MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2020 R3

Bedienungsanleitung für Administratoren

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

Inhalt

Copyright, Marken und Verzichtserklärung 21

Übersicht 22

Produktübersicht 22

Haupt-Systemkomponenten 22

Managementserver 22

Aufzeichnungsserver 23

Ereignisserver 23

Protokollserver 24

SQL Servers und Datenbanken 24

Mobile Server 24

Active Directory 25

Management Client (erklärt) 25

Optionale Systemkomponenten 25

Failover-Aufzeichnungsserver 25

Failover-Management-Server 26

Clients 26

XProtect Smart Client (erklärt) 26

XProtect Mobile Client (Erklärung) 27

XProtect Web Client (erklärt) 28

Einrichtung eines verteilten Systems 28

Erweiterungen 29

XProtect Access (erklärt) 29

XProtect LPR (erklärt) 30

XProtect Smart Wall (erklärt) 31

XProtect Transact (erklärt) 32

Milestone Open Network Bridge (erklärt) 32

XProtect DLNA Server (erklärt) 32

Vom System verwendete Ports 33

Produktvergleichstabelle 46
Lizenzierung 50
Lizenzen (Erklärung) 50
Softwarelizenzcode ändern 51
Anforderungen und Hinweise 52
Sommerzeit (Erklärung) 52
Zeitserver (Erklärung) 52
Größenbegrenzung für die Datenbank 53
IPv6 und IPv4 (Erklärung) 53
Schreiben von IPv6-Adressen (Erklärung) 55
Verwendung von IPv6-Adressen in URLs 56
Virtuelle Server 56
Mehrere Management-Server (Cluster) (Erklärung) 57
Anforderungen für Cluster 57
Schützen von Aufzeichnungsdatenbanken vor Beschädigungen 58
Festplattenfehler: Schützen Sie Ihre Laufwerke 58
Windows Task-Manager: Passen Sie auf beim Beenden von Prozessen 58
Stromausfälle: Nutzen Sie eine USV 58
SQL-Datenbanktransaktionsprotokoll (Erläuterung) 59
Mindestsystemanforderungen 59
Vor dem Start der Installation 59
Server und Netzwerk vorbereiten 59
Active Directory vorbereiten 60
Installationsmethode 61
Entscheiden Sie sich für eine Version von SQL Server 63
Dienstkonto auswählen 64
Kerberos Authentifizierung (Erklärung) 64
Virus scanning exclusions (Erläuterung) 66
Wie ist XProtect VMS so zu konfigurieren, dass es im FIPS 140-2-konformen Modus läuft? 68
Bevor Sie XProtect VMS auf einem FIPS-fähigen System installieren 68

Softwarelizenzcode registrieren ... 68
Gerätetreiber (Erklärung) ... 69
Anforderungen für Offline-Installationen ... 69
Sichere Kommunikation (Erläuterung). ... 69
Verschlüsselung des Managementservers (Erläuterung): ... 70
Verschlüsselung vom Management-Server zum Aufzeichnungsserver (Erläuterung) ... 72
Verschlüsselung zwischen dem Management Server und den Data Collector Server (Erläuterung) ... 73
Verschlüsselung an alle Clients und Dienste, die Daten vom Aufzeichnungsserver abrufen (Erläuterung) ... 74
Datenverschlüsselung des mobilen Servers (Erläuterung) ... 76
Anforderungen zur Verschlüsselung mobiler Server für Clients ... 77
Installation ... 78
Installation eines neuen XProtect-Systems ... 78
Installieren Sie XProtect Essential+ ... 78
Systeminstallation - Einzel-Computer-Option ... 83
Systeminstallation - Benutzerdefiniert ... 88
Installation neuer XProtect-Komponenten ... 93
Installation über Download Manager (Erläuterung) ... 93
Installation eines Aufzeichnungsserver über Download Manager ... 94
Installation eines Failover-Aufzeichnungsservers Download Manager ... 97
Stille Installation über eine Befehlszeilenoberfläche (Erläuterung) ... 99
Automatische Installation eines Aufzeichnungsservers ... 100
Stille Installation von XProtect Smart Client ... 102
Installation für Arbeitsgruppen ... 103
Installation in einem Cluster ... 103
Download Manager/Download-Webseite ... 106
Download Manager Standardkonfiguration ... 108
Download Manager Standardinstallationsprogramme (Benutzer) ... 110
Hinzufügen/Veröffentlichen von Komponenten des Download Manager-Installationsprogramms ... 110
Ausblenden/Entfernen der Download Manager Installationsprogrammkomponenten ... 111
Installationsprogramm für Treiberpaket - muss heruntergeladen werden ... 112

Installationsprotokolldateien und Fehlersuche 113
Konfiguration 114
Navigation in Management Client 114
Übersicht über das Anmeldeverfahren 114
Management Client Fenster-Übersicht 116
Fensterübersicht 118
Menü-Übersicht 120
Menü „Datei“ 120
Menü bearbeiten 120
Ansichtsmenü 120
Aktionsmenü 121
Menü „Extras“ 121
Hilfe-Menü 121
Einstellen von Optionen für das System 121
Registerkarte „Allgemein“ (Optionen) 122
Registerkarte „Serverprotokolle“ (Optionen) 124
Registerkarte „Mailserver“ (Optionen) 125
Registerkarte „AVI-Generierung“ (Optionen) 126
Netzwerk-Registerkarte (Optionen) 127
Lesezeichen-Registerkarte (Optionen) 128
Registerkarte „Benutzereinstellungen“ (Optionen) 128
Registerkarte „Customer Dashboard" (Kunden-Dashboard) (Optionen) 128
Registerkarte Beweissicherung (Optionen) 129
Registerkarte „Audionachrichten“ (Optionen) 129
Registerkarte „Zutrittskontrolleinstellungen“ (Optionen) 130
Registerkarte „Analyseereignisse“ (Optionen) 131
Registerkarte „Alarme und Ereignisse“ (Optionen) 132
Registerkarte „Generische Ereignisse“ (Optionen) 134
Aufgabenliste für die Erstkonfiguration 136
Konfigurieren des Systems im Site-Navigationsfenster 138

Site-Navigation: Grundlagen 138
Lizenzinformationen 138
Geräteänderungen ohne Aktivierung (Erklärung) 141
So berechnet sich die Zahl der Geräteänderungen ohne Aktivierung 142
Anzeigen der Lizenzübersicht 143
Automatische Lizenzaktivierung (Erklärung) 143
Automatische Lizenzaktivierung aktivieren 144
Automatische Lizenzaktivierung deaktivieren 144
Lizenzen online aktivieren 144
Lizenzen offline aktivieren 145
Lizenzen nach Übergangszeitraum aktivieren 145
Erhalten zusätzlicher Lizenzen 146
Lizenzen für einen Austausch von Geräten 146
Site-Informationen 147
Site-Informationen bearbeiten 147
Site-Navigation: Server und Hardware 147
Site-Navigation: Server und Hardware: Aufzeichnungsserver 147
Aufzeichnungsserver (Erklärung) 147
Registrieren eines Aufzeichnungsservers 149
Ändern oder überprüfen Sie die Basiskonfiguration eines Aufzeichnungsservers 150
Das Fenster mit den Einstellungen des Aufzeichnungsservers 152
Verschlüsselungsstatus an Clients anzeigen 153
Aufzeichnungsserver-Statussymbole 154
Registerkarte „Info“ (Aufzeichnungsserver) 155
Eigenschaften der Registerkarte Info (Aufzeichnungsserver) 156
Registerkarte „Speicher“ (Aufzeichnungsserver) 157
Lagerung und Archivierung (Erklärung) 158
Geben Sie an, wie das System sich verhalten soll, wenn kein Speicherplatz für Aufzeichnungen verfügbar ist 162
Einen neuen Speicher hinzufügen 163
Erstellen eines Archivs in einem Speicher 164

Anbinden eines Geräts oder eine Gruppe von Geräten an einen Speicher ... 164
Bearbeiten der Einstellungen für einen ausgewählten Speicher oder ein ausgewähltes Archiv ... 165
Digitale Signaturen für Export aktivieren ... 165
Verschlüsseln Sie Ihre Aufzeichnungen ... 166
Sichern archivierter Aufzeichnungen ... 168
Archivstruktur (Erklärung) ... 169
Löschen eines Archivs aus einem Speicher ... 171
Löschen eines Speichers ... 171
Verschieben nicht archivierter Aufzeichnungen von einem Speicher in einen anderen ... 172
Speicher- und Aufzeichnungseinstellungen (Eigenschaften) ... 172
Eigenschaften der Archiveinstellungen ... 174
Registerkarte „Failover" (Aufzeichnungsserver) ... 175
Zuweisen von Failover-Aufzeichnungsservern ... 176
Eigenschaften der Registerkarte „Failover" ... 178
Registerkarte „Multicast" (Aufzeichnungsserver) ... 178
Multicasting (Erklärung) ... 180
Aktivieren Sie Multicasting für den Recording-Server ... 181
Zuweisen eines IP-Adressbereichs ... 182
Festlegen von Datagramm-Optionen ... 182
Aktivieren von Multicasting für einzelne Kameras ... 183
Registerkarte „Netzwerk" (Aufzeichnungsserver) ... 183
Wozu dient eine öffentliche Adresse? ... 183
Festlegen von öffentlichen Adressen und Ports ... 184
Zuweisen lokaler IP-Bereiche ... 184
Site-Navigation: Server und Hardware: Failover-Server ... 184
Failover-Aufzeichnungsserver (Erklärung) ... 184
Failover-Schritte (Erklärung) ... 186
Die Funktionalität der Failover-Aufzeichnungsserver (Erklärung) ... 188
Failover-Aufzeichnungsserver einrichten und aktivieren ... 189
Gruppieren von Failover-Aufzeichnungsservern für Cold-Standby ... 190

