リンクをクリックして、無料のライセンスファイルをダウンロードします。

      無料のライセンス ファイルがダウンロードされ、ライセンス ファイルの場所を入力または参照フィールドに表示されます。続行をクリックします。
4. 単一のコンピューターを選択します。

   インストールするコンポーネントのリストが表示されます (このリストは編集できません)。続行をクリックします。
5. システム設定パスワードの割り当てページで、システム設定を保護するパスワードを入力します。システム回復時、またはシステムを拡張する際 (クラスターの追加など)、このパスワードが必要になります。

   > このパスワードを保存して安全に維持しておく必要があります。このパスワードをなくした場合は、システム設定を回復する能力に支障が出る可能性があります。

   システム設定をパスワードで保護したくない場合は、システム設定パスワードを保護しないことを選択し、システム設定が暗号化されないことを承知するを選択します。

   続行をクリックします。
6. レコーディング サーバーの設定ページで、様々なレコーディング サーバー設定を行います:
   1. レコーディングサーバー名フィールドに、レコーディングサーバー名を入力します。デフォルトはコンピュータ名です。
   2. 管理サーバーのアドレスフィールドに管理サーバーのアドレスとポート番号 (localhost:80) が表示されます。
   3. メディア データベース ロケーションの選択フィールドで、ビデオ録画を保存したい場所を選択します。ビデオ録画は、プログラムをインストールする場所とは別の、システム ドライブ以外の場所に保存するようMilestoneでは推奨します。デフォルトの場所は、最も容量のあるドライブです。
   4. ビデオ録画の保存期間フィールドでは、ビデオ録画の保存期間を定義します。保存期間は、7日がデフォルトで設定されていますが、1日から999日まで設定が可能です。
   5. 続行をクリックします。

7. 暗号化を選択ページでは、通信フローを安全に保護できます。

   - レコーディング サーバー、データコレクター、管理サーバー間

     内部通信フローに対して暗号化を有効にする場合は、サーバー証明書のセクションで証明書を選択してください。

     > レコーディング サーバーから管理サーバーへの通信を暗号化する場合、システムより、管理サーバーからレコーディング サーバーへの通信も暗号化する必要があります。

   - レコーディング サーバーとクライアント間

     レコーディング サーバーと、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クライアントコンポーネント間の暗号化を有効にする場合は、ストリーミング メディアの証明書セクションで、証明書を選択してください。

   - 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クライアントコンポーネント間の暗号化を有効にする場合は、モバイル 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。

   すべてのシステム コンポーネントに対して同じ証明書を使用することも、システム コンポーネントごとに異なる証明書を使用することもできます。

   安全な通信のためのシステム準備の詳細については、ページ67の安全な通信(説明付き)とMilestone証明書ガイドを参照してください。

   インストール後、通知エリアのManagement Server Managerトレイ アイコンのServer Configuratorから暗号化を有効にすることもできます。

8. ファイルの場所と製品言語を選択ページで以下を行います。

   1. ファイルの場所フィールドで、プログラムをインストールしたいロケーションを選択してください。

      > すでにMilestone XProtect VMSがコンピューターにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

   2. 製品の言語で、どの言語でXProtect製品をインストールするのか選択します。

   3. インストールをクリックします。

   ソフトウェアがインストールされます。まだコンピュータにインストールされていない場合は、インストール中にMicrosoft® SQL Server® ExpressとMicrosoft IISが自動的にインストールされます。

9. コンピュータを再起動するよう指示される場合があります。コンピュータの再起動後、セキュリティ設定によって1つまたは複数のWindowsセキュリティ警告が表示される場合があります。これらを許可すると、インストールが完了します。

10. インストールが完了すると、コンピューターにインストールされているコンポーネントのリストが表示されます。

    続行をクリックして、システムにハードウェアとユーザーを追加してください。

    > ここで閉じるをクリックすると設定ウィザードがスキップされ、XProtect Management Clientが開きます。Management Clientでは、システムを設定できます (ハードウェアやユーザーのシステムへの追加など)。

11. ハードウェアのユーザー名とパスワードを入力ページでは、(メーカーのデフォルト値から変更した) ハードウェアのユーザー名とパスワードを入力します。

    インストーラーにより、このハードウェアのネットワークと、メーカーのデフォルト資格情報が割り当てられたハードウェアのネットワークがスキャンされます。

    続行をクリックして、ハードウェアのスキャンが完了するまで待機します。

12. システムに追加するハードウェアを選択ページで、システムに追加したいハードウェアを選択します。続行をクリックして、ハードウェアが追加されるまで待機します。

13. デバイスの設定ページでは、ハードウェア名の横にある編集アイコンをクリックすると、ハードウェアにわかりやすい名前を付けることができます。この名前は、ハードウェアデバイスの名前の先頭に付きます。

    ハードウェアノードを展開して、カメラ、スピーカー、マイクなどのハードウェアデバイスを有効または無効にします。

    > デフォルトで、カメラは有効化、スピーカーとマイクは無効化されています。

    続行をクリックして、ハードウェアが設定されるまで待機します。

14. ユーザーの追加ページでは、ユーザーをWindowsユーザーまたは基本ユーザーとしてシステムに追加できます。これらのユーザーには、管理者またはオペレーターの役割を割り当てることができます。

    ユーザーを定義し、追加をクリックします。

    ユーザーの追加が終わったら、続行をクリックします。

15. インストールと初期設定が終了すると、設定が完了しましたページが開きます。ここには以下が表示されます:
    - システムに追加されたハードウェアデバイスのリスト
    - システムに加えられたユーザーのリスト
    - ユーザーと共有できるXProtect Web ClientとXProtect Mobileクライアントへのアドレス

    閉じるをクリックするとXProtect Smart Clientが開き、利用可能になります。

システムのインストール - シングルコンピュータオプション

シングルコンピュータオプションは、現在のコンピュータにすべてのサーバーコンポーネントとクライアントコンポーネントをインストールします。

> Milestoneでは、インストールの前に以下のセクションを注意して読むようお勧めしています:ページ58のインストールを開始する前に。

> FIPSインストールでは、WindowsオペレーティングシステムでFIPSが有効になっている場合、XProtect VMSをアップグレードできません。インストールする前に、VMSに含まれているすべてのコンピューターでWindows FIPSセキュリティポリシーを無効にします(SQLサーバーをホストしているコンピューターも含まれます)。ただし、XProtect VMSバージョン2020 R3以降にアップグレードしている場合は、FIPSを無効にする必要はありません。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、強化ガイドのFIPS 140-2準拠セクションを参照してください。

初期インストールの後、設定ウィザードを続けることができます。ハードウエアと構成に応じて、レコーディングサーバーがネットワーク上のハードウエアをスキャンします。その後、どのハードウェアデバイスをシステムに追加するか選択できます。カメラはビューに事前構成されており、マイクやスピーカーといったその他デバイスは、オプションで有効にできます。また、ユーザーにオペレーターの役割、あるいはシステム管理者の役割を持たせてシステムに加えることも可能です。インストールが終了するとXProtect Smart Clientが開き、システムを使用する準備が整います。

インストールウィザードを閉じると、XProtect Management Clientが開き、ハードウェアデバイスやユーザーのシステムへの追加といった手動設定が可能になります。

> 以前のバージョンの製品からアップグレードすると、システムはハードウェアのスキャン、または新しいビューとユーザーのプロファイル作成を行いません。

1. ソフトウェアをインターネット(https://www.milestonesys.com/downloads/)からダウンロードし、`Milestone XProtect VMS製品2020 R3システムInstaller.exe`ファイルを実行します。
2. インストールファイルが展開されます。セキュリティ設定によって、1つまたは複数のWindows®セキュリティ警告が表示されます。これらを許可すると、展開が続行されます。
3. 完了すると、**Milestone XProtect VMS**インストールウィザードが表示されます。
   1. インストール中に言語を選択します(これは、インストール後にシステムによって使用される言語ではありません。これは後の段階で選択します)。続行をクリックします。
   2. *Milestone使用許諾契約*を読みます。使用許諾契約の条項に同意しますチェックボックスを選択して、続行をクリックします。

3. ライセンスファイルの場所を入力または参照で、XProtectプロバイダーから入手したライセンスファイルを入力します。または、ファイルの場所を参照するか、**XProtect Essential+**リンクをクリックして無料ライセンスファイルをダウンロードします。無料のXProtect Essential+製品に課せられている制限については、ページ46の製品比較チャートを参照してください。続行する前に、ライセンスファイルがシステムで検証されます。続行をクリックします。

4. 単一のコンピューターを選択します。

   インストールするコンポーネントのリストが表示されます(このリストは編集できません)。続行をクリックします。

5. システム設定パスワードの割り当てページで、システム設定を保護するパスワードを入力します。システム回復時、またはシステムを拡張する際(クラスターの追加など)、このパスワードが必要になります。

   > このパスワードを保存して安全に維持しておく必要があります。このパスワードをなくした場合は、システム設定を回復する能力に支障が出る可能性があります。

   システム設定をパスワードで保護したくない場合は、システム設定パスワードを保護しないことを選択し、システム設定が暗号化されないことを承知するを選択します。

   続行をクリックします。

6. レコーディングサーバーの設定ページで、様々なレコーディングサーバー設定を行います:

   1. レコーディングサーバー名フィールドに、レコーディングサーバー名を入力します。デフォルトはコンピュータ名です。
   2. 管理サーバーのアドレスフィールドに管理サーバーのアドレスとポート番号(localhost:80)が表示されます。
   3. メディアデータベースロケーションの選択フィールドで、ビデオ録画を保存したい場所を選択します。ビデオ録画は、プログラムをインストールする場所とは別の、システムドライブ以外の場所に保存するようMilestoneでは推奨します。デフォルトの場所は、最も容量のあるドライブです。
   4. ビデオ録画の保存期間フィールドでは、ビデオ録画の保存期間を定義します。保存期間は、7日がデフォルトで設定されていますが、1日から999日まで設定が可能です。
   5. 続行をクリックします。

7. 暗号化を選択ページでは、通信フローを安全に保護できます。

   - レコーディング サーバー、データコレクター、管理サーバー間

     内部通信フローに対して暗号化を有効にする場合は、サーバー証明書のセクションで証明書を選択してください。

     > レコーディング サーバーから管理サーバーへの通信を暗号化する場合、システムより、管理サーバーからレコーディング サーバーへの通信も暗号化する必要があります。

   - レコーディング サーバーとクライアント間

     レコーディング サーバーと、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クライアントコンポーネント間の暗号化を有効にする場合は、ストリーミング メディアの証明書セクションで、証明書を選択してください。

   - 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クライアントコンポーネント間の暗号化を有効にする場合は、モバイル 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。

   すべてのシステム コンポーネントに対して同じ証明書を使用することも、システム コンポーネントごとに異なる証明書を使用することもできます。

   安全な通信のためのシステム準備の詳細については、ページ67の安全な通信(説明付き)とMilestone証明書ガイドを参照してください。

   インストール後、通知エリアのManagement Server Managerトレイ アイコンのServer Configuratorから暗号化を有効にすることもできます。

8. ファイルの場所と製品言語を選択ページで以下を行います。

   1. ファイルの場所フィールドで、プログラムをインストールしたいロケーションを選択してください。

      > すでにMilestone XProtect VMSがコンピューターにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

   2. 製品の言語で、どの言語でXProtect製品をインストールするのか選択します。

   3. インストールをクリックします。

   ソフトウェアがインストールされます。まだコンピュータにインストールされていない場合は、インストール中にMicrosoft® SQL Server® ExpressとMicrosoft IISが自動的にインストールされます。

9. コンピュータを再起動するよう指示される場合があります。コンピュータの再起動後、セキュリティ設定によって1つまたは複数のWindowsセキュリティ警告が表示される場合があります。これらを許可すると、インストールが完了します。

10. インストールが完了すると、コンピューターにインストールされているコンポーネントのリストが表示されます。

    続行をクリックして、システムにハードウェアとユーザーを追加してください。

    > ここで閉じるをクリックすると設定ウィザードがスキップされ、XProtect Management Clientが開きます。Management Clientでは、システムを設定できます (ハードウェアやユーザーのシステムへの追加など)。

11. ハードウェアのユーザー名とパスワードを入力ページでは、(メーカーのデフォルト値から変更した) ハードウェアのユーザー名とパスワードを入力します。

    インストーラーにより、このハードウェアのネットワークと、メーカーのデフォルト資格情報が割り当てられたハードウェアのネットワークがスキャンされます。

    続行をクリックして、ハードウェアのスキャンが完了するまで待機します。

12. システムに追加するハードウェアを選択ページで、システムに追加したいハードウェアを選択します。続行をクリックして、ハードウェアが追加されるまで待機します。

13. デバイスの設定ページでは、ハードウェア名の横にある編集アイコンをクリックすると、ハードウェアにわかりやすい名前を付けることができます。この名前は、ハードウェアデバイスの名前の先頭に付きます。

    ハードウェアノードを展開して、カメラ、スピーカー、マイクなどのハードウェアデバイスを有効または無効にします。

    > デフォルトで、カメラは有効化、スピーカーとマイクは無効化されています。

    続行をクリックして、ハードウェアが設定されるまで待機します。

14. ユーザーの追加ページでは、ユーザーをWindowsユーザーまたは基本ユーザーとしてシステムに追加できます。これらのユーザーには、管理者またはオペレーターの役割を割り当てることができます。

    ユーザーを定義し、追加をクリックします。

    ユーザーの追加が終わったら、続行をクリックします。

15. インストールと初期設定が終了すると、設定が完了しましたページが開きます。ここには以下が表示されます:
    - システムに追加されたハードウェアデバイスのリスト
    - システムに加えられたユーザーのリスト
    - ユーザーと共有できるXProtect Web ClientとXProtect Mobileクライアントへのアドレス

    閉じるをクリックするとXProtect Smart Clientが開き、利用可能になります。

システムのインストール - カスタムオプション

[カスタム]オプションでは管理サーバーがインストールされますが、現行のコンピュータに他のどのサーバー/クライアントコンポーネントをインストールするか選択することもできます。デフォルトでは、レコーディングサーバーはコンポーネントリスト内で選択されていません。選択によっては、未選択のシステムコンポーネントを後から他のコンピュータにインストールすることもできます。各システムコンポーネントとその役割の詳細については、「ページ23のメインシステムコンポーネント」を参照してください。他のコンピュータへのインストールは、Download Managerと名付けられた、マネジメントサーバーのダウンロードWebページを介して行われます。Download Managerを介したインストールの詳細については、「ページ88の新しいXProtectコンポーネントのインストール」を参照してください。

> Milestoneでは、インストールの前に以下のセクションを注意して読むようお勧めしています:ページ58のインストールを開始する前に。

> FIPSインストールでは、Windowsオペレーティングシステムで FIPSが有効になっている場合、XProtect VMSをアップグレードできません。インストールする前に、VMSに含まれているすべてのコンピューターでWindows FIPSセキュリティポリシーを無効にします(SQLサーバーをホストしているコンピューターも含まれます)。ただし、XProtect VMSバージョン2020 R3以降にアップグレードしている場合は、FIPSを無効にする必要はありません。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、強化ガイドのFIPS 140-2準拠セクションを参照してください。

1. ソフトウェアをインターネット(https://www.milestonesys.com/downloads/)からダウンロードし、`Milestone XProtect VMS製品2020 R3システムInstaller.exe`ファイルを実行します。
2. インストールファイルが展開されます。セキュリティ設定によって、1つまたは複数のWindows®セキュリティ警告が表示されます。これらを許可すると、展開が続行されます。
3. 完了すると、**Milestone XProtect VMS**インストールウィザードが表示されます。
   1. インストール中に言語を選択します(これは、インストール後にシステムによって使用される言語ではありません。これは後の段階で選択します)。続行をクリックします。
   2. *Milestone使用許諾契約*を読みます。使用許諾契約の条項に同意しますチェックボックスを選択して、続行をクリックします。
   3. ライセンスファイルの場所を入力または参照で、XProtectプロバイダーから入手したライセンスファイルを入力します。または、ファイルの場所を参照するか、**XProtect Essential+**リンクをクリックして無料ライセンスファイルをダウンロードします。無料のXProtect Essential+製品に課せられている制限については、ページ46の製品比較チャートを参照してください。続行する前に、ライセンスファイルがシステムで検証されます。続行をクリックします。
4. [カスタム]を選択します。インストールするコンポーネントリストが表示されます。マネジメントサーバーを除き、リストのすべてのコンポーネントはオプションです。デフォルトでは、レコーディングサーバーは選択されていません。[続行]をクリックします。

下記のステップにおいて、すべてのシステムコンポーネントがインストールされます。分散型システムについては、このコンピュータには少なめのシステムコンポーネントをインストールし、残りのコンポーネントは他のコンピュータにインストールします。インストールステップを認識できない場合、理由としてこのページに記されているシステムコンポーネントをインストールするよう選択していないことが考えられます。この場合は、次のステップに進みます。「ページ88の新しいXProtectコンポーネントのインストール」、「ページ88の新しいXProtectコンポーネントのインストール」、「ページ88の新しいXProtectコンポーネントのインストール」も参照してください。

5. [XProtectシステムに使用するIISのWebサイトを選択]ページは、コンピュータで複数のIIS Webサイトを利用できる場合にしか表示されません。XProtectシステムにどのWebサイトを使用するかを選択する必要があります。可能であれば、HTTPSバインドの付いたWebサイトを選択してください。このプロトコルはHTTPの高度かつ安全なバージョンです。[続行]をクリックします。

   Microsoft® IISがお使いのコンピューターにインストールされていない場合、ここでインストールされます。

6. ［Microsoft SQL Serverの選択］ページで、使用したいSQL Serverを選択します。「ページ88のSQL Serverカスタムインストール中のオプション」も参照してください。[続行] をクリックします。

   ローカルコンピュータにSQL Serverが存在しない場合はMicrosoft SQL Server Expressをインストールできますが、大規模な分散型システムにおいては通常、ネットワーク上で専用SQL Serverが使用されます。

7. ［データベースの選択］ページ(既存のSQL Serverを選択した場合にのみ表示) で、システム構成を保存するためのSQLデータベースを選択または作成します。既存のSQLデータベースを選択した場合、既存のデータを[保持]または[上書き]するかを決定します。アップグレードを行う場合は、システム設定が失われないよう既存のデータを維持するよう選択します。「ページ88のSQL Serverカスタムインストール中のオプション」も参照してください。[続行]をクリックします。

8. システム設定パスワードの割り当てページで、システム設定を保護するパスワードを入力します。システム回復時、またはシステムを拡張する際 (クラスターの追加など)、このパスワードが必要になります。

   このパスワードを保存して安全に維持しておく必要があります。このパスワードをなくした場合は、システム設定を回復する能力に支障が出る可能性があります。

   システム設定をパスワードで保護したくない場合は、システム設定パスワードを保護しないことを選択し、システム設定が暗号化されないことを承知するを選択します。

   続行をクリックします。

9. [サービスアカウントの選択]ページで、レコーディングサーバーを除く全システムコンポーネントのサービスアカウントとして、[この定義済みアカウント]または[このアカウント]のいずれかを選択します。必要に応じて、パスワードを入力します。[続行] をクリックします。

10. レコーディング サーバーのサービス アカウントを選択で、レコーディング サーバーのサービス アカウントとしてこの定義済みアカウントまたはこのアカウントのいずれかを選択します。

    必要に応じてパスワードを入力します。

    > アカウントのユーザー名は、ひとつの単語でなくてはなりません。スペースは使用できません。

    続行をクリックします。

11. レコーディング サーバーの設定ページで、様々なレコーディング サーバー設定を行います:

    1. レコーディングサーバー名フィールドに、レコーディングサーバー名を入力します。デフォルトはコンピュータ名です。
    2. 管理サーバーのアドレスフィールドに管理サーバーのアドレスとポート番号 (localhost:80) が表示されます。
    3. メディア データベース ロケーションの選択フィールドで、ビデオ録画を保存したい場所を選択します。ビデオ録画は、プログラムをインストールする場所とは別の、システム ドライブ以外の場所に保存するようMilestoneでは推奨します。デフォルトの場所は、最も容量のあるドライブです。
    4. ビデオ録画の保存期間フィールドでは、ビデオ録画の保存期間を定義します。保存期間は、7日がデフォルトで設定されていますが、1日から999日まで設定が可能です。
    5. 続行をクリックします。

12. 暗号化を選択ページでは、通信フローを安全に保護できます。

    - レコーディング サーバー、データコレクター、管理サーバー間

      内部通信フローに対して暗号化を有効にする場合は、サーバー証明書のセクションで証明書を選択してください。

      > レコーディング サーバーから管理サーバーへの通信を暗号化する場合、システムより、管理サーバーからレコーディング サーバーへの通信も暗号化する必要があります。

    - レコーディング サーバーとクライアント間

      レコーディング サーバーと、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クライアントコンポーネント間の暗号化を有効にする場合は、ストリーミング メディアの証明書セクションで、証明書を選択してください。

    - 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クライアントコンポーネント間の暗号化を有効にする場合は、モバイル 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。

    すべてのシステム コンポーネントに対して同じ証明書を使用することも、システム コンポーネントごとに異なる証明書を使用することもできます。

    安全な通信のためのシステム準備の詳細については、ページ67の安全な通信(説明付き)とMilestone証明書ガイドを参照してください。

    インストール後、通知エリアのManagement Server Managerトレイ アイコンのServer Configuratorから暗号化を有効にすることもできます。

13. ファイルの場所と製品の言語を選択ページで、プログラム ファイルのファイルの場所を選択します。

    > すでにMilestone XProtect VMSがコンピューターにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

14. 製品の言語フィールドで、どの言語でXProtect製品をインストールするのか選択します。インストールをクリックします。

    ソフトウェアがインストールされます。インストールが完了すると、正常にインストールされたシステム 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。

15. コンピュータを再起動するよう指示される場合があります。コンピュータの再起動後、セキュリティ設定によって1つまたは複数のWindowsセキュリティ警告が表示される場合があります。これらを許可すると、インストールが完了します。

16. Management Clientでシステムを構成します。ページ129の初期構成タスクリストを参照してください。

17. 選択内容によっては、Download Managerを介して他のコンピュータに残りのシステムコンポーネントをインストールします。「ページ88の新しいXProtectコンポーネントのインストール」を参照してください。

SQL Serverカスタムインストール中のオプション

どのSQL Serverとデータベースを以下のオプションと併用するかを決定します。

SQL Serverオプション:

- Microsoft® SQL Server® Expressをこのコンピュータにインストールする: このオプションは、SQL Serverがコンピュータにインストールされていない場合にのみ表示されます。
- SQL Serverをこのコンピュータで使用する: このオプションは、SQL Serverがすでにコンピュータにインストールされている場合にのみ表示されます。
- 検索を介してネットワーク上でSQL Serverを選択する: ネットワークサブネット上で検索可能なすべてのSQL Serverを検索できるようになります。
- ネットワーク上でSQL Serverを選択する: 検索を介しては見つけることができない可能性がある、SQL Serverのアドレス(ホスト名とIPアドレス)を入力できるようになります。

SQLデータベースオプション:

- 新しいデータベースを作成する: 主に新規インストール用
- 既存のデータベースを使用する: 主に既存のインストールのアップグレード用Milestoneでは、システム設定が失われないよう既存のSQLデータベースを再利用し、その中の既存のデータを維持するよう推奨しています。SQLデータベース内のデータを上書きするよう選択することも可能です。

新しいXProtectコンポーネントのインストール

Download Managerを介したインストール(説明付き)

マネジメントサーバーがインストールされているコンピュータ以外にシステムコンポーネントをインストールしたい場合は、マネジメントサーバーのダウンロードWebサイトDownload Managerを介してこれらのシステムコンポーネントをインストールする必要があります。

1. マネジメントサーバーがインストールされているコンピュータから、マネジメントサーバーのダウンロードWebページに移動します。Windowsのスタートメニューでプログラム > Milestone > 管理インストールページの順に選択し、将来、他のコンピュータにシステムコンポーネントをインストールする際に使用できるよう、インターネットアドレスを書き留めるかコピーします。アドレスは通常、*http://[management server address]/installation/Admin/default-en-US.htm*です。
2. 他のコンピュータにそれぞれログインし、他のシステムコンポーネントを1つまたは複数インストールします:
    - レコーディングサーバー(「ページ89のDownload Managerを介したレコーディングサーバーのインストール」または「ページ95の記録サーバーをサイレント・インストールします)も参照してください。
    - Management Client

- Smart Client
- イベントサーバー

> FIPS準拠環境でイベントサーバーをインストールしている場合は、インストール前にWindows FIPS 140-2モードを無効にする必要があります。

- ログサーバー
- モバイルサーバー

3. インターネットブラウザを開き、マネジメントサーバーのダウンロードWebページのアドレスをアドレスフィールドに入力して、関連するインストーラをダウンロードします。
4. インストーラを実行します。

別のインストールステップで何をどのように設定すべきか不明な場合は、ページ84のシステムのインストール - カスタムオプションを参照してください。

Download Managerを介したレコーディングサーバーのインストール

システム コンポーネントが別々のコンピュータで分散されている場合は、次の手順に従ってレコーディングサーバーをインストールできます。

> レコーディングサーバーは、シングルコンピュータインストールではすでにインストールされていますが、より多くの容量が必要な場合は、同じ手順を使用してレコーディングサーバーを追加することができます。

> フェールオーバーレコーディングサーバーのインストールが必要な場合は、「ページ88の新しいXProtectコンポーネントのインストール」を参照してください。

1. マネジメントサーバーがインストールされているコンピュータから、マネジメントサーバーのダウンロードWebページに移動します。Windowsのスタート メニューでプログラム > **Milestone** > 管理インストール ページの順に選択し、将来、他のコンピュータにシステム コンポーネントをインストールする際に使用できるよう、インターネットアドレスを書き留めるかコピーします。アドレスは通常、*http://[management server address]/installation/Admin/default-en-US.htm*です。
2. レコーディングサーバーをインストールしたいコンピュータにログインします。
3. インターネットブラウザを開き、マネジメントサーバーのダウンロードWebページのアドレスをアドレスフィールドに入力して、Enterキーを押します。
4. レコーディング サーバー インストーラーの下にあるべての言語]を選択して、レコーディング サーバーのインストーラーをダウンロードします。インストーラーを保存するか、Webページから直接実行します。

5. インストール中に使用する言語を選択します。続行をクリックします。
6. [インストールの種類を選択]ページで以下を選択します:

   [標準]: デフォルト値を使用してレコーディングサーバーをインストールします。

   [カスタム]: カスタム値を使用してレコーディング サーバーをインストールします。
7. レコーディング サーバーの設定ページで、様々なレコーディング サーバー設定を行います:
   1. レコーディングサーバー名フィールドに、レコーディングサーバー名を入力します。デフォルトはコンピュータ名です。
   2. 管理サーバーのアドレスフィールドに管理サーバーのアドレスとポート番号 (localhost:80) が表示されます。
   3. メディア データベース ロケーションの選択フィールドで、ビデオ録画を保存したい場所を選択します。ビデオ録画は、プログラムをインストールする場所とは別の、システム ドライブ以外の場所に保存するようMilestoneでは推奨します。デフォルトの場所は、最も容量のあるドライブです。
   4. ビデオ録画の保存期間フィールドでは、ビデオ録画の保存期間を定義します。保存期間は、7日がデフォルトで設定されていますが、1日から999日まで設定が可能です。
   5. 続行をクリックします。
8. [レコーディングサーバーのIPアドレス]ページは、[カスタム]を選択した場合にのみ表示されます。このコンピュータにインストールするRecording Serverの数を指定します。[続行] をクリックします。
9. レコーディング サーバーのサービス アカウントを選択で、レコーディング サーバーのサービス アカウントとしてこの定義済みアカウントまたはこのアカウントのいずれかを選択します。

   必要に応じてパスワードを入力します。

   > アカウントのユーザー名は、ひとつの単語でなくてはなりません。スペースは使用できません。

   続行をクリックします。

10. 暗号化を選択ページでは、通信フローを安全に保護できます。

    - レコーディング サーバー、データコレクター、管理サーバー間

      内部通信フローに対して暗号化を有効にする場合は、サーバー証明書のセクションで証明書を選択してください。

      > レコーディング サーバーから管理サーバーへの通信を暗号化する場合、システムより、管理サーバーからレコーディング サーバーへの通信も暗号化する必要があります。

    - レコーディング サーバーとクライアント間

      レコーディング サーバーと、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クライアントコンポーネント間の暗号化を有効にする場合は、ストリーミング メディアの証明書セクションで、証明書を選択してください。

    - 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クライアントコンポーネント間の暗号化を有効にする場合は、モバイル 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。

    すべてのシステム コンポーネントに対して同じ証明書を使用することも、システム コンポーネントごとに異なる証明書を使用することもできます。

    安全な通信のためのシステム準備の詳細については、ページ67の安全な通信(説明付き)とMilestone証明書ガイドを参照してください。

    インストール後、通知エリアのManagement Server Managerトレイ アイコンのServer Configuratorから暗号化を有効にすることもできます。

11. ファイルの場所と製品の言語を選択ページで、プログラム ファイルのファイルの場所を選択します。

    > すでにMilestone XProtect VMSがコンピューターにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

12. 製品の言語フィールドで、どの言語でXProtect製品をインストールするのか選択します。インストールをクリックします。

    ソフトウェアがインストールされます。インストールが完了すると、正常にインストールされたシステム 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。

13. フェールオーバーレコーディングサーバーがインストールされれば、Management Clientトレーアイコンでその状態を確認し、Recording Server Manager内でその設定を行うことができます。詳細については、ページ129の初期構成タスクリストを参照してください。

Download Managerを介したフェールオーバーレコーディングサーバーのインストール

ワークグループを実行している場合は、フェールオーバーレコーディングサーバーの代替インストール方法を使用する必要があります(ページ98のワークグループのインストールを参照)。

1. マネジメントサーバーがインストールされているコンピュータから、マネジメントサーバーのダウンロードWebページに移動します。Windowsのスタートメニューでプログラム > **Milestone** > 管理インストールページの順に選択し、将来、他のコンピュータにシステムコンポーネントをインストールする際に使用できるよう、インターネットアドレスを書き留めるかコピーします。アドレスは通常、*http://[management server address]/installation/Admin/default-en-US.htm*です。
2. フェールオーバーレコーディングサーバーをインストールしたいコンピュータにログインします。
3. インターネットブラウザを開き、マネジメントサーバーのダウンロードWebページのアドレスをアドレスフィールドに入力して、レコーディングサーバーインストーラをダウンロードします。インストーラを保存するか、Webページから直接実行します。
4. レコーディングサーバーインストーラーの下にあるべての言語]を選択して、レコーディングサーバーのインストーラーをダウンロードします。インストーラーを保存するか、Webページから直接実行します。
5. インストール中に使用する言語を選択します。続行をクリックします。
6. [インストールの種類を選択]ページで[フェールオーバー]を選択し、レコーディングサーバーをフェールオーバーレコーディングサーバーとしてインストールします。
7. レコーディングサーバーの設定ページで、様々なレコーディングサーバーの設定を行います。フェールオーバーレコーディングサーバーの名前、管理サーバーのアドレス、メディアデータベースへのパス。続行をクリックします。
8. フェイルオーバーレコーディングサーバーをインストールする際には、[レコーディングサーバーのサービスアカウントを選択]ページで[このアカウント]と名付けられた特定のユーザーアカウントを使用する必要があります。これにより、フェールオーバーユーザーアカウントが作成されます。必要に応じて、パスワードを入力して確認します。[続行]をクリックします。

9. 暗号化を選択ページでは、通信フローを安全に保護できます。

   - レコーディング サーバー、データコレクター、管理サーバー間

     内部通信フローに対して暗号化を有効にする場合は、サーバー証明書のセクションで証明書を選択してください。

     > レコーディング サーバーから管理サーバーへの通信を暗号化する場合、システムより、管理サーバーからレコーディング サーバーへの通信も暗号化する必要があります。

   - レコーディング サーバーとクライアント間

     レコーディング サーバーと、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クライアントコンポーネント間の暗号化を有効にする場合は、ストリーミング メディアの証明書セクションで、証明書を選択してください。

   - 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クライアントコンポーネント間の暗号化を有効にする場合は、モバイル 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。

   すべてのシステム コンポーネントに対して同じ証明書を使用することも、システム コンポーネントごとに異なる証明書を使用することもできます。

   安全な通信のためのシステム準備の詳細については、ページ67の安全な通信(説明付き)とMilestone証明書ガイドを参照してください。

   インストール後、通知エリアのManagement Server Managerトレイ アイコンのServer Configuratorから暗号化を有効にすることもできます。

10. ファイルの場所と製品の言語を選択ページで、プログラム ファイルのファイルの場所を選択します。

    > すでにMilestone XProtect VMSがコンピューターにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

11. 製品の言語フィールドで、どの言語でXProtect製品をインストールするのか選択します。インストールをクリックします。

    ソフトウェアがインストールされます。インストールが完了すると、正常にインストールされたシステム 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。

12. フェールオーバーレコーディングサーバーがインストールされると、フェールオーバーサーバーサービストレーアイコンでその状態を確認し、Management Client内でその設定を行うことができます。詳細については、ページ129の初期構成タスクリストを参照してください。

コマンドラインシェルを介したサイレントインストール(説明付き)

システム管理者はサイレントインストールを実行することで、該当するユーザーの介入なく、エンドユーザーへの影響を最小限に抑える形で、大規模なネットワークにわたってレコーディングサーバーとSmart Clientソフトウェアをインストールおよびアップグレードできます。

レコーディングサーバーとSmart Clientインストーラー(.exeファイル)のコマンドライン引数は異なります。それぞれが特有のコマンドラインパラメータセットを有しており、これらはコマンドラインシェルまたは引数ファイルを介して直接呼び出すことができます。コマンドラインシェルでは、インストーラに付属のコマンドラインオプションも使用できます。

Microsoft System Center Configuration Manager (SCCMまたはConfigMgrとも呼ばれます)のように、XProtectインストーラー、そのコマンドラインパラメータ、コマンドラインオプションを、サイレント配布およびソフトウェアインストール用のツールと組み合わせることができます。このようなツールの詳細については、メーカーのウェブサイトを参照してください。またMilestone Software Managerを、レコーディングサーバー、デバイスパック、Smart Clientのリモートインストールおよび更新に使用することもできます。詳細については、Milestone Software Managerのマニュアルを参照してください。

コマンドラインパラメータと引数ファイル

サイレントインストール中は、さまざまなVNSシステムコンポーネントと密接にリンクしている設定に加え、コマンドラインパラメータと引数ファイルを用いてその内部通信を指定することができます。コマンドラインパラメータと引数ファイルは、新規インストールにおいてのみ使用してください。これは、コマンドラインパラメータによって表される設定はアップグレード中には変更できないためです。

利用可能なコマンドラインパラメータを表示し、インストーラ用の引数ファイルを生成するには、コマンドラインシェルでインストーラが配置されているディレクトリに移動し、以下のコマンドを入力します:

```
[NameOfExeFile].exe --generateargsfile=[path]
```

例:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

保存された引数ファイル(Arguments.xml)内では、コマンドラインパラメータごとにその目的についての記述が添えられます。コマンドラインパラメータの値がインストールのニーズに適合するよう、引数ファイルを修正したうえで保存することができます。

インストーラで引数ファイルを使用したい場合は、以下のコマンドを入力することで`--arguments`コマンドラインオプションを使用します:

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

例:

```
MilestoneXProtectRecordingServerInstaller_ x64.exe --quiet
--arguments=C:\temp\arguments.xml
```

コマンドラインオプション

コマンドラインシェルでは、インストーラをコマンドラインオプションと組み合わせることもできます。コマンドラインオプションは通常、コマンドの動作を修正させる目的で使用します。

コマンドラインオプションの全リストを表示するには、コマンドラインシェルでインストーラが配置されているディレクトリに移動し、`[NameOfExeFile].exe --help`と入力します。インストールを成功させるためには、値を必要とするコマンドラインオプションに対して値を指定する必要があります。

コマンドラインパラメータとコマンドラインオプションは、両方とも同一のコマンド内で使用できます。その際、`--parameters`コマンドラインオプションを使用し、それぞれのコマンドラインパラメータをコロン(:) で区切ります。以下の例では、`--quiet`、`--showconsole`、`--parameters`はコマンドラインオプションである一方、`ISFAILOVER`と`RECORDERNAME`はコマンドラインパラメータとなっています:

```
MilestoneXProtectRecordingServerInstaller_ x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

記録サーバーをサイレント・インストールします

サイレントインストール時には、インストールが完了しても通知が送られません。通知を受けるには、コマンドに`--showconsole`コマンドラインオプションを加えます。インストールが完了すると、Milestone XProtect Recording Serverトレイアイコンが表示されます。

以下のコマンドラインの例では、角括弧([ ]) 内のテキストを角括弧ごと実数値に置き換える必要があります。例: [パス]の代わりに、**d:\program files**、**d:\record**、**\\network-storage-02\surveillance**などと入力します。`--help`コマンドラインオプションを使用すれば、各コマンドラインオプション値の正規形式について確認できます。

1. レコーディングサーバーコンポーネントをインストールするコンピュータにログインします。
2. インターネットブラウザを開き、管理者を対象としたマネジメントサーバーのダウンロード用ウェブページのアドレスをアドレスフィールドに入力し、Enterを押します。

   アドレスは通常、http://[マネジメントサーバーのアドレス]:[port]/installation/Admin/default-en-US.htmとなっています。
3. [Recording Serverインストーラ]の下にある [すべての言語] を選択して、レコーディングサーバーインストーラをダウンロードします。
4. 希望のコマンドラインシェルを開きます。Windowsコマンドプロンプトを開くには、Windowsの [スタート] メニューを開

いてcmdと入力します。

5. ダウンロードしたインストーラが保存されているディレクトリに移動します。
6. 以下の2通りのシナリオのいずれであるかに応じて、インストールを続行します：

シナリオ1：既存のインストールをアップグレードするか、マネジメントサーバーコンポーネントと併せてデフォルトの値でサーバーにインストールします

- 以下のコマンドを入力してインストールを開始します。

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

シナリオ2：分散システムにインストールする

1. 以下のコマンドを入力して、コマンドラインパラメータが記された引数ファイルを生成します。

```
MilestoneXProtectRecordingServerInstaller_ x64.exe   --generateargsfile=
[path]
```

2. 指定したパスから引数ファイル(Arguments.xml) を開き、必要に応じてコマンドラインパラメータの値を修正します。

> SERVERHOSTNAME とSERVERPORTのコマンドラインパラメータに有効な値が指定されていることを確認します。そうでない場合、インストールは完了しません。

4. 引数ファイルを保存します。
5. コマンドラインシェルに戻り、以下のコマンドを入力することで、引数ファイルで指定したコマンドラインパラメータ値でインストールを実行します。

```
MilestoneXProtectRecordingServerInstaller_x64.exe  --quiet  --arguments=
[path]\[filename]
```

XProtect Smart Clientサイレントインストール

サイレントインストール時には、インストールが完了しても通知が送られません。通知を受けるには、コマンドに`--showconsole`コマンドラインオプションを加えます。インストールが完了するとXProtect Smart Clientへのショートカットがデスクトップに表示されます。

以下のコマンドラインの例では、角括弧([ ]) 内のテキストと角括弧そのものを実数値に置き換える必要があります。例：[パス]の代わりに、**d:\program files**、**d:\record**、**\\network-storage-02\surveillance**などと入力します。`--help`コマンドラインオプションを使用すれば、各コマンドラインオプション値の正規形式について確認できます。

1. インターネットブラウザを開き、エンドユーザーを対象としたマネジメントサーバーのダウンロード用ウェブページのアドレスをアドレスフィールドに入力し、Enterを押します。

   アドレスは通常、http://[マネジメントサーバーのアドレス]:[port]/installation/default-en-US.htmとなっています。

2. [**XProtect Smart Client**インストーラ]の下にある[すべての言語]を選択して、XProtect Smart Clientインストーラをダウンロードします。

3. 希望のコマンドラインシェルを開きます。Windowsコマンドプロンプトを開くには、Windowsの[スタート]メニューを開いて**cmd**と入力します。

4. ダウンロードしたインストーラが保存されているディレクトリに移動します。

5. 以下の2通りのシナリオのいずれであるかに応じて、インストールを続行します：

   シナリオ**1**：既存のインストールをアップグレードするか、デフォルトのコマンドラインパラメータ値でインストールする

   - 以下のコマンドを入力してインストールを開始します。

     ```
     XProtect Smart Client 2020 R3 Installer.exe --quiet
     ```

   シナリオ**2**：**xml**引数をインプットとして使用して、コマンドラインパラメータのカスタム値でインストールする

   1. 以下のコマンドを入力して、コマンドラインパラメータが記された引数**xml**ファイルを生成します。

      ```
      XProtect Smart Client 2020 R3 Installer.exe --generateargsfile=[path]
      ```

   2. 指定したパスから引数ファイル(Arguments.xml) を開き、必要に応じてコマンドラインパラメータの値を修正します。

   3. 引数ファイルを保存します。

   4. コマンドラインシェルに戻り、以下のコマンドを入力することで、引数ファイルで指定したコマンドラインパラメータでインストールを実行します。

      ```
      XProtect Smart Client 2020 R3 Installer.exe --quiet --arguments=[path]\
      [filename]
      ```

ワークグループのインストール

Active Directoryサーバーのドメイン設定ではなく、ワークグループ設定を使用する場合は、インストール時に以下を実行します。

1. 共通管理者アカウントを使用して、Windowsへログインします。

   システムのすべてのコンピュータで同じアカウントを使用していることを確認します。

2. 必要に応じて、マネジメントサーバーまたはレコーディングサーバーのインストールを開始し、カスタムをクリックします。
3. 手順2の選択に応じて、共通のシステム管理者アカウントを使用して、マネジメントサーバーまたはレコーディングサーバーのインストールを選択します。
4. インストールを終了します。
5. 手順1～4を繰り返し、接続する他のすべてのシステムをインストールします。これらはすべて、共通管理者アカウントを使用してインストールしなければなりません。

ワークグループインストールをアップグレードする場合は、この方法を使用できません。代わりに、ページ477のワークグループ設定内でのアップグレードを参照してください。

クラスタへのインストール

クラスタにインストールする前に、ページ55の複数のマネジメントサーバー(クラスタリング)(説明付き)とページ56のクラスタリングの要件を参照してください。

ここでの説明と図は、実際に画面上に表示されるものとは異なる場合があります。

インストールとURLアドレスの変更:

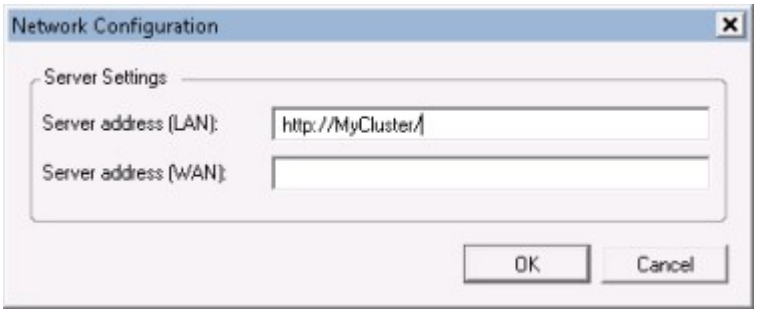
1. マネジメントサーバーと、そのすべてのサブコンポーネントをクラスタ内の最初のサーバーにインストールします。

   マネジメントサーバーはネットワークサービスとしてではなく、指定ユーザーと併せてインストールする必要があります。これには、[カスタム]インストールオプションを使用する必要があります。また、指定ユーザーには共有ネットワークドライブへのアクセスと、可能であれば無期限のパスワードを割り当てる必要があります。

2. マネジメントサーバーとManagement Clientをクラスタ内の最初のサーバーにインストールしたら、Management Clientを開き、[ツール]メニューで[登録済みサービス]を選択します。

1. [登録済みサービスの追加/削除]ウィンドウで[ログサービス]を選択し、[編集]をクリックします。
2. [登録済みサービスの編集]ウィンドウで、ログサービスのURLアドレスをクラスタのURLアドレスに変更します。

3. このステップを、[登録済みサービスの追加/削除]ウィンドウにリストされている全サービスに対して繰り返します。[ネットワーク]をクリックします。
4. [ネットワーク設定]ウィンドウで、サーバーのURLアドレスをクラスターのURLアドレスに変更します。(このステップはクラスター内の最初のサーバーにのみ適用されます。)[OK]をクリックします。



5. [登録済みサービスの追加と削除]ウィンドウで[閉じる]をクリックします。Management Clientを終了します。
6. マネジメントサーバーサービスとIISを停止します。IISを停止する方法については、Microsoft Webサイト(https://technet.microsoft.com/library/cc732317(WS.10).aspx/)を参照してください。
7. クラスタ内のすべての後続サーバーに対してこれらのステップを繰り返しますが、その際は既存のSQL Serverとデータベースをポイントします。ただし、マネジメントサーバーをインストールすることになる、クラスタ内の最後のサーバーについては、マネジメントサーバーサービスを停止しないでください。

マネジメントサーバーサービスを、フェールオーバークラスタ内の汎用サービスとして構成します:

1. マネジメントサーバーをインストールした最後のサーバーで[スタート] > [管理ツール]に移動し、Windowsのフェールオーバークラスタ管理を開きます。[フェールオーバークラスター管理]ウィンドウでクラスターを展開し、[サービスとアプリケーション]を右クリックして[サービスまたはアプリケーションとして設定]を選択します。

2. [高可用性]ダイアログボックスで[次へ]をクリックします。
3. [汎用サービス] を選択して[次へ]をクリックします。
4. ダイアログボックスの3ページ目では何も指定せずに、[次へ]をクリックします。
5. **Milestone XProtect Management Server**サービスを選択し、[次へ]をクリックします。サービスへのアクセス時にクライアントによって使用される名前(クラスタのホスト名)を指定し、[次へ]をクリックします。
6. サービスにストレージは不要なため、[次へ]をクリックします。レジストリ設定を複製せずに、[次へ]をクリックします。クラスタサービスが適宜に設定されていることを確認してから、[次へ]をクリックします。これで、マネジメントサーバーがフェールオーバークラスタ内の汎用サービスとして設定されます。[終了] をクリックします。
7. クラスタの設定では、イベントサーバーとData Collectorはマネジメントサーバーの依存サービスとして設定する必要があるため、マネジメントサーバーが停止するとイベントサーバーも停止します。
8. **Milestone XProtect Event Server**サービスをリソースとして**Milestone XProtect Management Server Cluster**サービスに追加するには、クラスタサービスを右クリックして[リソースの追加] > [4 - 汎用サービス]を選択してから、**Milestone XProtect Event Server**を選択します。

以下の構成設定を修正します:

マネジメントサーバーノードにおいて:

- C:\ProgramData\Milestone\XProtectマネジメントサーバー**ServerConfig.xml**で:

```
<AuthorizationServerUri>http://ClusterRoleAddress/IDP</AuthorizationServerUri>
```

- C:\Program Files\Milestone\XProtectマネジメントサーバー\IIS\IDP**appsettings.json**:

```
"Authority": "http://ClusterRoleAddress/IDP"
```

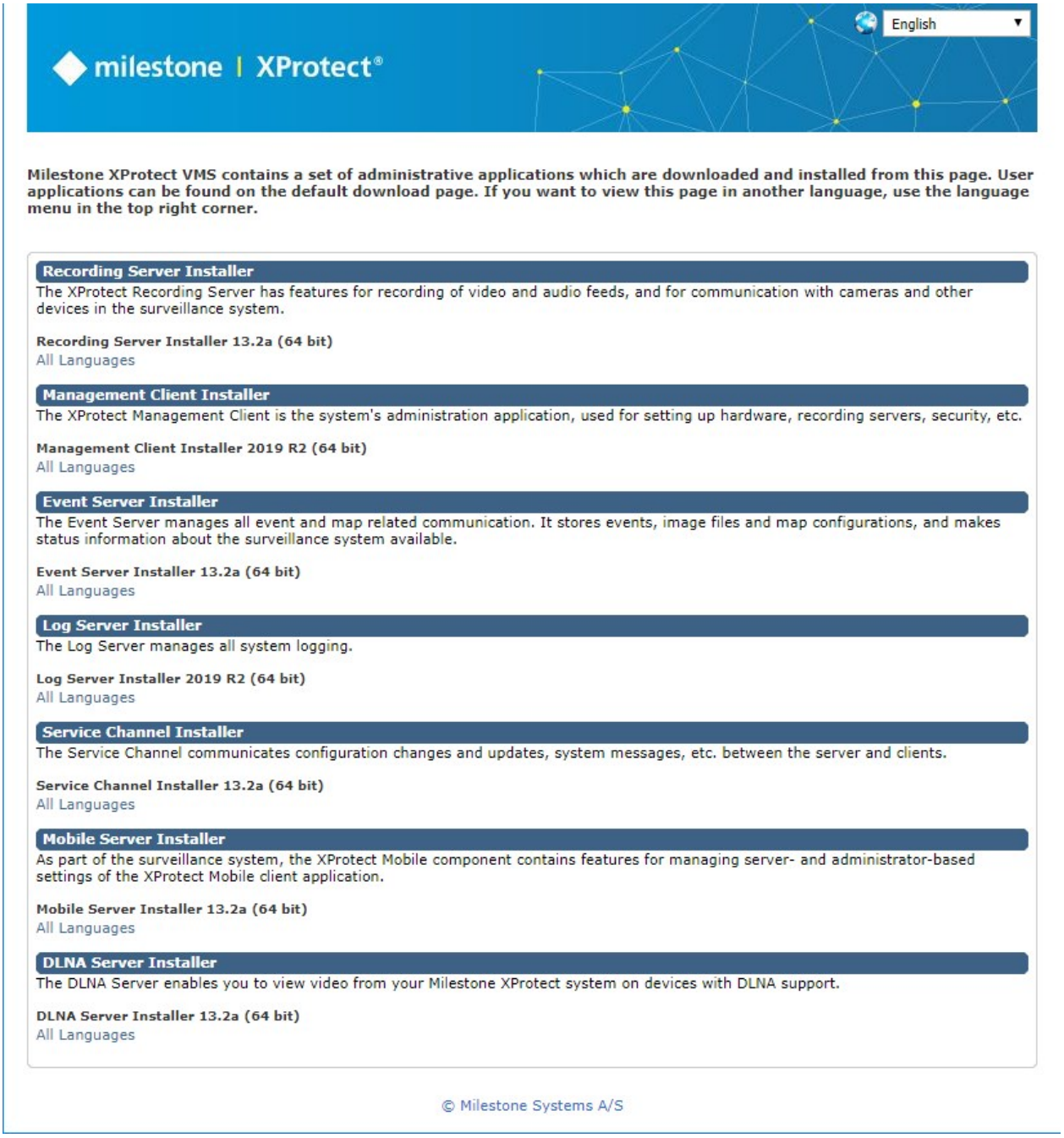
レコーディングサーバーで、authorizationserveraddressもクラスタ役割アドレスに設定されていることを確認します:

C:\ProgramData\Milestone\XProtectレコーディングサーバー**RecorderConfig.xml**で:

```
<authorizationserveraddress>http://ClusterRoleAddress/IDP</authorizationserveraddress>
```

Download Manager/ダウンロードWebページ

ManagementServerには、組み込みWebページがあります。このWebページを使うと、管理者やエンドユーザーはXProtectシステムの必要なコンポーネントを、任意の場所から(ローカルまたはリモートで) ダウンロードしてインストールすることができます。



このWebページは、デフォルトで、システムインストールの言語と一致する言語バージョンで、次の2種類のコンテンツを表示できます。

- 管理者向けのWebページでは、主要な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。通常、Webページはマネジメントサーバーのインストール終了後に自動的に読み込まれ、デフォルトのコンテンツが表示されます。マネジメントサーバーで、Windowsの[スタート]メニューから[プログラム]>Milestone>[管理インストールページ]の順に選択すると、Webページにアクセスできます。それ以外の場合は、以下のURLを入力してください。

  http://[マネジメントサーバーのアドレス]:[ポート]/installation/admin/

  [管理サーバーのアドレス]は管理サーバーのIPアドレスまたはホスト名であり、[ポート]は管理サーバーでIISが使用するように設定されたポート番号です。

- エンドユーザー向けのWebページでは、デフォルト設定を使用してクライアントアプリケーションにアクセスできます。マネジメントサーバーで、Windowsの[スタート]メニューから[プログラム]>Milestone>[公開インストールページ]の順に選択すると、Webページにアクセスできます。それ以外の場合は、以下のURLを入力してください。

  http://[マネジメントサーバーのアドレス]:[ポート]/installation/

  [管理サーバーのアドレス]は管理サーバーのIPアドレスまたはホスト名であり、[ポート]は管理サーバーでIISが使用するように設定されたポート番号です。

2つのWebページにはデフォルトのコンテンツがあるため、インストール後すぐに使用できます。なお、システム管理者としてDownload Managerを使用すると、Webページの表示内容をカスタマイズできます。また、Webページの2つのバージョン間で、コンポーネントを移動することもできます。コンポーネントを移動するには、コンポーネントをクリックし、コンポーネントを移動するWebページのバージョンをクリックします。

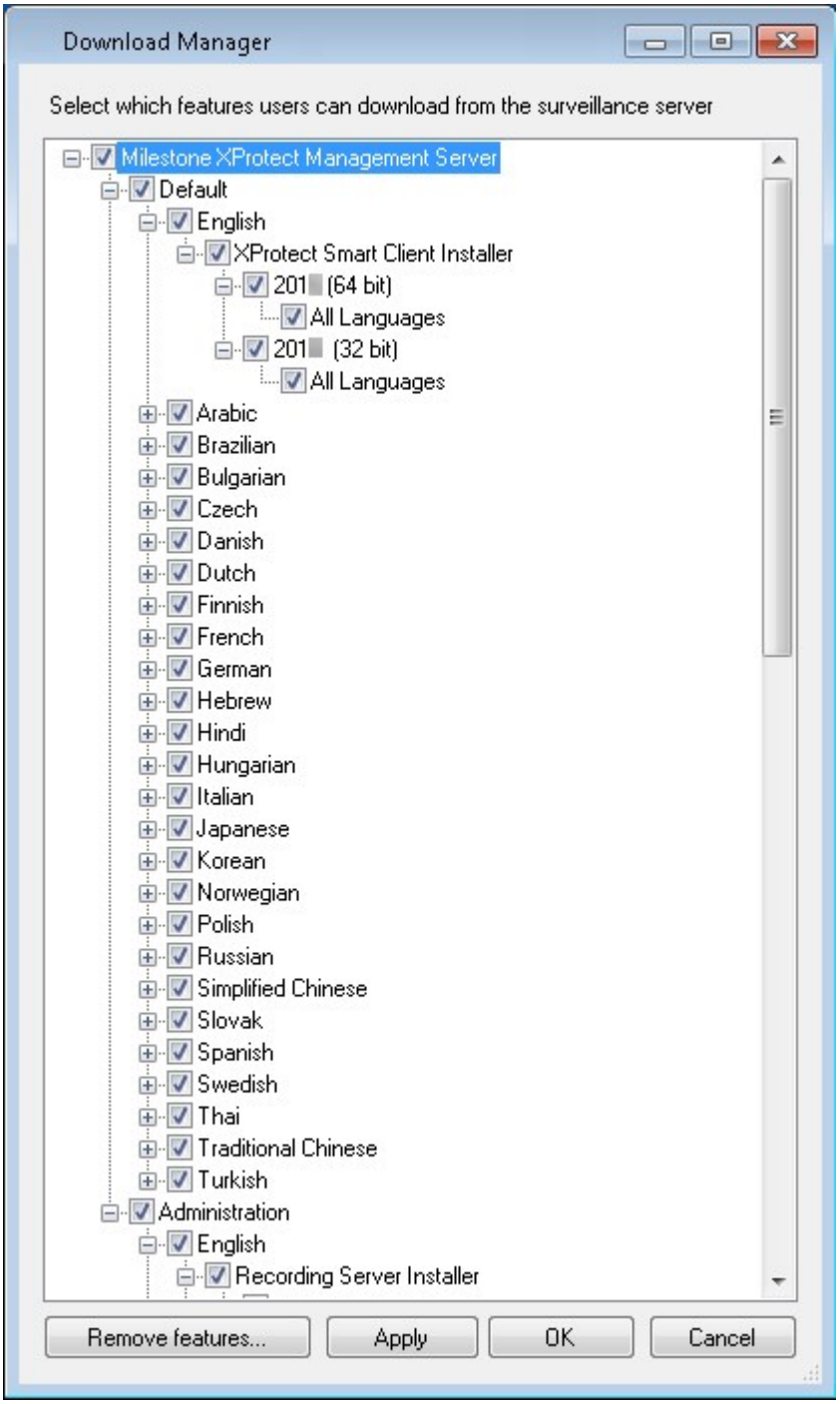
Download Managerでは、ユーザーがダウンロードしてインストールできるコンポーネントを制御できますが、ユーザーの権限管理ツールとして使用することはできません。こうした権限は、Management Clientで定義された役割によって決まります。

マネジメントサーバーで、Windowsの[スタート]メニューから[プログラム]>Milestone>XProtect Download Managerの順に選択しすれば、XProtect Download Managerにアクセスできます。

Download Managerのデフォルト設定

Download Managerには、デフォルトの設定があります。これにより、組織のユーザーは最初から標準のコンポーネントにアクセスできます。

デフォルト設定では、追加またはオプションのコンポーネントをデフォルト設定によってダウンロードできます。通常は、管理サーバーコンピュータからWebページにアクセスしますが、他のコンピュータからWebページにアクセスすることもできます。



- 1番目のレベル：XProtect製品を参照します。
- 2番目のレベル：Webページの2つの対象バージョンを示しています。デフォルトは、エンドユーザーに表示されるWebページのバージョンを示しています。[システム管理]は、システム管理者に表示されるWebページのバージョンを示しています。
- 3番目のレベル：Webページで使用できる言語を示しています。

- 4番目のレベル: ユーザーが使用できるか、使用可能にできるコンポーネントを示しています。
- 5番目のレベル: ユーザーが使用できるか、使用可能にできる各コンポーネントの特定のバージョンを示しています。
- 6番目のレベル: ユーザーが使用できるか、使用可能にできるコンポーネントの言語バージョンを示しています。

初期状態では標準のコンポーネントだけが使用可能であり、システムと同じ言語バージョンだけが使用可能になっていることで、インストールの時間を短縮し、サーバーのディスク容量を節約するのに役立ちます。誰も使用しないコンポーネントや言語バージョンがサーバーに存在する必要はないためです。

必要に応じてその他のコンポーネントや言語を使用可能にできます。また、不要なコンポーネントや言語を非表示にしたり削除したりできます。

Download Managerの標準インストーラ(ユーザー)

デフォルトでは、次のコンポーネントは、ユーザー向けの管理サーバーのダウンロードWebページから個別にインストールできます(Download Managerで制御)。

- フェールオーバーレコーディングサーバーを含む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は、最初にレコーディングサーバーとしてダウンロードおよびインストールされます。インストール処理中に、フェールオーバーレコーディングサーバーにすることを指定します。
- Management Client
- XProtect Smart Client
- イベントサーバー、マップ機能と組み合わせて使用されます。
- Logサーバーはシステム情報のロギングに必要な機能を提供するために使用されます。
- XProtect Mobileサーバー
- 組織によって、より豊富なオプションを利用できます。

デバイスパックのインストールについては、「ページ106のDevice Packのインストーラ- ダウンロードする必要があります」を参照してください。

Download Managerインストーラコンポーネントの追加/公開

次の2つの手順を実行し、標準以外のコンポーネントおよび新しいバージョンを管理サーバーのダウンロードページで使用可能にする必要があります。

最初に、新規/非標準コンポーネントをDownload Managerに追加します。次に、これを使用して、さまざまな言語バージョンのWebページで、どのコンポーネントを使用可能にするかを微調整します。

Download Managerが開いている場合は、閉じてから、新しいコンポーネントをインストールします。

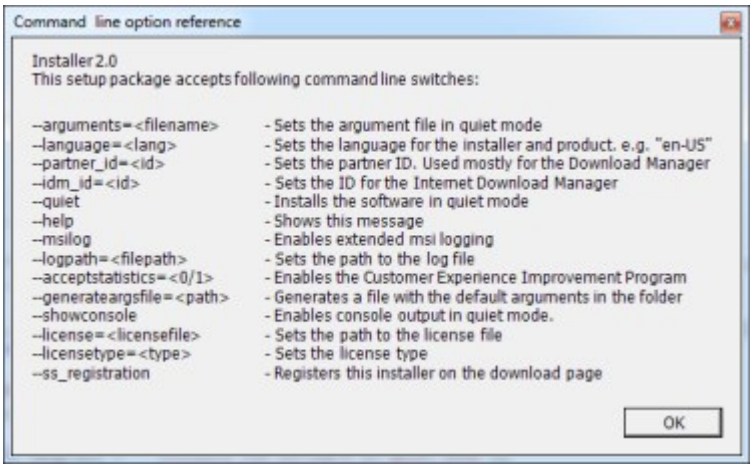
新規/非標準ファイルをDownload Managerに追加:

1. コンポーネントをダウンロードしたコンピュータで、Windowsの[スタート]に移動し、*コマンドプロンプト*に入ります。
2. *コマンドプロンプト*で、ファイル名(*.exe*) に[space]*--ss_registration*を付けて実行します。

   例: *MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

   これでファイルはDownload Managerに追加されましたが、現在お使いのコンピュータにはまだインストールされていません。

> インストーラコマンドの概要を取得するには、*コマンドプロンプト*で[スペース]*--help*と入力することで、以下のウィンドウを開きます:



新しいコンポーネントをインストールすると、Download Managerでデフォルトで選択され、Webページからすぐに使用可能になります。Download Managerのツリー構造でチェックボックスを選択または選択解除することで、Webページでいつでも機能を表示または非表示にすることができます。

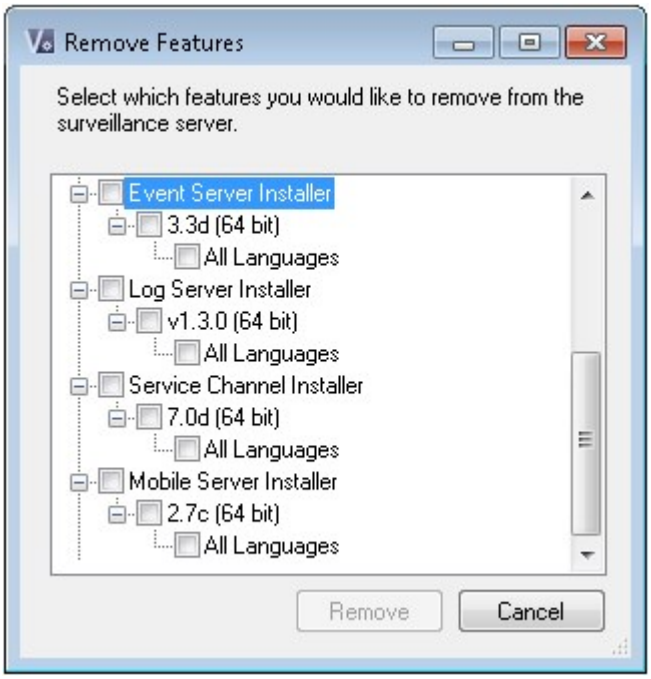
Webページで、コンポーネントが表示される順番を変更できます。Download Managerのツリー構造で、コンポーネントアイテムをドラッグして必要な場所でドロップすると、順番を変更できます。

Download Managerインストーラコンポーネントを非表示化/削除

次の3つのオプションがあります:

- のツリー構造のチェックボックスをクリアして、Webページからのコンポーネントを非表示にするDownload Managerことができます。コンポーネントはマネジメントサーバーにインストールされたままであり、Download Managerのツリー構造のチェックボックスを選択することで、迅速にコンポーネントを再び利用可能にできます。

- 管理サーバーにあるコンポーネントのインストールを削除します。コンポーネントはDownload Managerに表示されなくなりますが、コンポーネントのインストールファイルは*C:\Program Files (x86)\Milestone\XProtect Download Manager*に保存されるため、必要であれば、この後再インストールすることができます。
  1. Download Managerで、機能の削除をクリックします。
  2. 機能の削除ウィンドウで、削除する機能を選択します。



  3. **OK**とはいをクリックします。

- 不要な機能のインストールファイルは、マネジメントサーバーから削除できます。組織では使用しない機能が分かっている場合、これによって、サーバーのディスク容量を削減するのに役立ちます。

Device Packのインストーラ- ダウンロードする必要があります

元のインストールに含まれていたDevice Pack(デバイスドライバーを含む) は、Download Managerには含まれていません。このため、Device Packを再インストールするか、またはDevice Packインストーラを使用可能にするためには、Download Managerに最新のDevice Packインストーラを追加/公開する必要があります。

1. Milestone Webサイト(https://www.milestonesys.com/downloads/) のダウンロードのページで、最新のデバイスパックが入手できます。
2. 同じページにて、レガシードライバーでDevice Packをダウンロードできます。お使いのカメラが、レガシーデバイスパックのドライバーを使用しているかは、このWebサイト(https://www.milestonesys.com/community/business-partner-tools/device-packs/) で確認できます。
3. *--ss_registration*コマンドを使用して呼び出し、Download Managerに追加/発行します。

ネットワークに接続していない場合は、Download Managerからレコーディングサーバー全体を再インストールできます。レコーディングサーバーのインストールファイルは、コンピュータにローカル保存されます。これにより、デバイスパックが自動的に再インストールされます。

インストールログファイルとトラブルシューティング

インストール、アップグレード、アンインストール中は、以下をはじめとするさまざまなインストールログファイルにログエントリが書き込まれます：メインインストールログファイルであるinstaller.logと、インストールしている各種システムコンポーネントに属しているログファイル。いずれのログエントリにもタイムスタンプが刻まれ、最新のログエントリがログファイルの末尾に配置されます。

インストールログファイルはいずれもC:\ProgramData\Milestone\Installer\フォルダーに配置されます。 *I.logまたは*I[整数].logという名前を付けられたログファイルは新規インストールまたはアップグレードに関するログファイルです。一方、*U.logまたは*U[整数].logと名付けられたログファイルはアンインストールに関するものです。Milestoneパートナーを介して、XProtectシステムがインストール済みのサーバーを購入した場合は、インストールログファイルがない可能性があります。

ログファイルには、インストール、アップグレード、アンインストール中に使用される、コマンドラインパラメータとコマンドラインオプション、そしてその値に関する情報が記されます。使用したコマンドラインパラメータをログファイルで探すには、ログファイルの種類に応じて、**Command Line:**または**Parameter '**を検索します。

トラブルシューティングの際には、メインインストールログファイルを最初に調べることになります。インストール中に例外、エラー、警告が発生した場合、これらが記録されます。例外、エラー、警告がないか検索してみてください。「Exitcode:0」はインストールに成功したことを、「Exit code: 1」はその逆を表します。ログファイルでの情報をもとに、https://supportcommunity.milestonesys.com/s/knowledgebase?language=en_US/で解決策を特定できる可能性があります。それができない場合は、Milestoneパートナーにお問い合わせのうえ、該当するインストールログファイルを提供してください。

設定

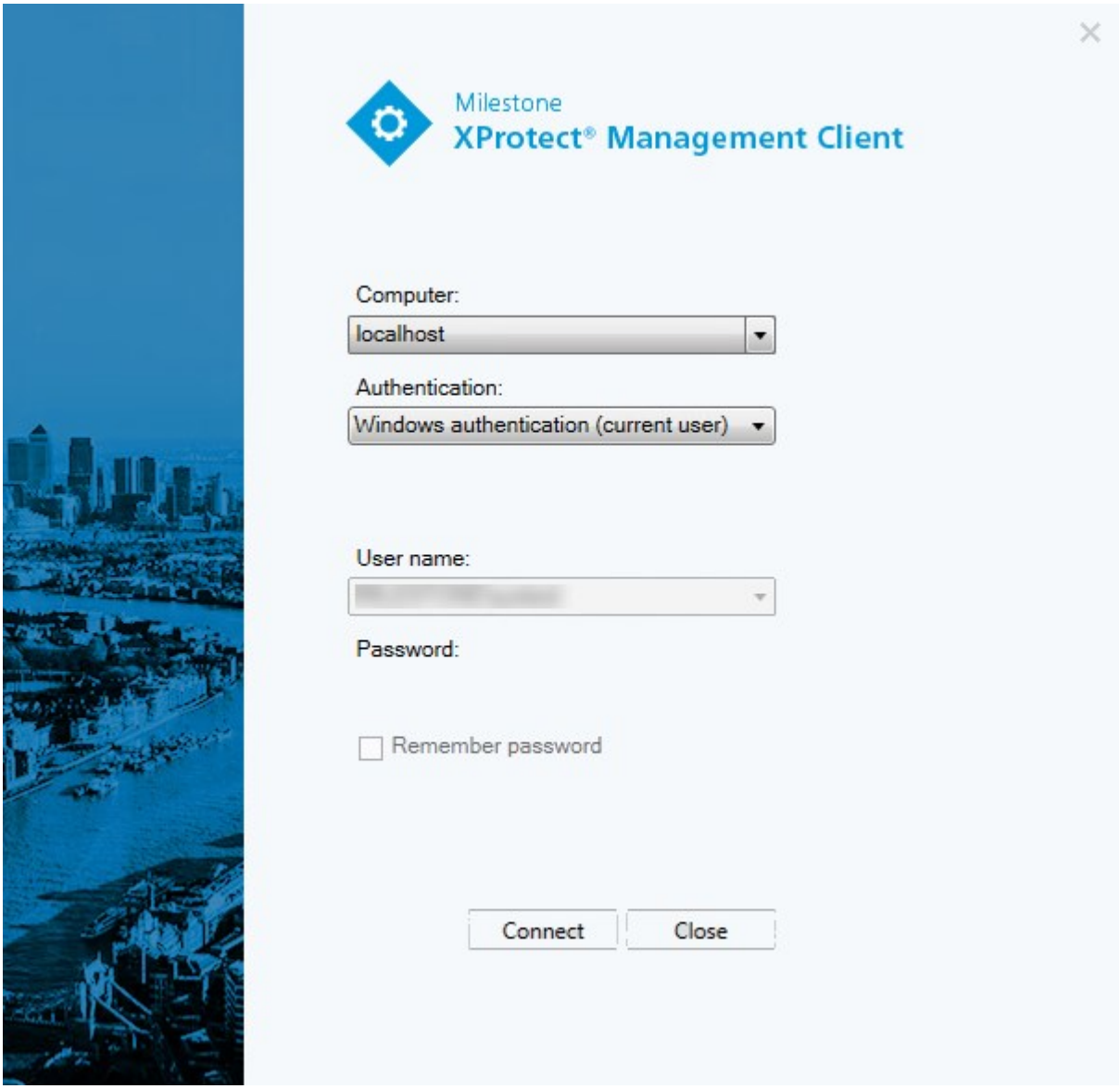
Management Clientをナビゲーション

このセクションでは、イントロダクションManagement Clientユーザーインターフェースのためのイントロダクションを提供します。

ログイン概要

Management Clientを起動するときには、まずログイン情報を入力し、システムに接続する必要があります。

XProtect Corporate 2016またはXProtect Expert 2016以降がインストールされていれば、パッチをインストールした後に古いバージョンの製品を実行するシステムにログインできます。サポートされるバージョンは、XProtect Corporate2013とXProtect Expert2013以降です。



ログイン認証(説明付き)

システム管理者は、ユーザーを設定することで、十分な権限を持つ2番目のユーザーがログインを許可した場合にのみシステムにログインさせることができます。この場合、XProtect Smart ClientまたはManagement Clientでは、ログイン中に2番目の認証を要求されます。

定義済みのシステム管理者の役割に関連付けられたユーザーは常に認証する権限があるため、2番目のログインが必要な別の役割に関連付けられていないかぎり、2番目のログインは要求されません。

ログイン認証を役割に関連付けるには：

- [役割]の[情報]タブ(ページ341の役割の設定を参照) で、選択した役割の[ログイン認証が必要]を設定し、ユーザーがログイン中に追加の認証を要求されるようにします。
- [セキュリティ全般]タブの [役割]の項目で、選択した役割に対して [ユーザーを認証]を設定します(「ページ341の役割の設定」を参照)

同じユーザーで両方のオプションを選択できます。つまり、ユーザーはログイン中に追加の認証を要求されますが、自分のログインを除き、他のユーザーのログインを認証することもできます。

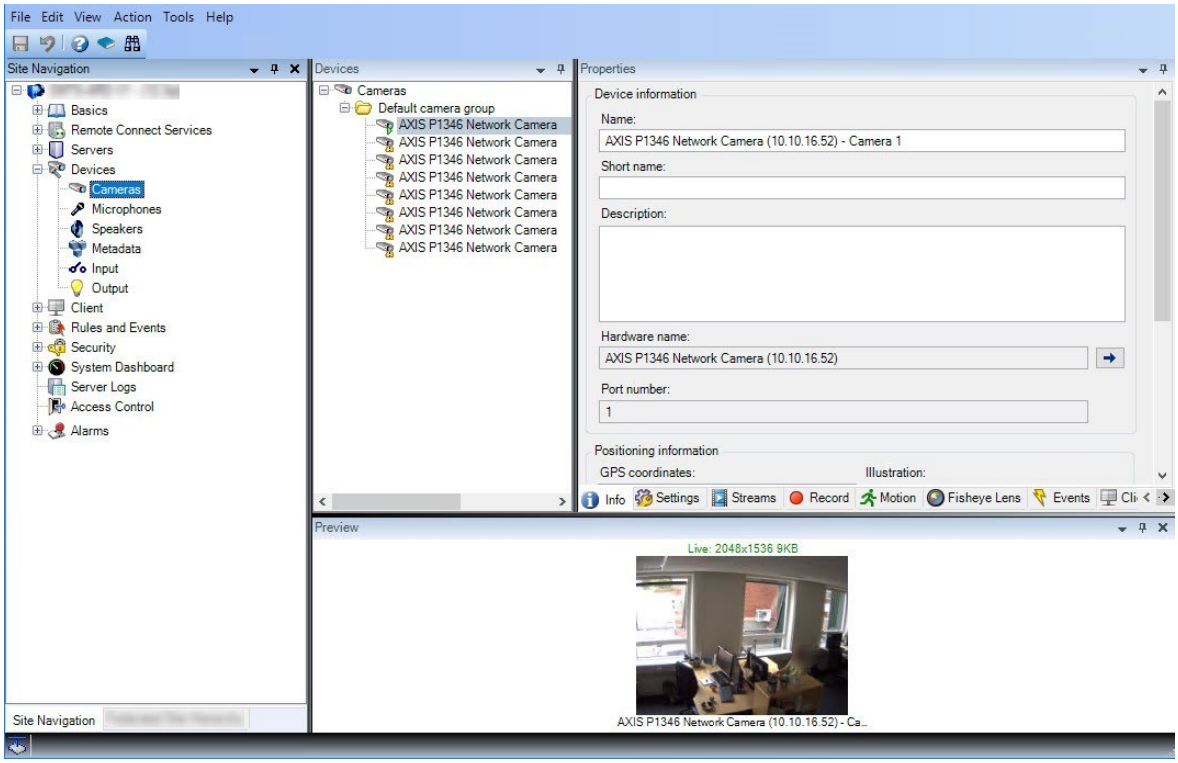
Management Clientウィンドウ概要

Management Clientウィンドウはペインに分割されます。ペインとレイアウトの数は以下によって異なります。

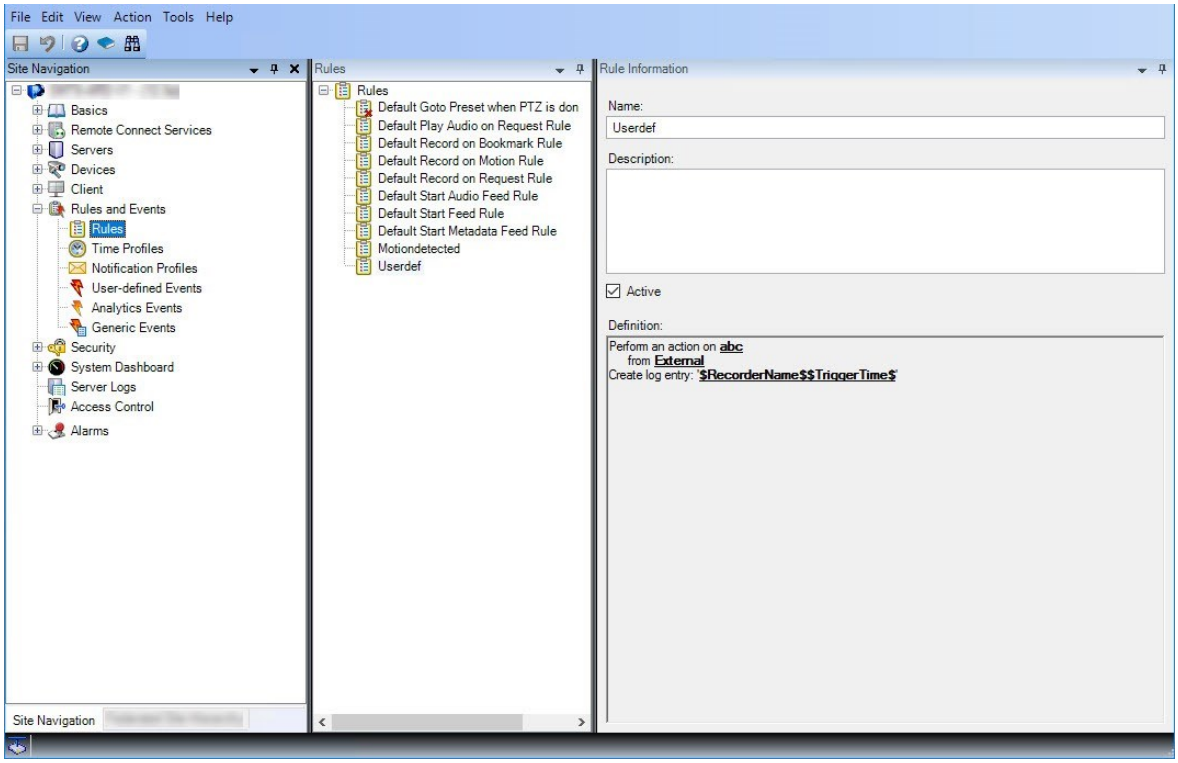
- システム構成
- タスク
- 使用可能な機能

以下は通常のレイアウト例です:

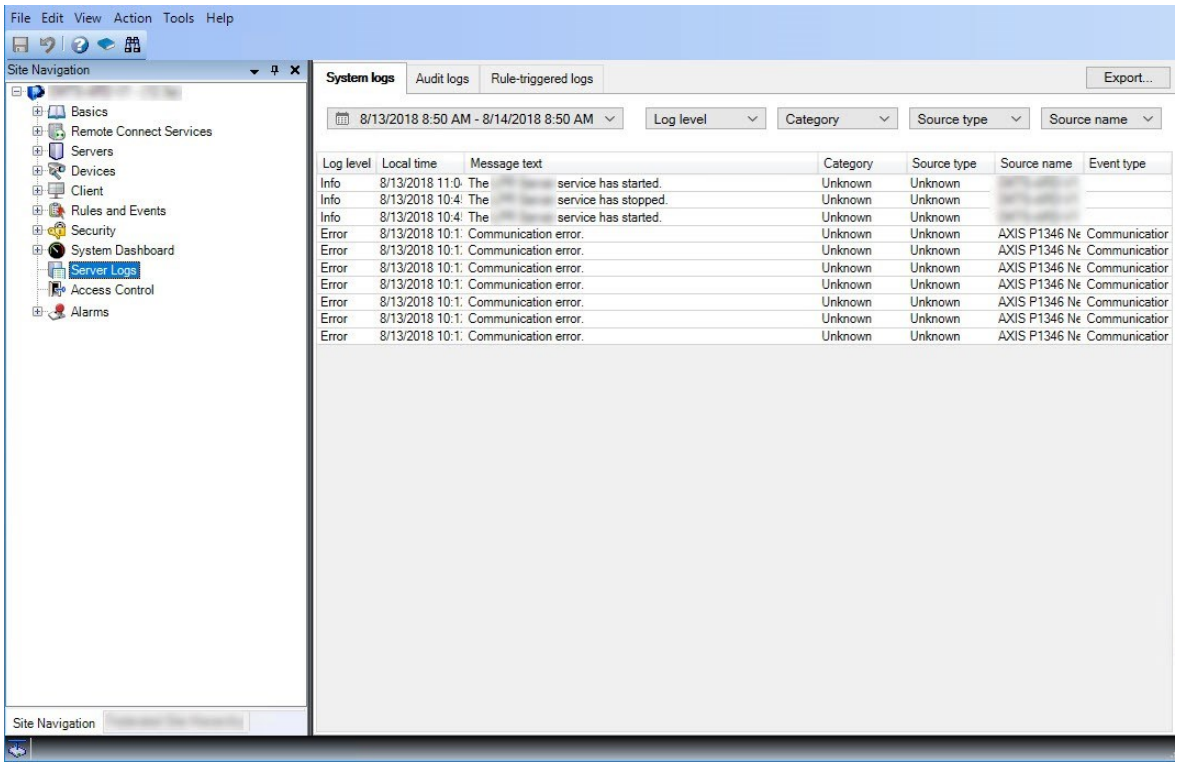
- レコーディングサーバーおよびデバイスで作業する場合：



- ルール、時間および通知プロファイル、ユーザー、ロールで作業する場合：

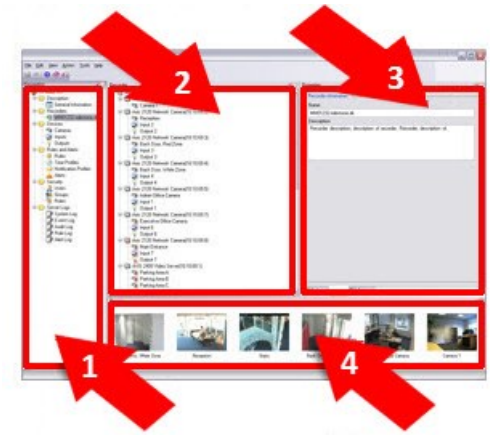


- ログを表示する場合：



ペインの概要

図は通常のウィンドウのレイアウトを概説しています。カスタマイズが可能なので、使用しているコンピュータによってレイアウトは異なります。



1. サイトナビゲーションペインおよびフェデレーテッドサイト階層ペイン
2. 概要ペイン
3. [プロパティ] ペイン
4. プレビューペイン

サイトナビゲーションペイン：これはManagement Clientの中心的なナビゲーションエレメントです。ログインしたサイトの名前、設定および構成が反映されます。サイト名はペインの上部に表示されます。ソフトウェアの機能を反映して、機能はカテゴリにグループ化されます。

フェデレーテッドサイト階層ペイン：これは親/子階層ですべてのMilestone Federated Architectureサイトを表示するナビゲーション要素です。

任意のサイトを選択して、そのサイトとサイトが起動するManagement Clientにログインできます。ログインしたサイトは、常に階層の最上位にあります。

概要ペイン：[サイトナビゲーション]ペインで選択した要素（例えば詳細リストなど）の概要を提供します。概要ペインでエレメントを選択すると、通常はプロパティペインにプロパティが表示されます。概要ペインでエレメントを右クリックすると、管理機能へのアクセスが得られます。

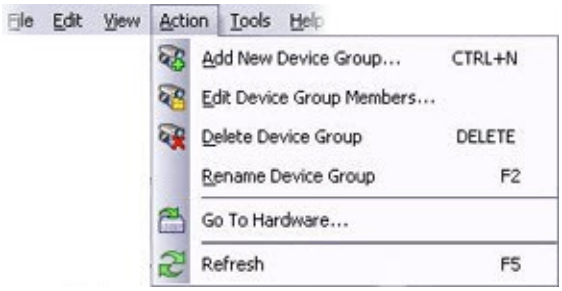
プロパティペイン：[概要]ペインで選択した要素のプロパティを表示します。プロパティは複数の専用タブに表示されます。

プレビューペイン: プレビューペインはレコーディングサーバーおよびデバイスで作業するときに表示されます。選択されたカメラからのプレビュー画像を表示したり、デバイスの状態についての情報を表示します。この例では、カメラのプレビュー画像およびカメラのライブストリームの解像度やデータ転送速度の情報を示しています。

デフォルトでは、カメラのプレビュー画像に表示されている情報はライブストリームに関する情報です。プレビュー画像の上に緑色のテキストで表示されます。代わりにレコーディングストリーム情報(赤色のテキスト)を表示したい場合は、メニューで[ビュー]>[レコーディングストリームを表示]を選択します。

プレビューペインで、多数のカメラからのプレビュー画像を高いフレームレートで表示すると、パフォーマンスに影響することがあります。プレビュー画像の数やフレームレートを制御するには、メニューで、[オプション]>[一般]を選択します。

メニュー概要



例、状況によって一部のメニューは異なります。

ファイルメニュー

変更を設定に保存して、アプリケーションを終了します。設定のバックアップもできます。ページ441のシステム設定のバックアップおよび復元についてを参照してください。

編集メニュー

変更を元に戻すことができます。

ビューメニュー

名前	説明
アプリケーションレイアウ	Management Clientのさまざまなペインのレイアウトをデフォルトの設定にリセットします。

名前	説明
トのリセット	
プレビューウィンドウ(P)	レコーディングサーバーやデバイスを操作する際に、プレビューペインをオンまたはオフに切り替えられます。
レコーディングストリームを表示(S)	デフォルトでは、プレビューペインのプレビュー画像に表示されている情報は、カメラのライブストリームに関する情報です。代わりにレコーディングストリームに関する情報が必要な場合は、レコーディングストリームを表示を選択します。
フェデレーテッドサイト階層	デフォルトでは、フェデレーテッドサイト階層ペインは有効になっています。
サイトナビゲーション	デフォルトでは、サイトナビゲーションペインは有効になっています。

アクションメニュー

アクションメニューの内容はサイトナビゲーションペインで選択したエレメントにより異なります。選択できるアクションはエレメントを右クリックする時と同じです。エレメントはページ130のサイトナビゲーションペインでのシステムの構成で説明されています。

各カメラのプレバッファ期間はページ220のプリバッファをサポートするデバイスを参照してください。

名前	説明
更新	常に使用可能であり、必要な情報をManagement Serverから再ロードします。

ツールメニュー

名前	説明
登録済みサービス	登録済みサービスの管理。 ページ467の登録済みサービスの管理を参照してください。
有効な役割	選択したユーザーまたはグループの役割をすべて表示します。
オプション	オプションダイアログボックスを開き、グローバルなシステム設定を定義および編集することができます。

ヘルプメニュー

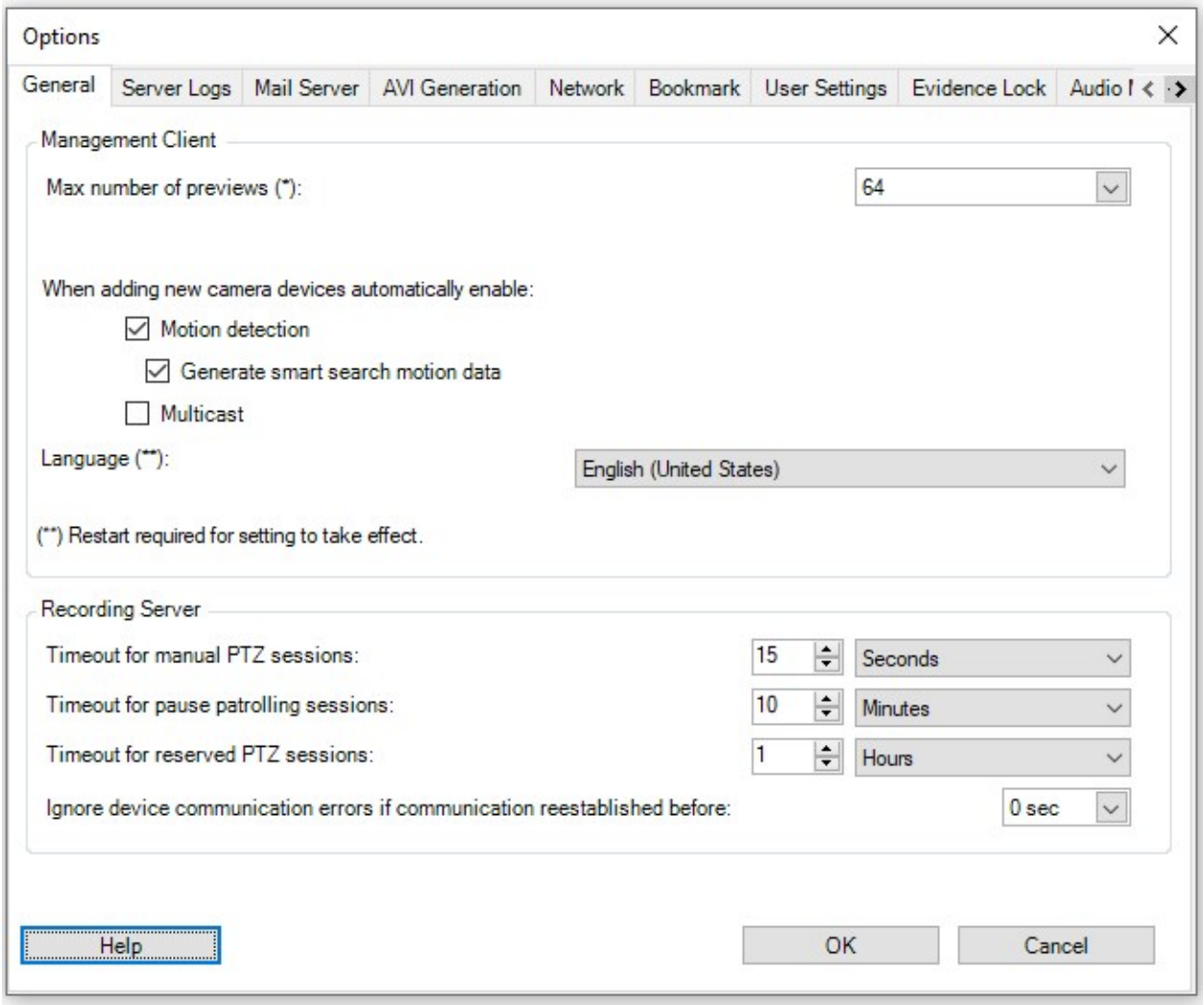
ヘルプシステムとManagement Clientのバージョンについての情報にアクセスできます。

システムのオプションを設定

オプションダイアログボックスで、全般的な表示およびシステムの機能に関連する複数の設定を指定できます。

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。

ダイアログボックスにアクセスするには、ツール > オプションを選択します。



一般タブ(オプション)

一般タブで、Management Clientおよびレコーディングサーバーの一般設定を指定できます。

Management Client

名前	説明
プレビューの最大数	プレビューペインに表示されるサムネイル画像の最大数を選択できます。デフォルトは、64個のサムネイル画像です。 メニューからアクション > 更新を選択して変更を有効にします。 サムネイル画像が大量に存在し、かつフレームレートが高い場合、システムが低速になる可能性があります。
新しいカメラデバイスを追加するときに自動的に有効にします: モーション検知	ハードウェアの追加ウィザードを使ってシステムに追加する際に、チェックボックスを選択して新規カメラでモーション検知を有効にします。 この設定は既存のカメラのモーション検知設定に影響しません。 カメラデバイスのモーションタブで、カメラのモーション検知を有効化/無効化できます。
新しいカメラデバイスを追加するときに自動的に有効にします: スマート検索用のモーションデータを生成	スマート検索モーションデータを生成するには、カメラのモーション検知が有効でなければなりません。 [ハードウェアの追加]ウィザードを使ってシステムに追加する際に、チェックボックスを選択して新規カメラでスマートサーチモーションデータの生成を有効にします。 この設定は既存のカメラのモーション検知設定に影響しません。 カメラデバイスのモーションタブで、カメラのスマート検索モーションデータの生成を有効化/無効化できます。
新しいカメラデバイスを追加するときに自動的に有効にします: マルチキャスト	ハードウェアの追加ウィザードを使って追加する際に、チェックボックスを選択して新規カメラでマルチキャストを有効にします。 この設定は既存のカメラのマルチキャスト設定に影響しません。 カメラデバイスのクライアントタブで、カメラのライブマルチキャストを有効化/無効化できます。
言語	Management Clientの言語を選択します。 新しい言語を使用するには、Management Clientを再起動します。

レコーディングサーバー

名前	説明
手動PTZセッションのタイムアウト	必要な権限を持つクライアントユーザーは、PTZカメラのパトロールを手動で中断できます。手動停止後に通常のパトロールを再開するまでに必要な時間を指定します。この設定は、システムのPTZカメラすべてに適用されます。デフォルトは15秒です。 カメラで個別のタイムアウトを設定する場合は、カメラの[プリセット]タブで指定します。
一時停止パトロールセッションのタイムアウト	十分なPTZ優先度のクライアントユーザーはPTZカメラでのパトロールを一時停止できます。一時停止後に通常のパトロールを再開するまでに必要な時間を指定します。この設定は、システムのPTZカメラすべてに適用されます。デフォルトは10分です。 カメラで個別のタイムアウトを設定する場合は、カメラの[プリセット]タブで指定します。
予約済みPTZセッションのタイムアウト	予約済みPTZセッションのデフォルト期間を設定します。ユーザーが予約済みPTZセッションを実行するときには、セッションが手動でリリースされる前か、期間がタイムアウトするときまで、他のユーザーはPTZカメラを使用できません。デフォルト設定は1時間です。 カメラで個別のタイムアウトを設定する場合は、カメラの[プリセット]タブで指定します。
通信が右記より前に再確立される場合は、デバイスの通信エラーを無視します	ハードウェアとデバイス上のシステムの全てのコミュニケーション エラーをこのシステムで記録します。しかしながら、コミュニケーション エラー イベントがルールエンジンのきっかけになる前に、どのくらい長くコミュニケーション エラーが存在させるべきかはここで選択します。

サーバーログタブ(オプション)

サーバーログタブで、システムのマネジメントサーバーログの設定を指定できます。

詳細については、ページ388のログ(説明付き)を参照してください。

名前	説明
ログ	設定するログの種類を選択します。 • システムログ • 監査ログ

名前	説明
	• ルールトリガーログ
設定	ログを無効または有効にして、保存期間を指定します。 2018 R2およびそれ以前のコンポーネントにログの書き込みを許可します 詳細については、ページ391のログを録画するため、2018 R2およびそれ以前のコンポーネントを許可します システムログで、記録するメッセージレベルを指定します。 • すべて - 未定義のメッセージを含みます • 情報と警告とエラー • 警告とエラー • エラー(デフォルト設定) 監査ログで、XProtect Smart Clientのすべてのユーザーアクションを記録する場合は、ユーザーアクセスログを有効にします。例えば、エクスポート、出力の有効化、カメラのライブまたは再生での表示が含まれます。 次を指定します。 • 再生シーケンスの長さ つまり、ユーザーがこの期間内で再生している限り、1つのログエントリだけが生成されます。期間外で再生すると、新しいログエントリが作成されます。 • システムがログエントリを作成する前にユーザーが表示する録画(フレーム)数。

メールサーバータブ(オプション)

[メールサーバー]タブで、システムのメールサーバーの設定を指定できます。詳細については、ページ320の通知プロファイルを参照してください。

名前	説明
送信者のEメールアドレス	すべての通知プロファイルについて、Eメールによる通知の送信者として表示するEメールアドレスを入力します。例:sender@organization.org

名前	説明
メールサーバーアドレス	Eメール通知を送信するSMTPメールサーバーの名前を入力します。例：mailserver.organization.org
メールサーバーポート	メールサーバーへの通信に使用されるTCPポート。デフォルトの暗号化されていないポートは25で、暗号化された通信では通常ポート465または587を使用します。
サーバーへの通信の暗号化	マネージメントサーバーとSMTPメールサーバー間で安全な通信を行いたい場合、このチェックボックスを選択します。 接続は、STARTTLS Eメール プロトコル コマンドで保護されています。このモードでは、非暗号化接続でセッションが開始し、STARTTLSコマンドがSMTPメールサーバーによりマネージメントサーバーへと発行されて、SSLを使用した安全な通信に切り替わります。
サーバーのログインが必要です	有効になっている場合は、メールサーバーにログインするユーザーのユーザー名およびパスワードを指定します。

AVI生成タブ(オプション)

AVI生成タブで、AVIビデオクリップファイルの生成の圧縮設定を指定できます。これらの設定は、ルール起動通知プロファイルにより送信されるEメール通知にAVIファイルを含める場合に必要になります。

ページ320の通知プロファイルもご覧ください。

名前	説明
圧縮プログラム	適用するコーデック(圧縮/解凍技術)を選択します。リストに使用可能なコーデックをより多く含むには、マネジメントサーバーにコーデックをインストールします。すべてのカメラがコーデックに対応しているわけではありません。
圧縮品質	(すべてのコーデックで利用できるわけではありません)。スライダーを使用して、コーデックが実行する圧縮の度合い(0-100)を選択します。 0は、圧縮なしという意味です。これは通常高画質で、ファイルサイズが大きくなります。100は、最大の圧縮という意味です。これは通常低画質で、ファイルサイズが小さくなります。

名前	説明
	スライダーが利用できない場合、圧縮の質は選択されたコーデックによって決定されます。
キーフレームごと	(すべてのコーデックで利用できるわけではありません)。キーフレームを使用する場合、このチェックボックスをオンにして、キーフレーム間の必要なフレーム数を指定します。 キーフレームは、指定された間隔で保存された単一のフレームです。キーフレームはカメラのビュー全体を記録しますが、続くフレームは変化したピクセルだけを記録します。これにより、ファイルのサイズを大幅に縮小できます。 チェックボックスが使用できない、または選択されていない場合は、各フレームにカメラのビュー全体が含まれます。
データ転送速度	(すべてのコーデックで利用できるわけではありません)。特定のデータ転送速度を使用する場合、このチェックボックスをオンにして、秒当たりのキロバイト数を指定します。 データ速度は添付されているAVIファイルのサイズを指定します。 このチェックボックスが利用できない場合、またはオンになっていない場合、データ転送速度は選択されたコーデックによって決定されます。

ネットワークタブ(オプション)

ネットワークタブで、クライアントがインターネット経由で録画サーバーに接続する場合は、ローカルクライアントのIPアドレスを指定できます。これにより、監視システムはローカルネットワークから来ていると認識します。

システムのIPバージョンも指定できます。IPv4またはIPv6。デフォルト値はIPv4です。

ブックマークタブ(オプション)

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。

[ブックマーク]タブで、ブックマーク、IDおよびXProtect Smart Clientの機能を指定できます。

名前	説明
ブックマークIDの接頭辞	XProtect Smart Clientのユーザーが作成するすべてのブックマークの接頭辞を指定します。

名前	説明
デフォルトのブックマーク時間	XProtect Smart Clientで設定されるブックマークのデフォルト開始時間と終了時間を指定します。 この設定は以下と一致している必要があります。 • デフォルトのブックマークルール(「ページ309のルール」を参照) • 各カメラのプレバッファ期間はページ220のプリバッファをサポートするデバイスを参照してください。

役割のブックマーク権限を指定するには、ページ366のデバイスタブ(役割)を参照してください。

ユーザー設定タブ(オプション)

ユーザー設定タブで、リモート記録が有効な場合にメッセージを表示するかどうかなどのユーザーの優先設定を指定できます。

カスタマーダッシュボードタブ(オプション)

[カスタマーダッシュボード]タブで、Milestone Customer Dashboardを有効または無効にできます。

カスタマーダッシュボードは、システム管理者やインストール情報へのアクセス権を持つユーザーに対して、発生の可能性がある技術的問題(カメラの障害など) を含むシステムの現在の状態の概要をグラフィカル表示として提供するオンラインのモニタリングサービスです。

チェックボックスをオンまたはオフにすると、いつでもカスタマーダッシュボード設定を変更できます。

エビデンスロックタブ(オプション)

> 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。

エビデンスロックタブでは、エビデンスロックプロファイルや、クライアントユーザーがデータを保護した状態にするよう選択できる期間を定義および編集できます。

名前	説明
エビデンスロックプロファイル	定義されたエビデンスロックプロファイルのリスト。 既存のエビデンスロックプロファイルを追加および削除できます。デフォルトのエビデンスロックプロファイルは削除できませんが、その時間オプションや名前は変更できます。
ロック時間オプション:	クライアントユーザーがエビデンスにロックをかけることを選択する期間。 使用できる時間オプションは時間、日、週、月、年、無期限またはユーザー定義になります。

役割に対してエビデンスロックアクセス権限を指定する方法については、「ページ366のデバイスタブ(役割)」で役割設定について参照してください。

音声メッセージタブ(オプション)

音声メッセージタブで、ルールによってトリガーされたメッセージの送信に使用する音声メッセージファイルをアップロードできます。

アップロードできるファイルの最大数は50で、各ファイルの最大サイズは1MBです。

名前	説明
名前	メッセージの名前を記載します。メッセージを追加する際に名前を入力します。メッセージをシステムにアップロードするには追加をクリックします。
説明	メッセージの説明を記載します。 メッセージを追加する際に説明を入力します。説明フィールドを使用して目的または実際のメッセージを説明することができます。
追加	音声メッセージをシステムにアップロードできます。 サポートされるフォーマットは、標準のWindows音声ファイルフォーマットです。 • .wav • .wma • .flac
編	名前と説明を修正するか、または実際のファイルを置き換えることができます。

名前	説明
集	
削除	音声メッセージをリストから削除します。
再生	Management Clientが稼働するコンピュータの音声メッセージを聞くにはこのボタンをクリックします。

音声メッセージの再生をトリガーするルールを作成するには、ページ309のルールを参照してください。

ルールで使用できる一般的なアクションの詳細については、ページ288のアクションおよびアクションの停止(説明付き)を参照してください。

入退室管理設定タブ(オプション)

XProtect Accessを使用する場合は、この機能の使用を許可する基本ライセンスを購入しておく必要があります。

名前	説明
開発プロパティパネルを表示する	選択すると、[入退室管理]>[一般設定]に対する追加の開発者情報が表示されます。 この設定は、入退室管理システム統合の開発者のみが使用することを前提としています。

アナリティクスイベントタブ(オプション)

アナリティクスイベントタブで、アナリティクスイベント機能を有効にして指定できます。

名前	説明
有効	アナリティクスイベントを使用するかどうかを指定します。デフォルトでは、この機能は無効になっています。
ポート	この機能で使用するポートを指定します。既定のポートは9090です。 関連するVCAツールプロバイダもこのポート番号を使用するようにしてください。ポート番号を変更した場合、プロバイダのポート番号も変更するようにしてください。
すべてのネットワークアドレスまたは指定ネットワークアドレス	すべてのIPアドレス/ホスト名からのイベントが許可されるのか、またはアドレスリスト(以下を参照)で指定されたIPアドレス/ホスト名からのイベントだけが許可されるのかを指定します。
アドレスリスト	信頼済みIPアドレス/ホスト名のリストを指定します。このリストは、特定のIPアドレス/ホスト名のイベントのみが許可されるように受信されるデータをフィルタリングします。ドメイン名システム(DNS)、IPv4およびIPv6アドレス形式の両方を使用できます。 それぞれのIPアドレスまたはホスト名をマニュアルで入力するか、あるいはアドレスの外部リストをインポートすることにより、リストにアドレスを追加できます。 • マニュアル入力: アドレスリストにIPアドレス/ホスト名を入力します。必要なアドレスを繰り返します。 • インポート: [インポート]をクリックして、アドレスの外部リストを参照します。外部リストは、それぞれのIPアドレスまたはホスト名が別のラインに入力された.txtファイルでなければなりません。

[アラームおよびイベント]タブ(オプション)

[アラームとイベント]タブで、アラーム、イベント、ログの設定を指定できます。これらの設定に関連して、ページ52のデータベースのサイズを制限も参照してください。

名前	説明
終了したアラームの保持期	データベース上で終了状態のアラームを保存する日数を指定します。値を0に設定すると、アラームは終了後に削除されます。

名前	説明
間	アラームには常にタイムスタンプが含まれます。アラームがカメラによりトリガーされる場合は、タイムスタンプにはアラームの時間からの画像が含まれます。アラーム情報自体はイベントサーバーに保存されますが、添付画像に対応するビデオ記録は、関連する監視システムサーバーに保存されます。 アラームの画像を表示するには、ビデオ録画が少なくともイベントサーバーにアラームを保存する期間以上、保存されるようにする必要があります。
他のすべてのアラームの保持期間	新規、進行中、または保留中の状態のアラームを保存する日数を指定します。値を0に設定すると、アラームはシステムに表示されますが、保存はされません。 アラームには常にタイムスタンプが含まれます。アラームがカメラによりトリガーされる場合は、タイムスタンプにはアラームの時間からの画像が含まれます。アラーム情報自体はイベントサーバーに保存されますが、添付画像に対応するビデオ記録は、関連する監視システムサーバーに保存されます。 アラームの画像を表示するには、ビデオ録画が少なくともイベントサーバーにアラームを保存する期間以上、保存されるようにする必要があります。
ログの保持期間	イベントサーバーログの保持日数を指定します。ログの保持期間が長期に及ぶ場合は、イベントサーバーが設置されているマシンのディスクに十分な空き領域があることを確認してください。
詳細ログインを有効にする	イベントサーバー通信のより詳細なログを保持するには、チェックボックスを選択します。ログの保持フィールドに指定された日数の間保持されます。
イベントタイプ	イベントをデータベースに保存する日数を指定します。カメラを正しく配置するには次の2つの方法があります。 • イベントグループ全体の保持期間を指定できます。[グループを受け継ぐ]の値を有するイベントタイプは、イベントグループの値を受け継ぎます。 • イベントグループの値を設定した場合でも、イベントタイプごとに保持期間を指定できます。 値を0に設定すると、イベントはデータベースに保存されません。

名前	説明
	外部イベント(ユーザー定義イベント、ジェネリックイベント、および入力イベント)は、デフォルトで 0 に設定されており、その値を変更することはできません。その理由は、これらの種類のイベントが頻繁に発生するため、データベースに保存するとパフォーマンスの問題が発生する可能性があるからです。

ジェネリックイベントタブ(オプション)

ジェネリックイベントタブで、ジェネリックイベントとデータソース関連の設定を指定できます。

実際のジェネリックイベントの設定方法についての詳細は、ページ331のジェネリックイベントを参照してください。

名前	説明
データソース	2つのデフォルトデータソースから選択してカスタムデータソースを定義できます。選択内容は、お使いのサードパーティ製プログラムおよび/またはインターフェース対象となるハードウェアまたはソフトウェアによって異なります。 互換:工場出荷時のデフォルト設定が有効。すべてのバイトをエコー。TCPおよびUDP。IPv4のみ。ポート1234。区切り文字なし。ローカルホストのみ。現在のコードページエンコーディング(ANSI)。 インターナショナル:出荷時設定が有効。統計のみをエコー。TCPのみ。IPv4+6。ポート1235。<CR><LF>を区切り文字として使用。ローカルホストのみ。UTF-8エンコード。(<CR><LF> = 13,10)。 [データソースA] [データソースB] のようになります。
新規	クリックすると新しいデータソースを定義できます。
名前	データソースの名前。
有効	データソースはデフォルトでは有効になっています。データソースを無効にするにはチェックボックスを解除します。
リセット	クリックして選択されたデータソースのすべての設定をリセットします。名前フィールドに入力された名前は

名前	説明
	残ります。
ポート	データソースのポート番号。
プロトコルタイプセレクタ	システムがジェネリックイベントを検出するために聞き、分析すべきプロトコル。 すべて: TCPおよびUDP。 TCP: TCPのみ。 UDP: UDPのみ。 ジェネリックイベントに使用するTCPおよびUDPパッケージに、@、#、+、~、等の特殊文字が含まれている場合があります。
IPタイプセレクタ	選択可能なIPアドレスタイプ: IPv4、IPv6、または両方。
区切り文字列	個別ジェネリックイベントのレコードを分離するために使用するセパレーターバイトを選択します。デフォルトのデータソースタイプインターナショナル(上記のデータソースをご覧ください) は13、10です。(13,10 = <CR><lF>)。
エコータイプセレクタ	使用可能なエコーリターン形式: • エコー統計: 次の形式をエコーします。[X],[Y],[Z],[ジェネリックイベント名] [X] = 要求番号。 [Y] = 文字数。 [Z] = ジェネリックイベントとの一致数。 [ジェネリックイベント名] = [名前] フィールドに入力された名前。 • すべてのバイトをエコー: すべてのバイトをエコーします。 • エコーなし: すべてのエコーを抑制します。
エンコーディングタイプセレクタ	デフォルトでは、もっとも関連のあるオプションのみがリストに表示されます。すべて表示チェックボックスを選択し、利用可能なすべてのエンコーディングを表示します。
使用可能な外部IPv4アドレス	外部イベントを管理するために、マネジメントサーバーが通信可能なIPアドレスを指定します。これを使用して、データを取得しないIPアドレスを除外することも可能です。

名前	説明
使用可能な外部IPv6アドレス	外部イベントを管理するために、マネジメントサーバーが通信可能なIPアドレスを指定します。これを使用して、データを取得しないIPアドレスを除外することも可能です。

初期構成タスクリスト

以下のチェックリストは、システムを構成するための初期タスクを示しています。インストール中にすでに完了している場合もあります。

チェックリストが完了しても、それだけでシステムが完全に組織の要件に一致することを保証しているわけではありません。システムを組織の必要性に一致させるために、Milestoneは、システムの起動後も、システムを継続的にモニターし、調整することをお勧めします。

たとえば、システムを起動した後、異なる物理的条件(昼/夜、強風/穏やかな天候など)で個々のカメラのモーション検知感度の設定をテストして調整することをお勧めします。

ルールの設定は、システムが実行するアクション(ビデオを録画する場合など)の大半を決定するものであり、組織のニーズに合わせて変更できる設定のもう一つの例です。

手順:	説明
☑	システムの初期インストールが完了しました。 「ページ76の新しいXProtectシステムのインストール」を参照してください。
☑	試用版SLCを恒久版SLCに変更します(必要な場合)。 「ページ50のソフトウェアライセンスコードの変更」を参照してください。
☑	Management Clientへログインします。 ページ108のログイン概要を参照.
☐	それぞれのレコーディングサーバーのストレージの設定が要件を満たしていることを確認します。 ページ148のストレージタブ(レコーディングサーバー)を参照してください。
☐	それぞれのレコーディングサーバーのアーカイブ設定が要件を満たしていることを確認します。 ページ148のストレージタブ(レコーディングサーバー)を参照してください。

手順：	説明
☐	それぞれのレコーディングサーバーに追加する必要があるハードウェア(例、カメラおよびビデオエンコーダー) を検出します。 ページ183のハードウェアの追加を参照してください。
☐	レコーディングサーバーごとに各カメラを設定する。 ページ200のカメラデバイス(説明付き) を参照してください。
☐	個別のカメラまたはカメラのグループのストレージとアーカイブを有効にします。この操作は、カメラごと、またはデバイスグループに対して行えます。 ページ148のストレージタブ(レコーディングサーバー) を参照してください。
☐	デバイスを有効にして設定します。 ページ199のサイトナビゲーション：デバイス：デバイスの使用を参照してください。
☐	ルールはシステムの動作を大きく決定します。カメラが録画するとき、パン/チルト/ズーム(PTZ)カメラがパトロールするとき、通知が送信されるときなどのルールを作成します。 ルールを作成する。 ページ286のルールおよびイベント(説明付き) を参照してください。
☐	役割をシステムに追加します。 ページ336の役割(説明付き) を参照してください。
☐	ユーザーまたはユーザーのグループを各役割に追加します。 ページ339のユーザーおよびグループの役割からの削除、役割への割り当てを参照してください。
☐	ライセンスをアクティベートする。 ページ131のライセンス情報またはページ131のライセンス情報を参照してください。

「ページ130のサイトナビゲーションペインでのシステムの構成を参照してください。

サイトナビゲーションペインでのシステムの構成

[サイトナビゲーション] ペインでは、システムを構成および管理し、ニーズに合わせて設定できます。システムが単一サイトシステムではなく、フェデレーテッドサイトを含む場合には、これらのサイトはフェデレーテッドサイト階層ペインで管理されることに注意してください。

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。

サイトナビゲーション: 基本

この記事では、ライセンスを表示・管理する方法、ならびにサイトに関する情報を追加する方法について説明します。

ライセンス情報

このサイトとすべての他のサイトの両方で、同じソフトウェアライセンスファイルを共有するすべてのライセンスおよび Milestone Careサブスクリプションを追跡し、ライセンスの認証方法を決定できます。異なるXProtectライセンスの基本情報については、ページ49のライセンス(説明付き) を参照してください。

ライセンス付与先

ソフトウェア登録中に入力したライセンス所有者の連絡先詳細情報を一覧表示します。[詳細の編集]をクリックして、ライセンス所有者情報を編集します。ここでは、インストール前に同意したエンドユーザー使用許諾契約へのリンクが表示されます。

Milestone Care

現在のMilestone Care™レベルの情報が表示されます。システムを購入した時点で、2年間のMilestone Care Plusサブスクリプション契約も締結しています。インストールには常にMilestone Care Basicが適用され、これにより、サポートWebサイト(https://www.milestonesys.com/support/) のナレッジベース記事、ガイド、チュートリアルなどのさまざまなタイプのセルフヘルプ資料を使用できます。Milestone Care Plusサブスクリプションの有効期限は、インストールされた製品テーブルに表示されます。システムをインストールした後にMilestone Careサブスクリプションを購入または更新する場合は、正しいMilestone Care情報が表示される前にライセンスを認証する必要があります。

Milestone Care Plusサブスクリプションにより、アップグレードを利用できます。Customer Dashboardサービス、Smart Connect機能、および完全プッシュ通知機能も利用できます。Milestone Care Premiumサブスクリプションがある場合は、Milestoneサポートに問い合わせ、サポートを受けることもできます。Milestoneサポートに問い合わせるときには、お使いのMilestone CareIDの情報を必ず含めてください。Milestone Care Premiumサブスクリプションの有効期限もわかるようにしてください。Milestone Careの詳細については、リンクに従ってください。

インストールされている製品

XProtect VMS用のすべてのインストールされた基本ライセンスと、同じソフトウェアライセンスファイルを共有するアドオン製品に関する次の情報が一覧表示されます。

- 製品とバージョン
- 製品のソフトウェアライセンスコード(SLC)。
- SLCの有効期限。通常は無制限です。

- Milestone Care Plusサブスクリプションの有効期限。
- Milestone Care Premiumサブスクリプションの有効期限。

> XProtect Essential+などのライセンスは、自動ライセンスアクティベーションが有効な状態でインストールされ、この設定を無効にすることはできません。

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2016	M01-C01-100-01-	Unlimited	01-10-2016	01-10-2016
Milestone XProtect Smart Wall	M01-P03-023-01-	Unlimited	Unlimited	
Milestone XProtect Access 2016 v10.0a	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact 2016	M01-P08-100-01-	Unlimited	Unlimited	

ライセンス概要 - すべてのサイト

アクティベーション済みハードウェアデバイスライセンスまたはソフトウェアライセンスファイルのその他のライセンス数と、システムで使用可能なライセンスの合計数を一覧表示します。追加ライセンスを購入せずにシステムを拡張できるかどうかを簡単に確認できます。

他のサイトでアクティベーションされたライセンスのステータスの詳細概要については、ライセンス詳細 - すべてのサイトリンクをクリックします。情報については、以下のライセンス詳細 - 現在のサイトセクションを参照してください。

License Overview - All sites License Details - All Sites...

License Type	Activated
Hardware Device	51 out of 100
Milestone Interconnect Camera	0 out of 100
Access control door	9 out of 2002
Transaction source	1 out of 101

アドオン製品のライセンスがある場合は、サイトナビゲーションペインのアドオン製品固有のノードの下に、これらに関する追加詳細情報が表示されます。

ライセンス詳細 - 現在のサイト

アクティベーション済み欄には、アクティベーション済みハードウェアデバイスライセンスまたはこのサイトの他のライセンスの数が一覧表示されます。

また、ページ133のアクティベーションなしのデバイスの変更(説明付き)を参照)。アクティベーションなしの変更欄では、1年間で使用可能な数も確認できます。

アクティベートしていないため猶予期間で実行されているライセンスがある場合は、猶予期間欄に一覧表示されます。期限切れの最初のライセンスの有効期限は、表の下に赤色で表示されます。

猶予期間が終了する前にライセンスをアクティベートし忘れた場合は、動画がシステムに送信されなくなります。これらのライセンスは終了した猶予期間欄に表示されます。詳細情報は、ページ137の猶予期間が切れた後にライセンスをアクティベートするを参照してください。

使用可能なライセンス数よりも使用済みライセンス数の方が多い場合は、ライセンスなし欄に一覧表示され、システムで使用できません。詳細については、ページ137の追加ライセンスの取得を参照してください。

猶予期間中または猶予期間が期限切れのライセンスがある場合、またはライセンスがない場合は、Management Clientにログインするたびに、通知メッセージがポップアップ表示されます。

License Details - Current Site: SYS[redacted]

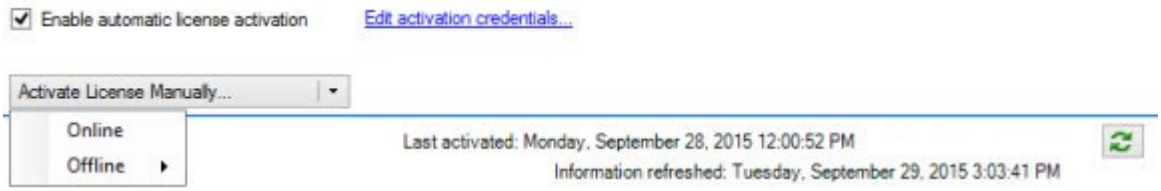
License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Hardware Device	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

Management Clientでは、ライセンスのないハードウェアデバイスは感嘆符「！」表示で識別されます。感嘆符「！」は他の目的でも使用されます。感嘆符の上にマウスを置くと、目的が表示されます。

ライセンスアクティベーションの機能

3つの表の下には、次の項目があります。

- 自動ライセンスアクティベーションを有効にするチェックボックスと、自動アクティベーションのユーザー資格情報を編集するためのリンク。詳細については、ページ135の自動ライセンスアクティベーション(説明付き)およびページ136の自動ライセンスアクティベーションを有効にするを参照してください。自動アクティベーションが失敗した場合、失敗したメッセージが赤色で表示されます。詳細については、[詳細]リンクをクリックします。
- ライセンスをオンラインまたはオフラインで手動アクティベートするためのドロップダウンリスト。詳細については、ページ136のライセンスをオンラインでアクティベーションまたはページ137のライセンスをオフラインでアクティベートを参照してください。
- ページの右下端には、最後にライセンスをアクティベート(自動または手動)した日時とページの情報が更新された日時が表示されます。日付スタンプは、ローカルコンピュータではなく、サーバーから取得されます。



アクティベーションなしのデバイスの変更(説明付き)

[基本]>[ライセンス情報]ページの[アクティベーションなしの変更]には、デバイスライセンスをアクティベートせずに交換または追加できるハードウェアデバイス数と、前回のアクティベーション以降に行った変更数が示されます。アクティベーションなしのデバイスの変更内に追加されたハードウェアデバイスは、完全に認証されたハードウェアデバイスライセンスとして実行されます。

最後のライセンスアクティベーションから1年が経過すると、使用済みのアクティベーションなしのデバイスの変更の数が自動的にゼロにリセットされます。リセットが発生したら、ライセンスをアクティベートせずに、ハードウェアデバイスを追加および交換し続けることができます。

アクティベーションなしのデバイスの変更数はインストールによって異なり、複数の変数に基づいて計算されます。詳細については、ページ131のライセンス情報を参照してください。

長期航行中の船舶状の監視システムやインターネットにアクセスできない遠隔地の監視システムなど、監視システムが長期間オフラインの場合は、Milestoneリセラーに連絡し、アクティベーションなしのデバイスの変更数を増やすように依頼できます。

アクティベーションなしのデバイスの変更数を増やす資格があると考える理由を説明する必要があります。Milestoneは各リクエストを個別に決定します。アクティベーションなしのデバイスの変更数が増えた場合は、ライセンスを認証して、XProtectシステムで登録するライセンス数を増やす必要があります。

アクティベーションなしのデバイスの変更数の計算方法

アクティベーションなしのデバイスの変更は、3つの変数に基づいて計算されます。Milestoneソフトウェアの複数のインストールがある場合は、変数はそれぞれに個別に適用されます。変数は以下のとおりです。

- アクティベーション済みライセンスの合計数の固定割合を示す**C%**。
- アクティベーションなしのデバイスの変更数の固定最小値を示す**Cmin**。
- アクティベーションなしのデバイスの変更数の固定最大値を示す**Cmax**。

アクティベーションなしのデバイスの変更数は、**Cmin**値より低くしたり、**Cmax**値より高くすることはできません。**C%**変数に基づいて計算された値は、システムの各インストールにあるライセンスアクティベーション済みデバイス数に応じて変化します。アクティベーションなしのデバイスの変更によって追加されたデバイスは、**C%**変数によるアクティベーションとしてカウントされません。

Milestoneは3つのすべての変数の値を定義します。値は通知なく変更される場合があります。変数の値は製品によって異なります。

製品の現在のデフォルト値の詳細については、My Milestoneを参照してください(https://www.milestonesys.com/device-change-calculation/) 。

C% = 15%、Cmin = 10、Cmax =100に基づく例

お客様が100個のハードウェアデバイスライセンスを購入します。100台のカメラをシステムに追加します。自動ライセンスアクティベーションを有効にしていない場合は、アクティベーションなしのデバイスの変更はゼロです。ライセンスをアクティベートすると、アクティベーションなしのデバイスの変更が15になります。

お客様が100個のハードウェアデバイスライセンスを購入します。100台のカメラをシステムに追加し、ライセンスをアクティベートします。ある顧客のアクティベーションなしのデバイスの変更は現在15です。その顧客はシステムからハードウェアデバイスを削除することを決定しました。現在99台のデバイスがアクティベートされ、アクティベーションなしのデバイスの変更数は14まで減りました。

顧客が1000個のデバイスライセンスを購入します。1000台のカメラを追加し、ライセンスをアクティベートします。ある顧客のアクティベーションなしのデバイスの変更は現在100です。C%変数に従えばアクティベーションなしのデバイスの変更数は150になったはずです。しかしCmax変数ではアクティベーションなしのデバイスの変更数は100以下に制限されています。

ある顧客が10のデバイスライセンスを購入します。10台のカメラをシステムに追加し、ライセンスをアクティベートします。Cmin変数のため、アクティベーションなしのデバイスの変更数は現在10です。数がC%変数にのみ基づいて計算されている場合は、1 (10の15% = 1.5、1に切り捨て)しかありません。

ある顧客が115個のデバイスライセンスを購入します。100台のカメラをシステムに追加し、ライセンスをアクティベートします。ある顧客のアクティベーションなしのデバイスの変更は現在15です。ライセンスのアクティベーションをせずに別の15台のカメラを追加します。アクティベーションなしのデバイスの変更15のうち15を使用します。50台のカメラをシステムから削除し、アクティベーションなしのデバイスの変更は7まで下がります。つまり、アクティベーションなしのデバイスの変更15を使用して前に追加したカメラ8台が猶予期間になります。お客様は50台の新しいカメラを追加します。前回ライセンスをアクティベートしたときにシステムで100台のカメラをアクティベートしたため、アクティベーションなしのデバイスの変更は15に戻ります。猶予期間になった8台のカメラはアクティベーションなしのデバイスの変更として元の状態に戻ります。50台の新しいカメラは猶予期間になります。

ライセンス概要の表示

同じソフトウェアライセンスファイル経由でライセンス付与されたすべてのサイトの、アクティベート済み、猶予期間中、期限切れ、および不足しているライセンスの一覧を表示するライセンス概要にアクセスできます。

- ライセンス概要をクリックします。

接続が停止している場合、アクティベートされたライセンス数だけが表示されます。猶予期間中、期限切れ、および不足しているライセンスには「なし」と表示されます。

自動ライセンスアクティベーション(説明付き)

メンテナンスを容易にし、柔軟性を高めるために、Milestoneは、自動ライセンスアクティベーションを有効にすることをお勧めします(ページ136の自動ライセンスアクティベーションを有効にするを参照)。これにより、メンテナンスを減らせます。自動ライセンスアクティベーションでは、マネジメントサーバーがオンラインでなければなりません。

これらの要件が満たされている場合、ハードウェアデバイスを追加、削除、または交換した後、またはライセンスの使用に影響するその他の変更を行った後、数分後に、ハードウェアデバイスまたは他のライセンスがアクティベーションされます。ライセンスアクティベーションを手動で開始する必要がありません。使用済みのアクティベーションなしのデバイスの変更数は常にゼロです。猶予期間あるいは期限切れのリスクのあるハードウェアデバイスはありません。基本ライセンスのいずれかが14日以内に期限切れになる場合は、XProtectシステムは、追加の対策として、毎夜自動的にライセンスを認証しようとします。

手動でライセンスをアクティベートしなければならないのは、以下の場合のみです:

- 追加ライセンスの購入(ページ137の追加ライセンスの取得を参照)
- アップグレードする(ページ473のアップグレード要件を参照)
- Milestone Careサブスクリプションの購入または更新(自動ライセンスアクティベーション(説明付き)を参照)
- アクティベーションなしのデバイスの変更での許容数を受け取る(ページ133のアクティベーションなしのデバイスの変更(説明付き)を参照)

自動ライセンスアクティベーションを有効にする

1. [ライセンス情報]ページで、[自動ライセンスアクティベーションを有効にする]を選択します。
2. 自動ライセンスアクティベーションで使用するユーザー名とパスワードを入力します。
   - 既存ユーザーの場合は、ユーザー名とパスワードを入力して、「Software Registration System(ソフトウェア登録システム)」にログインします。
   - 新規ユーザーの場合は、**Create new user**(新しいユーザーを作成する)リンクをクリックして、新しいユーザーアカウントを設定してから、登録手順を実行します。ソフトウェアライセンスコード(SLC)をまだ登録していない場合は、登録してください。

     資格情報はマネジメントサーバーのファイルに保存されます。
3. **OK** をクリックします。

自動ライセンスアクティベーション用のユーザー名またはパスワードを後から変更する場合は、[アクティベーション資格情報の編集]リンクをクリックします。

自動ライセンスアクティベーションを無効にする

自動ライセンスアクティベーションを無効にし、後から使用できるようにパスワードを保持する

1. [ライセンス情報]ページで、[自動ライセンスアクティベーションを有効にする]を解除します。パスワードとユーザー名はマネジメントサーバーにそのまま保存されます。

自動ライセンスアクティベーションを無効にし、パスワードを削除する

1. [ライセンス情報]ページで、[アクティベーション資格情報を編集する]をクリックします。
2. [パスワードの削除]をクリックします。
3. パスワードとユーザー名をマネジメントサーバーから削除することを確認します。

ライセンスをオンラインでアクティベーション

マネジメントサーバーを実行するコンピュータがインターネットに接続している場合は、ライセンスをオンラインでアクティベーションします。

1. [ライセンス情報]ノードで、[ライセンスの手動認証]、[オンライン]の順に選択します。
2. [オンライン認証]ダイアログボックスが開きます。
   - 既存のユーザーの場合は、ユーザー名とパスワードを入力します。
   - 新規ユーザーの場合は、[**Create new user**(新しいユーザーを作成)]リンクをクリックして、新しいユーザーアカウントを設定します。ソフトウェアライセンスコード(SLC)をまだ登録していない場合は、登録してください。
3. **OK** をクリックします。

オンラインアクティベーション中にエラーメッセージが発生した場合は、画面の手順に従って問題を解決するか、Milestoneサポートにお問い合わせください。

ライセンスをオフラインでアクティベート

マネジメントサーバーを実行するコンピュータがインターネットに接続していない場合、ライセンスをオフラインでアクティベートできます。

1. [ライセンス情報]ノードで、[ライセンスの手動アクティベーション]>[オフライン]>[アクティベートするライセンスをエクスポート]を選択し、追加したハードウェアデバイスに関する情報とともにライセンスリクエストファイル(.lrq)をエクスポートします。
2. ライセンスリクエストファイル(.lrq)には、自動的にSLCと同じ名前が付けられます。複数のサイトがある場合は、必ず名前を一意にし、どのファイルがどのサイトに属しているのか簡単に識別できるようにしてください。
3. インターネットに接続しているコンピュータにライセンスリクエストファイルをコピーし、Webサイト(https://online.milestonesys.com/) にログインして、アクティベーション済みのソフトウェアライセンスファイル(.lic)を取得します。
4. ライセンスリクエストファイルと同じ名前の.licファイルがインストールされたManagementClientコンピュータにコピーします。
5. [ライセンス情報]ページのManagement Clientで、[ライセンスをオフラインでアクティベーション]>[アクティベーションされたライセンスのインポート]を選択しアクティベーション済みのソフトウェア ライセンス ファイルを選択してインポートし、ライセンスを認証します。
6. 終了をクリックして、アクティベーションプロセスを終了します。

猶予期間が切れた後にライセンスをアクティベートする

猶予期間内にライセンス(ハードウェアデバイス、Milestone Interconnect、カメラ、ドアライセンス) を認証しない場合、デバイスが使用できなくなり、データを監視システムに送信できません。

- カメラの設定、およびその他の設定はManagement Clientから削除されません。
- ライセンスはシステム構成から削除されません
- 使用可能なデバイスを再度有効にするには、ライセンスを通常通りアクティブ化します。詳細については、ページ137のライセンスをオフラインでアクティベートまたはページ136のライセンスをオンラインでアクティベーションを参照してください。

追加ライセンスの取得

現在のライセンス数を超えて、その他のハードウェアデバイス、Milestone Interconnectシステム、またはドアを追加する場合または既に追加した場合、追加ライセンスを購入し、デバイスがデータをシステムに送信できるようにする必要があります。

- 使用しているシステムの追加ライセンスを入手するには、XProtect製品の代理店にお問い合わせください。

既存の監視システムバージョンの新しいライセンス:

- ライセンスを手動でアクティベートし、新しいライセンスを入手します。詳細については、ページ137のライセンスをオフラインでアクティベートまたはページ136のライセンスをオンラインでアクティベーションを参照してください。

新しいライセンスとアップグレードされた監視システムバージョン：

- 新しいライセンス、新しいバージョンの、更新されたソフトウェアライセンスファイル(.lic)(ページ49のライセンス(説明付き) を参照) を受け取ります。新しいバージョンのインストール中には、新しいソフトウェアライセンスファイルを使用する必要があります。詳細については、ページ473のアップグレード要件を参照してください。

ライセンスとハードウェアデバイスの交換

システムでライセンスがアクティベートされているカメラなどのハードウェアデバイスを新しいハードウェアデバイスと交換して、新しいハードウェアデバイスを有効にしライセンス付きにすることができます。

レコーディングサーバーからハードウェアデバイスを取り外すと、ハードウェアデバイスライセンスに空きができます。

あるカメラを同等のカメラ(メーカー、ブランド、およびモデル) と交換し、新しいカメラに同じIPアドレスを付与すると、すべてのカメラのデータベースへの完全なアクセスを維持できます。この場合、Management Clientでの設定は一切変更せずに、ネットワークケーブルを古いカメラから新しいカメラへ移動させます。

別のモデルのハードウェアデバイスと交換する場合は、ハードウェアの交換ウィザードを使用して、すべてのカメラ、マイク、入力、出力、および設定などの関連データベースをマップする必要があります(ページ455のハードウェアの交換を参照してください) 。

自動ライセンスアクティベーションを有効にした場合は(ページ136の自動ライセンスアクティベーションを有効にするを参照) 、新しいハードウェアデバイスが自動的に認証されます。

アクティベーションなしのデバイスの変更をすべて使用した場合は(ページ133のアクティベーションなしのデバイスの変更(説明付き) を参照) 、ライセンスを手動で認証する必要があります。詳細については、ページ137のライセンスをオフラインでアクティベートまたはページ136のライセンスをオンラインでアクティベーションを参照してください。

サイト情報

大規模なMilestone Federated Architecture設定の場合など、各サイトを容易に識別できるように、サイトに詳細情報を追加できます。サイト名以外に、次の情報を追加できます。

- アドレス/場所
- 管理者
- 詳細情報

サイト情報の編集

サイト情報を更新するには：

1. 編集を選択します。
2. タグを選択します。
3. 値フィールドに情報を入力します。
4. OK をクリックします。

サイトナビゲーション：サーバーとハードウェア

このセクションではレコーディングサーバーのインストールと設定方法を説明します。また、システムに新しいハードウェアを追加し、他サイトと相互接続するやり方も学べます。

- ページ139のサイトナビゲーション：サーバーとハードウェア：レコーディングサーバー
- ページ172のサイトナビゲーション：サーバーとハードウェア：フェールオーバーサーバー
- ページ183のサイトナビゲーション：サーバーとハードウェア：ハードウェア
- ページ197のサイトナビゲーション：サーバーとハードウェア：リモートサーバーの管理

サイトナビゲーション：サーバーとハードウェア：レコーディングサーバー

レコーディングサーバー(説明付き)

システムは、ビデオフィードのレコーディング、及び、カメラと他デバイスとのコミュニケーションのためのレコーディングサーバーを使用します。一般的に、監視システムには複数のレコーディングサーバーがあります。

レコーディングサーバーはレコーディングサーバーソフトウェアをインストールし、管理サーバーとコミュニケートするよう設定されたコンピュータです。[サーバー]フォルダーを展開し、[レコーディングサーバー]を選択すると、[概要]ペインにレコーディングサーバーが表示されます。

このバージョンのマネジメントサーバーよりも前のレコーディングサーバーのバージョンとの後方互換性は制限されています。旧バージョンのレコーディングサーバーの録画にアクセスすることはできますが、それらの設定を変更するには、このバージョンのマネジメントサーバーと一致していることを確認してください。Milestoneでは、システム内のすべての記録サーバーを、管理サーバーと同じバージョンにアップグレードすることをお勧めします。

レコーディングサーバーは、クライアントとサービスのためのデータストリームの暗号化をサポートします。さらに情報が必要な時は、ページ58のインストールを開始する前にを参照:

- ページ407のクライアントとサーバーに対して暗号化を有効にする
- ページ144のクライアントへの暗号化ステイタスを見る

レコーディングサーバーもまた、マネージメントサーバーとの通信の暗号化に対応しています。ページ58のインストールを開始する前にさらに情報が必要な時は、レコーディングサーバーデータ暗号化(説明付き)を参照:

- ページ404の暗号化を有効にする
- ページ405のレコーディング サーバーまたはリモートサーバーのサーバー暗号化を有効にする

レコーディングサーバーの管理については、次のような複数のオプションがあります。

- ページ183のハードウェアの追加
- ページ451のハードウェアの移動
- ページ469のレコーディングサーバーでのすべてのハードウェアの削除
- ページ469のレコーディングサーバーの削除

> レコーディングサーバーサービスの実行中は、WindowsExplorerや他のプログラムが、お使いのシステム設定に関連付けられたメディアデータベースファイルやフォルダーにアクセスしていないことが非常に重要です。アクセスしている場合は、レコーディングサーバーの名前を変更したり、関連するメディアファイルを移動できません。このためにレコーディングサーバーが停止することがあります。停止したレコーディングサーバーを再開するには、レコーディングサーバーサービスを停止し、関連するメディアファイルやフォルダーにアクセスしているプログラムを閉じ、レコーディングサーバーサービスを再起動してください。

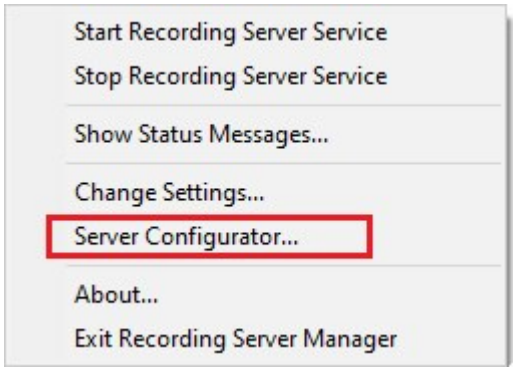
レコーディングサーバーを登録する

レコーディングサーバーをインストールすると、大抵の場合自動的に登録されます。ただし、次のような場合は手動で登録しなければなりません。

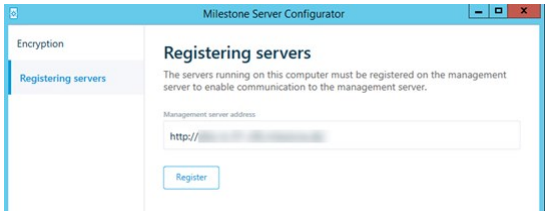
- レコーディングサーバーを交換しました。
- レコーディングサーバーがオフラインでインストールされており、その後でマネージメントサーバーに追加された
- マネージメントサーバーがデフォルトのポートを使用していません。ポート番号は暗号化の設定によって異なります。詳細については、ページ33のこのシステムで使用するポートを参照してください
- 自動登録は、管理サーバーのアドレスを変更した後や、サーバーの通信暗号化設定を有効または無効にした後などに失敗します。

レコーディングサーバーを登録すると、マネージメントサーバーに接続するように設定できます。登録を扱うマネージメントサーバーの一部は、Authorization Serverサービスです。

1. WindowsのスタートメニューまたはレコーディングサーバーのトレイアイコンのいずれかからServerConfiguratorを開きます。



2. Server Configuratorで[サーバーの登録]を選択します。



3. 管理サーバーのアドレスと、コンピュータ上のサーバーを接続したいスキーム (http またはhttps) を確認し、[登録]をクリックします。

管理サーバーの登録が成功したことを示す確認メッセージが表示されます。

「ページ450のレコーディングサーバーの交換」も参照してください。

レコーディングサーバーの基本的な設定を変更または確認する

Management Clientで、インストールしたすべてのレコーディングサーバーが表示されない場合、通常は、インストール中に設定パラメータを正しく設定しなかったことが原因です(マネジメントサーバーのIPアドレスやホスト名など) 。

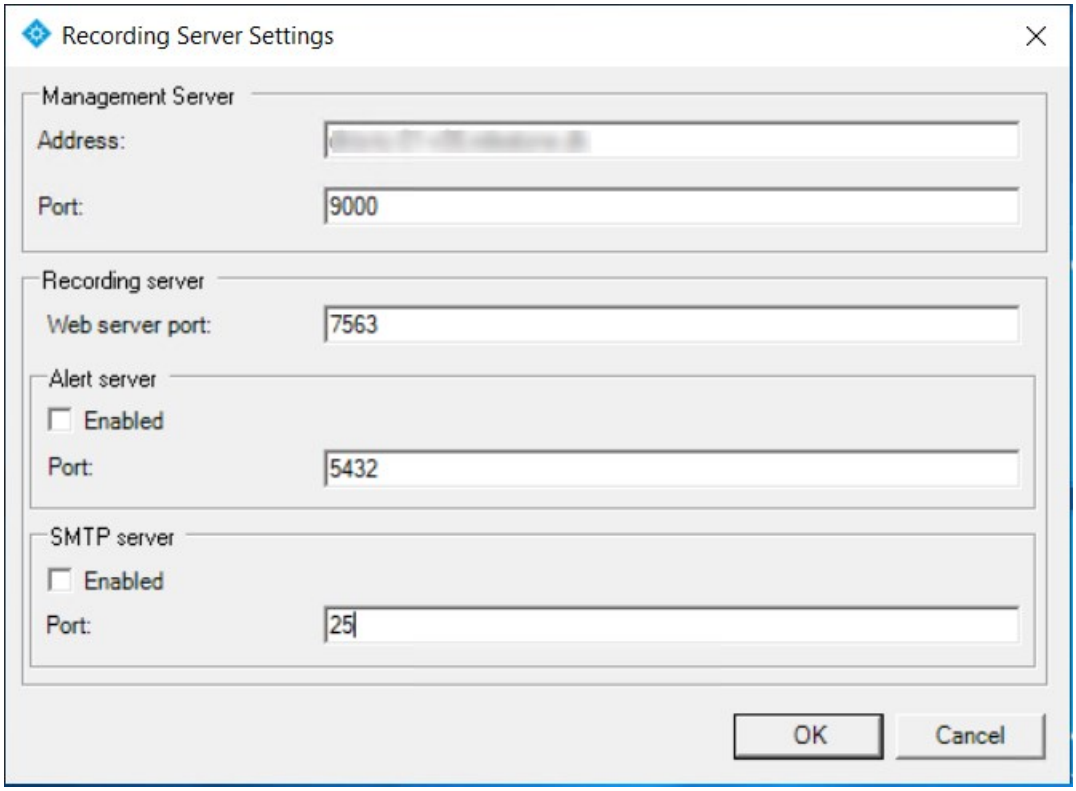
管理サーバーのパラメータを指定するには、レコーディングサーバーを再インストールする必要はありません。次の方法で基本設定を変更/確認できます。

1. レコーディングサーバーを実行しているコンピュータで、通知エリアにあるレコーディングサーバーアイコンを右クリックします。

2. レコーディングサーバーサービスの停止を選択。

3. レコーディングサーバーアイコンを再び右クリックし、設定の変更を選択します。

   レコーディングサーバーの設定ウィンドウが表示されます。



4. たとえば、以下の設定を確認するか変更します:
   - 管理サーバー: アドレス: レコーディングサーバーを接続する必要のある管理サーバーのIPアドレスまたはホスト名を指定します。
   - 管理サーバー: ポート: 管理サーバーと通信する際に使用するポート番号を指定します。これは必要に応じて変更できますが、ポート番号は常に管理サーバーで設定されているポート番号に一致しなくてはなりません。ページ33のこのシステムで使用するポートを参照してください。
   - レコーディングサーバー: Webサーバーポート: レコーディングサーバーのWebサーバーと通信する際に使用するポート番号を指定します。ページ33のこのシステムで使用するポートを参照してください。
   - レコーディングサーバー: アラートサーバーポート:レコーディングサーバーのアラートサーバーと通信する際に使用するポート番号を有効にして指定します。ここでデバイスからのイベントメッセージを受領します。ページ33のこのシステムで使用するポートを参照してください。
   - SMTPサーバー: ポート: レコーディングサーバーのSMTPサービスと通信する際に使用されるポート番号を有効にして指定します。ページ33のこのシステムで使用するポートを参照してください。
5. OK をクリックします。
6. レコーディングサーバーサービスを再開するには、[レコーディングサーバー]アイコンを右クリックして[レコーディングサーバーサービスの開始]を選択します。

> レコーディングサーバーサービスを停止すると、レコーディングサーバーの基本設定を確認/変更している間は、ビデオ録画やビデオのライブ再生ができません。

[レコーディング サーバーの設定]ウィンドウ

Recording Server Managerトレイ アイコンを右クリックして[設定の変更]を選択すると、以下を指定できます:

名前	説明
アドレス	IPアドレス (例: 123.123.123.123) またはレコーディング サーバーを接続する管理サーバーのホスト名 (例: ourserver)。レコーディング サーバーは管理サーバーと通信できるため、この情報は必要です。
ポート	管理サーバーと通信する際に使用されるポート番号。デフォルトは9000です。これは必要に応じて変更できます。
Webサーバーポート	Webサーバーのリクエストに対応する際に使われるポート番号 (例: PTZカメラコントロール コマンドの対応、参照およびXProtect Smart Clientからのライブ リクエスト)。デフォルトは7563です。これは必要に応じて変更できます。
アラートサーバーポート	レコーディング サーバーがTCP情報を受信する際に使われるポート番号 (イベント メッセージの送信でTCPを使用するデバイスもあります)。デフォルトはポート5432です (デフォルトで無効になっています)。必要に応じて、この順序は変更できます。
SMTPサーバーポート	レコーディング サーバーがSMTP情報を受信する際に使われるポート番号。SMTPは、サーバー間で電子メールメッセージを送信する標準です。メッセージや画像を監視システム サーバーに弟子メールで送信するためにSMTPを使用するデバイスもあります。デフォルトは25です。これは有効・無効にできます。必要に応じて、ポート番号は変更できます。
管理サーバーからレコーディングサー	暗号化を有効にして、リストからサーバー認証証明書を選択する前に、最初に管理サーバーで暗号化を有効にし、管理サーバー証明書がレコーティング サーバーで信頼されていることを確認します。 詳細については、ページ58のインストールを開始する前にを参照してください

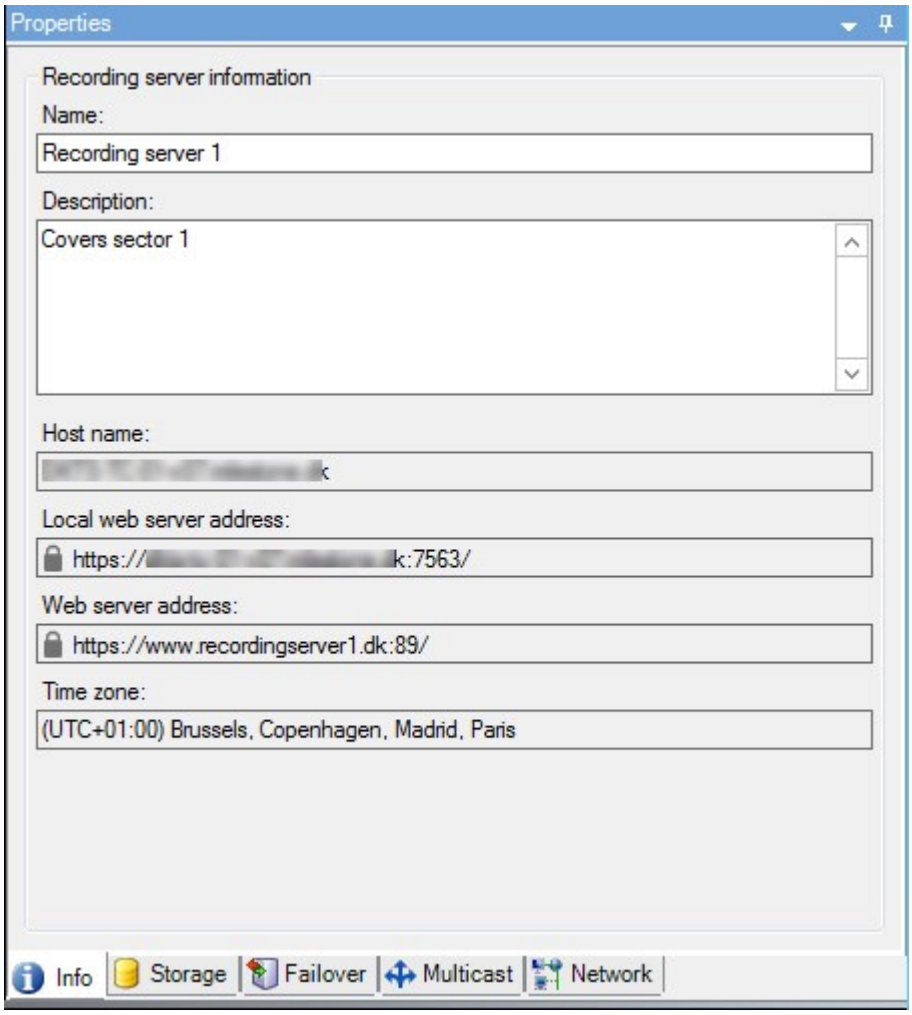
名前	説明
バーへの接続を暗号化	
データのストリーミングを行うクライアントとサービスへの接続を暗号化	暗号化を有効にして、リストからサーバー認証証明書を選択する前に、レコーティング サーバーからデータストリームを取得するサービスを実行しているすべてのコンピュータで証明書が信頼されていることを確認します。XProtect Smart Clientと、レコーディング サーバーからデータストリームを取得するサービスはすべて、バージョン2019 R1以降でなくてはなりません。MIP SDKの2019 R1よりも前のバージョンを使用して作成されたサードパーティ ソリューションは、更新が必要な可能性があります。詳細については、ページ58のインストールを開始する前にを参照してください。 レコーディング サーバーが暗号化を使用していることを確認するには、ページ144のクライアントへの暗号化ステイタスを見るを参照してください。
詳細	特定の証明書については、Windows証明書ストアの情報を確認してください。

クライアントへの暗号化ステイタスを見る

レコーディングサーバーが暗号化接続を行なっているかを確認するには:

1. Management Clientを開きます。
2. [サイトナビゲーション]ペインで、[サーバー]>[レコーディングサーバー]を選択します。レコーディングサーバーのリストが表示されます。

3. オーバービューパネル上で関連するレコーディングサーバー を選択し、インフォメーションタブへ。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クライアントとサーバーで暗号化が可能ならば、ローカルWebサーバーアドレスとオプショナルWebサーバーアドレスの前にパッドロックアイコンが現れます。



レコーディングサーバーステータスアイコン

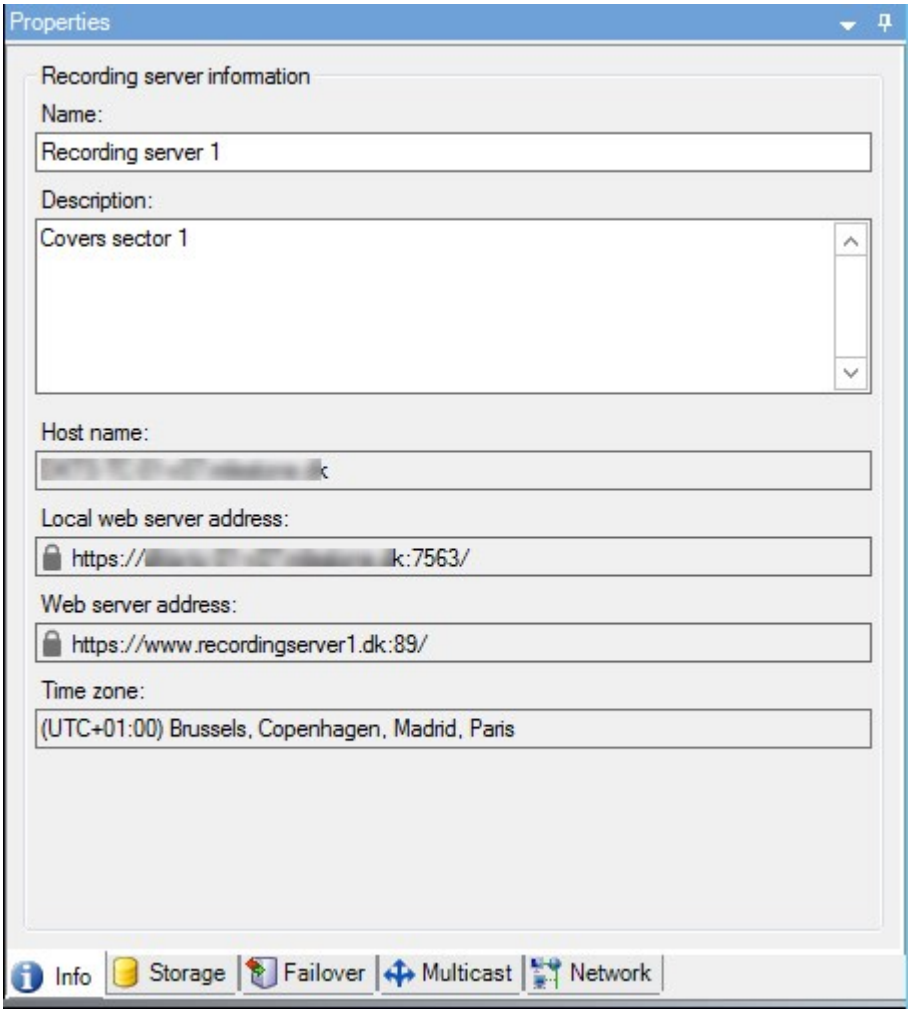
Management Clientは、次のアイコンを個別のレコーディングサーバーの状態を示すために使用します。

アイコン	説明
	レコーディングサーバーは実行中です
	Recording Serverは注意が必要です：レコーディングサーバーが実行されていないか、実行にエラーが伴っています。 1. レコーディングサーバーアイコンの上をマウスオーバーし、ステイタスメッセージを確認してください。 2. レコーディングサーバーをスタート、あるいはストップしたい場合、Recording Server Manager トレイアイコンを右クリックしてください。
	動作中のデータベース修復：電源障害の場合など、データベースが破損し、レコーディングサーバーが修復している時に表示されます。データベースが大きい場合は、修復に時間がかかります。 データベースの破損を避けるための有益な情報は、ページ56の記録データベースを破損から守るを参照してください。 起動時のデータベースの修復中は、レコーディングサーバーに接続されているカメラからビデオを録画することはできません。ライブ表示のみが可能です。 通常動作時のデータベースの修復は、録画に影響しません。

情報タブ(レコーディングサーバー)

インフォメーションタブ上で、レコーディングサーバーの名前と詳細を確認したり、変更したりできます。

ホスト名とアドレスを見ることができます。Webサーバーアドレスの前にあるパッドロックアイコンは、この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クライアントとサービスの通信が暗号化されていることを意味します。



インフォメーションタブ機能(レコーディングサーバー)

名前	説明
名前	入力するレコーディングサーバーの名前を選ぶことができます。この名前は、レコーディングサーバーがリスト化されている際、システムとクライアントにおいて使用されます。名前は一意である必要はありません。 レコーディングサーバーの名前を変更すると、名前はManagement Clientで一括変更されます。
説明	システム内にリスト化されている数字の中に表示される説明を入力することができます。説明は必須ではありません。
ホスト名	レコーディングサーバーのホスト名を表示します。

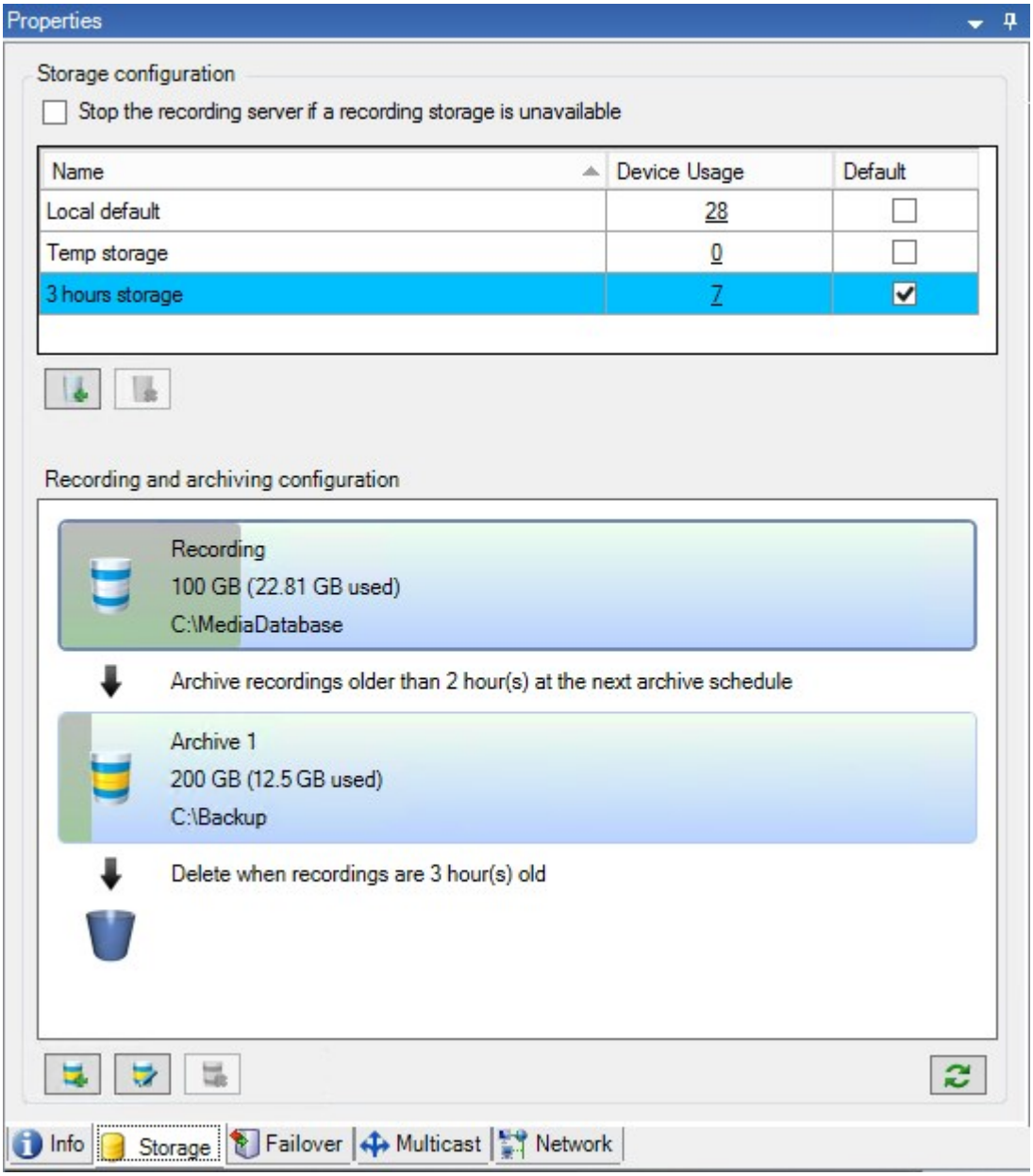
名前	説明
ローカルWebサーバーアドレス	レコーディングサーバーのWebサーバーのローカルアドレスを表示。例えば、PTZ カメラコントロール コマンドを使用したり、XProtect Smart Clientからのライブリクエストを閲覧する際には、ローカルアドレスを使用します。 Webサーバー コミュニケーションに使われているポートナンバー含むアドレス(標準ポート7563)。 暗号化を可能にする時は、パッドロックアイコンとhttpの代わりにhttpsを含むアドレスが表示されます。
Webサーバーアドレス	インターネット上でレコーディングサーバーのWebサーバーのパブリックアドレスを表示する。 クライアントがインターネット上でレコーディングサーバーに接続できる監視システムにアクセスできるよう、インストールにおいてファイアーオールあるいはNATルーターを使用する際は、ファイアーウォールまたはNATルーターのアドレスを入力してください。 パブリックアドレスとネットワークタブ上でポートナンバーを指定する。 暗号化を可能にする時は、パッドロックアイコンとhttpの代わりにhttpsを含むアドレスが表示されます。
時間ゾーン	レコーディングサーバーのあるタイムゾーンを表示する。

ストレージタブ(レコーディングサーバー)

ストレージタブで、選択したレコーディングサーバーのストレージを設定、管理および表示することができます。

レコーディングストレージとアーカイブでは、水平バーは現在の空き容量を表しています。レコーディングストレージが使用できない場合のレコーディングサーバーの動作を設定することができます。これはほとんどの場合、ご利用のシステムにフェールオーバーサーバーがあるときに関係する設定です。

エビデンスロックを使用している場合、エビデンスロックのビデオに使用される容量を示す縦の赤線があります。



ストレージとアーカイブ(説明)

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。

カメラやデバイスがビデオおよび/または音声を録画した場合、すべての指定された録画はデフォルトでそのデバイスに対して定義されているストレージに保存されます。各ストレージは、レコーディングデータベースレコーディング内に録画を保存しているレコーティングストレージからなります。ストレージにはデフォルトのアーカイブはありませんが、作成できます。

レコーディングデータベースがいっぱいになるのを避けるため、追加ストレージを作成できます (新規ストレージの追加を参照)。各ストレージ内でアーカイブ(「ストレージでのアーカイブの作成」を参照) を作成し、アーカイブプロセスを介してデータを保存することも可能です。

> アーカイブとは、カメラのレコーディングデータベースから別の場所などへの、録画の自動的な転送です。これにより、保存できる録画データ量は、録画データベースのサイズによって制限を受けません。アーカイブでは、録画を別のメディアにバックアップできます。

ストレージとアーカイブは、レコーディングサーバーごとに設定します。

アーカイブされた録画をローカルまたはアクセス可能なネットワークドライブに保存する限り、XProtect Smart Clientを使用して表示できます。

ディスクドライブが破損してレコーディングストレージが使用できなくなった場合、水平バーが赤に変わります。その場合でもXProtectSmartClientでライブビデオを見ることはできますが、ディスクドライブを復旧するまで録画やアーカイブはできません。システムがフェールオーバーレコーディングサーバーで構成されている場合は、レコーディングサーバーの実行を停止させて、フェールオーバーサーバーに引き継がせるように設定できます(レコーディングストレージを利用できない場合の動作を指定を参照)。

次の点は、一般的にカメラとビデオに該当しますが、スピーカー、マイク、音声、およびサウンドにも適用されます。

> Milestoneレコーディングストレージとアーカイブには専用のハードディスクドライブを使用し、ディスクのパフォーマンス低下を防止することをお勧めします。ハードディスクをフォーマットする際は、アロケーションユニットサイズの設定を4 KBから64 KBに変更することが重要です。この変更によって、ハードディスクの録画パフォーマンスが大幅に改善できます。単位サイズの割り当てとヘルプについては、Microsoft社のWebサイト(https://support.microsoft.com/help/140365/default-cluster-size-for-ntfs-fat-and-exfat/)を参照。

> 空き容量が5GB未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます(または、次のアーカイブが定義されていない場合は削除されます)。空き容量が1GB未満になった場合は、データは削除されます。データベースには、必ず250MBの空き容量が必要です。データが十分速やかに削除されていないため、この制限に達した場合、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より5GB少なくなります。

> 非FIPS準拠暗号で暗号化されている2017 R3よりも前のXProtect VMSのバージョンからのエクスポートとアーカイブ済みメディアデータベースのあるFIPS 140-2準拠システムでは、FIPSを有効にした後でもアクセスできる場所でデータをアーカイブする必要があります。
> FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、強化ガイドのFIPS 140-2準拠セクションを参照してください。

デバイスをストレージに接続する

レコーディングサーバーに対してストレージおよびアーカイブを設定すると、個別のカメラまたはカメラのグループに対してストレージおよびアーカイブを有効にできます。この操作は、個々のデバイス、またはデバイスグループから行えます。個別のデバイスまたはデバイスのグループをストレージに接続するを参照してください。

効果的なアーカイブ

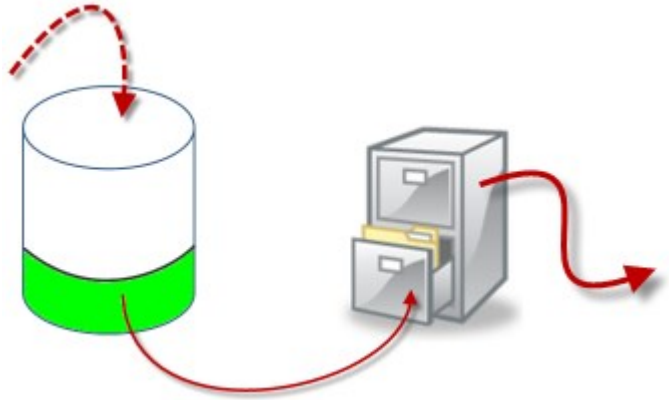
カメラまたはカメラのグループに対してアーカイブが有効であれば、レコーディングストレージの内容は定義した間隔で、自動的に最初のアーカイブへ移動します。

要件によって、それぞれのストレージに対して1つまたは複数のアーカイブを設定することができます。アーカイブは、レコーディングサーバーのコンピュータ、あるいはネットワークドライブなどのシステムが接続できる別の場所に配置することができます。

アーカイブを効果的に設定することで、ストレージのニーズを最適化できます。多くの場合、アーカイブされた録画がなるべくディスク容量を必要としないようにすることが望まれます。特に、長期的な観点では、画像品質を少し下げるだけでも意味があります。レコーディングサーバーのストレージタブで、次のような相互依存している設定を調整することで効果的にアーカイブを調整することが可能になります。

- レコーディングストレージの保持
- レコーディングストレージのサイズ
- アーカイブの保持
- アーカイブのサイズ
- アーカイブのスケジュール
- 暗号化
- 秒当たりのフレーム数(FPS)

サイズフィールドは、シリンダー単位での、レコーディングデータベースおよびそのアーカイブのそれぞれのサイズを定義します。



シリンダーにおける空きエリアによって例証される、録画ストレージデータベースの保持時間とサイズの設定で、古い録画をアーカイブするまでの期間を定義します。例の図では、アーカイブするのに充分な期間が経過すると、録画がアーカイブされます。

アーカイブの保存期間とサイズ設定は、録画がアーカイブにある期間を定義します。指定した期間、またはアーカイブが指定したサイズ上限に達するまで、録画がアーカイブに保存されます。これらの設定に該当すると、システムはアーカイブにある古い録画を上書きし始めます。

アーカイブのスケジュールによって、アーカイブが行われる頻度や開始時刻が定義されます。

FPSによって、データベースにおけるデータのサイズが決まります。

録画をアーカイブするには、こうしたパラメータをすべて、お互いに調和させながら設定する必要があります。これは、次回のアーカイブの保持時間は、現在のアーカイブまたは録画データベースの保持時間より長くなければならないことを意味しています。アーカイブに対して指定される保持日数には、プロセスで以前に指定されたすべての保存期間が含まれるためです。アーカイブは必ず保存期間より頻繁に行われなければなりません。そうしないとデータを失う恐れがあります。保持時間を24時間と設定した場合、24時間を経過したデータはすべて削除されます。従って、データを確実に次のアーカイブへ移動させるには、24時間毎より頻繁にアーカイブを行う必要があります。

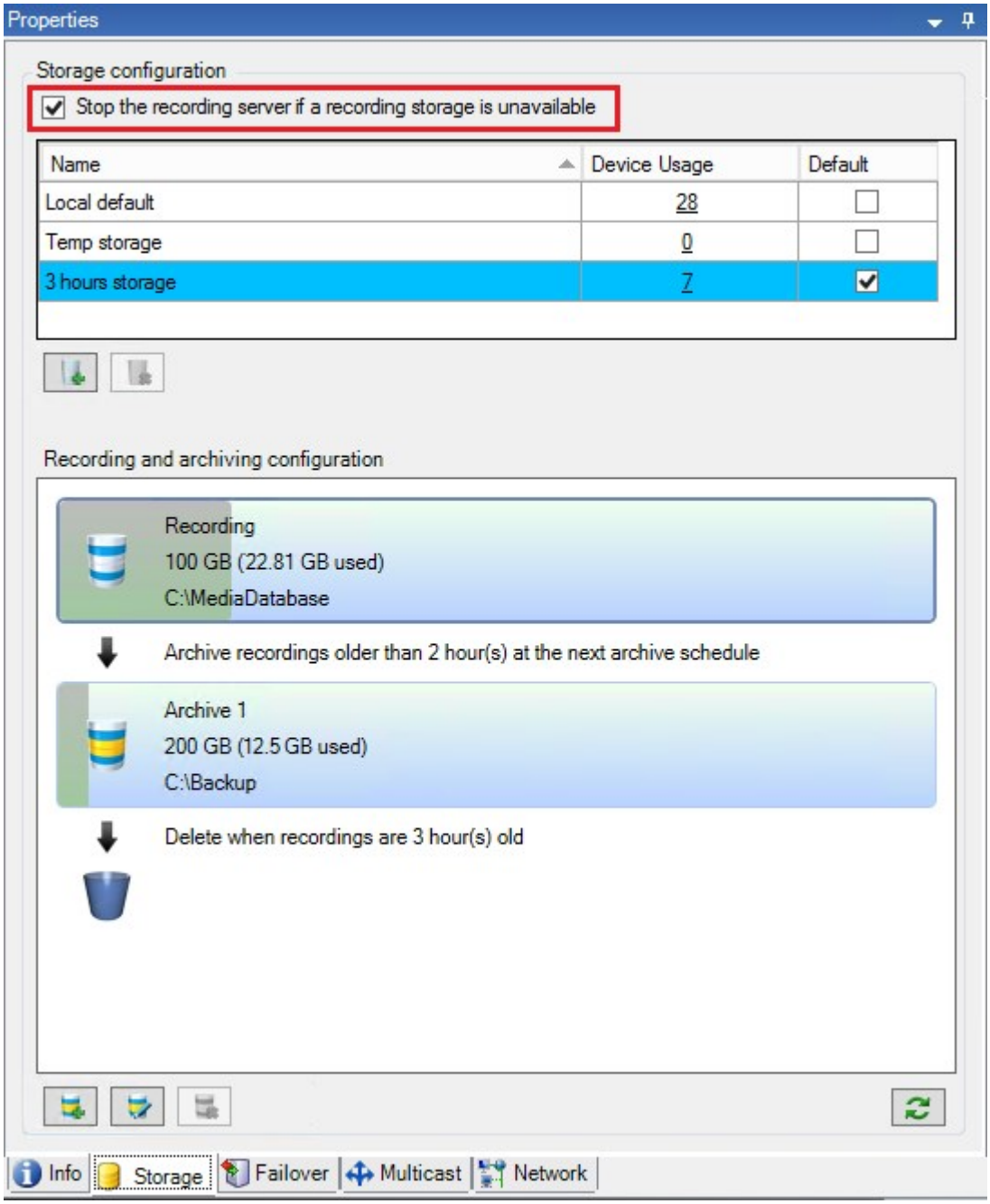
例：以下のストレージ(左の画像)の保持時間は4日であり、以下のアーカイブ(右の画像)の保持時間は10日です。アーカイブは毎日午前10時30分に行われるように設定されているため、必ず保持時間より頻繁にアーカイブが行われます。

ルールとイベントを使用してアーカイブをコントロールすることもできます。

レコーディングストレージが利用できない場合の動作を指定

デフォルトでは、レコーディングサーバーはレコーディングストレージが利用不可となっても実行し続けます。システムがフェールオーバーレコーディングサーバーで構成されている場合は、レコーディングサーバーの実行を停止させて、フェイルオーバーサーバーに引き継がせるよう設定できます:

1. 該当するレコーディングサーバーの[ストレージ]タブに移動します。
2. [レコーディングストレージが利用可能でない場合はレコーディングサーバーを止める]オプションを選択します。



新しいストレージの追加

新しいストレージを追加したときには、**Recording**という名前の定義済み記録データベースの録画ストレージを、常に1つ作成します。データベースの名前を変更することはできません。録画ストレージとは別に、ストレージには多数のアーカイブを保存できます。

1. 選択したレコーディングサーバーにさらにストレージを追加する場合は、ストレージ設定リストの下にあるボタンをクリックします。これによりストレージおよび録画設定ダイアログボックスが開きます。
2. 関連する設定を指定します(ストレージおよび録画設定のプロパティを参照)。
3. **OK** をクリックします。

これで、必要に応じて新しいストレージ内でアーカイブを作成する準備が整います。

ストレージでのアーカイブの作成

ストレージにはデフォルトのアーカイブはありませんが、作成できます。

1. アーカイブを作成するには、レコーディングおよびアーカイブの設定リストで必要なストレージを選択します。
2. レコーディングおよびアーカイブの設定リストの下にあるボタンをクリックします。
3. [アーカイブ設定]ダイアログボックスで、必要な設定を指定します(アーカイブ設定のプロパティを参照) 。
4. **OK** をクリックします。

個別のデバイスまたはデバイスのグループをストレージに接続する

レコーディングサーバーに対してストレージを設定した後で、個別のデバイス(カメラ、マイク、スピーカー) またはデバイスのグループに対して有効にすることができます。また、個別のデバイスまたはグループに対して、どのレコーディングサーバーのストレージエリアを使用するかを選択することも可能です。

1. デバイスを展開し、必要に応じてカメラ、マイクまたはスピーカーのいずれかを選択します。
2. デバイスまたはデバイスグループを選択します。
3. 記録タブを選択します。
4. ストレージエリアで、選択を選択します。
5. 表示されるダイアログボックスで、デバイスの記録を保存するデータベースを選択し、**OK**をクリックします。
6. ツールバーで保存をクリックします。

レコーディングサーバーのストレージタブで、ストレージエリアのデバイス使用数をクリックすると、表示されるメッセージレポートでデバイスを確認できます。

選択したストレージまたはアーカイブ設定の編集

1. レコーディングおよびアーカイブの設定リストで、ストレージを編集するには、記録データベースを選択します。アーカイブを編集するには、アーカイブデータベースを選択します。
2. レコーディングおよびアーカイブの設定リストの下にある レコーディングストレージの編集ボタンをクリックします。
3. 記録データベースの編集またはアーカイブの編集を行います。

> データベースの最大サイズを変更する場合、新しい上限を超える記録は自動アーカイブされます。
> 記録は次のアーカイブに自動アーカイブされるか、アーカイブ設定によっては削除されます。

エクスポートのデジタル署名を有効にします。

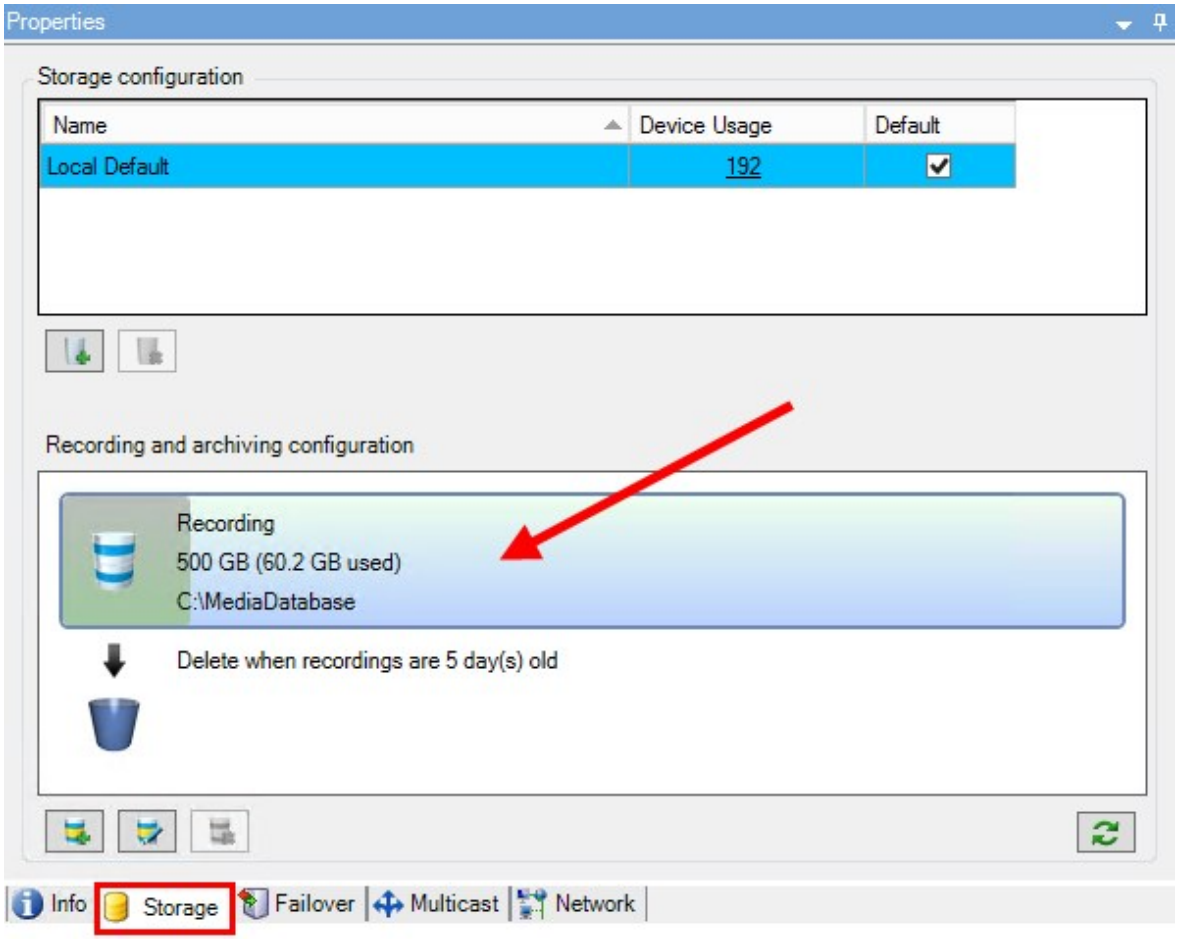
> 使用可能な機能は、使用しているシステムによって異なります。詳細については、https://www.milestonesys.com/solutions/platform/product-index/を参照してください。

録画ビデオのデジタル署名を有効にすれば、クライアントユーザーは録画ビデオが録画されてから改ざんされていないか検証できます。ビデオの信ぴょう性の検証は、ビデオがエクスポートされた後ユーザーがXProtect Smart Client - Playerで行います。

> 署名はXProtect Smart Client[エクスポート]ダイアログのでもアクティベーションしなければなりません。
> これを行わなければ、XProtect Smart Client - Playerの[署名の検証]ボタンは表示されません。

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ます。
2. レコーディングサーバーをクリックします。
3. 概要ペインで、署名を有効にしたいレコーディングサーバーをクリックします。

4. [プロパティ]ペインの下部にある [ストレージ] タブをクリックします。



5. 録画およびアーカイブ設定セクションで、録画データベースを表す水平バーをダブルクリックします。ストレージとレコーディングの設定 ウインドウが現れます。

6. 署名チェックボックスを選択します。

7. **OK** をクリックします。

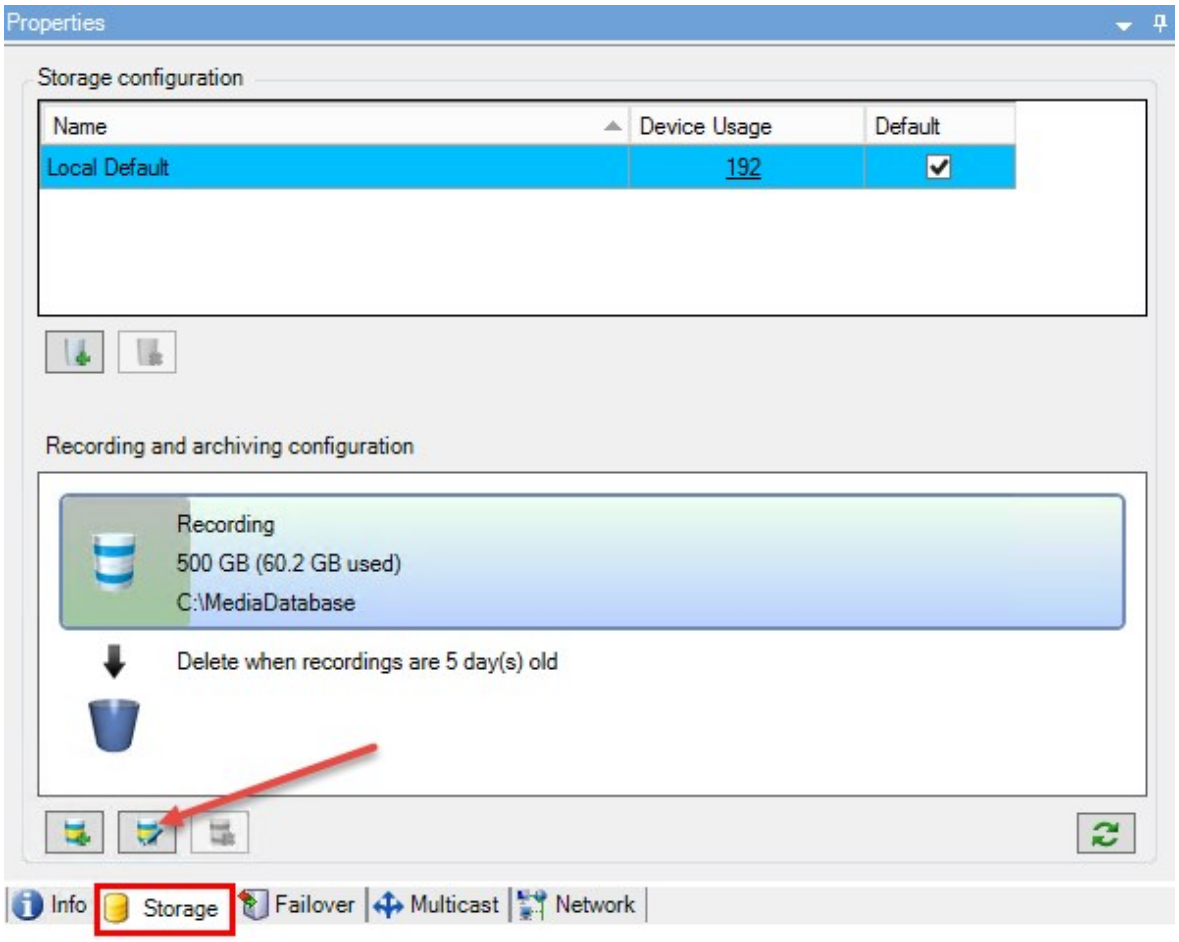
録画を暗号化する

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

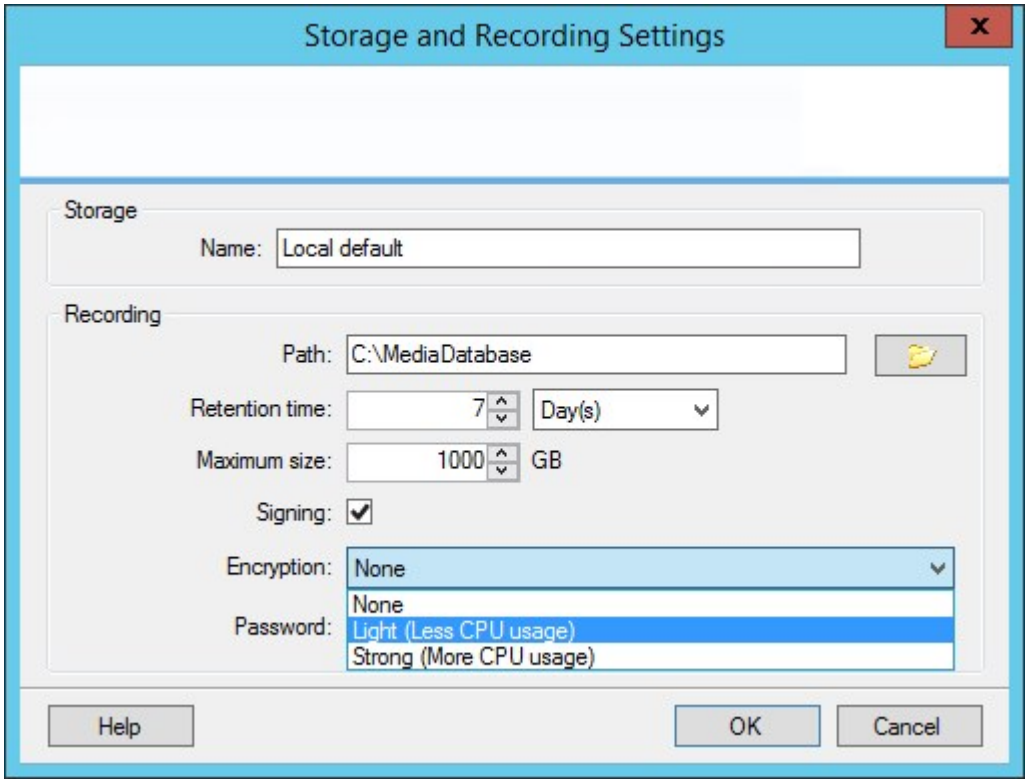
レコーディングサーバーのストレージおよびアーカイブで暗号化を有効にすることで、録画を守ることができます。簡易的な暗号化と、強化された暗号化から選ぶことができます。暗号化を有効にする選択をした場合、関連するパスワードも指定しなければなりません。

暗号化設定、あるいはパスワードを有効にする、あるいは変更する作業には時間がかかる場合があります。これは、データベースのサイズとドライブのパフォーマンスに依ります。現在のタスクの下で、進み具合を追うことができます。タスクの実行中は、レコーディングサーバーを停止させないでください。

1. 「レコーディングストレージおよびアーカイブの設定」リストの下にある［レコーディングストレージの編集］ボタンをクリックします。



2. 現れたダイアログボックスで、暗号化レベルを指定します。



3. パスワードの設定ダイアローグボックスに、自動的に遷移されます。パスワードを入力し、**OK**をクリックします。

アーカイブされた記録をバックアップする

多くの組織では、テープドライブや同等のものを使用して、記録をバックアップすることを考えています。これをどのように行うかは、組織で使用しているバックアップメディアによって異なります。ただし、以下の点を覚えておく必要があります：

カメラのデータベースではなくアーカイブをバックアップする

個別のカメラのデータベースではなく、必ずアーカイブの内容に基づいてバックアップを作成します。個別のカメラのデータベースに基づいてバックアップを作成すると、共有違反やその他の誤動作の原因となることがあります。

バックアップをスケジュールする際は、バックアップジョブのアーカイブ時間が決して重複しないように注意してください。ストレージタブを使用すると、各レコーディングサーバーのストレージエリアの、各レコーディングサーバーのアーカイブスケジュールを表示することができます。

アーカイブの構造を知ることでバックアップを効率化する

記録をアーカイブすると、アーカイブ内の特定のサブディレクトリ構造に保存されます。

全システムの標準的な使用中に、XProtect Smart Clientを使ってすべての録画を参照しているシステムユーザーにとって、サブディレクトリ構造はまったく認識されません。これは、アーカイブ済み記録と未アーカイブ記録の両方に当てはまります。アーカイブされた録画をバックアップするにはサブディレクトリ構造(アーカイブ構造(説明)を参照)を知ることが直接的に重要です(ページ441のシステム設定のバックアップおよび復元を参照)。

アーカイブ構造(説明付き)

録画をアーカイブすると、アーカイブ内の特定のサブディレクトリ構造に保存されます。

> 全システムの標準的な使用中に、録画がアーカイブされているかどうかにかかわらず、XProtect Smart Clientを使ってすべての録画を参照しているシステムユーザーにとって、サブディレクトリ構造はまったく認識されません。したがって、アーカイブされている録画をバックアップする場合には、サブディレクトリ構造を知ることは非常に重要です。

レコーディングサーバーのそれぞれのアーカイブディレクトリに、個別のサブディレクトリが自動的に作成されます。これらのサブディレクトリには、デバイス名とアーカイブデータベースに基づく名前が付きます。

別のカメラからの録画を同じアーカイブに保存することができ、それぞれのカメラのアーカイブは一定の間隔で実行されるので、サブディレクトリはさらに自動的に追加されます。

これらのサブディレクトリは、それぞれがほぼ1時間の録画を表します。1時間毎に分割することで、アーカイブの最大許容サイズに達した場合でも、アーカイブのデータの比較的小さい部分だけを削除することが可能になります。

サブディレクトリの名前は、録画がエッジストレージかSMTPのいずれによる録画であるかを示すデバイスの名前に続いて、サブディレクトリに含まれている最新のデータベースレコードの日付と時間を加えた名前になります。
名前の構造

```
...[ストレージのパス]\[ストレージ名]\[デバイス名] -最新の録画の日付と時間を追加]\
```

エッジ ストレージからの場合：

```
...[ストレージのパス]\[ストレージ名]\[デバイス名] (Edge) - 最新の録画の日付と時間を追加]\
```

SMTPからの場合：

```
...[ストレージのパス]\[ストレージ名]\[デバイス名] (SMTP) - 最新の録画の日付と時間を追加]\
```

現実の例

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

サブディレクトリ

さらにサブディレクトリがあれば、自動的に追加されます。これらのサブディレクトリの量と特性は、実際の録画の特性により異なります。たとえば、複数の異なるサブディレクトリは、録画が技術的にシーケンスに分割される場合に追加されます。これは多くの場合、録画をトリガーするためにモーション検知を使用する場合に当てはまります。

- メディア：このフォルダーには、ビデオまたは音声(両方ではない)の実際のメディアが含まれます。
- モーションレベル：このフォルダーには、当社のモーション検知アルゴリズムを使用して、ビデオデータから生成したモーションレベルのグリッドが含まれています。このデータで、XProtect Smart Clientのスマートサーチ機能が高速で検索を行うことができます。
- モーション：このフォルダーに、システムはモーションのシーケンスを保存します。モーションのシーケンスは、ビデオデータ中でモーションが検知されたタイムスライスです。たとえば、この情報はXProtectSmartClientのタイムラインで使用されます。
- レコーディング：このフォルダーに、システムはレコーディングのシーケンスを保存します。レコーディングのシーケンスは、メディアデータで一貫しているレコーディングのタイムスライスです。たとえば、この情報はXProtect Smart Clientでタイムラインを描画するために使用されます。
- 署名：このフォルダーには、メディアデータ用に生成された署名が含まれています(メディアフォルダーに)。この情報を使用すると、録画された後にメディアデータが改変されていないことを確認できます。

アーカイブをバックアップする場合、サブディレクトリ構造の基本を知ることで、正確にバックアップすることが可能になります。
バックアップの例

アーカイブ全体の内容をバックアップする場合、必要なアーカイブディレクトリとその内容のすべてをバックアップします。たとえば、次の下にあるすべてをバックアップします。