Bedeutung von Failover-Aufzeichnungsserver-Statussymbolen 190
Registerkarte Multicast (Failover-Server) 191
Eigenschaften der Registerkarte "Info" (Failover-Server) 192
Eigenschaften der Registerkarte "Info" (Failover-Gruppe) 194
Eigenschaften der Registerkarte "Sequenz" (Failover-Gruppe) 194
Failover-Aufzeichnugnsserver-Dienst (Erklärung) 194
Verschlüsselungsstatus auf einem Failover-Aufzeichnungsserver anzeigen 195
Anzeigen von Statusmeldungen 196
Anzeigen von Versionsinformationen 197
Site-Navigation: Server und Hardware: Hardware 197
Hardware (Erklärung) 197
Hardware hinzufügen 197
Hardwarevorkonfiguration (Erklärung) 199
Deaktivieren/Aktivieren von Hardware 200
Hardware bearbeiten 200
Aktivieren/Deaktivieren einzelner Geräte 204
Einrichten einer sicheren Verbindung zur Hardware 205
Aktivieren von PTZ auf einem Videoencoder 205
Hardware verwalten 206
Registerkarte „Info (Hardware)“ 206
Registerkarte Einstellungen (Hardware) 207
Registerkarte „PTZ (Videoencoder)“ 208
Gerätepasswortverwaltung (Erklärung) 208
Passwörter auf Hardwaregeräten ändern 209
Firmware Update für ein Gerät (Erläuterung) 210
Firmware auf einem Hardwaregerät aktualisieren 211
Site-Navigation: Server und Hardware: Verwalten von Remote-Servern 212
Registerkarte „Info (Remote-Server)“ 212
Registerkarte "Einstellungen" (Remote Server) 213
Registerkarte „Ereignisse (Remote-Server)“ 213

Registerkarte „Fernabfrage“ ... 213
Site-Navigation: Geräte: Arbeiten mit Geräten ... 214
Geräte (Erklärung) ... 215
Kameraregeräte (Erklärung) ... 215
Mikrofongeräte (Erklärung) ... 216
Lautsprecher-Geräte (Erklärung) ... 217
Metadaten-Geräte (Erklärung) ... 218
Eingabegeräte (Erklärung) ... 219
Manuelle Eingabeaktivierung zum Test ... 220
Ausgabegeräte (Erklärung) ... 220
Manuelle Ausgabeaktivierung zum Test ... 221
Aktivieren/Deaktivieren von Geräten über Gerätegruppen ... 222
Statussymbole von Geräten ... 222
Site-Navigation: Geräte: Verwendung von Gerätegruppen ... 224
Eine Gerätegruppe hinzufügen ... 225
Bestimmen, welche Geräte die Gruppe beinhalten soll ... 226
Bestimmen Sie die allgemeinen Eigenschaften für alle Geräte in einer Gerätegruppe ... 226
Site-Navigation: Registerkarten für Geräte ... 227
Registerkarte „Info (Geräte)“ ... 227
Registerkarte Info (Erklärung) ... 227
Registerkarte „Info“ (Eigenschaften) ... 228
Registerkarte „Einstellungen“ (Geräte) ... 230
Registerkarte Einstellungen (Erklärung) ... 230
Kamera-Einstellungen (Erklärung) ... 231
Registerkarte „Streams“ (Geräte) ... 232
Registerkarte Streams (Erklärung) ... 232
Multistreaming (Erklärung) ... 233
Stream hinzufügen ... 234
Registerkarte „Aufzeichnen“ (Geräte) ... 235
Registerkarte Aufzeichnung (erklärt) ... 235

Aufzeichnung aktivieren oder deaktivieren ... 237
Aktivieren der Aufzeichnung auf zugehörigen Geräten ... 237
Voralarm-Puffer (Erklärung) ... 237
Geräte, die Voralarm-Puffern unterstützen ... 238
Speicherort der temporären Voralarm-Puffer-Aufzeichnungen ... 238
Verwalten von Voralarm-Puffern ... 238
Manuelle Aufzeichnung verwalten ... 239
Bildrate der Aufzeichnung festlegen ... 240
Keyframe-Aufzeichnung aktivieren ... 240
Speicherort (Erklärung) ... 240
Umzug mit Geräten von einem Speicher zu einem anderen ... 242
Fernaufzeichnung (Erklärung) ... 242
Registerkarte „Bewegung" (Geräte) ... 243
Registerkarte Bewegung (Erklärung) ... 243
Aktivieren und Deaktivieren von Bewegungserkennung ... 246
Festlegen der Einstellungen für die Bewegungserkennung ... 246
Hardwarebeschleunigung (Erklärung) ... 246
Manuelle Empfindlichkeit aktivieren ... 248
Schwellenwert festlegen ... 248
Keyframe-Einstellungen auswählen ... 249
Bildverarbeitungsintervall auswählen ... 249
Erkennungsauflösung festlegen ... 249
Erzeugung von Bewegungsdaten für Smart Search ... 249
Ausschlussbereiche bestimmen ... 250
Registerkarte „Voreinstellungen" (Geräte) ... 251
Registerkarte Voreinstellungen (Erklärung) ... 251
Hinzufügen einer Preset-Position (Typ 1) ... 253
Verwendung der Preset Positionen der Kamera (Typ 2) ... 255
Zuweisen einer standardmäßigen Preset Position ... 255
Bearbeiten einer Preset-Position (nur Typ 1) ... 255

Umbenennen einer Preset Position (nur Typ 2) 257
Sperren einer Preset Position 257
Testen einer Preset-Position (nur Typ 1) 258
Reservierte PTZ-Sitzungen (Erklärung) 258
PTZ-Sitzung freigeben 258
Festlegen von PTZ-Sitzungs-Zeitüberschreitungen 258
PTZ-Sitzungs-Eigenschaften 259
Registerkarte „Wachrundgang" (Geräte) 260
Registerkarte Wachrundgang (Erklärung) 260
Hinzufügen eines Wachrundgangprofils 262
Festlegen von Preset-Positionen in einem Wachrundgangprofil 262
Festlegen der Zeit in jeder Preset Position 263
Übergänge anpassen (PTZ) 263
Festlegen einer Endposition 264
Manueller Wachrundgang (Erklärung) 265
Eigenschaften manueller Wachrundgänge 265
Registerkarte „Fischaugen-Linse" (Geräte) 266
Registerkarte Fischaugen-Linse (Erklärung) 266
Unterstützung für Fischaugen-Linse aktivieren und deaktivieren 267
Einstellungen für Fischaugen-Linse bestimmen 267
Registerkarte „Ereignisse" (Geräte) 268
Registerkarte Ereignisse (Erklärung) 268
Ein Ereignis hinzufügen 268
Ereigniseigenschaften festlegen 269
Verwenden von mehreren Instanzen eines Ereignisses 269
Registerkarte „Ereignis" (Eigenschaften) 269
Registerkarte „Client" (Geräte) 270
Registerkarte Client (Erklärung) 270
Eigenschaften der Registerkarte „Client" 271
Registerkarte Einrichtung von Privatsphärenausblendung (Geräte) 273

Registerkarte Privatsphärenausblendung (Erklärung) 273
Privatsphärenausblendung (Erklärung) 275
Aktivieren/Deaktivieren von Privatsphärenausblendung 277
Privatzonenmasken festlegen 277
Benutzerberechtigung zum Aufheben von Privatzonenmasken erteilen 278
Ändern des Timeout für aufgehobene Privatzonenmasken 279
Erstellen Sie einen Bericht von der Konfiguration Ihrer Privatsphärenausblendung 280
Registerkarte Privatsphärenausblendung (Eigenschaften) 281
Site-Navigation: Clients 283
Clients (Erklärung) 283
Site-Navigation: Clients: Konfigurieren von Smart Wall 284
XProtect Smart Wall Lizenzierung 284
Smart Walls konfigurieren 285
Benutzerrechte einrichten für XProtect Smart Wall 287
Verwendung von Regeln mit Smart Wall-Voreinstellungen (Erklärung). 288
Smart Wall Eigenschaften 288
Registerkarte „Info" (Smart Wall-Eigenschaften) 288
Registerkarte „Voreinstellungen" (Smart Wall-Eigenschaften) 289
Registerkarte „Layout" (Smart Wall-Eigenschaften) 290
Bildschirmeigenschaften 290
Registerkarte „Info" (Bildschirmeigenschaften) 290
Registerkarte „Voreinstellungen" (Bildschirmeigenschaften) 292
Site-Navigation: Clients: Ansichtsgruppen 292
Ansichtsgruppen und Rollen anzeigen (Erklärung) 293
Ansichtsgruppe hinzufügen 293
Site-Navigation: Clients: Smart Client Profile 293
Hinzufügen und Konfigurieren eines Smart Client-Profils 294
Kopieren eines Smart Client-Profils 294
Erstellen und Einrichten von Smart Client-Profilen, Rollen und Zeitprofilen 295
Einrichtung des vereinfachten Modus als Standardmodus 295

Verhinderung des Umschaltens zwischen dem einfachen und dem erweiterten Modus durch Anwender 297
Smart Client-Profileigenschaften 298
Registerkarte „Info" (Smart Client-Profile) 298
Registerkarte Allgemein (Smart Client-Profile) 298
Registerkarte Erweitert (Smart Client-Profile) 299
Registerkarte „Live" (Smart Client-Profile) 300
Registerkarte „Wiedergabe" (Smart Client-Profile) 300
Registerkarte Einrichtung (Smart Client-Profile) 301
Registerkarte „Export" (Smart Client-Profile) 301
Registerkarte „Zeitachse" (Smart Client-Profile) 301
Registerkarte Zutrittskontrolle (Smart Client-Profile) 301
Registerkarte Alarm-Manager (Smart Client-Profile) 302
Registerkarte „Smart Map" (Smart Client-Profile) 302
Registerkarte „Layout-Ansicht" (Smart Client-Profile) 303
Site-Navigation: Clients: Management Client Profile 303
Hinzufügen und Konfigurieren eines Management Client-Profils 304
Kopieren eines Management Client-Profils 304
Management Client-Profileigenschaften 304
Registerkarte „Info" (Management Client-Profile) 304
Registerkarte „Profil" (Management Client-Profile) 305
Site-Navigation: Clients: Konfigurieren von Matrix 308
Matrix Empfänger hinzufügen 308
Regeln dafür festlegen, wie Videoaufzeichnungen an Matrix-Empfänger gesendet werden 309
Dasselbe Video an mehrere XProtect Smart Client Ansichten senden 309
Site-Navigation: Regeln und Ereignisse 310
Regeln und Ereignisse (Erklärung) 310
Aktionen und Stopp-Aktionen (Erklärung) 312
Ereignisübersicht 328
Regeln 340
Regeln (Erklärung) 340

Standardregeln (Erklärung) 341
Regelkomplexität (Erklärung) 345
Validierung von Regeln (Erklärung) 346
Hinzufügen einer Regel 347
Bearbeiten, Kopieren und Umbenennen einer Regel 349
Deaktivieren und Aktivieren einer Regel 349
Wiederholte Zeit 349
Zeitprofile 350
Bestimmen eines Zeitprofils 351
Bearbeiten eines Zeitprofils 352
Zeitprofil für Tageslänge (Erklärung) 353
Hinzufügen eines Tageslängen-Zeitprofils 353
Eigenschaften der Tageslängen-Zeitprofile 354
Benachrichtigungsprofile 354
Benachrichtigungsprofile (Erklärung) 354
Anforderungen an die Erstellung von Benachrichtigungsprofilen 354
Hinzufügen von Benachrichtigungsprofilen 355
Auslösen von E-Mailbenachrichtigungen durch Regeln 357
Benachrichtigungsprofil (Eigenschaften) 357
Benutzerdefinierte Ereignisse 360
Benutzerdefinierte Ereignisse (Erklärung) 360
Benutzerdefiniertes Ereignis hinzufügen 361
Ein benutzerdefiniertes Ereignis umbenennen 362
Analyseereignisse 362
Analyseereignisse (Erklärung) 362
Ein Analyseereignis hinzufügen und bearbeiten 363
Ein Analyseereignis testen 363
Analyseereignisse testen (Eigenschaften) 364
Einstellungen für Analyseereignisse bearbeiten 367
Generische Ereignisse 367

Generische Ereignisse (Erklärung) 367
Hinzufügen eines generischen Ereignisses 368
Generisches Ereignis (Eigenschaften) 368
Generisches Ereignis: Datenquelle (Eigenschaften) 371
Site-Navigation: Sicherheit 373
Regeln (Erklärung) 373
Rechte einer Rolle (Erklärung) 373
Benutzer (Erklärung) 374
Hinzufügen und Verwalten einer Rolle 376
Kopieren, Umbenennen oder Löschen einer Rolle 376
Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen 377
Effektive Rollen anzeigen 378
Rolleneinstellungen 379
Registerkarte „Info“ (Rollen) 379
Benutzer und Gruppen-Registerkarte (Rollen) 381
Registerkarte „Gesamtsicherheit“ (Rollen) 381
Registerkarte „Geräte“ (Rollen) 409
PTZ-Registerkarte (Rollen) 417
Registerkarte „Sprache“ (Rollen) 419
Registerkarte „Fernaufzeichnungen“ (Rollen) 419
Smart Wall Registerkarte (Rollen) 420
Registerkarte „Externes Ereignis“ (Rollen) 420
Registerkarte „Ansichtsgruppe“ (Rollen) 421
Registerkarte „Server“ (Rollen) 421
Matrix Registerkarte (Rollen) 422
Registerkarte „Alarme“ (Rollen) 422
Registerkarte „Zutrittskontrolle“ (Rollen) 423
Registerkarte „LPR“ (Rollen) 423
MIP Registerkarte (Rollen) 424
Basisnutzer (Erklärung) 424

Erstellen von Basisnutzer ... 424
Site-Navigation: System-Dashboard ... 425
System-Dashboard (Erklärung) ... 425
Systemmonitor (Erklärung) ... 426
Dashboard anpassen ... 427
Systemmonitor-Details (Erklärung) ... 428
Schwellenwerte des Systemmonitors (Erklärung) ... 429
Schwellenwerte des Systemmonitors einstellen ... 432
Beweissicherung (Erklärung) ... 433
Derzeitige Aufgaben (Erklärung) ... 435
Konfigurationsberichte (Erklärung) ... 436
Einen Konfigurationsbericht hinzufügen ... 436
Berichtdetails konfigurieren ... 436
Site-Navigation: Server-Protokolle ... 437
Protokolle (erklärt) ... 437
Filterprotokolle ... 437
Protokolle exportieren ... 438
2018 R2 und früheren Komponenten erlauben, Protokolle aufzuzeichnen ... 439
Systemprotokolle (Eigenschaften) ... 440
Auditprotokoll (Eigenschaften) ... 440
Regelausgelöste Protokolle (Eigenschaften) ... 441
Seitennavigation: Verwendung von Metadaten ... 442
Was sind Metadaten? ... 442
Metadatensuche (Erklärung) ... 442
Suchanforderungen für Metadaten ... 443
Lassen Sie sich die Suchkategorien und Suchfilter für Metadaten anzeigen, in XProtect Smart Client ... 443
Site-Navigation: Alarme ... 443
Alarme (Erklärung) ... 444
Alarmkonfiguration (Erklärung) ... 445
Alarmdefinitionen ... 446

Hinzufügen eines Alarms 446
Alarmdefinitionen (Eigenschaften) 448
Alarmdateneinstellungen 450
Toneinstellungen 452
Verschlüsselung aktivieren 453
Die Verschlüsselung zum und vom Managementserver aktivieren 453
Verschlüsselung für Aufzeichnungsserver oder Remote Server aktivieren 455
Verschlüsselung zu Clients und Servern aktivieren 456
Aktivieren Sie die Verschlüsselung auf dem mobilen Server. 458
Verschlüsselungsstatus an Clients anzeigen 460
Konfigurieren von Milestone Federated Architecture 461
Einrichten Ihres Systems für föderale Standorte 465
Hinzufügen eines Standorts zur Hierarchie 467
Zustimmen der Aufnahme in die Hierarchie 468
Festlegen von Standorteigenschaften 468
Standorthierarchie aktualisieren 469
Anmelden an anderen Standorten in der Hierarchie 470
Trennen eines Standorts von der Hierarchie 470
Eigenschaften für einen föderalen Standort 470
Allgemein 470
Registerkarte „Übergeordneter Standort“ 471
Konfigurieren von Milestone Interconnect 472
Auswahl von Milestone Interconnect oder Milestone Federated Architecture (Erklärung) 472
Milestone Interconnect und Lizenzierung 473
Milestone Interconnect (erklärt) 473
Milestone Interconnect-Einrichtungen (Erklärung) 475
Einen Remote-Standort zum zentralen Milestone Interconnect-Standort hinzufügen 476
Benutzerrechte zuweisen 478
Hardware des Remote-Systems aktualisieren 478
Die Remote-Desktop-Verbindung zum Remote-Systeminstallation aufbauen 478