```
...F:\OurArchive\
```

特定の期間における特定のカメラからの録画をバックアップする場合は、関連するサブディレクトリの内容だけをバックアップします。たとえば、次の下にあるすべてをバックアップします。

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

ストレージでのアーカイブの削除

1. レコーディングおよびアーカイブの設定リストで、アーカイブを選択します。

   > リストで最後にあるアーカイブのみが削除できます。アーカイブを空にする必要はありません。

2. レコーディングおよびアーカイブの設定リストの下にあるボタンをクリックします。

3. はいをクリックします。

> オフラインの理由などによりアーカイブが利用できない場合は、アーカイブ削除の前に通信を復旧してください。

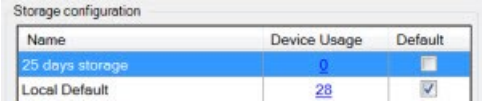
ストレージの削除

ライブレコーディングの録画ストレージとして使用するデフォルトのデバイスを削除することはできません。このためストレージを削除するにはデバイスとアーカイブされていない録画を他のストレージに移動する(ページ451のハードウェアの移動を参照) 必要があります。

1. このストレージを使用するデバイスを一覧表示するには、デバイス使用数をクリックします。

> 別のレコーディングサーバーに移動されたデバイスのデータがストレージにある場合は、警告が表示されます。リンクをクリックすると、デバイスの一覧が表示されます。

2. 「アーカイブされていない記録をあるストレージから別のストレージへ移動する」の手順を参照してください。
3. すべてのデバイスを移動し終わるまで続行します。
4. 削除するストレージを選択します。



5. ストレージ設定リストの下にあるボタンをクリックします。
6. はいをクリックします。

アーカイブされていない記録をあるストレージから別のストレージへ移動する

ある記録データベースから別の記録データベースへのコンテンツの移動は、デバイスの記録タブで行います。

1. デバイスタイプを選択します。概要ペインで、デバイスを選択します。
2. [録画] タブをクリックします。ストレージエリアの上部で、選択をクリックします。
3. ストレージの選択ダイアログボックスで、データベースを選択します。
4. OK をクリックします。
5. [記録アクション]ダイアログボックスで、既存のアーカイブされていない録画を削除して新しいストレージに移動するか、削除するかを選択します。
6. OK をクリックします。

ストレージおよび録画設定プロパティ

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。

ストレージおよび録画設定ダイアログボックスで、次の項目を指定します。

名前	説明
名前	必要に応じて、ストレージ名を変更します。名前は一意でなければなりません。
パス	このストレージで記録を保存するディレクトリへのパスを指定します。ストレージは、必ずしもレコーディングサーバーのコンピュータに存在する必要はありません。 ディレクトリが存在しない場合は作成できます。ネットワークドライブは、必ずUNC(汎用名前付け規則)のフォーマットを使用して指定する必要があります。例：*\\server\volume\directory*。
保存期間	アーカイブ設定に応じて、削除または次のアーカイブに移動するまでに記録がアーカイブに格納される期間を指定します。 保持期間は、前のアーカイブまたはデフォルトの録画データベースの保持期間より必ず長くなるようにしてください。アーカイブに対して指定される保持日数には、プロセスで以前に指定されたすべての保持期間が含まれるためです。
最大サイズ	記録データベースに保存する記録データの最大ギガバイト数を選択します。 指定されたギガバイト数を超える記録データは、指定された場合、自動的にリストの最初のアーカイブに移動されるか、削除されます。 空き容量が5GB未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます(または、次のアーカイブが定義されていない場合は削除されます)。空き容量が1GB未満になった場合は、データは削除されます。データベースには、必ず250MBの空き容量が必要です。この制限に達した場合(データが十分速やかに削除されていない場合)、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より5GB少なくなります。
電子署	記録への電子署名を有効にします。これはたとえば、再生時に、エクスポートされたビデオが修正や改変されていなかったことをシステムが確認することを意味します。

名前	説明
名中	システムはデジタル署名にSHA-2アルゴリズムを使用します。
暗号化	記録の暗号化レベルを選びます。 • 無し • 弱(CPU使用少) • 強(CPU使用大) システムは暗号化にAES-256アルゴリズムを使用します。 弱を選択する場合、録画の一部が暗号化されます。強を選択する場合、録画の全部が暗号化されます。 暗号化を有効にする選択をした場合、以下のパスワードも指定しなければなりません。
パスワード	暗号化されたデータの閲覧を許可されるユーザー用パスワードを入力します。 Milestoneは、強いパスワードを使用することを推奨しています。強いパスワードは、辞書で調べられる単語やユーザーの名前の一部は含みません。8文字以上の英数字、大文字および小文字、ならびに特殊文字を含みます。

アーカイブ設定のプロパティ

アーカイブ設定ダイアログボックスで、次の項目を指定します。

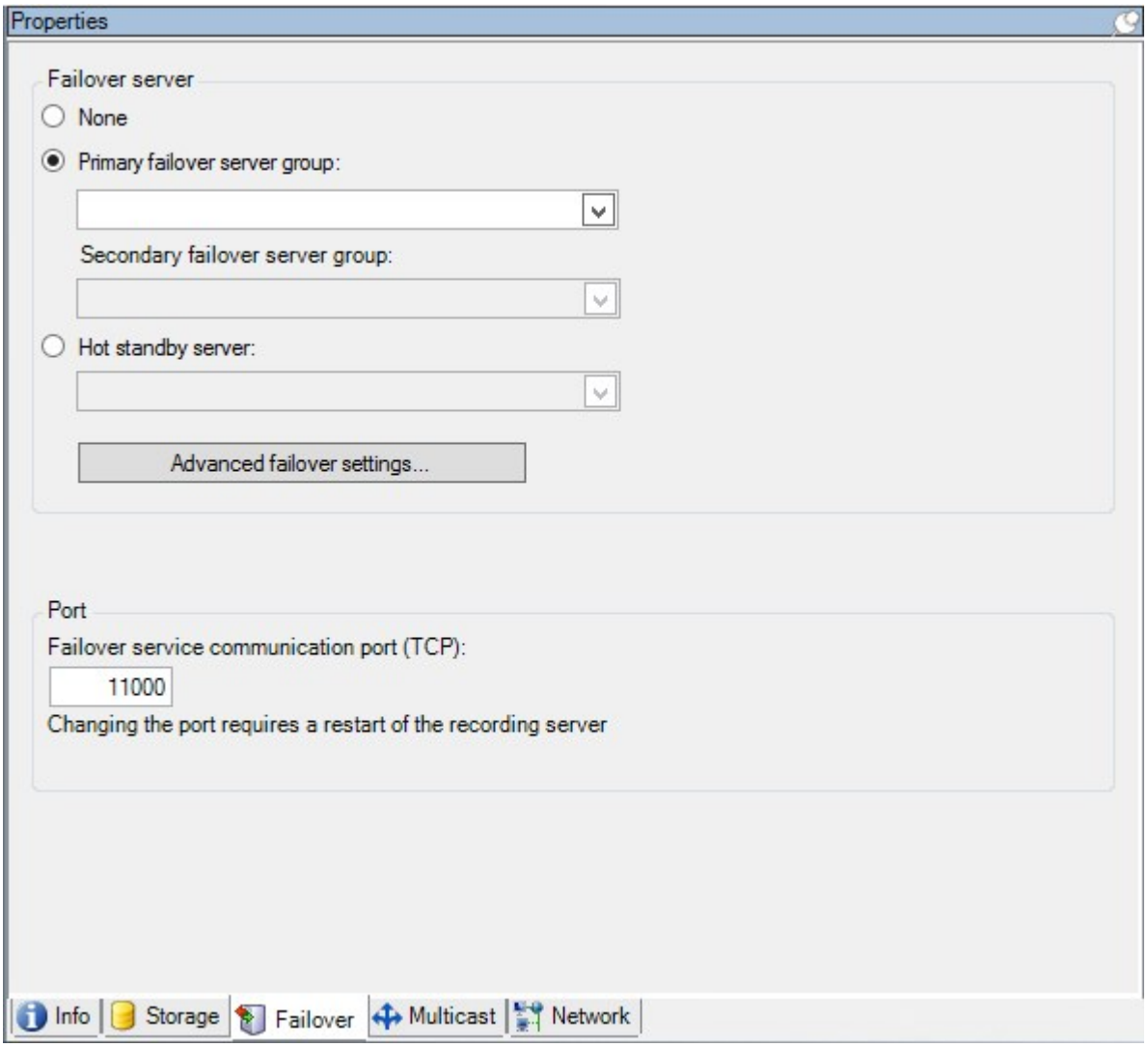
名前	説明
名前	必要に応じて、ストレージ名を変更します。名前は一意でなければなりません。
パス	このストレージで記録を保存するディレクトリへのパスを指定します。ストレージは、必ずしもレコーディングサーバーのコンピュータに存在する必要はありません。 ディレクトリが存在しない場合は作成できます。ネットワークドライブは、必ずUNC(汎用名前付け規則)のフォーマットを使用して指定する必要があります。例：*server**volume**directory*\。
保存期間	アーカイブ設定に応じて、削除または次のアーカイブに移動するまでに、記録がアーカイブに格納される期間を指定します。

名前	説明
	保持期間は、前のアーカイブまたはデフォルトの録画データベースの保持期間より必ず長くなるようにしてください。アーカイブに対して指定される保持日数には、プロセスで以前に指定されたすべての保持期間が含まれるためです。
最大サイズ	記録データベースに保存する記録データの最大ギガバイト数を選択します。 指定されたギガバイト数を超える記録データは、指定された場合、自動的にリストの最初のアーカイブに移動されるか、削除されます。 空き容量が5GB未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます(または、次のアーカイブが定義されていない場合は削除されます)。空き容量が1GB未満になった場合は、データは削除されます。データベースには、必ず250MBの空き容量が必要です。この制限に達した場合(データが十分速やかに削除されていない場合)、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より5GB少なくなります。
スケジュール	アーカイブプロセスが開始する間隔を示すアーカイブスケジュールを指定します。アーカイブは非常に高い頻度(原則として、1年中にわたって毎時毎にアーカイブ)、あるいは非常に低い頻度(たとえば、36か月ごとに一度、月初の月曜日にアーカイブ)で行うことができます。
フレームレートの低減	フレームレートの低減チェックボックスを選択し、アーカイブの際に秒当たりのフレーム数(FPS)を低減できるように、FPSを設定します。 選択した数のFPSでフレームレートを低減すると、アーカイブで記録が占める容量を低減できます。ただし、アーカイブ品質も低下します。MPEG-4/H.264/H.265は、最小限として自動的にキーフレームに低減されます。 0.1 = 1フレーム/10秒

フェールオーバータブ(レコーディングサーバー)

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。

フェールオーバーレコーディングサーバーを使用する場合、フェールオーバータブを使用して、フェールオーバーサーバーをレコーディングサーバーに割り当てます。フェールオーバータブのプロパティを参照してください。



フェールオーバーレコーディングサーバー、インストールと設定、フェールオーバーグループ、およびその設定の詳細については、ページ172のフェールオーバーレコーディングサーバー(説明付き)を参照してください。

フェールオーバーレコーディングサーバーの割り当て

レコーディングサーバーのフェールオーバータブでは、3種類のフェールオーバー設定の中から選択できます。

- フェールオーバー設定なし
- プライマリ/セカンダリフェールオーバー設定
- ホットスタンバイ設定

bおよび**c**を選択する場合、特定のサーバーまたはグループを選択する必要があります。**b**では、セカンダリフェールオーバーグループも選択できます。レコーディングサーバーが使用できなくなった場合、プライマリフェールオーバーグループのフェールオーバーレコーディングサーバーに切り替わります。セカンダリフェールオーバーグループも選択している場合、プライマリフェールオーバーグループのフェールオーバーレコーディングサーバーがすべてビジーである場合には、セカンダリグループのフェールオーバーレコーディングサーバーに切り替わります。このようにして、フェールオーバーソリューションが機能しないリスクは、プライマリのすべてのフェールオーバーレコーディングサーバーだけなくセカンダリフェールオーバーグループもビジーである場合だけになります。

1. [サイトナビゲーション]ペインで、[サーバー]>[レコーディングサーバー]を選択します。レコーディングサーバーのリストが表示されます。
2. 概要ペインで、必要なレコーディングサーバーを選択し、フェールオーバータブに移動します。
3. フェールオーバーセットアップのタイプを選択するには、以下から選びます：
   - 無し
   - プライマリフェールオーバーサーバーグループ / セカンダリフェールオーバーサーバーグループ
   - ホットスタンバイサーバー

   同じフェールオーバーグループをプライマリとセカンダリフェールオーバーグループとして選択したり、既にフェールオーバーグループに含まれている標準のフェールオーバーサーバーをホットスタンバイサーバーとして選択することはできません。
4. 次に、詳細フェールオーバー設定をクリックします。これで、フェールオーバー詳細設定ウィンドウが開き、選択したレコーディングサーバーに接続するすべてのデバイスのリストが表示されます。無しを選択した場合でも、フェールオーバー詳細設定を使用できます。選択項目はすべて保持され、後からフェールオーバー設定で使用できます。
5. フェールオーバーサポートのレベルを指定するには、リストの各デバイスでフルサポート、ライブ専用、無効のいずれかを選択します。**OK** をクリックします。
6. 必要に応じて、フェールオーバーサービス通信ポート**(TCP)** フィールドでポート番号を編集します。

もしフェールオーバーサポートを有効化し、レコーディングストレージが利用可能でない場合はレコーディングサーバーが実行され続けるように設定した場合、フェールオーバーレコーディングサーバーはテイクオーバーしません。フェールオーバーサポートワークをするには、レコーディングストレージが利用可能でない場合はレコーディングサーバーを止めるオプションを、ストレージタブで選択します。

フェールオーバータブのプロパティ

名前	説明
無し	フェールオーバー レコーディング サーバーなしで設定を選択します。

名前	説明
プライマリフェールオーバーサーバーグループ / セカンダリフェールオーバーサーバーグループ	1つのプライマリフェールオーバーサーバーグループと任意で1つのセカンダリフェールオーバーサーバーグループから成る通常のフェールオーバー設定を選択します。
ホットスタンバイサーバー	ホットスタンバイサーバーとして1つの専用レコーディングサーバーを用意し、ホットスタンバイ設定を選択します。
フェールオーバー詳細設定	[フェールオーバー詳細設定]ウィンドウを開きます。 • フルサポート: デバイスのフェールオーバーサポートを完全に有効にする • ライブ専用: デバイス上のライブストリームのフェールオーバーサポートのみを有効にする • 無効: デバイスのフェールオーバーサポートを無効にする
フェールオーバーサービス通信ポート(TCP)	デフォルトのポート番号は11000です。このポートがレコーディングサーバーとフェールオーバーレコーディングサーバー間での通信で使用されます。ポートを変更した場合、レコーディングサーバーが実行中でなければならず、また、その間マネジメントサーバーに接続されていなければなりません。

マルチキャストタブ(レコーディングサーバー)

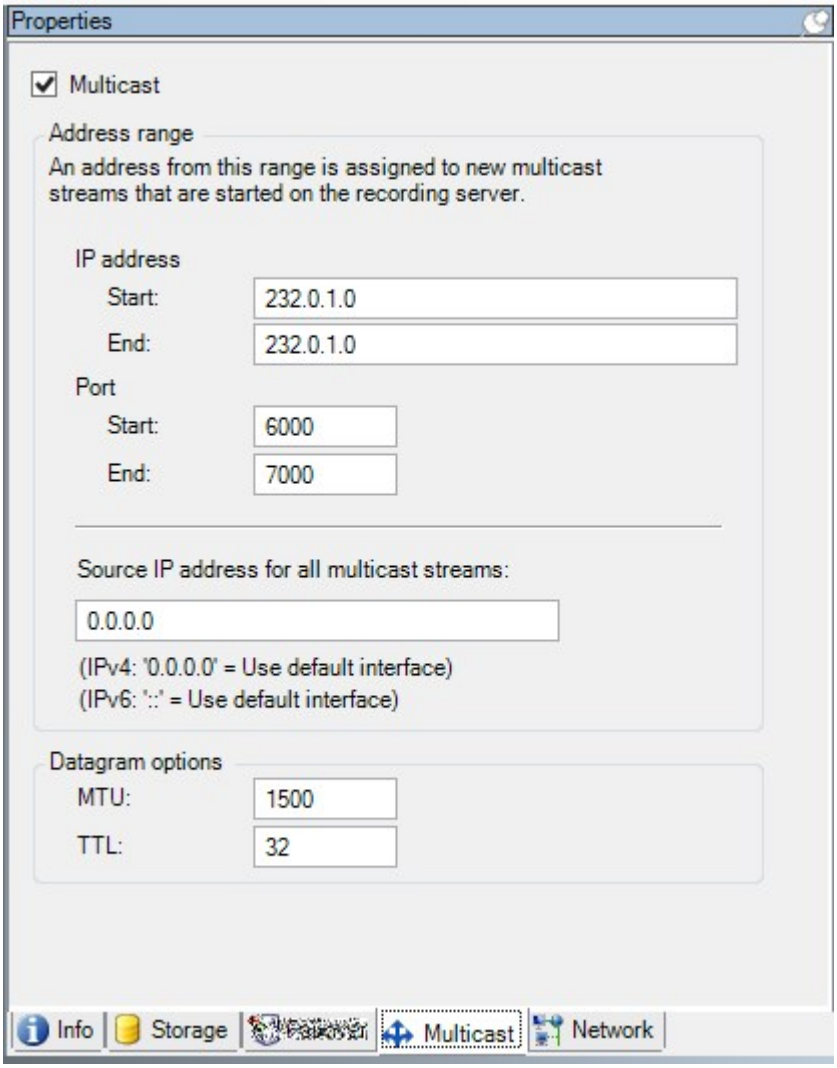
システムでは、レコーディングサーバーからのライブストリームのマルチキャストをサポートしています。多数のXProtect Smart Clientユーザーが同じカメラからのライブビデオを再生しようとする場合に、マルチキャストによってシステムリソースの消費量を大幅に低減できます。マルチキャストは、複数のクライアントが同じカメラからのライブビデオを頻繁に要求し、Matrix機能を使用する場合に特に便利です。

マルチキャストは、記録されたビデオ/音声ではなく、ライブストリームでのみ可能です。

> レコーディングサーバーに複数のネットワークインターフェースカードがある場合、マルチキャストはその中の1つのカードでだけ可能です。どのネットワークインターフェースカードを使用するか、Management Clientによって指定できます。

フェールオーバーサーバーを使用している場合は、フェールオーバーサーバー上のネットワークインタフェースカードのIPアドレスも指定します(ページ178のマルチキャストタブ(フェールオーバーサーバー)を参照) 。

マルチキャストを正しく実装するには、ネットワーク装置がマルチキャストのデータパケットを必要な受信者のグループだけに配信されるように設定されていることも必要です。そうでないと、マルチキャストはブロードキャストと変わらなくなり、ネットワーク通信速度が大幅に低下します。



マルチキャスト(説明付き)

通常のネットワーク通信で、各データパケットは単一の送信者から単一の受信者に送信され、ユニキャストと呼ばれます。一方、マルチキャストでは、単一のデータパケット(サーバーから)をグループ内の複数の受信者(クライアント)に送信できます。したがって、マルチキャストは帯域幅を節約できます。

- ユニキャストを使用する場合、発信元は必ずそれぞれの受信者に1つのデータストリームを転送しなければなりません。
- マルチキャストを使用する場合は、それぞれのネットワークセグメントで単一のデータストリームしか必要ではありません。

ここで説明しているマルチキャストは、カメラからサーバーへのビデオのストリーミングではありません。サーバーからクライアントへのストリーミングになります。

マルチキャストでは、IPアドレス範囲、各カメラにマルチキャストを有効化/無効化できる能力、最大許容データパケットサイズ(MTU)を定義する機能、データパケットを転送するための最大ルーター数(TTL)などのオプションを基に定義された受信者のグループを使用します。

> レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。

マルチキャストを、関連のないデータでもネットワークに接続している全員にデータを送信する、ブロードキャストと混合しないよう注意する必要があります。

名前	説明
ユニキャスト	単一のソースから単一の受信者へデータを送信します。
マルチキャスト	単一のソースから明確に定義されたグループ内の複数の受信者へデータを送信します。
ブロードキャスト	単一のソースからネットワーク上の全員へデータを送信します。このため、ブロードキャストによって、ネットワーク通信速度が大幅に低下する可能性があります。

レコーディングサーバーのマルチキャストを有効にする

マルチキャストを使用するには、ネットワークのインフラがIPマルチキャスト標準IGMP(インターネットグループ管理プロトコル)をサポートしている必要があります。

- [マルチキャスト]タブで、[マルチキャスト]チェックボックスを選択します。

マルチキャスト用のIPアドレス範囲の全体が既に1つまたは複数のレコーディングサーバーによって使用されている場合は、まずマルチキャスト用のIPアドレスを空けないと、それ以上のレコーディングサーバーでマルチキャストを有効にすることはできません。

レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。

IPアドレス範囲の割り当て

選択したレコーディングサーバーからのマルチキャストストリームにアドレスを割り当てる範囲を指定します。クライアントは、対象となるレコーディングサーバーからのマルチキャストビデオを再生する時に、これらのアドレスに接続します。

マルチキャストカメラフィードのそれぞれについて、IPアドレスとポートの組み合わせは一意でなければなりません。(IPv4の例：232.0.1.0:6000).1つのIPアドレスと複数のポートを、あるいは複数のIPアドレスと少数のポートを使用することができます。デフォルトでは、システムは単一のIPアドレスと1000のポートの範囲を使用するよう推奨しますが、必要であれば変更できます。

マルチキャストのIPアドレスは、IANAによるダイナミックホスト割り当てで定義された範囲内でなければなりません。IANAはグローバルIPアドレス割り当てを監視する機関です。

名前	説明
IPアドレス	開始フィールドで、必要な範囲の最初のIPアドレスを指定します。次に、範囲で最後のIPアドレスを終了フィールドで指定します。
ポート	開始フィールドで、必要な範囲で最初のポート番号を指定します。次に、範囲で最後のポート番号を終了フィールドで指定します。
すべてのマルチキャストストリームの送信元IPアドレス	マルチキャストは1つのネットワークインターフェースカードでだけできるため、レコーディングサーバーに複数のネットワークインターフェイスカードがあるか、複数のIPアドレスのネットワークインターフェイスカードが1つある場合に、このフィールドを使用します。 レコーディングサーバーのデフォルトのインターフェースを使用する場合は、フィールドの値を0.0.0.0 (IPv4の場合) または :: (IPv6の場合) のままにします。他のネットワークインターフェースカードを使用する場合、または同じネットワークインターフェースカードで別のIPアドレスを使用する場合、必要なインターフェースのIPアドレスを指定します。 • IPv4: 224.0.0.0 ～ 239.255.255.255. • IPv6、範囲については、IANA Webサイト(https://www.iana.org/) を参照してください。

データグラムオプションの指定

マルチキャストで転送するデータパケット(データグラム) の設定を指定します。

名前	説明
MTU	最大転送ユニット、許容される物理的データパケットの最大サイズです(単位はバイト) 。指定されたMTUより大きいメッセージは、送信する前に小さいパケットに分割されます。デフォルト値は1500バイトです。これは大半のWindowsコンピュータやイーサネットネットワークでのデフォルトでもあります。
TTL	生存時間、廃棄または返却されるまでに、データパケットが移動できるホップの最大数です。ホップとは、2つのネットワークデバイス(通常はルーター) の間のポイントのことです。デフォルト値は128です。

個々のカメラに対してマルチキャストを有効にする

関連するカメラでこれを有効にした場合にのみ、マルチキャストは動作します。

1. レコーディングサーバーを選択して、概要ペインで必要なカメラを選択します。
2. クライアントタブで、ライブマルチキャストチェックボックスを選択します。関連するすべてのカメラに対して繰り返します。

> レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。

ネットワークタブ(レコーディングサーバー)

レコーディングサーバーのパブリックIPアドレスはネットワークタブで定義します。

パブリックアドレスを使用する理由

XProtect Smart Clientなどのアクセス用クライアントが監視システムに接続する場合、連絡用アドレスの交換を含めて、一定量の初期データ通信がバックグラウンドで共有されます。これは自動的に行われ、ユーザーには全く認識されません。

クライアントはローカルネットワークに加えてインターネットから接続することもあります。いずれの場合にも、レコーディングサーバーからのライブビデオや録画済みビデオにクライアントがアクセスできるように、監視システムが適切なアドレスを提供する必要があります。

- クライアントがローカルで接続する場合、監視システムはローカルのアドレスおよびポート番号を返さなければなりません
- クライアントがインターネットから接続する場合、監視システムはレコーディングサーバーのパブリックアドレスに応答します。これはファイアウォールまたはNAT(ネットワークアドレス変換)ルーターのアドレスであり、多くの場合、異なるポート番号です。アドレスおよびポートは、サーバーのローカルアドレスおよびポートに転送できます。

  NAT(ネットワークアドレス変換)ファイアウォールの外側から監視システムにアクセスするには、パブリックアドレスとポート転送を使用します。これによって、ファイアウォールの外側にあるクライアントは、VPN(仮想プライベートネットワーク)を使用することなく、レコーディングサーバーへ接続できます。それぞれのレコーディングサーバーを特定のポートにマップし、ファイアウォールを通じて、このポートをサーバーの内部アドレスへ転送することができます。

パブリックアドレスとポートの定義

1. パブリックアクセスを有効にするには、パブリックアクセスを有効にするチェックボックスを選択します。
2. レコーディングサーバーのパブリックアドレスを定義します。ファイアウォールまたはNATルーターのアドレスを入力し、インターネットから監視システムにアクセスするクライアントがレコーディングサーバーに接続できるようにします。
3. パブリックポート番号を指定します。ファイアウォールまたはNATルーターで使用するポート番号を、ローカルで使用するポート番号と異なる番号にしておくことをお勧めします。

> パブリックアクセスを使用する場合、使用するファイアウォールまたはNATルーターを設定し、パブリックなアドレスおよびポートに送信されるリクエストが、関連するレコーディングサーバーのローカルなアドレスおよびポートに転送されるようにしてください。

ローカルIP範囲の割り当て

監視システムがローカルネットワークからの通信であると認識できるローカルIP範囲のリストを定義します。

- [ネットワーク]タブで、[設定]をクリックします。

サイトナビゲーション：サーバーとハードウェア：フェールオーバーサーバー

フェールオーバーレコーディングサーバー(説明付き)

> 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。

フェールオーバーレコーディングサーバーは、予備のレコーディングサーバーで、通常のレコーディングサーバーが使用できなくなったときに使用されます。フェールオーバーレコーディングサーバーは、コールドスタンバイサーバーとして、またはホットスタンバイサーバーとして、2つの方法で構成できます。

フェールオーバーレコーディングサーバーを標準レコーディングサーバーのようにインストールします(ページ88の新しいXProtectコンポーネントのインストールを参照) 。フェールオーバーレコーディングサーバーがインストールされると、Management Clientで表示されるようになります。Milestoneはすべてのフェールオーバーレコーディングサーバーを個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。フェールオーバーレコーディングサーバーが、マネジメントサーバーの正しいIPアドレス/ホスト名を用いて構成されていることを確認します。フェールオーバーサーバーサービスが実行されているユーザーアカウントのユーザー権限は、インストールプロセス中に付与されます。すなわち:

- フェールオーバーレコーディングサーバーを開始または停止するための開始/停止許可
- RecorderConfig.xmlファイルを読み取る/書き込むための読み取りおよび書き込みアクセス許可

暗号化に対して証明書が選択されている場合、管理者は選択した証明書プライベートキーにおいて、フェールオーバーユーザーに読み取りアクセス許可を付与する必要があります。

> Milestoneでは、フェールオーバーレコーディングサーバーが暗号化を使用しているレコーディングサーバーを引き継ぐ際、フェールオーバーレコーディングサーバーも暗号化を使用するよう準備する必要があります。詳細については、ページ58のインストールを開始する前におよびページ88の新しいXProtectコンポーネントのインストールを参照してください。

デバイスレベルで必要なフェールオーバーサポートのタイプを指定できます。レコーディングサーバー上の各デバイスで、フル、ライブのみ、フェールオーバーサポートなしを選択できます。これにより、フェールオーバーリソースに優先順位を付けることができます。例えば、ビデオのフェールオーバーのみを設定し、音声には設定しないことも可能です。また、重要性の低いカメラにはフェールオーバーせず、重要なカメラのみをフェールオーバーの対象にできます。

> システムがフェールオーバーモードの間は、ハードウェアの置き換えや削除、レコーディングサーバーの更新、ストレージ設定やビデオストリーム設定のようなデバイスの設定を行うことはできません。

コールドスタンバイ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フェールオーバーレコーディングサーバーの設定では、1つのフェールオーバーグループに複数のフェールオーバーレコーディングサーバーを集めます。複数の事前に選択されたレコーディングサーバーのいずれかが使用できなくなった場合に、フェールオーバーグループ全体が代わりに対応します。グループは希望する数だけ作成できます(コールドスタンバイ用にフェールオーバーレコーディングサーバーをグループ化を参照) 。

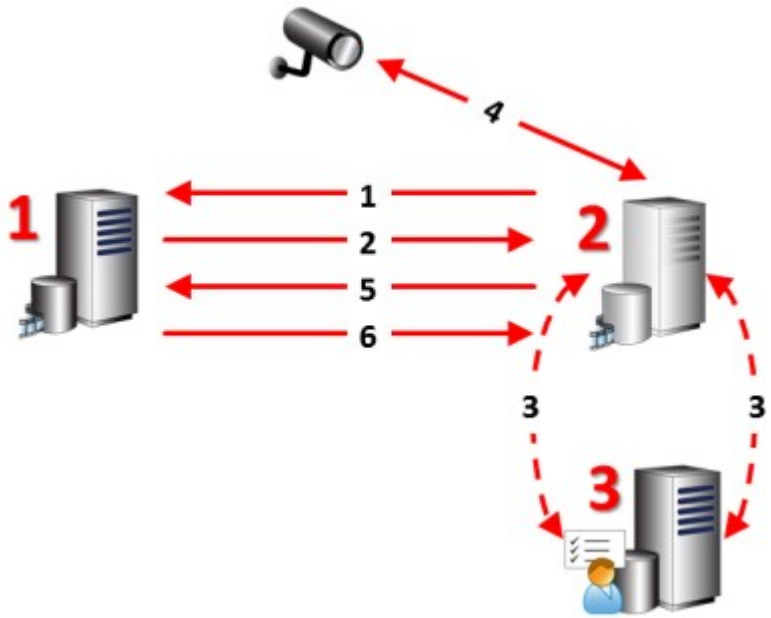
グループ化には明確なメリットがあります。レコーディングサーバーに取って代わるフェールオーバーレコーディングサーバーを後から指定する場合は、フェールオーバーレコーディングサーバーのグループを選択します。選択したグループに複数のフェールオーバーレコーディングサーバーがある場合、レコーディングサーバーを使用できなくなっても引き継ぎの準備ができているフェールオーバーレコーディングサーバーが1台以上あるため、安全です。プライマリグループのすべてのレコーディングサーバーが応答しない場合は、プライマリグループにとって代わるフェールオーバーサーバーのセカンダリグループを特定できます。1つのフェールオーバーレコーディングサーバーは、一度に1つのグループにのみ属することができます。

フェールオーバーグループのフェールオーバーレコーディングサーバーには順序があります。この順序に従い、フェールオーバーレコーディングサーバーが、レコーディングサーバーに取って代わる順序が決定されます。デフォルトでは、フェールオーバーグループでフェールオーバーレコーディングサーバーを統合した順序が反映されます。必要に応じて、この順序は変更できます。

ホットスタンバイフェールオーバーレコーディングサーバー

ホットスタンバイフェールオーバーレコーディングサーバー設定では、1つのフェールオーバー レコーディング サーバーを、1つのレコーディングサーバーにのみ取って代わるようにできます。このため、システムはこのフェールオーバー レコーディング サーバーを「スタンバイ」モードのままにできます。つまり、レコーディングサーバーの現在の正しい構成を使用して既に起動されており、専用であるため、コールドスタンバイフェールオーバー レコーディング サーバーよりも迅速に切り替えられます。前述の通り、ホットスタンバイサーバーは1つのレコーディングサーバーにのみ割り当てられ、グループ化できません。既にフェールオーバーグループに含まれているフェールオーバーサーバーは、ホットスタンバイレコーディングサーバーとして割り当てできません。

フェールオーバーの手順(説明付き)



説明
関連するサーバー(赤字は台数): 1. レコーディングサーバー 2. Failover Recording Server 3. マネジメントサーバー

説明
コールドスタンバイ設定のフェールオーバー手順： 1. 実行しているかどうかを確認するために、フェールオーバーレコーディングサーバーには、レコーディングサーバーへの継続的なTCP接続があります。 2. この接続は中断されます。 3. フェールオーバーレコーディングサーバーが、マネジメントサーバーから現在のレコーディングサーバーの設定を要求します。マネジメントサーバーが要求された設定を送ると、フェールオーバーレコーディングサーバーはレコーディングサーバーに代わって構成を受信して起動し、記録を開始します。 4. フェールオーバーレコーディングサーバーと関連するカメラはビデオデータを交換します。 5. フェールオーバーレコーディングサーバーは継続的にレコーディングサーバーへの接続を再確立します。 6. レコーディングサーバーへの接続が再確立されると、フェールオーバーレコーディングサーバーはシャットダウンし、レコーディングサーバーはダウンタイム中に(存在する場合)録画されたビデオデータを取得します。また、ビデオデータはレコーディングサーバーデータベースに再度統合されます。
ホットスタンバイ設定のフェールオーバー手順： 1. 実行しているかどうかを確認するために、ホットスタンバイサーバーには、割り当てられたレコーディングサーバーへの継続的なTCP接続があります。 2. この接続は中断されます。 3. ホットスタンバイサーバーは割り当てられたレコーディングサーバーの現在の構成をマネジメントサーバーから既に把握しており、独自に録画を開始します。 4. ホットスタンバイサーバーと関連するカメラはビデオデータを交換します。 5. ホットスタンバイサーバーは継続的にレコーディングサーバーへの接続を再確立します。 6. レコーディングサーバーへの接続が再確立され、ホットスタンバイサーバーがホットスタンバイモードに戻ると、フェールオーバーレコーディングサーバーはシャットダウンし、レコーディングサーバーはダウンタイム中に(存在する場合)録画されたビデオデータを取得します。また、ビデオデータはレコーディングサーバーデータベースに再度統合されます。

フェールオーバーレコーディングサーバー機能(説明付き)

- フェールオーバーレコーディングサーバーは、毎0.5秒ごとに関連するレコーディングサーバーの状態を確認します。2秒以内にレコーディングサーバーが応答しない場合、レコーディングサーバーは利用できないと見なされ、フェールオーバー レコーディングサーバーが取って代わります。

- コールドスタンバイフェールオーバーレコーディングサーバーは、使用できないレコーディングサーバーを引き継ぎます。この処理にかかる時間は、フェールオーバーレコーディングサーバーのレコーディングサーバーサービスが起動する時間と、カメラに接続する時間に、5秒間を加えた時間です。これとは対照的に、ホットスタンバイのフェールオーバーレコーディングサーバーでは、レコーディングサーバーサービスが既に正しい設定で実行中であり、フィードを配信するためにカメラに接続するだけでよいため、より迅速に切り替えられます。起動中は、該当するカメラからの録画の保存も、ライブビデオの表示もできません。
- レコーディングサーバーがもう一度使用可能になると、フェールオーバーレコーディングサーバーから自動的に引き継がれます。フェールオーバーレコーディングサーバーによって保存された録画は、自動的に標準レコーディングサーバーのデータベースに統合されます。統合にかかる時間は、録画の分量やネットワークの能力などに応じて異なります。統合プロセスの実施中、フェールオーバーレコーディングサーバーが代替していた時間中の録画を参照することはできません。
- コールドスタンバイフェールオーバーレコーディングサーバーの設定の統合処理中に、フェールオーバーレコーディングサーバーが別のレコーディングサーバーから引き継ぐ必要が生じた場合は、レコーディングサーバーAの統合処理が延期され、レコーディングサーバーBに取って代わります。レコーディングサーバーBがもう一度使用可能になると、フェールオーバーレコーディングサーバーがレコーディングサーバーAの統合処理を実行します。その後に、レコーディングサーバーBとの統合が開始します。ホットスタンバイ設定では、ホットスタンバイサーバーは1台のレコーディングサーバーに対してのみホットスタンバイ可能であるため、他のレコーディングサーバーから引き継ぐことはできません。
- ホットスタンバイ設定では、ホットスタンバイサーバーは1台のレコーディングサーバーに対してのみホットスタンバイできるため、他のレコーディングサーバーから引き継ぐことはできません。ただし、レコーディングサーバーで再度障害が発生した場合、ホットスタンバイは再度処理を引き継ぎ、前の期間からの録画も保持します。プライマリレコーダーに統合されるか、フェールオーバーレコーディングサーバーのディスク領域がなくなるまで、録画はレコーディングサーバーに保持されます。
- フェールオーバーソリューションでは、完全な冗長性が提供されません。これは、ダウンタイムを最小化するための信頼できる方法としてのみ利用できます。レコーディングサーバーがもう一度使用可能になると、フェールオーバーサーバーサービスは、レコーディングサーバーで録画を保存する準備ができていることを確認します。その場合にのみ、録画を保存する責務が標準のレコーディングサーバーに戻されます。したがって、この段階で録画が失われることはほとんどありません。
- クライアントユーザーは、フェールオーバーレコーディングサーバーへの切り替えが発生したことにほとんど気付かないはずです。フェールオーバーレコーディングサーバーが引き継ぐと、短い停止(通常は数秒)が発生します。この切断中は、該当するレコーディングサーバーからビデオにアクセスできません。クライアントユーザーは、フェールオーバーレコーディングサーバーが切り替えられるとすぐに、ライブビデオ表示を再開できます。最近の録画はフェールオーバーレコーディングサーバーに保存されるため、フェールオーバーレコーディングサーバーが引き継いだ後からも録画を再生できます。クライアントは、レコーディングサーバーが動作を再開して、フェールオーバーレコーディングサーバーから切り替えられるまで、対象のレコーディングサーバー上にのみ保存されている古い録画を再生することができません。アーカイブ済みの録画にはアクセスできません。レコーディングサーバーが動作を再開すると、フェールオーバー録画が、レコーディングサーバーのデータベースへと再統合される統合プロセスが実行されます。このプロセスの実施中、フェールオーバーレコーディングサーバーが代替していた時間中の録画を再生することはできません。

- コールドスタンバイ設定では、別のフェールオーバーレコーディングサーバーのバックアップとして、もう1つのフェールオーバーレコーディングサーバーを設定する必要はありません。特定のレコーディングサーバーを引き継ぐためにフェールオーバーグループを割り当て、特定のフェールオーバーレコーディングサーバーを割り当てないためです。フェールオーバーグループには、最低1つのフェールオーバーレコーディングサーバーを含む必要があり、いくつでもフェールオーバーレコーディングサーバーを追加できます。フェールオーバーグループに2つ以上のフェールオーバーレコーディングサーバーが含まれている場合、2つ以上のフェールオーバーレコーディングサーバーで引き継ぎが可能になります。
- ホットスタンバイ設定では、ホットスタンバイサーバーとして、フェールオーバー レコーディングサーバーまたはホットスタンバイサーバーを設定できません。

フェールオーバーレコーディングサーバーの設定と有効化

> フェールオーバーレコーディングサーバーを無効にしている場合、標準のレコーディングサーバーから切り替える前に有効にする必要があります。

次の手順を実行し、フェールオーバーレコーディングサーバーを有効にして、基本プロパティを編集します。

1. サイトナビゲーションペインで、サーバー>フェールオーバーサーバーを選択します。インストール済みのフェールオーバーレコーディングサーバーとフェールオーバーグループのリストが表示されます。
2. 概要ペインで、必要なフェールオーバーレコーディングサーバーを選択します。
3. 右クリックして、有効を選択します。フェールオーバーレコーディングサーバーが有効になりました。
4. フェールオーバーレコーディングサーバーのプロパティを編集するには、情報タブに移動します。
5. 完了すると、ネットワークタブに移動します。ここで、フェールオーバーレコーディングサーバーのパブリックIPアドレスなどを定義できます。これは、NAT(ネットワークアドレス変換)とポート転送を使用する場合に必要です。詳細については、標準のレコーディングサーバーのネットワークタブを参照してください。
6. サイトナビゲーションペインで、サーバー>レコーディングサーバーを選択します。フェールオーバーサポートを実行したいレコーディングサーバーを選択して、フェールオーバーサーバーを割り当てます(ページ164のフェールオーバータブ(レコーディングサーバー)を参照)。

フェールオーバーレコーディングサーバーのステータスを見るには、通知エリアにあるFailover Recording Server Managerトレイアイコンの上でマウスをホールドします。フェールオーバーレコーディングサーバーの説明フィールドに、入力された説明文がヒントとして表示されます。ここで、フェールオーバーレコーディングサーバーが、どのレコーディングサーバーを引き継ぐよう設定されているかを確認することができます。

> フェールオーバーレコーディングサーバーは、定期的にマネジメントサーバーに対してpingを行い、マネジメントサーバーがオンラインで、必要に応じて、標準レコーディングサーバーの構成に対して要求、応答できることを確認します。pingをブロックすると、フェールオーバーレコーディングサーバーは、標準レコーディングサーバーを代替できなくなります。

コールドスタンバイ用にフェールオーバーレコーディングサーバーをグループ化

1. サーバー>フェールオーバーサーバーを選択します。インストール済みのフェールオーバーレコーディングサーバーとフェールオーバーグループのリストが表示されます。
2. 概要ペインで最上位ノードのフェールオーバーグループを右クリックし、グループの追加を選択します。
3. 新しいグループの名前(この例では*Failover Group 1*)と説明(任意)を指定します。**OK**をクリックします。
4. 作成したグループ(*Failover Group 1*)を右クリックします。グループメンバーの編集を選択します。これによりグループメンバーの選択ウィンドウが開きます。
5. ドラッグアンドドロップするか、ボタンを使用して、左側から右側へ選択したフェールオーバーレコーディングサーバーを移動します。**[OK]** をクリックします。これで、選択したフェールオーバーレコーディングサーバーが、作成したグループ(*Failover Group 1*)に含まれます。
6. シーケンスタブに移動します。上と下をクリックし、グループの通常フェールオーバーレコーディングサーバーの内部シーケンスを設定します。

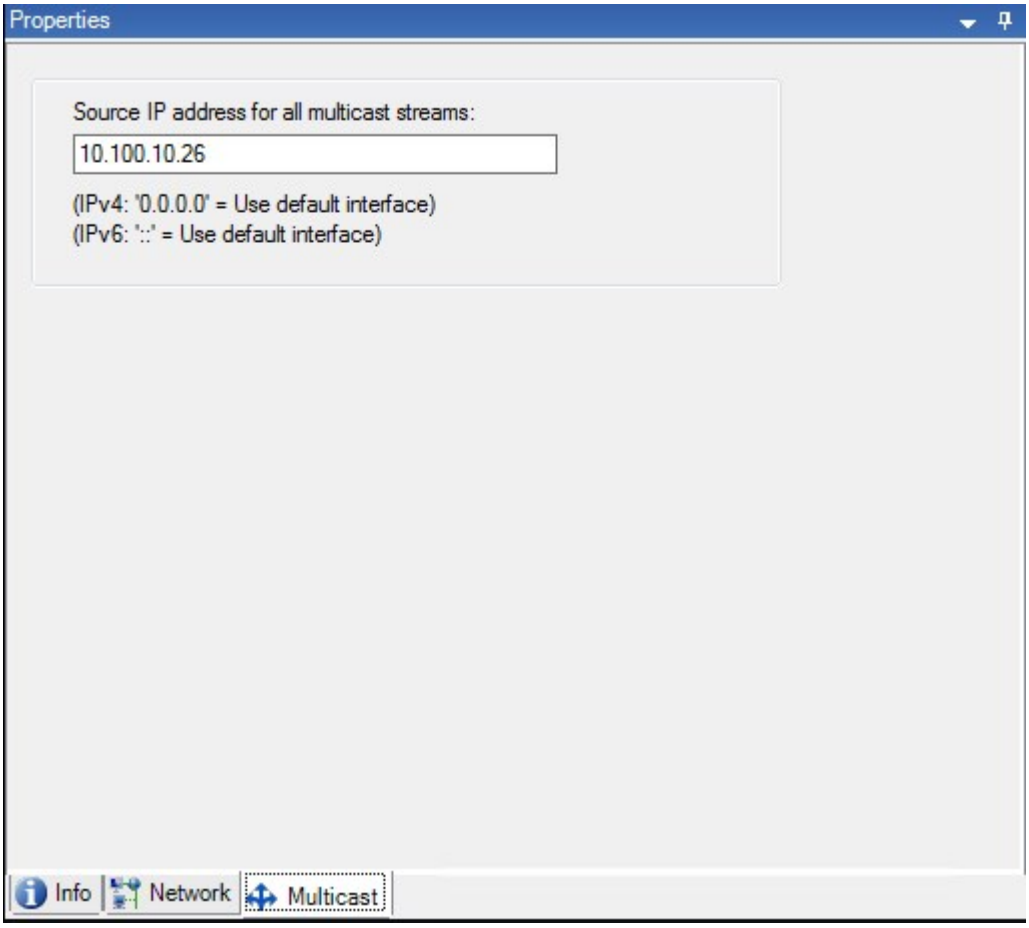
レコーディングサーバーのステータスアイコンの読み方

以下のアイコンは、フェールオーバーレコーディングサーバーのステータスを示します(アイコンは、概要ペインに表示されます)。

アイコン	説明
	フェールオーバーレコーディングサーバーが待機中または「監視中」です。待機中の場合、フェールオーバーレコーディングサーバーは他のレコーディングサーバーを引き継ぐようまだ設定されていません。「監視中」の場合は、フェールオーバーレコーディングサーバーは、1つ以上のレコーディングサーバーを監視するよう設定されています。
	フェールオーバーレコーディングサーバーは、指定されたレコーディングサーバーを引き継ぎました。サーバーアイコンの上にカーソルを置くと、ヒントが表示されます。このヒントを使用して、フェールオーバーレコーディングサーバーがどのレコーディングサーバーを引き継いだかを確認できます。
	フェールオーバーレコーディングサーバーへの接続が切断されています。

マルチキャストタブ(フェールオーバーサーバー)

フェールオーバーサーバーを使用している場合は、マルチキャストのライブストリームを有効にし、レコーディングサーバーとフェールオーバーサーバーの両方で使用しているネットワークインターフェースカードのIPアドレスを特定する必要があります。



マルチキャストの詳細については、ページ167のマルチキャストタブ(レコーディングサーバー) または ページ167のマルチキャストタブ(レコーディングサーバー) を参照してください。

情報タブのプロパティ(フェールオーバーサーバー)

次のフェールオーバーレコーディングサーバーのプロパティを指定します。

名前	説明
名前	Management Client、ログなどに表示されるフェールオーバーレコーディングサーバーの名前。
説明	引き継がれるレコーディングサーバーなど、フェールオーバーレコーディングサーバーを説明するために使用できるオプションのフィールド。

名前	説明
ホスト名	フェールオーバーレコーディングサーバーのホスト名を表示します。これは変更できません。
ローカルWebサーバーアドレス	フェールオーバーレコーディングサーバーのWebサーバーローカルアドレスを表示します。例えば、PTZカメラコントロールコマンドを使用したり、XProtect Smart Clientからのライブリクエストを閲覧する際には、ローカルアドレスを使用します。 Webサーバーコミュニケーションに使われているポート番号を含むアドレス(標準ポート7563)。 フェールオーバーレコーディングサーバーが暗号化しているレコーディングサーバーを引き継ぐときは、フェールオーバーレコーディングサーバーも暗号化の準備をする必要があります。 暗号化を有効にすると、パッドロックアイコンとhttpの代わりにhttpsを含むアドレスが表示されます。
Webサーバーアドレス	インターネット上のフェールオーバーレコーディングサーバーのWebサーバーパブリックアドレスを表示します。 インストールでファイアウォールまたはNATルーターを使用する際は、ファイアウォールまたはNATルーターのアドレスを入力すると、インターネット上で監視システムにアクセスできるクライアントが、フェールオーバーレコーディングサーバーには接続できません。 パブリックアドレスとネットワークタブ上でポート番号を指定します。 暗号化を有効にすると、パッドロックアイコンとhttpの代わりにhttpsを含むアドレスが表示されます。
UDPポート	フェールオーバーレコーディングサーバー間での通信に使用されるポート番号。デフォルトポートは8844です。
データベースの場所	録画の保存用にフェールオーバーレコーディングサーバーで使用されるデータベースへのパスを指定します。 データベースパスは、フェールオーバーレコーディングサーバーがレコーディングサーバーに代替している間には変更できません。ユーザーが行う変更は、フェールオーバーレコーディングサーバーがレコーディングサーバーの代替サーバーではなくなったときに適用されます。
このフェールオーバーサーバーを有効にする	クリアすると、フェールオーバーレコーディングサーバーが無効になります(デフォルトで選択されています)。レコーディングサーバーを切り替える前に、フェールオーバーレコーディングサーバーを無効にする必要があります。

情報タブの機能(フェールオーバーグループ)

フィールド	説明
名前	Management Client、ログなどに表示されるフェールオーバーグループの名前。
説明	説明(任意)。たとえば、サーバーの物理的な場所。

シーケンスタブのプロパティ(フェールオーバーグループ)

フィールド	説明
フェールオーバーシーケンスの指定	上と下をクリックし、グループの通常のフェールオーバーレコーディングサーバーの目的のシーケンスを設定します。

フェールオーバーレコーディングサーバーのサービス(説明付き)

フェールオーバーレコーディングサーバーには、次の2つのサービスがインストールされます。

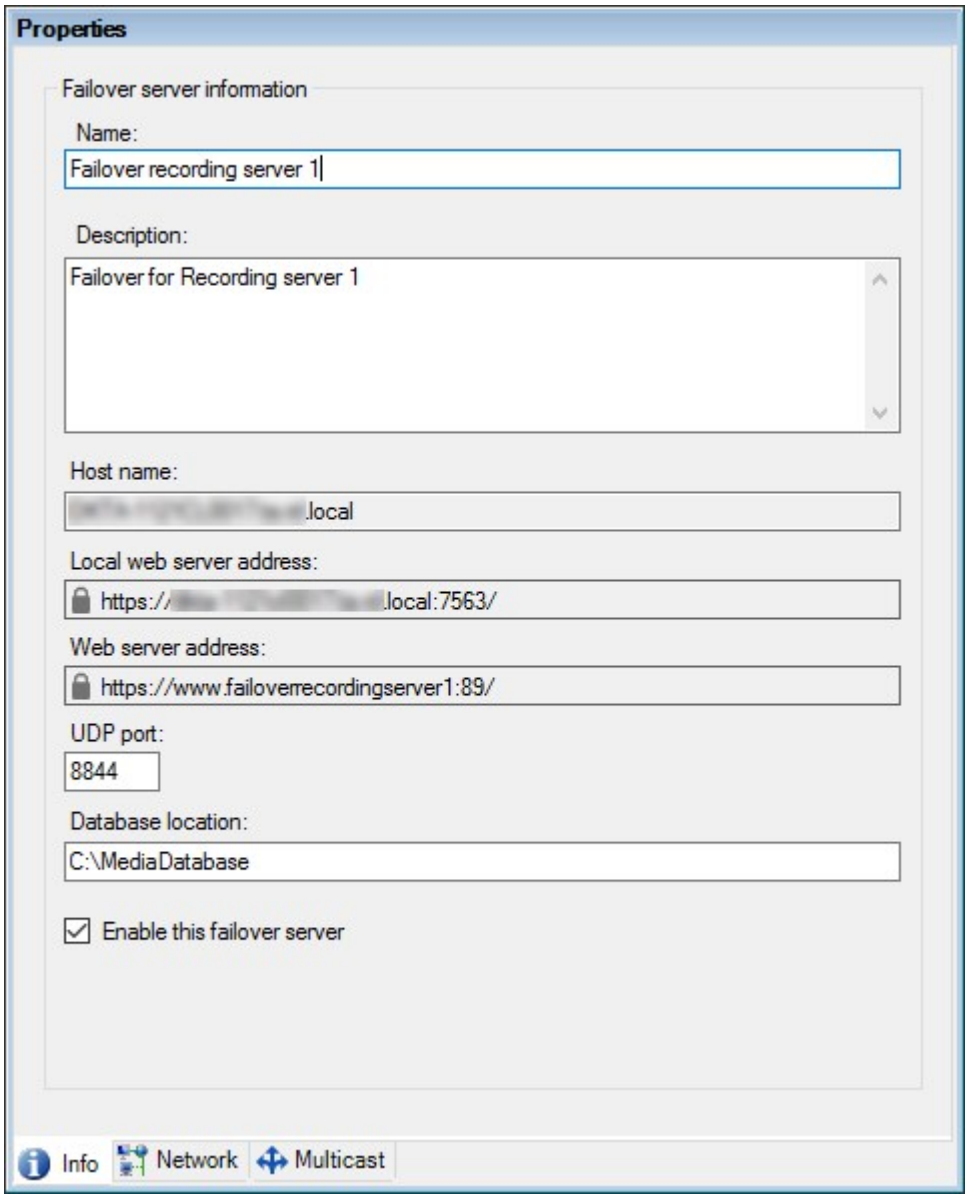
- フェールオーバーサーバーサービスは、レコーディングサーバーが使用できなくなった場合に処理を引き継ぎます。このサービスは絶えず関連するレコーディングサーバーの状態をチェックしているため、常に実行されています。
- Failover Recording Serverサービスは、レコーディングサーバーの役割を果たすようフェールオーバーレコーディングサーバーを有効にします。

  コールドスタンバイ設定では、このサービスは、レコーディングサーバーからコールドスタンバイフェールオーバーレコーディングサーバーに切り替える際など、必要なときにのみ開始されます。このサービスの開始には通常数秒かかりますが、ローカルのセキュリティ設定などに応じてそれよりも長くかかる場合もあります。ホットスタンバイ設定では、このサービスは常に実行されるため、ホットスタンバイサーバーは通常のフェールオーバーレコーディングサーバーがよりも迅速に切り替えることができます。

フェールオーバーレコーディングサーバーで暗号化ステータスを表示

フェールオーバーレコーディングサーバーを暗号化する時は、以下を確認します。

1. サイトナビゲーションペインで、サーバー>フェールオーバーサーバーを選択します。これでフェールオーバーレコーディングサーバーのリストが開きます。
2. 概要パネルで関連するレコーディングサーバーを選択し、情報タブに移動します。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クライアントとサーバーで暗号化が有効になっている場合は、ローカルWebサーバーアドレスとオプションのWebサーバーアドレスの前にパッドロックアイコンが現れます。



ステータスメッセージの表示

1. フェールオーバーレコーディングサーバーで、**Milestone Failover Recording Server**サービスアイコンを右クリックします。
2. ステータスメッセージの表示を選択します。フェールオーバーサーバーステータスメッセージウィンドウが表示され、タイムスタンプ付きのステータスメッセージが一覧表示されます。

バージョン情報の表示

製品サポートに連絡する必要がある場合、**Failover Recording Server**サービスの正確なバージョンを知っていると便利です。

1. フェールオーバーレコーディングサーバーで、**Milestone Failover Recording Server**サービスアイコンを右クリックします。
2. バージョン情報を選択します。
3. 小さいダイアログが開き、**Failover Recording Server**サービスの正確なバージョンが表示されます。

サイトナビゲーション：サーバーとハードウェア：ハードウェア

ハードウェア(説明付き)

ハードウェアは次のいずれかを表します。

- IP経由で監視システムのレコーディングサーバーに直接接続する物理ユニット(カメラ、ビデオエンコーダー、I/Oモジュールなど)。
- Milestone Interconnect設定のリモートサイトのレコーディングサーバー。

システムへのハードウェアの追加方法については、ページ183のハードウェアの追加を参照してください。

ハードウェアの追加

システム内の各レコーディングサーバーに対して、ハードウェアを追加するための複数のオプションがあります。

> ハードウェアがNAT対応ルーターまたはファイアウォールの背後にある場合、別のポート番号を指定し、ルーター/ファイアウォールを構成して、ハードウェアのポートとIPアドレスにマッピングされるようにしなければならない場合があります。

ハードウェアの追加ウィザードを使用して、ネットワーク上でカメラおよびビデオエンコーダーなどのハードウェアを検知し、システムのレコーディングサーバーに追加します。ウィザードでは、Milestone Interconnect設定のリモートレコーディングサーバーも追加できます。ハードウェアは、一度に1つのレコーディングサーバーにのみ追加してください。

1. ハードウェアの追加にアクセスするには、必要なレコーディングサーバーを右クリックし、ハードウェアの追加を選択します。
2. ウィザードオプション(以下を参照)のいずれかを選択し、画面の手順に従います。
3. インストール後、[概要]ペインにハードウェアとデバイスが表示されます。

> 初めてハードウェアを追加する際は、特定のハードウェアを事前に設定する必要があります。このようなハードウェアを追加すると、[ハードウェアデバイスの事前設定]ウィザードが現れます。詳細については、ページ185のハードウェアの事前設定(説明付き)を参照してください。

名前	説明
高速(推奨)	レコーディングサーバーのローカルネットワークで、新しいハードウェアがシステムにより自動的にスキャンされます。 他のレコーディングサーバーで実行中のハードウェアを表示チェックボックスを選択すると、検出したハードウェアが他のレコーディングサーバーで実行中であるかどうかを確認できます。 新しいハードウェアをネットワークに追加し、システムで使用するたびに、このオプションを選択できます。 このオプションを使用して、Milestone Interconnectセットアップでリモートシステムを追加することはできません。 HTTPとHTTPSハードウェアを追加するには、ラジオボタン[HTTPS(セキュア)]を選択した状態で高速検出を実行し、その後、[HTTP(セキュアでない)]を選択した状態で検出を実行してください。
アドレス範囲スキャン	ネットワーク上の関連するハードウェアとMilestone Interconnectリモートシステムがスキャンされます。 • これは、指定されたハードウェアのユーザー名とパスワードに従って実行されます。ハードウェアで出荷時設定のデフォルトユーザー名とパスワードが使用される場合には必要ありません。 • ドライバー • IP範囲(IPv4のみ) • ポート番号(デフォルト= 80) システムを拡張する場合など、ネットワークの一部だけをスキャンするときにはこのオプションを選択できます。
手動	各ハードウェアとMilestone Interconnectリモートシステムの詳細情報を個別に指定します。追加するハードウェア数が限られており、IPアドレス、関連するユーザー名およびパスワードが分かっている場合、またはカメラが自動検出機能をサポートしていない場合には、この選択が適しています。

名前	説明
リモート接続ハードウェア	リモート接続されているサーバー経由で接続されているハードウェアがスキャンされます。 Axis One-clickカメラの接続など、サーバーをインストールしている場合にこのオプションを使用できます。 このオプションを使用して、Milestone Interconnectセットアップでリモートシステムを追加することはできません。

ハードウェアの事前設定 (説明付き)

特定のメーカーは、ハードウェアを初めてVMSシステムに追加する前に新しいハードウェアで資格情報を設定するよう義務付けています。これはハードウェアの事前設定とも呼ばれ、[ハードウェア デバイスの事前設定]設定で実行されます。このウィザードは、このようなハードウェアがページ183のハードウェアの追加ウィザードで検出された場合に表れます。

[ハードウェア デバイスの事前設定]ウィザード:

- VMSシステムに追加される前に最初の資格情報が必要なハードウェアは、典型的なデフォルトの資格情報を使用しても追加できません。ウィザードで設定するか、ハードウェアに直接接続して設定する必要があります。
- 資格情報 (ユーザー名またはパスワード) は、未設定というマークの付いたフィールドにのみ適用できます
- ハードウェアのステータスが設定済みに設定されると、資格情報 (ユーザー名またはパスワード) を変更できなくなります。
- 事前設定は新しいハードウェアに適用され、一度だけ実行できます。事前設定後、ハードウェアは、以下の他のハードウェアと同様に管理できます:Management Client
- [ハードウェア デバイスの事前設定]ウィザードを閉じた後、事前設定されたハードウェアがページ183のハードウェアの追加ウィザードに表示され、システムに追加できます。

> [ハードウェア デバイスの事前設定]ウィザードを閉じた後、ページ183のハードウェアの追加ウィザードを完了して、事前設定されたハードウェアにシステムを追加するよう強くお勧めします。Management Clientは、ハードウェアがシステムに追加されなければ、事前設定された資格情報を保持しません。

ハードウェアの有効化/無効化

追加したハードウェアは、デフォルトでは有効になっています。

次の方法でハードウェアが有効化/無効化されたかどうかを確認できます。

有効

(無効)

(ライセンスまたはパフォーマンス上の理由で) 追加したハードウェアを無効にするには

1. レコーディングサーバーを展開し、無効にするハードウェアを右クリックします。
2. 有効を選択して、選択/解除します。

ハードウェアの編集

追加したハードウェアを右クリックし、[ハードウェアの編集]をクリックして、Management Client内のハードウェアのネットワーク構成とユーザー認証設定を修正します。

> ハードウェアによっては、[ハードウェアの編集]ダイアログでも設定をハードウェアデバイスに直接適用できる場合もあります。

[Management Client設定の編集]ラジオボタンが選択されると、[ハードウェアの編集]ダイアログに、Management Clientをハードウェアに接続するために使用する設定が表示されます。ハードウェアデバイスがシステムに適切に追加されたことを確認するため、メーカーのハードウェア構成インターフェースに接続する際に使用するものと同じ設定を入力します：

名前	説明
名前	ハードウェアの名前が、検出されたそのIPアドレス(括弧内)とともに表示されます。
ハードウェアURL	メーカーのハードウェア構成インターフェースのウェブアドレスであり、通常はハードウェアのIPアドレスも記されます。
ユーザー名	ハードウェアへの接続に使用したユーザー名。 ここにユーザー名を入力しても、実際のハードウェアデバイスのユーザー名が変化することはありません。[Management Clientとハードウェア設定の編集]ラジオボタンを選択して、対応ハードウェアデバイスの設定を変更します。
パスワード	ハードウェアへの接続に使用したパスワード。 ここにパスワードを入力しても、実際のハードウェアデバイスのパスワードが変化することはありません。[Management Clientとハードウェア設定の編集]ラジオボタンを選択して、対応ハードウェアデバイスの設定を変更します。

名前	説明
	複数のハードウェアデバイスのパスワードを変更する方法については、「ページ194のハードウェアデバイスでのパスワード変更」を参照してください。 あなたはシステム管理者として、Management Clientでパスワードを表示するための権限を他のユーザーに付与する必要があります。詳細については、ハードウェアの項目の「ページ341の役割の設定」を参照してください。

対応ハードウェアに対して［Management Clientとハードウェア設定の編集］ラジオボタンが選択されている場合、同様にハードウェアデバイスに直接適用される設定が［ハードウェアにの編集］ダイアログに表示されます。

このラジオボタンが選択された状態で設定を適用すると、ハードウェアデバイスの現在の設定が上書きされます。設定の適用中は、ハードウェアからレコーディングサーバーへの接続が一時的失われます。

名前	説明
名前	ハードウェアの名前が、検出されたそのIPアドレス(括弧内)とともに表示されます。
ネットワーク構成	ハードウェアのネットワーク設定。ネットワーク設定を調整するにはページ187の構成を選択します。
構成	［IPバージョン］ドロップダウンリストを使用して、対応ハードウェアデバイスのインターネットプロトコルを指定します。 • IPv4の値は以下の形式でなければなりません：(0-999).(0-999).(0-999).(0-999) • IPv6の値は、8つの16進数の値(コロン区切り)という形式でなければなりません。サブネットマスクは0～128の数値でなければなりません。 ［チェック］ボタンを押すと、入力したIPアドレスが、現在システム内の他のハードウェアデバイスによって使用されているのかテストできます。

名前	説明
	[チェック]を使用しても、オフになっている/XProtect VMSシステムの外部にある/他の理由で一時的に応答していないハードウェアデバイス間の競合を検出することはできません。
ユーザー名	ハードウェアへの接続に使用したユーザー名とレベル。ドロップダウンリストから別のユーザーを選択し、下記の[パスワード]フィールドを使用して新しいパスワードを追加します。 [認証]セクション下部にある下線が付いたアクションを用いてユーザーを追加または削除します(「ページ188のユーザーの追加」または「ページ189のユーザーの削除」を参照)。 メーカーが指定した最高レベルが割り当てられていないユーザーを選択すると、一部の機能が利用できなくなる可能性があります。
パスワード	ハードウェアへの接続に使用したパスワード。公開 アイコンを使用して入力中のテキストを表示します。 パスワードを変更する際は、特定のハードウェアデバイスで定められているパスワード規則について記されたメーカーのマニュアルを参照してください。または、[パスワードの生成] アイコンを使用すれば、要件に沿ったパスワードが自動的に生成されます。 複数のハードウェアデバイスのパスワードを変更する方法については、「ページ194のハードウェアデバイスでのパスワード変更」を参照してください。 あなたはシステム管理者として、Management Clientでパスワードを表示するための権限を他のユーザーに付与する必要があります。詳細については、ハードウェアの項目の「ページ341の役割の設定」を参照してください。
ユーザーの追加	下線の付いた[追加]リンクを選択して[ユーザーの追加]ダイアログを開き、ハードウェアデバイスにユーザーを追加します。 ユーザーを追加すると、このユーザーが自動的に現在アクティブなユーザーとして設定され、前回入力した資格情報が上書きされます。 パスワードを作成する際には、特定のハードウェアデバイスに伴うパスワード規則について記されたメーカーのマニュアルを参照するか、[パスワードの生成] アイコンを使用して要件を満たしたパスワードを自動的に生成

名前	説明
	してください。 ハードウェアデバイスで検出された最高ユーザーレベルが自動的に事前選択されます。ユーザーレベルをデフォルト値から変更することは推奨されません。 メーカーが指定した最高ユーザーレベル以外のレベルを選択すると、一部の機能が利用できなくなる可能性があります。
ユーザーの削除	下線の付いた [削除] リンクを選択して [ユーザーの削除] ダイアログを開き、ハードウェアデバイスからユーザーを削除します。 現在アクティブなユーザーを削除することはできません。新しいユーザーを設定するには、上記の [ユーザーの追加] ダイアログを使用してから、このインターフェースを使用して古いユーザーを削除します。

「ハードウェアの管理」も参照してください。

個々のデバイスの有効化/無効化

カメラは、デフォルトで有効です。

マイク、スピーカー、メタデータ、入力および出力は、デフォルトで無効です。

これは、システムで使用できるようにするには、マイク、スピーカー、メタデータ、入力および出力を個別に有効にしなければならないことを意味しています。理由は、監視システムは本質的にカメラに依存しているものの、マイクなどの使用の有無は、各組織のニーズによって極めて異なる場合が多いためです。

デバイスが有効か無効かを確認できます(例は出力です) 。

(無効)

有効

同じ方法でカメラ、マイク、スピーカー、メタデータ、入力、および出力を有効化/無効化することができます。

1. レコーディングサーバーとデバイスを展開します。有効にするデバイスを右クリックします。
2. 有効を選択して、選択/解除します。

ハードウェアへの安全な接続設定する

SSL(セキュアソケットレイヤー) を使用して、ハードウェアデバイスとレコーディングサーバーの間で安全なHTTPS接続を設定できます。

以下の手順を実行する前に、カメラメーカーにお問い合わせの上、ハードウェアの証明書の取得とハードウェアへのアップロードを行ってください。

1. 概要ペインで、レコーディングサーバーを右クリックし、ハードウェアを選択します。

2. 設定タブでHTTPSを有効にします。デフォルトでは無効になっています。
3. HTTPS接続で使用するレコーディングサーバーのポートを入力します。ポート番号は、デバイスのホームページで設定されたポートに対応する必要があります。
4. 必要に応じて変更し、保存します。

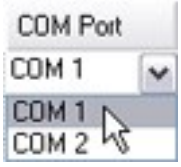
ビデオエンコーダーでのPTZの有効化

ビデオエンコーダーでPTZカメラの使用を有効にするには、**PTZ**タブで次の手順を実行します。

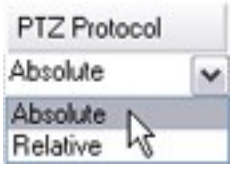
1. ビデオエンコーダーに接続されているデバイスのリストで、該当するカメラの**PTZ**を有効化ボックスを選択します。

2. **PTZ**デバイス**ID**列で、各カメラの**ID**を確認します。

3. COMポート列で、PTZ機能を制御するために使用する、ビデオエンコーダーのCOM(シリアル通信)ポートを選択します。



4. PTZプロトコル列で、使用する位置スキームを選択します。



- 絶対値:オペレータがカメラのPTZ(パン/チルト/ズーム)制御を使用すると、固定位置(カメラのホーム位置)に対して相対的にカメラが調整されます。
- 相対値:オペレータがカメラのPTZ(パン/チルト/ズーム)制御を使用すると、現在の位置に対して相対的にカメラが調整されます。

PTZプロトコル列の内容は、ハードウェアによって大きく異なります。5～8の異なるプロトコルがあります。カメラのマニュアルも参照してください。

5. ツールバーで保存をクリックします。

これで、各PTZカメラのプリセット位置とパトロールを設定できます。

- ページ234のプリセット位置を追加する(タイプ1)
- ページ243のパトロール設定の追加

ハードウェアの管理

情報タブ(ハードウェア)

リモートサーバーの情報タブの詳細については、ページ197の情報タブ(リモートサーバー)を参照してください。

情報タブ(ハードウェア)

名前	説明
名前	名前を入力します。この名前は、システムやクライアントでハードウェアが列挙されるたびに使用されま

名前	説明
	す。名前は一意である必要はありません。 ハードウェアの名前を変更すると、名前はManagement Clientで一括変更されます。
説明	ハードウェアの説明を入力します(オプション) 。説明は、システム内の複数のリストに表示されます。たとえば、概要ペインでハードウェア名にマウスポインタを移動すると表示されます：
モデル	ハードウェアモデルを規定します。
シリアル番号	メーカーが指定したハードウェアのシリアル番号。シリアル番号は、MACアドレスと同じであることがよくありますが、必ず一致するわけでもありません。
ドライバー	ハードウェアへの接続を処理しているドライバーを規定します。
IE	ハードウェア製造元のデフォルトホームページを開きます。このページはハードウェアの管理に使用します。
アドレス	ハードウェアのIPアドレスまたはホスト名。
MACアドレス	システムハードウェアのハードウェアメディア入退室管理(MAC)アドレスを指定します。MACアドレスは、ネットワーク上の各ハードウェアを一意に識別する12文字の16進数です。
最後に変更したパスワード	最後に変更したパスワードフィールドには、最後にパスワードを変更した際のタイムスタンプが表示されます。ここでは、パスワードを変更したコンピューターの現地の時刻設定が反映されます。

設定タブ(ハードウェア)

設定タブで、ハードウェアの設定を確認または編集できます。

> 設定タブの内容は、選択したハードウェアによって決定されます。このため、ハードウェアの種類によって内容が異なります。ハードウェアの種類によっては、設定タブの内容がまったく表示されないか、または読み取り専用の場合があります。

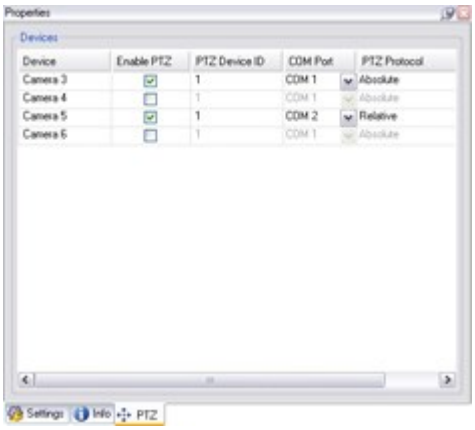
リモートサーバーの設定タブの詳細については、ページ198の設定タブ(リモートサーバー)を参照してください。

PTZタブ(ビデオエンコーダー)

PTZタブでは、ビデオエンコーダーのPTZ(パン/チルト/ズーム)を有効にできます。選択されたデバイスがビデオエンコーダーであるか、ドライバーが非PTZおよびPTZカメラの両方をサポートしている場合に、このタブを使用できます。

PTZタブの各ビデオエンコーダーのチャネルで、PTZの使用を個別に有効にすると、ビデオエンコーダーに接続されたPTZカメラのPTZ機能を使用できます。

> 一部のビデオエンコーダーは、PTZカメラに対応していません。PTZカメラの使用をサポートするビデオエンコーダーでも、PTZカメラを使用する前に、設定が必要な場合があります。通常は、デバイスのIPアドレスで、ブラウザベースの設定インターフェースを使用して、追加ドライバーをインストールします。



2つのビデオエンコーダーチャネルに対してPTZが有効になっている状態のPTZタブ

デバイスのパスワード管理(説明付き)

> 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。

1回の操作で、複数のハードウェアデバイスのパスワードを変更することができます。

まず、Canon、Axis、Bosch、Hanwa、Panasonic、Sony、Hikvision、ONVIFと互換性のあるハードウェアデバイスのモデルがサポートされており、モデルがサポートされているかどうかはユーザーインターフェイスに直接表示されます。対応モデルについては、弊社Webサイトでもご確認いただけます。 https://www.milestonesys.com/community/business-partner-tools/supported-devices/

パスワード管理に対応していないデバイスについては、ハードウェアデバイスのパスワードをWebページで変更してから、Management Clientで手動で新しいパスワードを入力します。. 詳細についてはページ186のハードウェアの編集を参照してください。

システムに各ハードウェアデバイスの個々のパスワードを生成させるか、あるいは、すべてのハードウェアデバイスにユーザーが指定した単一のパスワードを使用するかを選択することができます。パスワードには印刷可能なASCII文字しか使用できません。

システムが、ハードウェアデバイスのメーカーによる条件に基づきパスワードを生成します。

新しいパスワードを適用すると、ハードウェアデバイスはレコーディングサーバーへの接続が一瞬切れます。

新しいパスワードの適用後、各ハードウェアデバイスの結果が画面に表示されます。変更に失敗した場合、失敗の理由が表示されます(ハードウェアデバイスがその種の情報に対応している場合) 。ウィザード内からパスワード変更の成否レポートを作成することができますが、その結果は「サーバーログ」にも記録されます。.

ONVIFドライバと複数のユーザーアカウントのあるハードウェアデバイスについては、そのハードウェアデバイスの管理権限を持つXProtectのシステム管理者のみが監視カメラ管理ソフトウェアからパスワードを変更することができます。

1回の操作でパスワードを変更する方法については、ページ194のハードウェアデバイスでのパスワード変更.を参照してください。

ハードウェアデバイスでのパスワード変更

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。

1回の操作で、複数のハードウェアデバイスのパスワードを変更することができます。機能と対応モデルは、ページ193のデバイスのパスワード管理(説明付き) を参照してください。

要件:

- ハードウェアデバイスのモデルは、Milestoneによるデバイスのパスワード管理に対応しています。

手順:

1. [サイトナビゲーション]ペインで[レコーディングサーバー]ノードを選択します。
2. 概要ペインで、削除するレコーディングサーバーを右クリックします。
3. [ハードウェアのパスワード変更]を選択します。ウィザードが表示されます。

4. 指示に従って、プロセスを完了してください。

> 最後に変更したパスワードフィールドには、最後にパスワードを変更した際のタイムスタンプが表示されます。ここでは、パスワードを変更したコンピューターの現地の時刻設定が反映されます。

5. 最後にページに結果が表示されます。システムでパスワードが更新されなかった場合は、ハードウェアデバイスの横に表示された[失敗]をクリックして理由を確認します。
6. また、[レポートを印刷]ボタンをクリックして、すべてのデバイスの更新成功と失敗の一覧を出すことができます。
7. 失敗したハードウェアデバイスのパスワードを変更する場合は、[再試行]をクリックしてその失敗したハードウェアデバイスについてウィザードを再度始めてください。

> [再試行]をクリックすると、ウィザードを初めて完了したときのレポートはもう表示されません。

> セキュリティ上の制限により、数回連続してパスワード変更に失敗すると一定の期間使用不可になるハードウェアデバイスがあります。セキュリティの制限はメーカーにより異なります。

デバイス ファームウェアのアップデート(説明付き)

> 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。

Management Clientでは、VMSシステムに追加されたハードウェアのファームウェアを更新できます。同じファームウェア ファイルと互換性がある場合は、複数のハードウェア デバイスのファームウェアを同時に更新できます。

ユーザーインターフェイスには、モデルがファームウェアの更新に対応しているかどうかが直接表示されます。MilestoneのWebサイトで、モデルの対応状況を確認することもできます: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> ファームウェアの更新に対応していないデバイスの場合は、Webページからハードウェア デバイスのファームウェアを更新する必要があります。

ファームウェアを更新すると、ハードウェア デバイスはレコーディングサーバーへの接続を一瞬失います。

ファームウェアを更新すると、各ハードウェアデバイスの結果が画面に表示されます。変更に失敗した場合、失敗の理由が表示されます(ハードウェアデバイスがその種の情報に対応している場合) 。この結果は、[サーバーログ]でもログできます。

> ONVIFドライバーと複数のユーザーアカウントがあるハードウェアデバイスの場合は、そのハードウェアデバイスの管理者権限があるXProtectの管理者のみがVMSからファームウェアを更新できます。

1回の操作でパスワードを変更する方法については、ページ196のハードウェアデバイスでのファームウェア更新を参照してください。

ハードウェアデバイスでのファームウェア更新

> 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。

複数のハードウェアデバイスは1回の操作で更新することができます。機能と対応モデルについては、ページ195のデバイスファームウェアのアップデート(説明付き)を参照してください。

要件:

- このハードウェアデバイスのモデルは、Milestoneによるファームウェアの更新に対応しています。

手順:

1. [サイトナビゲーション]ペインで[レコーディングサーバー]ノードを選択します。
2. 概要ペインで、削除するレコーディングサーバーを右クリックします。
3. [ハードウェアのファームウェア更新]を選択します。ウィザードが表示されます。
4. 指示に従って、プロセスを完了してください。

> 同じファームウェアファイルと互換性のある複数のハードウェアデバイスのみを更新できます。ONVIFドライバーを介して追加されたハードウェアは、メーカー名ではなく、[その他]に含まれています。

6. 最後にページに結果が表示されます。システムでファームウェアを更新できなかった場合は、ハードウェアデバイスの横に表示された[失敗]をクリックして理由を確認します。

> Milestoneは、互換性のないファームウェアファイルまたはハードウェアデバイスが選択された場合にハードウェアデバイスに機能不全が生じても責任を負いません。

サイトナビゲーション：サーバーとハードウェア：リモートサーバーの管理

情報タブ(リモートサーバー)

名前	説明
名前	この名前は、システムやクライアントでリモートサーバーが列挙されるたびに使用されます。名前は一意である必要はありません。 サーバーの名前を変更すると、名前はManagement Clientで一括変更されます。
説明	リモートサーバーの説明を入力します(オプション)。 説明は、システム内の複数のリストに表示されます。たとえば、概要ペインでハードウェア名にマウスポインタを移動すると表示されます。
モデル	リモートサイトにインストールされたXProtect製品を表示します。
バージョン	リモートシステムのバージョンを表示します。
ソフトウェアライセンスコード	リモートシステムのソフトウェアライセンスコード。
ドライバー	リモートサーバーへの接続を処理しているドライバーを規定します。
アドレス	ハードウェアのIPアドレスまたはホスト名。
IE	ハードウェア製造元のデフォルトホームページを開きます。このページはハードウェアまたはシステムの管理に使用します。
リモートシステムID	ライセンスの管理などにXProtectが使用するリモートサイトの一意のシステムID。
Windowsユーザー名	リモートデスクトップ経由でアクセスするためのWindowsユーザー名を入力します。
Windowsパスワード	リモートデスクトップ経由でアクセスするためのWindowsパスワードを入力します。
接続	リモートサイトに接続するリモート接続が開きます(Windowsの資格情報が承認された後)。

設定タブ(リモートサーバー)

設定タブにリモートシステムの名前が表示されます。

イベントタブ(リモートサーバー)

リモートシステムから中央サイトにイベントを追加し、ルールを作成できます。これによって、リモートシステムからのイベントに即時対応できます。イベント数は、リモートシステムで設定されたイベントによって異なります。デフォルトのイベントは削除できません。

表示されるリストが不完全な場合:

1. 概要ペインで関連するリモートサーバーを右クリックし、ハードウェアの更新を選択します。
2. このダイアログボックスには、Milestone Interconnect設定が最後に確立または更新されてから、リモートシステムで行われたすべての変更(デバイスの削除、更新、および追加)のリストが表示されます。確認をクリックして、中央サイトにこれらの変更を更新します。

リモート取得タブ

リモート取得タブでは、Milestone Interconnect環境のリモートサイトのリモート記録取得設定を処理できます。

以下のプロパティを指定します。

名前	説明
最大で録画を取得	リモートサイトからの録画の取得に使用する最大帯域幅をキロビット/秒単位で規定します。取得の制限を有効にするには、チェックボックスを選択します。
次の間で録画を取得	リモートサイトからの記録取得を特定のタイムインターバルに限定するかどうかを決めます。 終了時間になると、未完了のジョブが完了するまで続行するため、終了時間が重要な場合、未完了のジョブが完了できるように終了時間を早く設定する必要があります。 システムが自動取得または取得のリクエストをタイムインターバル外にXProtect Smart Clientから受け取った場合、リクエストは受け付けられますが、選択されたタイムインターバルに達するまでは開始されません。 ユーザーが開始した保留中のリモート録画取得ジョブは、システムダッシュボード>現在のタスクから確認できます。
並列取得デバイス数	記録を同時に取得するデバイスの最大数を規定します。システムの機能にしたがって、容量を増減する必要がある場合にデフォルト値を変更します。

設定を変更すると、変更がシステムで反映されるまでに時間がかかることがあります。

> 上記のいずれも、リモート録画の直接再生には該当しません。直接再生されるように設定されたすべてのカメラは直接再生でき、必要に応じて帯域幅を使用します。

サイトナビゲーション：デバイス：デバイスの使用

ハードウェアをManagement Clientハードウェアの追加ウィザードで追加すると、デバイスがに表示されます。

デバイスが同じプロパティであれば、デバイスグループからデバイスを管理できます。ページ207のサイトナビゲーション：デバイス：デバイスグループの操作を参照。

デバイスを個別に管理することもできます。

- カメラ
- マイク
- スピーカー
- メタデータ
- 入力
- 出力

デバイス(説明付き)

ハードウェアには、以下のように、個別に管理できるデバイスが複数あります。

- 物理カメラには、カメラ部品(レンズ)を表すデバイスおよび、接続型または内蔵型のマイク、スピーカー、メタデータ、入力および出力などのデバイスが付いています
- ビデオエンコーダーには、複数のアナログカメラが接続されており、デバイスのリスト1枚に表示されます。これには、カメラ部品(レンズ)を表すデバイスおよび、接続型または内蔵型のマイク、スピーカー、メタデータ、入力および出力などのデバイスが含まれています
- I/Oモジュールには、ライトなど、入出力チャネルを表すデバイスが付いています
- 音声専用モジュールには、マイクやスピーカーの入出力を表すデバイスが付いています
- Milestone Interconnect設定では、リモートシステムは、リモートシステムからのすべてのデバイスが1つのリストとして表されたハードウェアとして表示されます

ハードウェアを追加すると、ハードウェアのデバイスが自動的に追加されます。

サポート対象ハードウェアについては、Milestone のウェブサイト(https://www.milestonesys.com/supported-devices/)のサポート対象ハードウェアページを参照してください。

以下のセクションでは、管理に使用できるタブへのリンク付きの各デバイスタイプについて説明します。

カメラデバイス(説明付き)

カメラデバイスは、システムにハードウェアを追加したときに自動的に追加され、デフォルトで有効化されます。

カメラデバイスは、ビデオストリームをシステムに送信し、クライアントユーザーはライブビデオビューを使用することができます。あるいは、ビデオストリームをシステムが録画して、クライアントユーザーは後日に再生できます。役割により、ユーザーがビデオを見る権限が決定されます。

サポート対象ハードウェアについては、Milestone のウェブサイト(https://www.milestonesys.com/supported-devices/)のサポート対象ハードウェアページを参照してください。

システムにはデフォルトの配信開始ルールがあります。このルールにより、接続されているすべてのカメラからの映像配信が自動的にシステムに送られます。他のルールと同様、必要に応じて、デフォルトルールを無効にしたり修正したりできます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。ページ206のデバイスグループ経由のデバイスの有効化/無効化を参照してください。

カメラのその他のすべての設定や管理を行うには、サイトナビゲーションペインでデバイスを展開してから、カメラを選択します。概要ペインで、カメラの概要を分かりやすくするためにカメラをグループ化します。初期グループ化は、ハードウェアの追加ウィザードの一部です。

この設定順序に従って、カメラデバイスの設定に関連する最も一般的なタスクを実行します。

1. カメラの設定(ページ212の設定タブ(デバイス)を参照してください)。
2. ストリームの設定(ページ214のストリームタブ(デバイス)を参照してください)。
3. モーションの構成(「ページ224のモーションタブ(デバイス)」を参照)。
4. 録画の構成(「ページ217の録画タブ(デバイス)」を参照)。
5. 必要に応じて他の設定を設定します。

マイクデバイス(説明付き)

多くのデバイスには、外部マイクを接続できます。マイクが内蔵されているデバイスもあります。

マイクデバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、ハードウェアの追加ウィザードから、または後日に有効にする必要があります。マイクには特にライセンスは必要ありません。システムで必要な数のマイクを無制限に使用できます。

マイクは、完全にカメラとは別に使用できます。

マイクデバイスは、音声ストリームをシステムに送信し、クライアントユーザーはライブ音声として聞くことができます。あるいは、音声ストリームをシステムが録音して、クライアントユーザーは後日に再生できます。関連するアクションをトリガーするマイク固有のイベントを受信するように、システムを設定できます。

> サポート対象ハードウェアについては、Milestone のウェブサイト(https://www.milestonesys.com/supported-devices/)のサポート対象ハードウェアページを参照してください。

役割により、ユーザーがマイクを聞く権限が決定されます。Management Clientからマイクからの音声を聞くことはできません。

システムにはデフォルトの音声配信開始ルールがあります。このルールに従って、接続されているすべてのマイクからの音声配信が自動的にシステムに送られます。他のルールと同様、必要に応じて、デフォルトルールを無効にしたり修正したりできます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。詳細は、ページ206のデバイスグループ経由のデバイスの有効化/無効化を参照してください。

カメラのその他すべての設定や管理を行うには、サイトナビゲーションペインでデバイスを展開してから、マイクを選択します。概要ペインでは、マイクをグループ化して、概要を把握しやすくすることができます。初期グループ化は、ハードウェアの追加ウィザードの一部です。

マイクデバイスは、以下のタブを使って設定できます。

- 情報タブ(ページ210の情報タブ(デバイス)を参照)
- [設定タブ](「ページ212の設定タブ(デバイス)」を参照)
- [録画]タブ(「ページ217の録画タブ(デバイス)」を参照) 。
- [イベント]タブ(「ページ248のイベントタブ(デバイス)」を参照)

スピーカーデバイス(説明付き)

多くのデバイスには、外部スピーカーを接続できます。スピーカーが内蔵されているデバイスもあります。

スピーカーデバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、ハードウェアの追加ウィザードから、または後日に有効にする必要があります。スピーカーには特にライセンスは必要ありません。システムで必要な数のスピーカーを無制限に使用できます。

スピーカーは、完全にカメラとは別に使用できます。

サポート対象ハードウェアについては、Milestoneのウェブサイト(https://www.milestonesys.com/supported-devices/)のサポート対象ハードウェアページを参照してください。

ユーザーがXProtect Smart Clientの会話ボタンを押すと、スピーカーに音声ストリームが配信されます。スピーカーの音声は、ユーザーがスピーカーに向かって話したときのみ録音されます。役割により、ユーザーがスピーカで話す権限を決定します。Management Clientからスピーカーを通して話すことはできません。

2人のユーザーが同時に話す場合は、スピーカーを通して話すユーザー権限は役割によって決定されます。役割の定義の一部として、スピーカーの優先度を「非常に高い」から「非常に低い」まで指定することができます。2人のユーザーが同時に話そうとする場合、優先度が一番高い役割を持つユーザーが話す機能を得ます。同じ役割の2人のユーザーが同時に話そうとする場合、「早く来たものから処理される」原則が適用されます。

システムにはデフォルトの音声配信開始ルールがあります。このルールに従って、デバイスが起動され、ユーザーが有効にした音声をデバイスからスピーカーに送信する準備ができます。他のルールと同様、必要に応じて、デフォルトルールを無効にしたり修正したりできます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。ページ206のデバイスグループ経由のデバイスの有効化/無効化を参照してください。

カメラのその他すべての設定や管理を行うには、サイトナビゲーションペインでデバイスを展開してから、スピーカーを選択します。概要ペインでは、スピーカーをグループ化して、概要を把握しやすくすることができます。初期グループ化は、ハードウェアの追加ウィザードの一部です。

スピーカーデバイスは、以下のタブを使って設定できます。

- ページ210の情報タブ(デバイス)
- ページ212の設定タブ(デバイス)
- ページ217の録画タブ(デバイス)

メタデータデバイス(説明付き)

メタデータデバイスは、クライアントユーザーがデータに関して参照できるデータストリームをシステムに配信します。たとえば、動画映像を説明するデータ、映像内のコンテンツまたはオブジェクト、または録画された映像の場所を説明することができます。メタデータは、カメラ、マイク、またはスピーカーに添付できます。

メタデータは以下の方法で生成できます。

- 自らデータを配信しているデバイス(ビデオを配信しているカメラなど)
- サードパーティシステムまたは統合で、汎用メタデータドライバーを経由した配信

デバイスで生成されたメタデータは、同じハードウェア上の1つまたは複数のデバイスに自動的にリンクされます。

サポート対象ハードウェアについては、Milestone のウェブサイト(https://www.milestonesys.com/supported-devices/)のサポート対象ハードウェアページを参照してください。

役割により、ユーザーがメタデータを参照する権限が決定されます。

システムにはデフォルトの配信開始ルールがあります。このルールに従って、メタデータをサポートする接続されているすべてのハードウェアからのメタデータ配信が自動的にシステムに送られます。他のルールと同様、必要に応じて、デフォルトルールを無効にしたり修正したりできます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。詳細は、ページ206のデバイスグループ経由のデバイスの有効化/無効化を参照してください。

メタデータデバイスのその他すべての設定や管理を行うには、サイトナビゲーションペインでデバイスを展開してから、メタデータを選択します。概要ペインでは、メタデータデバイスをグループ化して、概要を把握しやすくすることができます。初期グループ化は、ハードウェアの追加ウィザードの一部です。

メタデータデバイスは、以下のタブを使って設定できます。

- 情報タブ(ページ210の情報タブ(デバイス)を参照)
- 設定タブ](「ページ212の設定タブ(デバイス)」を参照)
- 録画]タブ(「ページ217の録画タブ(デバイス)」を参照) 。

入力デバイス(説明付き)

多くのデバイスには、デバイスの入力ポートに外部ユニットを取り付けることができます。入力ユニットは、通常は外部センサーです。たとえば、ドア、窓、あるいはゲートが開いた場合に、こうした外部センサーを使用して検知することができます。こうした外部入力ユニットからの入力は、システムではイベントとして処理されます。

これらのイベントは、ルールで使用できます。たとえば、入力が有効になるとカメラが録画を開始し、入力が無効になってから30秒経過すると録画を停止するように指定するルールを作成することができます。

入力デバイスは、完全にカメラとは別に使用できます。

デバイスで外部入力ユニットの使用を指定する前に、デバイス自体がセンサーの動作を認識しているか確認してください。大半のデバイスでは、設定用インターフェースかコモンゲートウェイインターフェース(CGI)スクリプトのコマンドでこれを表示できます。

入力デバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、ハードウェアの追加ウィザードから、または後日に有効にする必要があります。入力デバイスには特にライセンスは必要ありません。システムで必要な数の入力デバイスを無制限に使用できます。

サポート対象ハードウェアについては、Milestoneのウェブサイト(https://www.milestonesys.com/supported-devices/)のサポート対象ハードウェアページを参照してください。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。ページ206のデバイスグループ経由のデバイスの有効化/無効化を参照してください。

カメラのその他すべての設定や管理を行うには、サイトナビゲーションペインでデバイスを展開してから、入力を選択します。概要ペインでは、入力デバイスをグループ化して、概要を把握しやすくすることができます。初期グループ化は、ハードウェアの追加ウィザードの一部です。

入力デバイスは、以下のタブを使って設定できます。

- 情報タブ(ページ210の情報タブ(デバイス)を参照)
- 設定タブ](「ページ212の設定タブ(デバイス)」を参照)
- [イベント]タブ(「ページ248のイベントタブ(デバイス)」を参照)

手動で入力を有効にしてテストする

ルール機能を使用して、入力を自動的に有効化または無効化するルールを定義するか、またはManagement Clientから手動で有効化してルールをチェックできます。

1. 概要ペインで、関連する入力デバイスを選択します。
2. 物理的デバイスで入力を有効にします。
3. プレビューペインで、緑色のインジケータが点灯していることを確認します。これで、入力デバイスが動作します。

出力デバイス(説明付き)

多くのデバイスには、デバイスの出力ポートに外部ユニットを取り付けることができます。これによって、システムを通してライト、サイレンなどを有効/無効にすることができます。

出力は、ルールを作成する際に使用できます。出力を自動的に有効または無効にするルール、出力の状態が変化した時にアクションをトリガーするルールなどを作成できます。

出力は、Management ClientおよびXProtect Smart Clientから手動でトリガーできます。

デバイスで外部出力ユニットの使用を指定する前に、デバイス自体が出力に接続されたデバイスを制御できるかどうかを確認してください。大半のデバイスでは、設定用インターフェースかコモンゲートウェイインターフェース(CGI)スクリプトのコマンドでこれを表示できます。

出力デバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、ハードウェアの追加ウィザードから、または後日に有効にする必要があります。出力デバイスには特にライセンスは必要ありません。システムで必要な数の出力デバイスを無制限に使用できます。

サポート対象ハードウェアについては、Milestone のウェブサイト(https://www.milestonesys.com/supported-devices/)のサポート対象ハードウェアページを参照してください。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。ページ206のデバイスグループ経由のデバイスの有効化/無効化を参照してください。

カメラのその他すべての設定や管理を行うには、サイトナビゲーションペインでデバイスを展開してから、出力を選択します。概要ペインでは、入力デバイスをグループ化して、概要を把握しやすくすることができます。初期グループ化は、ハードウェアの追加ウィザードの一部です。

出力デバイスは、以下のタブを使って設定できます。

- ページ210の情報タブ(デバイス)
- ページ212の設定タブ(デバイス)

手動で出力を有効にしてテストします。

ルール機能を使用して、出力を自動的に有効化または無効化するルールを定義するか、またはクライアントから手動で有効化できます。

Management Clientから出力を手動で有効にして、機能をテストできます。

1. [概要]ペインで、関連する出力デバイスを選択します。
2. 通常は、プレビューペインでそれぞれの出力について以下の要素が表示されます。

3. チェックボックス を選択/選択解除すると、選択した出力を有効化/無効化します。出力が有効になると、緑色のインジケータが点灯します。

4. あるいは、長方形のボタン をクリックすると、設定タブの出力トリガー時間設定で定義される期間、出力が有効になります(この機能/設定はすべての出力で使用できるわけではありません) 。定義された期間が過ぎると、出力は自動的に無効になります。

デバイスグループ経由のデバイスの有効化/無効化

設定済みハードウェアからのみデバイスを有効化/無効化できます。ハードウェアの追加ウィザードから手動で有効化/無効化した場合を除いて、カメラデバイスはデフォルトで有効化されており、他のデバイスはデフォルトで無効化されています。

デバイスを有効または無効にするためにデバイスグループ経由でアクセスする方法：

1. サイトナビゲーションペインで、デバイスを選択します。
2. 概要ペインで、関連グループを展開してデバイスを検索します。
3. デバイスを右クリックして、ハードウェアに移動を選択します。
4. [+] ノードをクリックして、ハードウェア上のすべてのデバイスを表示します。
5. 有効/無効にするデバイスを右クリックして、有効を選択します。

デバイスのステータスアイコン

あるデバイスを選択すると、現在のステータスについての情報がプレビューペインに表示されます。以下のアイコンはデバイスのステータスを示します：

カメラ	マイク	スピーカー	メタデータ	入力	出力	説明
						有効なデバイスおよびデータの取得中：デバイスは有効化されており、ライブストリームを取得します。

カメラ	マイク	スピーカー	メタデータ	入力	出力	説明
						デバイスは録画中：デバイスはシステムにあるデータを記録中です。
						一時的に停止されているか、入力のないデバイス：停止している場合は、情報はシステムに転送されません。カメラの場合は、ライブビデオを表示できません。停止したデバイスは、デバイスが無効である場合とは対照的に、レコーディングサーバーと通信してイベントの取得、設定の設定などが可能です。
						無効なデバイス：ルールを通して自動的に開始されず、レコーディングサーバーと通信できません。カメラが無効な場合は、ライブまたは録画されたビデオを表示できません。
						デバイスデータベースを修復中です。
						デバイスに問題が発生しています。このデバイスは正しく機能しません。マウスポインタをデバイスアイコンの上で一次停止させて、ヒントに書かれている問題の説明を確認します。
						不明なステータスです：デバイスのステータスが不明です。例えば、レコーディングサーバーがオフラインの場合など。
						複数のアイコンを組み合わせることができます。例えばこの場合では有効なデバイスおよびデータの取得中がデバイスは録画中と組み合わされています。

サイトナビゲーション：デバイス：デバイスグループの操作

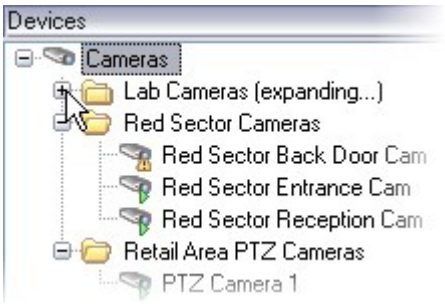
デバイスをデバイスグループに分類することは、ハードウェアの追加ウィザードの一部ですが、必要に応じていつでもグループを変更し、より多くのグループを追加できます。

システムにある異なる種類のデバイス(カメラ、マイク、スピーカー、メタデータ、入力、および出力) をグループ化すると便利です。

- デバイスグループによって、使用しているシステムのデバイスの概要を直観的に管理できます。
- デバイスは複数のグループに割り振ることができます。
- サブグループを作成したり、サブグループの中にサブグループを作成できます。
- デバイスグループのデバイスには、共通のプロパティを一度に指定することができます。
- グループに設定されたグループプロパティはグループには保存されませんが、個別のデバイスに保存されます。

- 役割を取り扱う場合、デバイスグループのすべてのデバイスに、共通のセキュリティ設定を一度に指定することができます
- 役割を取り扱う場合、デバイスグループのすべてのデバイスに、ルールを一度に適用することができます

必要な数のデバイスグループを追加できますが、異なる種類のデバイスを1つのデバイスグループで混ぜることはできません(例えばカメラとスピーカー)。



すべてのプロパティを表示し、編集できるように、400デバイス未満のデバイスグループを作成してください。

デバイスグループを削除すると、デバイスグループ自体のみが削除されます。例えばカメラなどのデバイスをシステムから削除する場合は、レコーディングサーバーレベルで行います。

以下の例は、カメラのデバイスグループへのグループ化に基づいていますが、原則はすべてのデバイスに適用されます。

ページ208のデバイスグループの追加

ページ209のデバイスグループに含めるデバイスの指定

ページ209のデバイスグループのすべてのデバイスに対する共通プロパティの指定

デバイスグループの追加

1. 概要ペインで、アイテムの中から、下にデバイスグループを作成するデバイスタイプを右クリックします。
2. デバイスグループの追加を選択します。
3. デバイスグループの追加ダイアログボックスで、新しいデバイスグループの名前と説明を指定します。

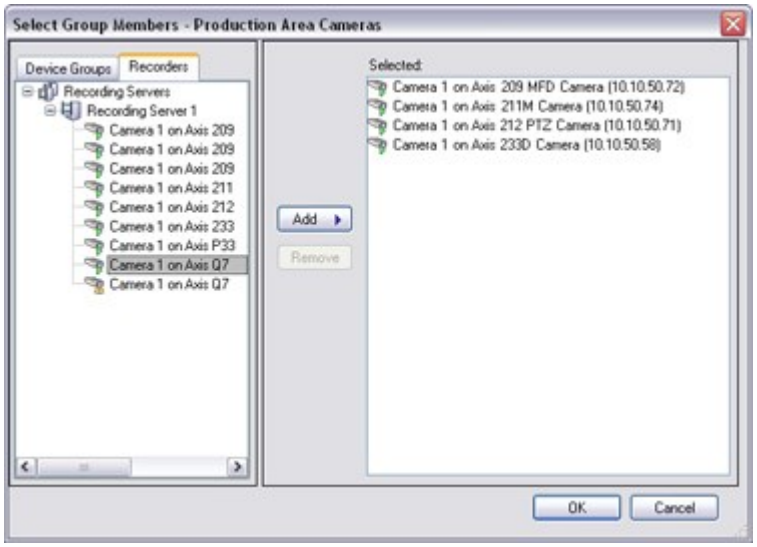
デバイスグループリストのデバイスグループの上でマウスポインタを一時停止させると、説明が表示されます。

4. OK をクリックします。新しいデバイスグループを表すフォルダーがリストに追加されます。
5. デバイスグループに含めるデバイスを指定します(ページ209のデバイスグループに含めるデバイスの指定を参照)。

デバイスグループに含めるデバイスの指定

1. 概要ペインで、関連するデバイスグループフォルダーを右クリックします。
2. デバイスグループメンバーを編集を選択します。
3. グループメンバーを選択ウィンドウで、デバイスを配置するタブを1つ選択します。

   デバイスは、複数のデバイスグループのメンバーになれます。
4. 含めたいデバイスを選択して、追加ボタンをクリックするかデバイスをダブルクリックします。



5. OK をクリックします。
6. 1グループに400デバイスの制限を超過する場合は、デバイスグループを他のデバイスグループのサブグループとして追加できます。

デバイスグループのすべてのデバイスに対する共通プロパティの指定

デバイスグループでは、特定のデバイスグループ内のすべてのデバイスの共通設定を指定できます。

1. 概要ペインで、デバイスグループをクリックします。

   プロパティペインには、デバイスグループのすべてのデバイスで使用できるすべてのプロパティが、タブでグループ化されて一覧表示されます。

2. 関連する共通のプロパティを指定します。

   設定タブで、すべてのデバイスの設定および個々のデバイスの設定の間で切り替えることができます。

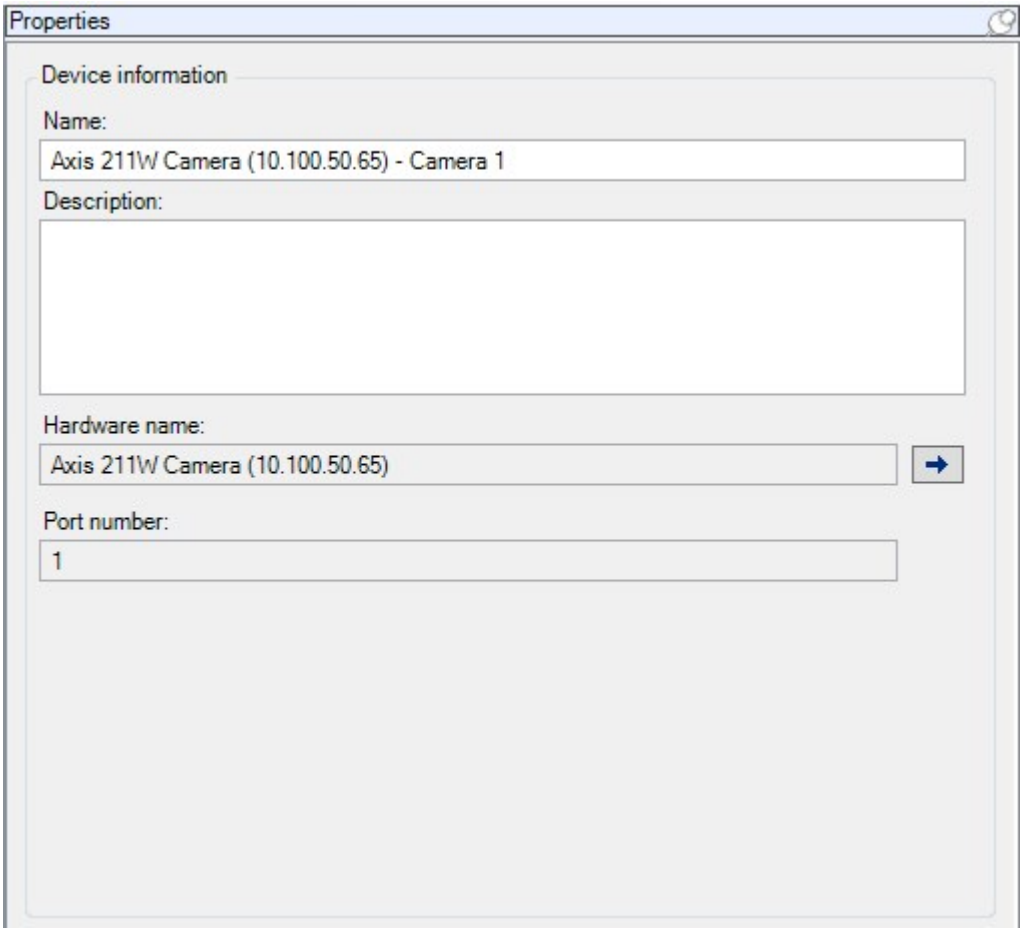
3. ツールバーで保存をクリックします。設定は個別のデバイスに保存され、デバイスグループには保存されません。

サイトナビゲーション: [デバイス]タブ

情報タブ(デバイス)

情報タブ(説明付き)

情報タブで、デバイスに関する基本情報を複数のフィールドで表示および編集することができます。すべてのデバイスに[情報]タブがあります。



情報タブのプロパティ

名前	説明
名前	デバイスがシステムおよびクライアントに一覧されるときにこの名前が使用されます。 デバイスの名前を変更すると、名前はManagement Clientで一括変更されます。
説明	デバイスの説明を入力します(オプション)。 説明は、システム内の複数のリストに表示されます。例えば、概要ペインで名前にマウスポインタを移動すると表示されます。
ハードウェア名	デバイスが接続されているハードウェアの名前を表示します。ここからはフィールドを編集できませんが、その横にある[移動]をクリックして変更することができます。これによりハードウェア情報に移動し、名前を変更できます。
ポート番号	デバイスがハードウェアに接続されているポートを表示します。 デバイスが1つしかないハードウェアでは、ポート番号は通常1になります。複数のチャネルがあるビデオサーバーなどのマルチデバイスハードウェアでは、通常、ポート番号はデバイスが接続されているチャネルを示しています(例、3)。
ショートネーム	カメラにショートネームをつけるには、ここに入力してください。最大文字数は128文字です。 スマートマップを使用している場合、スマートマップ上のカメラに自動的にショートネームが表示されます。または、フルネームが表示されます。
地理座標	カメラの地理的位置を緯度、経度のフォーマットで入力します。入力する値によって、XProtect Smart Clientのスマートマップ上のカメラアイコンの位置が決まります。 このフィールドは主にスマートマップとサードパーティー統合のためのものです。
方向	垂直軸上の真北の点に対するカメラの視線方向を入力します。入力する値によって、XProtect Smart Clientのスマートマップ上のカメラアイコンの位置が決まります。 デフォルト値は0.0.です。 このフィールドは主にスマートマップとサードパーティー統合のためのものです。
視界	視界を度で入力します。入力する値によって、XProtect Smart Clientのスマートマップ上のカメラアイコンの視界が決まります。

名前	説明
	デフォルト値は0.0.です。 このフィールドは主にスマートマップとサードパーティー統合のためのものです。
距離	カメラの深度をメートルまたはフィートで入力します。入力する値によって、XProtect Smart Clientのスマートマップ上のカメラアイコンの深度が決まります。 デフォルト値は0.0.です。 このフィールドは主にスマートマップとサードパーティー統合のためのものです。
ブラウザで位置をプレビューする...	入力した座標が適切であるかどうかを確認するには、ボタンをクリックします。通常お使いのインターネットブラウザの指定の場所でGoogle マップが開きます。 このフィールドは主にスマートマップとサードパーティー統合のためのものです。

設定タブ(デバイス)

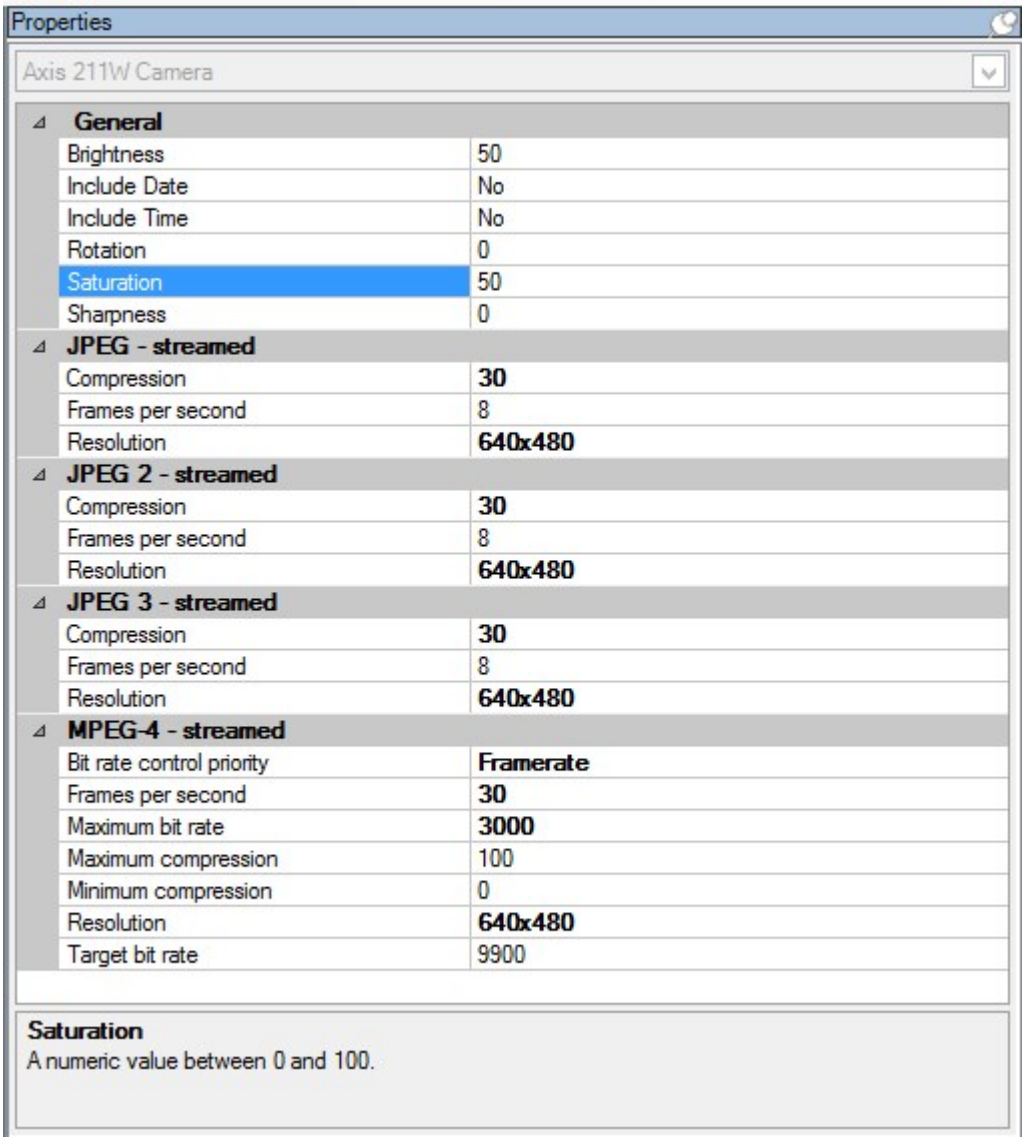
設定タブ(説明付き)

設定タブで、デバイスの設定を複数のフィールドで表示および編集することができます。すべてのデバイスに設定タブがあります。

表に表示される値は、変更可能または読み取り専用です。設定をデフォルト以外の値に変更した場合は、値が太字で表示されます。

テーブルの内容はデバイスドライバーによって異なります。

許可された範囲が設定表の下の情報ボックスに表示されます。



カメラ設定(説明付き)

以下の設定を表示または編集できます。

- デフォルトのフレームレート
- 解像度
- 圧縮
- キーフレーム間のフレームの最大数
- 選択したカメラまたは選択したデバイスグループ内のすべての、カメラの画面の日時およびテキスト表示

カメラのドライバーが設定タブのコンテンツを決定します。ドライバーはカメラのタイプによって異なります。

MJPEGやMPEG-4H.264/H.265などの、複数のストリームタイプをサポートしているカメラでは、マルチストリーミングを使用できます(ページ215のマルチストリーミング(説明付き)を参照)。

設定を変更する場合は、プレビューペインを有効にすると、変更の影響を簡単に確認できます。プレビューペインを使用してフレームレート変更の影響を判断することはできません。その理由は、プレビューペインのサムネイル画像ではオプションダイアログボックスで定義された他のフレームレートを使用しているためです。

キーフレーム間の最大フレームおよびキーフレームモード間の最大フレームの設定を変更すると、XProtect Smart Clientの一部の機能のパフォーマンスが低下するおそれがあります。たとえば、XProtect Smart Clientはビデオ表示の起動にキーフレームが必要なので、キーフレーム間の期間が長いと、XProtect Smart Clientの起動が長引きます。

ストリームタブ(デバイス)

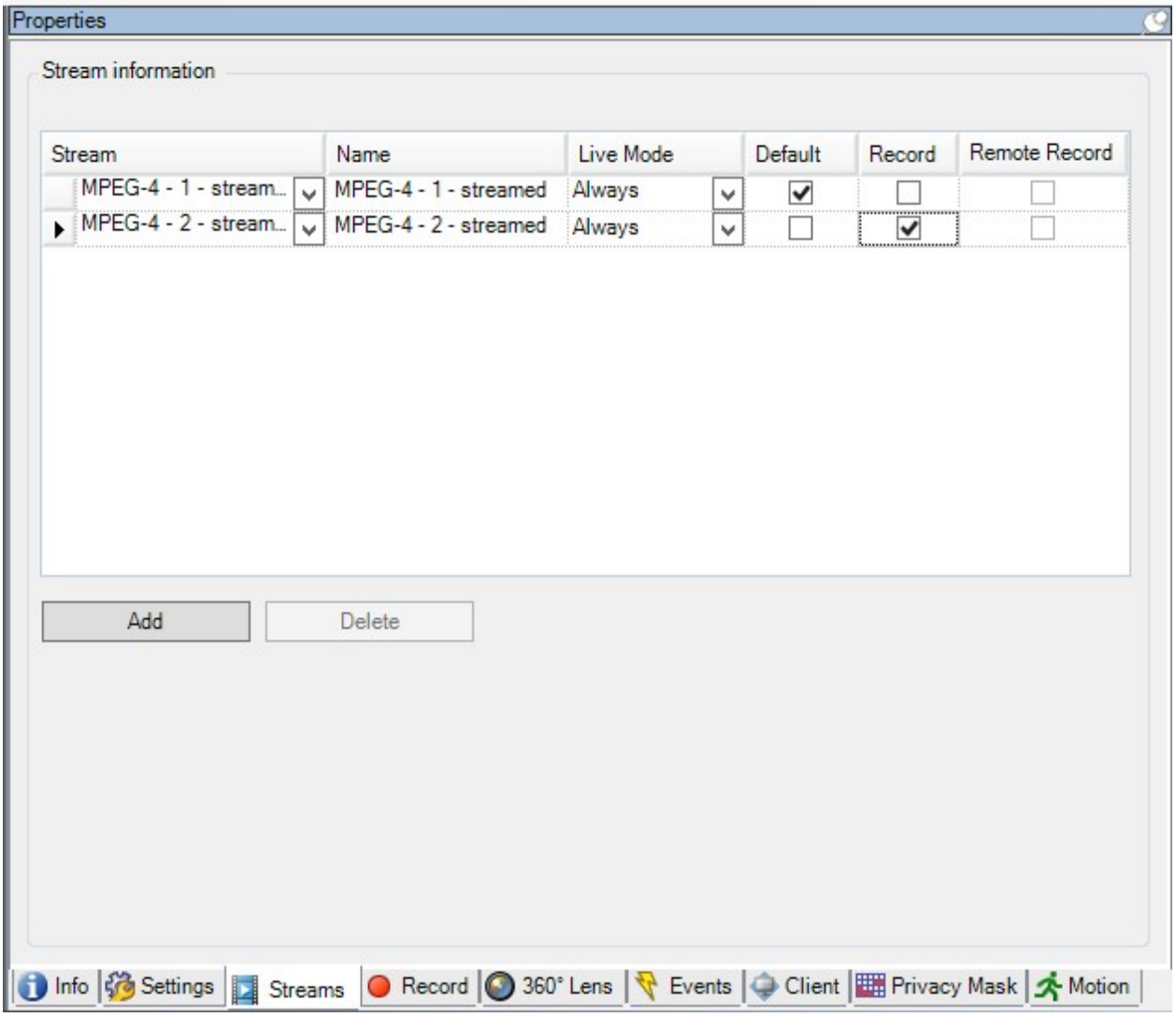
ストリームタブ(説明付き)

以下のデバイスにストリームタブがあります。

- カメラ

ストリームタブはデフォルトで単一のストリームを一覧表示します。このストリームは、選択したカメラのデフォルトのストリームであり、ライブビデオや、録画したビデオで使用されます。

ライブストリームには、カメラがサポートしている複数のライブストリームを設定できますが、録画には一度に1つのストリームしか選択できません。録画に使用するストリームを変更するには、録画するストリームの記録ボックスを選択します。



マルチストリーミング(説明付き)

ライブビデオの視聴および録画ビデオの再生には、必ずしも同じビデオ画質とフレームレートが必要とは限りません。ストリームのいずれか1つをライブ視聴用にして、もう1つを再生目的で使用することもできますし、または複数の独立したライブストリームとして、異なる解像度、エンコーディング、フレームレート設定で使用することも可能です。

ストリーミングを管理するため、そして不要なデータ転送を制限するため、ストリーミングは以下の条件下では開始しません:

- [ストリーム]タブで、[ライブモード]が[必要な場合]に設定されている
- [録画]タブで[録画]が無効になっている
- [モーション]タブで[モーション検出]が無効になっている

これらの条件が満たされた場合、ビデオストリームはクライアントによる視聴時にのみ実行されます。

例1: ライブビデオおよび録画ビデオ:

- ライブビデオの再生では、組織によって高いフレームレートでのH.264が望ましい場合があります。
- 録画ビデオを再生する場合、組織によっては低いフレームレートでのMJPEGを使用することで、ディスクの空き容量を保持できる方が望ましい場合もあります。

例2: ローカルビデオおよびリモートライブビデオ:

- ローカル接続された操作ポイントからライブビデオを視聴する場合、組織によっては可能な限り高品質のビデオを利用するために、高いフレームレートのH.264が望ましい場合があります。
- リモート接続された操作ポイントからライブビデオを視聴する場合、組織によってはネットワーク帯域を保持するために、低いフレームレートのMJPEGが望ましい場合もあります。

例3: アダプティブストリーミング:

- ライブビデオを視聴し、XProtect Smart Clientコンピュータの**CPU**と**GPU**の負荷を軽減するには、組織によっては複数の高フレームレートH.264/H.265を使用するものの、アダプティブストリーミングの使用時にはXProtect Smart Clientによって要求された解像度と一致させるために異なる解像度が使用されることが望ましい場合もあります。詳細については、「ページ276のSmart Clientプロファイルのプロパティ」を参照してください。

> カメラの[クライアント]タブでライブマルチキャストを有効にする場合は、デフォルトのビデオストリームでのみ作動します。

たとえカメラがマルチストリーミングをサポートしていても、カメラによって個々のマルチストリーミングの機能は異なります。詳細については、カメラの文書を参照してください。

カメラが異なるタイプのストリームを提供しているか確認するために、設定タブを確認してください。

ストリームの追加

1. ストリームタブで、追加をクリックします。この操作で、リストに2番目のストリームが追加されます。
2. 名前列で、ストリームの名前を編集します。名前はXProtect Smart Clientに表示されます。
3. ライブモード列で、いつライブストリームが必要かを選択します。
   - 常時：XProtect Smart Clientユーザーがストリームを要求しなくても、ストリームは実行されます。
   - 絶対：ストリームはオフです。例えば、ストリームを高画質で録画したいが帯域幅が必要な場合のみ、これを使用します
   - 必要時：ストリームはXProtect Smart Clientのユーザーが要求したときに開始します。
4. デフォルト列では、どのストリームをデフォルトにするか選択します。
5. 録画列で、このストリームを録画する場合はチェックボックスを選択し、ライブビデオのみに使用する場合はクリアします。
6. [保存]をクリックします。

ストリームが既定または記録に設定されている場合、ストリームは常にライブモード設定とは関係なく実行します。[必要な場合]および[常時]を選択しても同じ結果になります。また、[録画しない]を選択すると、ストリームは実行されますが、ライブ表示はできません。

誰もライブビデオを見ていない場合にストリームを実行しないようにするには、[デフォルトの映像配信開始ルール]を修正し、定義済みのクライアントライブフィードの要求イベントを使用して要求することで開始できます。

録画タブ(デバイス)

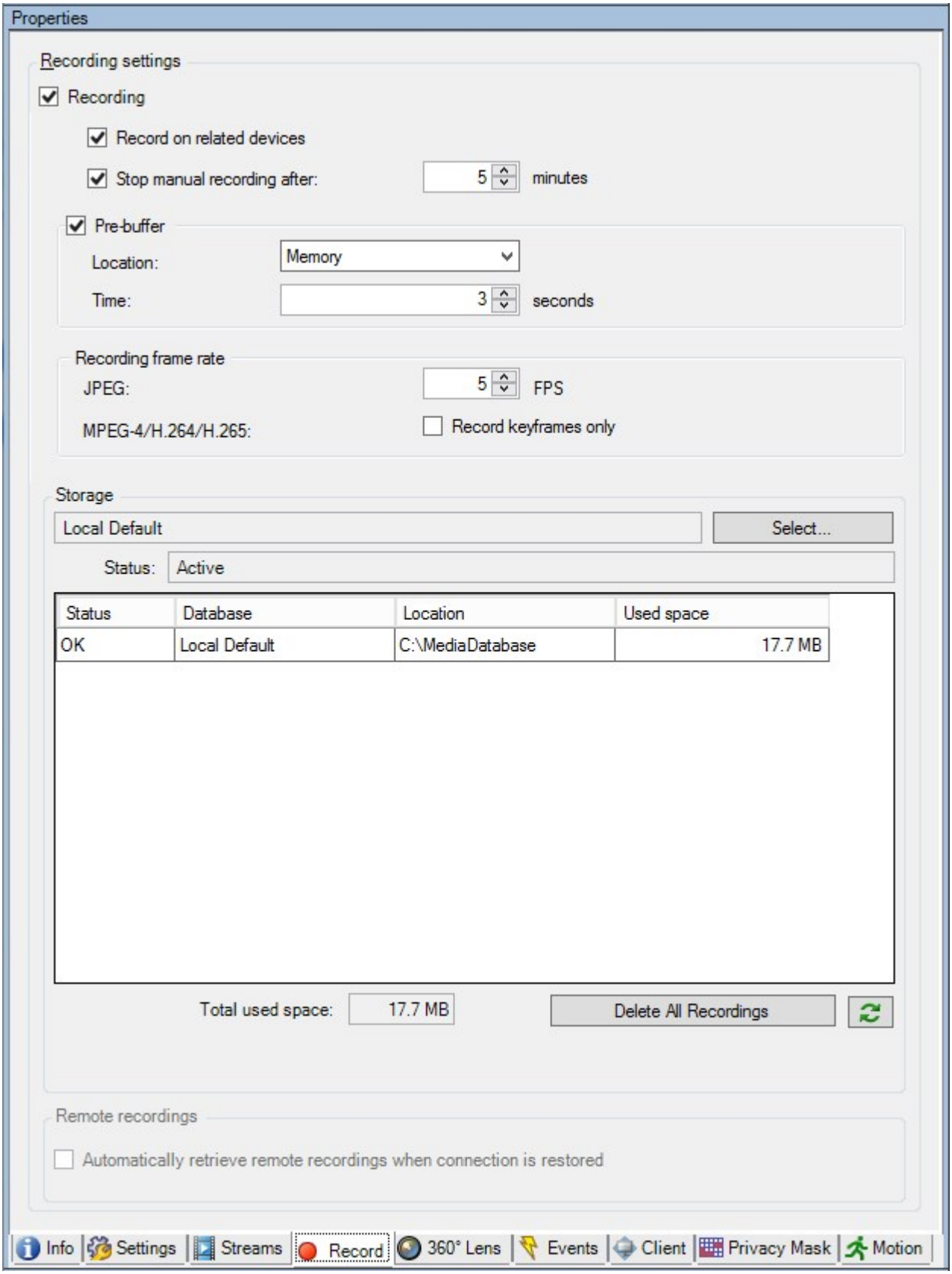
[録画]タブ(説明付き)

以下のデバイスに記録タブがあります。

- カメラ
- マイク
- スピーカー
- メタデータ

デバイスからの記録は、記録を有効にし、記録関連ルール条件が満たされたときにだけ、データベースに保存されます。

デバイスで設定できないパラメータは淡色表示されます。


Properties
Recording settings
Recording
Record on related devices
Stop manual recording after:
5
minutes
Pre-buffer
Location:
Memory
Time:
3
seconds
Recording frame rate
JPEG:
5
FPS
MPEG-4/H.264/H.265:
Record keyframes only
Storage
Local Default
Select...
Status:
Active
Status
Database
Location
Used space
OK
Local Default
C:\MediaDatabase
17.7 MB
Total used space:
17.7 MB
Delete All Recordings
Remote recordings
Automatically retrieve remote recordings when connection is restored
Info
Settings
Streams
Record
360° Lens
Events
Client
Privacy Mask
Motion

記録の有効化と無効化

デフォルトでは記録は有効になっています。記録を有効化/無効化する方法：

1. [サイトナビゲーション]ペインで、レコーディングサーバーを選択します。
2. 概要ペインで関連するデバイスを選択します。
3. 録画タブで、録画チェックボックスを選択します。

> カメラからのデータの録画を可能にするには、デバイスの録画を有効にする必要があります。デバイスの録画を無効にすると、デバイスの録画状態を指定するルールが動作しません。

関連するデバイスで録画を有効にする

カメラデバイスの場合、マイクなど同じレコーディングサーバーに接続されている関連するデバイスの録画を有効にすることができます。これは、カメラが録画する際に、関連するデバイスが録画することを意味します。

新しいカメラデバイスではデフォルトで関連するデバイスの録画が有効になっていますが、必要に応じて無効または有効にすることができます。システムにある既存のカメラデバイスの場合、このチェックボックスはデフォルトでクリアされています。

1. [サイトナビゲーション]ペインで、レコーディングサーバーを選択します。
2. 概要ペインで関連するカメラデバイスを選択します。
3. 録画タブで、関連するデバイスで録画するチェックボックスを選択します。
4. クライアントタブで、このカメラに関連付けるデバイスを指定します。

他のレコーディングサーバーに接続されている関連デバイスで録画を有効にしたい場合は、ルールを作成する必要があります。

プレバッファ(説明付き)

プリバッファは、実際のイベントトリガーが発生する前に音声およびビデオを記録する機能です。これは、例えばドアが開くなど、記録をトリガーするイベントにつながる音声またはビデオを記録したい時に便利です。

システムが接続済みのデバイスから継続的に音声およびビデオストリームを受信し、指定済みのプレバッファ期間一時的に保管するので、プレバッファが可能になります。

- 録画ルールがトリガーされると、ルールとして設定済みプリレコーディング時間に対応する一時レコーディングが恒久的になります
- 録画ルールがトリガーされないと、プレバッファにある一時レコーディングは、定義されたプレバッファ期間後、自動的に削除されます

プリバッファ機能を使用するには、デバイスを有効にしてストリームをシステムに送信する必要があります。

プリバッファをサポートするデバイス

カメラ、マイクおよびスピーカーがプリバッファをサポートします。スピーカーでは、XProtect Smart Clientユーザーがスピーカーで話す機能を使用している場合にのみストリームが送信されます。つまり、スピーカーストリームの記録がどのようにトリガーされるかによって、使用可能なプリバッファがわずかであったり、プリバッファがない場合が生じます。

ほとんどの場合、XProtect Smart Client ユーザーがスピーカーで話す機能を使用している場合に、スピーカーを録画するように設定されています。この場合は、スピーカーのプリバッファは利用できません。

一時プレバッファ録画の保存

一時プレバッファ録画の保存場所は次のいずれかを選択できます。

- メモリ内。プレバッファ期間は15秒までに制限されます。
- ディスク上(メディアデータベース内)。すべての値を選択できます。

ディスクではなくメモリに保存するとシステムパフォーマンスが向上しますが、プレバッファ期間が短くなります。

録画がメモリに保存され、一時レコーディングの一部を恒久的にすると、その他の一時レコーディングは削除され、復元することはできません。残りの録画を保持できるようにする必要がある場合は、録画をディスク上に保存します。

プリバッファの管理

プレバッファの有効化と無効化

プレバッファは、デフォルトでは3秒のプレバッファサイズで有効になっており、メモリに保存されます。