Aktivieren der direkten Wiedergabe von der Kamera am Remote-System 479
Abruf von Fernaufzeichnungen von Kamera an Remote-System 479
Konfigurieren Sie Ihren zentralen Standort, so dass er auf Ereignisse von Remote-Systemen reagiert 480
Konfigurieren von Fernzugriffsdiensten 481
Installieren Sie die STS-Umgebung für die One-Click-Kameraverbindung 482
STS hinzufügen/bearbeiten 483
Registrieren Sie eine neue Axis One-Click-Kamera 483
Verbindungseigenschaften der Axis One-Click-Kamera 484
Konfigurieren einer Smart Map 485
Geographische Hintergründe (Erklärung) 485
Erwerben Sie einen API-Schlüssel für Google Maps oder Bing Maps 486
Google Maps 486
Bing Maps 486
Aktivieren Sie Bing Maps oder Google Maps in Management Client 486
Aktivieren Sie Bing Maps oder Google Maps in XProtect Smart Client 487
Geben Sie den OpenStreetMap Tile Server an 487
Zwischengespeicherte Smart Map Dateien (Erklärung) 488
Aktivieren der Smart Map-Bearbeitung 489
Aktivieren der Kamerabearbeitung in Smart Map 490
Festlegen von Position, Ausrichtung, Sichtfeld und Tiefe einer Kamera (Smart Map) 490
Smart Map einrichten mit Milestone Federated Architecture 492
Wartung 494
Sicherung und Wiederherstellung einer Systemkonfiguration 494
Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung) 494
Gemeinsamen Sicherungsordner auswählen 495
Manuelle Sicherung der Systemkonfiguration 495
Wiederherstellen einer Systemkonfiguration aus einer manuellen Sicherung 495
Passwort für die Systemkonfiguration (Erklärung) 497
Passworteinstellungen für die Systemkonfiguration 497
Die Passworteinstellungen für die Systemkonfiguration ändern 498

Geben Sie die Einstellungen für das Passwort für die Systemkonfiguration ein (Wiederherstellung) 499
Manuelle Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung) 499
Sicherung und Wiederherstellung der Event-Server-Konfiguration (Erklärung) 500
Planmäßige Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung) 500
Sicherung der Systemkonfiguration mit planmäßiger Sicherung 501
Wiederherstellen einer Systemkonfiguration aus einer planmäßigen Sicherung 501
Sicherung der SQL-Datenbank des Protokollservers 502
Fehler bei der Sicherung und Wiederherstellung sowie weitere Problemfälle (Erklärung) 502
Den Management-Server bewegen 503
Nicht verfügbare Management-Server (Erklärung) 504
Verschieben der Systemkonfiguration 504
Ersetzen eines Aufzeichnungsservers 505
Hardware verschieben 506
Hardware verschieben (Assistent) 507
Hardware ersetzen 510
Verwaltung des SQL Server und der Datenbanken 513
Ändern des SQL Server und der Datenbankadressen (Erläuterung) 513
Ändern der SQL Server und der Datenbank des Protokollservers 514
Ändern der SQL-Adressen des Management-Servers und des Event-Servers 514
Serverdienste verwalten 515
Taskleistensymbole für den Servermanager (Erläuterung) 515
Starten oder Stoppen des Managementserver-Dienstes 520
Starten oder Stoppen des Aufzeichnungsserver-Dienstes 521
Statusmeldungen für Management-Server oder Aufzeichnungsserver ansehen 522
Verschlüsselung verwalten mit dem Server Configurator 522
Den Ereignisserver Dienst starten, anhalten oder neu starten 523
Den Ereignisserver-Dienst stoppen 524
Event Server oder MIP-Protokolle anzeigen 524
Verwaltung registrierter Dienste 525
Registrierte Dienste hinzufügen und bearbeiten 526

Netzwerkkonfiguration verwalten 526
Eigenschaften registrierter Dienste 526
Entfernen von Gerätetreibern (Erklärung) 527
Deinstallieren eines Aufzeichnungsservers 528
Löschen sämtlicher Hardware auf einem Aufzeichnungsserver 528
Fehlerbehandlung 529
Problem: Änderungen von SQL Server und Datenbankadressen verhindern den Zugriff auf die Datenbanken 529
Problem: Aufzeichnungsserver läuft aufgrund eines Portkonflikts nicht an 529
Problem: Aufzeichnungsserver geht beim Umschalten auf Managementserver Clusterknoten offline 530
Upgrade 531
Upgrade (Erklärung) 531
Upgrade-Anforderungen 532
Aktualisieren Sie XProtect VMS. damit Ihr System im FIPS 140-2-konformen Modus läuft 533
Optimale Vorgehensweise beim Upgrade 535
Upgrade in einem Arbeitsgruppen-Setup 537
Upgrade in einem Cluster 537

Copyright, Marken und Verzichtserklärung

Marken

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

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

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

Haftungsausschluss

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

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

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

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

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

Übersicht

Produktübersicht

Die XProtect VMS-Produkte sind Videomanagementsoftware für Installationen jeder Art und Größe. Ganz gleich, ob Sie Ihr Geschäft vor Vandalismus schützen oder eine Hochsicherheitsinstallation mit mehreren Standorten verwalten möchten – XProtect macht es möglich. Die Lösungen bieten eine zentralisierte Verwaltung aller Geräte, Server und Benutzer und stellen ein äußerst flexibles Regelsystem bereit, das von Zeitplänen und Ereignissen gesteuert wird.

Ihr System umfasst folgende Hauptkomponenten:

- Den **Management-Server** – das Zentrum Ihrer Installation, das aus mehreren Servern besteht
- Einen oder mehrere **Aufzeichnungsserver**
- Eine oder mehrere Installationen von **XProtect Management Client**
- **XProtect Download Manager**
- Eine oder mehrere Installationen von **XProtect® Smart Client**
- Eine oder mehrere Verwendungen von **XProtect Web Client** und/oder Installationen des **XProtect Mobile** Clients, falls erforderlich

Das System umfasst zudem die vollintegrierte Matrix-Funktionalität für die dezentrale Anzeige von Videos einer beliebigen Kamera in Ihrem Überwachungssystem auf einem Computer, auf dem XProtect Smart Client installiert ist.

Sie können Ihr System in einer verteilten Einrichtung auf virtualisierten Servern oder auf mehreren physischen Servern installieren. Siehe auch Einrichtung eines verteilten Systems auf Seite 28.

Darüber hinaus bietet das System die Möglichkeit, beim Exportieren von Videobeweisbildern vom XProtect Smart Client die Standalone-Lösung XProtect® Smart Client – Player mit einzubeziehen. XProtect Smart Client – Player ermöglicht es den Empfängern von Videobeweisbildern (z. B. Polizeibeamte, interne oder externe Ermittler usw.), die exportierten Aufzeichnungen zu durchsuchen und wiederzugeben, ohne Software auf ihrem Computer zu installieren.

Wenn die funktionsreichsten Produkte installiert sind (siehe Produktvergleichstabelle auf Seite 46), kann Ihr System eine unbegrenzte Zahl von Kameras, Servern und Benutzern an mehreren Standorten unterstützen. Das System unterstützt sowohl IPv4 als auch IPv6.

Haupt-Systemkomponenten

Managementserver

Der Management-Server ist die zentrale Komponente des VMS-Systems. Er speichert die Konfiguration des Überwachungssystems in einer SQL-Datenbank, entweder auf einem SQL Server auf dem Computer des Management-Servers selbst oder auf einem eigenen SQL Server im Netzwerk. Außerdem verwaltet er unter

anderem die Benutzeranmeldungen, Benutzerrechte und das Regelsystem. Zur Verbesserung der Systemleistung können Sie mehrere Management-Server als Milestone Federated Architecture™ ausführen. Der Management-Server wird als Dienst ausgeführt und wird üblicherweise auf einem eigenen Server installiert.

Benutzer stellen für die anfängliche Authentifizierung eine Verbindung zum Management-Server und anschließend – für Zugriff auf Videoaufzeichnungen usw. – eine transparente Verbindung zu den Aufzeichnungsservern her.

Aufzeichnungsserver

Der Aufzeichnungsserver ist für die Kommunikation mit den Netzwerkkameras und Videoencodern, die Aufzeichnung der abgerufenen Audio- und Videoinhalte sowie die Bereitstellung von Client-Zugriff auf Live- basierte und aufgezeichnete Audio- und Videoinhalte verantwortlich. Außerdem sorgt der Aufzeichnungsserver für die Kommunikation mit anderen Milestone-Produkten mittels der Milestone Interconnect-Technologie.

Gerätetreiber

- Netzwerkkameras und Videoencodern kommunizieren über einen Gerätetreiber, der speziell für einzelne Geräte oder eine Serie ähnlicher Geräte des gleichen Herstellers entwickelt wurde.
- Ab der Ausgabe 2018 R1 sind die Gerätetreiber in zwei Gerätepacks aufgeteilt: das reguläre Gerätepaket mit neueren Treibern und ein Stamm-Gerätepaket mit älteren Treibern
- Das reguläre Gerätepaket wird automatisch installiert, wenn Sie den Aufzeichnungsserver installieren. Später können Sie die Treiber aktualisieren, indem Sie eine neuere Version des Gerätepakets herunterladen und installieren
- Das Stammgerätepaket kann nur installiert werden, wenn ein reguläres Gerätepaket im System installiert ist. Die Treiber aus dem Stammgerätepaket werden automatisch installiert, wenn eine vorige Version bereits auf Ihrem System installiert ist. Sie steht auf der Software-Download-Seite (https://www.milestonesys.com/downloads/) zum manuellen Herunterladen und Installieren zur Verfügung.

Mediendatenbank

- Die abgerufenen Audio- und Videodaten werden vom Recording-Server in der maßgeschneiderten Hochleistungs-Mediendatenbank gespeichert, die für das Aufzeichnen und Speichern von Audio- und Videodaten optimiert ist.
- Die Mediendatenbank unterstützt verschiedene einzigartige Funktionen wie abgestufte mehrstufige Archivierung, Videoausdünnung, Verschlüsselung und das Hinzufügen einer digitalen Signatur zu den Aufzeichnungen.

Ereignisserver

Der Event-Server verarbeitet zahlreiche Aufgaben, die sich auf Ereignisse, Alarme, Karten und Drittanbieter-Integrationen über den MIP SDK beziehen.

Ereignisse

- Alle Systemereignisse werden auf einem Event-Server konsolidiert, sodass Partner Integrationen zur

Nutzung von Systemereignissen an einem Ort und über eine Schnittstelle vornehmen können

- Zudem ermöglicht der Event-Server Dritten über die Schnittstellen für generische Ereignisse oder Analyseereignisse das Senden von Ereignissen an das System

Alarme

- Der Event-Server hostet die Alarmfunktion, Alarmlogik und den Alarmstatus und verwaltet die Alarmdatenbank. Die Alarmdatenbank wird in derselben SQL-Datenbank gespeichert, der auch vom Management-Server verwendet wird

Karten

- Zudem hostet der Event-Server jene Karten, die im XProtect Smart Client konfiguriert und verwendet werden

MIP SDK

- Abschließend können auf dem Event-Server Plug-ins von Dritten installiert werden und Zugriff auf Systemereignisse erhalten

Protokollserver

Der Log-Server speichert alle Protokollnachrichten für das gesamte System in einer SQL-Datenbank. Diese SQL-Datenbank für Protokollmeldungen kann auf demselben SQL Server vorhanden sein wie die SQL-Datenbank für die Management-Server Systemkonfiguration, oder auf separaten SQL Server. Der Log-Server ist typischerweise auf dem selben Server installiert wie der Management-Server, kann jedoch auch auf einem separaten Server installiert sein, um die Leistung des Management- oder Log-Servers zu erhöhen.

SQL Servers und Datenbanken

Der Management-Server, der Event-Server und der Protokollserver speichern z.B. die Systemkonfiguration, Alarme Ereignisse und Protokollmeldungen in SQL-Datenbanken auf einer oder mehreren SQL Server-Installationen. Der Management-Server und der Event-Server verwenden dieselbe SQL-Datenbank, während der Protokollserver eine eigene SQL-Datenbank hat. Das System Installationsprogramm enthält Microsoft SQL Server Express, eine kostenlose Version von SQL Server.

Für sehr große Systeme, oder für Systeme mit vielen Transaktionen zu und von den SQL-Datenbanken, empfiehlt Milestone Ihnen, eine Microsoft® SQL Server® Standard oder Microsoft® SQL Server® Enterprise-Ausgabe von SQL Server auf einem eigenen Computer im Netzwerk und auf einem bestimmten Festplattenlaufwerk zu verwenden, das für keine anderen Zwecke verwendet wird. Die Installation von SQL Server auf einem eigenen Laufwerk verbessert die Leistung des gesamten Systems.

Mobile Server

Der mobile Server sorgt dafür, dass XProtect Mobile-Client und XProtect Web Client-Benutzer Zugriff auf das System erhalten.

Der mobile Server dient nicht nur als System-Gateway für die beiden Clients, sondern kann auch Video transcodieren, da der ursprüngliche Videostream einer Kamera für die Bandbreite, die Client-Benutzern zur Verfügung steht, oft zu groß ist.

Wenn Sie eine **Verteilte** oder **Benutzerdefinierte** Installation vornehmen, empfiehlt Milestone die Installation des mobilen Servers auf einem eigenen Server.

Active Directory

Active Directory ist ein verteilter Verzeichnisdienst, der von Microsoft für Windows-Domänennetzwerke implementiert wird. Dieser Dienst ist in den meisten Windows Server-Betriebssystemen enthalten. Er identifiziert die Ressourcen in einem Netzwerk, sodass Benutzer oder Anwendungen darauf zugreifen können.

Wenn der Dienst installiert ist, können Sie Windows-Benutzer aus Active Directory hinzufügen. Außerdem haben Sie die Möglichkeit, Basisnutzer ohne Active Directory hinzuzufügen. Im Zusammenhang mit Basisnutzer gelten bestimmte Systemeinschränkungen.

Management Client (erklärt)

Umfassend ausgestatteter Administrations-Client für die Konfiguration und die tagtägliche Verwaltung des Systems. In mehreren Sprachen verfügbar.

Wird üblicherweise auf der Administrator-Workstation des Überwachungssystems o. ä. installiert.

Eine genaue Übersicht über den Management Client finden Sie in der Navigation in Management Client auf Seite 114.

Optionale Systemkomponenten

Die folgenden Komponenten sind nicht Pflicht, aber es sind Komponenten, die Sie für verschiedene Zwecke hinzufügen können.

Failover-Aufzeichnungsserver

Der Failover-Aufzeichnungsserver übernimmt das Aufzeichnen, sollte einer der Aufzeichnungsserver ausfallen.

Der Failover-Aufzeichnungsserver kann in zwei Modi betrieben werden:

- Cold-Standby für die Überwachung mehrerer Aufzeichnungsserver
- Hot-Standby für die Überwachung eines einzelnen Aufzeichnungsservers

Der Unterschied zwischen den Modi Cold- und Hot-Standby ist, dass der Failover-Aufzeichnungsserver im Modus Cold-Standby nicht weiß, von welchem Server er die Aufzeichnung übernehmen wird, sodass er erst starten kann, wenn ein Aufzeichnungsserver ausfällt. Im Hot-Standby-Modus ist die Failover-Zeit deutlich kürzer, da der Failover-Aufzeichnungsserver bereits weiß, von welchem Aufzeichnungsserver er die Aufzeichnung zu übernehmen hat, und die Konfiguration somit im Voraus laden und komplett starten kann – mit Ausnahme des letzten Schritts: dem Verbinden mit den Kameras.

Failover-Management-Server

Failover-Unterstützung auf dem Management-Server wird durch das Installieren des Management-Servers in einem Microsoft Windows Cluster erreicht. Der Cluster sorgt dafür, dass ein anderer Server die Management-Server-Funktion übernimmt, falls der erste Server ausfällt.

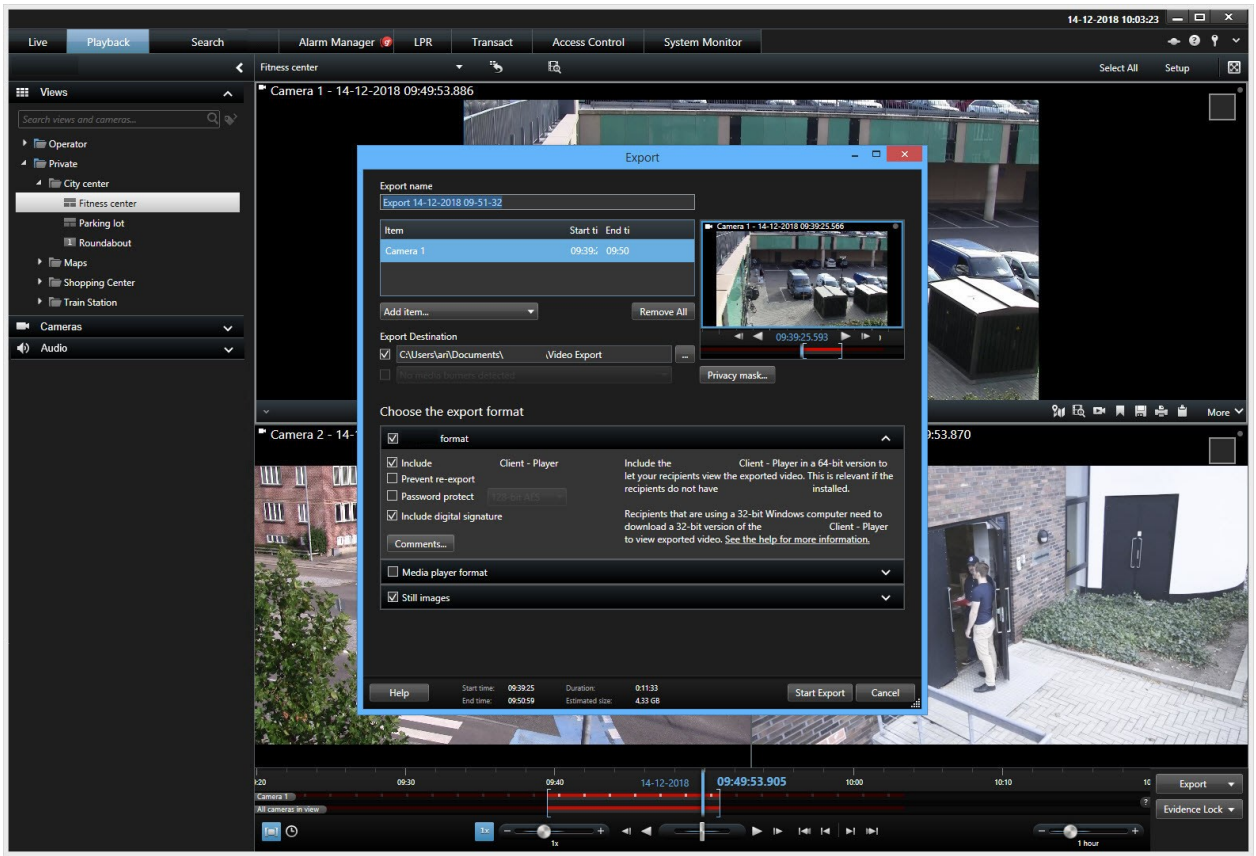
Clients

Dieser Abschnitt stellt die verschiedenen Clients vor, die von den Betreibern eines Systems verwendet werden.