1. プレバッファを有効化/無効化するには、[プレバッファ]チェックボックスを選択または選択解除します。

ストレージ場所とプレバッファ期間の指定

一時プレバッファ録画はメモリ内またはディスク上のいずれかに保存されます。

1. [場所]で、[メモリ]または[ディスク]を選択して、秒数を指定します。

   指定する秒数は、定義済みの様々な記録ルールでの要件に対応するに十分な大きさである必要があります。

   15秒を上回るプレバッファ期間が必要な場合は、[ディスク]を選択します。

2. 場所を[メモリ]に変更すると、期間が自動的に15秒に短縮されます。

ルールでプレバッファを使用

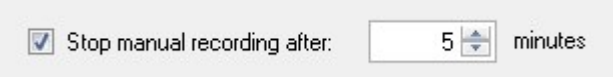
録画をトリガーするルールを作成する場合、録画が実際のイベントよりも少し前に始まるように選択できます(プリバッファ)。

例:以下のルールでは、カメラがモーションを検知する5秒前にカメラでの録画が始まるように指定しています。

プリバッファ録画機能をルールで使用するには、録画されるデバイスのプリバッファ機能を有効にし、プリバッファ長さを少なくともルールで定義した長さと同じに設定する必要があります。

手動記録の管理

デフォルトでは、次の時間が経過すると手動記録を停止が有効になっており、記録時間は5分です。これは、XProtect Smart Clientユーザーが開始したすべての録画が自動的に停止することを保証するためです。



1. 手動記録の自動停止を有効または無効にするには、次の時間が経過すると手動記録を停止チェックボックスをオンまたはオフにします。
2. 有効にする場合は、記録時間を指定します。指定する分数は、システムに負荷をかけ過ぎることなく、さまざまな手動記録の要件に対応するのに十分な長さにする必要があります。

役割に追加：

デバイスタブの役割で、各カメラのクライアントユーザーに対して、手動記録を開始および停止する権限を付与する必要があります。

ルールで使用する：

手動記録関連するルールを作成するときに使用できるイベント：

- 手動録画が開始されました
- 手動録画が停止されました

レコーディングフレームレートを指定する

JPEGのレコーディングフレームレートを指定できます。

- 「レコーディングフレームレート」にレコーディングフレームレート(FPS、フレーム数/秒)を選択または入力します。(JPEG)ボックス。

キーフレームレコーディングの有効化

MPEG-4/H.264/H.265ストリームのキーフレームレコーディングを有効にできます。つまり、ルール設定によって、キーフレームの録画とすべてのフレームの録画を切り替えます。

たとえば、ビューでモーションがないときにシステムにキーフレームを録画させ、モーションが検出された場合にだけすべてのフレームに切り替えてストレージを節約できます。

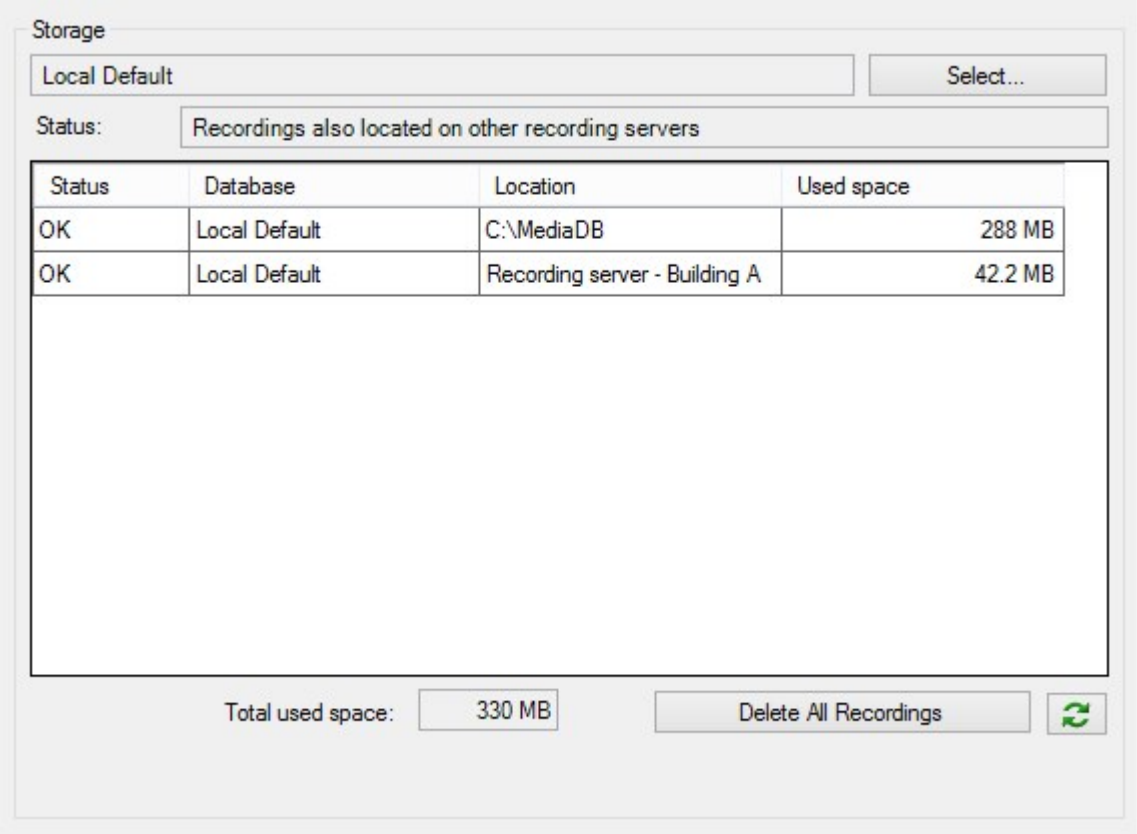
1. キーフレームのみの録画ボックスを選択します。

2. 機能を有効にするルールを設定します。ページ288のアクションおよびアクションの停止(説明付き)を参照してください。

ストレージ(説明付き)

[ストレージ]の下で、デバイス、または同じレコーディングサーバーに追加されたデバイスのグループのデータベースを監視および管理できます。

表の上では、選択されたデータベースとその状態が確認できます。この例では、選択されたデータベースはデフォルトのローカルデフォルトで、ステータスは録画が他のレコーディングサーバーにも存在するです。他のサーバーは建物Aのレコーディングサーバーです。



選択したデータベースで生じ得るステータス

名前	説明
録画は他のレコーディングサーバーにもあります	データベースがアクティブで稼動中であり、他のレコーディングサーバーのストレージにも録画があります。
アーカイブも古いストレージにあります	データベースはアクティブで実行中です。また、アーカイブは他のストレージにもあります。
アクティブ	データベースはアクティブで実行中です。
選択されたデバイスの一部に関するデータは現在他の場所に移動中です	データベースはアクティブで実行中です。グループ内の選択された1つ以上のデバイスで、ある場所から他の場所へデータを移動しています。
デバイスのデータは現在他の場所に移動中です	データベースはアクティブで実行中です。選択されたデバイスで、ある場所から他の場所へデータを移動しています。
フェールオーバーモードで利用可能な情報はありません	データベースがフェールオーバーモードの場合は、データベースのステータス情報を収集できません。

さらにウィンドウの下部には、各データベースのステータス(OK、オフライン古いストレージ)、各データベースの場所、および各データベースが占有する領域が表示されます。

すべてのサーバーがオンラインである場合は、[合計使用スペース]フィールドにストレージ全体で使用される合計領域を表示できます。

[すべての録画を削除]ボタンを使用すると、グループのすべてのデバイスを同じサーバーに追加した場合に、デバイスまたはデバイスグループのすべての録画を削除できます。保護されたデータは削除されません。

ストレージの設定についての詳細は、ページ148のストレージタブ(レコーディングサーバー)を参照してください。

デバイスをストレージ間で移動する

デバイスの新しいストレージ場所を選択するには、[ストレージ]で[選択....]を選択します。

これで、デバイスによる記録先となる別のレコーディングストレージが選択され、そのストレージの構成に従ってアーカイブが行われます。

記録の保存先となる新しい場所を選択しても、既存の記録は移されません。これまでと同じ場所にとどまり、自身が属するストレージの構成にもとづいた状態が示されます。

リモート録画(説明付き)

> リモート録画オプションは、選択されたカメラでエッジストレージがサポートされている場合、または選択されたカメラがMilestone Interconnect設定されている場合にのみ使用できます。

ネットワークに問題が発生した場合に確実にすべての録画を保存するには、[接続が復旧したときに自動的にリモート録画を取得する]を選択します。これにより、接続の再設定時に録画の自動取得が有効になります。

選択されたハードウェアのタイプによって、どこから記録を取得するかが決まります。

- ローカル録画ストレージのあるカメラの場合、録画はカメラのローカル録画ストレージから取得されます。
- Milestone Interconnectリモートシステムの場合、録画はリモートシステムのレコーディングサーバーから取得されます。

自動取得とは別に、以下の機能を使用できます。

- 手動録画
- は、<devices>ルールからリモート録画を取得および保存します。
- は<device>ルールから、<start and end time>間のリモート録画を取得し保存します

モーションタブ(デバイス)

モーションタブ(説明付き)

以下のデバイスにモーションタブがあります。

- カメラ

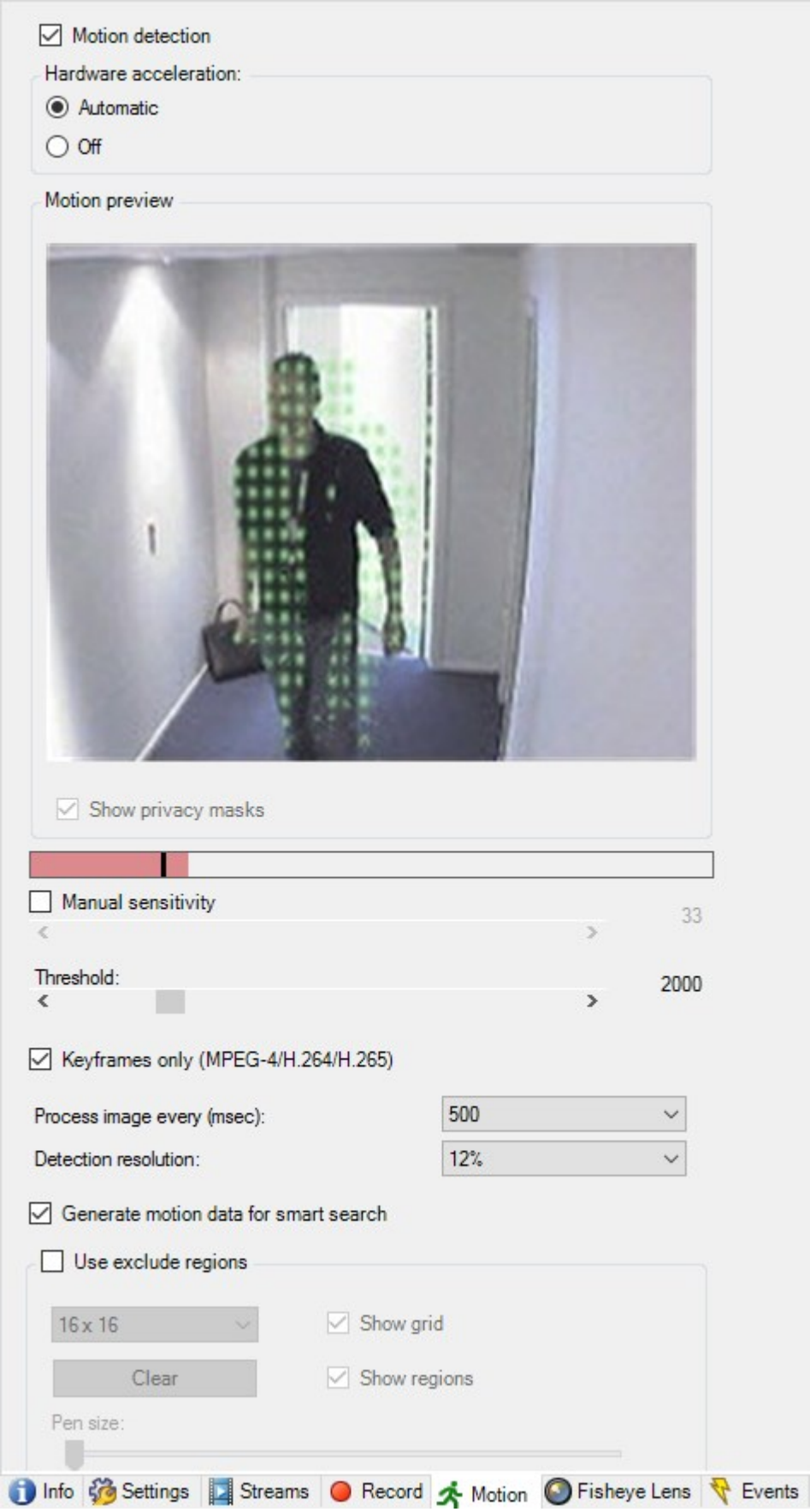
モーションタブでは、選択したカメラのモーション検知を有効にして、設定することができます。モーション検知の設定は、システムの重要な部分です。モーション検知の設定により、システムでモーションイベントを生成するタイミング、さらに通常はビデオを録画するタイミングを決定します。

それぞれのカメラに最適なモーション検知の構成が得られるようにあらかじめ調整しておくことで、後になって不必要な録画などを避けるのに役立ちます。カメラの物理的な位置によっては、異なる物理的条件(昼/夜、強風/無風など)でモーション検知の設定をテストすることをお勧めします。

カメラのモーション検知を設定する前に、Milestoneでは、カメラの画質の設定(解像度、ビデオコーデック、ストリーム設定など)を設定タブで設定しておくことを強くお勧めします。後で画質の設定を変更すると、必ずモーション検知の設定を変更後にテストしなくてはならなくなるからです。

プライバシープロテクションタブに、常設のプライバシーマスクを定義したエリアがある場合(ページ252のプライバシーマスクタブ(デバイス)を参照)には、モーションタブでプライバシーマスクを表示するチェックボックスを選択することで、プライバシーマスクを表示する選択をすることができます。

常設のプライバシーマスクでカバーされている領域にはモーション検知はありません。


Motion detection
Hardware acceleration:
Automatic
Off
Motion preview
Show privacy masks
Manual sensitivity
33
Threshold:
2000
Keyframes only (MPEG-4/H.264/H.265)
Process image every (msec):
500
Detection resolution:
12%
Generate motion data for smart search
Use exclude regions
16 x 16
Show grid
Clear
Show regions
Pen size:
Info
Settings
Streams
Record
Motion
Fisheye Lens
Events

カメラのグループのすべての設定を構成できますが、一般的にはカメラごとに除外領域を設定します。

モーション検知の有効化と無効化

[ツール] > [オプション] > [一般]タブで、カメラのモーション検知のデフォルト設定を指定できます。

後からカメラのモーション検知を有効化または無効化する方法:

- [モーション]タブの[モーション検知]チェックボックスを選択/解除します

> カメラのモーション検知を無効にすると、カメラのモーション検知関連のルールは機能しません。

モーション検知設定の指定

カメラのビューでモーションとみなされるために必要となる変更の量を設定することができます。例えば、モーション検知分析間の間隔や、モーションが無視されるビューの領域を指定できます。モーション検知検出の精度を調整し、それによってシステムリソース上の負荷を調整することもできます。

ハードウェアアクセラレーション(説明付き)

ハードウェアアクセラレーションによるビデオモーション検知を有効にするには自動化を選択します。これは、カメラを追加した際のデフォルト設定です。使用可能な場合、レコーディングサーバーはGPUリソースを使用しています。これによってビデオモーション解析中のCPU負荷を軽減し、レコーディングサーバーの一般的なパフォーマンスを向上します。

GPUリソースがオンの状態でのハードウェアアクセラレーションによるビデオモーション検出:

- Intel Quick SyncをサポートするIntel CPU。
- NVIDIA® あなたの録画サーバーに接続されているアダプターを表示 。

異なったリソース感のロードバランスは自動的に行われます。システムモニターノードにおいて、NVIDIA GPUリソースにおける現行のモーション分析ロードがシステムモニタースレッドノードの特定のリミット内に納まっている場合、検証が可能です。NVIDIA GPUロードの指標は以下の通りです:

- NVIDIAデコード
- NVIDIAメモリ
- NVIDIAレンダリング

> もしロードが高すぎる場合は、複数のNVIDIAディスプレイアダプタをインストールして、GPUリソースをお使いのPCに追加します。Milestoneはお使いのNVIDIAディスプレイアダプターでの、スケーラブル・リンク・インターフェイス(SLI)構成の使用を推奨しません。

NVIDIA製品は異なったコンピュート能力を持っています。お使いのNVIDIA製品が、Milestone XProtectシステムで使用されているコーデック向けハードウェアアクセラレーションをサポートしているか確認するためには、以下の表で、コンピュート能力バージョンに対してサポートされているコーデックを確認します。

お使いのNVIDIA製品におけるコンピュート能力のバージョンを確認するには、NVIDIA のウェブサイト (https://developer.nvidia.com/cuda-gpus/) にアクセスしてください。

コンピュート能力	アーキテクチャ	H.264	H.265
3.x	Kepler	✓	-
5.x	Maxwell	✓	-
6.x	Pascal	✓	✓
7.x	Volta	✓	✓

ビデオモーション検出が特定のカメラのハードウェアアクセラレーションであるかどうかを確認するには、レコーディングサーバーのログファイルの監視を有効にします。レベルをデバッグに設定し、診断法をDeviceHandling.logにします。ログは次のパターンに従います。
[time] [274] DEBUG - [guid] [name] Configured decoding: 自動：実際のデコーディング：Intel/NVIDIA

レコーディングサーバーのOSのバージョンとCPUの世代がハードウェアアクセラレーションビデオモーション検出のパフォーマンスに影響する場合があります。古いバージョンではGPUメモリ割り当てがしばしば障害となります (一般的な限界値は 0.5 GBから1.7 GBの間です)。

Windows 10 / Server 2016 および第6世代 CPU (Skylake) 以降のシステムは、GPUにシステムメモリの50%を割り当てることによってこの障害を低減または除去しています。

第6世代のIntel製CPUはH.265のハードウェアアクセラレーションデコーディングをサポートしているため、このバージョンのCPUのパフォーマンスはH.264と同程度になります。

手動感度の有効化

感度設定は、画像の中の各ピクセル数がどれだけ変化すればモーションと見なすかを決定します。

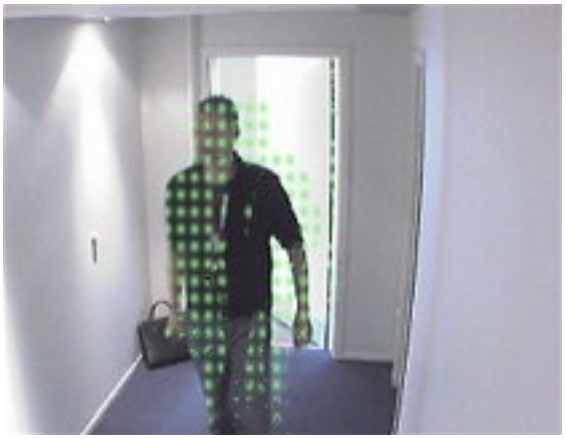
1. モーションタブの手動感度チェックボックスを選択/解除します。
2. スライダーを左に動かすと感度レベルが上がり、右に動かすと感度レベルが下がります。

   感度レベルが高くなるほど、より少ない各ピクセルの変化でもモーションと見なされます。

   感度レベルが低くなるほど、各ピクセルの変化がより多くなった際にモーションと見なされます。

   モーションが検知されたピクセルは、プレビュー画像で緑色に強調表示されます。

3. モーションと見なされたものだけが強調表示されるよう、スライダーの位置を選択します。



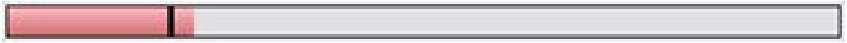
スライダーの右側の数により、カメラ間の正確な感度設定を比較することができます。

閾値の指定

モーション検知閾値は、画像の中のピクセル数がどれだけ変化すればモーションと見なすかを決定します。

1. スライダーを左に動かすとモーションレベルが上がり、右に動かすとモーションレベルが下がります。
2. モーションと見なされたものだけが検知されるよう、スライダーの位置を選択します。

モーション表示バーの黒い垂直線はモーション検知の閾値を示します。検知されたモーションが選択された検知閾値レベルを超える場合、バーの色が緑から赤に変わり、検知されたことを示します。



モーション検知バーの色は、しきい値を超えると緑から赤に変わり、モーションが検知されたことを示します。

キーフレーム設定の選択

モーション検知をキーフレームのみで行うか、ビデオストリーム全体に行うかを決定します。MPEG-4/H.264/H.265のみに適用されます。

キーフレームでのモーション検知により、分析の実施で使用される処理能力の消費量を減らします。

キーフレームのみにモーション検知を行う場合は、キーフレームのみ**(MPEG-4/H.264/H.265)**を選択します。

画像処理間隔を選択

システムがモーション検知分析を実施する頻度を選択できます。

画像処理間隔**(**ミリ秒**)**リストで、

- 間隔を選択します。例えば、1000ミリ秒ごとにすると1秒間に1回となります。デフォルト値は500ミリ秒ごとです。

  ここで設定した間隔よりも実際のフレームレートが高い場合に間隔が適用されます。

検出解像度の指定

画像の分析を行う範囲を限定するパーセンテージ(たとえば25%)を指定すると、モーション検知のパフォーマンスを最適化することができます。25%の分析ということは、すべてのピクセルではなく、画像のピクセルを4つ毎に1つだけ分析することになります。

検知を最適化すると、分析を実行する際の処理能力にかかる消費量は低減できますが、モーション検知の正確性も低下することを意味しています。

- 検出解像度リストから、希望の検出解像度を選択します。

スマート検索モーションデータの生成

スマート検索モーションデータの生成が有効な場合、モーション検知で使用される画像のモーションデータが生成されます。たとえば、キーフレームでだけモーション検知を選択すると、モーションデータはキーフレームでだけ生成されます。

追加のモーションデータにより、ユーザーは、スマート検索機能を使用して、画像の選択領域のモーションに基づいて、該当する録画をすばやく検索できます。このシステムは、常設のプライバシーマスクでカバーされている領域においてはモーションデータを作成しません。除去可能なプライバシーマスクの領域のみです(ページ252のプライバシーマスクタブ(デバイス)タブ(説明付き)を参照)。

モーション検知閾値と除外領域は、生成されたモーションデータに影響しません。

ツール > オプション > 一般タブで、カメラのスマート検索データの生成のデフォルト設定を指定できます。

領域の除外を指定

カメラのビューのうち、特定の領域のモーション検知を無効にできます。

> プライバシーマスクはモーション検知から除外されます。それらを表示するには、プライバシーマスクを表示するチェックボックスを選択してください。

特定の領域のモーション検知を無効にすると、例えば、カメラの撮影範囲に風で揺れる木があったり、背景に自動車が定期的に通過する場合など、無関係なモーションの検知を避けることができます。

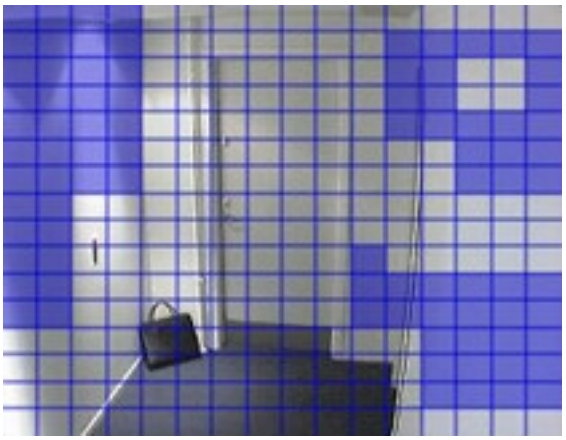
領域の除外をPTZカメラで使用している場合、カメラをパン/チルト/ズームしても、領域は対象ではなくカメラ画像にロックされているので、除外された領域はそれに合わせて移動しません。

1. 領域の除外を使用するには、領域の除外を使用チェックボックスを選択します。

   グリッドはプレビュー画像を選択可能なセクションに分割します。

2. 領域の除外を定義するには、マウスの左ボタンを押しながら、プレビュー画像の必要なエリアをマウスのポインタでドラッグします。マウスを右クリックすると、グリッドで区切られた部分がクリアできます。

必要な数の除外領域を定義できます。除外領域は青色で表示されます：



青い除外領域はモーションタブのプレビュー画像にのみ表示されます。Management Clientやアクセスクライアントの他のプレビュー画像では青く表示されません。

プリセットタブ(デバイス)

プリセットタブ(説明付き)

以下のデバイスにプリセットタブがあります。

- プリセット位置がサポートされているPTZカメラ

プリセットタブで、プリセット位置を作成またはインポートできます。例：

- イベント発生時にPTZ(パン/チルト/ズーム)カメラを特定のプリセット位置に移動させるためのルール
- 複数のプリセット位置間でPTZカメラを自動的に移動させるパトロール
- XProtect Smart Clientユーザーによる手動制御向け

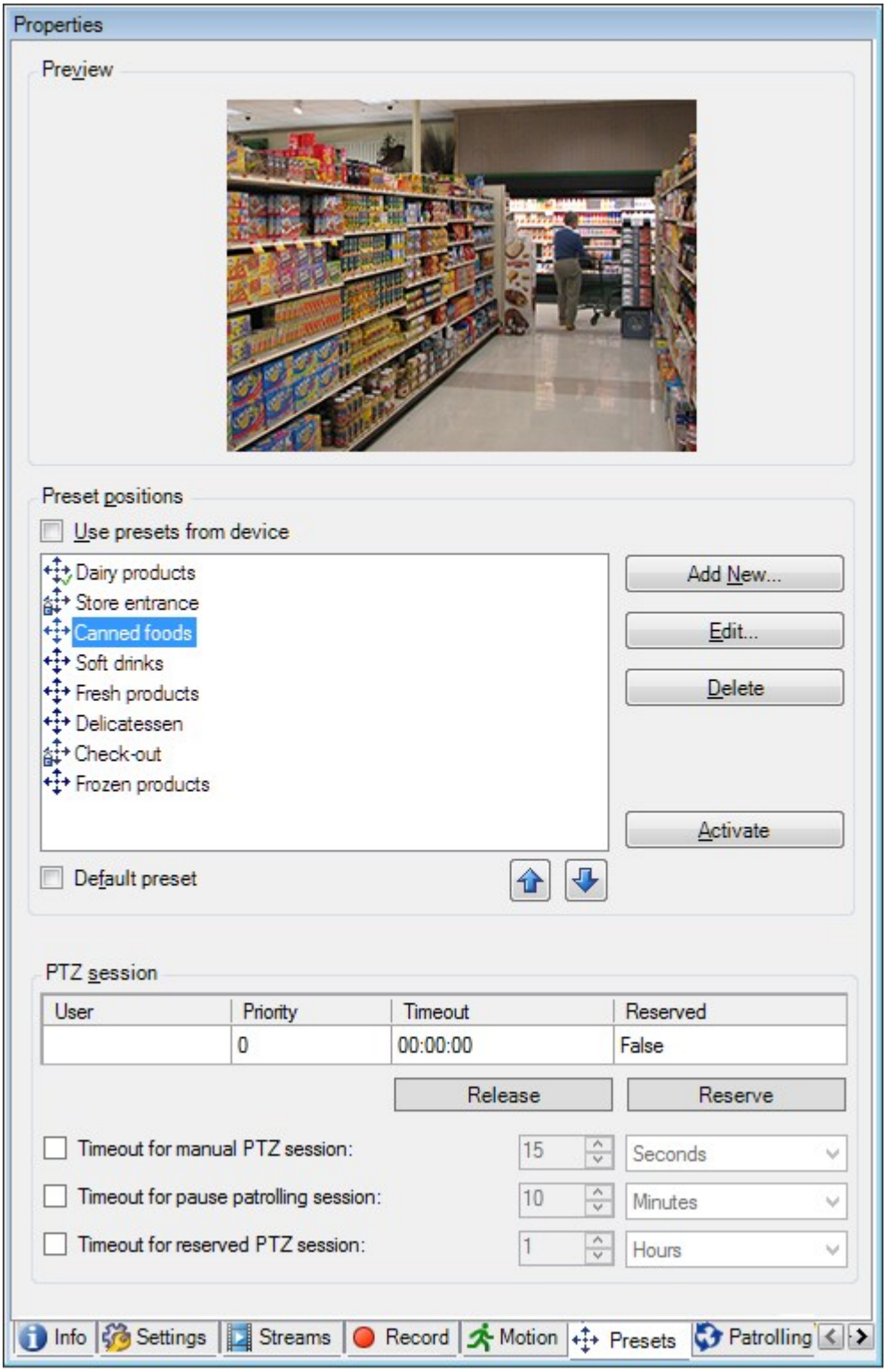
XProtect Smart Clientのユーザーまたは制限されたセキュリティ権限のユーザーがこのプリセットを更新できないようにする場合は、プリセット位置をロックできます。ロックされたプリセットには アイコンが表示されます。

予約されたPTZセッションを実行するセキュリティ権限を持つ管理者(ページ239の予約済みPTZセッション(解説済み)」)は、このモードでPTZカメラを実行できます。これにより、他のユーザーはカメラを制御できなくなります。十分な権限があれば、他のユーザーの予約済みPTZセッションをリリースできます(「ページ239のPTZセッションのリリース」を参照)。

［セキュリティ全般］タブ(「ページ343のセキュリティ全般タブ(役割)」を参照) または［PTZ］タブ(「ページ372のPTZタブ(役割)」を参照) でPTZ権限を役割に割り当てます。

PTZセッション領域で、現在パトロールを実行しているか、ユーザーが制御を取得したかどうかを監視できます。(「ページ240のPTZセッションの優先度」を参照)

カメラのPTZセッションタイムアウトも変更できます。


Properties
Preview
Preset positions
Use presets from device
Dairy products
Store entrance
Canned foods
Soft drinks
Fresh products
Delicatessen
Check-out
Frozen products
Add New...
Edit...
Delete
Activate
Default preset
PTZ session
User
Priority
Timeout
Reserved
0
00:00:00
False
Release
Reserve
Timeout for manual PTZ session:
15
Seconds
Timeout for pause patrolling session:
10
Minutes
Timeout for reserved PTZ session:
1
Hours
Info
Settings
Streams
Record
Motion
Presets
Patrolling

ページ234のプリセット位置を追加する(タイプ1)

ページ236のカメラからのプリセット位置を使用します(タイプ2)

ページ236のデフォルトのプリセット位置の割り当て

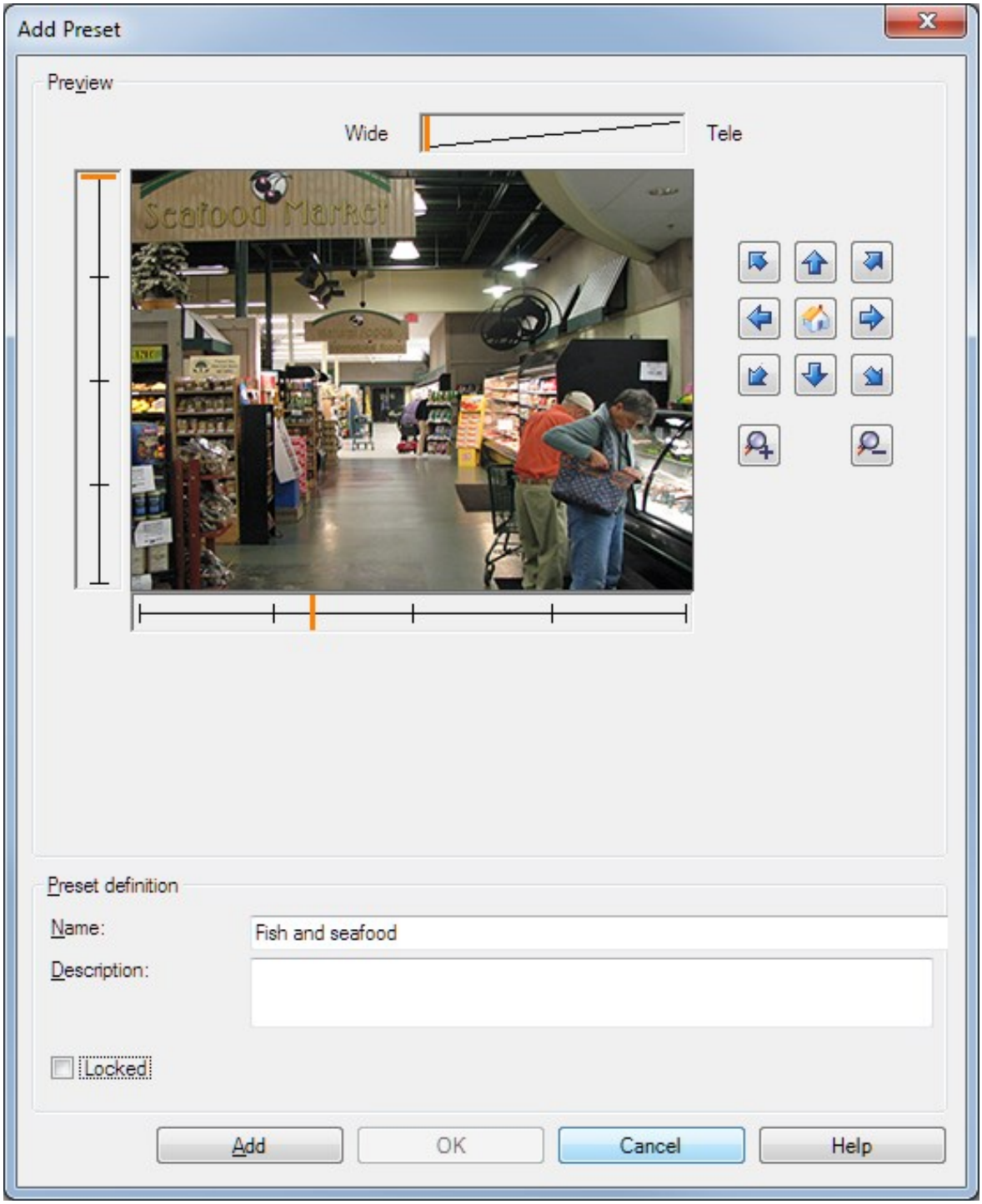
ページ236のプリセット位置を編集する(タイプ1のみ)

ページ239のプリセット位置をテストする(タイプ1のみ)

プリセット位置を追加する(タイプ1)

プリセット位置をカメラに追加する方法：

1. [新規追加] をクリックします。プリセットの追加ウィンドウが表示されます。



2. プリセットの追加ウィンドウはカメラからのライブプレビュー画像を表示します。ナビゲーションボタンおよび/またはスライダーを使用してカメラを必要な位置に移動します。

3. 名前フィールドにプリセット位置の名前を入力します。

4. オプションとして、[説明]フィールドにプリセット位置の説明を入力します。
5. プリセット位置をロックする場合は、[ロック]を選択します。十分な権限を持つユーザーだけが後から位置をロック解除できます。
6. [追加]をクリックしてプリセットを指定します。任意のプリセットになるまで、追加し続けます。
7. OK をクリックします。プリセットの追加ウィンドウが閉じ、プリセット位置がプリセットタブのカメラの利用可能なプリセット位置のリストに追加されます。

カメラからのプリセット位置を使用します(タイプ2)

プリセット位置をシステムに指定する代わりに、PTZカメラのプリセット位置をカメラ自体で指定できます。通常は、デバイス固有の設定Webページにアクセスして定義します。

1. プリセットをデバイスから使用を選択して、プリセットをシステムにインポートします。

   以前にカメラに定義したプリセットは削除され、定義済みルールおよびパトロールスケジュールに影響します。また、XProtect Smart Clientユーザーが利用可能なプリセットは削除されます。
2. 削除をクリックするとユーザーが必要ではないプリセットを削除します。
3. プリセットの表示名を変更したい場合は [編集]をクリックします(「ページ238のプリセット位置をテストする(タイプ2のみ)」を参照)。
4. このようなデバイス定義済みプリセットを後で編集する場合は、カメラで編集してから再インポートします。

デフォルトのプリセット位置の割り当て

必要に応じて、PTZカメラのプリセット位置のいずれかをカメラのデフォルトのプリセット位置に割り当てることができます。

デフォルトのプリセット位置が設定されていると、PTZカメラが手動で操作された後など、特定の状況下でPTZカメラがデフォルトのプリセット位置に移動するように指定して、ルールを定義できるため便利です。

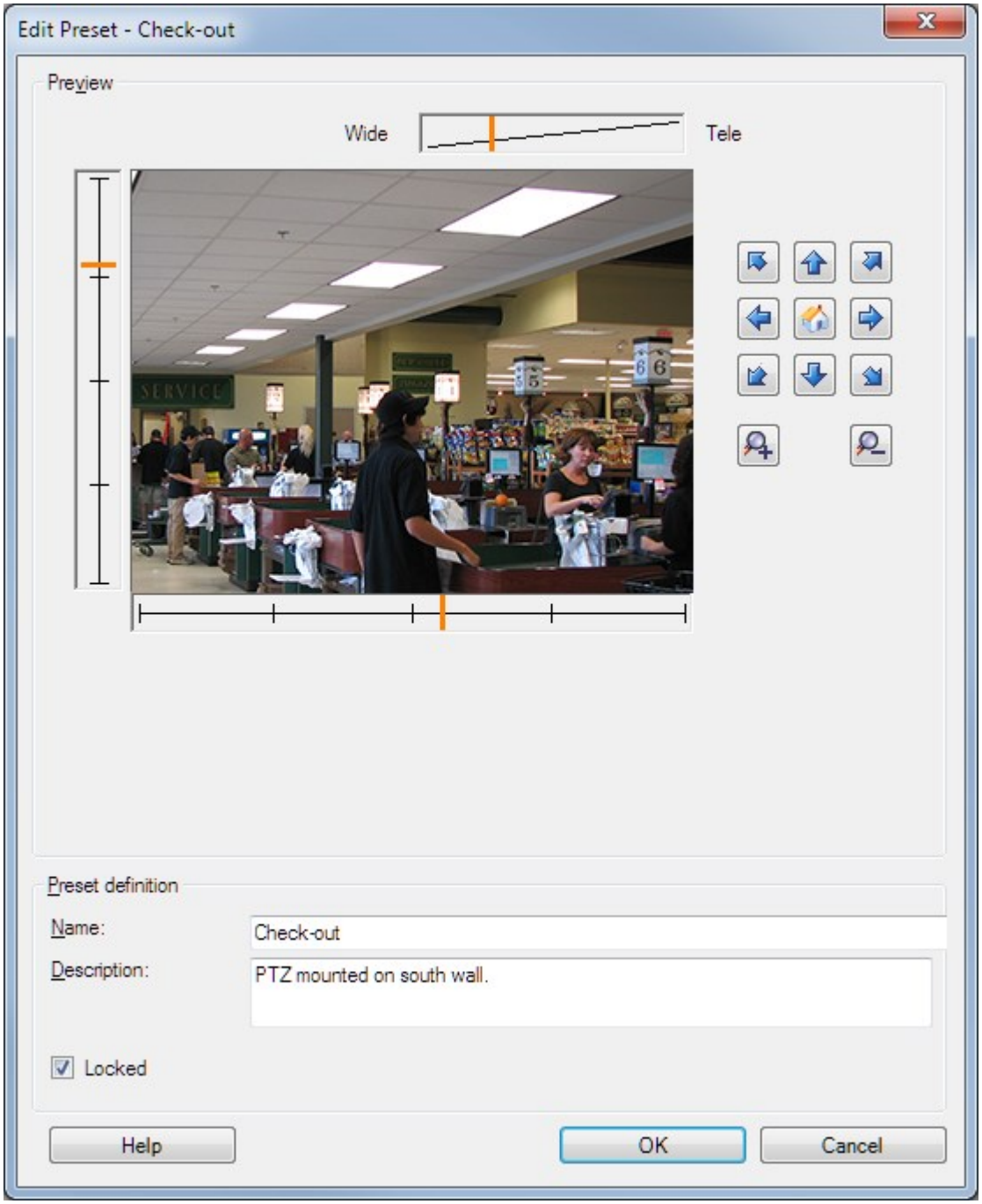
1. プリセット位置をデフォルトとして割り当てるには、定義済みのプリセット位置リストからプリセットを選択します。
2. リストの下にあるデフォルトのプリセットチェックボックスを選択します。

デフォルトのプリセット位置として指定できるのは、1つだけです。

プリセット位置を編集する(タイプ1のみ)

システムで定義済みの既存のプリセット位置を編集する方法:

1. プリセットタブのカメラで利用可能なプリセット位置のリストから、プリセット位置を選択します。
2. [編集] をクリックします。これにより、プリセットの編集ウィンドウが開きます。



3. [プリセットの編集]ウィンドウにはプリセット位置からのライブビデオを表示します。ナビゲーションボタンおよび/またはスライダーを使用して、プリセット位置を必要に応じて変更します。
4. 必要に応じて、プリセット位置の名前/番号および説明を変更します。

5. プリセット位置をロックする場合は、[ロック]を選択します。十分な権限を持つユーザーだけが後から位置をロック解除できます。

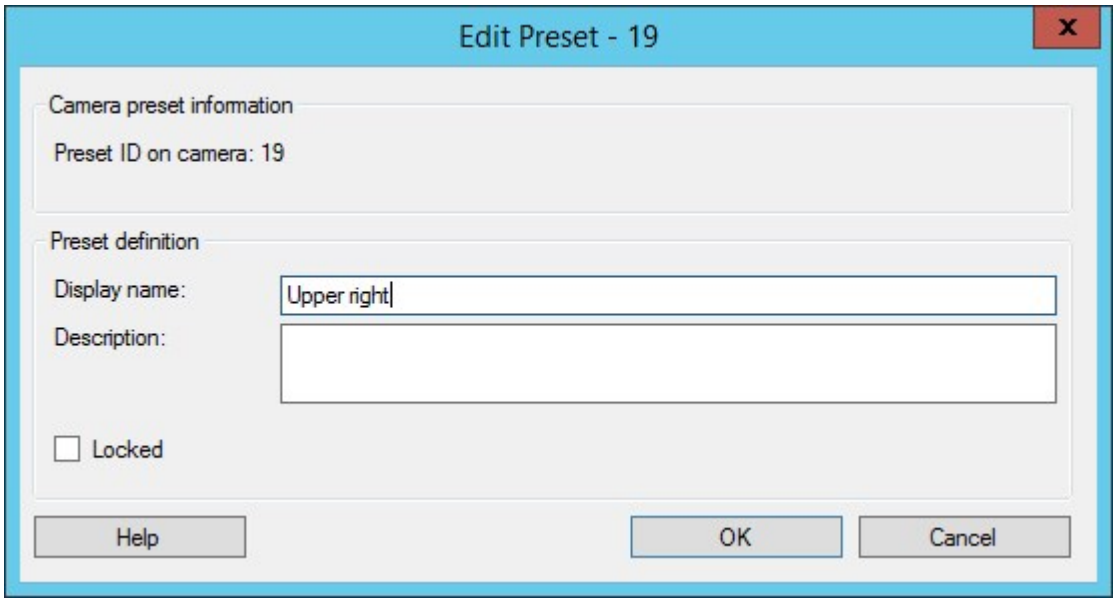
6. OK をクリックします。

プリセット位置をテストする(タイプ2のみ)

カメラで定義されたプリセット位置の名前を編集するには：

1. プリセットタブのカメラで利用可能なプリセットのリストから、プリセット位置を選択します。

2. [編集] をクリックします。これにより、プリセットの編集ウィンドウが開きます。



3. 必要に応じて、プリセット位置の名前を変更し、説明を追加します。

4. プリセット名をロックする場合は、ロックを選択します。XProtect Smart Clientのユーザーまたは制限されたセキュリティ権限のユーザーがこのプリセット名を更新またはプリセットを削除できないようにする場合は、プリセット名をロックできます。ロックされたプリセットには アイコンが表示されます。十分な権限を持つユーザーだけが後からプリセット名をロック解除できます。

5. OK をクリックします。

プリセット位置のロック

XProtect Smart Clientのユーザー、または制限されたセキュリティ権限のユーザーがこのプリセットを更新または削除できないようにする場合は、プリセット位置をロックできます。ロックされたプリセットには アイコンが表示されます。

プリセットのロックは、追加作業(「ページ234のプリセット位置を追加する(タイプ1) 」を参照) と編集作業(「ページ236のプリセット位置を編集する(タイプ1のみ) 」を参照) の一環として行います。

プリセット位置をテストする(タイプ1のみ)

1. プリセットタブのカメラで利用可能なプリセット位置のリストから、プリセット位置を選択します。
2. 実行をクリックします。
3. カメラが選択されたプリセット位置に移動します。

予約済みPTZセッション(解説済み)

監視システムによっては、PTZセッションを予約できます。

予約されたPTZセッションを実行するセキュリティ権限を持つ管理者は、このモードでPTZカメラを実行できます。これにより、他のユーザーはカメラを制御できなくなります。予約済みPTZセッションでは、標準PTZ優先度システムが無視され、より高いPTZ優先度のユーザーがセッションを中断しないようになります。

XProtect Smart ClientとManagement Clientの両方から予約済みPTZセッションでカメラを操作できます。

PTZセッションの予約は、他のユーザーによって中断されずに、PTZカメラまたはそのプリセットで緊急の更新またはメンテナンスを行う必要がある場合に有効です。

> 自分よりも高い優先度のユーザーがカメラを制御している場合や、別のユーザーが既にカメラを予約している場合は、予約済みPTZセッションを開始できません。

PTZ セッションのリリース

[リリース]ボタンを使用すると、他のユーザーがカメラを制御できるように、現在のPTZセッションをリリースできます。[リリース]をクリックすると、PTZセッションがただちに終了し、最初のユーザーがカメラを操作できます。

セキュリティ権限のPTZセッションのリリースが割り当てられた管理者には、いつでも他のユーザーの予約済みPTZセッションをリリース権限があります。たとえば、PTZカメラまたはプリセットを維持する必要がある場合や、他のユーザーが誤って緊急の状況でカメラをブロックした場合などに有用です。

PTZセッションタイムアウトの指定

必要な権限を持つManagementClientおよびXProtectSmartClientユーザーは、PTZカメラのパトロールを手動で中断できます。

定期パトロールがシステム上のすべてのPTZカメラで再開される前に経過する時間を指定できます。

1. [ツール]>[オプション]を選択します。
2. [オプション]ウィンドウの[全般]タブの次の場所で時間を選択します。
   - 手動PTZセッションのタイムアウトリスト(デフォルトは15秒)。
   - パトロールセッションを一時停止するタイムアウトリスト(デフォルトは10分)。
   - 予約されたPTZセッションのタイムアウトリスト(デフォルトは1時間)。

   この設定は、システムのPTZカメラすべてに適用されます。

各カメラのタイムアウトは個別に変更できます。

1. [サイトナビゲーション]ペインで、[カメラ]をクリックします。
2. 概要ペインで、カメラを選択します。
3. [プリセット]タブの次の場所で時間を選択します。
   - 手動PTZセッションのタイムアウトリスト(デフォルトは15秒)。
   - パトロールセッションを一時停止するタイムアウトリスト(デフォルトは10分)。
   - 予約されたPTZセッションのタイムアウトリスト(デフォルトは1時間)。

   設定はこのカメラにのみ適用されます。

PTZセッションの優先度

PTZセッション表には、PTZカメラの現在のステータスを示します。

名前	説明
ユーザー	[予約]ボタンを押し、現在PTZカメラを制御しているユーザーを表示します。 パトロールセッションがシステムによってアクティブ化された場合は、パトロールと表示されます。
優先度	ユーザーのPTZ優先度が表示されます。自分よりも低い優先度のユーザーからのみPTZセッションを取得できます。
タイムアウト	現在のPTZセッションの残り時間が表示されます。
予約	現在のセッションが予約済みPTZセッションであるかどうかを示します。 • 設定あり: 予約 • 設定無し: 予約されていません

各PTZカメラの次のタイムアウトを変更できます。

名前	説明
手動PTZセッションのタイムアウト	タイムアウトをデフォルト期間から変える場合には、このカメラの手動PTZセッションのタイムアウトを指定します。[オプション]の下の[ツール]メニューでデフォルト期間を指定します。
一時停止パトロールPTZのタイムアウト	タイムアウトをデフォルト期間から変える場合には、このカメラの一時停止パトロールPTZセッションのタイムアウトを指定します。[オプション]の下の[ツール]メニューでデフォルト期間を指定します。
予約済みPTZセッションのタイムアウト	タイムアウトをデフォルト期間から変える場合には、このカメラの予約済みPTZセッションのタイムアウトを指定します。[オプション]の下の[ツール]メニューでデフォルト期間を指定します。

パトロールタブ(デバイス)

パトロールタブ(説明付き)

以下のデバイスにパトロールタブがあります。

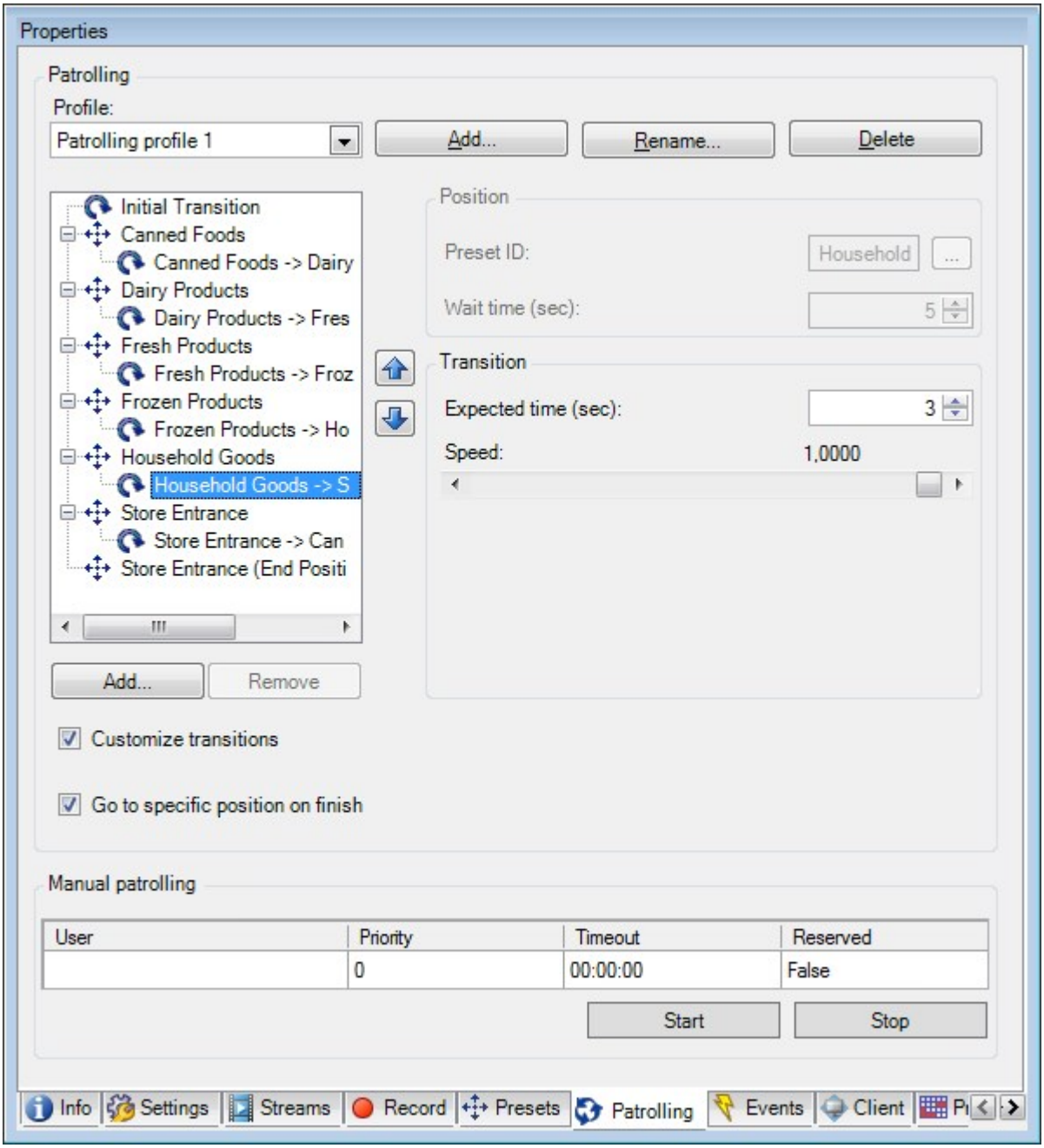
- PTZカメラ

パトロールタブでは、パトロール設定を作成して、PTZ(パン/チルト/ズーム)カメラによる多数のプリセット位置間の自動移動を設定できます。
パトロールを実行する前には、プリセットタブで2つ以上のプリセット位置をカメラで指定する必要があります。

パトロール設定では、パトロールの実行方法を定義します。これには、カメラがプリセット位置間を移動する順序や、カメラが各位置に停止する時間が含まれます。作成できるパトロール設定の数に制限はなく、作成したパトロール設定はルールで使用できます。例えば、1つのパトロール設定が日中の営業時間中に使用され、別のプロファイルが夜間に使用されるように指定するルールを作成できます。

たとえば、ルールでパトロール設定を適用する場合は、手動パトロールでパトロール設定をテストできます。PTZ優先度が高い場合は、手動パトロールを使用して、別のユーザーまたはルールによって有効にされたパトロールからパトロールを取得することもできます。

[手動パトロール]領域で、現在パトロールを実行しているか、ユーザーが制御を取得したかどうかを監視できます。



パトロールタブ、カスタマイズされた旋回動作を含むパトロール設定を表示。

ページ243のパトロール設定の追加

ページ243のパトロール設定でのプリセット位置の指定

ページ244の各プリセット位置での時間を指定

ページ244の旋回動作(PTZ)をカスタマイズ

ページ245の終了位置の指定

手動PTZセッションのタイムアウトを指定します(ページ231のプリセットタブ(デバイス)を参照)

パトロール設定の追加

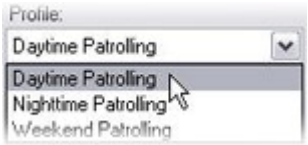
ルールで使用するプロファイルの追加：

1. [追加] をクリックします。プロファイルの追加ダイアログボックスが表示されます。
2. プロファイルの追加ダイアログボックスで、パトロール設定の名前を入力します。
3. OK をクリックします。名前が一意ではない場合は、ボタンは無効です。

   新しいパトロール設定がプロファイルリストに追加されました。これで、プリセット位置とパトロール設定の他の設定を指定できます。

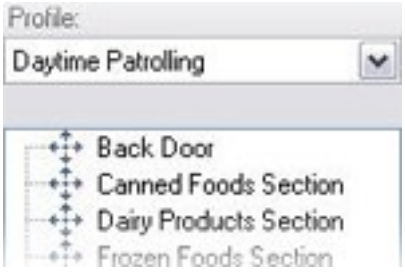
パトロール設定でのプリセット位置の指定

1. プロファイルリストからパトロール設定を選択します。



2. [追加] をクリックします。
3. プリセットの選択ダイアログで、パトロール設定のプリセット位置を選択します。

4. OK をクリックします。選択されたプリセット位置は、パトロール設定のプリセット位置のリストに追加されます。



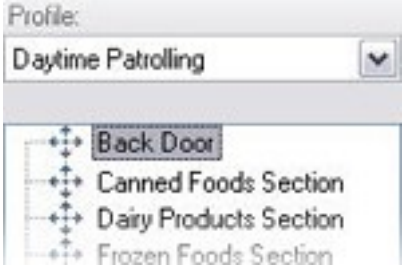
5. カメラはリストの最上位のプリセット位置を、カメラがパトロール設定に従ってパトロールを行うときの最初の停止位置として使用します。上から2番目のプリセット位置は、2番目の停止位置というようになっています。

各プリセット位置での時間を指定

パトロール時に、PTZカメラはパトロール設定で指定された各プリセット位置にデフォルトでは5秒間とどまります。

秒数を変更するには：

1. プロファイルリストからパトロール設定を選択します。
2. 時間を変更したいプリセット位置を選択します。



3. [位置の時間(秒)]フィールドに任意の時間を入力します。
4. 必要に応じて、他のプリセット位置でも繰り返します。

旋回動作(PTZ)をカスタマイズ

デフォルトでは、あるプリセット位置から別の位置に移動するために必要な時間(旋回動作)は3秒であると推定されています。カメラがプリセット位置間を移動するときに、関係のないモーションが検知される可能性が高いため、デフォルトでは、この期間のカメラのモーション検知が無効になっています。

カメラがPTZスキャンに対応し、設定されたプリセット位置がシステムのサーバーに保存されるタイプのカメラ(タイプ1 PTZカメラ)でのみ、旋回動作の速度をカスタマイズできます。それ以外のカメラでは、スピードスライダがグレイ表示になります。

以下をカスタマイズできます。

- 推定旋回動作時間
- カメラが旋回動作中に移動するスピード

異なるプリセット位置での旋回動作をカスタマイズする方法：

1. プロファイルリストからパトロール設定を選択します。
2. 旋回動作をカスタマイズチェックボックスを選択します。

旋回動作表示がプリセット位置のリストに追加されます。

3. リストで、旋回動作を選択します。

4. [予想時間(秒)]フィールドに推定旋回動作時間(秒)を入力します。

5. スピードスライダを使用して、旋回動作スピードを指定します。スライダが右端の位置に来ると、カメラはデフォルトのスピードで移動します。スライダを左に移動するほど、選択した旋回動作中のカメラの移動スピードが低下します。

6. 必要に応じて、他の旋回動作でも同じ操作を繰り返します。

終了位置の指定

選択したパトロール設定に基づくパトロールが終了した時点で、カメラを特定のプリセット位置に移動するように指定することができます。

1. プロファイルリストからパトロール設定を選択します。

2. [終了時に特定の位置に移動]チェックボックスを選択します。これにより、プリセットの選択ダイアログボックスが開きます。

3. 終了位置を選択し、**OK**をクリックします。

> 任意のカメラのプリセット位置を終了位置として指定できます。パトロール設定で使用するプリセット位置に制限はありません。

4. 選択された終了位置がプロファイルリストに追加されます。

   選択されたパトロール設定に基づくパトロールが終了した時点で、カメラは指定された終了位置に移動します。

手動パトロール(説明付き)

パトロール設定を設計すると、システムに適用する前に手動パトロールを使用してテストできます。[開始]および[停止]ボタンを使用して、手動パトロールを開始および停止します。

カメラが既にパトロール中であるか、別のユーザーによって制御されている場合は、自分の優先度が高い場合にのみ手動パトロールを開始できます。

カメラがルールでアクティブ化されたシステムパトロールを実行している間に手動パトロールを開始する場合は、手動パトロールを停止するときにこのパトロールを再開します。別のユーザーが手動パトロールを実行しているときに、自分の優先度が高く、手動パトロールを開始すると、他のユーザーの手動パトロールは再開されません。

手動パトロールを自分で停止しない場合は、より高い優先度のルールに基づくパトロールまたはユーザーに取得されるまで継続します。ルールに基づくシステムパトロールが停止すると、システムは手動パトロールを再開します。別のユーザーが手動パトロールを開始すると、自分の手動パトロールが停止し、再開されません。

手動パトロールを停止すると、[終了時に特定の位置に移動]を使用してパトロール設定の終了位置が定義されている場合は、カメラがこの位置に戻ります。

手動パトロールプロパティ

PTZパトロール表は、PTZカメラの現在のステータスを示します。

名前	説明
ユーザー	PTZセッションを予約したか、手動パトロールを開始して現在カメラを制御しているユーザーが表示されます。 パトロールセッションがシステムによってアクティブ化された場合は、パトロールと表示されます。
優先度	ユーザーのPTZ優先度が表示されます。自分よりも低い優先度のユーザーまたはパトロールプロファイルからのみ、PTZセッションを取得できます。
タイムアウト	現在の予約済みまたは手動PTZセッションの残り時間が表示されます。
予約	現在のセッションが予約済みPTZセッションであるかどうかを示します。 • 設定あり: 予約 • 設定無し: 予約されていません

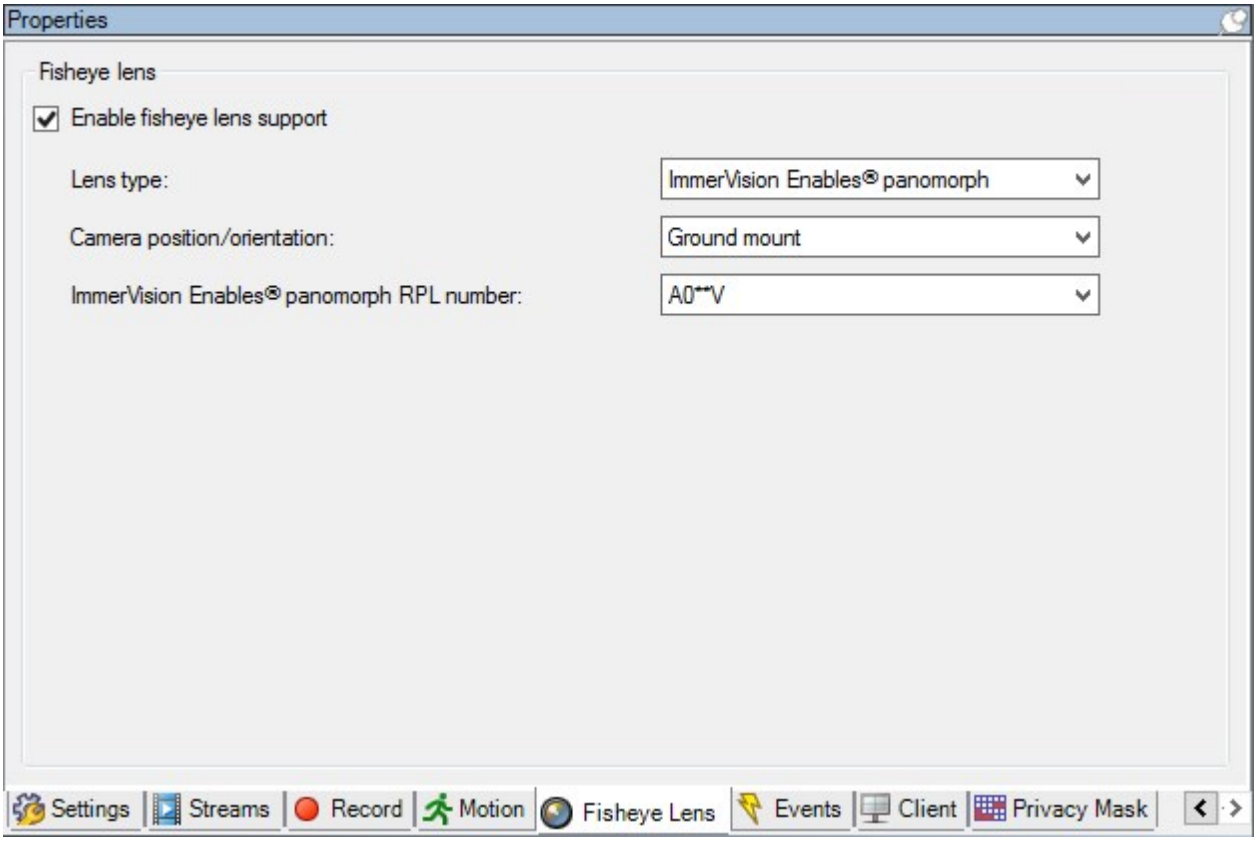
魚眼レンズタブ(デバイス)

魚眼レンズタブ(説明付き)

以下のデバイスに魚眼レンズタブがあります。

- 魚眼レンズを備えた固定カメラ

魚眼レンズタブでは、選択したカメラの魚眼レンズサポートを有効にして、設定することができます。



魚眼レンズサポートを有効/無効にする

魚眼レンズサポートは、既定では無効です。

有効化または無効化するには、[魚眼レンズ]タブの[魚眼レンズサポートを有効にする]チェックボックスを選択または選択解除します。

魚眼レンズ設定の指定

魚眼レンズサポートを有効にする場合：

1. レンズのタイプを選択してください。
2. カメラの物理的位置/方向をカメラの位置/方向リストから指定します。
3. ImmerVisionを可能にする®からぱのモーフRPLナンバーリストのRegistered Panomorph Lens(RPL)ナンバーを選択

   これは、カメラで使用するレンズを識別し、正しく設定するためです。RPL番号は、通常はレンズ本体またはカメラが入っていた箱に記載されています。ImmerVison、Panomorph(パノモーフ)レンズ、およびRPLの詳細については、ImmerVision Enables Webサイト(https://www.immervisionenables.com/)を参照。

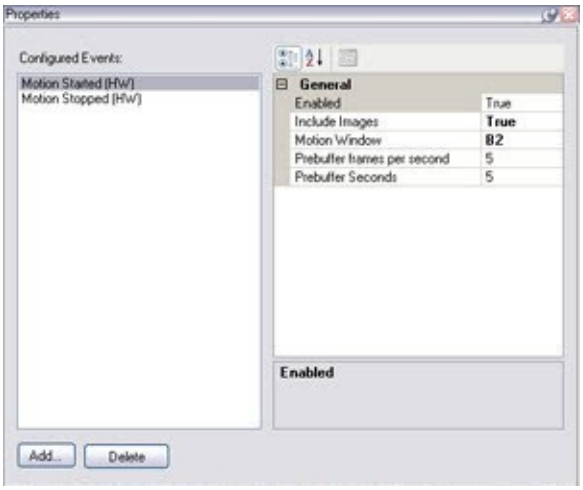
イベントタブ(デバイス)

イベントタブ(説明付き)

以下のデバイスにイベントタブがあります。

- カメラ
- マイク
- 入力

システムのイベントに加えて、一部のデバイスはイベントをトリガーするように設定できます。これらのイベントは、システムでイベントベースのルールを作成する場合に使用できます。技術的には、これらのイベントは、監視システムではなく実際のハードウェア/デバイス上で発生します。



カメラにおけるイベントタブの例

イベントを削除すると、イベントを使用するすべてのルールに影響を与えます。

- ページ248のイベントの追加
- ページ249のイベントプロパティの指定
- ページ249のイベントに複数のインスタンスを使用する

イベントの追加

1. 概要ペインで、デバイスを選択します。
2. イベントタブを選択し、追加をクリックします。この操作でドライバーイベントの選択ウィンドウが開きます。
3. イベントを選択します。一度に選択できるイベントは1つだけです。

4. すでに追加されたイベントを再び追加できるよう、全イベントの全リストを表示したい場合は、[すでに追加されたイベントを表示]を選択します。
5. **OK** をクリックします。
6. ツールバーで保存をクリックします。

イベントプロパティの指定

追加したイベントごとにプロパティを指定できます。プロパティの数は、対象となるデバイスやイベントによって異なります。目的どおりに機能するようにするには、デバイスの一部またはすべてのプロパティを、このタブと同一になるように指定する必要があります。

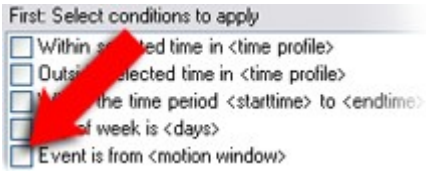
イベントに複数のインスタンスを使用する

1つのイベントに複数のインスタンスでの異なるプロパティを指定できるようにするために、複数のイベントを追加できます。

> 次の例は、カメラに固有です。

例：2つのモーションウィンドウ(A1、およびA2) があるカメラを設定しました。モーション開始(ハードウェア) イベントの2つのインスタンスが追加されました。1つのインスタンスのプロパティで、モーションウィンドウA1の使用を指定しました。もう1つのインスタンスのプロパティで、モーションウィンドウA2の使用を指定しました。

ルールでイベントを使用する場合、イベントはルールをトリガーするための特定のモーションウィンドウで検知されたモーションに基づくように指定できます。



イベントタブ(プロパティ)

名前	説明
設定済みイベント	設定済みイベントリストで、どのイベントを選択して追加できるかは、対象となるデバイスとその設定によって完全に決定されます。デバイスのタイプによっては、リストが空の場合もあります。
一般	プロパティのリストは、対象となるデバイスやイベントによって異なります。目的どおりに機能するようにするには、デバイスの一部またはすべてのプロパティを、このタブと同一になるように指定する必要があります。

クライアントタブ(デバイス)

[クライアント]タブ(説明付き)

以下のデバイスにクライアントタブがあります。

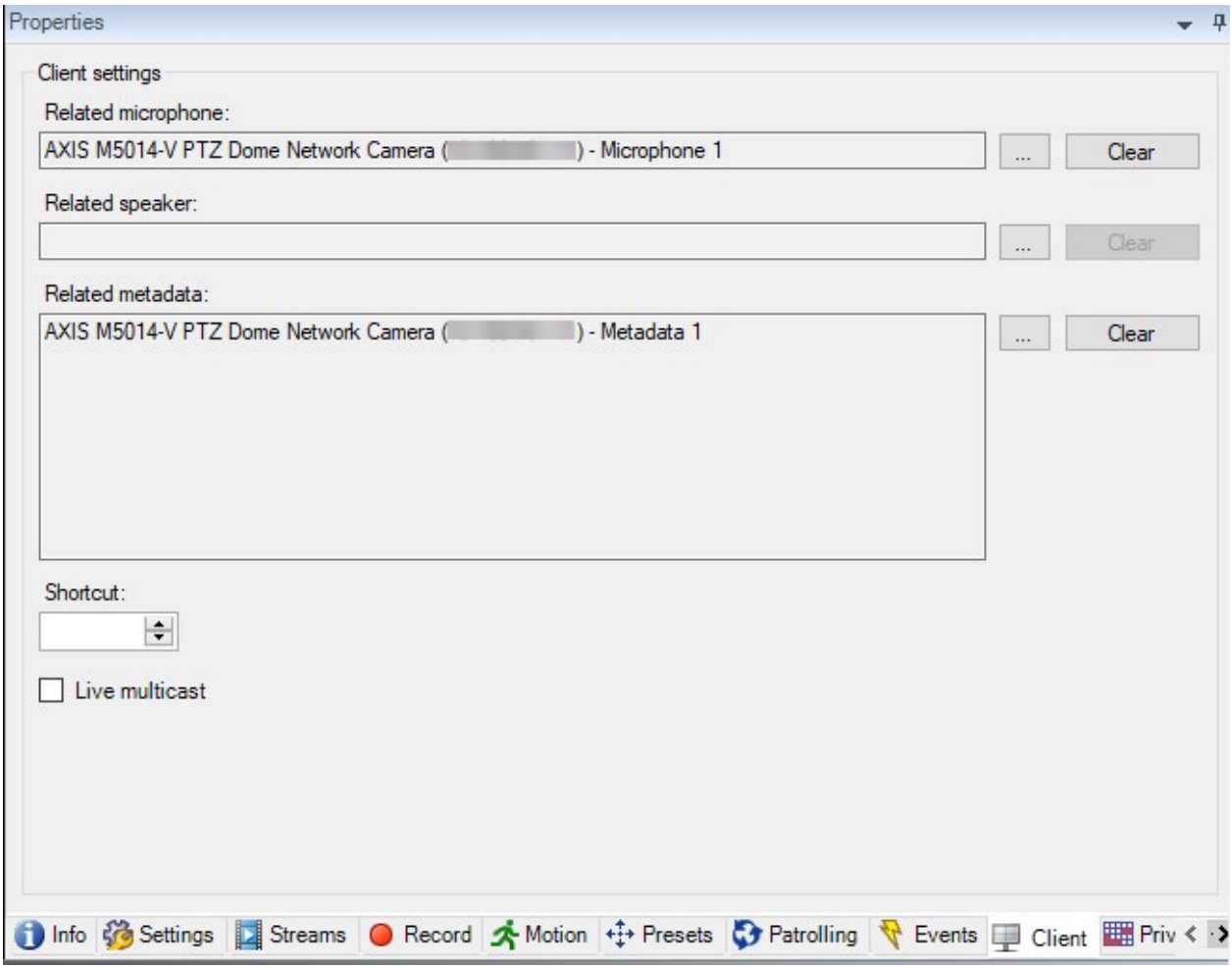
- カメラ

[クライアント]タブでは、XProtect Smart Client でカメラを使用する際に視聴できる他のデバイスを指定できます。

カメラによる録画時には、関連デバイスによっても録画が行われます(「ページ219の関連するデバイスで録画を有効にする」を参照)。

カメラのライブ マルチキャストを可能にできます。クライアントのためのレコーディングサーバー経由のカメラ マルチキャストライブストリームのことです。

> レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。



以下も参照してください：

- ページ169のレコーディングサーバーのマルチキャストを有効にする
- ページ169のマルチキャスト(説明付き)

クライアントタブのプロパティ

名前	説明
関連するマイク	XProtect Smart Clientユーザーがデフォルトでカメラのどのマイクから音声を受信するかを指定します。XProtect Smart Clientユーザーは必要に応じて別のマイクを手動で選択して聞くことができます。 音声付きビデオをストリームするビデオプッシュカメラに関連するマイクを特定します。 カメラが録画する際に、関連するマイクが録音します。
関連するスピーカー	デフォルトでXProtect Smart Clientユーザーがカメラのどのスピーカーで話すかを指定します。必要に応じてXProtect Smart Clientユーザーは別のスピーカーを手動で選択できます。 カメラが録画する際に、関連するスピーカーが録音します。
関連するメタデータ	XProtect Smart Clientユーザーがデータを受信する、カメラ上のメタデータデバイスを1つ以上指定します。 カメラが録画する際に、関連するメタデータデバイスが記録します。
ショートカット	XProtect Smart Clientユーザーがカメラを簡単に選択できるように、カメラにショートカットキーを定義します。 • カメラを一意に識別できるよう各ショートカットを作成します • カメラのショートカット番号は4桁以内である必要があります

名前	説明
ライブマルチキャスト	このシステムでは、レコーディングサーバーからXProtect Smart Clientへのライブストリームのマルチキャストをサポートしています。カメラからのライブストリームマルチキャストを可能にするには、チェックボックスを選択。 ストリームタブ上でカメラのデフォルトストリームとしてストリームを指定している時のみライブマルチキャスティングは可能です。 レコーディングサーバーに対してもマルチキャストを設定する必要があります。ページ167のマルチキャストタブ(レコーディングサーバー)。 レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。

プライバシーマスクタブ(デバイス)

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。

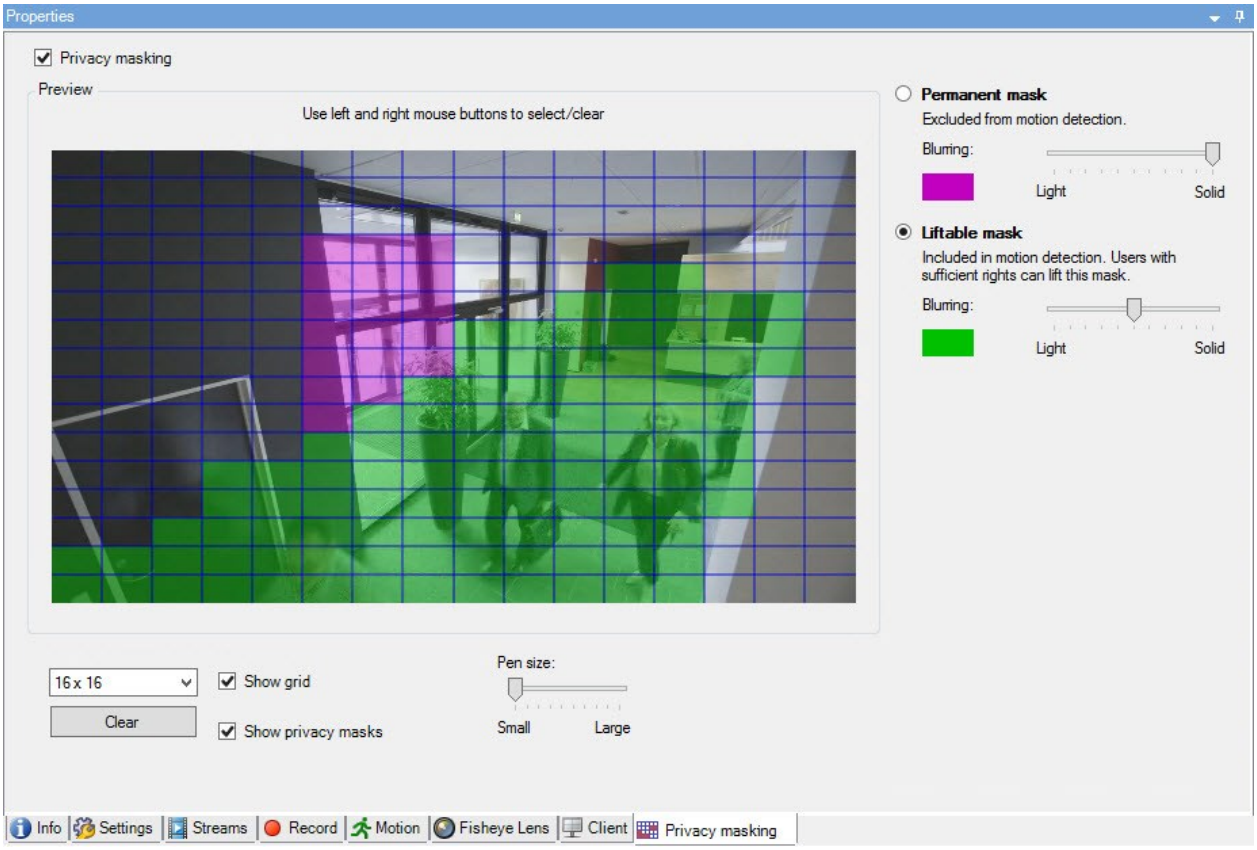
XProtect Essential+ 2018 R1以降は、プライバシーマスクをサポートしません。そのため、プライバシーマスクが適応されたシステムから更新を行った場合には、マスクは除去されます。

プライバシーマスクタブ(説明付き)

以下のデバイスにプライバシーマスクタブがあります。

- カメラ

プライバシーマスクタブでは、選択したカメラのプライバシーマスクを有効にして設定できます。



プライバシーマスクはカメライメージの領域に適応および固定されます。そのため、カバーされた領域はパンチルト動作を追わず、常に、カメライメージと同じ領域をカバーします。いくつかのPTZカメラにおいては、カメラ自体において、位置ベースのプライバシーマスを有効にすることができます。

Milestone Interconnect設定では、中央サイトは、リモートサイトで定義されたプライバシーマスクを無視します。同じプライバシーマスクを適用する場合は、中央サイトでもう一度定義します。

- ページ253のプライバシーマスク(説明付き)
- ページ256のプライバシーマスクの有効化/無効化
- ページ256のプライバシーマスクを定義する
- ページ258の除去されたプライバシーマスクのタイムアウトを変更する
- ページ257のプライバシーマスクの除去権限をユーザーに与える
- ページ259のプライバシーマスク設定のレポートを作成します

プライバシーマスク(説明付き)

プライバシーマスクでは、クライアントに見せる際に、カメラのビデオにおけるどの領域をプライバシーマスクでカバーしたいかを定義することができます。例えば、監視カメラで大通りを録画する場合、住民のプライバシーを保護するために、プライバシーマスクを使用して特定の建物(窓やドアなど) の領域を非表示にすることができます。いくつかの国では、これは法的要求事項で

す。

プライバシーマスクは、不透明のものかぼやけたものを選ぶことができます。マスクは、ライブ、録画、そしてエクスポートされたビデオをカバーします。

2種類のプライバシーマスクがあります：

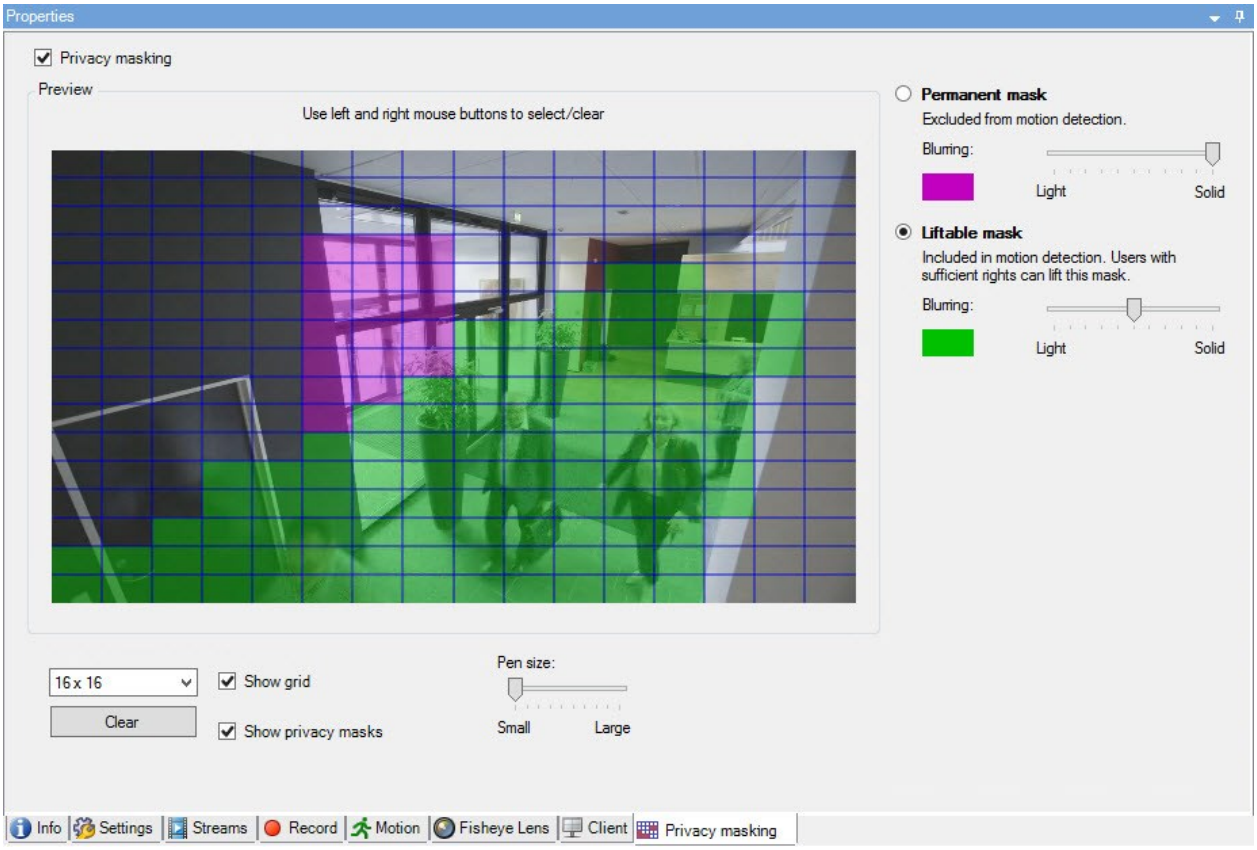
- 常設のプライバシーマスク：このタイプのマスクを持つ領域は、常にクライアントにおいてカバーされています。公的な場所や、監視カメラが許可されていない場所といった、監視が決して必要とされないビデオの領域をカバーすることに使われます。モーション検知は常設のプライバシーマスク領域から除外されます。
- 除去可能なプライバシーマスク：このタイプのマスクを持つ領域は、プライバシーマスク除去の権限をもつユーザーにより、一時的にXProtect Smart Clientにおけるカバーを外すことができます。もし、ログインしているXProtect Smart Clientユーザーがプライバシーマスク除去の権限を持たない場合は、システムは権限を持つユーザーに、除去の許可を依頼します。プライバシーマスクはタイムアウトまたはユーザーが再適用するまで除去されます。ユーザーがアクセス権を持つすべてのカメラのビデオで、プライバシーマスクが除去されますのでご注意ください。

もしプライバシーマスクが適応された2017 R3システム、あるいはそれより古いバージョンから更新した場合には、マスクは、除去可能なマスクとして移行されます。

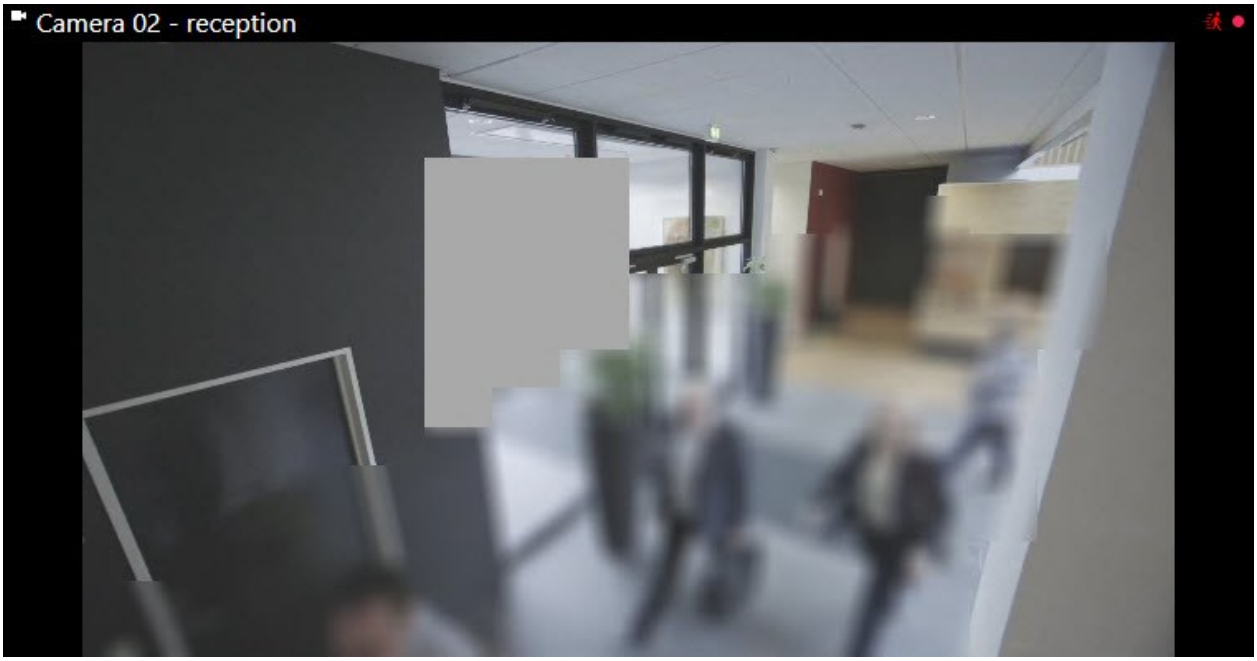
もしユーザーが、録画されたビデオをクライアントからエキスポート、あるいは再生した場合には、ビデオは録画時に設定されていたプライバシーマスクを含みます。それは、録画時より後にプライバシーマスクを変更、あるいは除去しても変わりません。もしプライバシープロテクションがエキスポート時に除去された場合には、エキスポートされたビデオは除去可能なプライバシーマスクを含みません。

もしプライバシーマスク設定を、週に1回といった高い頻度で変更する場合、システムはオーバーロードされる可能性があります。

プライバシーマスク設定を持つプライバシーマスクタブの例：



クライアントには、以下のように表示されます：



クライアントユーザーには、常設のおよび除去可能なプライバシーマスクについて、知らせることができます。

プライバシーマスクの有効化/無効化

プライバシーマスク機能は、デフォルトで無効になっています。

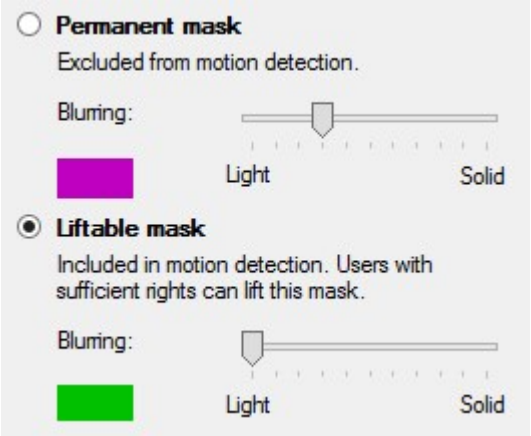
カメラのプライバシーマスク機能を有効化/無効化する方法：

- [プライバシーマスク]タブで[プライバシーマスク]チェックボックスを選択/解除します。

プライバシーマスクを定義する

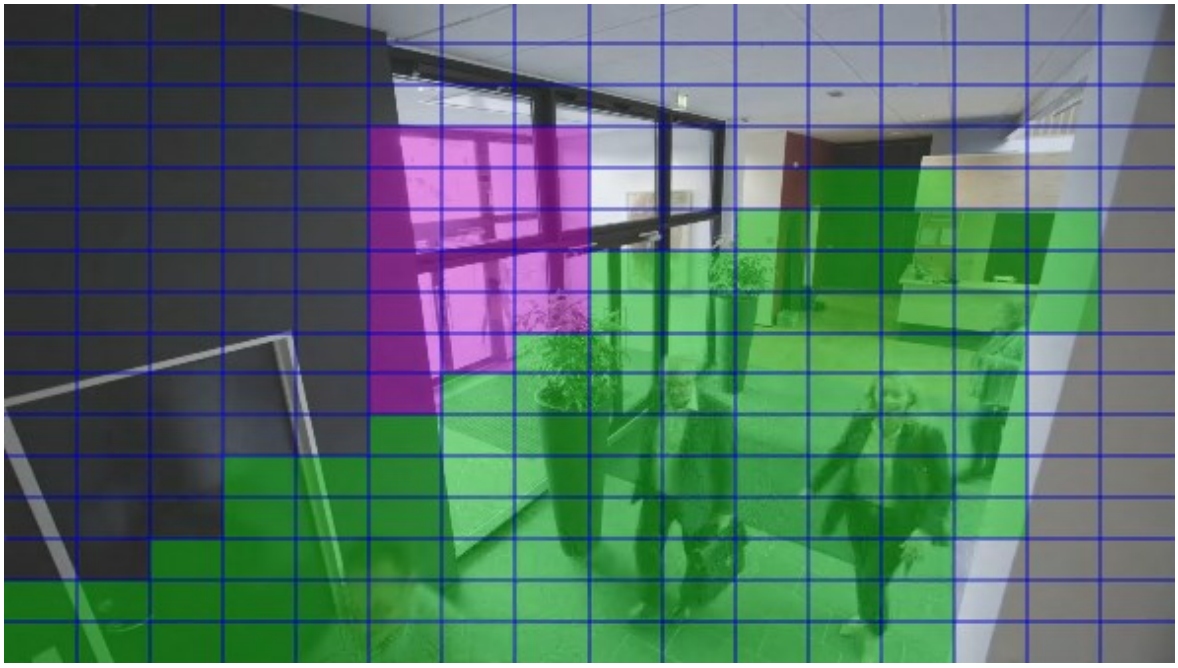
プライバシーマスクタブでプライバシーマスク機能を有効化すると、カメラプレビューにグリッドが適応されます。

1. プライバシーマスクを持つ領域をカバーするには、まず、常設のプライバシーマスクか除去可能なプライバシーマスクかを選択します。



2. マウスをプレビューの上でドラッグします。マウスの左ボタンで、グリッドセルを選択します。マウスの右ボタンで、グリッドセルを解除します。

3. 必要な数のプライバシーマスク領域を定義できます。常設のプライバシーマスクを持つ領域は、紫で表示され、除去可能なプライバシーマスクの領域は緑で表示されます。



4. クライアントに見せられる時に、ビデオにおいてカバーされた領域がどのように表示されるかを定義します。簡易的なぼやけたマスクから、完全な不透明のマスクに変更するには、スライダーを使用します。

> 常設のプライバシーマスクは、モーションタブにも表示されます。

5. XProtect Smart Clientで、プライバシーマスクが、定義した通りに表示されていることを確認してください。

プライバシーマスクの除去権限をユーザーに与える

デフォルト設定では、XProtect Smart Clientにおいていかなるユーザーもプライバシーマスクの除去権限は持っていません。

許可の有効化/無効化：

1. 役割の下で、プライバシーマスク除去の権限を与えたい役割を選択します。
2. 全体的なセキュリティタブで、カメラを選択します。
3. プライバシーマスク除去を許可するためには、許可チェックボックスを選択してください。

この役割にアサインされたユーザーは、その他のXProtect Smart Clientユーザーに除去の権限を与えるほか、自分自身の手でプライバシーマスクを除去可能なものとして設定することが可能です。

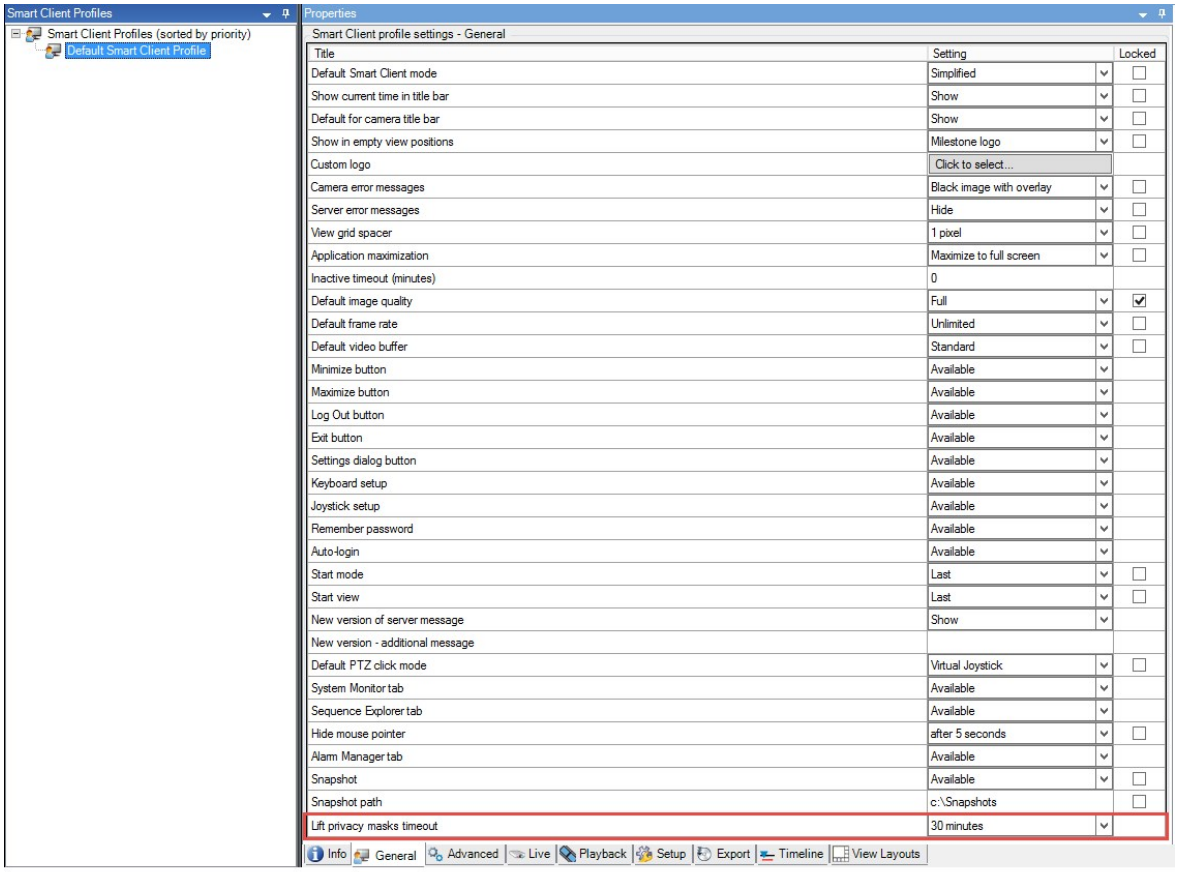
除去されたプライバシーマスクのタイムアウトを変更する

デフォルト設定では、プライバシーマスクはXProtect Smart Clientで30分の間除去され、その後は自動的に適応されます。しかし、この設定は変更可能です。

> タイムアウトを変更した場合は、プライバシーマスク除去の許可を持つ役割と関連するSmart Clientのプロファイルのためにそうすることを忘れないでください。

タイムアウトを変更するには：

1. Smart Clientプロファイルの下で、関連するSmart Clientのプロファイルを選択します。
2. 全般タブにおいて、プライバシーマスク除去タイムアウトを見つけます。



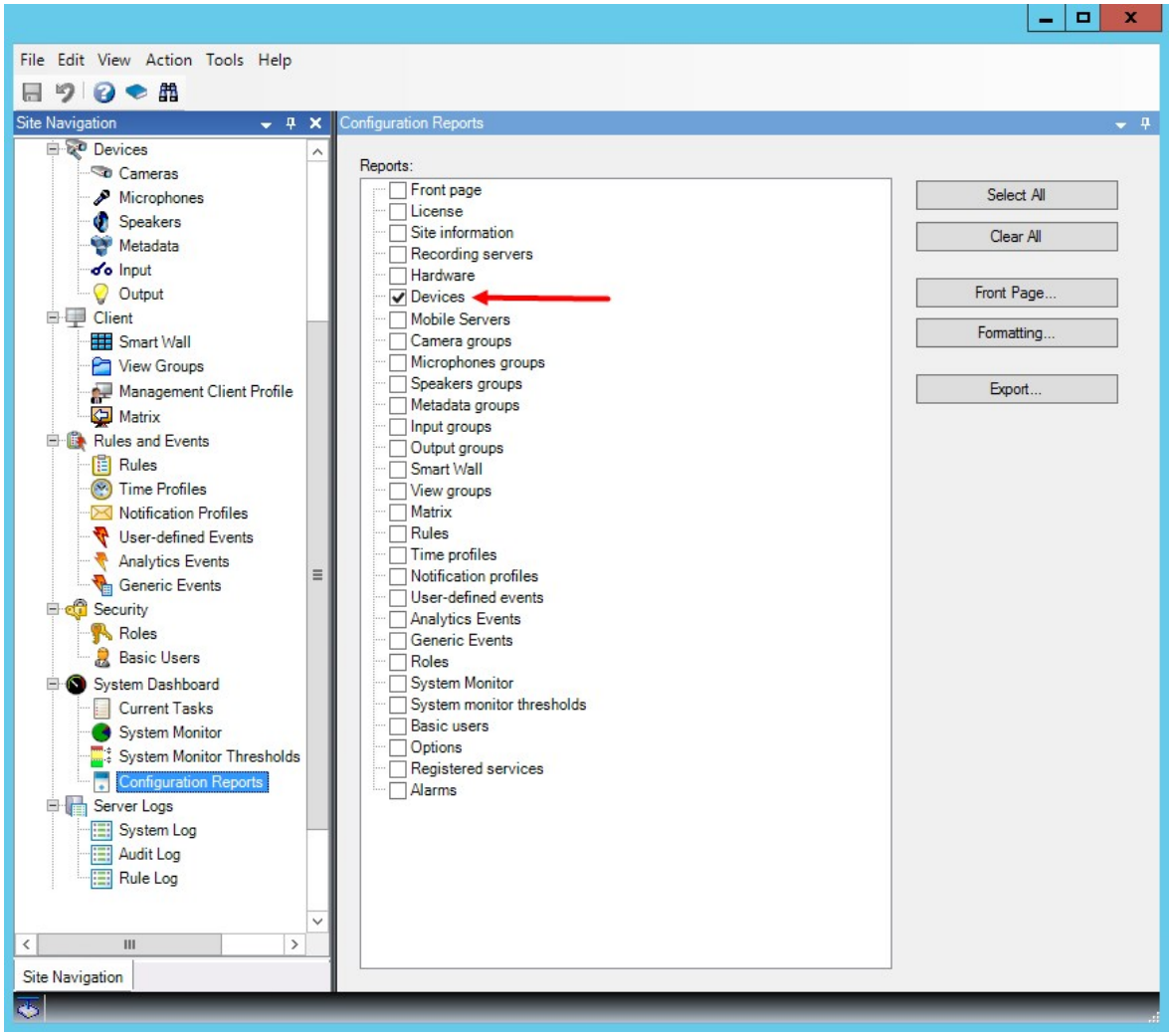
3. 以下の値の間で選択します：
    - 2 分
    - 10分
    - 30分
    - 1時間
    - 2時間
    - ログアウトするまで
4. [保存] をクリックします。

プライバシーマスク設定のレポートを作成します

デバイスレポートは、お使いのカメラの現行のプライバシーマスク設定に関する情報を含んでいます。

レポートを構成するには：

1. 構成レポートの下で、デバイスレポートを選択します。



2. もしレポートを変更したい場合は、フロントページとフォーマットを変更します。
3. エクスポートをクリックすると、システムがレポートをPDFファイルで作成します。

詳細に関しては、ページ387の設定レポート(説明付き)を参照してください。

プライバシーマスクタブ(プロパティ)

名前	説明
グリッドサイ	選択された値は、グリッドがプレビュー上で表示されるかどうかにかかわらず、グリッドの密度を決定します。

名前	説明
ズ	8×8、16×16、32×32または64×64から値を選択します。
クリア	指定したすべてのプライバシーマスクをクリアします。
グリッドを表示	グリッドを表示チェックボックスを選択してグリッドを表示します。
プライバシーマスクの表示	プライバシーマスクを表示するチェックボックス(デフォルト)を選択すると、常設のプライバシーマスクがプレビューに紫色で表示され、除去可能なプライバシーマスクは緑色で表示されます。 Milestoneは、プライバシーマスクを表示ボックスを選択しておくことを推奨しています。これにより、同僚が現行のプライバシー保護設定を見ることができます。
ペンサイズ	ペンサイズスライダーを使って、領域をクリック&ドラッグで選択するサイズを示します。デフォルトでは小さく設定されており、グリッドのマス1つ分に相当する大きさに設定されています。
永続的なマスク	このタブ、およびモーションタブのプレビューで、紫色で表示されます。 常設のプライバシーマスクは、常にXProtect Smart Clientにて表示され、除去することはできません。公的な場所や、監視が許可されていない場所といったビデオが決して必要とされない領域において、使うことができます。モーション検知は、常設のプライバシーマスクからは除外されます。 プライバシーマスクの範囲を、不透明か、ぼやけたレベルのどちらかに指定します。範囲設定は、ライブおよび録画されたビデオの両方に適応されます。
除去可能なマスク	本タブのプレビューに、緑色で表示されます。 除去可能なプライバシーマスクは、XProtect Smart Clientにおいて十分な権利を持つユーザーによる除去が可能です。デフォルト設定では、プライバシーマスクは30分間除去され、その後は自動的に適応されます。ユーザーがアクセス権を持つすべてのカメラのビデオでプライバシーマスクが除去されますのでご注意ください。 もし、ログインしているXProtect Smart Clientユーザーがプライバシーマスク除去の権限を持たない場合は、システムは権限を持つユーザーに、除去の容認を依頼します。 プライバシーマスクの範囲を、不透明か、ぼやけたレベルのどちらかに指定します。範囲設定は、ライブおよび録画されたビデオの両方に適応されます。
ぼかし:	簡易的なぼやけたマスクから、完全な不透明のマスクに変更するには、スライダーを使用します。 デフォルト設定では、常設のプライバシーマスクの領域は無地(不透明)です。デフォルト設定では、除去可能なプライバシーマスクは、中程度にぼやけています。 クライアントユーザーが、違いを理解できるよう、常設のプライバシーマスクと除去可能なプライバシーマスクの外観の違いを伝えてください。

サイトナビゲーション：クライアント

この記事では、XProtect Smart Clientのオペレータ用のユーザーインターフェース、ならびにManagement Clientのシステム管理者用のユーザーインターフェースをカスタマイズする方法について説明します。

クライアント(説明付き)

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。

Management Clientのクライアントセクションは以下で構成されています。

名前	説明
XProtect Smart Wall	XProtect Smart Wallはアドオンで、ビューコンテンツをXProtect Smart Client から専用ビデオウォールに送信できます。 XProtect Smart Wallの詳細については、ページ31のXProtect Smart Wall (説明付き)を参照してください。
ビューグループ	カメラからのビデオを再生する方法をビューと呼びます。XProtect Smart Clientを閲覧できる人を制限するために、ビューグループを作成して、論理エンティティのビューをグループ分けすることができます。これらのビューグループへのアクセス権を役割に割り当てることで、特定の役割をもつ個々のビューグループへのアクセスを制限できます。ビューグループを選択して、監視のニーズに合うように、ビューグループを設計して作業します。
Smart Client のプロファイル	XProtect Smart Clientユーザーを区別するには、Smart Clientプロファイルを作成して優先度を付け、手持ちの異なるタスクでの必要に応じてプロファイルをカスタマイズできます。
Management Client のプロファイル	Management Client管理者ユーザーを区別するには、Management Clientプロファイルを作成して優先度を付け、手持ちの異なるタスクでの必要に応じてプロファイルをカスタマイズできます。
Matrix	Matrixは動画のリモート配信機能です。Matrixを使用すると、XProtect Smart Clientを走らせているシステムのネットワーク上の任意のカメラから、ビデオを配信できます。

サイトナビゲーション：クライアント：Smart Wallの設定

この記事では、XProtect Smart Wallを構成する方法について説明します。

XProtect Smart Wallライセンス

XProtect Smart Wallでは、以下のビデオウォール関連ライセンスが必要です。

- ビデオウォールで動画表示する無制限の数のモニターを対象とするXProtect Smart Wallの基本ライセンス

XProtect Smart Wallの基本ライセンスは、XProtect Corporateの基本ライセンスに含まれます。XProtect Expertがある場合は、個別にXProtect Smart Wallの基本ライセンスを購入できます。

Smart Wallの構成

Smart Wallの設定では、Smart Wallを定義し、モニターを追加し、モニターレイアウトを定義し、オプションとしてSmart Wallプリセットや、異なるモニターのレイアウトとコンテンツを指定します。

Smart Wallプリセットは、XProtect Smart Clientユーザーがビデオウォールに手動でプッシュできるカメラや、XProtect Smart Clientビューのみを表示する場合は定義する必要がありません。

ルールを使用して、ビデオウォールに表示されるものを自動的に切り替えたり、あるいはシナリオが発生するたびにビデオウォールに同じコンテンツを表示する典型的な監視シナリオがある場合は、Smart Wallプリセットを定義する必要があります。

Smart Wallの設定は非常に柔軟です。ビデオウォール上のすべてのモニターを1つのSmart Wallに含めることができます。あるいはモニターをグループ化し各グループに対してSmart Wallを構成することができます。Smart Wallのプリセットは、Smart Wallのすべてのモニターあるいは一部のモニターでレイアウトと内容を変更できます。モニターは複数のSmart WallとSmart Wallプリセットの一部として含めることができます。典型的な監視シナリオに対応するために、Smart WallとSmart Wallプリセットを、必要な数だけ無制限に作成できます。

a. Smart Wallを定義

1. クライアントを展開し、**Smart Wall**を選択します。
2. 概要ペインで、**Smart Wall**を右クリックし、追加**Smart Wall**を選択します。
3. Smart Wallの設定を指定します。
4. 全般ビューアイテムのプロパティ設定で、カメラのレイアウト項目の上にシステムステータス情報とタイトルバーを表示するかどうか指定します。
5. **OK** をクリックします。

b. モニターを追加し、モニターレイアウトを定義します

1. Smart Wallを右クリックし、モニターの追加を選択します。
2. ビデオウォール上の物理モニターと同一になるように、モニターの寸法を設定します。
3. プリセット動作設定の空のプリセットおよび空のプリセットアイテムを使用して、空のプリセットレイアウトがモニターで表示する内容を定義します。または新しいSmart Wallプリセットが自動的にトリガーされたり、XProtect Smart Clientで手動で選択されたときに、プリセットの空のプリセット項目に表示する内容を定義します。空のプリセットおよび空のプリセットアイテムは、Smart Wallプリセットによって制御されないコンテンツに使用できます。
4. プリセット動作設定のエレメントの挿入を使用して、XProtect Smart Clientのユーザーが、Smart Wallプリセットのレイアウト項目にカメラをドラッグしたときの動作を定義します。独立を選択して、プリセットアイテムに既にあるカメラと新しいカメラを置き換えます。またはリンク済みを選択して、新しいカメラを挿入したところから、レイアウトアイテムのコンテンツを左から右に押します。
5. 物理ビデオウォールにある数だけのモニターを追加します。
6. Smart Wallを選択し、レイアウトタブで、編集をクリックして、ビデオウォールの物理モニターの配置と同一になるように、複数のモニターを配置します。
7. **[OK]** をクリックします。同じレイアウトがXProtect Smart Clientで使用されます。

c. Smart Wallプリセットを追加する**(** オプション**)** :

1. Smart Wallを選択し、プリセットタブから、新規追加をクリックします。
2. 名前と説明を入力して、**OK**をクリックします。
3. 実行をクリックすると、Smart Wallプリセットがビデオウォールに表示されます。
4. 必要な数のSmart Wallプリセットを作成します。

d. モニターにレイアウトとカメラを追加する**(Smart Wall**プリセットを必要とする**)** :

1. 作成したモニターのいずれかを選択し、プリセットタブから、選択したSmart Wallプリセットを使用する場合に、選択したモニターに表示する内容を設定するため、リストからプリセットを選択します。
2. 編集 をクリックします。
3. レイアウトボタンをクリックして、モニターで使用するレイアウトを選択し、**[OK]** をクリックします。

4. デバイスグループ、レコーディングサーバーまたはフェデレーテッドサイトタブからカメラを各レイアウトアイテムにドラッグします。フェデレーテッドサイト階層タブのカメラは、Milestone Federated Architecture設定からアクセスできます。Smart Wallプリセットによって制御されない他のコンテンツで使用できるようにするには、レイアウトアイテムを空のままにします。

5. 選択されたプリセットのレイアウトが、モニターに既にある場合は、クリアをクリックして新しいレイアウトを定義するか、Smart Wallプリセットによって制御されない他のコンテンツにモニターを使用できるように、Smart Wallプリセットからモニターを除外します。
6. OK をクリックします。
7. Smart Wallプリセットに含めるモニターに、レイアウトやカメラが追加されるまで手順を繰り返します。

XProtect Smart Wallのユーザー権限を設定

役割のユーザー権限を指定すると、XProtect Smart ClientユーザーがXProtect Smart Wallで実行できるタスクを制御できます。ユーザー権限は、役割に割り当てられるすべてのユーザーに適用されます。Smart Wall権限のある役割の詳細については、ページ341の役割の設定を参照してください。

読み取り、編集、削除ユーザー権限の選択は常に適用されます。操作および再生ユーザー権限については、時間設定を選択し、特定の期間の間にユーザー権限を付与できます。たとえば、標準の業務時間内にのみユーザーがSmart Wallで表示されるコンテンツを変更できるようにする場合に便利です。

役割のユーザー権限を指定するには、次の手順に従います。

1. サイトナビゲーションペインで、セキュリティを展開し、役割を選択します。
2. [役割]ペインで役割を選択するか、ペインを右クリックし、[役割の追加]を選択して新しい役割を作成します。
3. 役割設定ペインの上部でSmart Wallを選択します。
4. 役割設定ペインの下部で、Smart Wallタブをクリックしてから、割り当てるユーザー権限を選択します。
   - 読み取り- クライアントアプリケーションでSmart Wallを表示
   - 編集 - クライアントアプリケーションでSmart Wallを変更
   - 削除 - クライアントアプリケーションでSmart Wallを削除
   - 操作 - クライアントアプリケーションで選択したモニターにレイアウトを適用し、プリセットをアクティブ化
   - 再生 - ライブおよび録画されたビデオを確認して管理

   > 再生権限を選択しない場合、ユーザーは、ビデオウォールに表示されるコンテンツを表示できますが、変更できません。ユーザーが変更を行った場合は、システムが共有状態から自動的に切断され、ビデオウォールのコンテンツは影響を受けなくなります。共有ビューに戻るには、[Smart Wallモニターの再接続]をクリックします。

5. オプション: 特定の期間に操作または再生ユーザー権限を付与するには、チェックボックスを選択してから、時間設定を選択します。

Smart Wallプリセットのあるルールの使用(説明付き)

ルールとSmart Wallプリセットを組み合わせることによって、カメラなどの動作をシステムがルールを使って制御する方法と同様に、ビデオウォールに表示される内容を制御できます。たとえば、あるルールがビデオウォールをトリガして、特定の日に特定のSmart Wallプリセットを表示することができます。さらに、ルールを使ってビデオウォールディスプレイで各モニターに何が表示されるかを制御できます。ルールの作成方法については、ページ309のルールを参照してください。

ルールがSmart Wallプリセットをトリガーする例。

Smart Wallプロパティ

情報タブ(Smart Wallプロパティ)

の情報Smart Wallタブでは、Smart Wallを追加および編集できます。

名前	説明
名前	Smart Wallの名前。XProtect Smart ClientにSmart Wallビューグループ名として表示されます。
説明	Smart Wallの説明。説明はManagement Client内部でのみ使用されます。
ステータステキスト	選択すると、カメラとシステムステータス情報が、ビデオウォールのカメラのレイアウトアイテム全体で表示されます。
タイトルバーなし	選択すると、ビデオウォールに表示されるすべてのSmart Wallレイアウトアイテムにタイトルバーが表示されません。
タイトルバー	選択すると、ビデオウォールに表示されるすべてのSmart Wallレイアウトアイテムにタイトルバーが表示されます。
ライブインジケータ付きのタイトルバー	選択すると、ビデオウォールに表示されるすべてのSmart Wallレイアウトアイテムのタイトルバーにライブおよびモーションインジケータが表示されます。

プリセットタブ(Smart Wallプロパティ)

のプリセットSmart Wallタブでは、Smart Wallプリセットを追加および編集できます。

名前	説明
新規追加	クリックして、XProtect Smart Wallインストールにプリセットを追加します。 新しいSmart Wallプリセットの名前と説明を定義します。
編集	Smart Wallプリセットの名前および説明を編集します。
削除	Smart Wallプリセットを削除します。
実行	クリックすると、Smart Wallプリセットがビデオウォールに表示されます。Smart Wallプリセットの表示が自動的にトリガされるようにするには、Smart Wallプリセットを使ってルールを作成する必要があります。Smart Wallプリセットでのページ266のSmart Wallプリセットのあるルールの使用(説明付き)も参照してください。

レイアウトタブ(Smart Wallプロパティ)

のレイアウトSmart Wallタブで、ビデオウォール上の物理モニターの配置と一致するよう、Smart Wallのモニターを配置します。このレイアウトはXProtect Smart Clientでも使用されます。

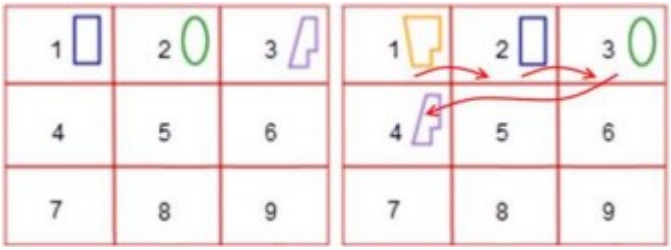
名前	説明
編集	クリックして、モニターの配置を調整します。
移動	モニターを新しい位置に移動するには、関連するモニターを選択し、任意の位置にドラッグするか、あるいは矢印ボタンのいずれかをクリックして、モニターを選択した方向に移動します。
ズームボタン	ボタンをクリックすると、Smart Wallレイアウトプレビューが拡大/縮小され、モニターを正しく配置することができます。
名前	モニターの名前。名前はXProtect Smart Clientに表示されます。
サイズ	ビデオウォールの物理モニターの寸法。
アスペクト比	ビデオウォールの物理モニターの高さおよび幅の比率。

モニタープロパティ

情報タブ(モニタープロパティ)

プリセットのモニターの情報Smart Wallタブで、モニターを追加し、モニター設定を編集できます。

名前	説明
名前	モニターの名前。名前はXProtect Smart Clientに表示されます。
説明	モニターの説明。説明はManagement Client内部でのみ使用されます。
サイズ	ビデオウォールの物理モニターの寸法。
アスペクト比	ビデオウォールの物理モニターの高さおよび幅の比率。
空のプリセット	XProtect Smart Clientで新しいSmart Wallプリセットがトリガーされるか、選択されたときに、プリセットレイアウトが空のモニターに表示する内容を定義します。 保存を選択すると、モニターの現在のコンテンツが維持されます。 クリアを選択すると、すべてのコンテンツがクリアされ、モニターには何も表示されなくなります。
空のプリセットアイテム:	XProtect Smart Clientで新しいSmart Wallのプリセットがトリガーされるか、選択されたときに、空のプリセットレイアウト項目に表示する内容を定義します。 保存を選択すると、レイアウトアイテムの現在のコンテンツが維持されます。 クリアを選択すると、すべてのコンテンツがクリアされ、レイアウトアイテムには何も表示されなくなります。

名前	説明
要素の挿入	XProtect Smart Clientで表示したときに、モニターのレイアウトにどのようにカメラが挿入されるかを定義します。独立を選択すると、影響のあるレイアウトアイテムのコンテンツのみが変更され、レイアウトの他のコンテンツは同じままで維持されます。リンク済みを選択すると、レイアウトアイテムのコンテンツは左から右へ押されます。たとえば、この図例では、カメラがポジション1に挿入されると、ポジション1の前のカメラはポジション2に押され、ポジション2の前のカメラはポジション3に押される、というように続きます。 

プリセットタブ(モニタープロパティ)

プリセットのモニターのプリセットSmart Wallタブでは、選択したSmart Wallプリセットでモニターのレイアウトとコンテンツを編集できます。

名前	説明
プリセット	選択されたSmart WallのSmart Wallプリセットのリスト。
編集	編集をクリックして、選択したモニターのレイアウトとコンテンツを編集します。 カメラをダブルクリックして、単一のカメラを削除します。 クリアをクリックすると、Smart Wallプリセットからモニターを除外する新しいレイアウトを定義します。これにより、Smart Wallプリセットによって制御されない他のコンテンツでモニターが使用できるようになります。 をクリックして、選択したプリセットのモニターで使用するレイアウトを選択し、**OK**をクリックします。 デバイスグループ、レコーディングサーバーまたはフェデレーテッドサイトタブからカメラを各レイアウトアイテムにドラッグします。Smart Wallプリセットによって制御されない他のコンテンツで使用できるようにするには、レイアウトアイテムを空のままにします。

サイトナビゲーション：クライアント：ビューグループ

クライアントでシステムが1つ以上のカメラからのビデオを表示する方法はビューと呼ばれます。ビューグループは、このようなビューの1つ以上の論理グループのコンテナです。クライアントでは、ビューグループは展開可能なフォルダーとして表示されます。ユーザーはこのフォルダーからグループを選択し、表示するビューを選択できます。

XProtect Smart Clientの例：矢印はビューグループを示します。ビューグループには論理グループが含まれ(アメニティと呼ばれる)、中に3つのビューが含まれます。

ビューグループと役割(説明付き)

デフォルトでは、Management Clientで定義する各役割は、ビューグループとしても作成されます。Management Clientに役割を追加すると、デフォルトで、役割がクライアントで使用できるビューグループとして表示されます。

- ビューグループを役割に基づいて、関連する役割に割り当てられたユーザー/グループに割り当てられます。これらのビューグループの権利は、後で特定の役割に設定することで、変更することができます。
- 役割に基づくビューグループには、役割の名前が付けられます。

  例：**Building A Security Staff**という名前の役割を作成する場合、**Building A Security Staff**という名前のビューグループがXProtect Smart Clientに表示されます。

  役割を追加するときに取得するビューグループだけではなく、必要に応じて他のビューグループも作成できます。また、役割を追加するときに自動的に作成されるビューグループを含め、ビューグループを削除できます。
- 役割を追加するたびにビューグループが作成されますが、ビューグループは役割に対応する必要はありません。必要に応じてビューグループを追加し、名前を変更したり、削除できます。

> ビューグループの名前を変更した場合、すでに接続済みのクライアントユーザーの場合、名前の変更が表示されるには、ログアウトしてから再度ログインする必要があります。

ビューグループの追加

1. ビューグループを右クリックして、ビューグループの追加を選択します。ビューグループの追加ダイアログボックスが開きます。
2. 新しいビューグループの名前とオプションの説明を入力し、[OK]をクリックします。

このような権限を指定するまで、役割には新規に追加されたビューグループを使用する権限はありません。新しく追加されたビューグループを使用できる役割を指定した場合、該当する役割を持つ接続済みのクライアントユーザーは、ビューグループを使用する前に、ログアウトしてから再度ログインする必要があります。

サイトナビゲーション：クライアント：Smart Clientプロファイル

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。

Smart Clientプロファイルを使用すると、システム管理者はXProtect Smart Clientの表示および動作方法、ならびにXProtect Smart Clientユーザーがアクセス権限のある機能およびペインを制御できます。ペインとオプション、最小化/最大化オプション、アイドル時間の制御、パスワードの記憶、ログイン後に表示されるビュー、印刷レポートのレイアウト、エクスポートパスなどのユーザー権限を設定できます。

システムでSmart Clientプロファイルを管理するには、クライアントを展開してSmart Clientプロファイルを選択します。Smart Clientプロファイル、役割、時間プロファイル間の関係について、また、これらを併用する方法についても学習できます(ページ 272のSmart Clientプロファイル、役割、時間プロファイルの作成と設定を参照) 。

Smart Clientプロファイルの追加と構成

まずSmart Clientプロファイルを作成してから、設定する必要があります。

1. プロファイルSmart Clientを右クリックします。
2. プロファイルの追加Smart Clientを選択します。
3. Smart Clientプロファイルの追加ダイアログで、新しいプロファイルの名前と説明を入力し、OKをクリックします。
4. 概要ペインで、作成したプロファイルをクリックして設定します。
5. 1つまたは複数、あるいは利用可能なすべてのタブでOKをクリックします。

Smart Clientプロファイルのコピー

Smart Clientプロファイルの設定や権限が複雑で、同様のプロファイルが必要な場合は、新しいプロファイルをゼロから作成するよりも、既存のプロファイルをコピーし、コピーしたプロファイルを少し修正する方が簡単な場合があります。

1. Smart Clientプロファイルをクリックし、概要ペインのプロファイルを右クリックしてSmart Clientプロファイルのコピーを選択します。
2. ダイアログボックスが表示されたら、コピーしたプロファイルの新しい一意の名前と説明を入力します。OKをクリックしま

す。

3. 概要ペインで、作成したプロファイルをクリックして設定します。1つまたは複数、あるいは利用可能なすべてのタブで設定の調整を行います。**OK** をクリックします。

Smart Clientプロファイル、役割、時間プロファイルの作成と設定

Smart Clientプロファイルで作業するときには、Smart Clientプロファイル、役割、時間プロファイルの間の関連性を理解しておくことが重要です。

- Smart Clientプロファイルは、XProtect Smart Clientでユーザー権限設定を処理します
- 役割はクライアント、MIP SDKなどでのセキュリティの設定を処理します
- 時間プロファイルはこの2つのプロファイルタイプの時間的側面を処理します

これらの3つの機能を連携させることで、XProtect Smart Clientのユーザー権限が独自の方法で制御でき、カスタマイズが可能になります。

例：XProtectSmartClientの設定で、通常の業務時間(午前8時～午後4時)に限り、選択したカメラからライブビデオを表示することのみが許可された(再生は不可)ユーザーを設定する必要があるとします。この場合、次の方法で設定が可能です。

1. Smart Clientプロファイルを作成し、例えばライブ専用などの名前を付けます。
2. ライブ専用に必要なライブまたは再生設定を指定します。
3. 時間プロファイルを作成し、例えば日中専用などの名前を付けます。
4. 日中専用に必要な期間を指定します。
5. 新規役割を作成し、例えば警備(選択したカメラ)などの名前を付けます。
6. 警備(選択したカメラ)が使用できるカメラを指定します。
7. ライブ専用Smart Clientプロファイルと日中専用時間プロファイルを警備(選択したカメラ)の役割に割り当て、3つの要素をリンクさせます。

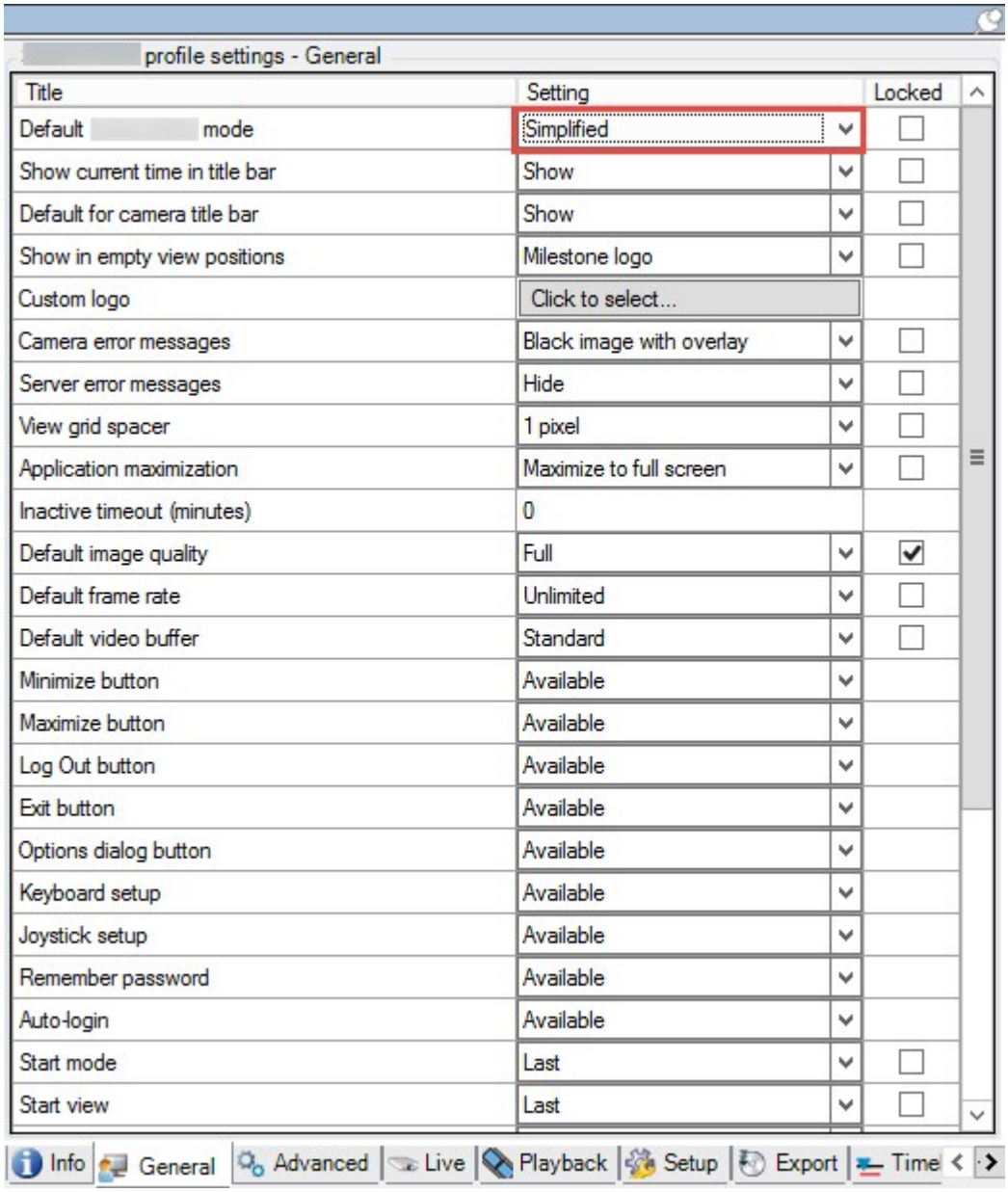
これで、3つの機能が統合され、必要な結果を作成し、簡単に微調整および調節ができるようになりました。さらに、役割を最初に作成して、次にSmart Clientプロファイルおよび時間プロファイルを作成するなど、上記とは異なる順序を含め、その他の任意の順序で設定することができます。

簡易モードをデフォルトモードとして設定

Smart Clientプロファイルを使用すると、機能とタブが制限された簡易モードで自動的にXProtect Smart Clientを開くようにシステムを構成できます。デフォルトで、XProtect Smart Clientはすべての機能とタブの詳細モードで開きます。

ある時点でXProtectSmartClientオペレータがデフォルトモード以外のモードに切り替えることを決めた場合、XProtectSmartClientは次回オペレータがプログラムを開くときのためにこの設定を記憶します。

1. Management Clientでクライアントノードを展開します。
2. 関連するSmart Clientプロファイルを選択します。
3. 全般タブをクリックします。

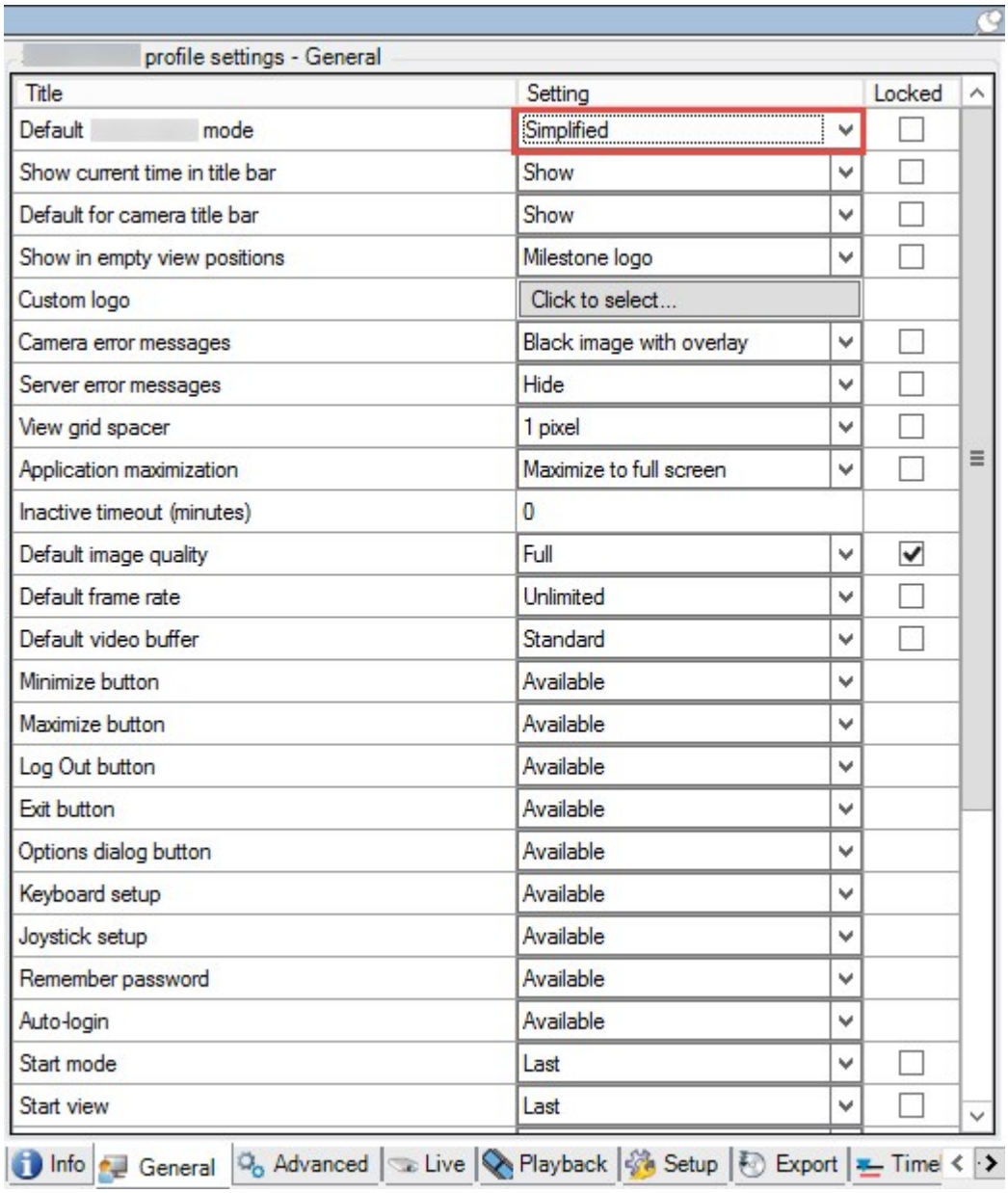


4. デフォルトSmart Clientモードリストで、簡易を選択します。ここでXProtect Smart Clientは、現在のSmart Clientプロファイルに関連付けられたユーザーを簡易モードで開きます。

オペレータが簡易モードと詳細モードで切り替えられないようにする

XProtect Smart Clientで、オペレータは簡易モードと詳細モードを切り替えることができます。ただし、XProtect Smart Clientオペレータがモードを切り替えられないようにすることができます。技術的には、XProtect Smart Clientが簡易モードまたは詳細モードで開くかどうかを決定する設定をロックする必要があります。

1. Management Clientでクライアントノードを展開します。
2. 関連するSmart Clientプロファイルを選択します。
3. 全般タブをクリックします。



4. デフォルトSmart Clientモードリストに適切な値があることを確認します。有効な場合、XProtect Smart Clientは簡易モードで開きます。
5. ロックチェックボックスを選択します。XProtect Smart Clientのモード切り替えボタンが非表示になります。

また、ページ272の簡易モードをデフォルトモードとして設定も参照してください。

Smart Clientプロファイルのプロパティ

次のタブでは、各Smart Clientプロファイルのプロパティを指定できます。XProtect Smart Clientのユーザーが変更できないように、必要に応じて、Management Clientで設定をロックできます。

情報タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
情報	名前と説明、既存のプロファイルの優先度、プロファイルを使用する役割の概要。 ユーザーがそれぞれにSmart Clientプロファイルが割り当てられた複数の役割に属している場合、Smart Clientプロファイルの取得が最優先されます。

全般タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
一般	メニュー設定の表示/非表示、および最小化と最大化、ログイン/ログアウト、起動、タイムアウト、情報、メッセージオプション、XProtect Smart Clientの特定のタブの有効化/無効化などの設定。 ⚠ カメラのエラーメッセージを非表示にすると、カメラへの接続が失われたことをオペレーターが見落としてしまうリスクが生じます。 **オンラインヘルプ**設定を使用すると、XProtect Smart Clientのヘルプシステムが無効になります。 ビデオチュートリアル設定を使用すると、XProtect Smart Clientのビデオチュートリアルボタンが無効になります。このボタンを押すとビデオチュートリアルページに移動します。https://www.milestonesys.com/support/help-yourself/video-tutorials/

詳細タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
詳細	最大デコードスレッド、インターレースの解除、および時間帯の設定などの詳細設定。 最大デコードスレッドは、ビデオストリームのデコードで使用されるデコードスレッドの数を制御します。これによって、ライブおよび再生モードで、マルチコアコンピュータのパフォーマンスを改善できます。実際のパフォーマンスの改善は、ビデオストリームによって異なります。この設定は、H.264/H.265のような高度にコード化された高解像度ビデオストリームを使用している場合に主に適用されます。この場合、大幅なパフォーマンスの改善が見られる可能性があります。たとえば、JPEGまたはMPEG-4などを使用している場合は効果が低くなります。 インターレースの解除により、ビデオはノンインターレース形式に変換されます。インターレースは、画面で画像をどのように更新するかを決定します。まず画像の奇数ラインをスキャンして画像を更新し、次に偶数のラインをスキャンしていきます。スキャン時に処理する情報が少なくなるため、より高速のリフレッシュレートが可能になります。ただし、インターレースによってちらつきが発生したり、画像のラインの半分だけが変化する場合があります。 アダプティブストリーミングを使用すれば、ビューアイテムによって要求された解像度に最も近い解像度がXProtect Smart Clientによって自動的に選択されます。これによってCPUとGPUの負荷が軽減するため、結果としてコンピュータのデコード能力とパフォーマンスが上がります。これには、異なる解像度を持つライブビデオストリームに対してマルチストリーミングを設定する必要があります。ページ214のストリームタブ(デバイス)を参照してください。

ライブタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
ライブ	ライブタブ/ペイン、カメラ再生、オーバーレイボタン、ブックマーク、境界ボックス、ライブ関連のMIPプラグインの可用性。

再生タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
再生	再生タブ/ペイン、印刷レポートのレイアウト、個別再生、ブックマーク、境界ボックス、再生関連のMIPプラグインの可用性。

設定タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
設定	一般設定/ペイン/ボタン、設定関連のMIPプラグインの可用性、およびマップの編集権限、ライブビデオバッファの編集権限。

エクスポートタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
エクスポート	パス、プライバシーマスク、ビデオ、静止画像フォーマット、ビデオおよび静止画像のエクスポート時に含まれる内容、XProtect Smart Client - Playerのエクスポートフォーマットなど。

タイムラインタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
タイムライン	音声を含めるかどうか、時間とモーションの表示/非表示、および再生ギャップを処理する方法。 他のソースから、追加のデータや追加のマーカーを表示するかどうかも選択できます。

入退室管理タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
入退室管理	イベントによってトリガーされた際に、XProtect Smart Client画面にアクセスリクエスト通知を表示するかどうかを選択します。

アラームマネージャータブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
アラームマネージャ	XProtect Smart Clientがインストールされているコンピュータに、アラームのデスクトップ通知を表示するかどうかを指定します。通知はXProtect Smart Clientの実行中にのみ(最小化されていても) 表示されます。 アラームのデスクトップ通知は、アラームに特定の優先度(中や高など) が割り当てられている場合にのみ表示されます。どのアラーム優先度で通知がトリガーされるかを設定するには、アラーム > アラームデータ設定 > アラームデータレベルに移動します。必要なアラーム優先度ごとにデスクトップ通知を有効化チェックボックスを選択します。ページ401のアラームデータ設定を参照してください。

スマートマップタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
スマートマップ	スマートマップ機能の設定を行います。 OpenStreetMapsを背景地図として使用できるようにするか、ユーザーがスマートマップにカスタムオーバーレイを追加した際にXProtect Smart Clientによって自動的に位置が作成されるようにするかを指定できます。 どれくらいの頻度でスマートマップ関連のデータがコンピューターから削除されるようにするかも指定できます。クライアント側では、XProtect Smart Clientでスマートマップがよりすばやく表示されよう、マップデータがお使いのコンピュータのキャッシュに保存されます。これにより、時間が経つにつれて、コンピュータの速度が低下する可能性があります。 コーチングはGoogle Mapsには適用されません。 Bing MapsまたはGoogle Mapsを背景地図として使用したい場合は、Bing Maps APIキーを入力するか、GoogleからMaps Static APIキーを取得します。

ビューレイアウトタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

サイトナビゲーション：クライアント：Management Clientプロファイル

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。

Management Clientプロファイルを使用すると、システム管理者は他のユーザーのManagement Clientのユーザーインターフェースを変更できます。Management Clientプロファイルを役割と関連付け、それぞれの管理者役割で使用できる機能が表示されるように、ユーザーインターフェースを制限します。

Management Clientプロファイルに役割を関連付けるには、役割の設定で情報タブに移動します。ページ341の情報タブ(役割)も参照してください。Management Clientプロファイルは、実際のアクセスではなく、システム機能の視覚的な表示のみに対応します。特定の役割でシステム機能への全体的なアクセスを制限するには、全体的なセキュリティタブに移動します。ページ343のセキュリティ全般タブ(役割) も参照してください。

マネジメントサーバーへのアクセス権を付与するには、役割設定 >マネジメントサーバー > ページ341の役割の設定で全ての役割に対して接続セキュリティ権限を有効にすることが重要です。

すべてのManagement Client要素の表示について、設定を変更できます。デフォルトでは、Management Clientプロファイルはすべての機能をManagement Clientで表示できます。

- 機能の表示を制限するには、このManagement Clientプロファイルに関係する役割を有するすべてのManagement Clientユーザーに対して、Management Clientからの機能表示を削除するために、関連する機能のチェックボックスを選択解除します。

定義済みの管理者の役割を除き、[全般セキュリティ]タブで管理サーバーのセキュリティの管理権限を割り当てられた役割に関連付けられたユーザーのみが、Management Clientプロファイルを追加、編集、および削除できます。

Management Clientプロファイルの追加と構成

既定のプロファイルを使用したくない場合は、Management Clientプロファイルを作成してから設定します。

1. プロファイルManagement Clientを右クリックします。
2. プロファイルの追加Management Clientを選択します。
3. ManagementClientプロファイルの追加ダイアログで、新しいプロファイルの名前と説明を入力し、OKをクリックします。
4. 概要ペインで、作成したプロファイルをクリックして設定します。
5. プロファイルタブで、Management Clientプロファイルの機能を選択または選択解除します。

Management Clientプロファイルのコピー

再利用したい設定を持つManagement Clientプロファイルがあれば、既に存在しているプロファイルをコピーし、新しいプロファイルを最初から作成する代わりに、このコピーに少し修正を加えて作成できます。

1. Management Clientプロファイルをクリックし、概要ペインのプロファイルを右クリックして、プロファイルManagement Clientのコピーを選択します。
2. ダイアログボックスが表示されたら、コピーしたプロファイルの新しい一意の名前と説明を入力します。OKをクリックします。
3. 概要ペインで、プロファイルをクリックし、情報タブまたはプロファイルタブへ移動して、プロファイルを設定します。

Management Clientプロファイルのプロパティ

情報タブ(Management Clientプロファイル)

情報タブでは、Management Clientプロファイルについて、以下を設定できます:

コンポーネント	要件
名前	Management Clientプロファイルの名前を入力します。
優先度	上矢印や下矢印キーを使用してManagement Clientプロファイルの優先度を設定します。
説明	プロファイルの説明を入力します。これはオプションです。
プロファイルManagement Clientを使用する役割	このフィールドは、Management Clientプロファイルに関連付けられた役割を表示します。これは編集できません。

プロファイルタブ(Management Clientプロファイル)

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。

プロファイルタブで、ManagementClientのユーザーインターフェースで、以下の要素の表示を有効または無効にすることができます:

ナビゲーション

このセクションで、Management Clientプロファイルと関連付けられている管理者ユーザーが、ナビゲーションペインにあるさまざまな特徴や機能を表示できるようにするかどうかを決めます。

ナビゲーションエレメント	説明
基本	Management Clientプロファイルと関連付けられている管理者ユーザーが、ライセンス情報およびサイト情報を表示できるようにします。
リモート接続サービス	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、Axis One-clickカメラの接続を表示できるようにします。
サーバー	Management Clientプロファイルと関連付けられている管理者ユーザーが、レコーディングサーバーおよびフェールオーバーサーバーを表示できるようにします。
デバイス	Management Clientプロファイルと関連付けられている管理者ユーザーが、カメラ、マイク、スピーカー、メタデータ、入力および出力を表示できるようにします。
Client	Management Clientプロファイルと関連付けられている管理者ユーザーが、Smart Wall、ビューグループ、Smart Clientプロファイル、Management ClientプロファイルおよびMatrixを表示できるようにします。
ルールとイベント	Management Clientプロファイルと関連付けられている管理者ユーザーが、ルール、時間プロファイル、通知プロファイル、ユーザー定義イベント、アナリティクスイベントおよびジェネリックイベントを表示できるようにします。
セキュリティ	Management Clientプロファイルと関連付けられている管理者ユーザーが、役割および基本ユーザーを表示できるようにします。

ナビゲーションエレメント	説明
システムダッシュボード	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、システムモニター、システムモニターしきい値、エビデンスロック、現在のタスク、設定レポートを表示できるようにします。
サーバーログ	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、システムログ、監査ログおよびルールトリガーログを表示できるようにします。
入退室管理	Management Clientプロファイルと関連付けられている管理者ユーザーが、システムに入退室管理システム統合またはプラグインを追加している場合、入退室管理機能を表示できるようにします。

詳細

このセクションで、Management Clientプロファイルと関連付けられている管理者ユーザーが、たとえばカメラの設定タブまたは録画タブなど、さまざまなタブで特定のデバイスチャネルを表示できるかどうかを決めます。

デバイスチャネル	説明
カメラ	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部のカメラ関連の設定やタブを表示できるようにします。
マイク	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部のマイク関連の設定やタブを表示できるようにします。
スピーカー	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部のスピーカー関連の設定やタブを表示できるようにします。
メタデータ	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部のメタデータ関連の設定やタブを表示できるようにします。
入力	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部の入力関連の設定やタブを表示できるようにします。
出力	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部の出力関連の設定やタブを表示できるようにします。

ツール メニュー

このセクションで、Management Clientプロファイルと関連付けられている管理者ユーザーが、ツールメニューの一部である要素を表示できるようにします。

ツールメニューのオプション	説明
登録済みサービス	Management Clientプロファイルと関連付けられている管理者ユーザーが、登録済みサービスを表示できるようにします。
有効な役割	Management Clientプロファイルと関連付けられている管理者ユーザーが、有効な役割を表示できるようにします。
オプション	Management Clientプロファイルと関連付けられている管理者ユーザーが、オプションを表示できるようにします。

フェデレーテッドサイト

Management Clientこのセクションでは、プロファイルと関連付けられている管理者ユーザーが、[フェデレーテッドサイト階層]ペインを表示できるかどうかを決めます。

サイトナビゲーション：クライアント：Matrixを設定中...

Matrixで、ビデオをシステムが動作しているネットワーク上のあらゆるカメラからMatrix受信者に送信できます。Matrix受信者はMatrixによってトリガーされたビデオを表示できるコンピュータです。以下の2種類のMatrix受信者があります。

- 専用のMatrixアプリケーションを実行しているコンピュータ
- XProtect Smart Clientを実行しているコンピュータ

Management Clientで設定されているMatrix受信者リストを表示するには、クライアントを[サイトナビゲーション]ペインで展開して、Matrixを選択します。Matrix設定のリストがプロパティペインに表示されます。

> コンピュータにMatrixまたはMatrix Monitorのいずれがある場合でも、各XProtect Smart Client受信者はMatrixによってトリガーされたビデオを受信するように設定されていなければなりません。詳細については、ページ31のXProtect Smart Wall (説明付き)とページ26のXProtect Smart Client (説明付き)を参照してください。

Matrix受信者の追加

Matrixで、既存のMatrix MonitorまたはXProtect Smart Clientインストールなどに既存の受信者を追加するにはManagement Client:

1. クライアントを展開し、**Matrix**を選択します。
2. 設定を右クリックして、**Matrix**の追加を選択します**Matrix**。
3. の追加**Matrix**ダイアログボックスのフィールドを入力します。
    1. アドレスフィールドに、目的のMatrix受信者のIPアドレスまたはホスト名を入力します。
    2. ポートフィールドにMatrix受信者のインストールで使用するポート番号を入力します。ポート番号とパスワードを次の方法で検索できます。Matrix Monitorアプリケーションの場合、Matrix Monitorの設定ダイアログボックスに移動します。XProtect Smart Clientについては、XProtect Smart Clientユーザーマニュアル。
4. **OK**をクリックします。

これで、ルールでMatrix受信者を使用できます。

> システムは指定されたポート番号またはパスワードが正しいこと、または指定されたポート番号、パスワード、またはタイプが実際のMatrix受信者に対応することを検証しません。情報を正しく入力したことを確認してください。

ビデオをMatrixの受領者へ送信するためのルールを定義

Matrix受信者にビデオを送信するには、関連するMatrix受信者へのビデオ転送をトリガーするルールにMatrix受信者を含める必要があります。操作方法:

1. [サイトナビゲーション]ペインで、[ルールとイベント]を展開し[ルール]を選択します。ルールを右クリックし、ルールの管理ウィザードを開きます。手順1でルールタイプを選択し、手順2で条件を選択します。
2. ルールの管理の手順3(手順**3:** [アクション]で[設定]**Matrix**を選択して<デバイス>アクションを表示します。
3. 初期のルール説明のMatrixリンクをクリックします。
4. 設定の**Matrix**選択ダイアログボックスで、関連するMatrix受信者を選択し、**OK**をクリックします。
5. 初期ルール説明のデバイスリンクをクリックし、Matrix受信者にビデオを送信するカメラを選択して、**OK**をクリックして選択を確認します。
6. ルールが完了すると終了をクリックするか、必要に応じて別のアクションまたは終了アクションを定義します。

> Matrix受信者を削除すると、Matrix受信者を含めるすべてのルールが動作を停止します。

複数のXProtect Smart Clientビューに同じビデオを送信

Matrix-受信者がXProtect Smart Clientの場合、ビューのMatrixの位置が同じポート番号とパスワードを使用していれば、同じビデオを複数のXProtect Smart ClientのビューのMatrix位置に送信できます:

1. XProtect Smart Clientで、関連するビューと、Matrix同じポート番号とパスワードを共有する位置を作成します。
2. Management Clientで、関連するXProtect Smart Client をMatrix-受信者として追加します。
3. Matrix受信者をルールに含めることができます。

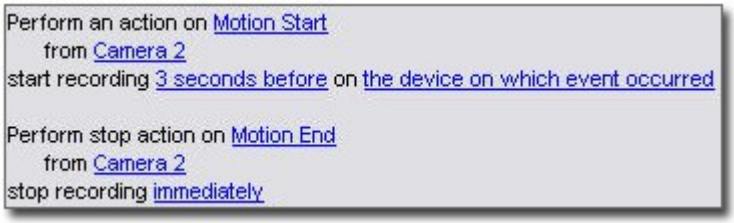
サイトナビゲーション: ルールとイベント

この記事では、イベントとルールをどのように構成すれば、システム内でアクションとアラームをトリガーしやくすなるかについて説明します。また、eメール通知とルール上のタイムリミットの設定法についても説明します。

ルールおよびイベント(説明付き)

ルールは、システムの中心的な要素です。ルールは、非常に重要な設定を決定します。例えばカメラの録画開始、PTZカメラのパトロール開始、通知送信等を開始するタイミングなどを決定します。

例¯モーションを検知したときに特定のカメラで録画を開始するよう指定したルール:



イベントはルールの管理ウィザードを使用している時の中心的な要素です。ウィザードでは、イベントはアクションをトリガーするために主に使用されます。例えば、モーションを検知した場合(イベント)に、監視システムが特定のカメラからのビデオの録画を開始するというアクションを取ることを指定するルールを作成します。

ルールは以下の2種類の条件によってトリガーされます:

名前	説明
イベント	イベントが監視システムで発生した場合(例えば、モーションを検知した時、あるいはシステムが外部センサーから入力を受信した時)。
タイムインターバル	特定の時間を入力した場合(例えば、 2007年8月16日火曜日07:00～07:59

名前	説明
	または毎週土曜日と日曜日
定期スケジュール	詳細な定期スケジュールでは、アクションをどの時点で実行するかを設定できます。 例: • 毎週火曜日の15:00～15:30の間に1時間おきに実行 • 3か月ごとにその月の15日の11:45に実行 • 毎日15:00～19:00の間に1時間おきに実行 ここでは、Management Clientがインストールされているサーバーのローカル時刻設定にもとづいた時刻が使用されます。 詳細については、「ページ316の定期スケジュール」を参照してください。

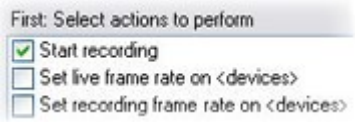
ルールとイベントで以下の作業ができます。

- ルール: ルールは、システムの中心的な要素です。監視システムの動作の大半が、ルールにより決定されます。ルールを作成するときには、すべてのタイプのイベントを使用できます
- 時間プロファイル: 時間プロファイルは、Management Clientで定義する期間です。これは、Management Clientでルールを作成するときに使用することができます。例えば、特定のアクションが特定の時間プロファイル内に発生することを指定するルールを作成するために使用できます
- 通知プロファイル: 通知プロファイルを使用して、事前定義されたEメール通知を設定できます。この通知は、ルールによってトリガーされ、例えば特定のイベントが発生したときに自動的に起動されます
- ユーザー定義イベント: ユーザー定義イベントは、カスタムメイドのイベントであり、ユーザーがシステムで手動でイベントをトリガーしたり、システムからの入力に応答することが可能になります
- アナリティクスイベント: アナリティクスイベントは、外部のサードパーティのビデオコンテンツ分析(VCA)プロバイダから受け取ったデータです。アナリティクスイベントはアラームの条件として使用できます
- ジェネリックイベント: ジェネリックイベントでは、単純な文字列をIPネットワーク経由でシステムに送信し、XProtectイベントサーバーのアクションをトリガーできます

イベントのリストについては、ページ298のイベント概要を参照してください。

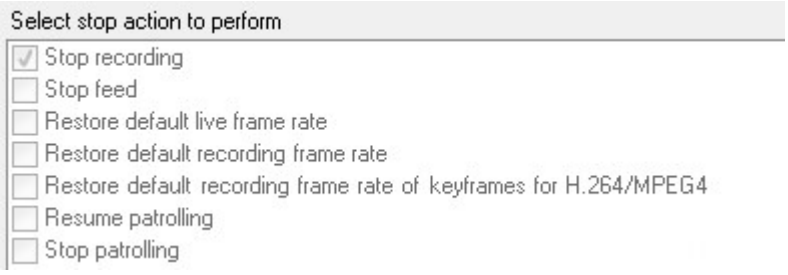
アクションおよびアクションの停止(説明付き)

ルールの管理ウィザードでルールを追加する場合(ページ314のルールの追加を参照)、次のさまざまなアクションから選択できます。



これらのアクションの一部は、終了アクションが必要です。例:録画の開始アクションを選択する場合は、録画が開始され、無限に続く可能性があります。したがって、録画の開始アクションには、レコーディング停止という強制終了アクションがあります。

ルールの管理ウィザードでは、必要に応じて停止アクションを指定できます:



終了アクションの選択。この例で、強制終了アクション(選択済み、淡色表示)、関連しない終了アクション(淡色表示)、およびオプションの終了アクション(選択可能)に注目してください。

XProtectシステムの各アクションのタイプについて説明されています。システムインストールがベンダー固有のプラグインなどを使用している場合には、追加のアクションを使用できる場合があります 各タイプのアクションでは、終了アクション情報も一覧表示されます。

アクション	説明
<デバイス>で録画を開始します	録画を開始し、選択されたデバイスからのデータベースへのデータの保存を開始します。 このタイプのアクションを選択すると、ルールの管理ウィザードにより、以下を指定するように指示されます。 録画の開始時期。これは、アクションを起こすデバイス上でただちに開始されるか、またはトリガータイムインターバルを開始する/イベントをトリガーする前に何秒か待ってから開始されます。 このタイプのアクションでは、アクションがリンクされているデバイス上で録画が有効になっている必要があります。プレバッファが該当するデバイスで有効になっている場合のみ、イベントまたはタイムインターバルの前からデータを保存できます。録画タブで、デバイスの録画を有効にし、プレバッファ設定を指定します。

アクション	説明
	終了アクションが必要: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。レコーディング停止。 この終了アクションがない場合、録画が無制限に続く可能性があります。また、その他の終了アクションを指定することもできます。
<デバイス>で映像配信を開始します	デバイスからシステムにデータ供給を開始します。デバイスからの配信が開始されると、データはデバイスからシステムに転送されます。この場合、データタイプに従ってライブ表示と録画が可能です。 このタイプのアクションを選択すると、ルールの管理ウィザードにより、配信を開始するデバイスを指定するように指示されます。システムには、配信が常にすべてのカメラで開始されることを保証するデフォルトのルールが含まれています。 終了アクションが必要: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。映像配信の停止。 また、その他の終了アクションを指定することもできます。 強制終了アクションの映像配信の停止を使用してデバイスからの配信を停止すると、データはデバイスからシステムに転送されません。この場合、たとえば、ビデオのライブ表示と録画ができなくなります。ただし、配信を停止したデバイスは、レコーディングサーバーとの通信が維持されます。また、デバイスを手動で無効にしたときとは異なり、デバイスからの配信をルールにより自動的に再開することが可能です。 このタイプのアクションにより、選択されたデバイスのデータ配信にアクセスできますが、録画設定は個別に指定する必要があるため、データが録画されることを保証するものではありません。
<Smart Wall> を <preset> に設定します	XProtect Smart Wallを選択したプリセットに設定します。プリセットSmart Wallタブでプリセットを指定します。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<Smart Wall> <monitor>を設定して、<cameras>を表示	特定のXProtect Smart Wallモニターに、このサイトまたはMilestone Federated Architectureで設定されている子サイト上で選択されているカメラからのライブビデオを表示するよう設定します。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントま

アクション	説明
	たは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<Smart Wall> <monitor>を設定して、テキスト <messages> を表示	特定のXProtect Smart Wallモニターを設定し、最大200文字のユーザー定義テキストメッセージを表示します。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<Smart Wall> モニター<monitor> から <<cameras>> を削除	特定のカメラのビデオの表示を停止します。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>のライブフレームレートを設定します	カメラのデフォルトのフレームレートの代わりに、選択したカメラからライブビデオをシステムで表示するときに使用する特定のフレームレートを設定します。この操作は設定タブで行います。 このタイプのアクションを選択すると、ルールの管理ウィザードにより、設定するフレームレートとデバイスを指定するように指示されます。必ず、指定するフレームレートが該当するカメラで利用できることを確認してください。 終了アクションが必要: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。デフォルトのライブフレームレートを復元します。 この終了アクションがない場合、デフォルトのフレームレートが復元されない可能性があります。また、その他の終了アクションを指定することもできます。
<デバイス>の録画のフレームレートを設定します	カメラのデフォルトのレコーディングフレームレートではなく、データベースの選択済みカメラから録画済みビデオを保存するときに使用する特定のフレームレートを設定します。 このタイプのアクションを選択すると、ルールの管理ウィザードにより、設定するレコーディングフレームレートとカメラを指定するように指示されます。 レコーディングフレームレートは、各フレームがJPEG画像に圧縮されるビデオコーデックであるJPEGでのみ指定できます。また、このタイプのアクションでは、アクションがリンクされているカメラ上で録画が有効になっている必要があります。録画タブで、カメラの録画を有効にします。指定できる最大フレームレートは、カメラタイプおよび選択された画像の解像度によって異なります。 終了アクションが必要: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。デフォルトのレコーディングフレームレートを復元します。

アクション	説明
	この終了アクションがない場合、デフォルトのレコーディングフレームレートが復元されない可能性があります。また、その他の終了アクションを指定することもできます。
<devices> にある **MPEG-4/H.264/H.265**のすべてのフレームのレコーディングフレームレートを設定	データベースで選択されたカメラから録画済みビデオを保存するときに、キーフレームだけではなく、すべてのフレームを録画するために使用するフレームレートを設定します。録画タブで、キーフレームのみの録画機能を有効にします。 このタイプのアクションを選択すると、ルールの管理ウィザードにより、アクションを適用するデバイスを選択するように指示されます。 MPEG-4/H.264/H.265のキーフレームレコーディングのみを有効にできます。また、このタイプのアクションでは、アクションがリンクされているカメラ上で録画が有効になっている必要があります。録画タブで、カメラの録画を有効にします。 終了アクションが必要: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。 **MPEG-4/H.264/H.265**のキーフレームのデフォルトのレコーディングフレームレートを復元 この終了アクションがない場合、デフォルト設定が永久に復元されない可能性があります。また、その他の終了アクションを指定することもできます。
PTZ 優先度 **<priority>** で **<profile>**を使用して **<device>** でのパトロールを開始	特定の優先度が設定された特定のPTZカメラで、特定のパトロール設定に従って、PTZパトロールを開始します。ここで、プリセット位置、タイミング設定などを含め、パトロールの実行方法を正確に定義します。 システムが古いバージョンのシステムからアップグレードされた場合、古い値(非常に低い、低、中、高および非常に高い) は次のように解釈されます。 • 非常に低い = 1000 • 低 = 2000 • 中 = 3000 • 高 = 4000 • 非常に高い = 5000 このタイプのアクションを選択すると、ルールの管理ウィザードにより、パトロール設定を選択するように指示されます。1つデバイスでは1つのパトロール設定のみを選択できます。複数のパトロール設定を選択することはできません。

アクション	説明
	このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスであることが必要です。 デバイスに1つ以上のパトロール設定が定義されている必要があります。パトロールタブで、PTZカメラのパトロール設定を定義します。 終了アクションが必要: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。 パトロールを停止します この終了アクションがない場合、パトロールが停止しない可能性があります。また、その他の終了アクションを指定することもできます。
<デバイス>でのパトロールの一時停止します	PTZパトロールの一時停止 このタイプのアクションを選択すると、ルールの管理ウィザードにより、パトロールを一時停止するデバイスを指定するように指示されます。 このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスであることが必要です。 デバイスに1つ以上のパトロール設定が定義されている必要があります。パトロールタブで、PTZカメラのパトロール設定を定義します。 終了アクションが必要: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。パトロールを再開します この終了アクションがない場合、パトロールが無制限に一時停止したままになる可能性があります。また、その他の終了アクションを指定することもできます。
PTZ優先度<priority>で<device>を<preset>位置に移動	特定のカメラを特定のプリセット位置に移動します。ただし、必ず優先度に従います。このタイプのアクションを選択すると、ルールの管理ウィザードにより、プリセット位置を選択するように指示されます。1つのカメラで選択できるのは、1つのプリセット位置のみです。複数のプリセット位置を選択することはできません。

アクション	説明
	このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスであることが必要です。 このアクションでは、デバイスに1つ以上のプリセット位置が定義されている必要があります。プリセットタブで、PTZカメラのプリセット位置を定義します。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
PTZ優先度<priority>で<devices>をデフォルトのプリセットに移動	1つ以上のカメラを該当するプリセット位置に移動します。ただし、必ず優先度に従います。このタイプのアクションを選択すると、ルールの管理ウィザードにより、アクションを適用するデバイスを選択するように指示されます。 このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスであることが必要です。このアクションでは、デバイスに1つ以上のプリセット位置が定義されている必要があります。プリセットタブで、PTZカメラのプリセット位置を定義します。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
デバイス出力を<状態>に設定します	デバイスの出力を特定の状態(有効化または無効化)に設定します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、設定する状態とデバイスを指定するように指示されます。 このタイプのアクションでは、アクションがリンクされるデバイスはそれぞれ、1つ以上の外部出力装置が出力ポートに接続されていなければなりません。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
ブックマークを<device>で作成	選択されたデバイスからライブストリーミングまたは録画のブックマークを作成します。ブックマークを使用すると、特定のイベントまたは期間を簡単に再追跡できます。ブックマーク設定は、オプショ

アクション	説明
	ンダイアログボックスで制御されます。このタイプのアクションを選択すると、ルールの管理ウィザードにより、ブックマークの詳細を指定し、デバイスを選択するように指示されます。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
＜デバイス＞で音声＜メッセージ＞を＜優先度＞で再生します	イベントによってトリガーされた選択したデバイスで音声メッセージを再生します。デバイスは主にスピーカーとカメラです。 このタイプのアクションでは、ツール > オプション> 音声メッセージタブでシステムにメッセージがアップロードされている必要があります。 同じイベントにさらにルールを作成したり、各デバイスへ異なるメッセージを送信することも可能です。シーケンスを制御する優先度はルールおよびスピーチタブの役割のためのデバイスに設定されたものです: • メッセージを再生しながら同じ優先度の別のメッセージを同じスピーカーに送信する場合、最初のメッセージが完了してから第2のメッセージが始まります • メッセージを再生しながら優先度の高い別のメッセージを同じスピーカーに送信する場合、最初のメッセージを中断し直ちに第2のメッセージが始まります
通知を<プロファイル>に送信します	特定の通知プロファイルを使用して通知を送信します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、通知プロファイルとプリアラーム画像を含めるデバイスを選択するように指示されます。1つの通知プロファイルのみを選択できます。複数の通知プロファイルを選択することはできません。1つの通知プロファイルには複数の受信PCを含めることができます。 同じイベントにさらにルールを作成したり、各通知プロファイルへ異なる通知を送信することも可能です。ルールリストのルールを右クリックすることで、ルールの内容をコピーして再利用できます。 このタイプのアクションでは、1つ以上の通知プロファイルを設定する必要があります。画像を含むオプションが該当する通知プロファイルで有効になっている場合のみ、プリアラーム画像が含まれます。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
新しい<ログエントリ>を追加します	ルールログにエントリを作成します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、ログエントリのテキストを指定するように指示されます。ログテキストを指定すると、**$DeviceName$**、**$EventName$**などの変数を簡単にログメッセージに挿入できます。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。

アクション	説明
<デバイス>のプラグインを開始します	1つ以上のプラグインを開始します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、必要なプラグインと、プラグインを起動するデバイスを選択するように指示されます。 このタイプのアクションでは、システムで1つ以上のプラグインがインストールされていることが必要です。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>のプラグインを停止します	1つ以上のプラグインを停止します。このタイプのアクションを選択すると、[ルールの管理]ウィザードにより、必要なプラグインと、プラグインを停止するデバイスを選択するように指示されます。 このタイプのアクションでは、システムで1つ以上のプラグインがインストールされていることが必要です。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
新しい設定を<デバイス>に適用します	1つ以上のデバイスのデバイス設定を変更します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、必要なデバイスを選択するように指示され、指定したデバイス関連の設定を定義できます。 複数のデバイスで設定を定義する場合は、指定したデバイスのすべてで使用可能な設定のみを変更できます。 例: アクションがデバイス1およびデバイス2にリンクするように指定します。デバイス1には、設定A、B、およびCがあり、デバイス2には設定B、C、およびDがあります。この場合、両方のデバイスで使用可能な設定BおよびCのみを変更できます。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
Matrix を ビュー <devices>に設定	選択されたカメラのビデオが、ビデオをトリガーするMatrixを表示可能なコンピュータ(XProtect Smart ClientまたはMatrix Monitorアプリケーションがインストールされているコンピュータ)に表示されるようにします。 このタイプのアクションを選択すると、ルールの管理ウィザードにより、Matrix受信PCと、選択されたMatrix受信PCでビデオを表示する1つ以上のデバイスを選択するように指示されます。 Matrixこのタイプのアクションでは、受信PCを一度に1つのみ選択できます。選択されたデバイスのビデオを複数のMatrix受信者で表示するには、各目的のMatrix受信者のルールを作成する

アクション	説明
	か、XProtect Smart Wall機能を使用する必要があります。ルールリストのルールを右クリックすることで、ルールの内容をコピーして再利用できます。このようにして、類似したルールをゼロから作成せずに済みます。 Matrix受信PC自体の設定の一部として、ユーザーはMatrix通信に必要なポート番号とパスワードを指定する必要があります。ユーザーがこの情報にアクセスできることを確認してください。Matrix一般的に、ユーザーは許可されたホストのIPアドレス(ビデオをトリガするの表示に関するコマンドが受信されるホスト)も定義する必要があります。この場合、ユーザーはマネジメントサーバー(または使用されるルーターまたはファイアウォール)のIPアドレスも把握していなければなりません。
SNMPトラップの送信	選択されたデバイスのイベントを録画する小さいメッセージを作成します。SNMPトラップのテキストは自動生成されるため、カスタマイズできません。これにはソースタイプとイベントが発生したデバイス名が含まれています。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>からリモート録画を取得して保存します	選択した(エッジ録画をサポートする)デバイスから、指定した期間の前後とトリガーイベント後のリモート録画を取得し保存します。 このルールは、接続が復旧したときに自動的にリモート録画を取得する設定とは関係ありません。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>から<開始時刻と終了時刻>間のリモート録画を取得して保存します	選択されたデバイス(エッジ録画に対応するデバイス)からリモート録画を取得して保存します。 このルールは、接続が復旧したときに自動的にリモート録画を取得する設定とは関係ありません。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
添付画像の保存	画像を受信しましたイベントから画像を受信(カメラからSMTPメール経由で送信)したとき、今後使用できるように画像を保存します。今後、他のイベントでもこのアクションをトリガーすることができます。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントま

アクション	説明
	たは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<アーカイブ> のアーカイブを有効にします	1つ以上のアーカイブでアーカイブを開始します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、必要なアーカイブを選択するように指示されます。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<サイト>の<ユーザー定義イベント>を起動します	通常はMilestone Federated Architectureに関連していますが、単一サイト設定でも使用可能です。このルールは、オンサイトでユーザー定義イベントをトリガーするために使用されます。通常は、フェデレーテッド階層内のリモートサイトです。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<アクセス リクエスト通知>を表示	XProtect Smart Clientスクリーン上でのアクセスリクエスト通知は、トリガーするイベントの条件を満たしたときにポップアップします。Milestoneでは、このアクションに対するイベントをトリガーするために入退室管理イベントを使用することをお勧めします。これは、アクセスリクエストの通知は通常関連する入退室管理コマンドとカメラの操作に対応して設定されているためです。 このタイプのアクションでは、システムで1つ以上の入退室管理プラグインが使用可能であることが必要です。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<カメラ>を<ルールに基づいたDLNA チャネル>に設定する	イベントごとに、カメラはルールで定められたDLNAチャネルに対して設定されます。この類のアクションには、お使いのシステムにDLNAサーバーがインストールされていることが必要となります。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<ルールに基づいたDLNAチャネル>から<カメラ>を削除する	カメラは、イベントに基づいて、ルールで定められたDLNAチャネルから除去されます。この類のアクションには、お使いのシステムにDLNAサーバーがインストールされていることが必要となります。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<ルールに基づいたDLNAチャネル>から現在のカメラを削除する	アクティブストリームのあるカメラは、ルールに定められたDLNAチャネルに基づいたイベントから削除されます。この類のアクションには、お使いのシステムにDLNAサーバーがインストールされていることが必要となります。 強制停止アクションなし: このタイプのアクションでは、停止アクションは必要ありません。イベントま

アクション	説明
	たは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
ハードウェアデバイスのパスワードを変更	選択したハードウェアデバイスのパスワードを、特定のハードウェアデバイスのパスワード要件にもとづいてランダム生成されたパスワードに変更します。対応ハードウェアデバイスのリストについては、https://www.milestonesys.com/community/business-partner-tools/supported-devices/を参照してください。 このアクションは、[<recurring time>へのアクションを実行]ルールタイプを使用してルールを設定した場合にのみ実行できます。 アクションに対して以下のイベントを利用できます: • ページ308の定期的なパスワード変更が開始 • ページ308の定期的なパスワード変更が正常に完了 • ページ308の定期的なパスワード変更がエラーを伴って完了 このタイプのアクションには、停止アクションがありません。 このアクションの進行状況は[現在のタスク]ノードで確認できます。詳細については、ページ387の現在のタスク(説明付き)を参照してください。 アクションの結果を表示するには、[システムログ]タブで[サーバーログ]ノードに移動します。詳細については、ページ118のサーバーログタブ(オプション)を参照してください。 詳細については、ページ392のシステムログ(プロパティ)を参照してください。

イベント概要

ルールの管理ウィザードでイベントベースのルールを追加する場合、さまざまなイベントタイプから選択できます。概要を把握するために、現在の状況に応じて、選択可能なイベントがグループに一覧表示されます。

ハードウェア:

一部のハードウェアでは、モーション検知などのイベントをそれ自体で作成できます。これらはイベントとして使用できますが、システムで使用する前にハードウェア上に設定する必要があります。すべてのタイプのカメラで改ざんや温度変化を検知できるとは限らないため、一部のハードウェアで表示されているイベントのみを使用できます。

ハードウェア - 設定可能イベント:

ハードウェアから設定可能なイベントは、デバイスドライバーから自動的にインポートされます。つまり、ハードウェアによって異なるため、ここでは説明していません。設定可能イベントは、ハードウェアのイベントタブで設定して、システムに追加されるまでトリガーされません。設定可能イベントの中には、カメラ(ハードウェア) 自体を設定する必要があるものもあります。

ハードウェア - 事前定義イベント:

イベント	説明
通信エラー(ハードウェア)	ハードウェアへの接続が失われたときに発生します。
通信が開始しました(ハードウェア)	ハードウェアとの通信が正常に確立されたときに発生します。
通信が停止しました(ハードウェア)	ハードウェアとの通信が正常に停止したときに発生します。

デバイス - 設定可能イベント:

デバイスから設定可能なイベントは、デバイスドライバーから自動的にインポートされます。つまり、デバイスによって異なるため、ここでは説明していません。設定可能イベントは、デバイスのイベントタブで設定して、システムに追加されるまでトリガーされません。

デバイス - 事前定義イベント:

イベント	説明
ブックマーク参照が要求されました	クライアントで、ライブまたは再生モードのブックマークが作成されたときに発生します。また、デフォルトのブックマーク録画ルールを使用するための要件です。
通信エラー(デバイス)	デバイスへの接続が失われたとき、およびデバイスとの通信の試みが発生し、試みが失敗したときに発生します。
通信が開始しました(デバイス)	デバイスとの通信が正常に確立されたときに発生します。

イベント	説明
通信が停止しました (デバイス)	デバイスとの通信が正常に停止したときに発生します。
エビデンスロックが変更されました	デバイスのエビデンスロックがクライアントユーザーまたはMIP SDKを通して変更されたときに発生します。
エビデンスロックが設定されました	デバイスのエビデンスロックがクライアントユーザーまたはMIP SDKを通して作成されたときに発生します。
エビデンスロックが解除されました	デバイスのエビデンスロックがクライアントユーザーまたはMIP SDKを通して解除されたときに発生します。
フィードオーバーフローを開始しました	レコーディングサーバーが受信したデータを指定された速度で処理できず、一部の録画が強制的に破棄される場合に、映像配信のオーバーフロー(メディアのオーバーフロー) が発生します。 サーバーが正常な場合、通常、映像配信のオーバーフローはディスク書き込み速度が遅いために発生します。書き込むデータ量を減らすか、ストレージシステムのパフォーマンスを改善することで解決できます。カメラのフレームレート、解像度、または画質を下げることで、データ書き込み量を減らすことができますが、これにより画質が落ちる場合があります。録画品質を下げたくない場合は、代わりに、追加のドライブを設置して負荷を分散するか、高速ディスクまたはコントローラを設置して、ストレージシステムのパフォーマンスを改善します。 このイベントは、レコーディングフレームレートの低下などの問題を回避するアクションをトリガーするために使用できます。
フィードオーバーフローが停止しました	フィード オーバーフロー (ページ300のフィードオーバーフローを開始しましたを参照) が終了すると発生します。
ライブクライアント映像配信が要	クライアントユーザーがデバイスからライブストリームを要求するときに発生します。 このイベントは要求時に発生します。その後、クライアントユーザーが要求されたライブ映像配信を表示する権限がない場合や、映像配信が何らかの理由で停止した場合など、クライアントのユーザーの要求が

イベント	説明
求されました	失敗した場合にも、イベントが発生します。
ライブクライアントフィードが終了しました	クライアントユーザーがデバイスからライブストリームを要求しなくなったときに発生します。
手動録画が開始されました	クライアントユーザーがカメラの録画セッションを開始したときに発生します。 イベントは、デバイスがルールアクションを通してすでに録画している場合でもトリガーされます。
手動録画が停止されました	クライアントユーザーがカメラの録画セッションを停止したときに発生します。 ルールシステムも録画セッションを開始した場合は、手動の録画が停止した後でも録画が続けられます。
印付きデータ(エビデンスロックまたはブックマーク)参照が要求されました	エビデンスロックがクライアントまたはMIP SDKを通して再生モードで作成されたときに発生します。 ルールで使用できるイベントが作成されます。
モーションが開始しました	システムがカメラから受信したビデオでモーションを検知したときに発生します。 このタイプのイベントでは、イベントがリンクされるカメラのシステムのモーション検知を有効にする必要があります。 システムのモーション検知に加え、カメラ自体でモーションを検知してモーション開始(ハードウェア)イベントをトリガーできるカメラもありますが、カメラハードウェアやシステムの設定によって異なります。ページ299のハードウェア - 設定可能イベント: も参照してください。
モーションが停止しました	受信したビデオでモーションを検知しなくなったときに発生します。ページ301のモーションが開始しましたも参照してください。 このタイプのイベントでは、イベントがリンクされるカメラのシステムのモーション検知を有効にする必要があります。 システムのモーション検知に加え、カメラ自体でモーションを検知してモーション停止(ハードウェア)イベントをトリガーできるカメラもありますが、カメラハードウェアやシステムの設定によって異なります。ページ299の

イベント	説明
	ハードウェア - 設定可能イベント: も参照してください。
出力がアクティブになりました	デバイスの外部出力ポートが有効になったときに発生します。 このタイプのイベントでは、システムの1つ以上のデバイスが出力ポートに対応している必要があります。
出力が変更されました	デバイスの外部出力ポートの状態が変更されたときに発生します。 このタイプのイベントでは、システムの1つ以上のデバイスが出力ポートに対応している必要があります。
出力が無効になりました	デバイスの外部出力ポートが無効になったときに発生します。 このタイプのイベントでは、システムの1つ以上のデバイスが出力ポートに対応している必要があります。
PTZ手動セッションを開始しました	(スケジュール済みパトロールまたはイベントによる自動トリガーに基づくPTZセッションとは異なり、) 手動で操作したPTZセッションがカメラで開始されたときに発生します。 このタイプのイベントでは、イベントがリンクされているカメラがPTZカメラである必要があります。
PTZ手動セッションを中止しました	(スケジュール済みパトロールまたはイベントによる自動トリガーに基づくPTZセッションとは異なり、) 手動で操作したPTZセッションがカメラで停止されたときに発生します。 このタイプのイベントでは、イベントがリンクされているカメラがPTZカメラである必要があります。
録画が開始しました	録画が開始したときに発生します。手動の録画が開始された場合は、別のイベントが発生します。
録画を中止しました	録画が停止したときに発生します。手動の録画が停止された場合は、別のイベントが発生します。
設定が変更されました	デバイスの設定が正常に変更されたときに発生します。
設定の変更エラー	デバイスの設定変更が試みられ、試みが失敗したときに発生します。

外部イベント- 事前定義イベント:

イベント	説明
音声メッセージ再生を要求しました	音声メッセージがMIP SDKを通じてリクエストされたときにアクティブ化されます。 MIP SDKによって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン(たとえば、外部入退室管理システムまたは同様の機能などとの統合) を開発できます。
録画の開始を要求しました	録画の開始がMIP SDK経由で要求されたときに有効になります。 MIP SDKによって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン(たとえば、外部入退室管理システムまたは同様の機能などとの統合) を開発できます。
録画の停止を要求しました	録画の停止がMIP SDK経由で要求されたときに有効になります。 MIP SDKによって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン(たとえば、外部入退室管理システムまたは同様の機能などとの統合) を開発できます。

外部イベント- ジェネリックイベント:

ジェネリックイベントでは、シンプルな文字列をIPネットワーク経由でシステムに送信し、システムのアクションをトリガーできます。ジェネリックイベントの目的は、可能な限り多くの外部ソースがシステムと相互作用できるようにすることです。

外部イベント- ユーザー定義イベント:

各システムに合うようカスタムメイドしたイベントも選択することができます。このようなユーザー定義イベントは、以下で使用できます。

- クライアントユーザーが手動でイベントをトリガーしながら、クライアントのライブビデオを視聴できるようにする
- その他多数の目的。たとえば、特定のデータタイプをデバイスから受信したときに発生するユーザー定義イベントを作成することができます

  ページ325のユーザー定義のイベント(説明付き) も参照してください

レコーディングサーバー:

イベント	説明
アーカイブが使用できます	レコーディング サーバーのアーカイブが利用不可の後に使用できるようになった場合に発生します。ページ304のアーカイブが使用できませんも参照してください。
アーカイブが使用できません	ネットワークドライブにあるアーカイブへの接続が失われた場合等、レコーディングサーバーのアーカイブが使用できなくなったときに発生します。このような場合、録画をアーカイブできません。 イベントを使って、Eメール通知が自動的に組織内の関連するスタッフに送信されるようにするために、アラームまたは通知プロファイルをトリガーすることができます。
アーカイブが終了していません	次の予定が開始する際、最後のアーカイブラウンドでレコーディングサーバーのアーカイブが終了していないときに発生します。
保持サイズを設定する前に、録画データベースを削除	保存期間のリミットが、データベースサイズのリミットより先に達した場合に発生します。
保持時間を設定する前に、録画データベースを削除	データサイズのリミットが、保存期間のリミットより先に達した場合に発生します。
データベースのディスクが一杯です – 自動アーカイブ中	データベースディスクが一杯のときに発生します。データベースディスクは、ディスクの残り容量が500 MB未満になると一杯とみなされます。 空き容量が5GB未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます(または、次のアーカイブが定義されていない場合は削除されます) 。
データベースのディスクが一杯です - 削除中	データベースディスクが満杯か、1GB未満の空き容量しかない場合に発生します。次のアーカイブが定義されていても、データは削除されます。データベースには、必ず250MBの空き容量が必要です。この制限に達した場合(データが十分速やかに削除されていない場合) 、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より5GB少なくなります。
データベースが一杯です - 自動アーカイブ中	レコーディングサーバーのアーカイブが一杯になり、ストレージのアーカイブに自動アーカイブする必要があるときに発生します。
データベースの修復	データベースが破損した場合に発生します。その場合、システムは自動的に以下の2つのデー

イベント	説明
	タベース修復方法を試行します。素早い修復と完全な修復
データベースストレージが使用できます	レコーディング サーバーのストレージが利用不可の後に使用できるようになった場合に発生します。ページ305のデータベース ストレージが使用できませんも参照してください。 例えば、データベースのストレージが使用できませんイベントにより停止された場合、このイベントを使って録画を開始することができます。
データベース ストレージが使用できません	ネットワークドライブにあるストレージへの接続が失われた場合など、レコーディングサーバーのストレージが使用できなくなったときに発生します。このような場合、録画をアーカイブできません。 イベントを使って、Eメール通知が自動的に組織内の関連する人に送信されるようにするために、録画を停止して通知プロファイルまたはアラームをトリガーできます。
フェールオーバー暗号化通信エラー	フェールオーバーサーバーと監視中のレコーディングサーバーとの間でSSL通信エラーが生じた際に発生します。
フェールオーバーが開始しました	レコーディングサーバーからフェールオーバーレコーディングサーバーに切り替わるときに発生します。ページ172のフェールオーバーレコーディングサーバー(説明付き)も参照してください。
フェールオーバーが停止しました	レコーディングサーバーが再び使用できるようになり、フェールオーバーレコーディングサーバーから引き継ぐことができるようになると発生します。

システムモニターイベント

システム モニター イベントは、[システム モニターしきい値]ノードで設定されたしきい値を超過するとトリガーされます。ページ382のシステムモニターしきい値(説明付き)も参照してください。

この機能は、Data Collectorサービスが実行中であることが必須です。

システムモニター> サーバー

イベント	説明
CPU使用率重大	CPU使用率が、重大CPUしきい値を上回った際に発生します。

イベント	説明
CPU使用率正常	CPU使用率が、警告CPUしきい値を下回った際に発生します
CPU使用率警告	CPU使用率が警告CPU使用値を上回った、あるいは重大CPU使用値を下回った際に発生します。
メモリ使用率重大	メモリ使用率が、重大メモリ値を上回った際に発生します
メモリ使用率正常	メモリ使用率が、警告メモリ値を下回った時に発生します
メモリ使用率警告	メモリ使用率が警告メモリ使用しきい値を上回った、あるいは重大メモリ使用しきい値を下回った際に発生します。
NVIDIAデコード重大	NVIDIAデコード使用値が、重大NVIDIAデコードしきい値を上回った際に発生します。
NVIDIAデコードノーマル	NVIDIAデコード使用値が、警告NVIDIAデコード値を下回った時に発生します。
NVIDIAデコード警告	NVIDIAデコード使用値が警告NVIDIAデコードしきい値を上回った、あるいは重大NVIDIAデコード値を下回った際に発生します。
NVIDIAメモリ重大	NVIDIAメモリ使用率が、重大NVIDIAメモリしきい値を上回った際に発生します。
NVIDIAメモリノーマル	NVIDIAメモリ使用率が、警告NVIDIAメモリしきい値を下回った時に発生します。
NVIDIAメモリ警告	NVIDIAメモリ使用率が警告NVIDIAメモリ使用値を上回った、あるいは重大NVIDIAメモリ使用値を下回った際に発生します。
NVIDIAレンダリング重大	NVIDIAレンダリング使用値が、重大NVIDIAレンダリングしきい値を上回った際に発生します
NVIDIAレンダリングノーマル	NVIDIAレンダリング使用値が、警告NVIDIAレンダリングしきい値を下回った時に発生します
NVIDIAレンダリング警告	NVIDIAレンダリング使用値が警告NVIDIAレンダリングしきい値を上回った、あるいは重大NVIDIAレンダリングしきい値を下回った際に発生します。
使用可能なサービス重大	サーバーサービスが実走を停止した際に発生します。 本イベントには、しきい値は存在しません。
使用可能なサービス正常	サーバーサービスステイタスが、実走に変更になった際に発生します。 本イベントには、しきい値は存在しません。

システムモニター — カメラ:

イベント	説明
ライブFPS重大	ライブFPS使用率が、重大ライブFPSしきい値を下回った際に発生します。
ライブFPS正常	ライブFPS使用率が、ライブFPS警告しきい値を上回った際に発生します。
ライブFPS警告	ライブFPS使用率がライブFPS警告しきい値を下回った、あるいは重大ライブFPS値を上回った際に発生します。
録画FPS重大	録画FPS使用率が、重大録画FPSしきい値を下回った際に発生します。
録画FPS正常	録画FPS使用率が、警告録画FPSしきい値を上回った際に発生します
録画FPS警告	録画FPS使用率が告録画FPS警値を下回った、あるいは重大録画FPSしきい値を上回った際に発生します。
使用済み領域重大	特定のカメラによる録画のための使用済み容量が重大使用済みスペースしきい値を上回った際に発生します。
使用済み領域正常	特定のカメラによる録画のための使用済み容量が警告使用済みスペースしきい値を下回った際に発生します。
使用済み領域警告	特定のカメラによる録画のための使用済み容量が警告使用済みスペースしきい値を上回った、あるいは重大使用済みスペースしきい値を下回った際に発生します。

システムモニター — ディスク:

イベント	説明
空き領域重大	ディスク空き領域が、重大空き領域しきい値を上回った際に発生します
空き領域正常	ディスク空き領域が、警告空き領域しきい値を下回った時に発生します
空き領域警告	ディスク空き領域が警告空き領域しきい値を上回った、あるいは警告空き領域しきい値を下回った際に発生します。

システムモニター—：ストレージ

イベント	説明
保存期間重大	システムがストレージが重大保存期間値よりも早く一杯になるだと予想した際に発生します。例えば、ビデオストリームからのデータが、予想していたよりも早く"ストレージ"を一杯にしてしまう、と言った場合です。
保存期間正常	システムがストレージが警告保存期間値よりも遅くに一杯になるだと予想した際に発生します。例えば、ビデオストリームからのデータが、予想していた速度でストレージを一杯にする、と言った場合です。
保存期間警告	システムストレージが、警告保存期間値よりも早く、あるいは重大保存期間値よりも遅くに、一杯になるとシステムが予期した際に発生します。例えば、ビデオストリームからのデータが、モーションを録画するように設定されたカメラからより多くのモーション検知があったことにより予想していたよりも早くストレージを一杯にしてしまう、と言った場合です。

その他：

イベント	説明
自動ライセンスアクティベーションが失敗しました	自動ライセンスアクティベーションが失敗した際に発生します。 本イベントにはしきい値は存在しません。
定期的なパスワード変更が開始	定期的なパスワード変更が開始した際に発生します。
定期的なパスワード変更が正常に完了	定期的なパスワード変更がエラーなしで完了した際に発生します。
定期的なパスワード変更がエラーを伴って完了	定期的なパスワード変更がエラーを伴って完了した際に発生します。

アドオン製品および統合からのイベント：

たとえば、ルールシステムでは、アドオン製品および統合からのイベントを使用できます。

- アナリティクスイベントは、ルールシステムでも使用できます

ルール

ルール(説明付き)

ルールは特定の条件下でどのようなアクションをするかを指定します。例：モーションが検知されたら(条件)、カメラは録画(アクション)を開始します。

以下はルールでできることの例です。

- 録画を開始および停止する
- 非デフォルトライブフレームレートを設定する
- 非デフォルトレコーディングフレームレートを設定する
- PTZパトロールを開始および停止する
- PTZパトロールを一時停止および再開する
- PTZカメラを特定の位置に移動する
- 出力を有効/無効状態に設定する
- Eメールで通知を送信する
- ログエントリを生成する
- イベントを生成する
- 新しいデバイス設定を適用する(例：カメラの解像度の変更)
- ビデオがMatrix受信者に見えるようにする
- プラグインを開始および停止する
- デバイスからのフィードを開始および停止する

デバイスを停止することは、ビデオがデバイスからシステムに転送されなくなることを意味し、ライブ視聴も録画もできなくなることを意味します。反対に、フィードを停止したデバイスは、レコーディングサーバーとの通信が維持されます。また、Management Clientでデバイスを手動で無効にしたときとは異なり、デバイスからのフィードはルールにより自動的に開始することが可能です。

> ルールの中には、特定の機能が関連するデバイスで有効であることが要件となるものもあります。例えば、カメラによる録画を指定するルールは、関連するカメラで録画が有効になっていないと機能しません。Milestoneでは、ルールを作成する前に、関連するデバイスが正しく動作するか確認しておくことを推奨しています。

デフォルトルール(説明付き)

システムには多くのデフォルトルールが設定されており、何も設定しなくても基本的な機能が使用できます。必要に応じてデフォルトルールを無効化または修正できます。デフォルトルールを修正または無効化すると、システムが希望通りに動作しなくなる場合があります。また、映像または音声のシステムへの自動配信が保証されなくなる場合があります。

デフォルトルール	説明
PTZが完了したらプリセットへ移動	PTZカメラを手動で操作した後、各デフォルトのプリセット位置に移動することを確認します。このルールはデフォルトでは無効になっています。 ルールを有効にした場合でも、ルールが動作するには、関連するPTZカメラでデフォルトプリセット位置を定義する必要があります。この操作はプリセットタブで行います。
要求があれば音声を再生します。	外部リクエストが発生すると、ビデオが自動的に録画されます。 リクエストは、常にお使いのシステムに外部的に統合されているシステムによってトリガーされます。また、ルールは主に外部システムまたはプラグインのインテグレータによって使用されます。
ブックマーク記録	オペレータがXProtect Smart Clientにブックマークを設定すると、ビデオが自動的に録画されます。これは関連するカメラの録画が有効になっていることが前提条件です。デフォルトでは録画が有効になっています。 このルールのデフォルトの録画時間は、ブックマークが設定された時点の3秒前、およびブックマークが設定された時点から30秒後です。ルールでデフォルトの録画時間を編集できます。録画タブで設定したプレバッファはプリレコーディング時間以上にする必要があることに留意してください。
モーション記録	カメラでモーションが検知される限り、関連するカメラの記録が有効になっていれば、ビデオが録画されることを確認します。デフォルトでは記録は有効になっています。 デフォルトルールでは、検知されたモーションに基づいて記録を指定しますが、1つ以上のカメラで個々のカメラの記録が無効になっている場合には、システムがビデオを記録することを保証するものではありません。記録が有効になっている場合でも、記録の品質は個々のカメラの記録設定の影響を受ける場合があることに留意してください。
リクエスト記録	関連するカメラの録画が有効になっていることを前提条件として、外部リクエストが発生するとビデオの録画が自動的に開始されることを確認します。デフォルトでは録画が有効になっています。 リクエストは、常にお使いのシステムに外部的に統合されているシステムによってトリガーされます。また、ルールは主に外部システムまたはプラグインのインテグレータによって使用されます。
音声配	すべての接続済みマイクとスピーカーからの音声配信がシステムに自動配信されることを保証します。

デフォルトルール	説明
信開始	このデフォルトルールにより、システムのインストール時に接続されたマイクとスピーカーの音声配信に即時にアクセスできます。ただし、記録設定は個別に指定する必要があるため、音声が記録されることを保証するものではありません。
配信開始	すべての接続済みカメラからの映像配信がシステムに自動配信されることを保証します。 このデフォルトルールにより、システムのインストール時に接続されたカメラの映像配信に即時にアクセスできます。ただし、カメラの記録設定は個別に指定する必要があるため、ビデオが録画されることを保証するものではありません。
メタデータ配信開始	すべての接続済みカメラからのデータ配信がシステムに自動配信されることを保証します。 このデフォルトルールにより、システムのインストール時に接続されたカメラのデータ配信に即時にアクセスできます。ただし、カメラの記録設定は個別に指定する必要があるため、データが記録されることを保証するものではありません。
アクセスリクエスト通知の表示	すべての入退室管理イベントが「アクセスリクエスト」に必ず分類されるようにします。こうすることで、Smart Clientプロファイルで通知機能が無効になっていない限り、XProtect Smart Clientでアクセスリクエスト通知のポップアップが表示されます。

デフォルトルールの再作成

誤ってデフォルトのルールを削除した場合には、次の内容を入力することで再作成できます。

デフォルトルール	入力するテキスト
PTZが完了したときにプリセットへ移動する	すべてのカメラからPTZ手動セッションを中止したときにアクションを実行します。 イベントが発生したデバイスでデフォルトのプリセットに即時に移動します。
要求があれば音声を再生します。	外部からの音声メッセージ再生要求があればアクションを実行します。 デバイス上でメタデータからの音声メッセージを優先度1のメタデータから再生します。
ブックマーク記録	すべてのカメラ、すべてのマイク、すべてのスピーカーからブックマーク参照が要求された時にアクションを実行すると、イベントが発生したデバイスで3秒前から録画が開始されます。 アクションを30秒間実行した後に、録画をすぐに停止します。

デフォルトルール	入力するテキスト
モーション記録	モーション時にすべてのカメラからの開始アクションを実行すると、イベントが発生したデバイスで3秒前から記録を開始します。 モーション時にすべてのカメラからの終了アクションを実行すると、3秒後に記録が停止します。
リクエスト記録	外部からの録画開始リクエスト時にアクションを実行すると、メタデータからデバイスの録画をただちに開始します。 外部から記録の停止を要求した際に停止アクションを実行し、録画がただちに停止されます。
音声配信開始	アクションをあるタイムインターバルで実行し、常にすべてのマイク、すべてのスピーカーで配信を開始します。 タイムインターバルが終了すると、アクションを実行し、配信をただちに停止します。
配信開始	アクションをあるタイムインターバルで実行し、常にすべてのカメラで映像配信を開始します。 タイムインターバルが終了すると、アクションを実行し、配信をただちに停止します。
メタデータ配信開始	アクションをあるタイムインターバルで実行し、常にすべてのメタデータで映像配信を開始します。 タイムインターバルが終了すると、アクションを実行し、配信をただちに停止します。
アクセスリクエスト通知の表示	システム[+ ユニット]からアクセスリクエスト(入退室管理カテゴリ)に対してアクションを実行する 組込みアクセスリクエスト通知の表示

ルールの複雑さ(説明付き)

正確なオプション数は、作成するルールのタイプ、およびシステムで使用できるデバイス数により異なります。ルールは高度な複雑さを伴います。イベントと時間条件を組み合わせたり、複数のアクションを1つのルールに指定したり、システムを構成する複数またはすべてのデバイスをカバーするルールを作成することができます。

必要に応じて、単純または複雑なルールを作成することができます。例えば、単純な時間ベースのルールを作成できます。

例	説明
非常に単純な時間ベースのルール	月曜日08:30から11:30(時間条件)という期間になったら、カメラ1とカメラ2が録画を開始(アクション)し、期間が終了したら録画を停止(アクション停止)します。

例	説明
非常に単純なイベントベースのルール	カメラ1でモーションが検出されたら(イベント条件)、カメラ1がすぐに録画を開始し(アクション)、10秒後に録画を停止します(アクション停止)。 イベントベースのルールは、1個のデバイスの1つのイベントで実行されますが、2つ以上のデバイスでアクションが実行されるように指定することもできます。
複数のデバイスを使用するルール	カメラ1でモーションが検知されたら(イベント条件)、カメラ2がすぐに録画を開始し(アクション)、出力3に接続されたサイレンがただちに鳴ります(アクション)。その60秒後に、カメラ2が録画を停止し(アクション停止)、出力3に接続されたサイレンが鳴り止みます(アクション停止)。
時間、イベント、デバイスを組み合わせたルール	カメラ1でモーションが検知された時(イベント条件)、曜日が土曜日または日曜日の場合(時間条件)、カメラ1とカメラ2がすぐに録画を開始し(アクション)、セキュリティマネージャに通知が送信されます(アクション)。カメラ1またはカメラ2でモーションが検知されなくなってから5秒後に、2つのカメラは録画を停止します(アクション停止)。

組織の要件に応じて異なりますが、複雑なルールを作成するよりも、単純なルールを複数作成することを推奨します。もしこれにより、システムにより多くのルールが存在しても、あなたのルールが実行することの概要を簡単に保管することができます。ルールを単純に保つことで、個別のルール要素を無効/有効にするときに、柔軟性を得ることができます。単純なルールであれば、必要に応じてすべてのルールを無効/有効にできます。

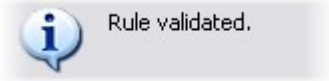
ルールの検証(説明付き)

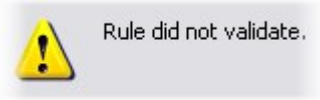
個々のルールまたはすべてのルールの内容を一度に検証することができます。ルールを作成したら、ルールの管理ウィザードで、すべてのルールの要素が矛盾していないか確認します。ルールが一定期間存在し、1つまたは複数のルールの要素が他の構成により影響を受けた場合、ルールが機能しなくなる場合があります。例えば、ルールが特定の時間プロファイルでトリガーされた場合、その時間プロファイルが後で削除されるか、権限がなくなると、ルールは機能しなくなります。このような構成上の意図せぬ影響については、確認が困難です。

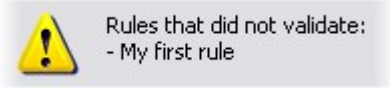
ルール検証は、どのルールが影響を受けたのかを確認するのに役立ちます。検証はルールごとに行われ、各ルールは個別に検証されます。すべてのルールの検証機能を使用しても、互いにルールを検証することはできません(例えば、あるルールが別のルールと矛盾するかを確認する場合など)。

> ルール外の要件の構成が、ルールの機能を妨害するかどうかを検証することはできない点に留意してください。例えば、関連するカメラでモーションが検知されたときに録画を開始するというルールでは、そのカメラでモーション検知(ルールではなくカメラレベルで有効になっている)が有効になっていなくても、ルールの要素自体が正しければ、検証結果は合格ということになります。

個々のルールまたはすべてのルールを一度に検証することができます。検証したいルールを右クリックして、ルールの検証またはすべてのルールの検証を選択します。ダイアログボックスが表示され、ルールが正常に検証されたかどうかを示します。1つ以上のルールを変更したり、1つ以上のルールが守られないと、影響するルールの名前をダイアログボックスがリスト化します。







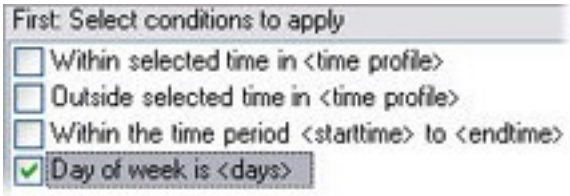
ルールの追加

ルールを作成する際に、関連するオプションを提供するルールの管理ウィザードが表示されます。

ルールに必要な要素が欠如しないようにサポートします。ルールの内容に基づき、ウィザードが自動的に適切な停止アクション(ルールが適用されなくなった後の動作)を提案するため、終わりのないルールを誤って作成することを防止します。

1. ルール アイテム > ルールの追加を右クリックします。ルールの管理ウィザードが開きます。ウィザードに従って、ルールの内容を指定します。
2. 新規ルールの名前と説明を名前と説明フィールドでそれぞれ指定します。
3. ルールのための関連するコンディションの種類を選択する: 特定のイベントが発生したときにアクションを実行するルールか、特定の時間を入力するとアクションを実行するルールのいずれかになります。
4. 次へをクリックしてウィザードの手順2に進みます。ウィザードの第2ステップで、ルールの詳細条件を定義します。

5. 1つまたは複数の条件を選択します。例曜日は<日>です。



選択に応じて、ウィザードウィンドウの下側で、ルールの説明を編集します。

太字斜体の下線付き項目をクリックして、正確な内容を指定します。例えば、日リンクをクリックすると、ルールが適用される曜日を選択することができます。

6. 正確な条件を指定したら、ウィザードの次へをクリックし、次のステップに進み、ルールでカバーするアクションを選択します。ルールの内容と複雑性に応じ、停止イベントや停止アクション等、より多くのステップを定義する必要がある場合があります。例えば、ある時間で(例、木曜日の08:00から10:30) デバイスが特定のアクションを実行するようルールを指定した場合、タイムインターバル終了時に何が起こるかを指定するようウィザードから指示されます。

7. ユーザーのルールを作成した時点で条件が満たされる場合は、デフォルトでルールがアクティブになります。ルールをすぐに適用したくない場合、アクティブチェックボックスを外します。

8. [終了] をクリックします。

ルールを編集、コピー、名前を変更する

1. 概要ペインで、関連するルールを右クリックします。

2. 以下のいずれかを選択します。

   ルールの編集またはルールのコピーまたはルールの名前変更。ルールの管理ウィザードが開きます。

3. ウィザードで、名前を変更するか、ルールを変更します。ルールのコピーを選択した場合、ウィザードが開き、選択したルールのコピーが表示されます。

4. [終了] をクリックします。

ルールを無効/有効にする

ルールの条件が適用され、ルールがアクティブになると、システムはすぐにルールを適用します。ルールをアクティブにしたくない場合は、ルールを無効にすることができます。ルールを無効にすると、ルールの条件が満たされても、システムではルールが適用されません。ルールを無効にした場合も、後で簡単にルールを有効にすることができます。
ルールを無効にする

1. 概要ペインで、ルールを選択します。
2. プロパティペインでアクティブチェックボックスを外します。
3. ツールバーの保存をクリックします。
4. 赤色のxのついたアイコンは、ルールがルールリストで無効化されたことを示します。

ルールを有効にする

ルールをもう一度有効にしたい場合は、ルールを選択し、アクティブチェックボックスを選択して、設定を保存します。

定期スケジュール

詳細な定期スケジュールでは、アクションをどの時点で実行するかを設定できます。

例:

- 毎週火曜日の15:00～15:30の間に1時間おきに実行
- 3か月ごとにその月の15日の11:45に実行
- 毎日15:00～19:00の間に1時間おきに実行

> ここでは、Management Clientがインストールされているサーバーのローカル時刻設定にもとづいた時刻が使用されます。

オプションとして、時間プロファイルを選択することで、ルールがその時間プロファイル間隔の中または外で確実に実行されるよう設定できます。

新しいルールの設定方法に関する一般的な説明については、ページ314のルールの追加を参照してください。

時間プロファイルの詳細については、「ページ316の時間プロファイル」を参照してください。

時間プロファイル

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。

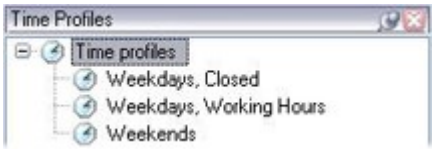
時間プロファイルは、管理者が定義する期間です。時間プロファイルは、ルールを作成するときに使用することができます。例えば、特定のアクションが特定の期間内に発生することを指定するルールを作成するときに使用できます。

時間プロファイルは、Smart Clientプロファイルだけでなく、役割にも割り当てられます。デフォルトでは、すべての役割はデフォルトの時間プロファイルである常時に割り当てられます。これは、デフォルトの時間プロファイルによる役割メンバーは、システムのユーザー権限で、時間ベースの制限がないことを意味します。別の時間プロファイルを役割に割り当てることも可能です。

時間プロファイルは非常にフレキシブルです：1つまたは複数の単一期間、1つまたは複数の繰り返し期間、あるいはそれらの組み合わせにより構成することができます。多くのユーザーは、Microsoft® Outlookのようなカレンダーアプリケーションでの単発や繰り返し期間のコンセプトに慣れています。

時間プロファイルは現地時間で必ず適用されます。つまり、お持ちのシステムが異なる時間ゾーンにレコーディングサーバーを設置している場合、時間プロファイルに関連するアクション(カメラの録画等) は、各レコーディングサーバーの現地時間に基づき実行されます。例：08:30～09:30の時間をカバーする時間プロファイルを使用する場合、ニューヨークに設置したレコーディングサーバーのアクションは、現地時間08:30～09:30に実行され、ロサンゼルスに設置したサーバーは、ロサンゼルスの現地時間が08:30～09:30になったときに遅れて実行されます。

ルールとイベント＞ 時間プロファイルを展開することで、時間プロファイルを作成して管理できます。時間プロファイルリストが開きます。一例：



時間プロファイルの代わりとして、ページ319の日中時間プロファイル(説明付き) を参照してください。

時間プロファイルの指定

1. 時間プロファイルリストで、時間プロファイル > 時間プロファイルの追加をクリックします。これにより、時間プロファイルウィンドウが開きます。
2. 〖時間プロファイル〗ウィンドウで、〖名前〗フィールドに新しい時間プロファイルの名前を入力します。オプションとして、新しい時間プロファイルの説明を〖説明〗フィールドに入力できます。
3. 時間プロファイルウィンドウのカレンダーで、日ビュー、週ビューまたは月ビューを選択してから、カレンダーの内側を右クリックして、1つの時間を追加または繰り返し時間を追加を選択します。
4. 時間プロファイルの必要な時間を指定したら、時間プロファイルウィンドウのOKをクリックします。システムが、新規時間プロファイルを時間プロファイルリストに追加します。後で時間プロファイルを編集または削除したい場合、時間プロファイルリストからも行うことができます。

1つの時間を追加

1つの時間を追加を選択すると、時間の選択ウィンドウが表示されます。

時刻と日付のフォーマットは、使用しているシステムの設定によって異なります。

1. 時間の選択ウィンドウで、開始時間と終了時間を指定します。時間が終日に渡る場合は、終日イベントボックスを選択します。
2. **OK** をクリックします。

繰り返し時間の指定

繰り返し時間を追加を選択すると、繰り返し時間の選択ウィンドウが表示されます。

1. 時間の選択ウィンドウで、時間範囲、繰り返しパターン、および繰り返し範囲を指定します。
2. **OK** をクリックします。

時間プロファイルには、複数の期間を含めることができます。時間プロファイルに、さらに期間を含めたい場合は、1つの時間または繰り返し時間を追加します。

時間プロファイルの編集

1. 概要ペインの時間プロファイルリストで、関連する時間プロファイルを右クリックし、時間プロファイルの編集を選択します。これにより、時間プロファイルウィンドウが開きます。
2. 必要に応じて時間プロファイルを編集します。時間プロファイルに変更を加えたら、時間プロファイルウィンドウの**OK**をクリックします。時間プロファイルリストに戻ります。

[時間プロファイル]の情報ウィンドウで、必要に応じて時間プロファイルを編集できます。時間プロファイルには1つ以上の期間が含まれ、期間が繰り返される場合があります。右上端の小さい月概要には、時間プロファイルが対応する期間の概要が簡単に表示されます。指定された時間を含む日付が太字で強調表示されます。

この例では、太字の日付は、期間が複数の日付で指定され、月曜日に繰り返し時間が指定されていることを示します。

日中時間プロファイル(説明付き)

カメラを屋外に設置した場合、カメラの解像度を頻繁に下げたり、黒/白を有効にしたり、暗くなったり明るくなったりした場合に他の設定を変更する必要があります。赤道からカメラの位置が離れれば離れるほど、日の出と日没時間が1年間のうちで大きく変化します。このため、通常の固定時間プロファイルを使用して、明るさに応じたカメラ設定の調整はできなくなります。

このような状況では、日の長さの時間プロファイルを作成して、特定の地勢条件での日の出と日没を定義することができます。地理座標を使用することで日の出と日の入りの時刻が算出されるほか、該当する場合はサマータイムの調整も毎日施されます。その結果、時間プロファイルが選択した場所の日の出/日没の年間の変化を自動的に追跡し、必要な時だけプロファイルが有効になるようにします。日時はすべてマネジメントサーバーの日時設定に基づきます。また、開始時間(日の出)と終了時間(日没)のプラスまたはマイナスオフセット(分)を設定することも可能です。開始と終了のオフセットは、同一または別にすることができます。

日の長さの時間プロファイルは、ルールと役割の両方を作成するときに使用できます。

日の長さの時間プロファイルの作成

1. [ルールとイベント]フォルダー > [時間プロファイル]を選択します。
2. 時間プロファイルリストで、時間プロファイルを右クリックし、日の長さの時間プロファイルの追加を選択します。
3. 日の長さの時間プロファイルウィンドウで、必要な情報を入力します。明るくなったり暗くなったりする間の移行期間に対処するために、プロファイルの有効/無効をオフセットすることが可能です。さらに、コンピュータの言語/地域設定で使用している言語で、時間と月が表示されます。
4. 入力した地理座標の場所をマップ上で確認するには、[ブラウザーで位置を表示]をクリックします。これによりブラウザが開いて位置を確認できます。
5. OK をクリックします。

日の長さの時間プロファイルのプロパティ

日の長さの時間プロファイルに以下のプロパティを設定します。

名前	説明
名前	プロファイルの名前。
説明	プロファイルの説明です(任意)。
地理座標	プロファイルに割り当てられた、カメラの物理的な場所を示す地理座標。
日の出オフセット	日の出によりプロファイルの作動がオフセットされる分数です(+/-)。
日没オフセット	日没によりプロファイルの無効化がオフセットされる分数です(+/-)。
時間ゾーン	カメラの物理的位置を示す時間帯です。

通知プロファイル

通知のプロファイル(説明付き)

通知プロファイルで、前もって作ったメール通知を設定することができます。通知は、ルールによって(例えば特定のイベントが発生したとき)自動的にトリガーされます。

通知プロファイルの作成時には、メッセージテキストを指定するほか、静止画像とAVIビデオクリップをメール通知に含めたいかどうかを決定します。

また、Eメールスキャナがある場合、Eメールによる通知を送信するアプリケーションを妨害する可能性があるため、これを無効にする必要があります。

通知のプロファイル作成の要件

通知プロファイルを作成する前に、Eメール通知のメールサーバー設定を指定する必要があります。

メールサーバーに必要なセキュリテ証明書がインストールされていれば、メールサーバーと安全に通信できます。

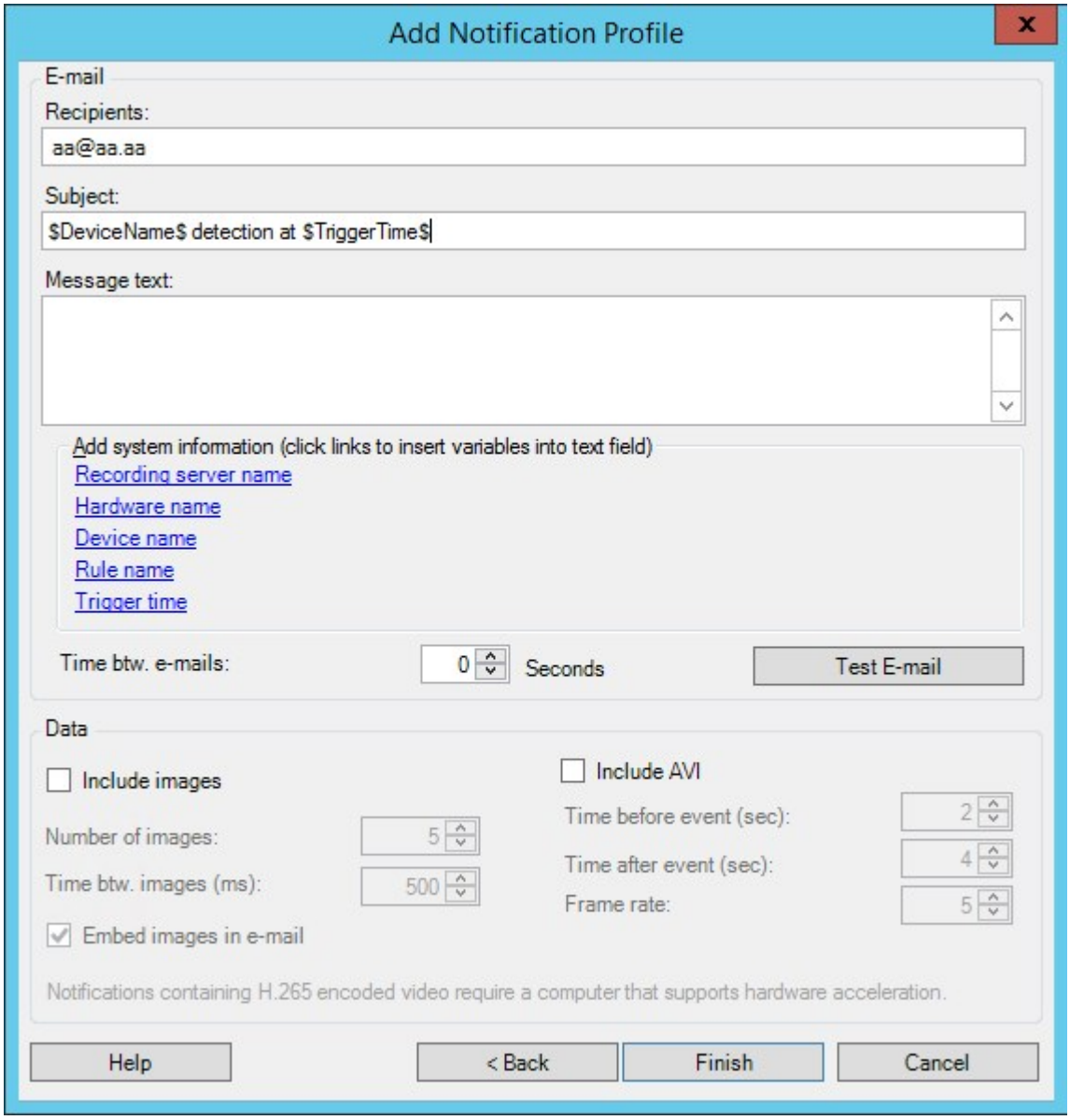
Eメール通知にAVIムービークリップを含めるには、使用する圧縮設定も指定する必要があります。

1. ツール > オプションに移動します。これにより、オプションウィンドウが開きます。
2. メールサーバーを[メールサーバー]タブ(ページ119のメールサーバータブ(オプション))で、また、圧縮設定を[AVI生成]タブ(ページ120のAVI生成タブ(オプション))で設定します。

通知プロファイルの追加

1. [ルールとイベント]を展開し、[通知プロファイル] > [通知プロファイルの追加]を右クリックします。これにより、通知プロファイルの追加ウィザードが開きます。
2. 名前と説明を指定します。[次へ] をクリックします。

3. 受信者、件名、本文、Eメール間の時間を指定します。



4. テストのEメール通知を指定の受信者に送信したい場合は、Eメールのテストをクリックします。

5. 静止画像を添付したい場合、画像を含めるを選択して、画像数、画像間の時間、画像をEメールに埋め込むか否かを指定します。

6. AVIビデオクリップを含めるには、AVIを含めるを選択し、イベント前後の時間とフレームレートを指定してください。

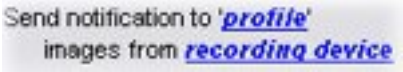
> H.265でエンコードされた動画を添付する場合は、ハードウェアアクセラレーションをサポートするコンピュータが必要です。

7. [終了] をクリックします。

Eメール通知をトリガーするルールを使用する

ルールを作成するためにルールの管理を使用します。ウィザードがすべての関連するステップをガイドします。ステップに従ってルールのアクションを指定し、通知プロファイルの使用を指定します。

<プロファイル>に通知を送信するアクションを選択すると、関連する通知プロファイルを選択でき、通知プロファイルのEメール通知に含む録画がどのカメラからのものかを選択できます。



[ルールの管理]で、選択を行うリンクをクリックします。

実際に何らかの記録がされていない限り、通知プロファイルのEメール通知に記録を含むことができなことにご注意ください。静止画像またはAVIビデオクリップをEメール通知に含めたい場合は、録画の開始を指定するルールを検証します。次の例は、記録の開始アクションと通知を送信しますアクションを含むルールの例です。

通知プロファイル(プロパティ)

通知プロファイルの以下のプロパティを指定します。

コンポーネント	要件
名前	通知プロファイルの分かりやすい名前を入力します。名前は、ルール作成中に通知プロファイルを選択したときに表示されます。
説明(オプション)	通知プロファイルの説明を入力します。説明は、概要ペインの通知プロファイルリストの通知プロファイルにマウスポインタを合わせると表示されます。
受信者	通知プロファイルのEメール通知を送信する宛先となるEメールアドレスを入力します。2つ以上のEメールアド

コンポーネント	要件
	レスを入力する場合は、セミコロンでアドレスを区切ってください。例：aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
件名	Eメールによる通知で、件名として表示するテキストを入力します。 件名とメッセージテキストフィールドには、デバイス名などのシステム変数を挿入できます。変数を挿入するには、フィールド下のボックスの必要な変数リンクをクリックします。
メッセージテキスト	Eメールによる通知で、本文として表示するテキストを入力します。メッセージテキストの他に、Eメール通知の本文には、以下の情報が自動的に追加されます。 • Eメールによる通知がトリガーされた原因 • 添付静止画像またはAVIビデオクリップのソース
Eメール間の時間	各Eメール通知を送信する間隔の最小時間(秒)を指定します。例： • 120を指定した場合、2分経過する前にルールにより通知プロファイルが再びトリガーされた場合でも、各Eメール通知は最低2分経過するまで送信されません • 0を指定すると、通知プロファイルがルールでトリガーされるたびにEメール通知が送信されます。これによりEメール通知が大量に送信される可能性があります。したがって、値に0を使用する場合、ルールが頻繁にトリガーされる通知プロファイルを送信する際は注意が必要です
画像の数	各通知プロファイルのEメール通知に添付する最大静止画像数を指定します。デフォルトの画像数は5個です。
画像間の時間(ミリ秒)：	添付画像に提示された記録間のミリ秒数を指定します。例：デフォルトは500ミリ秒で、添付画像は1/2秒間隔で記録を表示します。
イベント前の時間(秒)	この設定はAVIファイルの開始を指定する際に使用します。デフォルトでは、AVIファイルには通知プロファイルがトリガーされる2秒前からの録画が含まれます。これは、必要な秒数に変更できます。
イベント後の時間(秒)	この設定はAVIファイルの終了を指定する際に使用します。デフォルトでは、AVIファイルは通知プロファイルがトリガーされた4秒後に終了します。これは、必要な秒数に変更できます。
フレーム	AVIファイルに含める秒当たりのフレーム数を指定します。デフォルトは1秒当り5フレームです。フレームレート

コンポーネント	要件
レート	が高ければ高いほど、画質とAVIファイルサイズが大きくなります。
Eメールに画像を埋め込む	選択すると(デフォルト)、画像がEメール通知の本文に挿入されます。選択しなければ、画像は添付ファイルとしてEメール通知に添付されます。

ユーザー定義イベント

ユーザー定義のイベント(説明付き)

目的のイベントがイベント概要リストにない場合は、ユーザー定義イベントを作成できます。このようなユーザー定義のイベントを使用して、他のシステムを監視システムに統合します。

ユーザー定義イベントを使用すると、サードパーティー製の入退室管理システムから受信したデータをシステム内でイベントとして使用できます。イベントは後でアクションをトリガーできます。例えば、誰かが建物に入ったときに、該当するカメラからビデオ記録を開始できます。

また、ユーザー定義イベントを使用すると、XProtect Smart Clientのライブビデオを表示しているときに手動でイベントをトリガーしたり、ルールで使用されている場合は自動的にイベントをトリガーできます。例えば、ユーザー定義イベント37が発生すると、PTZカメラ224がパトロールを停止して、プリセット位置18に移動します。

役割を通して、どのユーザーがユーザー定義イベントをトリガーできるかを定義できます。ユーザー定義イベントを2つの方法で使用し、必要な場合は同時に使用できます。

イベント	説明
XProtect Smart Clientで手動でイベントをトリガーできるようにする方法	この場合、エンドユーザーが手動でイベントをトリガーしながら、のライブビデオを視聴することができますXProtect Smart Client。XProtect Smart Clientのユーザーにより手動でトリガーされたためにユーザー定義イベントが発生すると、ルールによりシステムで行うべき1つまたは複数のアクションがトリガーされます。
APIを通してイベントをトリガーできるようにする方法	この場合、監視システムの外のユーザー定義イベントをトリガーできます。この方法でユーザー定義イベントを使用するには、ユーザー定義イベントをトリガーする際に、個別のAPI(アプリケーションプログラムインターフェース。ソフトウェアアプリケーションの作成またはカスタマイズに必要な構築ブロックのセット)が必要です。この方法でユーザー定義イベントを使用するに

イベント	説明
	は、Active Directoryからの認証が必要です。これにより、ユーザー定義イベントが監視システムの外側からトリガー可能にも関わらず、認証されたユーザーのみが実行可能となります。 また、ユーザー定義イベントは、APIよりメタデータに関連付けし、特定のデバイスまたはデバイスグループを定義することができます。これは、ユーザー定義のイベントを使用してルールをトリガーする際に非常に便利です。それぞれのデバイスに対するルールを持つことを避けるのと、基本的に同じことを行います。例：ある企業には出入り口が35箇所あり、入退室管理を使用しており、それぞれに入退室管理デバイスがあります。入退室管理デバイスを有効にすると、システムでユーザー定義イベントがトリガーされます。このユーザー定義イベントをルールで使用して、有効な入退室管理デバイスに関連するカメラで録画を開始することができます。どのカメラがどのルールに関連付けられるかは、メタデータで定義されます。この方法により、企業は35個のユーザー定義イベントと35個のユーザー定義イベントでトリガーされたルールを作成する必要がなくなります。単一のユーザー定義イベントと、単一のルールで十分な管理が可能になります。 ユーザー定義イベントをこの方法で使用する場合、XProtect Smart Clientの手動トリガーで常に使用できるようにしておきたくない場合もあるでしょう。役割を使用して、どのユーザー定義イベントがXProtect Smart Clientに表示されるか決定することができます。

ユーザー定義イベントをどのように使用しても、各ユーザー定義イベントをManagement Clientで追加する必要があります。

> ユーザー定義イベントの名前を変更した場合、すでに接続済みのXProtect Smart Clientユーザーの場合、名前の変更が表示されるには、ログアウトしてから再度ログインする必要があります。

> また、ユーザー定義イベントを削除すると、ユーザー定義イベントが使用されていたルールに影響が出ます。さらに、削除されたユーザー定義イベントは、XProtect Smart Clientユーザーがログアウトしてから XProtect Smart Clientはじめて削除されます。

ユーザー定義イベントの追加

1. [ルールとイベント] >[ユーザー定義イベント]を展開します。
2. 概要ペインで、[イベント] > [ユーザー定義イベントの追加]を右クリックします。
3. 新規ユーザー定義イベントの名前を入力し、[OK]をクリックします。新しく追加したユーザー定義イベントが、[概要]ペインのリストに表示されます。

ユーザーに権限がある場合は、ユーザーはXProtectSmartClientでユーザー定義イベントを手動でトリガーできるようになります。

ユーザー定義イベントの名前変更

1. [ルールとイベント] >[ユーザー定義イベント]を展開します。
2. 概要ペインで、ユーザー定義イベントを選択します。
3. プロパティペインで、既存の名前を上書きします。
4. ツールバーで保存をクリックします。

アナリティクスイベント

アナリティクスイベント(説明付き)

アナリティクスイベントは、一般的に、外部のサードパーティのビデオコンテンツ分析(VCA)プロバイダから受け取ったデータです。

基本的に、アナリティクスイベントに基づいてアラームを使用する場合には、3段階のプロセスがあります。

- 1. アナリティクスイベント機能を有効にし、セキュリティを設定します。許可されたアドレスのリストを使用して、イベントデータをシステムに送信できるユーザーおよびサーバーがリスニングするポートを制御できます。
- 2. イベントの説明などを使用してアナリティクスイベントを作成し、テストします。
- 3. アラーム定義のソースとしてアナリティクスイベントを使用します。

サイトナビゲーションペインのルールとイベントリストでアナリティクスイベントを設定します。

VCAベースのイベントを使用する場合は、データをシステムに配信するために、サードパーティー製のVCAツールが必要です。ユーザーの選択した任意のVCAツールを使用できます。ただし、ツールが作成するデータは、指定された形式に準拠していなければなりません。この形式については、アナリティクスイベントに関するMIP SDKマニュアルで説明されています。

詳細はシステムプロバイダにお問い合わせください。サードパーティー製のVCAツールは、Milestoneオープンプラットフォームに基づいてソリューションを提供する独立系パートナーによって開発されています。これらのソリューションは、システムのパフォーマンスに影響する場合があります。

アナリティクスイベントの追加と編集

アナリティクスイベントの追加

1. ルールとイベントを展開し、分析イベントを右クリックし、新規追加を選択します。
2. [プロパティ]ウィンドウで、[名前]フィールドにイベントの名前を入力します。
3. 必要な場合は[説明]フィールドに説明テキストを入力します。

4. ツールバーで保存をクリックします。イベントのテストをクリックして、イベントの妥当性をテストすることができます。テストに示されたエラーを何度も修正し、プロセスのどこからでもテストを何度でも実行することができます。

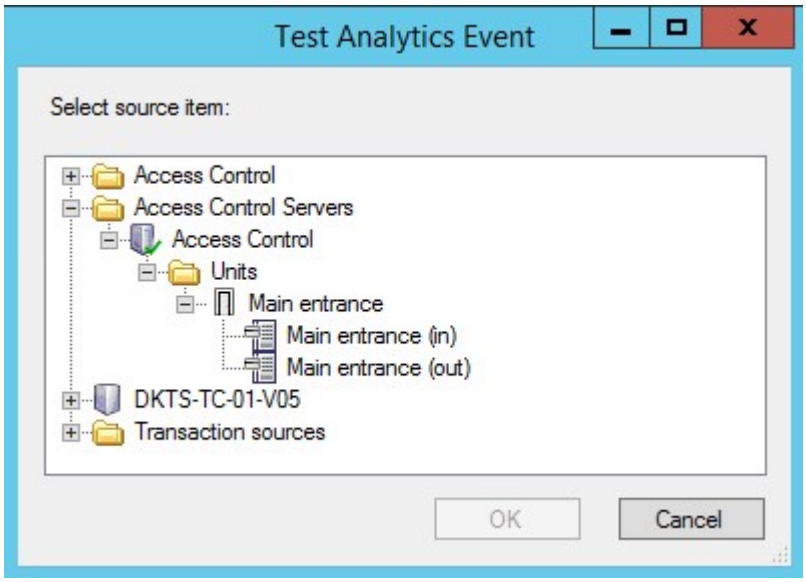
アナリティクスイベントの編集

1. 既存の分析イベントをクリックして、関連するフィールドを編集できるプロパティウィンドウを表示します。
2. イベントのテストをクリックして、イベントの妥当性をテストすることができます。テストに示されたエラーを何度も修正し、プロセスのどこからでもテストを何度でも実行することができます。

アナリティクスイベントのテスト

アナリティクスイベントを作成したら、要件(ページ329のアナリティクスイベントをテストする(プロパティ)を参照)をテストすることができます。例えば、そのアナリティクスイベントがManagement Clientで機能しているかテストできます。

1. 現行の分析種目を選んで下さい。
2. プロパティの中から、「種目テスト」ボタンをクリックして下さい。可能なすべての種目を示すウインドーが表示されます。



3. 種目テストのソースを、例えば、カメラを選んで下さい。そのウインドーは閉じられ、分析種目が機能するための四つの条件を満たす新しい画面が表示されます。

追加テストとして、XProtect Smart Clientで、アナリティックイベントがイベントサーバーに送信されたことを確認できます。このためには、XProtect Smart Clientを開いて[アラームマネージャー]タブの種目を表示します。

参照

ページ327のアナリティクスイベント(説明付き)

アナリティクスイベントをテストする(プロパティ)

アナリティクスイベントの要件をテストする場合は、4つの条件を確認し、エラーがある場合はエラーの説明と解決策を示すウィンドウが表示されます。

条件	説明	エラーメッセージと解決策
保存した変更	イベントが新しい場合は保存されますか? または、イベント名を変更した場合は、変更内容は保存されますか?	アナリティクスイベントをテストする前に変更を保存してください。解決策/説明:変更を[保存]します。
アナリティクスイベントが有効です	アナリティクスイベント機能は有効ですか?	アナリティクスイベントは有効ではありません。解決策/説明:アナリティクスイベント機能を有効にしてください。これを実行するためには、[ツール] > [オプション] > [アナリティクスイベント]をクリックし、[有効]チェックボックスを選択します。
許可されるアドレス	イベントを送信するマシンのIPアドレスまたはホスト名は許可(アナリティクスイベントアドレスリストに登録)されていますか?	**Analytic Event**サービスに対して許可されているアドレスとして、ローカルホスト名を追加する必要があります。解決策/説明:許可されるIPアドレスまたはホスト名のアナリティクスイベントアドレスリストに、使用しているマシンを追加します。 ローカル ホスト名の解決中にエラーがありました。解決策/説明:マシンのIPアドレスまたはホスト名が見つからないか無効です。
アナリティクスイベントを送信する	テストイベントはイベントサーバーに正常に送信されましたか?	下のテーブルを参照してください。

各ステップは失敗 ✗ または成功 ✓.

条件 アナリティクスイベントの送信に対するエラーメッセージと解決策:

エラーメッセージ	解決策
イベントサーバーが見つかりません。	イベントサーバーが登録済みサーバーのリストにありません。
イベントサーバーへの接続中にエラーが発生しました	指定されたポートでイベントサーバーに接続できません。一般的には、ネットワークの問題か、イベントサーバーサービスが停止しているため、エラーが発生します。
アナリティクスイベントの送信エラーが発生しました	イベントサーバーサービスへの接続は確立しますが、イベントを送信できません。一般的には、タイムアウトなどのネットワークの問題のため、エラーが発生します。
イベントサーバーからの応答の受信中にエラーが発生しました	イベントサーバーにイベントが送信されましたが、応答が受信されません。一般的には、ネットワークの問題またはポートがビジー状態のため、エラーが発生します。 通常は *ProgramData\Milestone\XProtect Event Server\logs* にあるイベントサーバーログを確認してください。
イベントサーバーには不明なアナリティクスイベントです	イベントサーバーサービスがイベントを認識しません。エラーが発生する最も可能性の高い理由は、イベントまたはイベントの変更が保存されていないことです。
イベントサーバーが無効なアナリティクスイベントを受信しました	イベントのフォーマットが正しくありません。
送信者はイベントサーバーによって承認されていません。	認証されたリスト上にIP アドレスまたはホスト名あなたのマシンがないケースがあり得ます。
イベントサーバーの内部エラーが発生しました	イベントサーバーエラー。 通常は *ProgramData\Milestone\XProtect Event Server\logs* にあるイベントサーバーログを確認してください。
イベントサーバーが無効な応答を受信しました。	応答は無効です。ポートがビジー状態か、ネットワークに問題がある可能性があります。 通常は *ProgramData\Milestone\XProtect Event Server\logs* にあるイベントサーバーログを確認してください。
イベントサーバーから不明な応答を受信しました	応答は有効ですが、理解不能です。エラーが発生しているのは、ネットワークの問題またはポートがビジー状態のためである可能性があります。 通常は *ProgramData\Milestone\XProtect Event Server\logs* にあるイベントサーバーログを確認してください。
予期しないエラーが発生しました	Milestoneサポートにお問い合わせください。

アナリティクスイベント設定の編集

ツールバーで[ツール] > [オプション] > [アナリティクスイベント]タブを選択して、関連する設定を編集します。

ジェネリックイベント

ジェネリックイベント(説明付き)

この機能は、XProtectイベントサーバーがインストールされていないと動作しません。

ジェネリックイベントでは、単純な文字列をIPネットワーク経由でシステムに送信し、XProtectイベントサーバーのアクションをトリガーできます。

TCPまたはUDPを使用して文字列を送信できるハードウェアまたはソフトウェアを使用して、ジェネリックイベントをトリガーできます。システムは、受信したTCPまたはUDPデータパッケージを分析して、特定の基準が満たされたときに、ジェネリックイベントを自動的にトリガーできます。この方法で、お持ちのシステムと、例えば入退室管理システムやアラームシステム等の外部ソースを統合することができます。目的は、可能な限り多くの外部ソースがシステムと相互作用できるようにすることです。

データソースのコンセプトにより、サードパーティ製ツールでシステムの基準を満たす必要がなくなります。データソースを使用して、指定したIPポートで特定のハードウェアまたはソフトウェアと通信し、そのポートに達するバイトの解釈方法を微調整することが可能になります。各ジェネリックイベントタイプは、データソースとペアになり、特定のハードウェアまたはソフトウェアとの通信に使用される言語を構成します。

データソースを使用する場合、IPネットワークの一般的知識およびインターフェースを使用する個別のハードウェアまたはソフトウェアの知識が必要となります。使用できるパラメータは多数あり、実行方法はあらかじめ決められていません。基本的に、システムはツールを提供しますが、解決策は提供しません。ユーザー定義イベントとは異なり、ジェネリックイベントは認証がありません。これによって簡単にトリガーができますが、安全性を損なわないように、ローカルホストからのイベントのみが許可されます。オプションメニューのジェネリックイベントタブから、その他のクライアントIPアドレスも可能です。

ジェネリックイベントの追加

VMSが外部システムからのTCPまたはUDPパケットの特定文字列を認識できるようにジェネリックイベントを定義することができます。ジェネリックイベントに基づいて、録画またはアラームの開始などのアクションをトリガするようにManagement Clientを設定することができます。

要件

ジェネリックイベントを有効にし、許可されるソース宛先を指定しています。詳細については、「ページ127のジェネリックイベントタブ(オプション)」を参照してください。

ジェネリックイベントを追加するには：

1. [ルールとイベント]を展開します。
2. [ジェネリックイベント]を右クリックして、[新規追加]を選択します。
3. 必要な情報とプロパティを入力します。詳細については、「ページ332のジェネリックイベント(プロパティ)」を参照してください。
4. (オプション)検索式が有効であることを検証するため、予測されるパッケージに対応する[表現がイベント文字列と一致するかチェック]フィールドに次の検索文字列を入力します。
   - 一致 - 文字列を検索式に対して検証することができます
   - 一致しない - 検索式は無効です。検索式を変更して、再試行してください

> XProtectSmartClientでは、イベントサーバーによってジェネリックイベントが受信されたかどうかを検証できます。これは、[イベント]を選択することで、[アラームマネージャ]タブの[アラームリスト]で実行します。

ジェネリックイベント(プロパティ)

コンポーネント	要件
名前	ジェネリックイベントの一意の名前。名前は、ユーザー定義イベント、アナリティクスイベント等すべてのタイプのイベントに対して一意のものでなければなりません。
有効	ジェネリックイベントはデフォルトでは有効になっています。イベントを無効にするにはチェックボックスを解除します。
条件式	データパッケージの分析時にシステムが参照すべき表現。次の演算子を使用できます。 • **( )**: 関連項を論理ユニットとして同時に処理するために使用されます。分析で特定の処理順序を強制するために使用されます 例：検索条件「**(User001** OR **Door053)** AND **Sunday**」を使用する場合、括弧内の2つの項が先に処理され、その結果が文字列の最後の部分と結合されます。つまり、システムはまず**User001**または**Door053**という項を含むパッケージを参照し、その後に結果を取得し、**Sunday**という項を含むパッケージを検索します。 • **AND**：AND演算子では、AND演算子の両側の項が存在する必要があることを指定します 例：検索基準「**User001**AND **Door053** AND **Sunday**」は、**Door001**、**Door053**および**Sunday**のすべてが表現に含まれている場合のみ結果を返します。用語のいずれかまたは2つが存在するだけでは足りませ

コンポーネント	要件
	ん。語句をANDで結合すればするほど、返される結果は少なくなります。 • **OR**: OR演算子により、いずれか1つの項が存在する必要があることを指定します 例：検索基準「**User001** OR **Door053** OR **Sunday**」は、**User001**、**Door053** または**Sunday**のいずれかが含まれている結果を返します。語句をORで結合すればするほど、返される結果は多くなります。
条件式のタイプ	受信したデータパッケージを分析する時に特定のシステムがあるべき状態を示します。オプションは以下の通りです。 • 検索：イベントを発生させるには、受信したパッケージに、［表現］フィールドで指定したテキストが含まれていなければなりませんが、他の内容も含まれている可能性があります。 例：受信したパッケージに**User001**および**Door053**が含まれるよう指定した場合、受信したパッケージに**User001**、**Door053**、**Sunday**が含まれる場合、受信したパッケージに2つの必要な語句が含まれるため、イベントがトリガーされます。 • 一致：イベントが発生するためには、受信したデータパッケージに［表現］フィールドに指定したものと全く同一のテキストだけが存在するものとし、他のものは含まれません。 • 通常の表現：イベントが発生するためには、受信したデータパッケージ内に［表現］フィールドで指定した特定のパターンが存在する必要があります。 検索または一致から正規表現に切り替えると、表現フィールドのテキストは、自動的に正規表現に変換されます。
優先度	0(最低優先度)～999999(最高優先度)の数値によって優先度を指定してください。 同じデータパッケージが異なるイベントで分析される場合があります。各イベントに優先度を割り当てる機能により、受信したパッケージが複数のイベントの基準に一致したときに、どのイベントをトリガーするか管理することができます。 システムがTCPおよびUDPパッケージを受信した場合、そのパケットの分析が、最高優先度のイベントで開始されます。これにより、パッケージが複数のイベントの基準と一致する場合、最高優先度のイベントのみがトリガーされます。パッケージが同じ優先度で複数のイベントの基準と一致した場合、たとえば、優先度999のイベントが2つある場合、その優先度のすべてのイベントがトリガーされます。
表現がイベント文字列と一致するかチェック:	［表現］フィールドに入力した表現に対してイベント文字列をテストします。

ジェネリックイベントデータソース(プロパティ)

コンポーネント	要件
データソース	2つのデフォルトデータソースから選択してカスタムデータソースを定義できます。選択内容は、お使いのサードパーティ製プログラムおよび/またはインターフェース対象となるハードウェアまたはソフトウェアによって異なります。 互換:工場出荷時のデフォルト設定が有効。すべてのバイトをエコー。TCPおよびUDP。IPv4のみ。ポート1234。区切り文字なし。ローカルホストのみ。現在のコードページエンコーディング(ANSI)。 インターナショナル:出荷時設定が有効。統計のみをエコー。TCPのみ。IPv4+6。ポート1235。<CR><LF>を区切り文字として使用。ローカルホストのみ。UTF-8エンコード。(<CR><LF> = 13,10)。 [データソースA] [データソースB] のようになります。
新規	クリックすると新しいデータソースを作成できます。
名前	データソースの名前。
有効	データソースはデフォルトでは有効になっています。データソースを無効にするにはチェックボックスを解除します。
リセット	クリックして選択されたデータソースのすべての設定をリセットします。名前フィールドに入力された名前は残ります。
ポート	データソースのポート番号。
プロトコルタイプセレクタ	システムがジェネリックイベントを検出するために聞き、分析すべきプロトコル。 すべて:TCPおよびUDP。 TCP:TCPのみ。 UDP:UDPのみ。 ジェネリックイベントに使用するTCPおよびUDPパッケージに、@、#、+、~、等の特殊文字が含まれている場合があります。
IPタイプセレクタ	選択可能なIPアドレスタイプ:IPv4、IPv6、または両方。

コンポーネント	要件
区切り文字列	個別ジェネリックイベントのレコードを分離するために使用するセパレーターバイトを選択します。データソースタイプ「インターナショナル」のデフォルト(ページ334のデータソースを参照)は**13.10**です(13.10 = <CR><IF>)。
エコータイプセレクタ	使用可能なエコーリターン形式: • エコー統計:次の形式をエコーします。**[X],[Y],[Z],**[ジェネリックイベント名] **[X]** = 要求番号。 **[Y]** = 文字数。 **[Z]** = ジェネリックイベントとの一致数。 [ジェネリックイベント名] = [名前] フィールドに入力された名前。 • すべてのバイトをエコー:すべてのバイトをエコーします。 • エコーなし:すべてのエコーを抑制します。
エンコーディングタイプセレクタ	デフォルトでは、もっとも関連のあるオプションのみがリストに表示されます。[すべて表示]チェックボックスを選択し、利用可能なすべてのエンコーディングを表示します。
すべて表示	前の項目を参照してください。
使用可能な外部IPv4アドレス	外部イベントを管理するために、マネジメントサーバーが通信可能なIPアドレスを指定します。これを使用して、データを取得しないIPアドレスを除外することも可能です。
使用可能な外部IPv6アドレス	外部イベントを管理するために、マネジメントサーバーが通信可能なIPアドレスを指定します。これを使用して、データを取得しないIPアドレスを除外することも可能です。

範囲は、**100**、**105**、**110**～**120**等4つの位置にそれぞれ指定できます。例えば、10.10ネットワークのすべてのアドレスは、**10.10.[0-254].[0-254]**または**10.10.255.255**により使用可能になります。

サイトナビゲーション:セキュリティ

この記事では、基本ユーザーを作成する方法、役割を設定する方法、そして役割に対してユーザー権限を指定し、ユーザーを割り当てる方法について説明します。

役割(説明付き)

役割により、ユーザーがアクセスできるデバイスが決定されます。また、役割は権限を決定し、ビデオ管理システムのセキュリティも取り扱います。まず、役割を追加し、次にユーザーとグループを追加して、最後にSmart ClientおよびManagement Clientプロファイルと共に、それぞれの役割に属しているその他のデフォルトのプロファイルも追加します。システムで作成できる役割には、それぞれにXProtect Smart Clientにおける独自のビューグループがあり、これを通じてビューを作成、保存できます。

> マネジメントサーバーへのアクセス権を付与するには、[役割設定] >[マネジメントサーバー] > [ページ343のセキュリティ全般タブ(役割)] タブですべての役割に対して [接続] セキュリティ権限を有効化することが重要となります。

ユーザーやグループを管理者役割に追加する方法は、他の役割の場合と同じです。ページ339のユーザーおよびグループの役割からの削除、役割への割り当てを参照してください。

管理者役割に加え、必要な数の役割を追加することができます。例えば、カメラへのアクセス権や類似の制限に応じて、XProtect Smart Clientのユーザーに異なる役割を持たせることもできます。システムで役割を設定するには、セキュリティ> 役割を展開します。

役割の権利(説明付き)

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。

システムで役割を作成する際に、関連する役割がアクセス、使用できるシステムのコンポーネントや機能に対して複数の権限をその役割に付与することができます。たとえば、XProtect Smart Clientの機能に対する権限だけを有する役割、あるいは特定のカメラを表示できる権限を有する他のMilestone閲覧クライアントなどを作成する必要があるとします。こうした役割を作成する場合、これらの役割がManagement Clientに対するアクセス、使用の権限を有する必要はありませんが、XProtect Smart Client またはその他のクライアントにある機能の一部または全部へのアクセスだけは必要です。これを解決するには、たとえば、カメラ、サーバー、類似の機能を追加、削除できる権限など、一部または大半の一般的な管理者権限を有する役割を設定する必要があるかもしれません。

システム管理者の機能の一部または大半を有する役割を作成できます。たとえば、これは組織でシステムのサブセットを管理する人と、システム全体を管理する人を分けたい場合などに関連するものです。この機能によって、たとえば、システムのサーバーまたはカメラの設定の編集できる権限など、システムのさまざまな機能にアクセス、編集、変更ができる異なる管理者権限を提供できるようになります。セキュリティ全般タブでこれらの権限を指定します(ページ343のセキュリティ全般タブ(役割)を参照)。最低限、特別なシステム管理者がManagement Clientを起動できるようにするには、管理サーバー上でその役割に読み取り権限を付与する必要があります。

> マネジメントサーバーへのアクセス権を付与するには、[役割設定] >[マネジメントサーバー] > [ページ343のセキュリティ全般タブ(役割)] タブですべての役割に対して [接続] セキュリティ権限を有効化することが重要となります。

また、役割とユーザーインターフェースから対応するシステム機能を取り除いたManagement Clientプロファイルを対応させることで、同じ制限をそれぞれの役割に対するManagement Clientのユーザーインターフェースに反映させることもできます。詳細はページ280のサイトナビゲーション：クライアント：Management Clientプロファイルを参照してください。

このように異なる権限を役割に付与するには、デフォルトのすべてのシステム管理者役割を有する人が、セキュリティ> 役割> 情報タブ > 新規追加で役割を設定しなければなりません。新しい役割を設定する場合、システムで他の役割を設定したり、システムのデフォルトのプロファイルを使用したりするのと同じように、役割に関連付けられるのは独自のプロファイルだけです。詳しくは、ページ338の役割の追加および管理を参照してください。

どのプロファイルを役割に関連付けるかを指定したら、セキュリティ全般タブへ移動して、その役割の権限を指定します。

> 役割に対して設定できる権限は、製品間で異なります。役割に付与できるのは、XProtect Corporateで使用可能な権利だけです。

ユーザー(説明付き)

ユーザーという用語は、主にクライアントを通じて監視システムに接続するユーザーを意味します。こうしたユーザーは、次の2種類の方法で設定できます。

- 基本ユーザーとして、ユーザー名/パスワードの組み合わせで認証
- Windowsユーザーとして、Windowsログインに基づく認証。

Windowsユーザー

Active Directoryを使用して、Windowsユーザーを追加します。Active Directory(AD)は、Windowsドメインのネットワーク向けにMicrosoftが実装したディレクトリサービスです。これは、ほとんどのWindows Serverオペレーティングシステムに搭載されています。このサービスは、ユーザーやアプリケーションがアクセスできるネットワーク上のリソースを識別します。Active Directoryは、ユーザーおよびグループの概念を使用します。

ユーザーはActive Directoryのオブジェクトで、ユーザーアカウントを持つ個人を指します。例：

グループは、複数のユーザーを持つActive Directoryオブジェクトです。この例では、管理グループに3人のユーザーがいます:

グループにはユーザーを何人でも含めることができます。グループをシステムに追加すると、1回でメンバー全員を追加できます。グループをシステムに追加した後で、Active Directoryのグループに行った変更は(新規メンバーの追加や旧メンバーの削除など)、すぐにシステムに反映されます。ユーザーは一度に複数のグループに所属できます。

Active Directoryを使用して既存のユーザーとグループの情報をシステムに追加することには以下のようなメリットがあります。

- ユーザーおよびグループはActive Directoryで一元的に指定できるため、システムで最初からユーザーアカウントを作成する必要がなくなります
- Active Directoryで認証を処理しているシステムでは、ユーザーの認証を設定する必要はありません

Active Directoryサービスでユーザーやグループを追加する前に、ネットワーク上でActive Directoryをインストールしたサーバーが必要です。

基本ユーザー

システムがActive Directoryにアクセスできない場合、基本ユーザーを作成します(ページ337のユーザー(説明付き))。基本ユーザーを設定する方法については、「ページ378の基本ユーザーの作成」を参照してください。

役割の追加および管理

1. セキュリティを展開して、役割を右クリックします。
2. 役割の追加を選択します。これにより、役割の追加ダイアログボックスが開きます。
3. 新しい役割の名前と説明を入力し、[OK]をクリックします。
4. 新しい役割が役割リストに追加されます。デフォルトでは、新しい役割にはユーザー/グループは関連付けられていませんが、関連付けられたデフォルトのプロファイルがあります。
5. 異なるSmart ClientおよびManagement Clientプロファイル、エビデンスロックプロファイル、時間プロファイルを選択するには、ドロップダウンリストをクリックします。
6. これで、ユーザー/グループを役割に割り当てて、どのシステム機能にユーザー/グループがアクセスできるかを指定できます。

詳細については、「ページ339のユーザーおよびグループの役割からの削除、役割への割り当ておよびページ341の役割の設定」を参照してください。

役割のコピー、名前の変更、削除

役割のコピー

役割の設定や権限が複雑で、ほぼ同様の役割が必要な場合は、新しい役割をゼロから作成するよりも、既存の役割をコピーし、コピーした役割を少し修正する方が簡単な場合があります。

1. セキュリティを展開し、役割をクリックし、関連する役割を右クリックして、役割のコピーを選択します。
2. ダイアログボックスが開いたら、コピーした役割の新しい一意の名前と説明を入力します。
3. **OK** をクリックします。

役割の名前の変更

役割の名前を変更しても、役割をベースとしたビューグループの名前は変更されません。

1. セキュリティを展開して、役割を右クリックします。
2. 必要な役割を右クリックし、役割の名前の変更を選択します。
3. ダイアログボックスが開いたら、役割の名前を変更します。
4. **OK** をクリックします。

役割の削除

1. セキュリティを展開し、役割をクリックします。
2. 対象外の役割を右クリックし、役割の削除を選択します。
3. はいをクリックします。

役割を削除しても、役割をベースとしたビューグループは削除されません。

ユーザーおよびグループの役割からの削除、役割への割り当て

Windowsユーザー、グループまたは基本ユーザーを役割から削除したり、役割に割り当てるには、以下を行います。

1. セキュリティを展開し、役割を選択します。次に、概要ペインで必要な役割を選択します。
2. プロパティペインの下部でユーザーおよびグループタブを選択します。
3. 追加をクリックし、**Windows**ユーザーまたは基本ユーザーから選択します。

役割にWindowsユーザーおよびグループを割り当てる

1. Windowsユーザーを選択します。ユーザーの選択、コンピュータ、およびグループの選択ダイアログボックスが開きます。
2. 必要なオブジェクトタイプを指定しているか確認します。例えば、コンピュータを追加する必要がある場合、オブジェクトタイプをクリックし、コンピュータをマークします。さらに、この場所からフィールドで必要なドメインを指定したか確認します。指定されていなければ、場所をクリックして、必要なドメインを参照します。
3. [選択するオブジェクト名を入力]ボックスで、関連するユーザー名、イニシャル、またはActive Directoryが認識できるその他の識別子タイプを入力します。名前のチェック機能を使用して、入力した名前やイニシャルをActive Directoryが認識できることを確認します。または、[詳細...] 機能でユーザーまたはグループを検索します。
4. OK をクリックします。選択したユーザー/グループは、これで選択した役割に割り当てたユーザーのユーザーおよびグループタブのリストに追加されます。セミコロン(;)で区切って複数の名前を入力することで、さらに多くのユーザーやグループを追加することができます。

役割に基本ユーザーを割り当てる

1. 基本ユーザーを選択します。これにより、ロールに追加する基本ユーザーを選択ダイアログボックスが開きます。
2. この役割に割り当てる基本ユーザーを選択します。
3. オプション: 新規をクリックすると新しい基本ユーザーを作成できます。
4. OK をクリックします。選択した基本ユーザーは、これで選択した役割に割り当てた基本ユーザーのユーザーおよびグループタブのリストに追加されます。

役割からユーザーおよびグループを削除する

1. ユーザーおよびグループタブで、削除したいユーザーまたはグループを選択し、タブ下の削除をクリックします。必要に応じて、複数のユーザーまたはグループ、あるいはグループや個人ユーザーの組み合わせを選択することができます。
2. 選択したユーザーまたはグループを削除することを確認します。はいをクリックします。

> ユーザーは、グループメンバーを経由して役割を有することもあります。この場合、その役割から個別ユーザーを削除することはできません。グループメンバーは、個人として役割を持つ場合もあります。ユーザー、グループ、または個別のグループメンバーが有する役割を検索するには、有効な役割の表示機能を使用します。

有効な役割の表示

有効な役割機能により、選択したユーザーまたはグループのすべての役割を表示することができます。この機能は、グループを使用している場合に特に便利であり、個別のユーザーがどのメンバーの役割であるかを表示する唯一の方法です。

1. セキュリティを展開して有効な役割を開き、役割を右クリックして有効な役割を選択します。
2. 基本ユーザーの情報を確認するには、[ユーザー名]フィールドに名前を入力します。更新をクリックすると、ユーザーの役割が表示されます。
3. Active DirectoryでWindowsユーザーまたはグループを使用している場合は、**[...]**参照ボタンをクリックします。オブジェクトタイプを選択して名前を入力し、**OK**をクリックします。ユーザーの役割が自動的に表示されます。

役割の設定

情報タブ(役割)

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。

役割の情報タブで、以下を設定できます:

名前	説明
名前	ロールの名前を入力します。
説明	ロールの説明を入力します。
Management Client外形	役割と関連付けるManagement Clientのプロファイルを選択します。 これを、デフォルトの管理者役割に適用することはできません。 マネジメントサーバーでセキュリティを管理する権限が必要です。
Smart Client外形	役割と関連付けるSmart Clientのプロファイルを選択します。 マネジメントサーバーでセキュリティを管理する権限が必要です。
既定の時間設定	役割と関連付けるデフォルトの時間設定を選択します。 これを、デフォルトの管理者役割に適用することはできません。
エビデンスロックプロファイル	役割と関連付けるエビデンスロックのプロファイルを選択します。
Smart Client時間プロ	この役割に関連付けられているXProtect Smart Clientユーザーがログインできる時間プロ

名前	説明
ファイル内でのログイン	ファイルを選択します。 有効期限切れの期間にXProtect Smart Clientユーザーがログインすると、自動的にログオフになります。 これを、デフォルトの管理者役割に適用することはできません。
Smart Clientログインを許可する	チェックボックスを選択すると、この役割に関連付けられているユーザーがXProtect Smart Clientへログインすることができます。 Smart Clientへのアクセスはデフォルトで許可されます。チェックボックスをオフにするとXProtect Smart Clientへのアクセスを拒否します。
XProtect Mobileクライアントへのログイン許可	チェックボックスを選択すると、このロールに関連付けられているユーザーがXProtect Mobileクライアントにログインすることができます。 XProtect Mobileクライアントへのアクセスはデフォルトで許可されています。チェックボックスをオフにするとXProtect Mobileクライアントへのアクセスを拒否します。
XProtect Web Clientログインを許可する	チェックボックスを選択すると、この役割に関連付けられているユーザーがXProtect Web Clientへログインすることができます。 XProtect Web Clientへのアクセスはデフォルトで許可されます。チェックボックスをオフにするとXProtect Web Clientへのアクセスを拒否します。
ログイン認証が必要	チェックボックスを選択して、ログイン認証を役割と関連付けます。つまり、ユーザーがログインする際には、XProtect Smart ClientまたはManagement Clientは第2認証が必要となることを意味します(通常は、スーパーユーザーまたはマネージャーが認証)。 管理者がユーザーを認証できるようにするには、セキュリティ全般タブでマネジメントサーバーのユーザーを認証する権限を設定します。 これを、デフォルトの管理者役割に適用することはできません。
PTZセッション中にユーザーを匿名にする	チェックボックスを非表示にすると、この役割に関連付けられたユーザーがPTZセッションを制御するときに、これらのユーザーの名前を非表示にします。

ユーザーおよびグループタブ(役割)

ユーザーとグループタブ上で、ユーザーとグループを枠割に割り当てます(ページ339のユーザーおよびグループの役割からの削除、役割への割り当てを参照)。Windowsユーザーとグループ、または基本ユーザーを割り当てることができます(「ページ337のユーザー(説明付き)」を参照)。

名前	説明
名前	この役割に割り当てられたユーザーまたはグループの名前が表示されます。
説明	基本ユーザーが作成されたときに入力した説明が表示されます。

セキュリティ全般タブ(役割)

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。

セキュリティ全般タブで、役割の全般的な権限を設定します。システムで利用できるコンポーネントごとに [許可] または [拒否] と設定することで、役割に対するアクセス権限を定義します。ある役割からのコンポーネントへのアクセスが「拒否」に設定された場合、この役割が割り当てられたユーザーの [セキュリティ全般] タブにはそのコンポーネントが表示されません。

> オーバーオール セキュリティタブ はXProtect Essential+においては利用できません。

XProtect Expert、XProtect Professional+、そしてXProtect Express+よりXProtect Corporate のために、さらにアクセス権限を定義することができます。これは、XProtect Corporateでは差異化されたシステムシステム管理者の権利のみしか設定できないのに対し、XProtect Smart Client、XProtect Web Client、あるいは XProtect Mobile クライアントを使用する全ての役割に対しては全体的な権利をすべての製品で設定できるためです。

> セキュリティ全般の設定は、現在のサイトだけに適用されます。

もしユーザーを複数の役割と関連付けた場合、セキュリティ設定に関して、ある役割で拒否を選択し、別の役割で許可を選択した場合、拒否権限の方が許可権限より優先します。

以下の説明は、関連する役割に対して許可を選択した場合、さまざまなシステムコンポーネントのそれぞれの権限について個々に何が起こるかを示しています。XProtect Corporateを使用する場合、それぞれのシステムコンポーネントでどの設定が使用できないかをお使いのシステムでのみ表示できます。

すべてのシステムコンポーネントや機能について、完全なシステムシステム管理者は許可または拒否のチェックボックスを使用して、役割に関するセキュリティ権限を設定できます。ここで設定するセキュリティ権限は、システムコンポーネントや機能の全体の設定に関するものです。したがって、たとえば、カメラで [拒否] チェックボックスを選択すると、システムに追加されるすべてのカメラがそのロールでは使用できなくなります。対照的に、許可チェックボックスを選択すると、この役割ではシステムに追加されるすべてのカメラを表示できるようになります。カメラでの許可または拒否の選択は、デバイスタブでのカメラの設定となり、特定の役割に対してすべてのカメラが使用可能または使用不能となるように、セキュリティ全般タブでの選択が継承されます。

個別のカメラ、あるいはそれに類似するカメラに対してセキュリティ権限を設定したい場合、セキュリティ全般タブでシステムコンポーネントあるいは機能に対し、権限全般の設定はしないならば、関連するシステムコンポーネント、あるいは機能のタブで個々の権限を設定することが可能です。

以下の記述は、MIP SDKを通して環境設定できる権限に対して適用することもできます。

> ⚠ 基本ライセンスをXProtect Corporateからその他の製品のいずれかにスイッチする場合、XProtect Corporateでのみ利用可能なセキュリティ権限はすべて削除するようにしてください。これらの権限を削除しない場合は、スイッチを完了することはできません。

Management Server

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	
接続	ユーザーがマネジメントサーバーに接続できるようになります。 この権限はデフォルトで有効となっています。 メンテナンスプロセス時には役割に対する接続権限を一時的に無効にし、後でシステムにアクセスを再適用できます。 ⚠ システムへのアクセスを許可するには、この権限を選択する必要があります。	
読み取る	以下を含む幅広い機能へのアクセス権を有効にする： • 以下を伴うログインManagement Client • 現在のタスクのリスト • サーバーログ また、以下に対するアクセス権も有効にします： • リモート接続サービス • Smart Clientプロフィール • Management Clientプロフィール • Matrix	のみ使用可能

セキュリティ権限	説明	XProtect Corporate
	• 時間設定 • 登録済みサーバーおよびサービス登録API	
編集	以下を含む広範囲の機能におけるデータを修正する権利を有効にする • オプション • ライセンス管理 また、ユーザーが以下を作成、削除、編集できるようにします。 • リモート接続サービス • デバイスグループ • Matrix • 時間設定 • 通知設定 • 登録済みサーバー レコーディングサーバーでネットワークを設定する際に、ローカルIP範囲を設定する権限を有効にします。	のみ使用可能
システムモニター	システムモニターのデータを表示する権限を有効にします。	のみ使用可能
ステータスAPI	レコーディングサーバーに存在するステータスAPIに対するクエリを実行できる権限を有効にします。これは、この権限が有効になっている役割が、レコーディングサーバーに存在するアイテムのステータスの読み取りにアクセスできることを意味します。	
フェデレーテッドサイト階層を管理	現在のサイトを、フェデレーテッドサイト階層にある他のサイトに追加および分離できる権限を有効にします。 この権限を子サイトでのみ有効にしても、ユーザーはサイトを親サイトから分離できます。	のみ使用可能
バックアップ設定	システムのバックアップおよび復元機能を使用してシステム構成のバックアップを作成できる権限を有効にします。	のみ使用可能

セキュリティ権限	説明	XProtect Corporate
ユーザーを認証	XProtect Smart ClientまたはManagement Clientに二回目のログインをするように要求された場合、ユーザーを許可する権利を有効にします。役割がログイン認証を必要とするかどうかを情報タブで定義します。	