XProtect Smart Client (erklärt)

XProtect Smart Client ist eine Desktop-Anwendung, mit der Sie ihre IP-Überwachungskameras verwalten können. Sie bietet die intuitive Kontrolle über Sicherheitsinstallationen, indem sie dem Benutzer Zugriff auf Live-Video und Videoaufzeichnungen, die sofortige Kontrolle über Kameras und angeschlossene Sicherheitsgeräte, sowie die Möglichkeit gibt, erweiterte Suchen nach Aufzeichnungen und Metadaten vorzunehmen.

Der in verschiedenen Sprachen verfügbare XProtect Smart Client bietet eine anpassbare Benutzeroberfläche, die sich für die Aufgaben einzelner Benutzer optimieren und an besondere Fähigkeiten und Berechtigungsstufen anpassen lässt.



Die Benutzeroberfläche erlaubt es Ihnen, Ihre Anzeige für ganz bestimmte Arbeitsumgebungen zu gestalten, indem Sie ein helles oder ein dunkles Thema auswählen. Außerdem verfügt sie über für einzelne Aufgaben optimierte Registerkarten und eine integrierte Zeitachse für Videos, um eine einfache Überwachung zu ermöglichen.

Mithilfe des MIP SDK kann der Benutzer verschiedene Arten von Sicherheits- und Geschäftssystemen sowie Videoanalytikanwendungen integrieren, die Sie über XProtect Smart Client verwalten können.

XProtect Smart Client muss auf den Computern des Betreibers installiert sein. Überwachungssystemadministratoren verwalten den Zugriff zum Überwachungssystem über die Management Client. Von Clients angezeigte Aufzeichnungen stellt Ihr XProtect System über dessen Image Server-Dienst bereit. Der Dienst wird auf dem Server des Überwachungssystems im Hintergrund ausgeführt. Es wird keine separate Hardware benötigt.

XProtect Mobile Client (Erklärung)

Der XProtect Mobile-Client ist eine mobile Überwachungslösung, die nahtlos mit dem Rest Ihres XProtect-Systems integriert ist. Er läuft auf Ihrem Android-Tablet oder Smartphone oder auf Ihrem Apple®-Tablet, Smartphone oder tragbaren Musikplayer und gibt Ihnen den Zugriff auf Kameras, Ansichten und weitere Funktionen, die im Management Client eingerichtet sind.

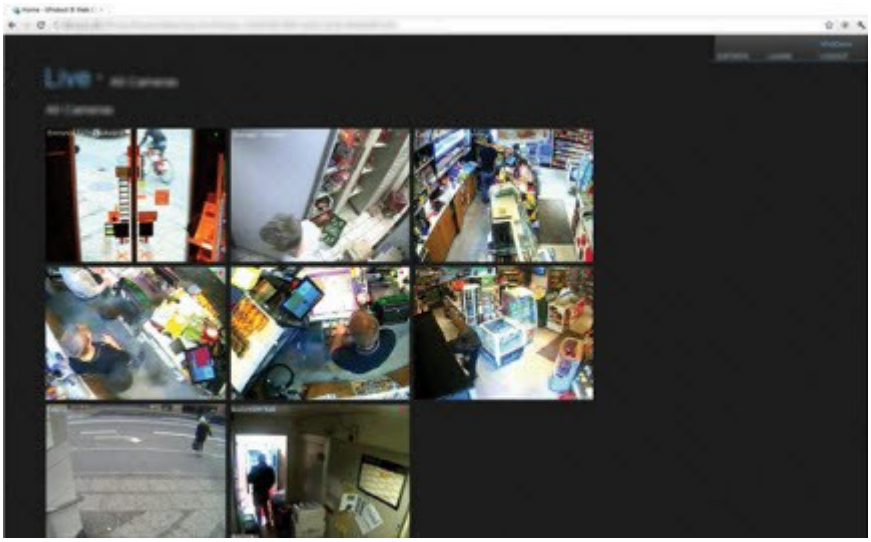
Nutzen Sie den XProtect Mobile-Client, um von einer oder mehreren Kameras Live-Videos oder Videoaufzeichnungen anzuzeigen und wiederzugeben, PTZ-Kameras (Pan/Tilt/Zoom) zu steuern, Ausgaben und Ereignisse auszulösen sowie mit der Video Push-Funktion Videodaten von Ihrem Gerät an das XProtect-System zu senden.

Wenn Sie den XProtect Mobile-Client für Ihr System verwenden möchten, müssen Sie über einen XProtect Mobile-Server verfügen, um eine Verbindung zwischen dem XProtect Mobile-Client und Ihrem System herstellen zu können. Wenn der XProtect Mobile Server einmal eingerichtet ist, laden Sie den XProtect Mobile Client gratis von Google Play oder App Store herunter, um mit der Nutzung von XProtect Mobile zu beginnen.

Sie benötigen für jedes Gerät, das Video an Ihr XProtect-System übermitteln soll, eine Gerätelizenz.

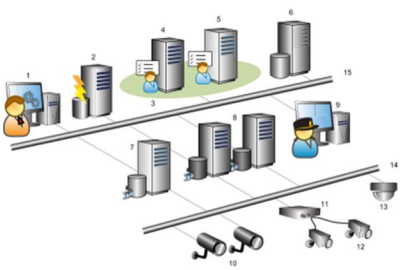
XProtect Web Client (erklärt)

XProtect Web Client ist eine webbasierte Client-Anwendung für die Anzeige, Wiedergabe und Freigabe von Videoinhalten. Sie bietet unmittelbaren Zugriff auf die am häufigsten verwendeten Überwachungsfunktionen inkl. Anzeige von Live-Videos, Wiedergabe aufgezeichneter Videoinhalte und Exportieren von Beweisen. Welche Funktionen verfügbar sind, hängt von den jeweiligen Benutzerberechtigungen ab, die in Management Client konfiguriert werden.



Für den Zugriff auf XProtect Web Client müssen Sie über einen XProtect Mobile-Server verfügen, der die Verbindung zwischen XProtect Web Client und Ihrem System herstellt. XProtect Web Client selbst erfordert keine Installation und funktioniert mit den meisten Internetbrowsern. Nach Einrichtung des XProtect Mobile-Servers können Sie Ihr XProtect-System mit beliebigen Computern oder Tablets, die über einen Internetanschluss verfügen, von jedem Ort aus überwachen (solange Sie die richtige externe Adresse bzw. Internetadresse, den Benutzernamen und das Passwort kennen).

Einrichtung eines verteilten Systems



Beispiel für die Einrichtung eines verteilten Systems. Die Zahl der Kameras, Aufzeichnungsserver und verbundenen Clients kann beliebig hoch sein.

Legende:

1. Management Client(s)
2. Ereignisserver
3. Microsoft Cluster
4. Managementserver
5. Failover-Management-Server
6. Server mit SQL Server
7. Failover-Aufzeichnungsserver
8. Aufzeichnungsserver
9. XProtect Smart Client(s)
10. IP-Videokameras
11. Videoencoder
12. Analogkameras
13. PTZ-IP-Kamera
14. Kameranetzwerk
15. Servernetzwerk

Erweiterungen

Milestone hat Zusatzprodukte entwickelt, die sich vollständig in XProtect integrieren, um Ihnen zusätzliche Funktionen zur Verfügung zu stellen. Der Zugriff auf Zusatzprodukte wird durch Ihren Softwarelizenzcode (SLC) bestimmt.

XProtect Access (erklärt)

Zur Nutzung von XProtect Access müssen Sie eine Basislizenz erworben haben, die Ihnen den Zugriff auf diese Funktion innerhalb Ihres XProtect-Systems erlaubt. Zudem benötigen Sie für jede Tür, die Sie kontrollieren möchten, eine Zutrittskontrolltür-Lizenz.

Sie können XProtect Access zusammen mit Zutrittskontrollsystemen anderer Anbieter verwenden, sofern diese über ein anbieterspezifisches Plug-in für XProtect Access verfügen.

Die Funktion der Zutrittskontrollintegration führt neue Funktionalität ein, die eine einfache Integration der Zutrittskontrollsysteme von Kunden mit XProtect ermöglichen. Sie erhalten:

- Eine allgemeine Bedienoberfläche für Anwender für mehrere Zutrittskontrollsysteme in XProtect Smart Client
- Schnellere und bessere Integration der Zutrittskontrollsysteme
- Mehr Funktionalität für den Anwender (siehe unten)

In XProtect Smart Client erhält der Anwender:

- Live-Überwachung von Ereignissen an Zutrittspunkten
- Anwendergestützter Zutritt für Zutrittsanforderung
- Karten-Integration
- Alarmdefinitionen für Ereignisse bezogen auf die Zutrittskontrolle
- Untersuchung von Ereignissen am Zutrittspunkt
- Zentralisierte Übersicht und Kontrolle von Türstatus
- Kartenhalter-Informationen und -Verwaltung

Das **Auditprotokoll** protokolliert die Befehle, die jeder Benutzer im Zutrittskontrollsystem von XProtect Smart Client ausführt.