セキュリティを管理	Management Serverの権限を管理できる権限を有効にします。 また、ユーザーが以下の機能を作成、削除、編集できるようにします。 • 役割 • 基本ユーザー • Smart Clientプロフィール • Management Clientプロフィール	のみ使用可能

レコーディングサーバー

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
編集	マネジメントサーバーでの編集権限を必要とするネットワーク構成設定を除き、レコーディングサーバーでのプロパティを編集できる権限を有効にします。
削除	レコーディングサーバーを削除する権限を有効にします。これを行うには、ユーザーに以下の削除権限を与える必要があります： • ハードウェアをレコーディングサーバーに追加している場合は、ハードウェアのセキュリティグループ レコーディングサーバーにあるデバイスにエビデンスロックが含まれているなら、レコーディングサーバーを削除できるのはオフラインである場合だけです。
ハードウェアの管理	レコーディングサーバーにハードウェアを追加する権限を有効にします。

セキュリティ権限	説明
ストレージを管理	レコーディングサーバーのストレージ コンテナを管理、つまりストレージ コンテナを作成、削除、移動、空にする権限を有効にします。
セキュリティを管理	レコーディングサーバーのセキュリティ権限を管理する権限を有効にします。

フェールオーバー サーバー

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	Management Clientにおいて、フェイルオーバーサーバーの閲覧とアクセスの権利を有効にする。
編集	Management Clientにおいて、フェイルオーバーサーバーの作成・更新・消去・移動・有効化/無効化にする権利を有効にする。
セキュリティを管理	フェールオーバーサーバーのセキュリティ権限を管理する権限を有効にします。

モバイルサーバー

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	Management Clientにおいてモバイルサーバーの閲覧とアクセスの権利を有効にする。
編集	Management Clientにおいてモバイルサーバーを編集・削除する権利を有効にする。
セキュリティを管理	モバイルサーバーのセキュリティ権限を管理する権限を有効にします。
作成	システムにモバイルサーバーを追加する権限を有効にします。

ハードウェア

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
編集	ハードウェアのプロパティを編集する権限を有効にします。
削除	ハードウェアを削除する権限を有効にします。 いずれかのハードウェアデバイスにエビデンスロックが含まれているなら、ハードウェアを削除できるのはレコーディングサーバーがオフラインである場合だけです。
ドライバーコマンド	特殊コマンドをドライバーに送信する権利を有効にし、それによってデバイス自体にある機能や設定を制御します。 ドライバコマンドの権利は、クライアント内の特別に開発されたMIPプラグインのためだけのものです。標準構成タスクは制御できません。
パスワードを見る	[ハードウェアの編集]ダイアログボックスで、ハードウェアデバイスのパスワードを見る権限を有効にします。
セキュリティを管理	ハードウェアのセキュリティ権限を管理する権限を有効にします。

カメラ

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	
読み取る	クライアントとManagement Clientのカメラデバイスを見る権利を有効にする。	

セキュリティ権限	説明	XProtect Corporate
編集	Management Clientで、カメラのプロパティを編集する権利を有効にする。また、ユーザーに対してカメラを有効または無効にします。	のみ使用可能
ライブ表示	クライアントとManagement Clientのカメラからライブビデオを見る権利を有効にする.	
再生	すべてのクライアントのカメラで録画されたビデオを再生する権限を有効にします。	
リモート録画の取得	リモートサイトのカメラやカメラのエッジストレージからクライアントの録画を取り出す権利を有効にする。	
シーケンスを読み取る	クライアントでの録画ビデオの再生などに関連するシーケンス情報を読み取る権限を有効にします。	
スマートサーチ	クライアントでスマートサーチを使用する権限を有効にします。	
エクスポート	クライアントから録画をエクスポートする権限を有効にします。	
ブックマークを作成	クライアントで録画ビデオやライブビデオにブックマークを作成する権限を有効にします。	
ブックマークを読み取る	クライアントでブックマークの詳細を検索、読み取りする権限を有効にします。	
ブックマークを編集	クライアントでブックマークを編集する権限を有効にします。	
ブックマークを削除	クライアントでブックマークを削除する権限を有効にします。	
エビデンスロックの作成・拡張	クライアントでエビデンスロックを作成、延長する権限を有効にします。	のみ使用可能
エビデンスロックを読み取る	クライアントでエビデンスロックを検索、読み取りする権限を有効にします。	のみ使用可能
エビデンスロックの削除・縮小	クライアントでエビデンスロックを削除または短縮する権限を有効にします。	のみ使用可能
手動録画を開始	クライアントでビデオの手動録画を開始する権限を有効にします。	

セキュリティ権限	説明	XProtect Corporate
手動録画を停止	クライアントでビデオの手動録画を停止する権限を有効にします。	
AUXコマンド	クライアントからカメラの補助(AUX)コマンドを利用する権利を有効にする。 AUX コマンドは、たとえばビデオエンコーダー経由で接続されているカメラのワイパーのコントロールを可能にします。補助接続で接続されているカメラ関連デバイスは、クライアントからコントロールされます。	
手動PTZ	クライアントとManagement ClientのPTZカメラにおけるPTZ機能を利用する権利を有効にする。	
PTZプリセットまたはパトロール設定をアクティブ化する	位置のプリセット、プロフィールパトロールの開始・停止、クライアントのパトロールを一時停止させるようPTZカメラを動かす権利を有効にするManagement Client。 この役割がカメラの他のPTZ機能を使用することを許可するには、手動PTZ権限を有効にします。	
PTZプリセットまたはパトロールプロファイルの管理	クライアントとManagement ClientのPTZカメラにおけるPTZプリセットとパトロールプロフィールを追加・編集・削除する権利を有効にする。 この役割がカメラの他のPTZ機能を使用することを許可するには、手動PTZ権限を有効にします。	
PTZプリセットのロック/ロック解除	Management Clientにおいて、PTZプリセットをロック・解除する権利を有効にする。これにより、他のユーザーがクライアントおよびManagement Clientにおいてプリセット位置を変更することを許可したり、防いだりすることが可能です。	のみ使用可能
PTZセッションの予約	クライアントとManagement Clientの予約されたPTZセッションモードにおいてPTZカメラを設定する権利を有効にする。 予約されたPTZセッションでは、より高いPTZ優先度の他のユーザーでも制御を取得できません。 この役割がカメラの他のPTZ機能を使用することを許可するには、手動PTZ権限を有効にします。	のみ使用可能
PTZセッションのリリース	Management Clientより他のユーザーのPTZセッションを解放する権利を有効にする。 この権限がなくても、自分のPTZセッションは常にリリースできます。	のみ使用可能

セキュリティ権限	説明	XProtect Corporate
録画を削除	Management Clientを介して、保存されているビデオ録画をシステムから削除する権利を有効にする。	のみ使用可能
プライバシーマスクの除去	XProtect Smart Clientで一時的にプライバシーマスクを除去する権利を有効化します。それにより、その他のXProtect Smart Clientユーザーがプライバシーマスクを除去する権限を与えることができます。 プライバシーマスクの除去は、Management Clientにおいて除去可能なプライバシーマスクとして設定されたプライバシーマスクにのみ適応されます。	
セキュリティを管理	Management Clientにおいて、カメラに対するセキュリティ権限を管理する権利を有効にする。	のみ使用可能

マイク

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	
読み取る	クライアントとManagement Clientのマイク装置を見る権利を有効にする。	
編集	Management Clientにおいて、マイクのプロパティを編集する権利を有効にする。また、ユーザーがカメラを有効または無効にすることも可能になります。	のみ使用可能
聴く	クライアントとManagement Clientのマイクからライブオーディオを聴く権利を有効にする。	
再生	クライアントでマイクからの録音された音声を再生する権限を有効にします。	
リモート録画の取得	リモートサイトのマイク、あるいはカメラのエッジストレージからクライアントの録音を取得する権利を有効にする。	
シーケンスを読み	クライアントの[再生]タブなどに関連するシーケンス情報を読み取る権限を	

セキュリティ権限	説明	XProtect Corporate
取る	有効にします。	
エクスポート	クライアントから録画をエクスポートする権限を有効にします。	
ブックマークを作成	クライアントでブックマークを作成する権限を有効にします。	
ブックマークを読み取る	クライアントでブックマークの詳細を検索、読み取りする権限を有効にします。	
ブックマークを編集	クライアントでブックマークを編集する権限を有効にします。	
ブックマークを削除	クライアントでブックマークを削除する権限を有効にします。	
エビデンスロックの作成・拡張	クライアントでエビデンスロックを作成または延長する権限を有効にします。	のみ使用可能
エビデンスロックを読み取る	クライアントでエビデンスロックの詳細を検索、読み取りする権限を有効にします。	のみ使用可能
エビデンスロックの削除・縮小	クライアントでエビデンスロックを削除または短縮する権限を有効にします。	のみ使用可能
手動録画を開始	クライアントで音声の手動録画を開始する権限を有効にします。	
手動録画を停止	クライアントで音声の手動録画を停止する権限を有効にします。	
録画を削除	保存されているシステムからの録画を削除する権限を有効にします。	のみ使用可能
セキュリティを管理	Management Clientにおいて、マイクに対するセキュリティ権限を管理する権利を有効にする。	のみ使用可能

スピーカー

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	

セキュリティ権限	説明	XProtect Corporate
読み取る	クライアントのスピーカー装置を調べる権利を有効にするManagement Client。	
編集	Management Clientにおいて、スピーカーのプロパティを編集する権利を有効にする。また、ユーザーがスピーカーを有効または無効にすることも可能になります。	のみ使用可能
聴く	クライアントとManagement Clientのスピーカーからライブオーディオを聴く権利を有効にする。	
通話	クライアントでスピーカーを通して通話する権限を有効にします。	
再生	クライアントでスピーカーからの録音された音声を再生する権限を有効にします。	
リモート録画の取得	リモートサイトのスピーカー、あるいはカメラのエッジストレージからクライアントの録音を取り出す権利を有効にする。	
シーケンスを読み取る	クライアントでスピーカーから録音した音声をブラウズしながら、シーケンス機能を使用する権限を有効にします。	
エクスポート	クライアントでスピーカーから録音した音声をエクスポートする権限を有効にします。	
ブックマークを作成	クライアントでブックマークを作成する権限を有効にします。	
ブックマークを読み取る	クライアントでブックマークの詳細を検索、読み取りする権限を有効にします。	
ブックマークを編集	クライアントでブックマークを編集する権限を有効にします。	
ブックマークを削除	クライアントでブックマークを削除する権限を有効にします。	
エビデンスロックの作成・拡張	権利が、クライアント内の録音音声を守るために、エビデンスロックの作成または延長をする権限を有効にします。	のみ使用可能
エビデンスロックを読み取る	クライアント内の、エビデンスロックにより守られた録音音声を表示する権限を有効にします。	のみ使用可能
エビデンスロックの	クライアント内の、守られた録音音声にあるエビデンスロックを削除または削	のみ使用可能

セキュリティ権限	説明	XProtect Corporate
削除・縮小	減する権限を有効にします。	
手動録画を開始	クライアントで音声の手動録画を開始する権限を有効にします。	
手動録画を停止	クライアントで音声の手動録画を停止する権限を有効にします。	
録画を削除	保存されているシステムからの録画を削除する権限を有効にします。	のみ使用可能
セキュリティを管理	Management Clientにおいてスピーカーに対するセキュリティ権限を管理する権利を有効にする。	のみ使用可能

メタデータ

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	
読み取る	クライアントでメタデータを受け取る権限を有効にします。	
編集	Management Clientにおいてメタデータのプロパティを編集する権利を有効にする。また、ユーザーがメタデータデバイスを有効または無効にすることも可能になります。	のみ使用可能
ライブ	クライアントでカメラからのライブメタデータを受信する権限を有効にします。	
再生	クライアントでメタデータデバイスからの録画データを再生する権限を有効にします。	
リモート録画の取得	リモートサイトのメタデータ装置、あるいはカメラのエッジストレージからクライアントの録画を取り出す権利を有効にする。	
シーケンスを読み取る	クライアントの[再生]タブなどに関連するシーケンス情報を読み取る権限を有効にします。	
エクスポート	クライアントで録画をエクスポートする権限を有効にします。	

セキュリティ権限	説明	XProtect Corporate
エビデンスロックの作成・拡張	クライアントでエビデンスロックを作成する権限を有効にします。	のみ使用可能
エビデンスロックを読み取る	クライアントでエビデンスロックを表示する権限を有効にします。	のみ使用可能
エビデンスロックの削除・縮小	クライアントでエビデンスロックを削除または短縮する権限を有効にします。	のみ使用可能
手動録画を開始	クライアントでメタデータの手動録画を開始する権限を有効にします。	
手動録画を停止	クライアントでメタデータの手動録画を停止する権限を有効にします。	
録画を削除	保存されているシステムからの録画を削除する権限を有効にします。	のみ使用可能
セキュリティを管理	メタデータManagement Clientに対し、以下のセキュリティ権限を管理する権利を有効にする。	のみ使用可能

入力

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	のみ使用可能
読み取る	クライアントとManagement Clientの入力デバイスを見る権利を有効にする。	
編集	Management Clientの入力デバイスのプロパティを編集する権利を有効にする。また、ユーザーが入力デバイスを有効または無効にすることも可能になります。	のみ使用可能
セキュリティを管理	入力デバイスに対し、Management Clientのセキュリティ権限を管理する権利を有効にする。	のみ使用可能

出力

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	
読み取る	クライアントで出力デバイスを表示する権限を有効にします。	
編集	Management Clientの出力デバイスのプロパティを編集する権利を有効にする。また、ユーザーが出力デバイスを有効または無効にすることも可能になります。	のみ使用可能
実行	クライアントで出力をアクティブ化する権限を有効にします。	
セキュリティを管理	出力デバイスに対し、Management Clientのセキュリティ権限を管理する権利を有効にする。	のみ使用可能

Smart Wall

以下の設定は、XProtect ExpertおよびXProtect Corporateでのみ利用ができます。

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	
読み取る	クライアントのSmart Wallを表示する権利を有効にします。	
編集	Smart WallでManagement Clientのプロパティを編集する権限を有効にします。	のみ使用可能
削除	Smart Wallで既存のManagement Clientを削除する権限を有効にします。	のみ使用可能
操作	Smart Wallをアクティブにし修正する権利を有効にする。例えば、プリセットを変更・アクティブにする、あるいはクライアントやManagement Clientのビューにカメラを向けるなど。	
Smart Wallの作成	Smart Wallで新規のManagement Clientを作成する権限を有効にします。	のみ使用可能

セキュリティ権限	説明	XProtect Corporate
セキュリティを管理	Management Clientのセキュリティ権限を管理する権利を有効にする(Smart Wallのため)。	のみ使用可能
再生	クライアントのSmart Wallから録画されたデータを再生する権限を有効にします。	

ビューグループ

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	
読み取る	クライアントとManagement Clientのビューグループを見る権利を有効にする。ビューグループが以下に作成されますManagement Client。	
編集	Management Clientのビューグループに関するプロパティを編集する権利を有効にする。	のみ使用可能
削除	Management Clientのビューグループを削除する権利を有効にする。	
操作	XProtect Smart Clientにあるビューグループを使用する権利を有効にします。これにより、サブグループとビューの作成と削除が可能になります。	
ビューグループの作成	Management Clientのビューグループを作成する権利を有効にする。	のみ使用可能
セキュリティを管理	ビューグループに対し、以下のセキュリティ権限をManagement Client管理する権利を有効にする。	のみ使用可能

ユーザー定義イベント

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	
読み取る	クライアントのユーザー定義イベントを見る権利を有効にする。	
編集	Management Clientのユーザー定義イベントのプロパティを編集する権利を有効にする。	のみ使用可能
削除	Management Clientのユーザー定義イベントを削除する権利を有効にする。	のみ使用可能
トリガー	クライアントでユーザー定義イベントをトリガーする権限を有効にします。	
セキュリティを管理	ユーザー定義イベントに対し、Management Clientのセキュリティ権限を管理する権利を有効にする。	のみ使用可能
ユーザー定義イベントの作成	Management Clientのユーザー定義イベントを新規作成する権利を有効にする。	のみ使用可能

アナリティクスイベント

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	Management Clientの解析イベントを見る権利を有効にする。
編集	Management Clientの解析イベントのプロパティを編集する権利を有効にする。
セキュリティを管理	全てのシステムモニターに対し、Management Clientのセキリュリティ権限を管理する権利を有効にする。

ジェネリックイベント

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	クライアントとManagement Clientの一般的なイベントを見る権利を有効にする。
編集	Management Clientの一般的なイベントのプロパティを編集する権利を有効にする。
セキュリティを管理	一般的なイベントに対し、Management Clientのセキュリティ権限を管理する権利を有効にする。

Matrix

セキュリティ権限	説明	XProtect Corporate
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。	のみ使用可能
読み取る	ビデオを選択し、クライアントからMatrix受信者へビデオを送る権利を有効にする。	
編集	Management ClientでのMatrixプロパティを編集する権限を有効にします。	のみ使用可能
削除	Management ClientでMatrixを削除する権利を有効にする。	のみ使用可能
Matrixの作成	Matrixで新規のManagement Clientを作成する権限を有効にします。	のみ使用可能
セキュリティを管理	全てのManagement Clientに対し、Matrixのセキュリティ権限を管理する権利を有効にする。	のみ使用可能

ルール

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。

セキュリティ権限	説明
読み取る	Management Clientの既存のルールを見る権利を有効にする。
編集	ルールのプロパティを編集し、Management Clientにおけるルールの作用を定義する権利を有効にする。 ユーザーは、ルールに影響される全てのデバイスの読み出し権限を持っていることが要求されます。
削除	Management Clientからルールを削除する権利を有効にする。 また、ルールによって影響を受けるすべてのデバイスに、ユーザーの読み取り権限があることも必要です。
ルールを作成	Management Clientのルールを新規作成する権利を有効にする。 また、ルールによって影響を受けるすべてのデバイスに、ユーザーの読み取り権限があることも必要です。
セキュリティを管理	全てのルールに対し、Management Clientのセキリュリティ権限を管理する権利を有効にする。

サイト

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	Management Clientにおいて他のサイトを見る権利を有効にする。接続されているサイトはMilestone Federated Architectureを経由して接続されています。 プロパティを編集するには、各サイトのマネジメントサーバーにおいて編集権限を持っていなければなりません。
セキュリティを管理	すべてのサイトにおけるセキュリティ権限を管理する権限を有効にします。

システムモニター

以下の設定は、XProtect ExpertおよびXProtect Corporateでのみ利用ができます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	XProtect Smart Clientのシステムモニターを表示する権利を有効にします。
編集	Management Clientのシステムモニターのプロパティを編集する権利を有効にします。
セキュリティを管理	全てのシステムモニターに対し、Management Clientのセキュリティ権限を管理する権利を有効にする。

メタデータ検索

以下の設定は、XProtect ExpertおよびXProtect Corporateでのみ利用ができます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	Management Clientとその関連設定でメタデータ使用機能を表示する権利を有効にしますが、設定を変更する権利は有効になりません。
メタデータ検索設定の編集	Management Clientでメタデータ検索カテゴリを有効または無効にする権利を有効にします (人や車両のメタデータなど)。
セキュリティを管理	メタデータ検索のセキュリティ権限を管理する権利を有効にします。

検索

以下の設定は、XProtect ExpertおよびXProtect Corporateでのみ利用ができます。

セキュリティ権限	説明
パブリックサーチの読み取り	XProtect Smart Clientに保存されているパブリックサーチを表示および開く権限を有効にします。
パブリックサーチの作成	新たに構成した検索をパブリックサーチとしてXProtect Smart Clientに保存する権限を有効にします。

セキュリティ権限	説明
パブリックサーチの編集	XProtect Smart Clientに保存されているパブリックサーチの詳細または構成(名前、説明、カメラ、検索カテゴリなど) を編集する権限を有効にします。
パブリックサーチの削除	保存されているパブリックサーチを削除する権限を有効にします。
セキュリティを管理	検索におけるManagement Clientのセキュリティ許可を管理する権限を有効にします。

アラーム

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
管理	Management Clientでアラームを管理する権限を有効にします。例えば、アラームの優先度を変更したり、他のユーザーにアラームを委譲するなどのアラームの管理、例えば新規から割り当て済みへなどのアラームの確認や状態の変更を、複数のアラームについて同時に行うことができます。 これを許可に設定した場合だけ、オプションダイアログのアラームおよびイベントタブが表示されます。
編集	警告を見て、警告レポートを印刷する権利を有効にする。
アラームを無効にする	警告を無効にする権利を有効にする。
通知の受	XProtect Mobileクライアントと XProtect Web Clientのアラームに関する通知を受信する権限を有効にする。

セキュリティ権限	説明
信	
セキュリティを管理	アラームのセキュリティ権限を管理する権限を有効にします。
作成	Management Clientにおいて、警告定義を新規作成する権利を有効にする。

サーバーログ

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
システムログエントリの読み取り	システムログエントリを読み取る権限を有効にします。
音声ログエントリの読み取り	音声ログエントリを読み取る権限を有効にします。
ルールトリガーログエントリの読み取り	ルールによってトリガーされるログエントリを読み取る権限を有効にします。
ログ設定の読み取り	**[ツール] > [オプション] > [サーバーログ]**でログ設定を読み取る権限を有効にします。
ログ設定の更新	**[ツール] > [オプション] > [サーバーログ]**でログ設定を変更する権限を有効にします。
セキュリティを管理	アラームのセキュリティ権限を管理する権限を有効にします。

入退室管理

XProtect Corporateでは、以下の設定だけが利用できます。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
編集	Management Clientで入退室管理のプロパティを編集する権利を有効にする。
入退室管理の使用	クライアントの入退室管理関連の機能をユーザーが使用できるようにします。
カードホルダーの一覧表示	クライアントの[入退室管理]タブでユーザーはカードホルダーリストを表示できます。
通知の受信	ユーザーがクライアントでアクセスリクエストに関する通知の受信が可能になります。
セキュリティを管理	すべての入退室管理システムのセキュリティ権限を管理する権限を有効にします。

LPR

システムでXProtect LPRが動作している場合、ユーザーに対して、以下の権限を指定します。

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
LPRを使用	クライアントでナンバープレート認識関連機能を使用する権限を有効にします。
ナンバープレート一致リストの管理	Management Clientのナンバープレート一致リストを追加、インポート、修正、エクスポート、削除する権利を有効にする。
ナンバープレート一致リストの読み取り	ナンバープレート一致リストを表示する権利を有効にする。
セキュリティを管理	全てのトランザクション定義に対し、Management Clientのセキリュリティ権限を管理する権利を有効にする。

トランザクションソース

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	Management Clientのトランザクションソースのプロパティを見る権利を有効にする。
編集	Management Clientのトランザクションソースのプロパティを編集する権利を有効にする。
削除	Management Clientのトランザクションソースを削除する権利を有効にする。
作成	Management Clientのトランザクションソースを作成する権利を有効にする。
セキュリティを管理	全てのトランザクションソースに対し、Management Clientのセキュリティ権限を管理する権利を有効にする。

トランザクションの定義

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	Management Clientのトランザクション定義のプロパティを見る権利を有効にする。
編集	Management Clientのトランザクション定義のプロパティを編集する権利を有効にする。
削除	Management Clientのトランザクション定義のプロパティを削除する権利を有効にする。
作成	Management Clientのトランザクション定義のプロパティを作成する権利を有効にする。
セキュリティを管理	全てのトランザクション定義に対し、Management Clientのセキュリティ権限を管理する権利を有効にする。

MIPプラグイン

MIP SDKによって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン(たとえば、外部入退室管理システムまたは同様の機能などとの統合) を開発できます。

デバイスタブ(役割)

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。

[デバイス]タブでは、各デバイス(カメラ等)またはデバイスグループについて、選択した役割のユーザー/グループがXProtect Smart Clientで各デバイス(カメラなど)またはデバイスグループを使用できるかを指定できます。

それぞれのデバイスに対して繰り返すことを忘れないでください。また、デバイスグループを選択し、一度にグループのすべてのデバイスの役割権限を指定することもできます。

この四角で埋められたチェックボックスを選択したり選択解除することはできますが、この場合は、デバイスグループのすべてのデバイスに選択が適用されます。または、デバイスグループの個別デバイスを選択し、どのデバイスに権限が適用されるかを正確に確認することができます。

カメラ関連の権限

カメラデバイスに以下の権限を指定します:

名前	説明
読み取る	選択したカメラが、クライアントで表示されます。
ライブ表示	クライアントで選択したカメラからビデオのライブ表示ができるようにします。XProtect Smart Clientでは、クライアントの[ライブ]タブを表示する権限が役割に付与されていることが必要になります。この権限は、アプリケーション権限の一部として付与されます。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 時間プロファイル内	クライアントで選択したカメラから録画ビデオの再生ができるようにします。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 再生の制限	クライアントで選択したカメラから録画ビデオの再生ができるようにします。再生の制限を指定するか、制限なしを適用します。
シーケンスを読み取る	たとえば、クライアントのシーケンスエクスプローラに関連するシーケンス情報の読み取りを有効にします。
スマートサーチ	クライアントでユーザーがスマートサーチ機能を使用できるようにします。
エクスポート	クライアントから、ユーザーが録画をエクスポートできるようにします。
手動録画を開始	クライアントで選択したカメラからビデオの手動録画を開始できるようにします。

名前	説明
手動録画を停止	クライアントで選択したカメラからビデオの手動録画を停止できるようにします。
ブックマークを読み取る	クライアントでブックマーク詳細の検索、読み取りを許可します。
ブックマークを編集	クライアントでブックマークの編集を許可します。
ブックマークを作成	クライアントでブックマークの追加を許可します。
ブックマークを削除	クライアントでブックマークの削除を許可します。
AUXコマンド	クライアントからの、補助コマンドの使用を許可します。
エビデンスロックの作成と期間の延長	クライアントが、以下のことをできるようにします： • カメラを新規または既存のエビデンスロックに追加 • 既存のエビデンスロックの有効期限を延長 • 既存のエビデンスロックの保護期間を延長 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックの削除と期間の短縮	クライアントが、以下のことをできるようにします： • 既存のエビデンスロックからカメラを削除 • 既存のエビデンスロックを削除 • 既存のエビデンスロックの有効期限を短縮 • 既存のエビデンスロックの保護期間を短縮 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックを読み取る	クライアントユーザーが、エビデンスロックの詳細を検索、読み取りを許可します。

マイク関連の権限

マイクデバイスに、以下の権限を指定します：

名前	説明
読み取る	選択したマイクが、クライアントに表示されます。
ライブ > 聴く	クライアントで選択したマイクからのライブ音声を聞くことができるようにします。XProtect Smart Clientでは、クライアントの[ライブ]タブを表示する権限が役割に付与されていることが必要になります。この権限は、アプリケーション権限の一部として付与されます。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 時間プロファイル内	クライアントで選択したマイクからの録音した音声を再生できるようにします。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 再生の制限	クライアントで選択したマイクからの録音した音声を再生できるようにします。再生の制限を指定するか、制限なしを適用します。
シーケンスを読み取る	たとえば、クライアントのシーケンスエクスプローラに関連するシーケンス情報の読み取りを有効にします。
エクスポート	クライアントから、ユーザーが録画をエクスポートできるようにします。
手動録画を開始	クライアントで選択したマイクからの音声の手動録音を開始できるようにします。
手動録画を停止	クライアントで選択したマイクからの音声の手動録音を停止できるようにします。
ブックマークを読み取る	クライアントでブックマーク詳細の検索、読み取りを許可します。
ブックマークを編集	クライアントでブックマークの編集を許可します。
ブックマークを作成	クライアントでブックマークの追加を許可します。
ブックマークを削除	クライアントでブックマークの削除を許可します。
エビデンスロックの作成と期間の延長	クライアントが、以下のことをできるようにします： • 新規または既存のエビデンスロックにマイクを追加 • 既存のエビデンスロックの有効期限を延長 • 既存のエビデンスロックの保護期間を延長 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。

名前	説明
エビデンスロックの削除と期間の短縮	クライアントが、以下のことをできるようにします： • 既存のエビデンスロックからマイクを削除 • 既存のエビデンスロックを削除 • 既存のエビデンスロックの有効期限を短縮 • 既存のエビデンスロックの保護期間を短縮 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックを読み取る	クライアントユーザーが、エビデンスロックの詳細を検索、読み取りを許可します。

スピーカー関連の権限

スピーカーデバイスに以下の権限を指定します：

名前	説明
読み取る	選択したスピーカーが、クライアントで表示されます
ライブ > 聴く	クライアントで選択したスピーカーからのライブ音声を聞くことができるようにします。XProtect Smart Clientでは、クライアントの[ライブ]タブを表示する権限が役割に付与されていることが必要になります。この権限は、アプリケーション権限の一部として付与されます。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 時間プロファイル内	クライアントで選択したスピーカーから録音した音声を再生できるようにします。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 再生の制限	クライアントで選択したスピーカーから録音した音声を再生できるようにします。再生の制限を指定するか、制限なしを適用します。
シーケンスを読み取る	たとえば、クライアントのシーケンスエクスプローラに関連するシーケンス情報の読み取りを有効にします。

名前	説明
エクスポート	クライアントから、ユーザーが録画をエクスポートできるようにします。
手動録画を開始	クライアントで選択したスピーカーからの音声の手動録音を開始できるようにします。
手動録画を停止	クライアントで選択したスピーカーからの音声の手動録音を停止できるようにします。
ブックマークを読み取る	クライアントでブックマーク詳細の検索、読み取りを許可します。
ブックマークを編集	クライアントでブックマークの編集を許可します。
ブックマークを作成	クライアントでブックマークの追加を許可します。
ブックマークを削除	クライアントでブックマークの削除を許可します。
エビデンスロックの作成と期間の延長	クライアントが、以下のことをできるようにします： • 新規または既存のエビデンスロックにスピーカーを追加 • 既存のエビデンスロックの有効期限を延長 • 既存のエビデンスロックの保護期間を延長 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックの削除と期間の短縮	クライアントが、以下のことをできるようにします： • 既存のエビデンスロックからスピーカーを削除 • 既存のエビデンスロックを削除 • 既存のエビデンスロックの有効期限を短縮 • 既存のエビデンスロックの保護期間を短縮 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックを読み取る	クライアントユーザーが、エビデンスロックの詳細を検索、読み取りを許可します。

メタデータ関連の権限

メタデータデバイスに、以下の権限を指定します：

名前	説明
読み取る	クライアントでメタデータデバイスを表示し、メタデータデバイスからデータを取得することを有効にします。
編集	メタデータのプロパティを編集する権限を有効化 また、ユーザーがManagement ClientでMIP SDKを介して、メタデータデバイスを有効または無効にすることも可能になります。
ライブ表示	クライアントでカメラからのメタデータを表示する権限を有効にします。XProtect Smart Clientでは、クライアントの[ライブ]タブを表示する権限が役割に付与されていることが必要になります。この権限は、アプリケーション権限の一部として付与されます。
再生	クライアントでメタデータデバイスからの録画データを再生する権限を有効にします。
シーケンスを読み取る	クライアントでメタデータデバイスからの記録されたデータをブラウズしながら、シーケンス機能を使用する権限を有効にします。
エクスポート	クライアントでメタデータデバイスから録音した音声をエクスポートする権限を有効にします。
エビデンスロックの作成と期間の延長	クライアントでメタデータのエビデンスロックを作成、延長する権限を有効にします。
エビデンスロックを読み取る	クライアントでメタデータのエビデンスロックを表示する権限を有効にします。
エビデンスロックの削除と期間の短縮	クライアントでメタデータのエビデンスロックを削除または短縮する権限を有効にします。
手動録画を開始	クライアントでメタデータの手動録画を開始する権限を有効にします。
手動録画を停止	クライアントでメタデータの手動録画を停止する権限を有効にします。

入力関連権限

入力デバイスに、以下の権限を指定します：

名前	説明
読み取る	選択した入力は、クライアントで表示されます。

出力関連権限

出力デバイスに、以下の権限を指定します：

名前	説明
読み取る	選択した出力は、クライアントで表示されます。表示される場合、出力はクライアントのリストで選択できます。
実行	選択した出力は、Management Clientおよびクライアントからアクティブ化できます。時間プロファイルを指定するか、デフォルト値のままにします。

PTZタブ(役割)

PTZ(パン/チルト/ズーム) カメラの権限は、PTZタブで設定します。ユーザー/グループがクライアントで使用できる機能を指定できます。個別のPTZカメラを選択したり、PTZカメラを含んでいるデバイスグループを選択することができます。

PTZに、以下の権限を指定します。

名前	説明
手動PTZ	選択した役割が、選択したカメラでPTZ機能を使用し、パトロールを一時停止できるかどうかを決定します。 時間設定を指定するか、[常時]を選択するか、その役割の[情報]タブで定義されたデフォルト時間設定に対応するデフォルト値のままにします。
PTZプリセットまたはパトロールプロファイルの実行	選択した役割が選択したカメラをプリセット位置に移動し、パトロールプロファイルを開始および停止し、パトロールを一時停止できるかどうかを決定します。 時間設定を指定するか、[常時]を選択するか、その役割の[情報]タブで定義されたデフォルト時間設定に対応するデフォルト値のままにします。 この役割がカメラの他のPTZ機能を使用することを許可するには、手動PTZ権限を有効にします。
PTZ優先度	PTZカメラの優先度を決定します。監視システムの複数のユーザーが同時に同じPTZカメラを制御しようとすると、競合が発生する可能性があります。 選択済みの役割を持つユーザー/グループが選択したPTZカメラを使用する優先度を指定することで、この状況を回避できます。1～32,000の範囲で優先度を指定します。1が最低優先度です。

名前	説明
	デフォルトの優先度は 3,000 です。最高の優先度を持つ役割は、PTZカメラをコントロールできる人の役割です。
PTZプリセットまたはパトロールプロファイルの管理	Management ClientとXProtect Smart Clientの両方で選択したカメラのPTZプリセットとパトロール設定を追加、編集、および削除する権限を決定します。 この役割がカメラの他のPTZ機能を使用することを許可するには、手動PTZ権限を有効にします。
PTZプリセットのロック/ロック解除	役割が選択したカメラのプリセット位置をロックおよびロック解除できるかどうかを決定します。
PTZ セッションの予約	予約されたPTZセッションモードで、選択したカメラを設定する権限を決定します。 予約されたPTZセッションでは、より高いPTZ優先度の他のユーザーまたはパトロールセッションでも制御を取得できません。 この役割がカメラの他のPTZ機能を使用することを許可するには、手動PTZ権限を有効にします。
PTZ セッションのリリース	選択した役割が他のユーザーのPTZセッションをManagement Clientからリリースできるかどうかを決定します。 この権限がなくても、自分のPTZセッションは常にリリースできます。

通話タブ(役割)

スピーカーがシステムで使用できる場合のみ該当します。スピーカーに、以下の権限を指定します:

名前	説明
通話	選択したスピーカーを通じて、ユーザーが通話を許可されるかどうかを決定します。時間プロファイルを指定するか、デフォルト値のままにします。
通話優先度	複数のクライアントユーザーが同じスピーカーから同時に通話したい場合、対立が生じることがあります。 選択済みの役割を持つユーザー/グループが選択したスピーカーを使用する優先度を指定することで、この問題を解決できます。優先度を非常に低い～非常に高いに指定します。最高の優先度の役割は、他の役割に優先してスピーカーを使用できます。 同じ役割の2人のユーザーが同時に通話しようとする場合、先着順の原則が適用されます。

リモート録画タブ(役割)

リモート録画について、以下の設定を指定します。

名前	説明
リモート録画の取得	リモートサイトのカメラ、マイク、スピーカー、ならびにメタデータデバイス、あるいはカメラのエッジストレージからクライアントの記録を取り出す権利を有効にする。

Smart Wallタブ(役割)

クライアントユーザーに対し、役割を通して以下のSmart Wall機能に対するユーザー関連のユーザー権利を与えるSmart Wallことができます。

名前	説明
読み取る	クライアントの選択アイテムをユーザーが見ることSmart Wallを許可する。
編集	以下の選択アイテムSmart Wallをユーザーが編集することを許可するManagement Client。
削除	以下の選択アイテムSmart Wallをユーザーが削除することを許可するManagement Client。
操作	ユーザーがクライアントの選択アイテムにレイアウトを適用し、Smart Wall選択されたプリセットをアクティブにすることを許可する。
再生	ユーザーに対し、クライアント内の選択されたSmart Wallから録画されたデータを再生することを許可します。

外部イベントタブ(役割)

以下の外部イベント権限を指定します。

名前	説明
読み取る	ユーザーが、クライアントや以下の任意の外部システムイベントを検索し、見ることを許可しますManagement Client。

名前	説明
編集	ユーザーが、クライアントや以下の任意の外部システムイベントを編集することを許可しますManagement Client。
削除	ユーザーが、クライアントや以下の任意の外部システムイベントを削除することを許可します Management Client。
トリガー	ユーザーが、クライアントや以下の選択された外部システムイベントをトリガーすることを許可します。

ビューグループタブ(役割)

ビューグループタブで、任意の役割を持ったユーザーとユーザーグループが、クライアントでどのビューグループを使うことができるか特定します。

ビューグループに、以下の権限を指定します:

名前	説明
読み取る	クライアントとManagement Clientのビューグループを見る権利を有効にする。ビューグループがManagement Clientに作成されます。
編集	Management Clientのビューグループのプロパティを編集する権利を有効にする。
削除	Management Clientのビューグループを削除する権利を有効にする。
操作	XProtect Smart Clientにあるビューグループを使用する権利を有効にします。これにより、サブグループとビューの作成と削除が可能になります。

サーバータブ(役割)

[サーバー]タブでの役割権限の指定は、システムがMilestone Federated Architectureの設定で動作する場合のみ有効です。

名前	説明
サイト	Management Clientにおいて、任意のサイトを見る権利を有効にする。接続されているサイトはMilestone Federated Architectureを経由して接続されています。 プロパティを編集するには、各サイトのマネジメントサーバーにおいて編集権限を持っていなければなりません。

詳細については、ページ412のMilestone Federated Architectureの設定を参照してください。

Matrixタブ(役割)

システムで、Matrix受信者を設定している場合、Matrix役割権限も設定します。クライアントから、選択したMatrix受信者へビデオを送信できます。これを受信できるユーザーをMatrixタブで選択します。

以下の権限が利用できます。

名前	説明
読み取る	選択した役割のユーザーおよびグループが、クライアントからビデオを選択して、Matrix受信者へ送信できるかどうかを決定します。

アラームタブ(役割)

システム設定において警告を使用して、中央部の概観やインストールの制御(他の全てのXProtectサーバーを含む)警告タブを使って、任意の役割を持つユーザー/グループが持つべき警告権(例えば、クライアントの警告の処理の仕方)を指定することができます。

アラームに、以下の権限を指定します:

名前	説明
管理	警告を管理する(例えば、警告の優先度を変更する)、警告を他のユーザーへ委託する、警告を確認する、複数の警告のステータスを同時に変更する(例えば新規から割り当て済へ変更)。
ビュー	警告を見て、警告レポートを印刷する権利を有効にする。

名前	説明
アラームを無効にする	警告を無効にする権利を有効にする。
通知の受信	XProtect Mobileクライアントと XProtect Web Clientのアラームに関する通知を受信する権限を有効にする。

入退室管理タブ(役割)

基本ユーザーやWindowsのユーザー、グループを追加または編集する際に、入退室管理の設定を指定できます。

名前	説明
入退室管理の使用	クライアントの入退室管理関連の機能をユーザーが使用できるようにします。
カードホルダーの一覧表示	クライアントの[入退室管理]タブでユーザーはカードホルダーリストを表示できます。
通知の受信	ユーザーがクライアントでアクセスリクエストに関する通知の受信が可能になります。

LPR タブ(役割)

システムでXProtect LPRが動作している場合、ユーザーに対して以下の権限を指定します。

名前	説明
LPRを使用	クライアントで LPR関連機能を使用する権利を有効にします。
ナンバープレートマッチリストの管理	Management Clientのナンバープレートのマッチリストを追加、インポート、修正、エクスポート、削除する権利を有効にする。
ナンバープレートマッチリストの読み取り	ナンバープレートのマッチリストを見る権利を有効にする。

MIPタブ(役割)

MIP SDKによって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン(たとえば、外部入退室管理システムまたは同様の機能などとの統合)を開発できます。

変更する設定は、実際のプラグインによって異なります。MIPタブから、プラグイン用のカスタム設定を見つけてください。

基本ユーザー(説明付き)

基本ユーザーを追加する際、個別のユーザーについて、基本ユーザー名とパスワード認証で監視システム専用のユーザーアカウントを作成します。これは、Active Directoryを使用して追加されたWindowsユーザーとは対照的です。

基本ユーザーの操作を行う際には、基本ユーザーとWindowsユーザーの違いを理解しておくことが重要です。

- 基本ユーザーは、システム固有のユーザー名とパスワードの組み合わせによって認証されます。基本ユーザーのユーザー名kとパスワードが同じでも、あるフェデレーテッドサイトで作成された基本ユーザーは他のフェデレーテッドサイトにはアクセスできません
- Windowsユーザーは、マシン固有のWindowsログインに基づいて認証されます

基本ユーザーの作成

基本ユーザーを作成するには:

1. [セキュリティ]を展開し[基本ユーザー]をクリックします。
2. [基本ユーザー]ペインを右クリックして、[基本ユーザーの作成]を選択します。
3. ユーザー内とパスワードを指定し、パスワードを再入力して、正しく入力されていることを確認します。

> パスワードはマネジメントサーバー サービスがインストールされたコンピュータ上のWindows オペレーティング システムのための求める複雑性要件を満たす必要があります。

4. OKをクリックして、新しい基本ユーザーを作成します。

サイトナビゲーション:システムダッシュボード

この記事では、レポートの作成やデータの保護などを含む、システムの監視方法について説明します。

システムダッシュボード(説明付き)

システムダッシュボードには、システムとコンポーネントを監視する機能があります。

次の機能にアクセスします。

名前	説明
システムモニター	定義するパラメータでサーバーとカメラのステータスを監視します。
システムモニターしきい値	システムモニターで使用されるサーバーおよびモニタータイルで監視されるパラメータのしきい値を設定します。
エビデンスロック	システムで保護されているすべてのデータの概要を把握できます。
現在のタスク	選択したレコーディングサーバーの実行中のタスクの概要を把握できます。
設定レポート	印刷する前に、システム設定レポートに何を含めるかを決定します。

システムモニター(説明付き)

システムモニターでは、システムのサーバーとカメラの現在の状態の概要が、システムハードウェアを表す色付きのタイルによって視覚的に表示され、簡単に確認できます。既定では、すべてのレコーディングサーバー、すべてのサーバー、およびすべてのカメラを表すタイルが表示されます。

タイルの色：

タイルの色	説明
緑	正常状態。すべてが正常に動作しています。
黄色	警告状態。1つ以上のモニターパラメータが正常状態のしきい値を超えています(ページ382のシステムモニターしきい値(説明付き)を参照)。
赤	重大状態。1つ以上の監視パラメータが正常状態と警告状態のしきい値を超えています。

ダッシュボードに表示するタイルの数を増減する場合は、サーバーおよびカメラタイルをカスタマイズできます。たとえば、1台のサーバー、1台のカメラ、カメラのグループ、またはサーバーグループを表すようにタイルを設定できます。また、タイルを使用しない場合や、監視パラメータを編集する場合は、タイルを削除できます。たとえば、監視パラメータは、CPU利用率またはサーバーの空きメモリなどです。これらのパラメータをサーバータイルから削除すると、タイルは該当するタイルでこれらのパラメータを監視しません。タブの右上端で[カスタマイズ]をクリックすると、[ダッシュボードのカスタマイズ]ウィンドウが開きます。詳細については、「ダッシュボードのカスタマイズ」を参照してください。

システムモニターしきい値で設定されたしきい値に基づいて、タイルの状態と色が変わります。システムではデフォルトしきい値の一部が設定されませんが、各3つの状態のしきい値を自分で決定できます。しきい値を設定または変更するには、システムモニターしきい値を使用できます。ページ382のシステムモニターしきい値(説明付き)を参照してください。

タイルの色が変わり、タイルの色の変化につながるサーバー/パラメータを確認する場合は、タイルをクリックします。これにより、画面の下に概要が開き、タイルで有効にした各監視パラメータの色(赤、黄、緑)が表示されます。[詳細]ボタンをクリックすると、状態が変わった原因に関する詳細情報が表示されます。

警告サインが現れた場合は、マウスをその上に持っていくと、システムがエラーメッセージが表示されます。

システムモニターの機能では、Data Collectorが実行されていることが必要となります。

ダッシュボードのカスタマイズ

新しいカメラまたはサーバータイルの追加：

1. [システムモニター]ウィンドウで[カスタマイズ]をクリックします。
2. [ダッシュボードのカスタマイズ]ウィンドウが表示されたら、[サーバータイル]または[カメラタイル]の下で[新規]をクリックします。
3. [新しいサーバータイル/新しいカメラタイル]ウィンドウで、監視するサーバーまたはカメラを選択します。
4. [監視パラメータ]の下で、該当するタイルから追加または削除するパラメータのチェックボックスをオンまたはオフにします。
5. OK をクリックします。新しいサーバーまたはカメラタイルがダッシュボードに表示されるタイルに追加されます。

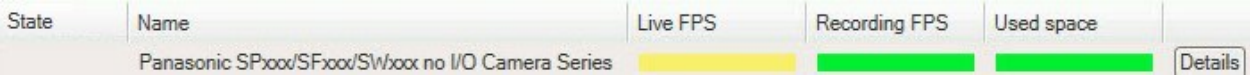
監視パラメータの編集：

1. [システムモニターダッシュボード]ウィンドウで[カスタマイズ]をクリックします。
2. [ダッシュボードのカスタマイズ]ウィンドウが表示されたら、[サーバータイル]または[カメラタイル]の下で[編集]をクリックします。
3. [サーバータイルの編集]または[カメラタイルの編集]ウィンドウで、編集するサーバーコンポーネントまたはカメラを選択します。
4. [監視パラメータ]ボックスで、該当するタイルから追加または削除する監視パラメータのチェックボックスをオンまたはオフにします。
5. OK をクリックします。変更された監視パラメータは、該当するタイルの一部か、該当するタイルから削除されます。

必要に応じて、システムの履歴データを有効および無効にできます。このデータを無効にする場合は、前のシステムの動作のグラフを表示できません。SQL Serverとデータベース、または帯域幅の負荷を軽減したい場合は、履歴データのサンプリング間隔を減らすことができます。履歴データのサンプリング間隔を低くする場合は、グラフに表示される詳細が少なくなります。

システムモニターの詳細(説明付き)

サーバーまたはカメラタイルをクリックすると、ダッシュボードの下に選択した監視パラメータのステータスがそれぞれ表示されます。



例：カメラのライブFPS監視パラメータが警告状態に達しました。

[状態]フィールドにはカメラの状態が表示されます。たとえば、デバイスへの接続が切断された場合は、赤色の警告が表示されます。アイコンにはツールチップがあり、警告の原因となる問題が簡単に説明されています。

[使用されているスペース]フィールドには、デバイスが以前に他のレコーディングサーバー上にあった場合など、このデバイスの録画がある他のレコーディングサーバーのデータが表示されます。

該当するカメラ/サーバーの[詳細]ボタンをクリックすると、システム情報を表示し、次の項目に関するレポートを作成できます。

コンポーネント	説明
マネジメントサーバー	選択したマネジメントサーバーのデータを表示します
レコーディングサーバー	選択したレコーディングサーバーのデータを表示します。以下を元に表示できます。 • ディスク • ストレージ • ネットワーク • カメラ
フェールオーバーレコーディングサーバー	選択したフェールオーバーレコーディングサーバーのデータを表示します。
追加のサーバー	ログサーバー、イベントサーバーなどでデータを表示します。
カメラ	設定にある任意のカメラグループの任意のカメラでデータを表示します。

これらの各要素は、クリックして展開できます。この領域をクリックすると、このサーバーまたはカメラの関連する動的データが表示されます。

カメラバーには、選択の対象となるカメラグループのリストが含まれています。グループを選択すると、特定のカメラを選択してその動的データを表示することができます。すべてのサーバーが、CPU使用率および使用可能メモリの情報を表示できます。レコーディングサーバーも、接続ステータスの情報を表示します。それぞれのビューには、履歴リンクがあります。それをクリックすると、履歴データとレポートが表示されます(カメラのレポートを表示するには、カメラの名前をクリックします)。それぞれの履歴レポートで、最近24時間、7日または30日のデータを表示できます。レポートを保存および/または印刷するには、PDFへ送信アイコンをクリックします。「<」およびホームアイコンを使用して、システムモニターをナビゲートします。

デバイスが現在存在するレコーディングサーバーのデータを使用した場合にのみ履歴レポートを作成できます。

サーバーのオペレーティングシステムからシステムモニターの詳細にアクセスした場合、Internet Explorer Enhanced Security Configurationに関連するメッセージが表示されることがあります。メッセージの指示に従って、「システムモニター]のページを信頼済みサイトゾーンに追加してから続行してください。

システムモニターしきい値(説明付き)

システムモニターしきい値を使用することで、システムハードウェアの状態の変化についてシステムモニター上のタイルで視覚的に示さなければならない場合(たとえばサーバーのCPU使用が正常状態(緑)から警告状態(黄)に変化した場合など)に、グローバルしきい値を設定および調整すること可能となります。

システムにはデフォルトのしきい値が設定されているため、システムを設定した時点よりシステムハードウェアのモニタリングを開始できます。しきい値を変更する方法については、「ページ384のシステムモニターしきい値の設定」を参照してください。

デフォルトでは、特定のハードウェアの全ユニット(すべてのカメラまたはサーバーなど)のしきい値を表示するよう設定されています。個々のサーバーまたはカメラ、あるいはこれらのサブセットのしきい値を設定することも可能です。個々のサーバーまたはカメラのしきい値を設定するという操作は、たとえば一部のカメラに対して他のカメラよりも高いライブFPSまたはレコーディングFPSを設定したい場合などに有効となり得ます。

サーバー、カメラ、ディスク、ストレージのしきい値を設定できます。しきい値を変更するには、しきい値コントロールスライダーを使用します。しきい値コントロールスライダーの(状態分割地点にある)ハンドルを上下にドラッグすることで、しきい値を増減します。しきい値コントロールスライダーは、システムモニターのサーバー/カメラタイルと同じように色分けされています(ページ382のシステムモニターしきい値(説明付き)を参照)。

システムハードウェアの使用/負荷が短時間(1秒前後)しか高しきい値に達しなかった場合に重大または警告状態が表示されないようにするには、計算間隔を使用します。計算間隔機能では、システムハードウェア状態の短時間の変更または頻繁な変更の影響が平均化されます。具体的には、この計算間隔機能によって経時的なハードウェア変更の影響が均一化されるため、しきい値を超えるたびにアラートが発生することがなくなります。

たとえば、[計算間隔]を1分間に設定した場合、1分間全体にわたる平均値がしきい値を超えた場合にのみアラートが発生します。この利点として、ハードウェアの頻繁かつ恐らくは無関係な状態変更に関するアラートを避けつつ、CPU使用やメモリの消費といった継続的な問題を示すアラートのみが表示されるように設定できます。計算間隔の値を変更する方法については、「ページ384のシステムモニターしきい値の設定」を参照してください。

サーバーのしきい値

しきい値	説明	単位
CPU使用率	モニタリングしているサーバーのCPU使用のしきい値。	%
使用可能なメモリ容量	モニタリングしているサーバーのRAMメモリ使用のしきい値。	MB
NVIDIAデコード	モニタリングしているサーバーのNVIDIAデコード使用のしきい値。	%
NVIDIAメモリ	モニタリングしているサーバーのNVIDIA RAMメモリ使用のしきい値。	%
NVIDIAレンダリング	モニタリングしているサーバーのNVIDIAレンダリング使用のしきい値。	%

カメラのしきい値

しきい値	説明	単位
ライブFPS	モニタリングしているカメラにライブビデオが表示されている際の、使用中のカメラのFPSのしきい値。	%
レコーディングFPS	モニタリングしているカメラでビデオが録画されている際の、使用中のカメラのFPSのしきい値。	%
使用済み領域	モニタリングしているカメラによって使用されている領域のしきい値。	GB

ディスクのしきい値

しきい値	説明	単位
空き領域	モニタリングしているディスクの空き容量のしきい値。	GB

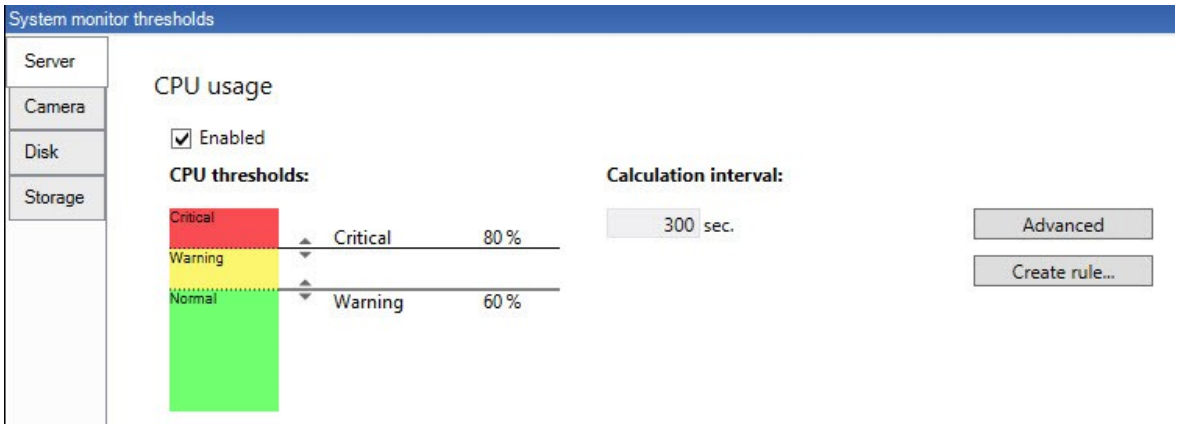
ストレージのしきい値

しきい値	説明	単位
保存期間	ストレージの領域がどの時点でなくなるかの予測を表すしきい値。状態はシステムの設定にもとづいて表示され、1日に2回更新されます。	日数

ルールを設定(「ページ309のルール」を参照) することで、しきい値がある状態から別の状態に変化した際に、特定のアクションを実行したりアラームをアクティブ化したりもできます(「ページ378のシステムダッシュボード(説明付き)」を参照) 。

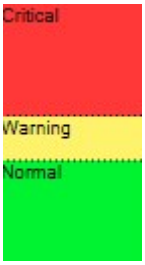
システムモニターしきい値の設定

1. [サイトナビゲーション]ペインで、[システムモニターしきい値]を選択します。
2. まだ有効にしていない場合は、関連するシステムハードウェアの[有効にする]チェックボックスを選択します。以下の値が例として挙げられます。



3. しきい値コントロールスライダを上下にドラッグし、しきい値を増減します。しきい値コントロールに表示される各システムハードウェアで使用可能なスライダは2つあり、[正常]、[警告]、[重大]レベルを識別します。
4. 計算間隔のための値を入力、あるいはデフォルトの値を保持します。
5. それぞれのハードウェアにおいて値を設定したい場合は、[アドバンスド]をクリックします。
6. 特定のイベントに対する、あるいは特定のタイムインターバルにおけるルールを設定したい場合、[ルールを作成する]をクリックします。
7. 関連するしきい値レベルおよび計算間隔を設定したら、メニューから[ファイル] > [保存]を選択します。

しきい値設定の例：



- 赤色は、[重大]ステイタスに達したことを示します。
- 黄色は、[警告]ステイタスです。これは、あなたが[重大]レベルに近づいていることを示します。
- 緑色は、正常状況で、利用者が選択したしきい値内にあることを示します。

エビデンスロック(説明付き)

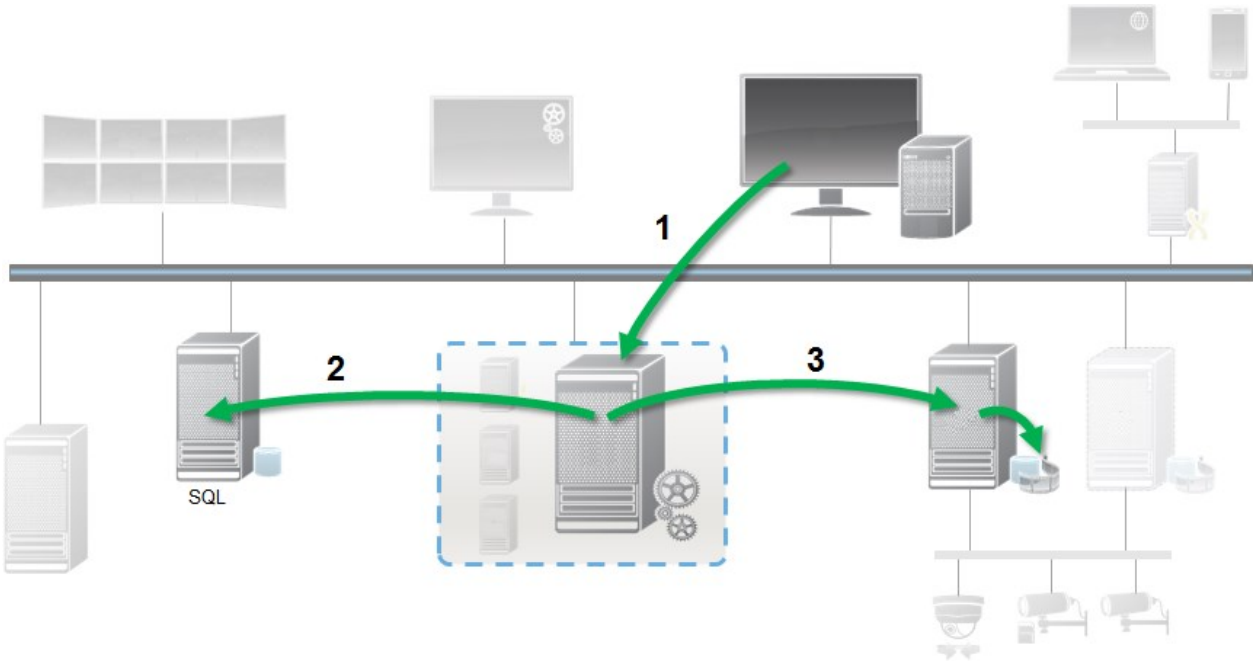
使用可能な機能は、使用しているシステムによって異なります。詳細については、https://www.milestonesys.com/solutions/platform/product-index/を参照してください。

XProtect VMSバージョン2020 R2の時点において、マネジメントサーバーを以前のバージョンからアップグレードしても、バージョン2020 R1またはそれ以前のレコーディングサーバーでのエビデンスロックの作成または修正は、これらのレコーディングサーバーをアップグレードしない限り行うことはできません。これは、ハードウェアが(2020 R1またはそれ以前の)レコーディングサーバーから別のレコーディングサーバーへと移され、以前のサーバーに記録が残っている場合でも、エビデンスロックを作成または修正できないことを意味します。

エビデンスロック機能を使用して、クライアントオペレータは、例えば捜査や裁判が行われている間、必要に応じて、音声や他のデータを含むビデオシーケンスが削除されないように保護できます。エビデンスロックをかける方法については、XProtect Smart Clientマニュアルを参照してください。

保護されている場合、システムのデフォルト保持時間を過ぎた場合の自動削除や、クライアントユーザーによる手動削除によっても、データは削除できなくなります。システムまたはユーザーは、十分なユーザー権限を持つユーザーがエビデンスをロック解除しない限り、データを削除できません。

エビデンスロックのフロー図：



1. ユーザーはXProtect Smart Clientでエビデンスロックを作成します。情報がマネジメントサーバーに送信されます。
2. Management Serverには、SQLデータベース内のエビデンスロックに関する情報が保存されます。
3. マネジメントサーバーはレコーディングサーバーに対して、データベースの保護された録画を保存して保護するように指示します。

オペレータがエビデンスロックを作成するときには、保護されたデータは録画されたレコーディングストレージにあり、保護されていないデータとともにアーカイブディスクに移動されます。一方、保護されたデータは次のように処理されます。

- エビデンスロックに設定された保持時間。これは無期限になる可能性があります。
- 保護されていないデータにグルーミングが設定されている場合でも、録画の元の品質が維持されます。

オペレータがロックを作成すると、シーケンスの最小サイズは、データベースが録画されたファイルを分割する期間です。デフォルトでは、1時間のシーケンスです。この値は変更できますが、レコーディングサーバーのRecorderConfig.xmlファイルをカスタマイズする必要があります。小さいシーケンスが2つの1時間の期間にまたがる場合は、両方の期間で録画がロックされます。

Management Clientの監査ログでは、ユーザーが証拠ロックを作成、編集、または削除した日時を確認できます。

ディスクの領域が不足した場合、保護されたデータには影響しません。この場合、最も古い保護されていないデータが削除されます。削除する保護されていないデータがない場合は、システムは録画を停止します。ディスクが満杯のイベントによってトリガーされるルールとアラームを作成し、自動的に通知を発行することができます。

大量のデータが長期にわたり保存され、ディスク領域に影響する可能性がある場合を除き、このようなエビデンスロック機能はシステムのパフォーマンスに影響しません。

ハードウェアを別のレコーディングサーバーに移動する場合(「ページ451のハードウェアの移動」を参照)：

- エビデンスロックで保護された録画は、作成された時点でエビデンスロックに設定された保存期間に従い、古いレコーディングサーバーに残ります。
- XProtect Smart Clientユーザーは、別のレコーディングサーバーに移動する前に、カメラで作成された録画でエビデンスロックを使用してデータを保護できます。カメラを複数回移動する場合でも、録画は複数のレコーディングサーバーに保存されます。

デフォルトでは、すべてのオペレータにデフォルトのエビデンスロックプロファイルが割り当てられていますが、この機能に対するユーザーアクセス権は割り当てられていません。役割のエビデンスロックアクセス権限を指定するには、ページ366のデバイスタブ(役割)で役割設定について参照してください。役割のエビデンスロックプロファイルを指定するには、ページ341の情報タブ(役割)で役割設定について参照してください。

Management Clientでは、デフォルト証拠ロックプロファイルのプロパティを編集したり、代わりに追加の証拠ロックプロファイルを作成して、役割に割り当てることができます。

システムダッシュボードのエビデンスロックには、現在の監視システム内で保護されているデータすべての概要が表示されます。

- 保護データの開始日と終了日
- エビデンスをロックしたユーザー
- エビデンスのロックが解除された時刻
- データの保存場所
- 各エビデンスロックのサイズ

エビデンスロックに表示されているすべての情報はスナップショットです。F5を押すと画面が更新されます。

現在のタスク(説明付き)

現在のタスクノードは任意の記録サーバーのタスクの概要、始動時刻、推定終了時刻と経過を表示します。現在のタスクに表示されているすべての情報はスナップショットです。プロパティペインの右下にある更新ボタンをクリックすることで更新できます。

設定レポート(説明付き)

PDF設定レポートを作成する際、システムのあらゆる要素をレポートに含めることができます。例えば、ライセンス、デバイス設定、アラーム設定などを含めることが可能です。また、フォントとページの設定をカスタマイズしたり、カスタマイズした表紙を含めることができます。

設定レポートの追加

1. システムダッシュボードを展開して、設定レポートをクリックします。これによりレポート設定ページが開きます。
2. レポートに含める要素を選択します。
3. オプション: 表紙をクリックして表紙をカスタマイズします。表示されるウィンドウで、必要な情報を入力します。レポートに含める要素として表紙を選択します。選択しないと、カスタマイズする表紙はレポートに含まれなくなります。
4. フォーマットをクリックして、フォント、ページのサイズ、余白をカスタマイズします。表示されるウィンドウで、必要な設定を選択します。
5. エクスポートする準備ができたら、エクスポートをクリックし、名前を選択して、レポートの保存場所を選択します。

設定レポートの詳細

以下は、レポート設定時に使用できます。

名前	説明
すべて選択	リストのすべての要素を選択します。
全てクリアする	リストのすべての要素をクリアします。
フロントページ	レポートの表紙をカスタマイズします。
フォーマッティング	レポートをフォーマットします。
エクスポート	レポートの保存場所を選択してPDFを作成します。

サイトナビゲーション: サーバーログ

この記事では、ログ設定を変更する方法、ログにフィルターをかける方法、そしてエクスポートを作成する方法について説明します。

ログ(説明付き)

ログは、ユーザーアクティビティ、イベント、アクション、そしてシステムにおけるエラーの詳細な録画です。

ログを見るには、[サイトナビゲーション] ペインから、[サーバーログ]を選択してください。

ログタイプ	何がログをされているか?
システムログ	システム関連情報
監査ログ	ユーザーアクティビティ
ルールトリガーログ	ユーザーが新しい<ログエントリ>の作成アクションを指定したルールを録画します。<ログエントリ>アクションの詳細については、ページ288のアクションおよびアクションの停止(説明付き)を参照してください。

別の言語でログを表示するには、ページ116の一般タブ(オプション)下のオプションを参照してください。

コンマで区切られた値‾‾(.csv)ファイル形式ーーでログをエクスポートするには、ページ390のログのエクスポートをご覧ください。

ログ設定を変更するには、ページ118のサーバーログタブ(オプション)を参照してください。

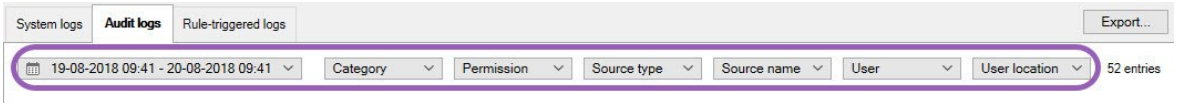
フィルターログ

それぞれのログウィンドウでは、フィルターをかけ、例えば特定のタイムスパンにおける、あるいは特定のデバイスやユーザーの使用におけるログエントリーを確認することができます。

1. [サイトナビゲーション]ペインで、[サーバーログ]を選択します。デフォルトでは、システムログタブが表示されます。

   ログタイプ間をナビゲートするには、別のタブを選択してください。

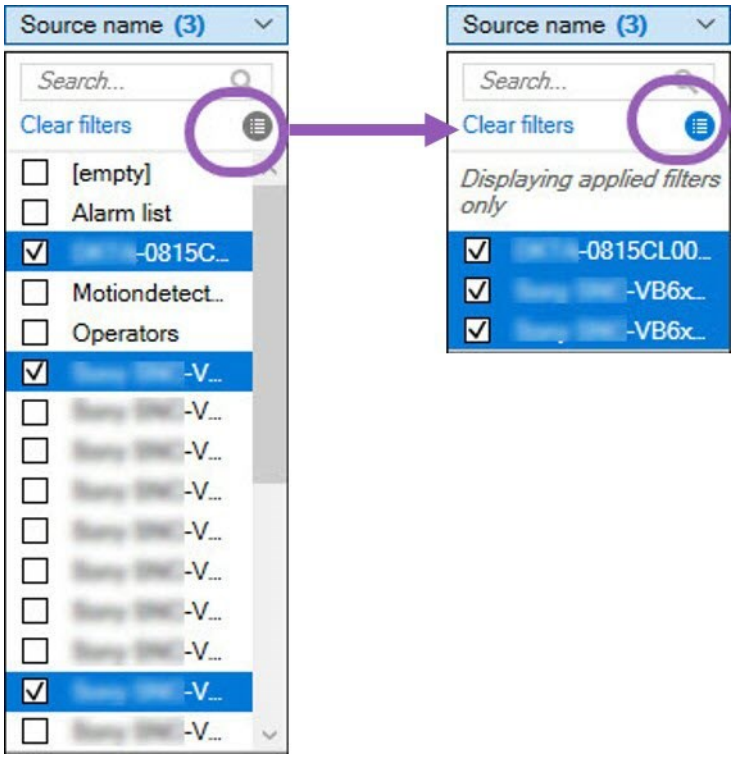
2. このタブの下では、[カテゴリー]、[ソースタイプ]、あるいは[ユーザー]のようなフィルターグループを選択します。



   フィルターの一覧が表示されます。

3. 使用するフィルターを選択します。フィルターを除去するには、もう一度選択します。

   オプション：フィルターのリストで、アプライしたフィルターのみを閲覧するには、使用したフィルターのみを表示するを選択します。



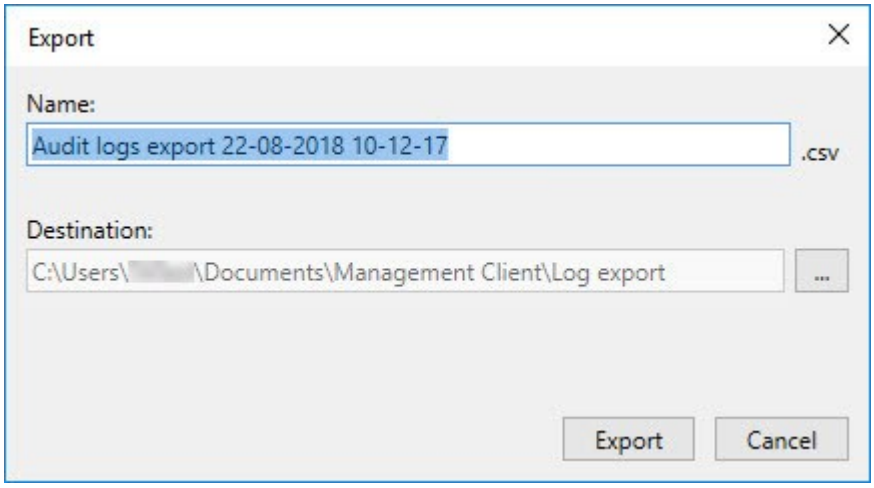
あなたのエクスポートのコンテンツは、使用されたフィルターによって異なります。エクスポートの詳細については、ページ390のログのエクスポート。

ログのエクスポート

ログのエクスポートは、ログの保持期間を越えてログエントリーを保存する、というように便利に活用できます。ログはコンマ区切り値 (.csv) ファイルとしてクスポートできます。

ログをエクスポートするには：

1. 右上コーナーの[エクスポート]を選択します。Exportウィンドウが表示されます。



2. [Name]ウィンドウにおける[Export]フィールドで、ログファイルのための名前を指定します。
3. デフォルトでは、ログのエクスポートフォルダーにエクスポートしたファイルが保存されます。別のロケーションを指定するには、[...][Destination]フィールドの右を選択します。
4. ログをエクスポートするには[Export]を選択します。

あなたのエクスポートのコンテンツは、使用されたフィルターによって異なります。エクスポートの詳細については、ページ389のフィルターログ。

ログを録画するため、2018 R2およびそれ以前のコンポーネントを許可します

ログサーバーの2018 R3バージョンは、強化されたセキュリティのため認証を導入します。これにより、2018 R2およびそれ以前のコンポーネントが新しいログサーバーにログを書くを防ぎます。

影響を受けるコンポーネント:

- XProtect Smart Client
- XProtect LPRプラグイン
- LPRサーバー
- 入退室管理プラグイン
- Event Server
- アラームプラグイン

上記に記載されているコンポーネントの、2018 R2あるいはそれ以前のバージョンをお使いの場合、コンポーネントの新しいログサーバーへの書き込みを許可するかどうかを決定しなければなりません:

1. [ツール]>[オプション]を選択します。
2. [サーバーログ]タブの最下部にある[オプション]ダイアローグボックスで、2018 R2およびそれ以前のコンポーネントのログの書き込みの許可チェックボックスを探します。
   - 2018 R2およびそれ以前のコンポーネントのログの書き込みを許可する場合、チェックを入れます。
   - 2018 R2およびそれ以前のコンポーネントのログの書き込みを許可しない場合、チェックを外します。

システムログ(プロパティ)

ログの各列はログエントリを表します。ログエントリにはさまざまな情報フィールドがあります。

名前	説明
ログレベル	情報、警告、あるいはエラー。
現地時間	システムのサーバーのローカル時間のタイムスタンプ。
メッセージテキスト	記録されたインシデントの識別番号。
カテゴリ	録画したインシデントのタイプ。
ソースタイプ	録画したインシデントが発生した機器のタイプ(サーバーまたはデバイスなど)。
ソース名	録画されたインシデントが発生したサービスの名前。
イベントタイプ	録画されたインシデントで表されたイベントのタイプ。

監査ログ(プロパティ)

ログの各列はログエントリを表します。ログエントリにはさまざまな情報フィールドがあります。

名前	説明
現地時間	システムのサーバーのローカル時間のタイムスタンプ。
メッセージテキスト	録画されたインシデントの説明を表示します。
許可	リモートユーザーアクションが可能か(許可されているか)どうかについての情報。
カテゴリ	録画したインシデントのタイプ。
ソースタイプ	録画したインシデントが発生した機器のタイプ(サーバーまたはデバイスなど)。
ソース名	録画されたインシデントが発生したサービスの名前。
ユーザー	録画されたインシデントを引き起こすリモートユーザーのユーザー名。
ユーザーの場所	リモートユーザーが録画されたインシデントを引き起こしたコンピュータのIPアドレスまたはホスト名。

ルールによってトリガーされるログ(プロパティ)

ログの各列はログエントリを表します。ログエントリにはさまざまな情報フィールドがあります。

名前	説明
現地時間	システムのサーバーのローカル時間のタイムスタンプ。
メッセージテキスト	録画されたインシデントの説明を表示します。
カテゴリ	録画したインシデントのタイプ。
ソースタイプ	録画したインシデントが発生した機器のタイプ(サーバーまたはデバイスなど)。
ソース名	録画されたインシデントが発生したサービスの名前。
イベントタイプ	録画されたインシデントで表されたイベントのタイプ。
ルール名	ログエントリをトリガーするルールの名前。
サービス名	録画されたインシデントが発生したサービスの名前。

サイトナビゲーション: メタデータの使用

この記事では、ビデオ監視システムでメタデータが使用されるよう構成を行う方法について説明します。

> メタデータデバイスの管理と構成については、「ページ202のメタデータデバイス(説明付き)」を参照してください。

メタデータとは?

メタデータとは、あるデータに関するデータを意味します。一例として、ビデオ映像について説明しているデータ、映像内のコンテンツまたはオブジェクト、または録画された映像の場所などが挙げられます。

メタデータは以下の方法で生成できます。

- 自らデータを配信しているデバイス(ビデオを配信しているカメラなど)
- サードパーティシステムまたは統合で、汎用メタデータドライバーを経由した配信

メタデータ検索(説明付き)

メタデータ検索とは、XProtect Smart Clientでのビデオ録画の検索のうち、メタデータに関連した検索カテゴリ/フィルターを使用するものを指します。

デフォルトのMilestoneメタデータ検索カテゴリは以下のとおりです。

- 場所
- 人物
- 車両

メタデータ検索の要件

検索結果を得るには、以下のいずれかひとつが必要となります。

- ビデオ監視システムに、適切に構成されており、かつビデオ分析を実行できるデバイスが少なくともひとつ存在する
- ビデオ監視システムで、メタデータが生成されるビデオ処理サービスが有効になっている

いずれの場合も、メタデータは必要なメタデータ形式でなくてはなりません。

詳細については、メタデータ検索の統合ドキュメントを参照してください。

XProtect Smart Clientでメタデータ検索カテゴリおよび検索フィルターを表示/非表示にする

管理者権限を持っているXProtect Management Clientのユーザーは、XProtect Smart Clientでデフォルトの Milestoneメタデータ検索カテゴリ/検索フィルターを表示または非表示にできます。デフォルトでは、これらの検索カテゴリ/検索フィルターは非表示になっています。ビデオ監視システムがメタデータ検索要件を満たしている場合、これらを表示することで便利な機能を

使用できます。

> この設定は全XProtect Smart Clientユーザーに適用されます。
>
> この設定は以下の可視性には影響しません。
>
> - 他の非メタデータMilestone検索カテゴリ/検索フィルター(モーション、ブックマーク、アラーム、イベントなど)
> - サードパーティの検索カテゴリ/検索フィルター

1. XProtect Management Clientの[サイトナビゲーション]ペインで、[メタデータの使用]>[メタデータ検索]の順に選択します。
2. [メタデータ検索]ペインで、可視性設定を変更したい検索カテゴリを選択します。
3. 検索カテゴリ/検索フィルターの可視性を有効にするには、該当するチェックボックスをオンにします。検索カテゴリ/検索フィルターの可視性を無効にするには、チェックボックスをオフにします。

サイトナビゲーション：アラーム

この記事では、イベントによってトリガーされるアラームがシステムに表示されるよう設定する方法について説明します。

アラーム(説明付き)

> この機能は、XProtect Event Serverがインストールされている場合のみ作動します。

イベントサーバーで処理される機能に基づくアラーム機能により、組織全体の任意のインストール数(他のXProtectシステムも含む)で、一元的なアラームの確認、コントロール、およびアラームの拡張性が得られます。以下のいずれかによりアラームが生成されるように設定できます。

- 内部システム関連のイベント

  例：モーション、サーバーの応答/非応答、アーカイブ上の問題、ディスク空き容量不足など。

- 外部統合イベント

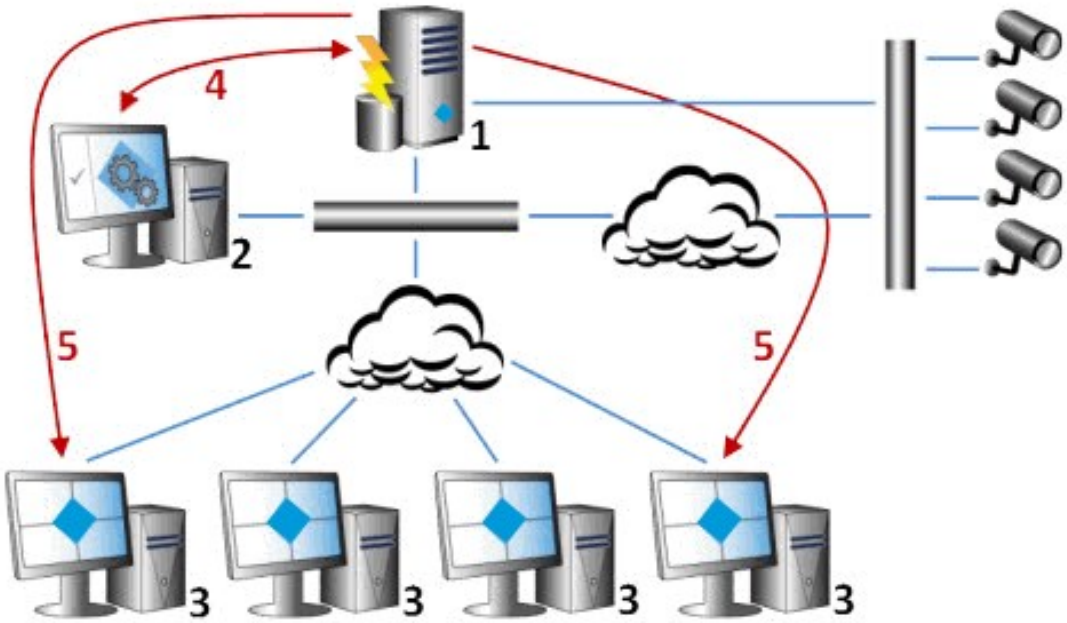
  複数の種類の外部イベントからこのグループを構成することができます。

  - アナリティクスイベント

    一般的に、外部のサードパーティのビデオコンテンツ分析(VCA)プロバイダから受け取ったデータ。

  - MIPプラグインイベント

    MIP SDKによって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン(たとえば、外部入退室管理システムまたは同様の機能などとの統合) を開発できます。



凡例：

1. 監視システム
2. Management Client
3. XProtect Smart Client
4. アラーム設定
5. アラームデータフロー

アラームを処理し、XProtect Smart Clientにあるアラームリストに委譲します。アラームはXProtect Smart Clientのスマートマップおよびマップ機能とも統合できます。

アラーム設定(説明付き)

アラーム設定には以下が含まれます。

- アラーム処理のダイナミックな役割ベース設定
- すべてのコンポーネントの中央技術概要：サーバー、カメラ、および外部装置
- すべての受信アラームとシステム情報の一元的ログ設定
- プラグインの処理、外部入退室管理またはVCAベースシステムなどの他のシステムとのカスタム統合が可能です。

一般的に、アラームを発生させるオブジェクトの視認性によりアラームが制御されます。これにより、アラームに関する4つの側面を活用でき、制御/管理するユーザーと、制御/管理の度合いが関連します。

名前	説明
ソース/デバイス視認性。	アラームを発生させるデバイスが、ユーザーの役割で認識できるように設定されていない場合、ユーザーはXProtect Smart Clientのアラームリストのアラームを確認することはできません。
ユーザー定義イベントをトリガーする権限	この権限は、ユーザーの役割がXProtect Smart Clientの選択したユーザー定義イベントをトリガーできるかどうかを決定します。
外部プラグイン	外部プラグインがシステムに設定されている場合、これらはアラームを処理するユーザーの権限をコントロールする場合があります。
一般役割権限	ユーザーがアラームを確認できるだけか、あるいはアラームを管理できるかを決定します。 アラームのユーザーがアラームにできることは、ユーザーの役割とその役割に課された設定により異なります。

オプションのアラームおよびイベントタブで、アラーム、イベント、ログの設定を指定できます。

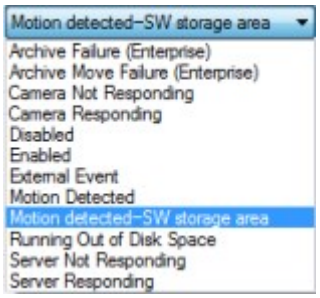
アラーム定義

システムがイベントをシステムに登録する際は、システムをXProtect Smart Clientでアラームを生成するように設定できます。これらを使用する前にアラームを定義する必要があります。アラームはシステムサーバーに登録したイベントに基づき定義してください。また、ユーザー定義イベントを使用してアラームをトリガーしたり、同じイベントを使用して複数の異なるアラームをトリガーすることも可能です。

アラームの追加

アラームを定義するには、アラーム定義を作成する必要があります。ここでは、アラームをトリガーする項目、オペレータが実行する必要がある作業の手順、アラームを停止させる操作やタイミングなどを指定します。設定の詳細については、アラーム定義(プロパティ)を参照してください。

1. サイトナビゲーションペインで、アラームを展開し、アラーム定義を右クリックします。
2. 新規追加を選択します。
3. 次のプロパティを入力します:
   - 名前:アラーム定義の名前を入力します。アラーム定義が一覧表示されるたびに、アラーム定義の名前が表示されます。
   - 手順:アラームを受信するオペレータの手順を作成できます。
   - イベントのトリガー:ドロップダウンメニューを使用して、アラームがトリガーされるときに使用されるイベントタイプとイベントメッセージを選択します。

     選択可能なトリガーイベントのリスト。アナリティクスイベントを使用して、ハイライトされたイベントが作成され、カスタマイズされます。
   - ソース:アラームをトリガーするためのイベントが発生するカメラおよびその他のデバイスを選択します。選択できるオプションは、選択したイベントのタイプにより異なります。
   - 時間設定:特定の期間中にアラームをアクティブ化する場合は、ラジオボタンを選択してから、ドロップダウンメニューでタイムインターバルを選択します。
   - イベントベース:イベントによってアラームをアクティブ化する場合は、ラジオボタンを選択し、アラームを開始するイベントを指定します。また、アラームを停止するイベントも指定する必要があります。
4. 時間制限ドロップダウンメニューで、オペレータのアクションが必要なときの時間制限を指定します。
5. トリガーされたイベントドロップダウンメニューで、時間制限が経過したときにトリガーするイベントを指定します。
6. 関連するカメラや初期アラーム所有者などの追加設定を指定します。

アラーム定義(プロパティ)

アラーム定義の設定:

名前	説明
有効	既定では、アラーム定義は有効です。無効にするには、チェックボックスをオフにします。
名前	アラームの名前は一意である必要はありませんが、一意で分かりやすい名前を使用すると、多くの場合に便利です。
手順	アラームに関する説明や、アラームの原因となる問題を解決する方法に関する説明テキストを入力します。 ユーザーがアラームを処理すると、テキストがXProtect Smart Clientで表示されます。
イベントのトリガー	アラームがトリガーされた時に使用するイベントメッセージを選択します。2つのドロップダウンから選択します。 • 1つ目のドロップダウン:アナリティクスイベントやシステムイベントなどのイベントのタイプを選択します。 • 2つ目のドロップダウン:使用する特定のイベントメッセージを選択します。使用可能なメッセージは、最初のドロップダウンメニューで選択したイベントタイプによって決定されます。
ソース	イベントが発生するソースを指定します。カメラまたは他のデバイスから切断し、ソースは、VCAやMIPなどの定義済みのソースに接続することもできます。選択できるオプションは、選択したイベントのタイプにより異なります。

アラームトリガー:

名前	説明
時間プロファイル	時間プロファイルラジオボタンを選択して、アラーム定義がアクティブなタイムインターバルを指定します。ルールとイベントノードで定義した時間設定だけが一覧に表示されます。何も定義されていない場合は、常時オプションのみを使用できます。

名前	説明
対象のイベント	イベントに基づくアラームにするには、このラジオボタンを選択します。選択した後には、開始イベントと停止イベントを指定します。カメラ、ビデオサーバー、入力で定義されているハードウェアイベントを選択できます。ページ298のイベント概要も参照してください。グローバル/手動イベントも使用できます。ページ325のユーザー定義イベントも参照してください。

オペレータのアクションが必要：

名前	説明
時間制限	オペレータのアクションが必要になる時間制限を選択します。デフォルトは1分です。トリガーされたイベントドロップダウンメニューでイベントを登録するまで、時間制限はアクティブになりません。
トリガーされたイベント	時間制限が経過した場合に、どのイベントをトリガーするか選択します。

マップ：

名前	説明
アラームマネージャービュー	アラームがXProtect Smart Client>アラームマネージャーにリストされている際に、スマートマップまたはマップのいずれかをアラームに割り当てます。 スマートマップには、カメラでトリガーされた場合、およびカメラたスマートマップに追加された場合にアラームが表示されます。スマートマップへのカメラ追加の詳細については、スマートマップでのカメラの追加、削除、編集を参照してください。

その他：

名前	説明
関連するカメラ	カメラ自体がアラームをトリガーしない場合でも、15台までアラーム定義に含めるカメラを選択します。例えば外部イベントメッセージ(ドアが開いているなど) をアラームのソースとして選択している場合です。ドア付近のカメラを1台または複数定義することで、定義したカメラの録画のインシデントをアラームに関連付けることができます。
初期アラームの所有者	アラームに対して責任を負うデフォルトのユーザーを選択します。
初期アラームの優先度	アラームの優先度を選択します。これらの優先度はXProtect Smart Clientで使用し、アラームの重要度を決定します。
アラームのカテゴリ	アラームのカテゴリ、例えば誤警報または要調査を選択します。
アラームでトリガーされるイベント	XProtect Smart Clientでアラームがトリガーできるイベントを定義します。
アラームを自動で閉じる	特定のイベントによってアラームを自動的に停止する場合は、このチェックボックスを選択します。すべてのイベントがアラームをトリガーするわけではありません。最初から新しいアラームを無効にしたい場合は、チェックボックスを選択解除します。
管理者にアサインできるアラーム	アサイン先リストで管理者の役割のあるユーザーを含めるようチェックボックスを選択します。。 アサイン先リストは、XProtect Smart Clientの アラームマネジャータブのアラーム詳細にあります。 チェックボックスをクリアすると、管理者の役割があるユーザーをアサイン先リストからフィルターアウトして、リストを短縮できます。

アラームデータ設定

アラームデータ設定を行う際には、以下を指定します。

アラームデータレベルタブ
優先度

名前	説明
レベル	選択したレベル番号の新しい優先度を追加するか、デフォルトの優先度レベル(1、2 、3などの数) を使用/編集します。これらの優先度レベルは、[初期アラームの優先度]設定を行うために使用されます。
名前	エンティティの名前を入力します。必要な数だけ作成できます。
サウンド	アラームに関連付けられる音声を選択します。音声の設定で、デフォルトの音声を使用するか、さらに追加します。
音声をリピート	音声を1回だけ再生するか、XProtect Smart Clientでオペレータがアラームリストの中のアラームをクリックするまで繰り返すかを決めます。
デスクトップ通知を有効化	デスクトップ通知はアラームの優先度ごとに有効/無効にできます。Smart Clientプロファイルに対応しているXProtect VMSを使用している場合は、必須Smart Clientプロファイルでも通知を有効にする必要があります。ページ279のアラームマネージャータブ(Smart Clientプロファイル) を参照してください。

ステータス

名前	説明
レベル	デフォルトの状態レベル(番号1、4、9、11、これらは編集または再利用は不可) に加えて、選択したレベル番号の新しい状態を追加します。このような状態レベルは、XProtect Smart Clientのアラームリストにのみ表示されます。

カテゴリ

名前	説明
レベル	選択したレベル番号の新しいカテゴリを追加します。これらのカテゴリレベルは、初期アラームの優先度設定を行うために使用されます。
名前	エンティティの名前を入力します。必要な数だけ作成できます。

アラーム リストの構成タブ

名前	説明
使用できる列	「>」を使用して、XProtect Smart Clientのアラームリストに表示すべき列を選択します。「<」を使用して選択をクリアします。完了したら選択した列には、含める項目が表示されます。

閉じる理由タブ

名前	説明
有効	すべてのアラームが閉じられる前に、閉じる理由を割り当てる必要があるようにするには、選択して有効にします。
理由	アラームを閉じる際にユーザーが選択できる、閉じる理由を追加します。この例は、*解決済み-侵入者*または*偽警告*です。必要な数だけ作成できます。

音声の設定

音の設定を行う際には、以下を指定します。

名前	説明
音声	アラームに関連付けられる音声を選択します。音声リストには、デフォルトのWindows音声が多数含まれています。新しい音声(.wavまたは.mp3)を追加することもできます。
追加	音声を追加します。音声ファイルをブラウズし、1つ以上の.wavまたは.mp3ファイルをアップロードします。
削除	選択された音を、手動で追加された音の一覧から削除します。デフォルト音は削除できません。
テスト	音をテストします。リストから音を選択します。音が1回再生されます。

暗号化を有効にする

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。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。

管理サーバーとの間で暗号化を有効にする

管理サーバーとレコーディングサーバー、またはデータコレクターのある他のリモートサーバー間では双方向接続を暗号化できます(イベントサーバー、ログサーバー、LPRサーバー、モバイルサーバー)。

システムに複数のレコーディングサーバーまたはリモートサーバーが含まれている場合は、これらすべてで暗号化を有効にする必要があります。詳細については、ページ68のサーバーの暗号化を管理(説明付き)を参照してください。

前提条件:

- サーバー認証が管理サーバーをホストしているコンピューターで信頼されている

まず、管理サーバーで暗号化を有効にします。

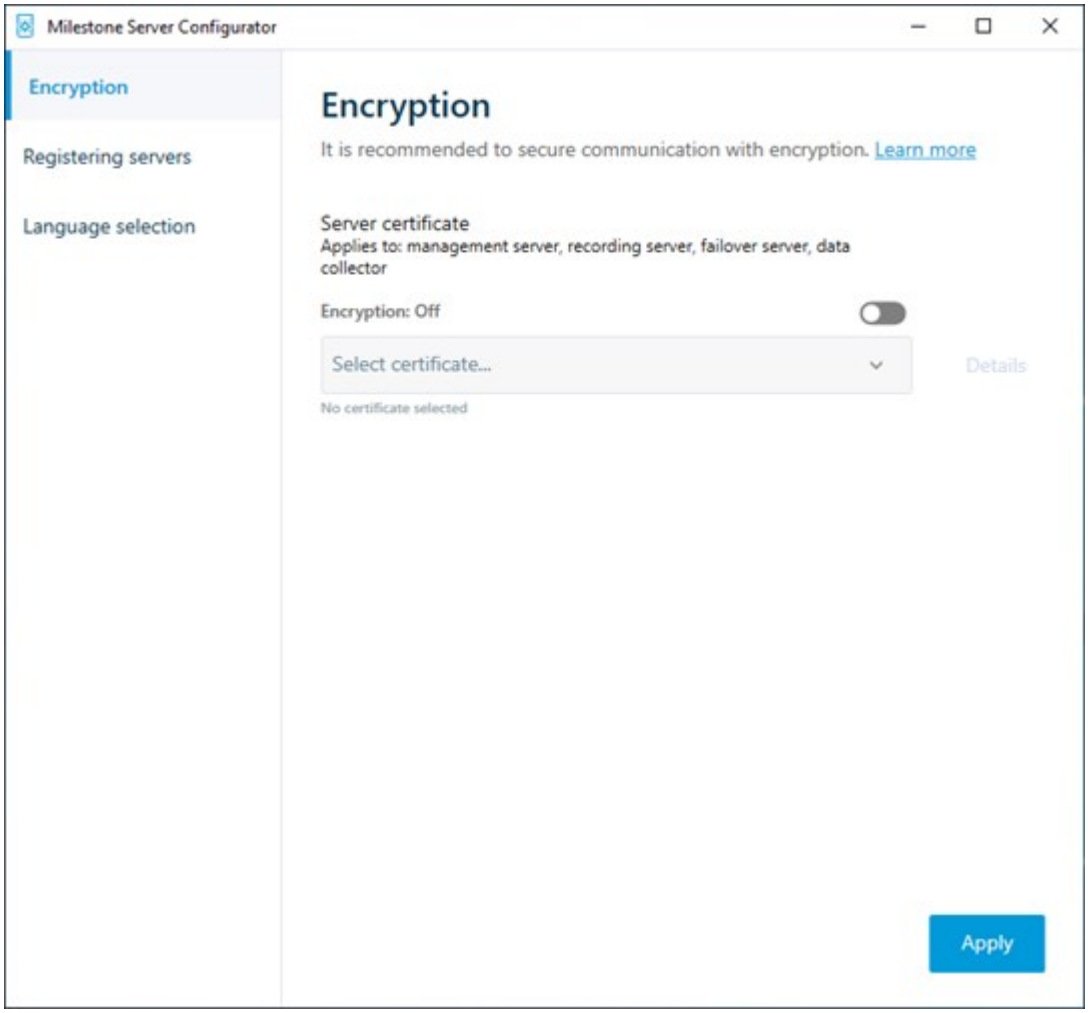
手順:

1. 管理サーバーがインストールされているコンピューターで、以下からServer Configuratorを開きます。
   - Windowsのスタートメニュー

   または

   - コンピューターのタスクバーでManagement Server Managerアイコンを右クリックしたManagement Server Manager
2. Server Configuratorのサーバー証明書で、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、プライベートキーがあり、Windows証明書ストアでローカルコンピューター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. レコーディングサーバー、管理サーバー、フェールオーバーサーバー、データコレクターサーバー間で通信を暗号化するために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。



5. 適用をクリックします。

暗号化の有効にするための次のステップは、各レコーディングサーバーと、データコレクターのある各サーバーで暗号化設定をアップデートすることです(イベントサーバー、ログサーバー、LPRサーバー、モバイルサーバー)。

詳しくは、ページ405のレコーディングサーバーまたはリモートサーバーのサーバー暗号化を有効にするを参照してください。

レコーディングサーバーまたはリモートサーバーのサーバー暗号化を有効にする

管理サーバーとレコーディングサーバー、またはデータコレクターのある他のリモートサーバー間では双方向接続を暗号化できます(イベントサーバー、ログサーバー、LPRサーバー、モバイルサーバー)。

システムに複数のレコーディングサーバーまたはリモートサーバーが含まれている場合は、これらすべてで暗号化を有効にする必要があります。詳細については、ページ69の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) とページ71のマネジメントサーバーとData Collector Server間の暗号化(説明付き)を参照してください。

前提条件:

- 管理サーバーで暗号化を有効にしました。ページ404の暗号化を有効にするを参照してください。

手順:

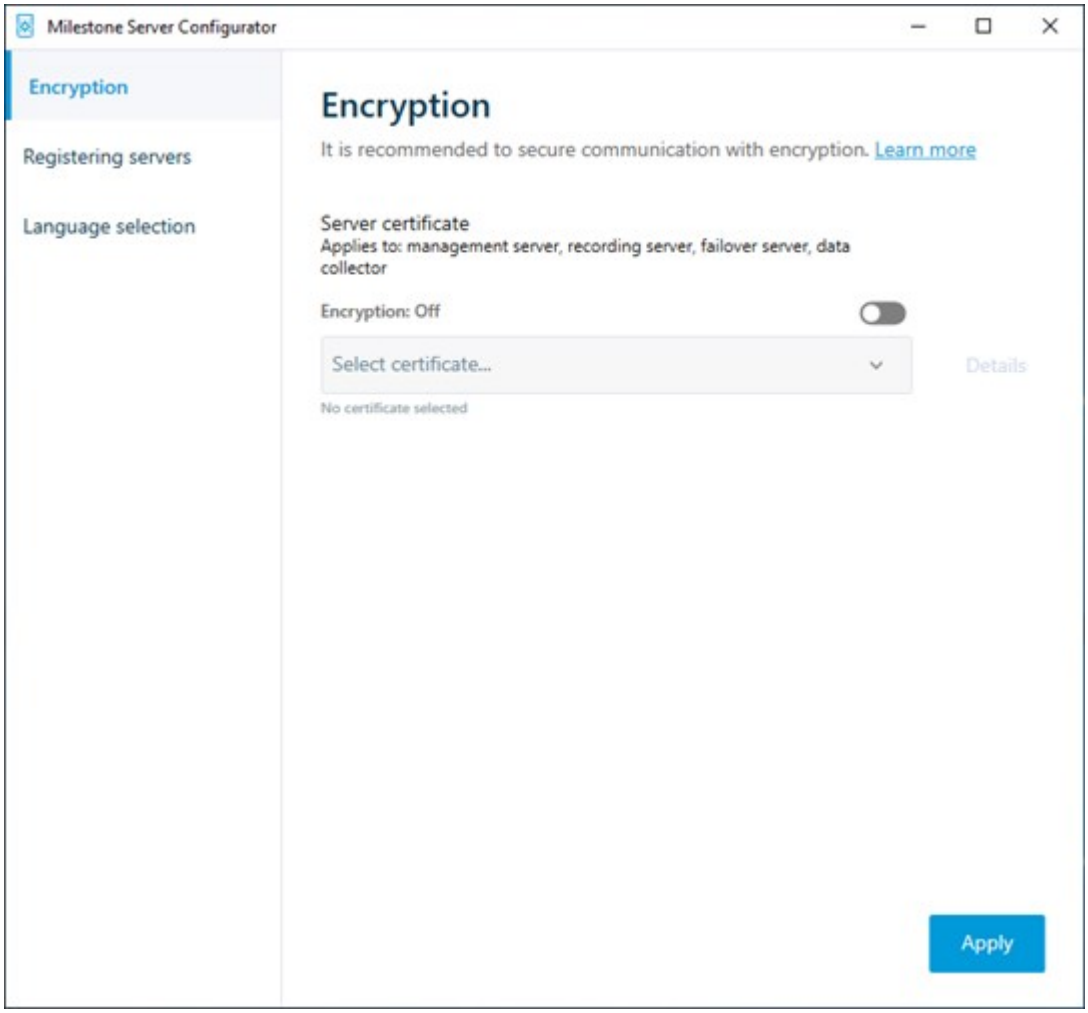
1. レコーディングサーバーがインストールされているコンピューターで、以下からServer Configuratorを開きます。
   - Windowsのスタートメニュー

   または

   - コンピューターのタスクバーでRecording Server Managerアイコンを右クリックしたRecording Server Manager
2. Server Configuratorのサーバー証明書で、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、プライベートキーがあり、Windows証明書ストアでローカルコンピューター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. レコーディングサーバー、管理サーバー、フェールオーバーサーバー、データコレクターサーバー間で通信を暗号化するために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。

レコーディングサーバー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、すべてのクライアントで信頼されている必要があります。



2. 適用をクリックします。

証明書を適用すると、レコーディング サーバーは停止してから再起動します。レコーディングサーバーサービスを停止すると、レコーディング サーバーの基本設定を確認したり、変更したりしている間、ライブ ビデオを表示できなくなります。

クライアントとサーバーに対して暗号化を有効にする

レコーディング サーバーからデータをストリーミングするクライアントおよびサーバーに対するレコーディング サーバーからの接続を暗号化できます。詳細については、ページ72の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)を参照してください。

前提条件:

- 使用されるサーバー認証は、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

コンピューターで信頼されています

- XProtect Smart Clientと、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はすべて、バージョン2019 R1以降でなくてはなりません。
- MIPSDK以前の2019R1バージョンを使用して作られているサードパーティソリューションはアップデートする必要があります。

手順:

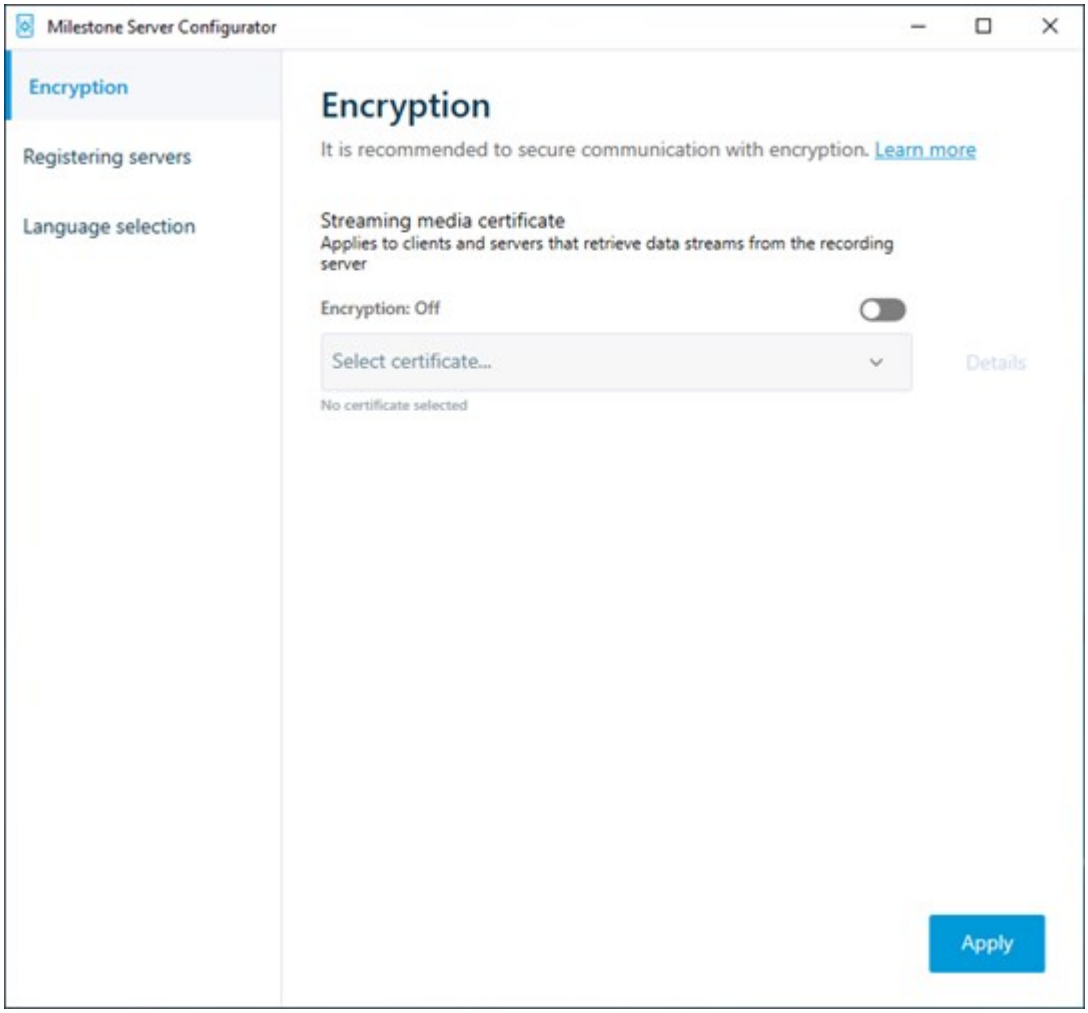
1. レコーディングサーバーがインストールされているコンピューターで、以下からServer Configuratorを開きます。
   - Windowsのスタートメニュー

   または

   - コンピューターのタスクバーでRecording Server Managerアイコンを右クリックしたRecording Server Manager
2. Server Configuratorの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、プライベートキーがあり、Windows証明書ストアでローカルコンピューター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. 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クライアントとサーバー間の通信を暗号化するために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。

レコーディングサーバー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、すべてのクライアントで信頼されている必要があります。



2. 適用をクリックします。

> 証明書を適用すると、レコーディング サーバーは停止してから再起動します。レコーディングサーバーサービスを停止すると、レコーディング サーバーの基本設定を確認したり、変更したりしている間、ライブ ビデオを表示できなくなります。

レコーディング サーバーで暗号化が用いられているかどうか確認する方法については、クライアントへの暗号化ステータスを表示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、「ページ74のレコーディングサーバー データ暗号化(説明付き)」と「ページ75のクライアントに対するモバイルサーバー暗号化の条件」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。

手順:

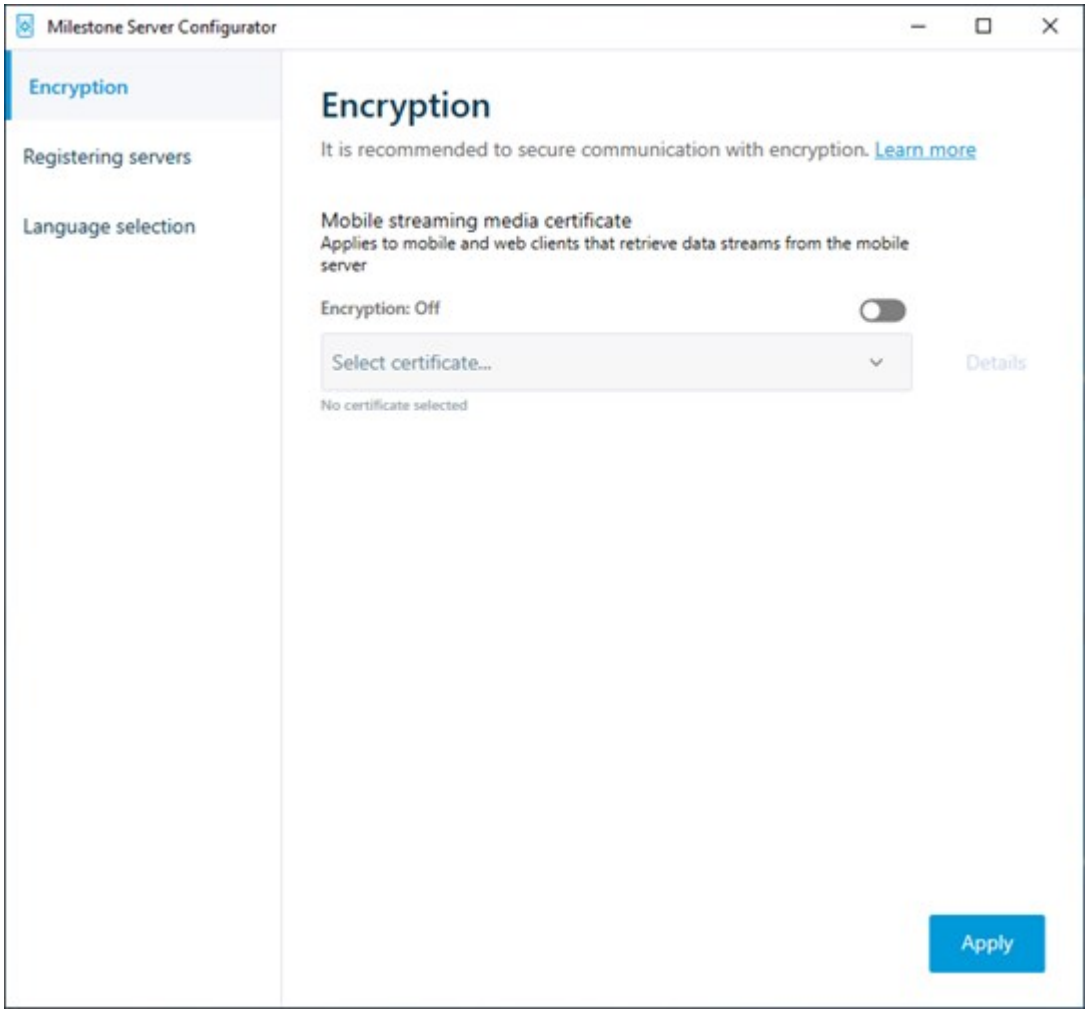
1. モバイル サーバーがインストールされているコンピュータで、以下からServer Configuratorを開きます:
   - Windowsのスタート メニュー

   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. 証明書の選択をクリックすると、秘密キーがあり、Windows証明書ストアでローカル コンピューター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。

モバイルサーバーサービス 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イアントで信頼される必要があります。



2. [適用]をクリックします。

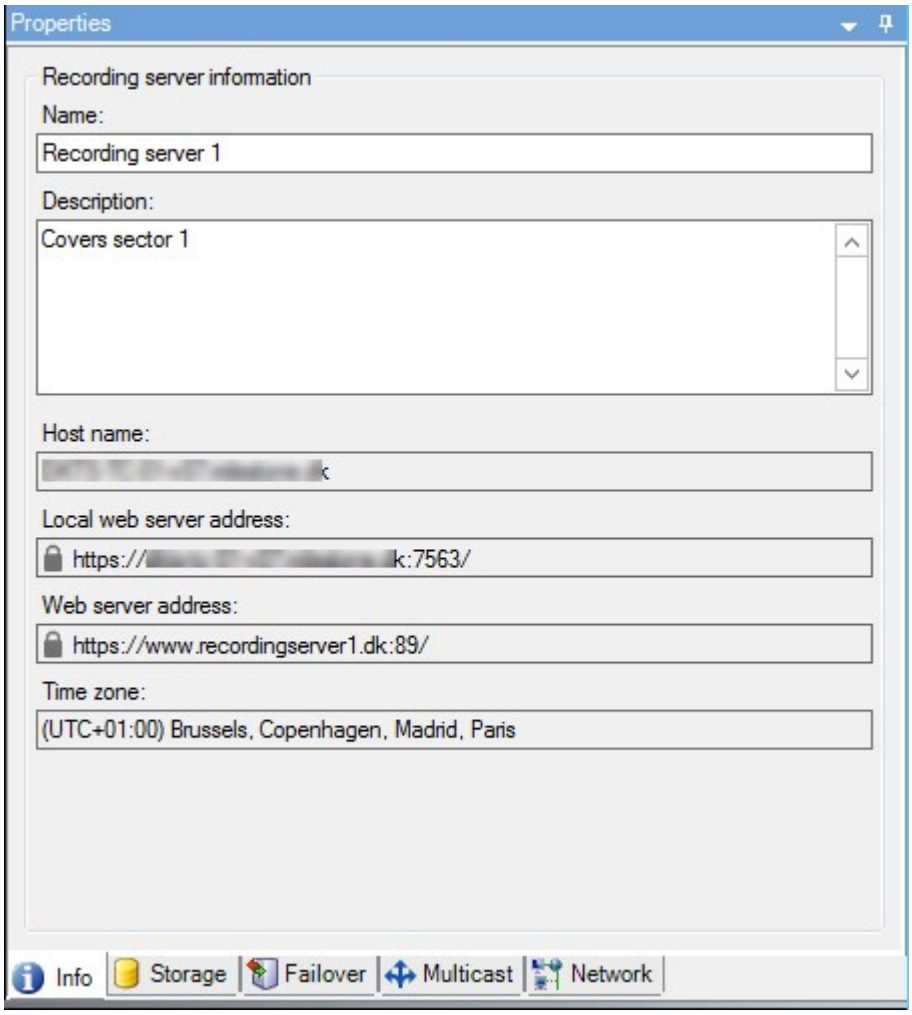
> ⚠ 証明書を適用すると、モバイルサーバーサービスが再起動します。

クライアントへの暗号化ステイタスを見る

レコーディングサーバーが暗号化接続を行なっているかを確認するには:

1. Management Clientを開きます。
2. [サイトナビゲーション]ペインで、[サーバー]>[レコーディングサーバー]を選択します。レコーディングサーバーのリストが表示されます。

3. オーバービューパネル上で、必要なレコーディングサーバーを選択し情報タブへ。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クライアントとサーバーで暗号化が可能ならば、ローカルWebサーバーアドレスとオプショナルWebサーバーアドレスの前にパッドロックアイコンが現れます。



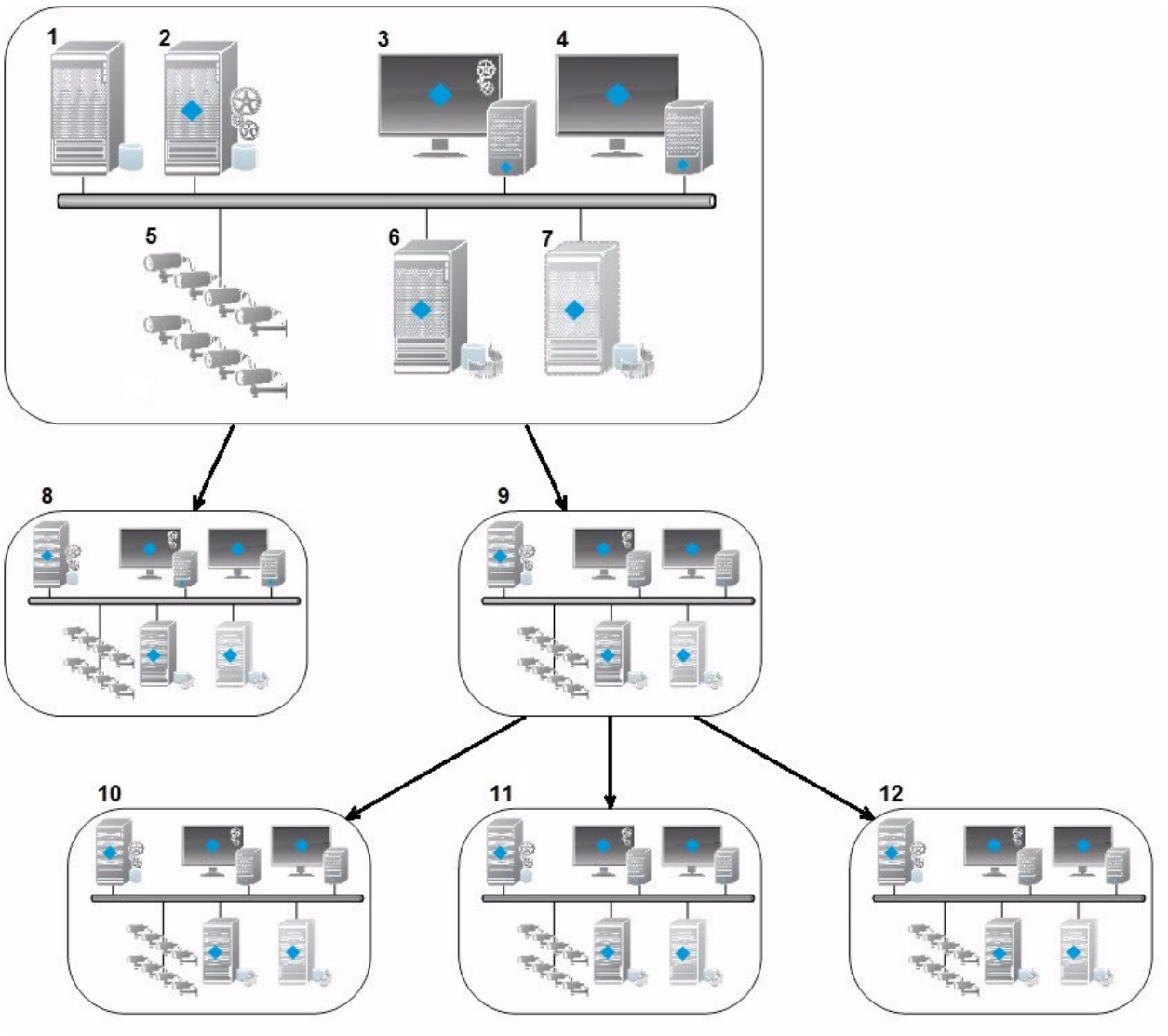
Milestone Federated Architectureの設定

XProtect Expertは子サイトとしてのみフェデレートできます。

Milestone Federated Architectureは、複数の別個の標準システムを親/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。十分な権限を持つクライアントユーザーは、個別のサイト全体にわたり、ビデオ、音声およびその他のリソースへシームレスにアクセスできます。管理者は各サイトの管理者権限に基づき、フェデレートされた階層内で2018 R1以降のバージョンの全てのサイトを中央で管理できます。

基本ユーザーはMilestone Federated Architectureシステムでサポートされていないので、Active Directoryサービスを介してWindowsユーザーとしてユーザーを追加する必要があります。

Milestone Federated Architectureは1つの中央サイト(最上位サイト)と任意の数のフェデレートされたサイトで設定されます(ページ416のフェデレーテッドサイトを実行するためのシステムの設定を参照)。サイトにログインすると、すべての子サイトと子サイトの子サイトの情報にアクセスできます。親サイトからリンクを要求した時点で、2つのサイト間でリンクが確立されます(ページ417のサイトを階層に追加を参照)。子サイトは1つの親サイトとのみリンクできます。フェデレートされたサイト階層に追加する際、子サイトの管理者でない場合は、子サイトの管理者によってリクエストが許可されなくてはなりません。



Milestone Federated Architectureセットアップのコンポーネント:

1. SQL Serverを備えたサーバー
2. マネジメントサーバー
3. Management Client
4. XProtect Smart Client
5. カメラ

6. レコーディングサーバー
7. フェールオーバーレコーディングサーバー
8. ～12。フェデレーテッドサイト

階層の同期化

親サイトには、現在接続されている子サイト、子サイトの子サイトなど、全てに関する更新されたリストがあります。フェデレーテッドサイト階層には、サイト間でスケジュールされている同期化のほか、サイトが追加または削除されるたびに管理によりトリガーされる同期化が含まれています。システムが階層を同期化する場合、レベルごとに実施し、情報を要求しているサーバーに到達するまで各レベルが通信を転送し、応答します。システムは、毎回1MB未満を送信します。レベルの数によって、階層への変更がManagement Clientで表示されるまでに時間がかかることがあります。独自の同期化をスケジュールすることはできません。

データトラフィック

ユーザーや管理者がライブビデオまたは録画ビデオを表示したり、サイトを設定したりすると、システムは通信または設定データを送信します。データの量は、何がどの程度表示または設定されたかによって異なります。

他の製品を伴うMilestone Federated Architecture

- 中央サイトがXProtect Smart Wallを使用している場合、フェデレーテッドサイト階層のXProtect Smart Wall機能も使用できます。XProtect Smart Wallの設定については、ページ263のSmart Wallの構成を参照してください
- 中央サイトでXProtectAccessが使用されている状態で、XProtectSmartClientユーザーがフェデレーテッドサイト階層にログインする場合、XProtectSmartClientにはフェデレーテッドサイトからのアクセスリクエスト通知も表示されます。
- XProtect Expert 2013システムまたはそれ以降を、親サイトとしてではなく、子サイトとしてフェデレーテッドサイト階層に追加できます。
- Milestone Federated Architectureは追加ライセンスを必要としません。
- ユースケースと利点の詳細については、Milestone Federated Architectureに関する白書を参照してください。

フェデレーテッドサイト階層の確立

Management Clientは、Milestoneで階層を作成する前に、サイトを相互にリンクする方法を計画することをお勧めします。

各サイトを、フェデレーテッド階層で、標準のシステムコンポーネント、設定、ルール、スケジュール、管理者、ユーザー、およびユーザー権限がある通常のスタンドアロンシステムとして設定します。既にサイトがインストールおよび構成されており、必要な作業はフェデレーテッドサイト階層で結合することだけである場合は、システムを設定できます。

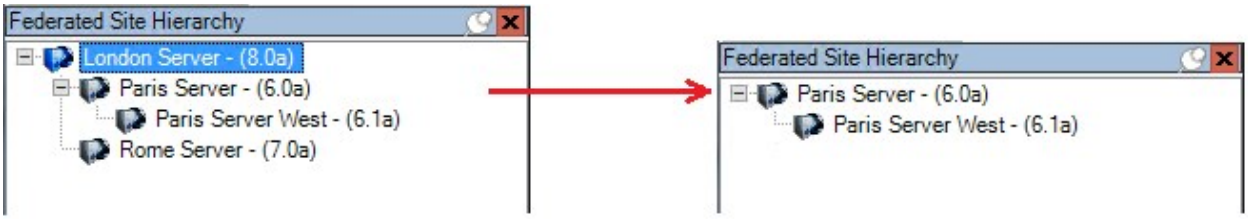
個々のサイトがインストールされた後、これらがフェデレーテッドサイトとして実行されるよう設定する必要があります(ページ416のフェデレーテッドサイトを実行するためのシステムの設定を参照) 。

階層を開始するには、中央サイトとして作業を行いたいサイトにログインし、最初のフェデレーテッドサイトを追加します(ページ417のサイトを階層に追加を参照) 。フェデレーション・サイト階層にリンクが確立されると、2つ階層を展開するための複数のサイトを追加できるManagement Clientウィンドウでフェデレーション・サイト階層を自動的に作成します。

フェデレーテッドサイト階層が作成された後、ユーザーと管理者はサイトにログインし、そのサイトと関連付けられた任意のフェデレーテッドサイトにアクセスできます。フェデレーテッドサイトへのアクセスは、ユーザー権限によって異なります。

フェデレーテッド階層に追加できるサイトの数は無制限です。また、古い製品バージョンのサイトを新しいバージョンのサイトにリンクできます。逆も可能です。バージョン番号は自動的に表示され、削除できません。ログインしたサイトは常にフェデレーテッドサイト階層ペインの最上部に表示され、ホームサイトと呼ばれます。

以下が、Management Clientのフェデレーテッドサイトの例です。左では、ユーザーがトップサイトにログインしています。右では、ユーザーが子サイトの一つ、Paris Server、つまりホームサイトにログインしています。



Milestone Federated Architectureのステータスアイコン

アイコンはサイトの状態を表します。

説明	アイコン
階層全体での最上位サイトが動作中。	
階層全体での最上位サイトはまだ動作中ですが、1つまたは複数の問題に注意が必要です。最上位サイトのアイコン上に表示されます。	
サイトが動作中。	
サイトは、階層での許可待ち中です。	
サイトは接続していますが、まだ動作していません。	

フェデレーテッドサイトを実行するためのシステムの設定

Milestone Federated Architectureの動作のためにシステムを準備するには、マネジメントサーバーのインストール時に一定の選択が必要です。ITインフラストラクチャの設定によって、3つの異なる代替方法のいずれかを選択します。

代替方法1：同じドメインからサイトに接続する(共通ドメインユーザーを使用)

マネジメントサーバーのインストール前に、共通ドメインユーザーを作成し、フェデレーテッドサイト階層に関与するすべてのサーバー上の管理者としてこのユーザーを設定する必要があります。サイトにどのように接続するかは、作成されたユーザーアカウントに応じて異なります。

Windowsユーザーアカウントを使用

1. マネジメントサーバーとして使用されるサーバーに製品をインストールし、カスタムを選択します。
2. ユーザーアカウントを使用して、マネジメントサーバーのインストールを選択します。選択したユーザーアカウントは、すべてのマネジメントサーバーで使用される管理者アカウントである必要があります。フェデレーテッドサイト階層で他のマネジメントサーバーをインストールする場合は、同じユーザーアカウントを使用する必要があります。
3. インストールを終了します。手順1～3を繰り返し、フェデレーテッドサイト階層に追加する他のシステムをインストールします。
4. 階層にサイトを追加します(ページ417のサイトを階層に追加を参照)。

Windows組み込みユーザーアカウントを使用(ネットワークサービス)

1. マネジメントサーバーとして使用される最初のサーバーに製品をインストールし、単一のコンピュータまたはカスタムを選択します。これにより、ネットワークサービスアカウントを使用して、マネジメントサーバーがインストールされます。このステップを、フェデレーテッドサイト階層のすべてのサイトについて繰り返します。
2. フェデレーテッドサイト階層の中央サイトにするサイトにログインします。
3. Management Clientで、セキュリティ> 役割 > 管理者を展開します。
4. ユーザーとグループタブで追加をクリックして、Windowsユーザーを選択します。
5. ダイアログボックスで、オブジェクトタイプとしてコンピュータを選択し、フェデレーテッドサイトのサーバー名を入力してOKをクリックし、中央サイトの管理者の役割にサーバーを追加します。この方法ですべてのフェデレーテッドサイトのコンピュータを追加するまでこの手順を繰り返し、アプリケーションを終了します。
6. 各フェデレーテッドサイトにログインし、同じ方法で次のサーバーを管理者の役割に追加します。
   - 親サイトサーバー。
   - このフェデレーテッドサイトに直接接続する子サイトサーバー。
7. 階層にサイトを追加します(ページ417のサイトを階層に追加を参照)。