Abgesehen von einer XProtect Access-Basislizenz, müssen Sie ein händlerspezifisches Integrations-Plug-In auf dem Event-Server installieren, bevor Sie eine Integration beginnen können .

XProtect LPR (erklärt)

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

XProtect LPR bietet videobasierte Inhaltsanalyse (VCA) sowie die Erkennung von Nummernschildern und interagiert mit Ihrem Überwachungssystem und Ihrem XProtect Smart Client.

Zur Erkennung der Zeichen auf einem Nummernschild verwendet XProtect LPR eine optische Zeichenerkennung auf Bildern, unterstützt durch spezielle Kameraeinstellungen.

Sie können LPR (Nummernschilderkennung) mit anderen Überwachungsfunktionen wie Aufzeichnung und ereignisbasierter Aktivierung von Ausgängen kombinieren.

Beispiele für Ereignisse in XProtect LPR:

- Auslösen von Aufzeichnungen des Überwachungssystems in besonderer Qualität
- Aktivieren von Alarmen
- Abgleich mit positiven/negativen Nummernschild-Übereinstimmungslisten
- Öffnen von Toren
- Einschalten der Beleuchtung
- Verschieben eines Videos mit Vorfällen auf die Computerbildschirme von bestimmtem Sicherheitspersonal
- Senden von SMS-Nachrichten

Bei einem Ereignis können Sie Alarme im XProtect Smart Client aktivieren.

XProtect Smart Wall (erklärt)

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

XProtect Smart Wall ist ein zusätzliches, erweitertes Hilfsmittel, mit dem Organisationen Videowände erstellen können, die auf ihre speziellen Sicherheitsanforderungen zugeschnitten sind. Smart Wall gibt eine Übersicht über alle Videodaten im VMS[1]-System und kann von mehreren Benutzern gemeinsam genutzt werden.

Mit XProtect Smart Wall können Benutzer Inhalte fast jeden beliebigen Typs gemeinsam verwenden, die in XProtect Smart Client zur Verfügung stehen, z.B. Video, Bilder, Text, Alarme und Smart Maps.

Zunächst wird XProtect Smart Wall von einem Systemadministrator in XProtect Management Client konfiguriert. Hierzu gehören auch Voreinstellungen, die das Layout des Smart Wall steuern sowie die Art und Weise, wie Kameras auf die verschiedenen Monitore verteilt werden. In XProtect Smart Client können die Benutzer ändern, was auf dem Smart Wall angezeigt wird, indem sie verschiedene Voreinstellungen anwenden. Auch Anzeigeänderungen können durch Regeln gesteuert werden, die die Voreinstellungen automatisch ändern.

[1]Abkürzung für "Video Management Software".

Mit der Smart Wall-Übersicht können die Benutzer bestimmte Inhalte oder ganze Ansichten einfach mithilfe der Drag-and-Drop-Funktion zu Smart Wall-Monitoren hinzufügen.

XProtect Transact (erklärt)

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

XProtect Transact ist ein Add-on für die IP-Videoüberwachungslösungen von Milestone.

XProtect Transact dient zur Überwachung laufender Transaktionen und zur Untersuchung vergangener Transaktionen. Die Transaktionen sind zur Überwachung der Transaktionen mit dem digitalen Überwachungsvideo verknüpft, um beispielsweise Beweismittel gegen einen Straftäter bereitzustellen oder einen Betrugsfall nachzuweisen. Dabei besteht zwischen den Transaktionsleitungen und den Videobildern eine 1-zu-1-Beziehung.

Die Transaktionsdaten stammen möglicherweise von verschiedenen Transaktionsquellen, in der Regel Point-of-Sale-Systeme (PoS) oder Geldautomaten.

Milestone Open Network Bridge (erklärt)

ONVIF ist ein offenes, weltweites Forum, das aktiv an einer Standardisierung und Sicherung der Art und Weise arbeitet, wie IP-Videoüberwachungsprodukte miteinander kommunizieren. Das Ziel ist es, den Austausch von Videodaten zu vereinfachen. Um beispielsweise Vollstreckungsbehörden, Überwachungszentren oder ähnliche Organisationen schnellen Zugriff zu aufgezeichneten und Live-Videostreams in jeglichen IP-basierten Überwachungssystemen zu bieten.

Milestone Systems möchte dies unterstützen und hat daher die Milestone Open Network Bridge entwickelt. Milestone Open Network Bridge ist ein Teil der Milestone-Open Platform und bietet eine Schnittstelle, die Teile des ONVIF-Standards zum Abruf von aufgezeichnetem und Live-Video aus jedem Milestone VMS-Produkt unterstützt.

Dieses Dokument bietet folgendes:

- Informationen über den ONVIF-Standard und Links zu Referenzmaterial
- Anleitungen zur Installation und Konfiguration der Milestone Open Network Bridge in Ihrem XProtect VMS-Produkt.
- Beispiele zur Aktivierung verschiedener Typen von ONVIF-Clients zum Streamen von aufgezeichnetem und Live-Video von XProtect VMS-Produkten.

XProtect DLNA Server (erklärt)

DLNA (Digital Living Network Alliance) ist ein Standard zur Verbindung von Multimediageräten. Elektronikhersteller lassen ihre Produkte DLNA-zertifizieren, um die Interoperabilität zwischen verschiedenen Anbietern und Geräten zu gewährleisten. Dies ermöglicht ihnen die Verteilung von Multimediainhalten, wie z B. Audio, Video und Fotos.

Öffentliche Bildschirme und TVs verfügen oftmals über eine DLNA-Zertifizierung und sind mit einem Netzwerk verbunden. Sie können das Netzwerk nach Medien scannen, sich zum Gerät verbinden und einen Medienstream zu ihrem integrierten Media-Player anfordern. XProtect DLNA Server kann von gewissen DLNA-zertifizierten Geräten gefunden werden und Live-Videostreams von ausgewählten Kameras an DLNA-zertifizierte Geräte mit einem Media-Player liefern.

Die DLNA-Geräte verfügen über eine Live-Videoverzögerung von 1-10 Sekunden. Dies wird durch verschiedene Puffergrößen in den Geräten verursacht.

XProtect DLNA Server muss mit demselben Netzwerk verbunden werden wie das XProtect-System, und das DLNA-Gerät muss mit demselben Netzwerk verbunden werden, wie XProtect DLNA Server.

Vom System verwendete Ports

Alle XProtect-Komponenten sowie die von Ihnen benötigten Ports sind weiter unten aufgeführt. Damit die Firewall nur ungewünschten Traffic blockiert, müssen Sie die vom System genutzten Ports bestimmen. Sie sollten nur diese Ports freigeben. Die Liste enthält auch die verwendeten Ports der lokalen Prozesse.

Sie sind in zwei Gruppen unterteilt:

- **Serverkomponenten** (Dienste) bieten ihre Dienste über bestimmte Ports an, weshalb sie auf Clientanfragen auf diesen Ports reagieren. Daher müssen diese Ports in der Windows Firewall für eingehende und ausgehende Verbindungen geöffnet werden
- **Clientkomponenten** (Clients) initiieren Verbindungen zu bestimmten Ports in Serverkomponenten. Daher müssen diese Ports für ausgehende Verbindungen geöffnet werden. Ausgehende Verbindungen sind normalerweise standardmäßig in der Windows Firewall geöffnet

Sollte nichts weiteres angegeben sein, müssen Ports für Serverkomponenten für eingehende Verbindungen geöffnet werden und Ports für Clientkomponenten für ausgehende Verbindungen.

Denken Sie jedoch daran, dass Serverkomponenten als Clients für andere Serverkomponenten dienen können. Diese sind in diesem Dokument nicht ausdrücklich aufgeführt.

Die Portnummern sind Standardzahlen, können aber geändert werden. Kontaktieren Sie den Milestone-Support, wenn Sie diejenigen Ports ändern möchten, die nicht über den Management Client konfigurierbar sind.

Serverkomponenten (eingehende Verbindungen)

Jeder der folgenden Abschnitte führt die Ports auf, welche für einen bestimmten Dienst geöffnet werden müssen. Damit Sie erfahren, welche Ports auf einem bestimmten Computer geöffnet werden müssen, sollten Sie alle Dienste auf diesem Computer ausführen.

Managementserver-Dienst und zugehörige Prozesse

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
80	HTTP	IIS	Alle XProtect-Komponenten Der Managementserver-Dienst und die Aufzeichnungsserver-Dienste	Hauptverbindung, beispielsweise, Authentifizierung und Konfigurationen. Registrierung von Aufzeichnungsservern und Management Servern durch den Identity Server App Pool (IDP).
443	HTTPS	IIS	XProtect Smart Client und die Management Client	Authentifizierung von Basis-Benutzern.
6473	TCP	Managementserver-Dienst	Management Server Manager Taskleistensymbol, nur lokale Verbindungen.	Zeigt Status und verwaltet den Dienst.
8080	TCP	Managementserver	Nur lokale Verbindung.	Kommunikation zwischen internen Prozessen auf dem Server.
9000	HTTP	Managementserver	Aufzeichnungsserver-Dienste	Webdienst für die interne Kommunikation zwischen Servern.
12345	TCP	Managementserver-Dienst	XProtect Smart Client	Kommunikation zwischen dem System und Matrix-Empfängern. Sie können die Portnummer im Management Client ändern.
12974	TCP	Managementserver-Dienst	Windows SNMP-Dienst	Kommunikation mit dem SNMP-Erweiterungsagenten.