代替方法2：異なるドメインからのサイトの接続

ドメインを超えてサイトに接続するには、これらのドメインが互いに信頼関係にあることを確認します。Microsoft Windowsドメイン構成で相互に信頼するようにドメインを設定します。フェデレーテッドサイト階層で各サイトの異なるドメイン間に信頼関係を確立した場合は、代替方法1と同じ説明に従ってください。信頼されるドメインの設定方法の詳細については、Microsoft Web サイト(https://docs.microsoft.com/previous- versions/windows/it- pro/windows- 2000- server/cc961481(v=technet.10)/)を参照してください。

Milestoneは、Milestone Interconnectを使用して、接続されたマルチサイトシステムと複数のドメインを作成することを推奨しています。

代替方法3: ワークグループでのサイトの接続

ワークグループ内でサイトを接続する場合、フェデレーテッドサイト階層で接続されるすべてのサーバーに同じ管理者アカウントが存在する必要があります。システムをインストールする前に管理者アカウントを定義する必要があります。

1. 共通管理者アカウントを使用して、Windowsへログインします。
2. 製品のインストールを開始し、カスタムをクリックします。
3. 共通システム管理者アカウントを使用して、マネジメントサーバーをインストールするように選択します。
4. インストールを終了します。手順1～4を繰り返し、接続する他のすべてのシステムをインストールします。これらすべてのシステムで、共通の管理者アカウントをインストールする必要があります。
5. 階層にサイトを追加します(ページ417のサイトを階層に追加を参照)。

Milestoneは、サイトがドメインの一部でない場合、Milestone Interconnectを使用して接続されたマルチサイトシステムを作成することを推奨しています。

ドメインとワークグループを混在させることはできません。これは、ドメインからワークグループのサイトへ、あるいはその逆に接続することはできないことを意味します。

サイトを階層に追加

システムを展開する際に、システムが正しく設定されているなら、最上位サイトとその子サイトの両方に追加できます。

1. フェデレーテッドサイト階層ペインを選択します。
2. 子サイトを追加するサイトを選択し、右クリックしてサイトを階層に追加をクリックします。
3. 要求された子のURLをサイトを階層に追加ウィンドウに入力し、OKをクリックします。
4. 親サイトがリンクリクエストを子サイトへ送信し、しばらくすると2つのサイトの間のリンクがフェデレーテッドサイト階層ペインに追加されます。
5. 子サイトの管理者による許可をリクエストすることなく新しい子サイトへのリンクを確立できる場合は、手順7に進みます。

   それ以外の場合は、子サイトの管理者がリクエストを許可するまで子サイトには許可の待機アイコンが表示されます。

6. 子サイトのシステム管理者が親サイトのからのリンク要求を承認していることを確認します(ページ418の階層に含むことを許可を参照) 。

7. 新しい親/子リンクが確立され、フェデレーテッドサイトの階層ペインが新しい子のアイコンで更新されます。

階層に含むことを許可

子サイトが、子サイトへの管理者権限を持っていない親サイトになる可能性があるサイトからリンク要求を受信すると、許可の待機 アイコンが表示されます。

リンク要求を許可するには:

1. サイトにログインします。

2. フェデレーテッドサイト階層ペインで、サイトを右クリックし、階層に含むことを許可を選択します。

   サイトでXProtect Expertバージョンが実行されている場合は、サイトナビゲーションペインでサイトを右クリックします。

3. はいをクリックします。

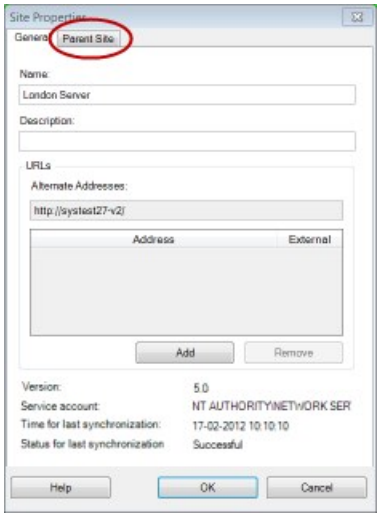
4. 新しい親/子リンクが確立され、フェデレーテッドサイト階層ペインが、選択されたサイトの標準サイトアイコンで更新されます。

> 親サイトから離れている子への変更はすべて、フェデレーテッドサイト階層ペインに反映されるまで時間がかかる場合があります。

サイトプロパティの設定

ホームサイトとその子サイトのプロパティを表示し、編集することがおそらく可能です。

1. Management Clientでは、フェデレーテッドサイト階層ペイン内で、該当するサイトを選択し、右クリックして、プロパティを選択します。



2. 必要であれば、以下を変更します。

   一般タブ(ページ420の一般タブを参照)

   親サイトタブ(ページ421の親サイトタブを参照)(子サイトでのみ利用可能)

> 同期化の問題のため、リモートの子に対して行われた変更がサイトナビゲーションペインに反映されるまで多少時間がかかる場合があります。

サイト階層の更新

システムは、すべてのレベルの親/子設定を通じて、定期的に階層の自動同期化を実行します。反映される変更をすぐに階層で確認したくて、次回の自動同期化まで待ちたくない場合は、手動で更新することができます。

手動での更新を実行するために、サイトにログインする必要はありません。前回の同期化以降にこのサイトによって保存されている変更だけが、更新で反映されます。これは、階層の下の方で行われた変更は、変更がまだサイトに到達していない場合、手動更新では反映されないことを意味しています。

1. 関連するサイトにログインします。
2. フェデレーテッドサイト階層ペインでトップのサイトを右クリックし、サイト階層の更新をクリックします。

   これには、数秒かかります。

階層の他のサイトへのログイン

他のサイトにログインし、これらのサイトを管理できます。ログインしたサイトがホームサイトです。

1. フェデレーテッドサイト階層ペインで、ログインするサイトを右クリックします。
2. サイトにログインをクリックします。

   そのサイトのManagement Clientが表示されます。
3. ログイン情報を入力して、**OK**をクリックします。
4. ログイン後、そのサイトの管理タスクを実行できます。

階層からのサイトの分離

親サイトからサイトを分離すると、サイト間でのリンクは外れます。中央サイト、サイト自体、または親サイトからサイトを分離できます。

1. フェデレーテッドサイト階層ペインで、サイトを右クリックし、階層からサイトを分離を選択します。
2. はいをクリックしてフェデレーテッドサイト階層ペインを更新します。

   分離するサイトに子サイトがある場合、階層のこのブランチの新しいトップサイトになり、通常のサイトのアイコンがトップサイトのアイコンに変わります。
3. **OK** をクリックします。

階層への変更は、手動更新または自動同期化後に反映されます。

フェデレーテッドサイトのプロパティ

このセクションでは一般 タブとペアレントサイトタブについて説明します

一般タブ

現在ログインしているサイトに関連する情報の一部を変更することができます。

名前	説明
名前	サイトの名前を入力します。
説明	サイトの説明を入力します。
URL	リストを使用してこのサイトのURLを追加および削除し、URLが外部URLかどうかを示します。外部アドレスが、ローカルネットワークの外部から到達可能である。
バージョン	サイトのマネジメントサーバーのバージョン番号。

名前	説明
サービスアカウント	マネジメントサーバーが実行されているサービスアカウント。
最後に同期化した時間	階層の最後の同期化の時刻と日付。
最後の同期時のステータス	階層の最後の同期化のステータス。これは、成功または失敗のいずれかです。

親サイトタブ

このタブは、現在ログインしているサイトの親のサイトに関する情報を表示します。サイトに親サイトがなければ、タブは表示されません。

名前	説明
名前	親サイトの名前を入力します。
説明	親サイトの説明を表示します(オプション) 。
URL	親サイトのURLを一覧表示し、URLが外部URLであるかどうかを示します。外部アドレスが、ローカルネットワークの外部から到達可能である。
バージョン	サイトのマネジメントサーバーのバージョン番号。
サービスアカウント	マネジメントサーバーが実行されているサービスアカウント。
最後に同期化した時間	階層の最後の同期化の時刻と日付。
最後の同期時のステータス	階層の最後の同期化のステータス。これは、成功または失敗のいずれかです。

Milestone Interconnectの設定

このセクションではMilestone Interconnectと機能の設定方法について説明します。

Milestone InterconnectまたはMilestone Federated Architectureの選択(説明付き)

中央サイトのユーザーがリモートサイトのビデオにアクセスする必要がある、物理的に分散化されたシステムでは、Milestone Interconnect™またはMilestone Federated Architecture™を選択することができます。

Milestoneでは、以下の場合にMilestone Federated Architectureを推奨しています。

- 中央サイトとフェデレーテッドサイトの間でのネットワーク接続が安定している。
- ネットワークが同一ドメインを使用している。
- 大きなサイトが少数ある。
- 帯域は、必要要件に対して十分である。

Milestoneでは、以下の場合にMilestone Interconnectを推奨しています。

- 中央サイトとリモートサイトのネットワーク接続が不安定。
- 自分または組織が、リモートサイトで別のXProtect製品を使用することを希望している。
- ネットワークが異なるドメインまたはワークグループを使用している。
- 小さいサイトが多数ある。

Milestone Interconnectおよびラインセンス

Milestone Interconnectを実行するには、中央サイトに、リモートサイトのハードウェアデバイスから動画を表示するためのMilestone Interconnectカメラライセンスが必要です。XProtect Corporateのみが中央サイトとして動作できます。

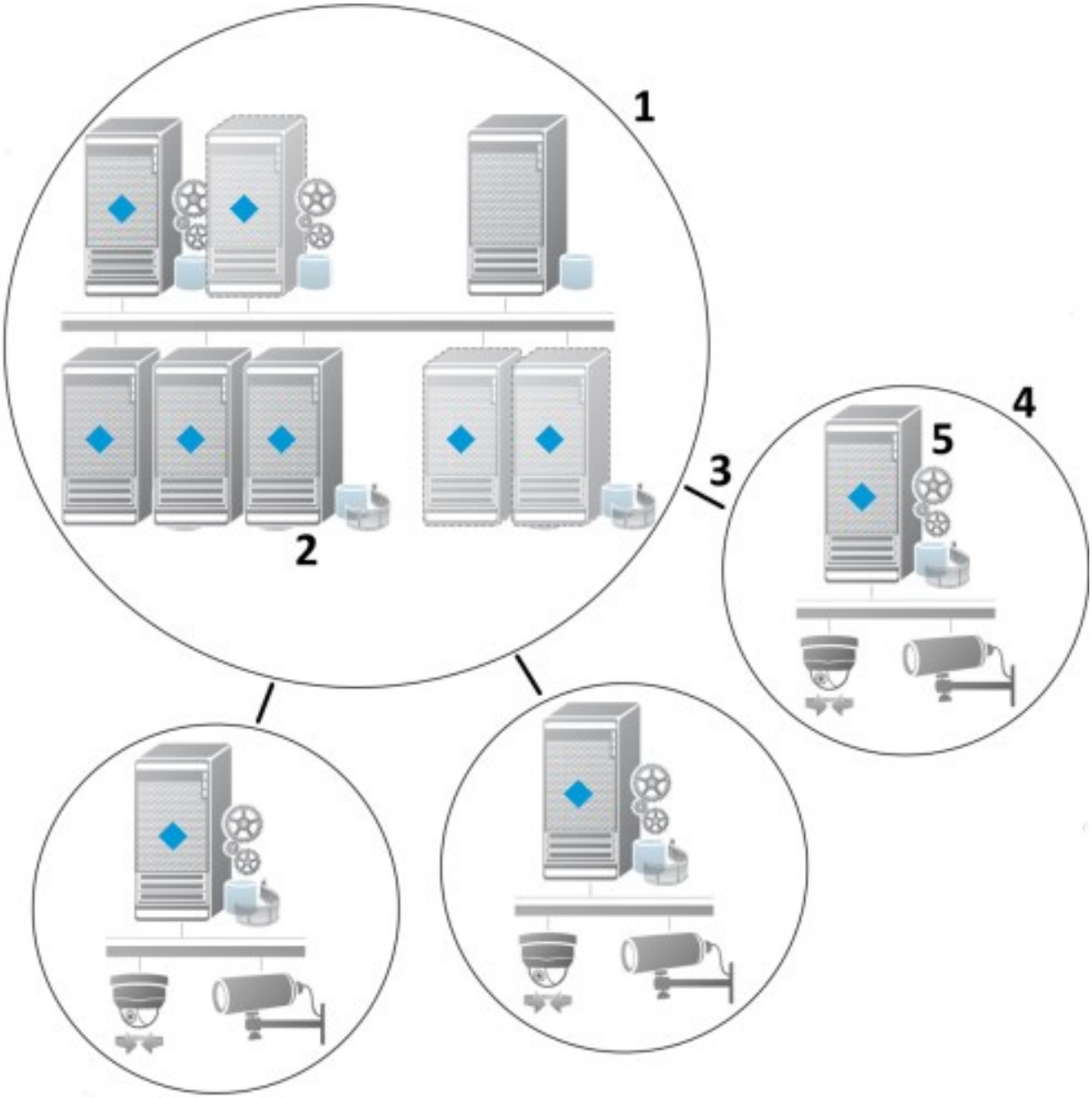
Milestone Interconnectカメラライセンスのステータスは、中央サイトのライセンス情報ページに一覧表示されます。

Milestone Interconnect(説明付き)

> 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。

Milestone Interconnect™では、物理的に断片化された、より少ない数を統合し、1つのXProtect Corporate中央サイトでXProtectをリモートインストールできます。リモートサイトと呼ばれるこれらの小さいサイトは船舶、バス、電車などのモバイルユニットにインストールできます。つまり、このようなサイトは恒久的にネットワークに接続する必要がありません。

次の図は、システムに設定する方法Milestone Interconnectを示します。



1. Milestone Interconnect中央XProtect Corporateサイト
2. MilestoneInterconnectドライバー(中央サイトのレコーディングサーバーとリモートサイト間の接続を処理します。ハードウェアの追加ウィザードを使ってリモートシステムを追加する場合は、ドライバーのリストから選択する必要があります。)
3. Milestone Interconnectの接続
4. Milestone Interconnectリモートサイト(システムのインストールによる完全なリモートサイト、ユーザー、カメラなど)
5. Milestone Interconnectリモートシステム(リモートサイトでの実際の技術的なインストール)

中央サイトからハードウェアの追加ウィザードを使用して中央サイトにリモートサイトを追加します(ページ425のリモートサイトを中央Milestone Interconnectサイトに追加を参照) 。

各リモートサイトは独立して実行され、通常の監視タスクを実行することが可能です。ネットワーク接続および適切なユーザー権限(ページ426のユーザー権限の割り当てを参照) に応じて、Milestone Interconnectではリモートサイトカメラのライブビューの指示、および中央サイト上のリモートサイト録画の再生を提供します。

中央サイトは、指定されたユーザー・アカウント(リモートサイトを追加したとき) がアクセス権を持つデバイスを表示し、アクセスすることのみ可能です。これにより、ローカルシステム管理者は、中央サイトとそのユーザーが使用できるデバイスを制御できます。

中央サイトでは相互接続されたカメラ用システムのステータスを表示できますが、リモートサイトのステータスを直接表示することはできません。その代わりに、リモートサイトをモニターするため、中央サイトでアラームまたは他の通知をトリガーするリモートサイトのイベントを使用できます(ページ428のリモートサイトからのイベントに応答するように中央サイトを構成するを参照) 。

XProtect Smart Clientユーザーによるイベント、ルール/スケジュール、または手動の要求のいずれかに基づいて、リモートサイトの録画を中央サイトに転送することが可能です。

XProtectCorporateシステムだけが、中央サイトとして動作できます。XProtectCorporateを含む他のすべての製品は、リモートサイトとして動作できます。中央サイトがリモートサイトで発生したデバイスやイベントを処理できるかどうかや、処理できる場合には、その方法、どのバージョン、何台のカメラを処理できるかは設定によって異なります。特定のXProtect製品をMilestone Interconnect設定で連携する方法の詳細については、Milestone InterconnectのWebサイト(https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/) を参照してください。

Milestone Interconnectの設定(説明付き)

Milestone Interconnectを実行する方法は3つあります。設定の実行方法は、ネットワーク接続、録画の再生方法、リモート録画を取得するかどうか、またどの程度取得するかによって異なります。

以下では、最も一般的な3つの設定ついて説明しています。

リモートサイトから直接再生(安定したネットワーク接続)

最も単純な設定です。中央サイトは常にオンラインでリモートサイトに接続し、中央サイトのユーザーはリモートサイトから直接録画を再生します。このためにはリモートシステムから録画を再生オプションを使用する必要があります(ページ427のリモートサイトのカメラからの直接再生を可能にするを参照)。

ルールまたはXProtect Smart Clientに基づく、リモートサイトからの選択したリモート録画シーケンスの取得(一時的に制限されたネットワーク接続)

選択した録画シーケンス(リモートサイトから開始) を、リモートサイトからの独立を保証するために中央に保存する必要があるときに使用します。ネットワーク障害やネットワークが制限された場合に、独立性は非常に重要になります。リモート録画の取得設定は、リモート取得タブで構成します(ページ198のリモート取得タブを参照) 。

必要に応じて、またはルールを設定できる場合にXProtect Smart Clientからリモート録画の取得を開始できます。シナリオによっては、リモートサイトをオンラインにしておいたり、あるいはほとんどの時間オフラインにすることができます。これは多くの場合、業界によって異なります。中央サイトがリモートサイトと恒久的に接続されていることが一般的な業界もあります(小売業の本社(中央サイト)と多数の店舗(リモートサイト)など)。また、運輸業など、リモートサイトがモバイル(バス、電車、船舶など)であり、断続的にしかネットワークに接続できない業界もあります。リモート録画取得中にネットワーク接続で障害が発生した場合、ジョブは次の機会に続行されます。

自動取得またはXProtect Smart Clientからの取得リクエストをリモート取得タブで指定されているタイムインターバル外に検出した場合、リクエストは受け付けられますが、選択されたタイムインターバルに達するまでは開始されません。新しい録画取得ジョブはキューに入れられ、許容されるタイムインターバルに達したときに開始されます。保留中のリモート録画取得ジョブは、システムダッシュボード>現在のタスクから確認できます。

接続エラーの後、取得できなかったリモート録画はデフォルトでリモートサイトから取得されます。

レコーティングサーバーなどのリモートサイトは、カメラのエッジストレージを使用します。通常、リモートサイトは中央サイトとオンラインで接続されており、中央サイトにより録画されるようライブストリームをフィードしています。何らかの原因でネットワークが切断されると、中央サイトは録画シーケンスを失います。ただし、ネットワークが復旧すると、中央サイトは、ダウン期間中のリモート録画を自動的に取得します。これを行うには、カメラの録画タブで接続の復旧時に自動的にリモート録画を取得するオプションを選択する必要があります(ページ427のリモートサイトのカメラからリモート録画を取得するを参照)。

お客様の組織のニーズに合わせて上記の方法を組み合わせることができます。

リモートサイトを中央Milestone Interconnectサイトに追加

ハードウェアの追加ウィザードを使用して、リモートサイトを中央サイトに追加します。
要件

- 十分な数のMilestone Interconnectカメラライセンス(ページ422のMilestone Interconnectおよびラインセンスを参照)
- 中央XProtectCorporateシステムがアクセスできるデバイスの権限がある、ユーザーアカウント(基本ユーザー、ローカルWindowsユーザー、またはWindows Active Directoryユーザー)を含む別の設定済みあるいは運転中のXProtectシステム
- リモートサイトで使用されるポートへのアクセスまたはポート転送による、中央XProtect Corporateサイトとリモートサイト間のネットワーク接続

リモートサイトを追加するには:

1. 中央サイトで、サーバーを展開し、レコーディングサーバーを選択します。
2. 概要ペインで、該当するレコーディングサーバーを展開して右クリックします。
3. ハードウェアの追加を選択して、ウィザードを開始します。
4. 最初のページで、アドレス範囲のスキャンまたは手動を選択して、次へをクリックします。

5. ユーザー名とパスワードを指定します。ユーザーアカウントはリモートシステムで定義されている必要があります。追加をクリックして、必要なだけユーザー名とパスワードを追加できます。準備ができたら、次へをクリックします。
6. スキャンに使用するドライバを選択します。この場合、Milestoneドライバ間で選択します。次へ をクリックします。
7. スキャンするIPアドレスとポート番号を指定します。デフォルトはポート80です。次へをクリックします。

   システムがリモートサイトを検出している間、お待ちください。ステータスインジケータに、検出プロセスが表示されます。正常に検出された場合は、成功メッセージがステータス列に表示されます。追加できなかった場合は、失敗エラーメッセージをクリックすると、その理由を確認できます。
8. 選択すると、正常に検出されたシステムを有効または無効にします。次へ をクリックします。
9. システムがハードウェアを検出し、デバイス固有の情報を収集している間、お待ちください。次へ をクリックします。
10. 検出が成功したハードウェアおよびデバイスを有効にするか、無効にするかを選択します。次へ をクリックします。
11. デフォルトグループを選択します。終了 をクリックします。
12. インストール後、概要ペインにシステムとデバイスが表示されます。

    リモートサイト上で選択されたユーザーのユーザー権限に従って、中央サイトはすべてのカメラおよび機能、またはその一部にアクセスできます。

ユーザー権限の割り当て

役割を作成して機能へのアクセスを割り当てることで、相互接続されているカメラに対し、他のカメラと同様にユーザー権限を設定できます。

1. 中央サイトのサイトナビゲーションペインで、セキュリティを展開して役割を選択します。
2. 概要ペインで組み込み管理者の役割を右クリックし、役割の追加を選択します(ページ338の役割の追加および管理を参照)。
3. 役割に名前を付け、デバイスタブの設定(ページ341の役割の設定を参照)と、リモート録画タブの設定(ページ341の役割の設定を参照)を行います。

リモートサイトのハードウェアの更新

カメラやイベントの追加や削除など、リモートサイトで構成が変更された場合は、中央サイトで構成を更新し、リモートサイトで新しい構成を反映する必要があります。

1. 中央サイトで、サーバーを展開し、レコーディングサーバーを選択します。
2. 概要ペインで、必要なレコーディングサーバーを展開して、該当するリモートシステムを選択します。右クリックします。
3. ハードウェアの更新を選択します。これにより、ハードウェアの更新ダイアログボックスが開きます。
4. このダイアログボックスには、Milestone Interconnect設定が最後に確立または更新されてから、リモートシステムで行われたすべての変更(デバイスの削除、更新、および追加)のリストが表示されます。確認をクリックして、中央サイトにこれらの変更を更新します。

リモートシステムにリモートデスクトップを接続

Milestone Interconnect設定でリモートからシステムに接続できます。

要件

リモート接続するコンピュータへのリモートデスクトップ接続が起動し、実行中である必要があります。

1. 中央サイトで、サーバーを展開し、レコーディングサーバーを選択します。
2. 概要ペインで、必要なレコーディングサーバーを展開して、該当するリモートシステムを選択します。
3. プロパティペインで、情報タブを選択します。
4. リモート管理エリアで、適切なWindowsユーザー名とパスワードを入力します。
5. ユーザー名とパスワードが保存されると、接続をクリックしてリモートデスクトップ接続を確立します。
6. ツールバーで保存をクリックします。

リモートサイトのカメラからの直接再生を可能にする

中央サイトがリモートサイトと常に接続している場合は、システムを構成し、ユーザーがリモートサイトから直接録画を再生できるようにすることができます。詳細については、ページ424のMilestone Interconnectの設定(説明付き)を参照してください。

1. 中央サイトで、サーバーを展開し、レコーディングサーバーを選択します。
2. 概要ペインで、必要なレコーディングサーバーを展開して、該当するリモートシステムを選択します。関連する相互接続されたカメラを選択します。
3. プロパティペインで、記録タブを選択し、リモートシステムから録画を再生オプションを選択します。
4. ツールバーで保存をクリックします。

Milestone Interconnect設定では、中央サイトは、リモートサイトで定義されたプライバシーマスクを無視します。同じプライバシーマスクを適用する場合は、中央サイトでもう一度定義します。

リモートサイトのカメラからリモート録画を取得する

中央サイトが常にリモートサイトと接続していない場合は、リモート録画を中央で保存するように構成し、ネットワーク接続が最適なときにリモート録画を取得するように構成できます。詳細については、ページ424のMilestone Interconnectの設定(説明付き)を参照してください。

ユーザーが実際に録画を取得できるようにするには、関連する役割でこの許可を有効にする必要があります(ページ341の役割の設定を参照)。

システムを構成するには:

1. 中央サイトで、サーバーを展開し、レコーディングサーバーを選択します。
2. 概要ペインで、必要なレコーディングサーバーを展開して、該当するリモートシステムを選択します。関連するリモートサーバーを選択します。

3. プロパティペインでリモート取得タブを選択し、設定を更新します(ページ198のリモート取得タブを参照) 。

何らかの原因でネットワークが切断されると、中央サイトは録画シーケンスを失います。ネットワークが再確立された時点で、中央サイトで自動的にリモート録画を取得し、停止した期間をカバーするようにシステムを構成できます。

1. 中央サイトで、サーバーを展開し、レコーディングサーバーを選択します。
2. 概要ペインで、必要なレコーディングサーバーを展開して、該当するリモートシステムを選択します。関連するカメラを選択します。
3. プロパティペインで、録画タブを選択し、接続の復旧時に自動的にリモート録画を取得するオプションを選択します(ページ220のプリバッファをサポートするデバイスを参照) 。
4. ツールバーで保存をクリックします。

または、ルールを使用するか、必要な場合はXProtect Smart Client からリモート録画の取得を開始します。

Milestone Interconnect設定では、中央サイトは、リモートサイトで定義されたプライバシーマスクを無視します。同じプライバシーマスクを適用する場合は、中央サイトでもう一度定義します。

リモートサイトからのイベントに応答するように中央サイトを構成する

リモートサイトで定義されたイベントを使用して、中央サイトでルールとアラームをトリガーし、リモートサイトのイベントに即時応答できます。これには、リモートサイトが接続され、オンラインであることが必要です。イベント数とタイプは、リモートシステムで設定および事前定義されたイベントによって異なります。

サポートされているイベントの一覧は、Milestone Webサイト(https://www.milestonesys.com/) を参照してください。

事前定義されたイベントは削除できません。

要件:

- トリガーイベントとしてリモートサイトからユーザー定義または手動イベントを使用する場合は、まずリモートサイトでこれらを作成する必要があります。
- リモートサイトからのイベントのリストが更新されていることを確認してください(ページ426のリモートサイトのハードウェアの更新を参照) 。

リモートサイトからユーザー定義または手動イベントを追加する:

1. 中央サイトで、サーバーを展開し、レコーディングサーバーを選択します。
2. 概要ペインで、該当するリモートサーバーとイベントタブを選択します。
3. このリストには定義済みのイベントが含まれます。追加をクリックすると、リモートサイトのユーザー定義または手動イベントがリストに追加されます。

リモートサイトのイベントを使用して、中央サイトのアラームをトリガーする:

1. 中央サイトで、アラームを展開し、アラーム定義を選択します。
2. 概要ペインで、アラーム定義を右クリックし、新規追加をクリックします。
3. 必要に応じて値を入力します。
4. トリガーイベントフィールドでは、サポートされている定義済みのイベントとユーザー定義イベントから選択できます。
5. ソースフィールドで、アラームを起動するリモートサイトを表すリモートサーバーを選択します。
6. 完了したら、構成を保存します。

リモートサイトのイベントを使用して、中央サイトのルールに基づくアクションをトリガーする:

1. 中央サイトで、ルールとイベントを展開し、ルールを選択します。
2. 概要ペインで、ルールを右クリックし、ルールの追加をクリックします。
3. 表示されるウィザードで、**<event>**でアクションを実行を選択します。
4. ルール説明の編集領域で、イベントをクリックして、サポートされている定義済みイベントとユーザー定義イベント間を選択します。**OK** をクリックします。
5. デバイス/レコーディングサーバー/マネジメントサーバーをクリックし、中央サイトでアクションを開始するリモートサイトを表すリモートサーバーを選択します。**OK** をクリックします。
6. 次へをクリックして、ウィザードの次のページに進みます。
7. このルールに適用する条件を選択します。条件を選択しない場合は、ルールが常に適用されます。次へをクリックします。
8. ルール説明の編集領域で、アクションを選択し、詳細を指定します。次へ をクリックします。
9. 必要に応じて、停止条件を選択します。次へ をクリックします。
10. 必要に応じて、停止アクションを選択します。終了 をクリックします。

リモート接続サービスの設定

> 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。

リモート接続サービス機能には、Axis Communicationsが開発したAxis One-clickカメラ接続テクノロジーが組み込まれています。 これにより、通常はファイアウォールやルーターネットワーク設定によって接続の開始が妨げられるような外部カメラからも、ビデオ(および音声) を取得できるようになります。実際の通信はセキュアトンネルサーバー(STサーバー) を介して行われます。STサーバーではVPNが使用されます。VPN内では有効なキーを持つデバイスしか動作できません。これは、パブリックネットワークでデータを安全にやり取りするための安全なトンネルとなります。
リモート接続サービスにより以下が可能となります

- Axis Dispatchサービス内で資格情報を編集する
- リモートSTサーバーを追加、編集、削除する
- Axis One-clickカメラを登録/登録解除して編集
- Axis One-Clickカメラに関連したハードウェアに移動する

Axis One-clickカメラの接続を使用するには、最初に適切なSTサーバー環境をインストールする必要があります。セキュアトンネルサーバー(STサーバー) 環境およびAxis One-clickカメラを使用するには、まず、Axis Dispatchサービスに必要なユーザー名とパスワードをシステムプロバイダーから入手する必要があります。

One-Clickカメラ接続のSTS環境をインストール

要件

- Axis Dispatchサービスに必要なユーザー名とパスワードを取得するには、システムプロバイダーに連絡してください。
- カメラがAxisビデオホスティングシステムに対応していることを確認します。Axis Webサイトにアクセスし、対応デバイスについて確認(https://www.axis.com/products/axis-guardian)
- 必要に応じて、Axisカメラを最新のファームウェアで更新します。Axis Webサイトにアクセスしてファームウェアをダウンロード(https://www.axis.com/techsup/firmware.php/)

1. それぞれのカメラのホームページから基本設定>TCP/IPに移動し、AVHSを有効化と常時を選択します。
2. マネジメントサーバーからMilestoneダウンロードページ(https://www.milestonesys.com/downloads/) に移動し、AXIS One-Clickソフトウェアをダウンロードします。プログラムを実行して、適切なAxisセキュアトンネルフレームワークを設定します。

STSの追加/編集

1. 以下のいずれか1つを実行します。
   - STサーバーを追加するには、Axisセキュアトンネルサーバーのトップノードを右クリックし、Axisセキュアトンネルサーバーの追加を選択します。
   - STサーバーを編集するには、これを右クリックし、Axisセキュアトンネルサーバーの編集を選択します。
2. ウィンドウが開くので関連情報を入力します。
3. Axis One-Click Connectionコンポーネントのインストール時に資格情報を使用するよう選択した場合、資格情報を使用するチェックボックスを選択し、Axis One-Click Connectionコンポーネントに使用したものと同じユーザー名とパスワードを入力します。
4. OK をクリックします。

新しいAxis One-Clickカメラの登録

1. カメラをSTサーバーに登録するには対象を右クリックし、**Axis One-Click**カメラの登録を選択します。
2. ウィンドウが開くので関連情報を入力します。
3. **OK** をクリックします。
4. これでカメラが関連STサーバーに表示されます。

カメラは以下のように色分けできます:

色	説明
赤	初期状態。登録されていますが、まだSTサーバーに接続されていません。
黄色	登録済み。STサーバーに接続されていますが、まだハードウェアとして追加されていません。
緑	ハードウェアとして追加済み。STサーバーに接続されている場合も接続されていない場合もあります。

新しいカメラを追加した際には、状態は必ず緑になります。接続状態は、概要ペインのレコーディングサーバーのデバイスに表示されます。概要ペインで、カメラを簡単に把握できるようカメラをグループ化します。この時点でカメラをAxis Dipatchサービスに登録しない場合でも、後で右クリックメニューから登録を行うことができます(**Axis One-Click**カメラの編集を選択) 。

Axis One-Clickカメラの接続プロパティ

名前	説明
カメラのパスワード	入力/編集します。購入時にカメラとともに提供されます。詳細については、カメラのマニュアルを参照するか、Axis Webサイト(https://www.axis.com/) を参照してください。
カメラのユーザー	詳細については、カメラのパスワードを参照してください。
説明	カメラの説明を入力/編集します。
外部アドレス	カメラが接続しているSTサーバーのWebアドレスを入力/編集します。
内部アドレス	レコーディングサーバーが接続しているSTサーバーのWebアドレスを入力/編集します。
名前	必要に応じて、アイテム名を編集します。

名前	説明
所有者認証キー	カメラのパスワードを参照してください。
パスワード(Dispatchサーバー用)	パスワードを入力します。システムプロバイダーから受け取ったものと同じでなければなりません。
パスワード(STサーバー用)	パスワードを入力します。Axis One-Click Connection Connectionコンポーネントをインストールした際に入力したものと同一でなくてはなりません。
Axis Dispatchサービスに登録/登録解除	お持ちのAxisカメラをAxis Dispatchサービスに登録するかどうかが示されます。これは設定時または後で行うことができます。
シリアル番号	メーカーが指定したハードウェアのシリアル番号。シリアル番号は、MACアドレスと同じであることがよくありますが、必ず一致するわけでもありません。
資格情報を使用	このチェックボックスは、STサーバーのインストール時に資格情報を使用する場合に選択します。
ユーザー名(Dispatchサーバー用)	ユーザー名を入力します。ユーザー名は、システムプロバイダーから受け取ったものと同じでなければなりません。
ユーザー名(STサーバー用)	ユーザー名を入力します。Axis One-Click Connectionコンポーネントをインストールした際に入力したものと同一でなくてはなりません。

スマートマップを設定する

このセクションでは以下を実行する方法について説明します。

- スマートマップ用に選択可能な背景地図を構成する
- スマートマップの編集を有効にする(XProtect Smart Clientのカメラを含む)
- Milestone Federated Architectureでスマートマップを設定する

背景地図(説明付き)

XProtect Smart Clientで地理的背景を選択する前に、まず、XProtect Management Clientで背景地図を構成する必要があります。

- 基本的な世界地図 - XProtect Smart Clientで提供される標準的な地理的背景を使用します。構成は不要です。このマップでは、一般的な基準として使用することを意図しており、国の境界線、都市、またはその他の詳細などの機能が含まれていません。ただし、他の背景地図と同様、地理参照データは含まれています。

- **Bing Maps** - Bing Mapsに接続します。
- **Google Maps** - Google Mapsに接続します。
- **OpenStreetMap**には以下の3つのオプションがあります。
  - 選択したコマーシャルタイルサーバーに接続
  - 自身のローカルタイルサーバーに接続する

> Bing MapsとGoogle Mapsのオプションは、インターネットへの接続が必要で、Microsoftまたは Googleからキーを購入する必要があります。
>
> 自身のローカルタイルサーバーを使用する場合を除き、OpenStreetMapにはインターネットアクセスも必要です。

デフォルトで、Bing MapsとGoogle Mapsにはサテライト画像が表示されます(サテライト) 。XProtect Smart Clientの画像は、航空画像や地形表示などに変えて、他の情報を表示させることもできます。

Google MapsまたはBing MapsのAPIキーの取得

Google Maps

お使いのスマートマップにGoogle Mapsを埋め込むには、GoogleからMaps Static APIキーを取得する必要があります。APIキーを取得するには、最初にGoogle Cloud請求先アカウントを作成する必要があります。これにより、毎月読み込んだマップの量に応じて請求が行われます。

APIキーを入手した後、これをXProtect Management Clientに入力してください。ページ434のManagement ClientでBing MapsまたはGoogle Mapsを有効化を参照してください。

詳細については以下を参照：

- Google Mapsプラットフォーム - はじめに: https://cloud.google.com/maps-platform/
- Google Mapsプラットフォーム請求ガイド: https://developers.google.com/maps/billing/gmp-billing
- Maps Static API開発者ガイド: https://developers.google.com/maps/documentation/maps-static/dev-guide

Bing Maps

Bing Mapsをお使いのスマートマップに埋め込むには、ベーシックキーまたはエンタープライズキーが必要です。これらの相違点として、ベーシックキーは無料ですが、トランザクションの数に制限が設けられています。この制限を超えると、トランザクションに対して請求が行われるか、マップサービスが拒否されるようになります。エンタープライズキーは有料ですが、トランザクションを無制限に実行できます。

Bing Mapsの詳細については、https://www.microsoft.com/en-us/maps/licensing/を参照してください。

APIキーを入手した後、これをXProtect Management Clientに入力してください。ページ434のManagement ClientでBing MapsまたはGoogle Mapsを有効化を参照してください。

Management ClientでBing MapsまたはGoogle Mapsを有効化

Management ClientのSmart Clientプロファイルにキーを入力することで、複数のユーザーが使用できるキーを作成できます。プロファイルに割り当てられているすべてのユーザーがこのキーを使用します。

手順：

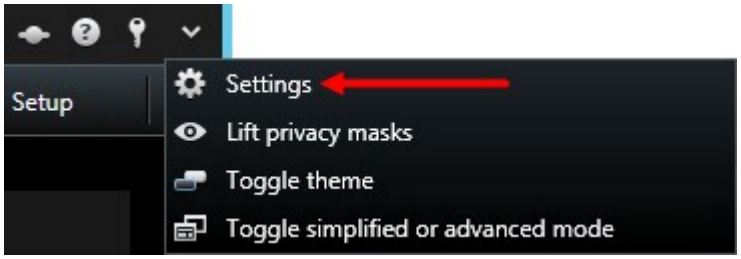
1. Management Clientのサイトナビゲーションペインで、**Smart Client**プロファイルをクリックします。
2. **Smart Client**プロファイル ペインで該当するSmart Clientプロファイルを選択します。
3. プロパティペインでスマートマップタブを以下のようにクリックします。
   - BingMapsについては、お持ちのベーシックキーまたはエンタープライズキーを**BingMaps**キーフィールドに入力します
   - Google Mapsでは、**Google Maps**のプライベートキーフィールドでMaps Static APIキーを入力します
4. XProtect Smart Clientオペレータが別のキーを使用するのを防ぐため、ロック済みチェックボックスを選択します。

XProtect Smart ClientでBing MapsまたはGoogle Mapsを有効化

XProtect Smart Clientオペレータによって**Smart Client**プロファイルキー以外の別のキーを使用できるようにするには、そのキーをXProtect Smart Clientの設定に入力する必要があります。

手順：

1. XProtect Smart Clientで設定ウィンドウを開きます。



2. スマートマップをクリックします。
3. 利用したい地図により、以下のいずれかを行ってください：
   - Bing Mapsでは、**Bing Maps**キーフィールドにキーを入力します。
   - Google Mapsでは、**Google Maps**のプライベートキーフィールドでキーを入力します

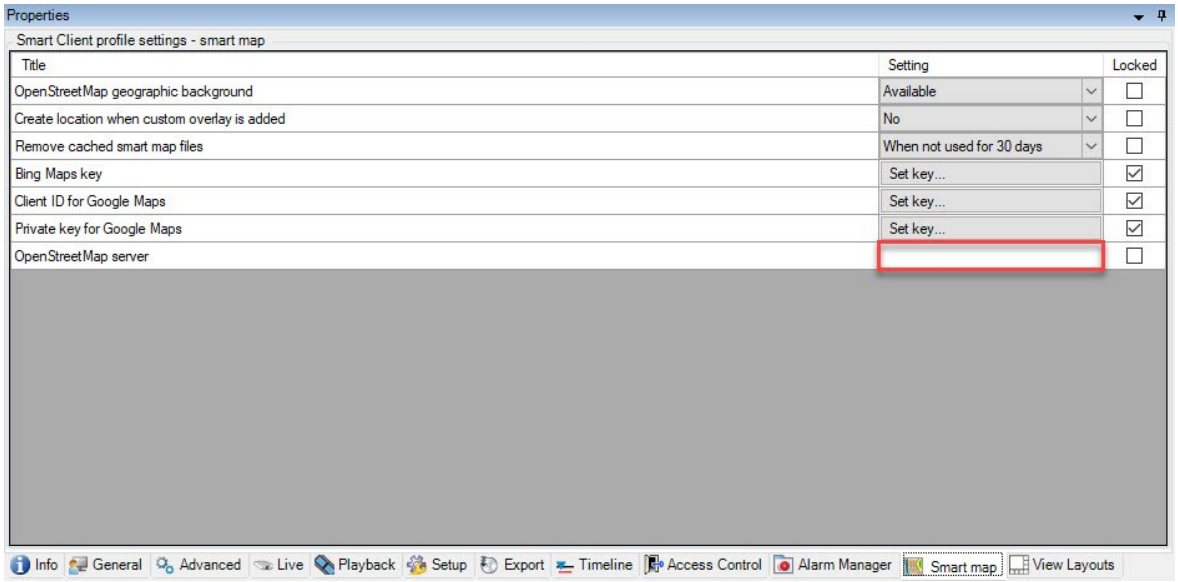
OpenStreetMapタイルサーバーの指定

スマートマップの地理的な背景としてOpenStreetMapを使用する場合は、タイル化された画像の取得先を指定する必要があります。これは、コマーシャルタイルサーバーまたはローカルタイルサーバーのいずれかのタイルサーバーアドレスを指定すると実行できます(所属組織に空港や港といった地域の独自の地図がある場合など)。

> XProtect Smart Clientの設定ウィンドウで、タイルサーバーアドレスを指定することもできます。

手順:

1. サイトナビゲーションペインでクライアントノードを展開し、**Smart Client**プロファイルをクリックします。
2. 概要ペインで関連するSmart Clientプロファイルを選択します。
3. プロパティペインでスマートマップタブをクリックします。



4. **OpenStreetMap**サーバーフィールドにタイルサーバーのアドレスを入力します。
5. XProtect Smart Clientでこの設定を強制するには、ロック済みチェックボックスを選択します。その後、XProtect Smart Clientオペレータはアドレスを変更できません。
6. 変更を保存します。

キャッシュされたスマートマップファイル(説明付き)

> 地理的背景としてGoogle Mapsを使用している場合、ファイルはキャッシュされません。

地理的な背景で使用するファイルはタイルサーバーから取得します。ファイルがキャッシュフォルダーにどれだけの期間保存されるかは、XProtect Smart Clientの設定ダイアログの削除されたキャッシュ済みスマートマップファイルリストでどの値を選択するかに応じて変化します。ファイルは次のどちらかで保存されます。

- 無期限(絶対になし)
- ファイルが使用されていない場合は30日間(30日間使用されていない場合)
- オペレータがXProtect Smart Clientに存在する場合(終了時)

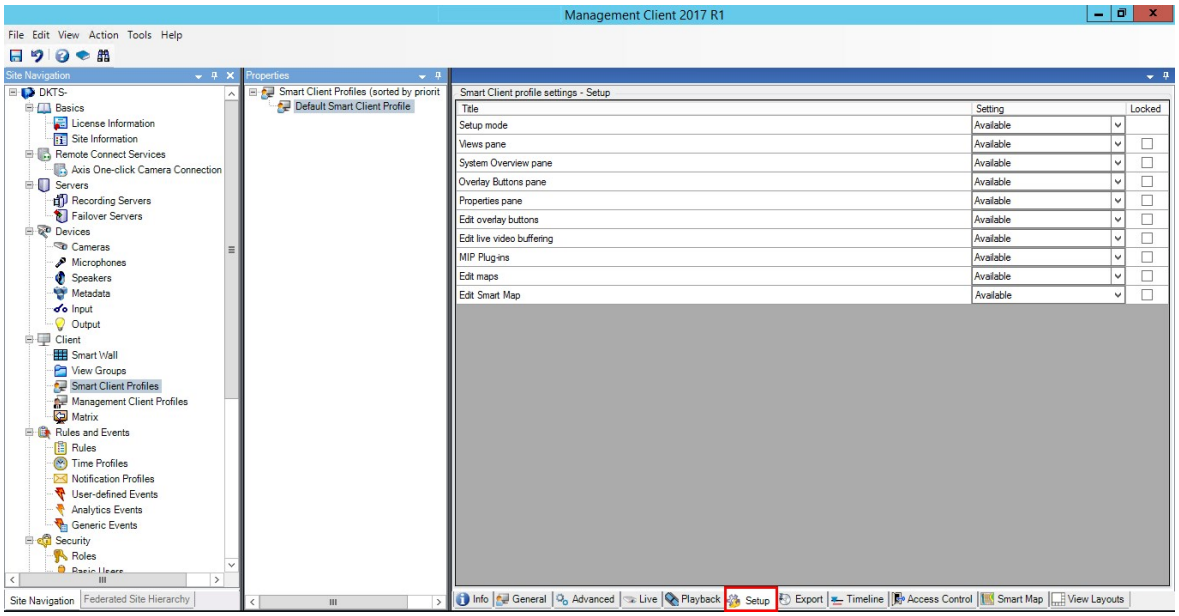
タイルサーバーのアドレスを変更すると、新規キャッシュフォルダーが自動的に作成されます。前のマップファイルは、ローカルコンピュータにある関連のキャッシュフォルダーに保持されています。

スマートマップの編集を有効にする

オペレータは編集がManagement Clientで有効になっている場合にのみXProtect Smart Clientの設定モードでスマートマップを編集できます。まだ有効になっていない場合、関連する各Smart Clientプロファイルの編集を有効にする必要があります。

手順:

1. サイトナビゲーションペインでクライアントノードを展開します。
2. Smart Clientプロファイルをクリックします。



3. 概要ペインで関連するSmart Clientプロファイルを選択します。
4. プロパティペインで設定タブをクリックします。
5. スマートマップの編集リストで、使用可能を選択します。

6. 関連する各Smart Clientプロファイルについてこれらのステップを繰り返します。
7. 変更を保存します。選択したSmart Clientプロファイルに割り当てられたユーザーが次にXProtect Smart Clientにログインする時には、スマートマップを編集できるようになります。

> 編集を無効にするには、スマートマップの編集リストで使用不可を選択します。

スマートマップ上のカメラの編集を有効にする

オペレータがスマートマップ上にカメラを配置して視野と方向を調節できるようにするには、役割ごとにカメラの編集を有効にしなければなりません。

要件

始める前に、スマートマップの編集が有効になっているか確認してください(ページ436のスマートマップの編集を有効にするを参照)。これはオペレータの役割に関連するSmart Clientプロファイルで実行します。

手順:

1. セキュリティノード > 役割を展開します。
2. 役割ペインで、オペレータが関連する役割を選択します。
3. 役割に編集権を与えるには:
   - セキュリティ全般タブをクリックし、役割設定ペインでカメラを選択します。
   - 許可列で、全制御または編集チェックボックスを選択します。
4. 変更を保存します。

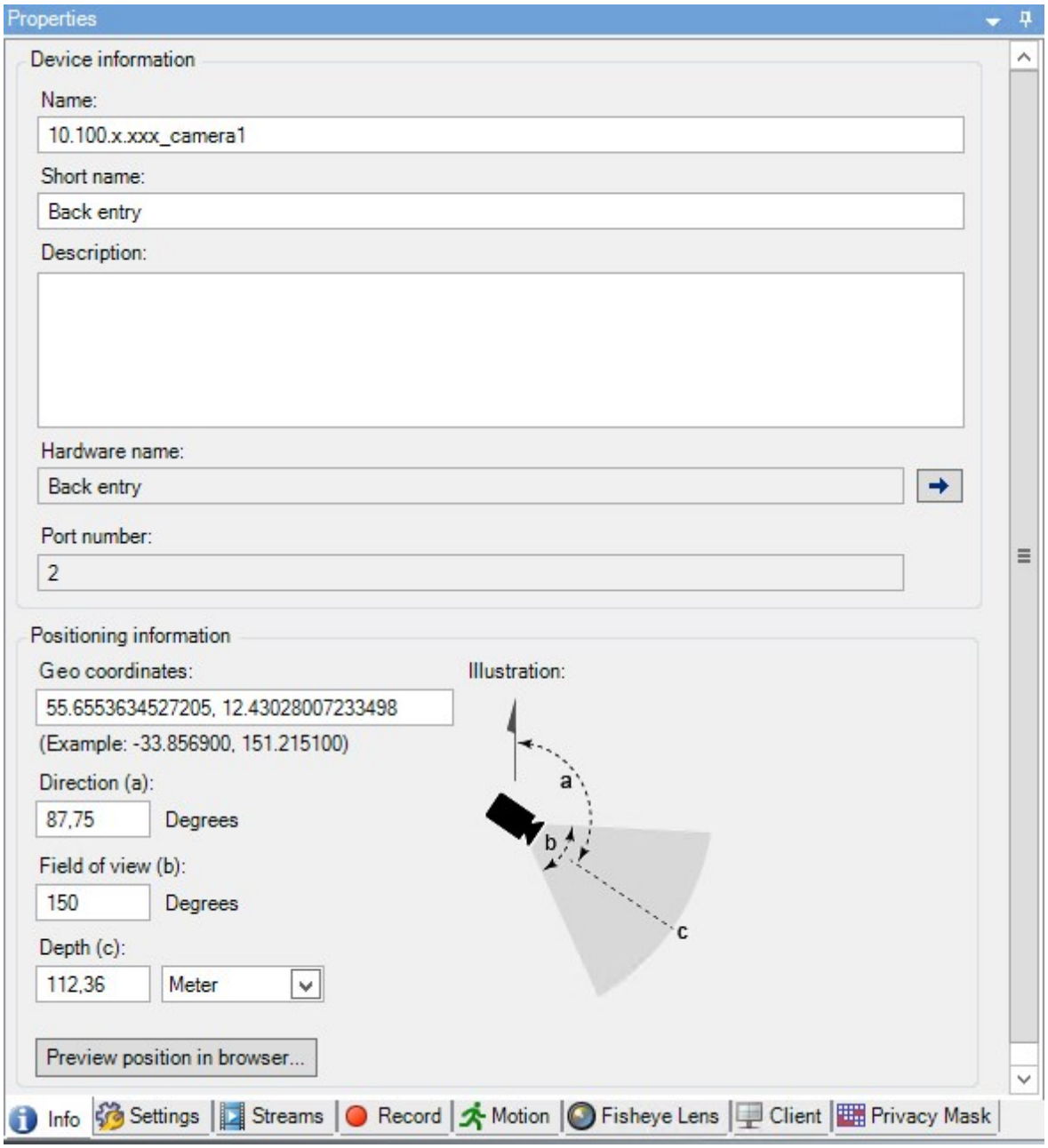
> 上記のステップで、役割にすべてのカメラを編集する権利が与えられます。個々のカメラの編集を有効にするには、デバイスタブに行き該当するカメラを選択します。

カメラの位置、方向、視野、および深度を設定する(スマートマップ)

カメラがスマートマップに適切に配置されるよう、地理座標、カメラの向き、視野、被写界深度を調整することができます。これを行う場合、次回オペレータがXProtect Smart Clientに読み込ませた時点でカメラが自動的にスマートマップに追加されます。

手順:

1. Management Clientで、デバイスノードを展開しカメラを選択します。
2. デバイスペインで、該当するカメラグループとカメラを選択します。
3. 情報タブで、位置情報までスクロールダウンします。



4. 地理座標フィールドで、緯度、経度の順に指定します。値を区切る小数点およびコンマとしてピリオドを使用します。
5. 方向フィールドに、0から360度の範囲の値を入力します。
6. 視野フィールドに、0から360度の範囲の値を入力します。
7. 深度フィールドに、視界深度を、メートルまたはフィートのいずれか一方で入力します。

8. 変更を保存します。

また、レコーディングサーバーのプロパティも設定できます。

Milestone Federated Architectureとともにスマートマップを設定する。

Milestone Federated Architectureにおいてスマートマップを使用するときには、接続されているサイトからのすべてのカメラがスマートマップに現れます。このトピックにおける全体的なステップは、フェデレーテッドアーキテクチャにおいてどのようにスマートマップを設定するかを記載しています。

Milestone Federated Architectureに関する一般的な情報は、ページ412のMilestone Federated Architectureの設定を参照してください。

1. 子サイトを持つトップサイトに接続する前に、全サイトの全カメラでその地理座標が指定されていることを確認します。XProtect Smart Clientを介してカメラをスマートマップに配置すると、地理的な座標が自動的に追加されますが、Management Clientではカメラのプロパティで手動で追加することも可能です。詳細については、ページ437のカメラの位置、方向、視野、および深度を設定する(スマートマップ) を参照してください。
2. Windowsユーザーとして、Smart Clientオペレータを親サイトおよびすべてのフェデレーテッドサイトに追加する必要があります。少なくともトップサイトに置いては、Windowsユーザーはスマートマップ編集権限を持っている必要があります。これによって、トップサイトおよびすべての子サイトにおいてスマートマップの編集をできるようになります。次に、子サイトのWindowsユーザーがスマートマップの編集権を持つ必要があるのか決めなければなりません。Management Clientで初めにWindowsユーザーを役割で作成した後、スマートマップ編集を有効にします。詳細については、ページ436のスマートマップの編集を有効にするを参照してください。
3. トップサイトでは、子サイトをWindowsユーザーがシステム管理者権限の役割を持つユーザーとして追加する必要があります。オブジェクトタイプを特定する際、コンピュータのチェックボックスを選択してください。
4. 各子サイトにおいては、トップサイトをWindowsユーザーがトップサイトと同じシステム管理者役割を持つユーザーとして追加する必要があります。オブジェクトタイプを特定する際、コンピュータのチェックボックスを選択してください。
5. トップサイトでは、フェデレーテッドサイト階層ウィンドウが必ず表示されるようにしてください。Management Clientでは、ビューからフェデレーテッドサイト階層を選択してください。各子サイトをトップサイトに追加します。さらなる情報に関しては、ページ417のサイトを階層に追加を参照してください。
6. それでは、XProtect Smart Clientで機能するかテストをしてみましょう。システム管理者、あるいはオペレータとしてトップサイトに入り、スマートマップを含むビューを開きます。もし設定が正しく行われていれば、トップサイトおよびすべての子サイトからのカメラがスマートマップ上に現れます。もし子サイトの一つにログインした場合、そのサイトとその子サイトのカメラしか見ることができません。

カメラのポジションやアングルの変更など、スマートマップ上でカメラを編集する場合、ユーザーはカメラ編集権利を持っている必要があります。

メンテナンス

システム設定のバックアップおよび復元

Milestoneでは、障害復旧時の手段として、使用しているシステム設定のバックアップを定期的に行うようお勧めしています。通常、設定が失われることはあまりありませんが、失われる可能性はあります。技術的または組織的な対策を通して、バックアップを保護することが重要です。

システム設定のバックアップおよび復元について

システムでは、Management Clientで定義できるシステム設定をすべてバックアップする内蔵機能が提供されています。監査ログファイルを含む、ログサーバーデーターベースおよびログファイルはこのバックアップには含まれていません。

大規模システムの場合、Milestoneは、スケジュールされたバックアップを定義することをお勧めします。これは、次のサードパーティツールを使用して実行できます。Microsoft® SQL Server Management Studio。このバックアップには、手動バックアップと同じデータが含まれています。

バックアップ中、システムはオンラインのままになります。

設定をバックアップするには時間がかかることがあります。バックアップの所要時間は以下に依ります：

- システム設定
- ハードウェア
- SQL Server、イベントサーバーコンポーネント、マネジメントサーバーコンポーネントを単一または複数のサーバーのいずれにインストールしたか

手動操作およびスケジュールの双方に沿ってバックアップを作成するたびに、SQLデータベースのトランザクションログファイルがフラッシュされます。 トランザクション ログ ファイルのフラッシュ方法の詳細については、ページ57のSQLデータベーストランザクションログ(説明付き) を参照してください。

> バックアップを作成する際は、システム設定パスワードを把握しておいてください。

> 非FIPS準拠暗号で暗号化されている2017 R3よりも前のXProtect VMSのバージョンからのエクスポートとアーカイブ済みメディアデータベースのあるFIPS 140-2準拠システムでは、FIPSを有効にした後でもアクセスできる場所でデータをアーカイブする必要があります。
> FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、強化ガイドのFIPS 140-2準拠セクションを参照してください。

共有バックフォルダーの選択

システム設定をバックアップして復元する前に、この目的でバックアップフォルダーを設定しなければなりません。

1. 通知エリアのマネジメントサーバーサービスアイコンを右クリックし、[共有バックフォルダーの選択]を選択します。
2. 表示されるウィンドウで、希望するファイルの場所を参照します。
3. OKを2回クリックします。
4. 現在のバックアップフォルダー内のファイルを削除するか尋ねられたら、必要に応じて、はいまたはいいえをクリックします。

システム設定の手動バックアップ

1. メニューバーから、[ファイル]>[バックアップ構成]を選択します。
2. ダイアログボックスの注記を読んで、バックアップをクリックします。
3. .cnfファイルの名前を入力します。
4. フォルダーの宛先を入力し、保存をクリックします。
5. バックアップが終了するまで待ち、閉じるをクリックします。

すべての関連するシステム設定ファイルは、1つの.cnfファイルにまとめられ、指定された場所に保存されます。バックアップ中、すべてのバックアップファイルはまず、マネジメントサーバー上の一時システムのバックアップフォルダーにエクスポートされます。通知エリアのマネジメントサーバーサービスアイコンを右クリックし、共有バックフォルダーの選択を選択すると、他の一時フォルダーを選択できます。

システム設定の復元(手動バックアップから)

重要な情報

- インストールを実行したユーザーと復元を行ったユーザーの双方とも、マネジメントサーバーおよびSQL Server上のシステム構成SQLデータベースのローカル管理者でなければなりません
- レコーディングサーバーを除き、システムは復元の期間中完全にシャットダウンされます。復元されるまで多少時間のかかる場合があります。
- バックアップは、バックアップが作成されたシステムインストール上でのみ復元できます。設定がバックアップの作成時のものと、できる限り同じであることを確認します。そうしないと、復元が失敗する場合があります。
- 回復中にシステム設定パスワードを聞かれた場合は、バックアップの作成時に有効だったシステム設定パスワードを入力する必要があります。このパスワードがなければ、バックアップから設定を回復できません。

- SQLデータベースをバックアップし、これをクリーンなSQL Serverに復元した場合、SQLデータベースから返されたraiseエラーは機能しないため、SQL Serverから一般エラーメッセージを1通のみ受け取ることになります。これを避けるため、まずはクリーンなSQL Serverを使用してXProtectシステムを再インストールしてから、その上にバックアップを復元してください
- 検証フェーズ中に復元できない場合は、変更がないため、古い設定を再度開始できます。プロセスの他の場所で復元できない場合は、古い設定にロールバックすることはできません。バックアップファイルが破損していない限り、別の復元を実行することができます。
- 復元すると、現在の設定が置き換えられます。これは、前回のバックアップ以降の設定変更がすべて失われることを意味します。
- ログ(監査ログを含む)は復元されません。
- 復元が開始されると、取り消しできません。

復元

1. 通知エリアのマネジメントサーバーサービスアイコンを右クリックし、[設定の復元]を選択します。
2. 重要な注記を読んでから、復元をクリックします。
3. [ファイルを開く]ダイアログボックスで、システム構成バックアップファイルの場所を参照し、これを選択して[開く]をクリックします。

> バックアップファイルは、Management Clientコンピュータ上にあります。Management Clientが他のサーバーにインストールされている場合は、バックアップ先を選択する前にこのサーバーにバックアップファイルをコピーします。

4. 設定の復元ウィンドウが表示されます。復元が終了するまで待ち、閉じるをクリックします。

システム設定パスワード(説明付き)

システム設定パスワードを割り当てると、システム設定全体を保護できます。システム設定パスワードを割り当てると、バックアップはこのパスワードによって保護されます。パスワードの設定は、安全なフォルダーで管理サーバーを実行しているコンピュータに格納されます。以下を行うためにこのパスワードが必要になります:

- 現在のパスワード設定とは異なるパスワード設定を使用して作成された設定バックアップから設定を回復する
- ハードウェアエラーが原因で別のコンピュータに管理サーバーを移動またはインストール(回復)
- クラスタリングを使用してシステムで追加管理サーバーを設定する

> システム設定パスワードはインストール中、またはインストール後に割り当てることができます。パスワードは、パスワードに関するWindowsのポリシーで定義されているWindowsの複雑さ要件を満たす必要があります。

システム管理者は、このパスワードを保存して安全に維持しておく必要があります。システム設定パスワードが割り当てられており、バックアップを回復している場合は、システム設定パスワードを入力するよう求められます。このパスワードがなければ、バックアップから設定を回復できません。

システム設定パスワードの詳細

システム設定パスワードの詳細は変更できます。システム設定パスワードについては以下のオプションがあります。

- システム設定パスワードを割り当てて、システム設定をパスワードで保護します。
- システム設定パスワードの変更
- 割り当てられたシステム設定パスワードを削除することで、システム設定をパスワードで保護しないでください。

システム構成パスワードの設定変更

パスワードを変更する場合は、様々なバックアップに関連のあるパスワードをシステム管理者が保存し、安全に維持しておくことが重要になります。バックアップを回復する際、バックアップの作成時に有効だったシステム設定パスワードを入力するよう求められることがあります。このパスワードがなければ、バックアップから設定を回復できません。

変更を適用するには、管理サーバーサービスを再起動する必要があります。

1. 管理サーバーのトレイアイコンを見つけて、サーバーが実行していることを確認してください。
2. 通知エリアのマネジメントサーバーサービスアイコンを右クリックし、[システム設定パスワードの変更]を選択します。
3. システム設定パスワードの変更ウィンドウが表示されます。

パスワードの割り当て

1. [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。
2. [新しいパスワードを再入力] フィールドで新しいパスワードを再入力し、**Enter**を選択します。
3. 通知を読み、[はい]をクリックして変更を承諾します。
4. 変更の確認を待ってから、[閉じる]を選択します。
5. 変更を適用するには、管理サーバーサービスを再起動する必要があります。
6. 再起動後、管理サーバーが実行していることを確認してください。

パスワード保護を削除する

パスワードによる保護が必要ない場合は、オプトアウトできます。

1. 以下のチェックボックスを選択します:[システム設定パスワードを保護しないことを選択し、システム設定が暗号化されないことを承知する]。その後、**Enter**をクリックします。
2. 通知を読み、[はい]をクリックして変更を承諾します。
3. 変更の確認を待ってから、[閉じる]を選択します。
4. 変更を適用するには、管理サーバー サービスを再起動する必要があります。
5. 再起動後、管理サーバーが実行していることを確認してください。

システム設定パスワードの設定入力 (回復)

パスワードの設定が含まれているフィールドがハードウェアのエラーやその他の理由で削除された場合は、システム設定のあるデータベースにアクセスする際、システム設定パスワードが必要になります。新しいコンピュータでのインストール中、システム設定パスワードを入力するよう求められます。

ただし、パスワードの設定が含まれているファイルが削除されるか、破損した場合、管理サーバーを実行しているコンピューターに他の問題が発生していなければ、システム構成パスワードの設定を入力することができます。

1. 管理サーバーのトレイ アイコンを見つけます。
2. 通知エリアのマネジメントサーバーサービス アイコンを右クリックし、[システム設定パスワードの入力]を選択します。
3. システム設定パスワードの入力ウィンドウが表示されます。

システム設定はパスワードで保護されている

1. [パスワード]フィールドでパスワードを入力し、**Enter**を選択します。
2. パスワードが承諾されるのを待ちます。[閉じる]を選択します。
3. 管理サーバーが実行していることを確認してください。

システム設定はパスワードで保護されていない

1. 以下のチェックボックスを選択します:[このシステムはシステム設定パスワードを使用していません]。その後、**Enter**を選択します。
2. この設定が承諾されるのを待ちます。[閉じる]を選択します。
3. 管理サーバーが実行していることを確認してください。

システム設定の手動バックアップについて(説明付き)

システム構成が含まれるマネジメントサーバーのSQLデータベースの手動バックアップを実行したい場合は、システムがオンライン状態に維持されるよう徹底してください。マネジメントサーバーのSQLデータベースのデフォルト名は監視です。

バックアップを開始する前に、次の点を考慮してください。

- SQLデータベースのバックアップを使用して、システム構成を他のシステムにコピーすることはできません
- SQLデータベースのバックアップにはある程度の時間を要します。これは、システム構成やハードウェアに応じて、ならびにSQL Server、マネジメントサーバー、Management Clientが同一のコンピュータにインストールされているかどうかに応じて異なります。
- ログ(監査ログを含む)はログサーバーのSQLデータベースに保存されているため、マネジメントサーバーのSQLデータベースのバックアップの一部とはなっていません。ログサーバーのSQLデータベースのデフォルト名は**SurveillanceLogServerV2**です。双方のSQLデータベースとも同じ方法でバックアップします。

イベントサーバー構成のバックアップと復元について(説明付き)

イベントサーバー設定の内容は、システム設定のバックアップおよび復元を実行する際に含められます。

イベントサーバーを初めて実行する際には、その構成ファイルのすべてが自動的にSQLデータベースへと移されます。イベントサーバーを再起動する必要なく、復元された設定をイベントサーバーに復元できます。イベントサーバーは、設定の復元のロード中にすべての外部通信を開始および停止できます。

システム設定のスケジュールされたバックアップと復元(説明付き)

マネジメントサーバーのSQLデータベースにはシステム構成が保存されます。Milestoneでは障害復旧対策として、このSQLデータベースの定期バックアップを実行するようお勧めしています。システム構成が失われることはまれですが、不運な状況のもとではその可能性も否定できません。幸いにもバックアップには1分し要せず、SQLデータベースのトランザクションログがフラッシュされるという追加の利点も得られます。

小規模な設定で定期的なバックアップが必要ない場合には、システム設定を手動でバックアップできます。その方法については、「ページ445のシステム設定の手動バックアップについて(説明付き)」を参照してください。

マネジメントサーバーをバックアップ/復元する際には、システム構成が含まれるSQLデータベースがバックアップ/復元に含まれていることを確認してください。

スケジュールされたバックアップおよび復元を使用するための要件

Microsoft® SQL Server Management Studio - Webサイト(https://www.microsoft.com/downloads/)から無料でダウンロードできるツール。

このツールは、SQL Serverとそのデータベースの管理機能に加え、簡単に使用できるバックアップ/復元機能もいくつか備えています。お使いのマネジメントサーバーに、ツールをダウンロードしてインストールします。

スケジュールされたバックアップによるシステム設定のバックアップ

1. Windowsの［スタート］メニューでMicrosoft® SQL Server Management Studioを起動します。
2. 接続時に、必須のSQL Serverの名前を指定します。SQLデータベースの作成に使用したアカウントを使用します。
    1. 全システム構成(イベントサーバー、レコーディングサーバー、カメラ、インプット、アウトプット、ユーザー、ルール、パトロールプロファイルなどを含む)が含まれるSQLデータベースを探します。このSQLデータベースのデフォルト名は監視です。
    2. SQLデータベースのバックアップを作成し、以下について確認します：
        - 正しいSQLデータベースが選択されている
        - バックアップのタイプがフルであることを確認します。
        - 繰り返しバックアップのスケジュールの設定。スケジュールされたバックアップと自動バックアップの詳細については、Microsoft Web サイト(https://docs.microsoft.com/en- us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017)を参照してください。
        - 提案されたパスでよいことを確認するか、代替のパスを選択します
        - [終了時にバックアップの確認]および[メディアに書き込む前のチェックサムの実行]への選択をします。
3. ツールの指示に最後まで従います。

また、ログサーバーのSQLデータベースについても、同じ方法でログとともにバックアップすることを検討してください。ログサーバーのSQLデータベースのデフォルト名は**SurveillanceLogServerV2**です。

システム設定の復元(スケジュールされたバックアップから)

要件

システム構成SQLデータベースの復元中にシステム構成が変更されるのを防ぐため、以下を停止します：

- マネジメントサーバーサービス(ページ460のサーバーサービスの管理を参照)
- イベントサーバーサービス(Windowsサービスから実行可能、お使いのコンピューターで**services.msc**を検索してください)。サービス内で、**Milestone XProtect Event Server**を検索))
- World Wide Web Publishingサービス(別称インターネットインフォメーションサービス(IIS)) IISを停止する方法(https://technet.microsoft.com/library/cc732317(WS.10).aspx/)については以下を参照してください。

Windowsの［スタート］メニューでMicrosoft® SQL Server Management Studioを開きます。

ツールで、以下を実行します。

1. 接続時に、必須のSQL Serverの名前を指定します。SQLデータベースの作成に使用したユーザーアカウントを使用します。
2. 全システム構成(イベントサーバー、レコーディングサーバー、カメラ、インプット、アウトプット、ユーザー、ルール、パトロールプロファイルなどを含む)が含まれるSQLデータベース(デフォルト名：監視)を探します。

3. SQLデータベースを復元し、以下について確認します：
    - デバイスからバックアップするように選択します。
    - バックアップメディアタイプファイルを選択します。
    - バックアップファイル(.bak) を探して選択する
    - [既存のデータベースを上書きする]ように選択します。
4. ツールの指示に最後まで従います。

同じ方法を用いて、ログサーバーのSQLデータベースをログとともに復元します。ログサーバーのSQLデータベースのデフォルト名はSurveillanceLogServerV2です。

> システムは、マネジメントサーバーサービスが停止中には動作しません。データベースの復元が完了した後、すべてのサービスを忘れずに再起動することが重要です。

ログサーバーのSQLデータベースのバックアップ

ログサーバーのSQLデータベースは、前述のシステム構成の処理と同じ方法で処理します。ログサーバーのSQLデータベースには、レコーディングサーバーとカメラから報告されたエラーをはじめとする、あらゆるシステムログが含まれています。ログサーバーのSQLデータベースのデフォルト名はSurveillanceLogServerV2です。

SQLデータベースは、ログサーバーのSQL Serverに配置されています。通常、ログサーバーとマネジメントサーバー双方のSQLデータベースが同一のSQL Serverに配置されます。ログサーバーSQLデータベースにはシステム構成が一切含まれていないため、そのバックアップは不可欠ではありませんが、マネジメントサーバーのバックアップ/復元前にシステムログにアクセスできるという利点は得られます。

バックアップ/復元の失敗と問題のシナリオについて(説明付き)

- 前回のシステム設定バックアップ後、イベントサーバーや、ログサーバーなどの登録済みサービスを移動した場合は、新しいシステムにどの登録サービスを設定するか選択する必要があります。システムが古いバージョンに復元された後に、新しい構成を保持することが可能です。サービスのホスト名を見て選択してください。
- イベントサーバーが特定の宛先にない(古い登録済みサービス設定を選択した場合など) ために、システム設定の復元が失敗した場合は、もう1回復元してください。
- 設定バックアップの回復中に、誤ったシステム設定パスワードを入力した場合は、バックアップの作成時に有効だったシステム設定パスワードを入力する必要があります。

マネジメントサーバーの移動

マネジメントサーバーのSQLデータベースにはシステム構成が保存されます。物理サーバーから別のサーバーへとマネジメントサーバーを移動している最中には、新しいマネジメントサーバーからもこのSQLデータベースにアクセスできていることを確認することが欠かせません。システム構成SQLデータベースは以下の2種類の方法で保存できます：

- ネットワークSQL Server：システム構成をネットワーク上にあるSQL ServerのSQLデータベースに保存している場合、マネジメントサーバーソフトウェアを新しいマネジメントサーバーにインストールする際に、そのSQL ServerでSQLデータベースの場所をポイントすることができます。このようなケースにおいては、管理者サーバーのホスト名のあるパラグラフに続く管理者サーバーホスト名についての続くパラグラフのみIPアドレスを適応します。残りのトピックは無視してください:

  管理者サーバー ホスト名 とIP アドレス: 1つの物理サーバーから別の物理サーバーへとマネジメントサーバーを移動するときには、古いものと同じホスト名とIPアドレスを新しいサーバーに割り当てることが最も簡単な方法です。これは、レコーディングサーバーが古いマネージメントサーバーのホスト名とIPアドレスに自動的に接続するためです。新しいマネージメントサーバーに新しいホスト名および/またはIPアドレスを与えると、レコーディングサーバーはマネージメントサーバーを見つけることができないため、各レコーディングサーバーサービスを手動で止め、マネージメントサーバーのURLを変更し、レコーディングサーバーを再登録して、その後でレコーディングサーバーサービスを起動します。

- ローカルSQL Server：システム構成をマネジメントサーバー本体に存在するSQL ServerのSQLデータベースに保存している場合、移動前に、既存のマネジメントサーバーのシステム構成SQLデータベースをバックアップすることが重要です SQLデータベースをバックアップし、後の段階で新しいマネジメントサーバーのSQL Serverに復元することで、移動後にカメラ、ルール、時間プロファイルなどを再構成する必要がなくなります

> 管理サーバーを移動する場合は、バックアップを回復するために最新のシステム設定パスワードが必要になります。ページ443のシステム設定パスワード(説明付き)を参照してください。

要件

- 新しいマネジメントサーバーにインストールするためのソフトウェアインストールファイル
- システムを購入し、初めてインストールしたときに受け取ったソフトウェアライセンスファイル(.lic)。手動オフラインアクティベーション後に受け取ったアクティベーション済みソフトウェアライセンスファイルを使用しないでください。アクティベーション済みソフトウェアライセンスファイルには、システムがインストールされた特定のサーバーの情報が含まれます。このため、アクティベーション済みソフトウェアライセンスファイルは新しいサーバーに移動すると再利用できません。

移動してシステムライセンスをアップグレードしている場合は、新しいソフトウェアライセンスファイルが提供されます。このファイルを使用してください。

- ローカルSQL Serverユーザーのみ：Microsoft® SQL Server Management Studio
- マネジメントサーバーが利用できない間はどうしますか? ページ449のマネジメントサーバーの利用不可(説明付き))
- ログサーバーデータベースをコピーする(「ページ448のログサーバーのSQLデータベースのバックアップ」を参照)

マネジメントサーバーの利用不可(説明付き)

- レコーディングサーバーは現在もの録画ができます。現在動作しているレコーディングサーバーはすべて、マネジメントサーバーからの設定のコピーを受け取るので、マネジメントサーバーがダウンしている間でも、動作して記録を保存できます。このため、スケジュールされた録画とモーショントリガーの録画は動作します。イベントトリガー録画も、マネジメントサーバーまたはその他のレコーディングサーバーに関連しているイベント(マネジメントサーバーを経由するイベント)

に基づいていない限り動作します。

- レコーディングサーバーは一時的にログデータをローカルに保存します。マネジメントサーバーが再度利用可能になったときに、レコーディングサーバーは自動的にログデータをマネジメントサーバーへ送信します。
  - クライアントがログインできません。クライアントアクセスは、マネジメントサーバーを通じて承認されます。マネジメントサーバーなしではクライアントはログインできません。
  - すでにログインしているクライアントは、最大1時間ログインした状態を継続できます。クライアントがログインした場合、マネジメントサーバーによって承認され、最大1時間レコーディングサーバーと通信することができます。新しいマネジメントサーバーを1時間以内に稼働できれば、ユーザーの大半に影響が及ぶことはありません。
  - システムを構成する能力がありません。マネジメントサーバーがなければ、システム設定を変更することができません。

Milestoneでは、管理サーバーがダウンしている間は、監視システムとの通信が切断される危険性があることをユーザーに通知するようお勧めしています。

システム設定の移動

システム設定の移動は、次の3段階のプロセスに従って行います。

1. システム設定のバックアップを保存します。これは定期的なバックアップを行う場合と同じです。ページ447のスケジュールされたバックアップによるシステム設定のバックアップも参照してください。
2. 新しいサーバーに新しいマネジメントサーバーをインストールします。スケジュールされたバックアップの手順2を参照してください。
3. 新しいシステムにシステム設定を復元します。ページ447のシステム設定の復元(スケジュールされたバックアップから)も参照してください。

レコーディングサーバーの交換

レコーディングサーバーが動作しないため、新しいサーバーと交換し、古いレコーディングサーバーの設定を継承する場合：

1. 交換するレコーディングサーバーから、レコーディングサーバーIDを取得します。
   1. レコーディングサーバーを選択し、概要ペインで古いレコーディングサーバーを選択します。
   2. ストレージタブを選択します。
   3. キーボードでCtrlキーを押したままにして、情報タブを選択します。

4. 情報タブの下の部分にあるレコーディングサーバーID番号をコピーします。文字*ID*の部分はコピーしないで、番号だけをコピーしてください。

2. 新しいレコーディングサーバーで、レコーディングサーバーIDを置き換えます。

   1. 古いレコーディングサーバーでレコーディングサーバーサービスを停止してから、Windowsのサービスで、サービスの[スタートアップの種類]を[無効]に設定します。

      同じIDを持つ2つのレコーディングサーバーを同時に起動しないことが重要です。

   2. 新しいレコーディングサーバーで、エクスプローラを開いて、*C:\ProgramDataMilestone\XProtect Recording Server*またはレコーディングサーバーがあるパスへ移動します。
   3. *RecorderConfig.xml*のファイルを開きます。
   4. タグ*<id>*と*</id>*の間に記載されているIDを削除します。

   5. コピーしたレコーディングサーバーIDを、タグ*<id>*と*</id>*の間に貼り付けます。*RecorderConfig.xml*のファイルを保存します。
   6. レジストリに移動します。*HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation*
   7. **RecorderIDOnMachine**を開き、古いレコーディングサーバーIDを新しいIDに置換します。

3. 新しいレコーディングサーバーをマネージメントサーバーに登録します。RecordingServerManagerトレイアイコンを右クリックして、[登録]をクリックします。詳細については、ページ140のレコーディングサーバーを登録するを参照してください。
4. レコーディングサーバーサービスを再起動します。新しいレコーディングサーバーサービスが起動すると、古いレコーディングサーバーの設定がすべて継承されます。

ハードウェアの移動

同じサイトに属するレコーディングサーバー間でハードウェアを移動できます。移動後に、ハードウェアとそのデバイスは新しいレコーディングサーバーで実行され、新しい録画がこのサーバーに保存されます。移動はクライアントユーザーに透過的です。

古いレコーディングサーバーの録画は、次の処理が発生するまで保存されたままです。

- 保持期間が経過したときにシステムによって録画が削除されます。他の人物がエビデンスロックを用いて保護した録画(「ページ385のエビデンスロック(説明付き)」を参照)は、エビデンスロックの保存期間が経過するまでは削除されません。エビデンスロックの保持期間はエビデンスロックを作成するときに定義します。保存期間が設定されない可能性もあります。
- [録画]タブで各デバイスの新しいレコーディングサーバーから録画を削除する。

まだ録画が含まれるレコーディングサーバーを削除しようとすると、警告が表示されます。

> 現在ハードウェアが追加されていないレコーディングサーバーにハードウエアを移動する場合は、クライアントユーザーはログアウトしてからログインし直し、デバイスからデータを取得する必要があります。

ハードウェアの起動機能を使用すると、次のことができます。

- ロードバランシング:例えば、レコーディングサーバーのディスクが過負荷状態の場合、新しいレコーディングサーバーを追加し、一部のハードウェアを移動できます。
- アップグレード:例えば、レコーディングサーバーをホストするサーバーを新しいモデルで置換する場合は、新しいレコーディングサーバーをインストールし、古いサーバーから新しいサーバーにハードウェアを移動できます。
- 障害があるレコーディングサーバーの交換:たとえば、サーバーがオフラインで、オンラインに戻らない場合は、ハードウェアを他のレコーディングサーバーに移動し、システムを実行し続けることができます。古い録画にはアクセスできません。詳細については、「ページ450のレコーディングサーバーの交換」を参照してください。

リモート録画

ハードウェアを別のレコーディングサーバーに移動すると、相互接続されたサイトまたはカメラのエッジストレージからの実行中の取得または予定された取得はキャンセルされます。録画は削除されませんが、想定通りにデータは取得されず、データベースに保存されません。この場合は警告が表示されます。ハードウェアの移動を開始したときに取得を開始したXProtect Smart Clientユーザーの場合、取得は失敗します。XProtect Smart Clientユーザーには通知が表示され、後から再試行できます。

別のユーザーがリモートサイトでハードウェアを移動した場合は、[ハードウェアの更新]オプションを使用して、手動で中央サイトを同期し、リモートサイトの新しい構成を反映する必要があります。同期しない場合は、移動されたカメラは中央サイトから切断されています。

ハードウェアの移動(ウィザード)

1つのレコーディングサーバーから別のサーバーへハードウェアを移動するには、[ハードウェアの移動]ウィザードを実行します。ウィザードは必要な手順を案内し、1つ以上のハードウェアデバイスを移動します。

要件

ウィザードを開始する前に行う手順:

- 新しいレコーディングサーバーがネットワーク経由で物理カメラにアクセスできることを確認します。
- ハードウェアの移動先としたいレコーディングサーバーをインストールする(「ページ88の新しいXProtectコンポーネントのインストール」または「ページ88の新しいXProtectコンポーネントのインストール」を参照)
- 同一のデバイスパックバージョンを、既存のサーバーで実行することになる新しいレコーディングサーバーにインストールする(「ページ66のデバイスドライバー(説明付き)」を参照)

ウィザードを実行するには:

1. [サイトナビゲーション]ペインでレコーディングサーバーを選択します。
2. [概要]ペインで、ハードウェアの移動元のレコーディングサーバーを右クリックするか、特定のハードウェアデバイスを右クリックします。
3. [ハードウェアの移動]を選択します。

> ハードウェアの移動元のレコーディングサーバーが切断されている場合は、エラーメッセージが表示されます。レコーディングサーバーがオンラインにならないことが確かである場合にのみ、切断されたレコーディングサーバーからハードウェアを移動してください。ハードウェアを移動し、サーバーがオンラインに戻った場合は、同じハードウェアが2つのレコーディングサーバーで実行される期間があるため、システムで予期しない動作が発生するおそれがあります。たとえば、ライセンスエラーや、イベントが正しいレコーディングサーバーに送信されないといった問題が生じる可能性があります。

4. レコーディングサーバーレベルでウィザードを開始した場合は、[移動するハードウェアを選択]ページが表示されます。移動するハードウェアデバイスを選択します。
5. [ハードウェアの移動先となるレコーディングサーバーを選択]ページで、このサイトにインストールされたレコーディングサーバーのリストから選択します。
6. [将来の録画で使用するストレージを選択]ページで、ストレージ使用状況バーに、アーカイブではなくライブ録画のみのレコーディングデータベースの空き領域が表示されます。合計保存期間は、レコーディングデータベースとアーカイブの両方の保存期間です。
7. システムが要求を処理します。
8. 移動が成功した場合は、[閉じる]をクリックします。Management Clientで新しいレコーディングサーバーを選択する場合は、移動されたハードウェアが表示され、録画がこのサーバーに保存されます。

   移動が失敗した場合は、以下に従って問題をトラブルシューティングできます。

> 相互接続されたシステムでは、リモートサイトのハードウェアを移動した後に中央サイトを手動で同期し、自分または他のシステム管理者がリモートサイトで行った変更を反映する必要があります。

ハードウェアの移動のトラブルシューティング

移動が失敗した場合は、次の理由のいずれかが原因である可能性があります。

エラータイプ	トラブルシューティング
レコーディングサーバーが接続されていないか、フェールオーバーモードです。	レコーディングサーバーがオンラインであることを確認してください。登録しなければならない場合があります。 サーバーがフェールオーバーモードの場合は、待機してから再試行してください。
レコーディングサーバーは最新バージョンではありません。	レコーディングサーバーを更新し、マネジメントサーバーと同じバージョンで実行されるようにします。
レコーディングサーバーが設定に見つかりません。	レコーディングサーバーが削除されていないことを確認してください。
構成の更新または構成データベースとの通信が失敗しました。	SQL Serverとデータベースが接続されており、稼働していることを確認します。
現在のレコーディングサーバーでハードウェアを停止できませんでした。	他のプロセスによってレコーディングサーバーがロックされているか、レコーディングサーバーがエラーモードに入っている可能性があります。 レコーディングサーバーが実行中であることを確認し、再試行してください。
ハードウェアが存在しません。	移動するハードウェアが別のユーザーと同時にシステムから削除されていないことを確認してください。この状況が発生することはほとんどありません。
ハードウェアが削除されたレコーディングサーバーがオンラインに戻りましたが、オフラインのときに無視するように選択しました。	一般的に、**[**ハードウェアの移動**]**ウィザードを開始したときに古いレコーディングサーバーがオンラインにならないことを確認しましたが、移動中にサーバーがオンラインになりました。 再度ウィザードを開始して、サーバーが再びオンラインになったかどうかを確認する操作に対して [いいえ] を選択します。
ソースのレコーディングストレージが使用できません。	現在オフラインになっているレコーディングストレージのあるデバイスをともなうハードウェアを移動しようとしています。 レコーディングストレージは、ディスクがオフラインまたは何らかの理由で利用できない場合、オフラインになります。

エラータイプ	トラブルシューティング
	レコーディングストレージがオンラインであることを確認し、再試行してください。
移動先のレコーディングサーバー上にあるレコーディングストレージがすべて使用可能である必要があります。	ハードウェアを、1つ以上のレコーディングストレージが現在オフラインになっているレコーディングサーバーに移動しようとしています。 移動先のレコーディングサーバー上のレコーディングストレージがすべてオンラインになっていることを確認してください。 レコーディングストレージは、ディスクがオフラインまたは何らかの理由で利用できない場合、オフラインになります。

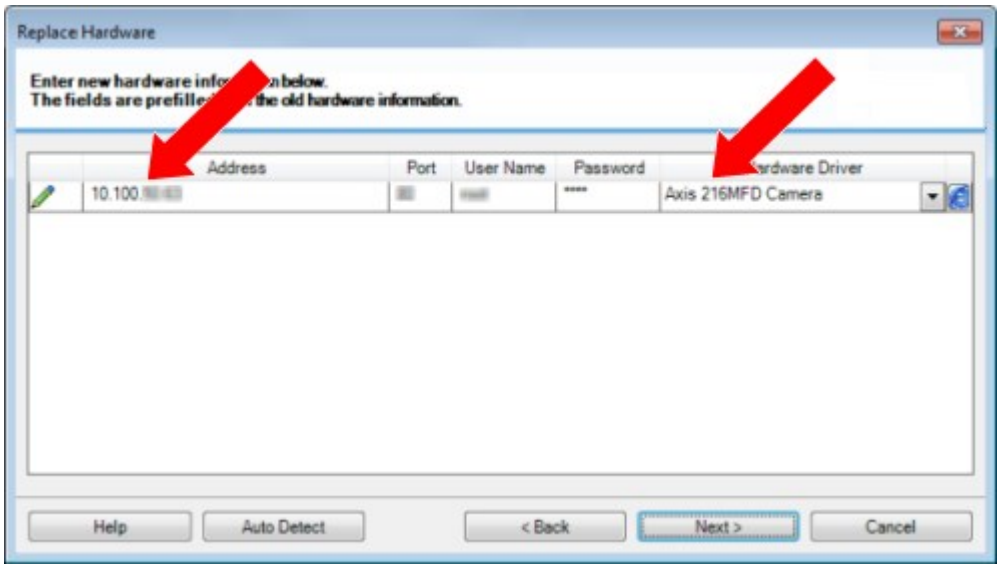
ハードウェアの交換

ネットワーク上のハードウェアデバイスを他のハードウェアデバイスに交換する場合、新しいハードウェアデバイスのIPアドレス、ポート、ユーザー名およびパスワードを知っている必要があります。

> ページ131のライセンス情報を有効にせず、アクティベーションなしのデバイスの変更(ページ131のライセンス情報を参照)をすべて使用した場合は、ハードウェアデバイスを交換した後に、手動でライセンスをアクティベートする必要があります。ハードウェアデバイスの新しい数がハードウェアデバイスライセンスの合計数を超えた場合、新しいハードウェアデバイスライセンスを購入する必要があります。

1. 必要なレコーディングサーバーを展開し、交換するハードウェアを右クリックします。
2. ハードウェアの交換を選択します。
3. ハードウェアの交換ウィザードが表示されます。[次へ] をクリックします。

4. ウィザードで、アドレスフィールド(図中の赤い矢印)に、新しいハードウェアのIPアドレスを入力します。既知であれば、ハードウェアドライバーのドロップダウンリストから、関連するドライバーを選択します。それ以外の場合は、自動検出を選択します。新しいハードウェアのポート、ユーザー名または/およびパスワードのデータが異なる場合は、自動検出プロセスが開始する前に(必要な場合)これらを訂正します。



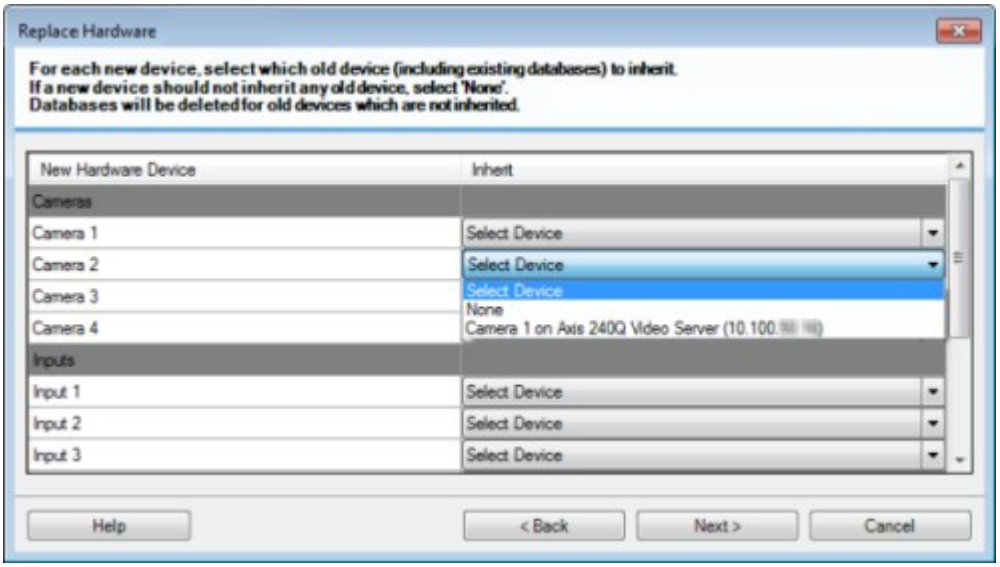
ウィザードでは、既存のハードウェアのデータが事前に入力されています。類似のハードウェアデバイスと交換する場合、たとえばポートやドライバーの情報など、これらのデータを再利用できます。

5. 以下のいずれか1つを実行します。
   - 必要なハードウェアデバイスのドライバーをリストから直接選択している場合は、[次へ]をクリックします。
   - リストで[自動検出]を選択している場合は、[自動検出]をクリックし、このプロセスが正常に完了するまで(左端に✔のマークが出るまで)待ってから、[次へ]をクリックします。

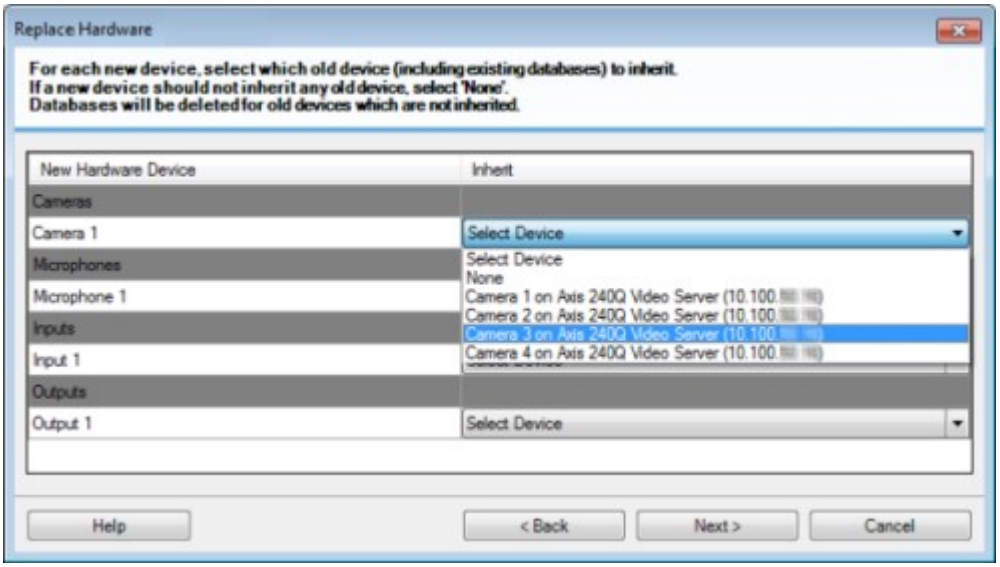
   この手順は、古いハードウェアデバイスと新しいハードウェアデバイスのそれぞれに取り付けられているカメラ、マイク、入力、出力などの数に応じて、デバイスとデータベースをマップするのに役立つように設計されています。

   古いハードウェアデバイスのデータベースから新しいハードウェアデバイスのデータベースへ、どのようにマップするか検討することが重要です。個々のデバイスの実際のマッピングは、右側の列で対応するカメラ、マイク、入力、出力またはなしを選択して行います。

   > ⚠ 必ず、すべてのカメラ、マイク、入力、出力などをマッピングしてください。なしにマッピングされた内容は失われます。



古いハードウェアデバイスに、新しいハードウェアデバイスより多くの個別のデバイスがある例



[次へ] をクリックします。

6. 追加、交換または削除されるハードウェアの一覧が表示されます。確認をクリックします。
7. 最後の手順は、追加、交換および継承されるデバイスとその設定の概要です。クリップボードへコピーをクリックして、内容をWindowsクリップボードコピーするか、閉じるをクリックしてウィザードを終了します。

SQL Serverとデータベースの管理

SQL Serverとデータベースアドレスの変更(説明付き)

システムを試用版としてインストールする場合、または大規模インストールを再構築する場合は、別のSQL Serverとデータベースを使用しなくてはならない場合があります。これは、SQL Serverアドレス更新ツールを用いて実行できます。

このツールを使用すれば、マネジメントサーバーとイベントサーバーによって使用されているSQL Serverとデータベースのアドレス、そしてログサーバーによって使用されているSQL Serverとデータベースのアドレスを変更することができます。唯一の制限として、マネジメントサーバーとイベントサーバーのSQLアドレスは、ログサーバーのSQLアドレスと同時に変更することはできません。変更は1つずつ順番に行います。

マネジメントサーバー、イベントサーバー、ログサーバーがインストールされたコンピュータで、SQL Serverとデータベースアドレスをローカルで変更する必要があります。マネジメントサーバーとイベントサーバーが別々のコンピュータにインストールされている場合、両方のコンピュータでSQL Serverアドレス更新ツールを実行する必要があります。

> 次へ進む前にSQLデータベースをコピーする必要があります。

ログサーバーのSQL Serverとデータベースを変更

1. マネジメントサーバーがインストールされているコンピュータに移動し、*%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress*フォルダー(コンテンツ入り)をイベントサーバーの一時フォルダーにコピーします。
2. コピーしたフォルダーを、ログサーバーがインストールされているコンピュータの一時的な場所にコピーし、そこに包含されているファイルを実行します：*VideoOS.Server.ChangeSqlAddress.exe*。 [SQL Serverアドレスの更新]ダイアログボックスが開きます。
3. **Log Server**を選択して、[次へ]をクリックします。
4. 新しいSQL Serverを入力または選択して、[次へ]をクリックします。
5. SQLデータベースを新しく選択して、選択をクリックします。
6. アドレスが変更されるまで待ちます。**OK**をクリックして確定します。

マネジメントサーバーとイベントサーバーのSQLアドレスを変更

マネジメントサーバーとイベントサーバーは、同じSQLデータベースを使用します。

1. マネジメントサーバーおよびイベントサーバーが、
    1. 同一のコンピュータにある状態で、SQLアドレスを更新したい場合は、マネジメントサーバーがインストールされているコンピュータに移動します。
    2. 別々のコンピュータにある状態で、マネジメントサーバーのSQLアドレスを更新(続けてイベントサーバーSQLアドレスも更新)したい場合は、マネジメントサーバーがインストールされているコンピュータに移動します。
    3. 別々のコンピュータにある状態で、イベントサーバーSQLアドレスのみを更新したい場合(またはすでにマネジメントサーバーでこれを更新済みの場合)、マネジメントサーバーがインストールされているコンピュータに移動し、*%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress*ディレクトリ(コンテンツ入り)をイベントサーバーの一時ディレクトリにコピーします。
2. あるいは：
    1. **1.1**および**1.2**を選択した場合、タスクバーの通知エリアに移動します。マネジメントサーバーアイコンを右クリックし、**SQL**アドレスの更新を選択します。イベントサーバーのSQLアドレスを更新するには、同じ手順を繰り返してください。
    2. **1.3**を選択した場合、コピーしたディレクトリをイベントサーバーがインストールされているコンピュータの一時領域にコピーし、その中のファイル：*VideoOS.Server.ChangeSqlAddress.exe*を実行します。
3. [SQL Serverアドレスの更新]ダイアログボックスが開きます。**Management Server**サービスを選択し、**[次へ]**をクリックします。
4. 新しいSQL Serverを入力または選択して、[次へ]をクリックします。
5. SQLデータベースを新しく選択して、選択をクリックします。
6. アドレスが変更されるまで待ちます。確認メッセージが表示されたら、**OK**をクリックします。

サーバーサービスの管理

サーバーサービスを実行するコンピュータでは、通知領域にサーバーマネージャートレイアイコンを見つけることができます。アイコンを使用すると、サービスの情報を取得し、特定のタスクを実行できます。これには、サービスの状態の確認、ログまたはステータスメッセージの表示、サービスの起動と停止などがあります。

サーバーマネージャーのトレーアイコン(説明付き)

テーブルのトレーアイコンには、マネジメントサーバー、レコーディングサーバー、フェイルオーバーレコーディングサーバー、イベントサーバーを実行しているサービスの各種状態が示されます。これらは、サーバーがインストールされているコンピュータの通知領域に表示されます:

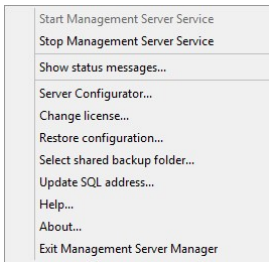
Management Server Manager トレーアイコン	Recording Server Manager トレーアイコン	Event Server Manager トレイアイコン	Failover Recording Server Manager トレイアイコン	説明
				実行中 サーバーサービスが有効になって起動した際に表示されます。 Failover Recording Server サービスが実行されている場合、標準レコーディングサーバーに不具合が生じた際に、このサービスが処理を引き継ぎます。
				停止 サーバーサービスが停止した際に表示されます。

Management Server Manager トレーアイコン	Recording Server Manager トレーアイコン	Event Server Manager トレイアイコン	Failover Recording Server Manager トレイアイコン	説明
				Failover Recording Server サービスが停止した場合、標準レコーディングサーバーに不具合が生じても、このサービスが処理を引き継ぐことはできません。
				開始中 サーバーサービスが開始プロセスに入った際に表示されます。通常の状態では、トレーアイコンはしばらくしてから[実行中]に変化します。
				停止中 サーバーサービスが停止プロセスに入った際に表示されます。通常の状態では、トレーアイコンはしばらくしてから[停止中]に変化します。
				中間状態 サーバーサービスが最初に読み込まれてから最初の情報を受信するまで表示されます。通常の状態では、トレーアイコンは[開始中]に、続いて[実行中]に変化します。
				オフラインで実行 通常はレコーディングサーバーまたはフェールオーバーレコーディングサーバーが実行されているものの、マネジメントサーバーサービスが実行されていない場合に表示されます。

マネジメントサーバーサービスの開始または停止

Management Server Managerトレイアイコンは、[実行中]などの、マネジメントサーバーサービスのステータスを示します。このアイコンを使用して、マネジメントサーバーサービスを開始、停止できます。マネジメントサーバーサービスが停止したときには、Management Clientは使用できません。

1. 通知領域で、Management Server Managerアイコンを右クリックします。コンテキストメニューが表示されます。



2. サービスが停止した場合は、[マネジメントサーバーサービス開始]をクリックして開始します。トレイアイコンが変わり、新しい状態を示します。

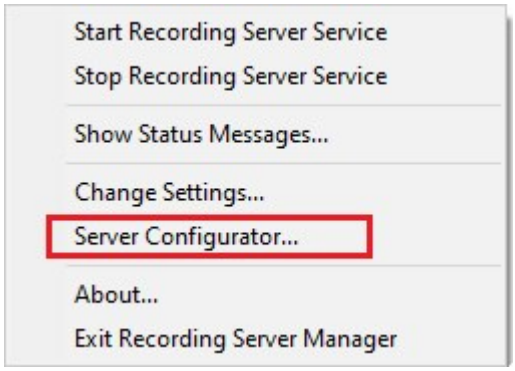
3. サービスを停止するには、[マネジメントサーバーサービス停止]をクリックします。

詳細については、ページ460のサーバーマネージャーのトレーアイコン(説明付き)を参照してください。

レコーディングサーバーサービスの開始または停止

Recording Server Managerトレイアイコンは、[実行中]などの、レコーディングサーバーサービスのステータスを示します。このアイコンを使用して、レコーディングサーバーサービスを開始、停止できます。レコーディングサーバーサーバーを停止した場合は、サーバーに接続されたデバイスと連携できません。つまり、ライブビデオの表示またはビデオの録画ができません。

1. 通知領域で、Recording Server Managerアイコンを右クリックします。コンテキストメニューが表示されます。



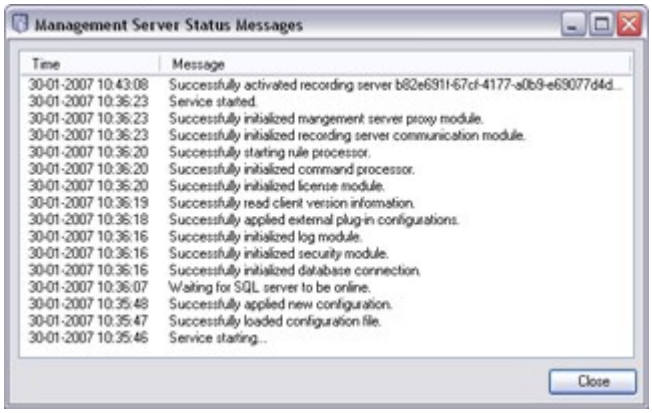
2. サービスが停止した場合は、[レコーディングサーバーサービス開始]をクリックして開始します。トレイアイコンが変わり、新しい状態を示します。

3. サービスを停止するには、[レコーディングサーバーサービス停止]をクリックします。

詳細については、ページ460のサーバーマネージャーのトレーアイコン(説明付き)を参照してください。

マネジメントサーバーまたはレコーディングサーバーのステータスメッセージの表示

1. 通知領域で、該当するトレイアイコンを右クリックします。コンテキストメニューが表示されます。
2. ステータスメッセージの表示を選択します。サーバーの種類に応じて、[マネジメントサーバーのステータスメッセージ]または[レコーディングサーバーのステータスメッセージ]ウィンドウが表示され、タイムスタンプの付いたステータスメッセージが一覧表示されます。



暗号化の管理 - 方法:Server Configurator

Server Configuratorを使用して、ローカルサーバーで暗号化された通信用の証明書を選択し、証明書によってサーバーとの通信が許可されるようにするためサーバーサービスを登録してください。

WindowsのスタートメニューまたはマネジメントサーバーのトレイアイコンのいずれかからServer Configuratorを開きます。

詳細については、XProtect VMSの保護方法に関する証明書ガイドを参照してください。暗号化を有効にする前に、管理サーバーと、レコーディングサーバーがあるコンピュータすべてにセキュリテ証明書をインストールしてください。

Server Configuratorの[暗号化]セクションで、以下のタイプの暗号化を設定します。

- サーバー証明書

  マネジメントサーバー、データコレクタ、レコーディングサーバー間の双方向接続を暗号化するために使用される証明書を選択してください。

  モバイルサーバーの暗号化は、モバイルサーバートレイアイコンから有効化されます。

- ストリーミングメディアの証明書

  レコーディングサーバーと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すべてのクライアント、サーバー、統合間の通信を暗号化するために使用される証明書を選択してください。

- モバイル ストリーミング メディアの証明書

  モバイル サーバーと、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およびWebクライアントの間の通信を暗号化するために使用する証明書を選択します。

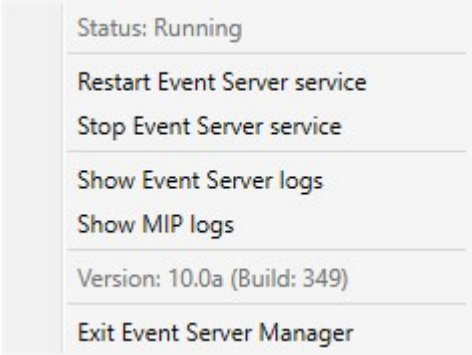
Server Configuratorの [サーバーの登録] セクションで、指定されたマネジメントサーバーのあるコンピュータ上で実行するサーバーを登録してください。

サーバーを登録するには、マネジメントサーバーのアドレスを確認し、[登録] を選択します。

イベントサーバーサービスの開始、停止、再開

Event Server Managerトレイアイコンは、[実行中]などの、イベントサーバーサービスのステータスを示します。このアイコンを使用して、イベントサーバーサービスを開始、停止、再起動できます。サービスを停止する場合は、イベントとアラームを含むシステムの一部が動作しません。ただし、ビデオの表示と録画はできます。詳細については、ページ465のイベントサーバーサービスの停止を参照してください。

1. 通知領域で、Event Server Managerアイコンを右クリックします。コンテキストメニューが表示されます。



2. サービスが停止した場合は、[イベントサーバーサービス開始]をクリックして開始します。トレイアイコンが変わり、新しい状態を示します。

3. サービスを再起動または停止するには、[イベントサーバーサービスの再起動]または[イベントサーバーサービスの停止]をクリックします。

> 詳細については、ページ460のサーバーマネージャーのトレーアイコン(説明付き)を参照してください。

イベントサーバーサービスの停止

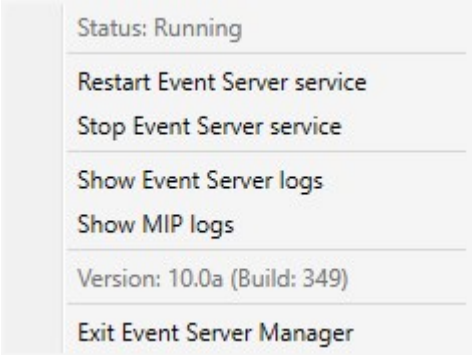
イベントサーバーにMIPプラグインをインストールするときには、まずイベントサーバーサービスを停止してから、再起動する必要があります。ただし、サービスが停止している間は、VMSシステムのほとんどの領域が機能しません。

- イベントやアラームはEvent Serverに保存されません。ただし、システムおよびデバイスイベントはこの時点でも、録画の開始などのアクションをトリガーします。
- アドオン製品は、XProtect Smart Clientにおいて動作せず、またManagement Clientから設定することはできません。
- アナリティクスイベントは動作しません。
- ジェネリックイベントは動作しません。
- アラームはトリガーされません。
- XProtect Smart Clientでは、マップビューアイテム、アラームリストビューアイテム、アラームマネージャワークスペースは動作しません。
- イベントサーバーのMIPプラグインを実行できません。
- Management ClientおよびXProtect Smart ClientのMIPプラグインは正しく動作しません。

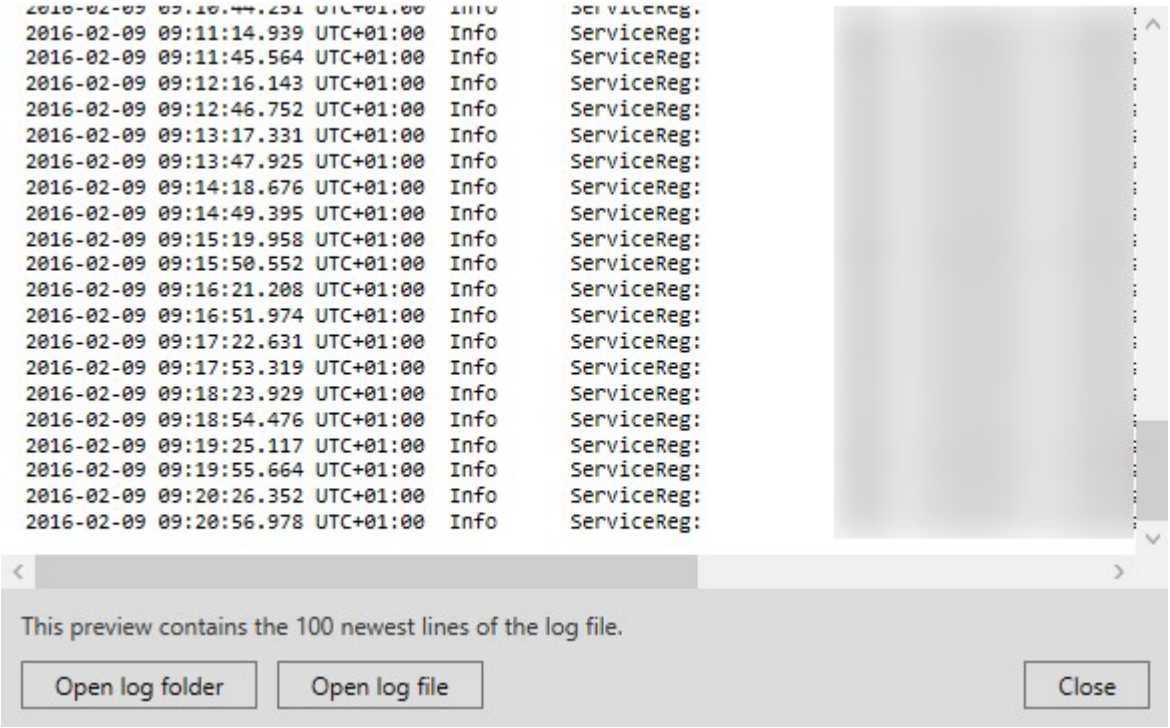
Event ServerまたはMIPログの表示

Event ServerログでEvent Serverアクティビティに関するタイムスタンプ付き情報を表示できます。サードパーティ統合に関する情報は、Event Serverフォルダーのサブフォルダーにあるログに出力されます。

1. 通知領域で、Event Server Managerアイコンを右クリックします。コンテキストメニューが表示されます。



2. イベントサーバーログで最新の100行を表示するには、[イベントサーバーログの表示]をクリックします。ログビューアが表示されます。



   1. ログファイルを表示するには、[ログファイルを開く]をクリックします。
   2. ログフォルダーを開くには、[ログフォルダーを開く]をクリックします。

3. MIPログで最新の100行を表示するには、コンテキストメニューに戻り、[MIPログの表示]をクリックします。ログビューアが表示されます。

ログディレクトリからログファイルが削除された場合、メニュー項目が灰色で表示されます。ログビューアを開くには、まず、ログファイルを次のフォルダーのいずれかにコピーする必要があります。*C:\ProgramData\Milestone\XProtect Event Server\logs* または *C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs*。

登録済みサービスの管理

場合によっては、システムとの通信機能が必要なサーバーまたはサービスのうち、システムに直接含まれていないものがあります。一部のサービスはシステムに自動的に登録できます(自動登録されないものもあります)。自動登録可能なサービス:

- イベントサーバーサービス
- ログサーバーサービス

自動登録されるサービスは、登録済みサービスのリストに表示されます。

サーバーまたはサービスは、Management Clientで登録済みサービスとして手動で指定できます。

登録済みサービスの追加と編集

1. 登録済みサービスの追加/削除ウィンドウで、必要に応じて追加または編集をクリックします。
2. 前の選択により開いた登録済みサービスの追加または登録済みサービスの編集ウィンドウで、設定を指定または編集します。
3. OK をクリックします。

ネットワーク設定の管理

ネットワーク設定で、マネジメントサーバーのサーバーLANアドレスとWANアドレスを指定し、マネジメントサーバーと信頼済みサーバーが通信できるようにします。

1. 登録されているサービスの追加と削除ウィンドウで、ネットワークをクリックします。
2. マネジメントサーバーのLANおよび/またはWAN IPアドレスを指定します。

   すべての関係するサーバー(マネジメントサーバーと信頼済みサーバーの両方)がローカルネットワークにある場合は、LANアドレスを指定するだけです。1つまたは複数の関係するサーバーがインターネット接続でシステムにアクセスする場合は、WANアドレスも指定する必要があります。

3. OK をクリックします。

登録済みサービスのプロパティ

登録済みサービスの追加または登録済みサービスの編集ウィンドウで、以下を指定します。

コンポーネント	要件
タイプ	事前に入力されているフィールド。
名前	登録されているサービスの名前です。Management Clientでは名前は表示目的でのみ使用されます。
URL	追加をクリックし、登録済みサービスのIPアドレスまたはホスト名を追加します。URLの一部としてホスト名を指定する場合、そのホストが存在し、ネットワークで使用できる必要があります。URLは*http://*または*https://*から始まるものとし、以下の文字を使用してはなりません：*< > & ' " * ? | [ ] ".* 一般的な URL 形式の例：*http://ipaddress:port/directory* (ポートおよびディレクトリはオプションです) 。必要に応じて複数のURLを追加することもできます。
信頼済み	登録済みサービスをすぐに信頼済みにすべき場合に選択します(これが大半の場合に当てはまりますが、登録済みサービスを追加してから後で、これを編集して信頼済みにすることもできます) 。 信頼済みステータスに変更すると、その登録済みサービスに定義した1つまたは複数のURLを共有する登録済みサービスの状態も変更されます。
説明	登録されているサービスの説明です。Management Clientでは、説明は表示目的でのみ使用されます。
詳細	サービスが高度な場合、定義するホストアドレスごとに特定のURIスキーマ(http、https、tcp、udpなど) を設定する必要があります。このため、ホストアドレスには複数のエンドポイントが含まれ、それぞれが独自のスキーマ、ホストアドレス、およびスキーマのIPポートを持ちます。

デバイスドライバの削除(説明付き)

デバイスドライバーがコンピュータ上で不要になった場合は、Device Packをシステムから削除できます。その場合は、プログラムを削除するWindowsの標準手順に従います。

複数のDevice Packがインストールされ、ファイルを削除してしまう問題がある場合は、Device Packのインストールフォルダーにあるスクリプトを使って完全に削除します。

デバイスドライバーを削除すると、レコーディングサーバーとカメラデバイスは通信できなくなります。アップグレード時にはDevice Packを削除しないでください。古いバージョンの上に新しいバージョンをインストールできます。システム全体をアンインストールする場合にのみ、Device Packを削除します。

レコーディングサーバーの削除

> レコーディングサーバーを削除すると、そのレコーディングサーバーに関連付けられたすべてのハードウェア(カメラ、入力デバイスなど) について、Management Clientでそのレコーディングサーバーに対して指定したあらゆる設定が削除されます。

1. 概要ペインで、削除するレコーディングサーバーを右クリックします。
2. レコーディングサーバーの削除を選択します。
3. 削除するには、はいをクリックします。
4. レコーディングサーバーと、関連するすべてのハードウェアが削除されます。

レコーディングサーバーでのすべてのハードウェアの削除

> ハードウェアを削除すると、ハードウェアに関連付けられたすべての録画データが完全に削除されます。

1. すべてのハードウェアを削除するレコーディングサーバーを右クリックします。
2. すべてのハードウェアの削除を選択します。
3. 削除を確認します。

トラブルシューティング

問題：SQL Serverとデータベースのアドレスを変更するとデータベースにアクセスできなくなる

SQL Serverを実行しているコンピュータのホスト名が変更されるなどして、SQL Serverとデータベースのアドレスが変更されると、レコーディングサーバーからデータベースへのアクセスが失われます。
解決策：**Recording Server Manager**トレーアイコンのSQLアドレス更新ツールを使用します。

問題：ポートの競合が原因でレコーディングサーバーを起動できない

この問題は、ポート25を使用する簡易メール転送プロトコル(SMTP)サービスが実行されている場合にのみ発生します。このサービスによってポート25がすでに使用されている場合は、レコーディングサーバーサービスを起動できない可能性があります。レコーディングサーバーのSMTPサービスに対してポート番号25が使用できる状態になっていることが重要です。

SMTPサービス: 確認と解決策

SMTPサービスがインストールされていることを確認するには:

1. Windowsの[スタート]メニューで[コントロールパネル]を選択します。
2. [コントロール パネル]で[プログラムの追加と削除]をダブルクリックします。
3. [プログラムの追加と削除]ウィンドウの左側で、[Windowsコンポーネントの追加と削除]をクリックします。
4. [Windowsコンポーネント]ウィザードで[インターネットインフォメーションサービス(IIS)]を選択し、[詳細]をクリックします。
5. [インターネット インフォメーション サービス (IIS)]ウィンドウで、[SMTPサービス]チェックボックスが選択されていることを確認します。選択されていれば、SMTPサービスはインストールされています。

SMTPサービスがインストールされている場合は、以下のいずれかの解決策を講じます:

解決策1: SMTPサービスを無効にするか、手動スタートアップに設定する

この解決策により、毎回SMTPサービスを停止することなく、レコーディングサーバーを起動できます:

1. Windowsの[スタート]メニューで[コントロールパネル]を選択します。
2. [コントロール パネル]で[管理ツール]をダブルクリックします。
3. [管理ツール]ウィンドウで[サービス]をダブルクリックします。
4. [サービス]ウィンドウで[簡易メール転送プロトコル (SMTP)]をダブルクリックします。

5. [SMTPプロパティ]ウィンドウで[停止]をクリックし、[スタートアップの種類]を[手動]または[無効]に設定します。

   [手動]に設定した場合、SMTPサービスを[サービス]ウィンドウから手動で、または*net start SMTPSVC*コマンドを使用してコマンドプロンプトから起動できます。

6. OK をクリックします。

解決策2: SMTPサービスを削除する

SMTPサービスを削除すると、SMTPサービスを使用している他のアプリケーションに影響が及ぶ可能性があります。

1. Windowsの[スタート]メニューで[コントロールパネル]を選択します。
2. [コントロール パネル]ウィンドウで[プログラムの追加と削除]をダブルクリックします。
3. [プログラムの追加と削除]ウィンドウの左側で、[Windowsコンポーネントの追加と削除]をクリックします。
4. [Windowsコンポーネント]ウィザードで[インターネット インフォメーション サービス(IIS)]の項目を選択し、[詳細]をクリックします。
5. [インターネット インフォメーション サービス(IIS)]ウィンドウで、[SMTPサービス]チェックボックスをオフにします。
6. [OK]、[次へ]、[終了]の順にクリックします。

問題：レコーディングサーバーが、マネジメントサーバークラスタノードを切り替える際にオフラインになる

マネジメントサーバー冗長性に対してMicrosoftクラスタを設定した場合、クラスタノード間でマネジメントサーバーを切り替える際に、レコーディングサーバーまたはレコーディングサーバーもオフラインになる場合があります。

この問題を是正するには、以下の構成設定を修正します:

マネジメントサーバーノードにおいて:

- C:\ProgramData\Milestone\XProtectマネジメントサーバー\ServerConfig.xmlで：

```
<AuthorizationServerUri>http://ClusterRoleAddress/IDP</AuthorizationServerUri>
```

- C:\Program Files\Milestone\XProtectマネジメントサーバー\IIS\IDP\appsettings.json:

```
"Authority": "http://ClusterRoleAddress/IDP"
```

レコーディングサーバーで、authorizationserveraddressもクラスタ役割アドレスに設定されていることを確認します:

C:\ProgramData\Milestone\XProtectレコーディングサーバー\RecorderConfig.xmlで：

```
<authorizationserveraddress>http://ClusterRoleAddress/IDP</authorizationserveraddress>
```

アップグレード

アップグレード(説明付き)

アップグレード時には、現在コンピュータにインストールされているすべてのコンポーネントがアップグレードされます。アップグレード中にインストール済みコンポーネントを削除することはできません。インストール済みコンポーネントを削除するには、アップグレードの前後にWindowsの[プログラムの追加と削除]機能を使用します。アップグレード時には、マネジメントサーバーデータベースを除く、すべてのコンポーネントが自動的に削除および置換されます。これにはDevice Packのドライバーも含まれます。

マネジメントサーバーデータベースは、システム全体の設定(レコーディングサーバーの設定、カメラの設定、ルールなど)を含んでいます。マネジメントサーバーデータベースを削除しない限り、システムの設定を再構成する必要はありません(ただし、新しいバージョンの新機能の設定が必要になる場合もあります)。

> 現在のバージョンに限定されている以前のXProtectバージョンのレコーディングサーバーとの互換性アクセスそのような古いレコーディングサーバー上でも録画にはアクセスできます。けれども設定を変える際には、現在と同じバージョンである必要があります。このため、Milestoneはシステムのすべてのレコーディングサーバーをアップグレードすることを強くお勧めします。

レコーディングサーバーを含めてアップグレードするときには、ビデオデバイスドライバーを更新するか保持するかを確認するメッセージが表示されます。更新を選択する場合、システムの再起動後、ハードウェアデバイスが新しいビデオデバイスドライバーと接続するまでに数分かかる場合があります。これは、新しくインストールされたドライバーについて、いくつかの内部チェックが行われるためです。

> 2017 R3以前のバージョンから2018 R1以降のバージョンへ更新する場合、ならびにお使いのシステムが古いカメラを持っている場合は、弊社のWebサイト(https://www.milestonesys.com/downloads/)のダウンロードページから、Device Packをレガシードライバーとともに、手動でダウンロードする必要があります。レガシーDevice Pack内のドライバーを使っているカメラを所有しているかをチェックするには、弊社のWebサイト(https://www.milestonesys.com/community/business-partner-tools/device-packs/)のこのページにアクセスしてください。

> 2018 R1から、あるいは2018 R2より前の、あるいは後のバージョンから更新した場合には、アップグレードを始める前に、お使いのシステムにおけるすべてのレコーディングサーバーをセキュリティパッチとともにアップデートしてください。セキュリティパッチなしでアップグレードすることは、レコーディングサーバーの失敗を招く可能性があります。

お使いのレコーディングサーバーにセキュリティパッチをインストールする方法は、弊社のWebサイトhttps://supportcommunity.milestonesys.com/s/article/XProtect- VMS- NET- security-vulnerability-hotfixes-for-2016-R1-2018-R1/を参照してください。

システム内の全レコーディング サーバーをバージョン2019 R2以降にアップグレードする場合、Milestoneでは、管理サーバー設定ファイルでUseRemotingを「False」設定するよう推奨しています。サイバー攻撃に対してXProtect VMSを保護する方法の詳細については、強化ガイドを参照してください。

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接続を暗号化する場合は、すべてのレコーディングサーバーを2019 R2以降にアップグレードしてください。

アップグレード要件

- お使いのソフトウェア ライセンス ファイル(ページ49のライセンス(説明付き) を参照) (.lic) の準備を完了させます。
  - サービスパックアップグレード: マネジメントサーバーのインストール中に、ウィザードで、ソフトウェアライセンスファイルの場所を指定しなければならない場合があります。システム(最新のアップグレード)の購入後に入手したソフトウェアライセンスコードと、最後のライセンスアクティベーションの後に入手したアクティベーション済みソフトウェアライセンスファイルの両方を使用できます。
  - バージョンアップグレード: 新しいバージョンを購入した後で、新しいソフトウェアライセンスファイルを受け取ります。マネジメントサーバーのインストール中に、ウィザードで、新しいソフトウェアライセンスファイルの場所を指定する必要があります

  続行する前に、ソフトウェアライセンスファイルがシステムで検証されます。既に追加されたハードウェアデバイスとライセンスが必要なその他のデバイスは、猶予期間に入ります。自動ライセンスアクティベーションを有効にしていない場合は(「 ページ136の自動ライセンスアクティベーションを有効にする」を参照) 、猶予期間内にライセンスを手動でアクティベートすることを忘れないでください。 ソフトウェアライセンスファイルがない場合は、XProtectのリセラーまでお問い合わせください。
- 新しい製品バージョンソフトウェアを用意してください。MilestoneWebサイトのダウンロードページからダウンロードできます。

- システム構成のバックアップを作成していることを確認してください(「ページ441のシステム設定のバックアップおよび復元について」を参照)

  マネジメントサーバーのSQLデータベースにはシステム構成が保存されます。SQLデータベースは、SQL Serverマネジメントサーバーのマシン本体、またはネットワーク上のSQL Serverに配置できます。

  SQLデータベースをネットワーク上のSQL Serverで使用する場合、SQLデータベースを作成、移動、アップグレードするには、SQL Serverにおいてマネジメントサーバーに管理者権限が必要となります。SQLデータベースの日常的な使用とメンテナンスについては、マネジメントサーバーはSQLデータベース所有者権限しか必要としません。

- インストールの間に暗号化を可能にしたい時は、該当するコンピュータに適切な認証がインストールされ信頼されている必要があります。詳細については、「ページ67の安全な通信(説明付き)」を参照してください。

アップグレードを開始する準備ができれば、「アップグレードの推奨手順」ページ475のアップグレードの推奨手順。

FIPS 140-2準拠モードで実行するようXProtect VMSをアップグレードする

2020 R3バージョンからXProtect VMSは、FIPS 140-2認定アルゴリズムのインスタンスのみを使用して実行するよう設定されています。

FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、強化ガイドのFIPS 140-2準拠セクションを参照してください。

> 非FIPS準拠暗号で暗号化されている2017 R3よりも前のXProtect VMSのバージョンからのエクスポートとアーカイブ済みメディアデータベースのあるFIPS 140-2準拠システムでは、FIPSを有効にした後でもアクセスできる場所でデータをアーカイブする必要があります。

以下のプロセスは、FIPS 140-2準拠モードで実行するようXProtect VMSを実行するには何が必要が説明しています。

1. VMSに含まれているすべてのコンピューターでWindows FIPSセキュリティポリシーを無効にします(SQLサーバーをホストしているコンピューターも含まれます)。

   アップグレードの際、FIPSがWindowsオペレーティングシステムで有効になっていると、XProtect VMSをインストールできません。

2. FIPSが有効になったWindowsオペレーティングシステムで、スタンドアロン型サードパーティ統合を実行できることを確認します。

   スタンドアロン統合はFIPS 140-2に準拠していない場合、WindowsオペレーティングシステムをFIPSモードで操作するよう設定した後は実行できません。

   これを防ぐには:

   - 以下へのあらゆるスタンドアロン統合のインベントリを作成:XProtect VMS
   - この統合のプロバイダーに連絡し、統合がFIPS 140-2準拠かどうか聞いてください
   - FIPS 140-2準拠スタンドアロン統合を展開

3. ドライバー(およびデバイスへの通信)がFIPS 140-2に準拠していることを確認します。

   XProtect VMSは、以下の基準が満たされると、確実に操作のFIPS 140-2準拠モードを強制できます。

   - デバイスは以下に接続する際、テスト済みのドライバーのみを使用します:XProtect VMS

     コンプライアンスを確保して強制できるドライバーの詳細については、強化ガイドのFIPS 140-2コンプライアンスのセクションを参照してください。

     > ドライバーモジュールは、HTTPを介した接続のFIPS140-2準拠を保証できません。接続は準拠している可能性がありますが、実際に準拠しているという保証はありません。

   - デバイスは、バージョン11.1以降のデバイスパックを使用します

     レガシードライバーのデバイスパックからのドライバーでは、FIPS 140-2に準拠した接続を保証できません。

   - デバイスはHTTPSを介して接続されるほか、ビデオストリームではHTTPSを介してSecure Real-Time Transport Protocol (SRTP)またはReal Time Streaming Protocol (RTSP)のいずれかで接続されます。

   - レコーディングサーバーを実行しているコンピュータは、FIPSモードが有効になっている状態でWindows OSを実行します。

4. メディアデータベースのデータがFIPS 140-2準拠暗号で暗号化されていることを確認します。

   これを行うには、メディアデータベースアップグレードツールを実行します。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、強化ガイドのFIPS 140-2準拠セクションを参照してください。

5. Windowsオペレーティングシステムで**FIPS**を有効にする前、また、XProtect VMSシステムを設定して、すべてのコンポーネントとデバイスがFIPSの有効な環境で実行できることを確認した後、XProtect Management Clientで既存のハードウェアのパスワードを更新します。

   これを行うには、Management Clientの[レコーディングサーバー]ノードで選択されたレコーディングサーバーから、[ハードウェアの追加...]を右クリックして選択します。[ハードウェアの追加]ウィザードを実行します。これにより、現在の資格情報がすべて更新され、FIPSに準拠するよう暗号化されます。

VMS全体(すべてのクライアントを含む)をアップグレードするまでは**FIPS**を有効にできません。

アップグレードの推奨手順

実際のアップグレードを開始する前に、SQLデータベースバックアップを含むアップグレード要件(ページ473のアップグレード要件を参照)をお読みください。

> デバイスドライバーは2つのDevice Packに分けられます:より新しいドライバーを持つレギュラーDevice Packと、古いバージョンのドライバーを持つレガシーDevice Packです。レギュラーDevice

Packは常に、更新あるいはアップグレード時に自動でインストールされます。レガシーDevice Packからのデバイスドライバーを使用する古いカメラを持っている場合、そしてレガシーDevice Packをまだインストールしていない場合、システムはレガシーDevice Packを自動でインストールしません。

お使いのシステムが古いバージョンのカメラを持っている場合は、Milestoneは、そのカメラがレガシーデバイスパックからのドライバーを使用しているかどうかを、このページ(https://www.milestonesys.com/community/business-partner-tools/device-packs/)でチェックすることを推奨しています。もしレガシーパックをすでにインストールしているかをチェックするには、XProtectシステムフォルダーをチェックします。レガシーデバイスパックをダウンロードする必要がある場合は、このダウンロードページ(https://www.milestonesys.com/downloads/)にアクセスします。

単一のコンピュータシステムの場合、新しいソフトウェアを既存のインストールの上にインストールできます。

Milestone InterconnectまたはMilestone Federated Architectureシステムにおいて、まずセントラルサイトをアップグレードし、その後リモートサイトもアップグレードしなくてはなりません。

ディストリビュートシステムにおいては、この順序でアップグレードを行います:

1. インストーラで[分散型]オプションを使用してマネジメントサーバーをアップグレードします(ページ84のシステムのインストール - カスタムオプションを参照)。
    1. コンポーネントを選択するウィザードのページでは、すべてのマネジメントサーバーコンポーネントがあらかじめ選択されています。
    2. SQL Serverとデータベースを指定します。データベース内の既存のデータを維持するため、すでに使用しているSQLデータベースを維持するかどうかを決定します。

        インストールを開始すると、フェールオーバーレコーディングサーバーの機能は失われます(ページ172のフェールオーバーレコーディングサーバー(説明付き)を参照)。

        マネジメントサーバーの暗号化を有効にすると、レコーディングサーバーは、マネジメントサーバーの暗号化を有効にするまでオフラインとなります(ページ58のインストールを開始する前にを参照)。

2. フェールオーバー レコーディングサーバーをアップグレードする。管理者サーバーのダウンロード webページから(Download Managerによりコントロールされています)、レコーディングサーバーをインストール。

> フェールオーバー レコーディングサーバーにおいて暗号化を有効にする場合、また、フェールオーバー機能を維持する場合は、暗号化をせずにフェールオーバー レコーディングサーバーをアップグレードし、レコーディングサーバーをアップグレードした後で暗号化を有効にします。

この時点で、フェールオーバーサーバー機能が復帰します。

3. レコーディングサーバー または フェールオーバー レコーディングサーバーからクライアントへの暗号化を有効にする場合は、クライアントがアップグレードの間にデータを取得することができ、また、レコーディングサーバーのアップグレードの前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すべてのクライアントとサービスをアップグレードしておくことが重要です。該当するクライアントとサービスは以下のとおりです:

   - XProtect Smart Client
   - Management Client
   - マネジメントサーバー
   - XProtect Mobileサーバー
   - XProtect Event Server
   - DLNA Server Manager
   - Milestone Open Network Bridge
   - 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
   - MIP SDK サードパーティインテグレーション

4. レコーディングサーバーをアップグレードします。レコーディングサーバーは、インストールウィザードを使用してインストール(「ページ88の新しいXProtectコンポーネントのインストール」を参照) するか、またはサイレントでインストール(「ページ88の新しいXProtectコンポーネントのインストール」を参照) できます。サイレント・インストールの利点は、遠隔で行うことができることです。

> 暗号化を可能にし、選択されたサーバー認証が該当する実行中のコンピュータで信頼されていない時は、このコンピュータは接続を失います。さらに情報が必要な時は ページ58のインストールを開始する前にを参照 。

システムの他のサイトでもこの手順を続けます。

ワークグループ設定内でのアップグレード

ドメイン設定ではなくワークグループ設定を使用する場合は、アップグレード時に以下を実行する必要があります。

1. マネジメントサーバーでローカルWindowsユーザーを作成します。
2. Windowsの[コントロールパネル]で、Data Collectorサービスを検索します。これを右クリックしてプロパティを選択し、ログオンタブを選択します。Data Collectorサービスを設定して、レコーディングサーバーで作成したローカルWindowsユーザーとして実行します。
3. マネジメントサーバーで、同じローカルWindowsユーザー(同じユーザー名とパスワード)を作成します。
4. Management Clientで、このローカルWindowsユーザーを管理者グループに追加します。

ワークグループを使用してインストールする場合は、ページ98のワークグループのインストールを参照してください。

クラスタでのアップグレード

クラスタを更新する前に、データベースのバックアップを行います。

1. クラスタにあるすべてのマネジメントサーバーで、マネジメントサーバーサービスを停止します。
2. クラスタにあるすべてのサーバーから、Management Serverをアンインストールします。
3. クラスタへのインストールの説明に従って、マネジメントサーバーをクラスタにインストールするための手順を実行します。ページ76の新しいXProtectシステムのインストールを参照してください。

> インストール時には、現在システム構成が保存されている既存のSQL Serverと既存のSQLデータベースを必ず再使用してください。システム構成は自動的にアップグレードされます。

JVCケンウッド
カスタマーサポートセンター

固定電話 0120−2727−87
携帯電話･PHS 0570−010−114
一部のIP電話など 045-450-8950
FAX 045-450-2308
〒221-0022 神奈川県横浜市神奈川区守屋町3-12

ご相談窓口におけるお客様の個人情報は、お問合せへの対応、修理およびその確認に使用し、適切に管理を行い、お客様の同意なく個人情報を第三者に提供または開示することはありません。

株式会社 JVCケンウッド・公共産業システム

〒 221-0022 神奈川県横浜市神奈川区守屋町 3-12

ホームページ https://jkpi.jvckenwood.com/

© 2021 JVCKENWOOD Public & Industrial Systems Corporation

B5A-3749-00