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
				Verwenden Sie den Port nicht für anderen Zwecke, selbst wenn Ihr System SNMP nicht anwendet. In XProtect-Systemen von 2014 und älter, lautete die Portnummer 6475. In XProtect-Systemen der Version 2019 R2 und älter lautete die Portnummer 7475.

SQL Server-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
1433	TCP	SQL Server	Managementserver-Dienst	Speichern und Abruf von Konfigurationen.
1433	TCP	SQL Server	Ereignisserver-Dienst	Speichern und Abruf von Ereignissen.
1433	TCP	SQL Server	Protokollserver-Dienst	Speichern und Abruf von Protokolleinträgen.

Data Collector Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
7609	HTTP	IIS	Auf dem Computer des Management-Servers: Data Collector Dienste auf allen anderen Servern. Auf anderen Computern: Data Collector-Dienst auf dem Management-Server.	Systemmonitor.

Ereignisserver-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
1234	TCP/UDP	Ereignisserver-Dienst	Jeder Server, der generische Ereignisse an Ihr XProtect-System sendet.	Mithören generischer Ereignissen von externen Systemen oder Geräte. Nur wenn die relevante Datenquelle aktiviert ist.
1235	TCP	Ereignisserver-Dienst	Jeder Server, der generische Ereignisse an Ihr XProtect-System sendet.	Mithören generischer Ereignissen von externen Systemen oder Geräte. Nur wenn die relevante Datenquelle aktiviert ist.
9090	TCP	Ereignisserver-Dienst	Jeder Server oder Gerät, das Analyseereignisse an Ihr XProtect-System senden.	Mithören von Analyseereignissen von externen Systemen oder Geräte. Nur relevant, wenn die Analyseereignisfunktion aktiviert ist.
22331	TCP	Ereignisserver-Dienst	XProtect Smart Client und die Management Client	Konfiguration, Ereignisse, Alarme und Kartendaten.
22333	TCP	Ereignisserver-Dienst	MIP Plug-ins und Anwendungen.	MIP-Messaging.

Aufzeichnungsserver-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
25	SMTP	Aufzeichnungsserve	Kameras, Encoder	Mithören von

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
		r-Dienst	und I/O-Geräte.	Ereignismeldungen von Geräten. Der Port ist standardmäßig abgeschaltet.
5210	TCP	Aufzeichnungsserver-Dienst	Failover-Aufzeichnungsserver.	Zusammenführen von Datenbanken, nachdem ein Failover-Aufzeichnungsserver ausgeführt wurde.
5432	TCP	Aufzeichnungsserver-Dienst	Kameras, Encoder und I/O-Geräte.	Mithören von Ereignismeldungen von Geräten. Der Port ist standardmäßig abgeschaltet.
7563	TCP	Aufzeichnungsserver-Dienst	XProtect Smart Client, Management Client	Abrufen von Video- und Audiostreams, PTZ-Befehlen.
8966	TCP	Aufzeichnungsserver-Dienst	Recording Server Manager Taskleistensymbol, nur lokale Verbindungen.	Zeigt Status und verwaltet den Dienst.
9001	HTTP	Aufzeichnungsserver-Dienst	Managementserver	Webdienst für die interne Kommunikation zwischen Servern. Wenn mehrere Aufzeichnungsserverinstanzen verwendet werden, benötigt jede einzelne Instanz ihren eigenen Port. Zusätzliche Ports werden 9002, 9003 usw. sein.

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
11000	TCP	Aufzeichnungsserver-Dienst	Failover-Aufzeichnungsserver	Abfrage des Status der Aufzeichnungsserver.
12975	TCP	Aufzeichnungsserver-Dienst	Windows SNMP-Dienst	Kommunikation mit dem SNMP-Erweiterungsagenten. Verwenden Sie den Port nicht für anderen Zwecke, selbst wenn Ihr System SNMP nicht anwendet. In XProtect-Systemen von 2014 und älter, lautete die Portnummer 6474. In XProtect-Systemen der Version 2019 R2 und älter lautete die Portnummer 7474.
65101	UDP	Aufzeichnungsserver-Dienst	Nur lokale Verbindung	Mithören von Ereignis-Mitteilungen der Treiber.

Abgesehen von den eingehenden Verbindungen zu den oben aufgeführten Diensten des Aufzeichnungsserver stellt der Aufzeichnungsserver-Dienst ausgehende Verbindungen zu Kameras, NVRs und untereinander verbundenen, entfernten Standorten her (Milestone Interconnect ICP).

Failover Server-Dienst und Failover Recording Server-Service

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
25	SMTP	Failover Recording	Kameras, Encoder und I/O-Geräte.	Mithören von Ereignismeldungen von Geräten.

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
		Server Dienst		Der Port ist standardmäßig abgeschaltet.
5210	TCP	Failover Recording Server-Dienst	Failover-Aufzeichnungsserver	Zusammenführen von Datenbanken, nachdem ein Failover-Aufzeichnungsserver ausgeführt wurde.
5432	TCP	Failover Recording Server-Dienst	Kameras, Encoder und I/O-Geräte.	Mithören von Ereignismeldungen von Geräten. Der Port ist standardmäßig abgeschaltet.
7474	TCP	Failover Recording Server-Dienst	Windows SNMP-Dienst	Kommunikation mit dem SNMP-Erweiterungsagenten. Verwenden Sie den Port nicht für anderen Zwecke, selbst wenn Ihr System SNMP nicht anwendet.
7563	TCP	Failover Recording Server-Dienst	XProtect Smart Client	Abrufen von Video- und Audiostreams, PTZ-Befehlen.
8844	UDP	Failover Recording Server-Dienst	Nur lokale Verbindung.	Kommunikation zwischen den Servern.
8966	TCP	Failover Recording Server Dienst	Failover Recording Server Manager Taskleistensymbol, nur lokale Verbindungen.	Zeigt Status und verwaltet den Dienst.
8967	TCP	Failover Server-Dienst	Failover Server Manager Taskleistensymbol, nur lokale Verbindungen.	Zeigt Status und verwaltet den Dienst.

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
8990	TCP	Failover Server-Dienst	Managementserver-Dienst	Überwachung des Status des Failover Server-Dienstes.
9001	HTTP	Failover Server-Dienst	Managementserver	Webdienst für die interne Kommunikation zwischen Servern.

Abgesehen von den eingehenden Verbindungen zu den oben aufgeführten Diensten des Failover Servers / Failover Recording Servers, stellt der Dienst des Failover Servers / Failover Recording Servers ausgehende Verbindungen zu den regelmäßigen Aufnahmegeräten, Kameras sowie für Video Push her.

Protokollserver-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
22337	HTTP	Protokollserver-Dienst	Alle XProtect-Komponenten außer Management Client und der Recording-Server.	Sie können auf den Log-Server schreiben, von ihm lesen und ihn konfigurieren.

Mobile Server-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
8000	TCP	Mobile Server-Dienst	Mobile Server Manager Taskleistensymbol, nur lokale Verbindungen.	SysTray Anwendung.

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
8081	HTTP	Mobile Server-Dienst	Mobile Clients, Web Clients und Management Client.	Senden von Datenstreams; Video und Audio.
8082	HTTPS	Mobile Server-Dienst	Mobile Clients, Web Clients.	Senden von Datenstreams; Video und Audio.
40001 - 40099	HTTP	Mobile Server-Dienst	Aufzeichnungsserverdienst	Mobile Server Push-Video. Dieser Portbereich ist standardmäßig abgeschaltet.

LPR Server Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
22334	TCP	LPR Server Dienst	Ereignisserver	Abruf erkannter Nummernschilder und Server-Status. Für eine Verbindung muss der Event-Server das LPR Plug-in installiert haben.
22334	TCP	LPR Server Dienst	LPR Server Manager Taskleistensymbol, nur lokale Verbindungen.	SysTray Anwendung

Milestone Open Network Bridge-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
580	TCP	Milestone Open Network Bridge-Dienst	ONVIF Clients	Authentifizierung und Anfrage für die Videostreamkonfiguration.
554	RTSP	RTSP-Dienst	ONVIF Clients	Streamen von angefordertem Video an ONVIF-Clients.

XProtect DLNA Server-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
9100	HTTP	DLNA Server Dienst	DLNA-Gerät	Geräteerkennung und Bereitstellung der Konfiguration von DLNA-Kanälen. Anfrage für Videostreams.
9200	HTTP	DLNA Server Dienst	DLNA-Gerät	Streamen von angeforderten Video an DLNA-Geräte.

XProtect Screen Recorder-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
52111	TCP	XProtect Screen Recorder	Aufzeichnungsserver-Dienst	Stellt Video von einem Bildschirm bereit. Es erscheint und handelt in der gleichen Art wie eine Kamera auf dem Aufzeichnungsserver. Sie können die Portnummer im Management Client ändern.

Serverkomponenten (ausgehende Verbindungen)

Managementserver-Dienst

Portnummer	Protokoll	Verbindungen zu...	Zweck
443	HTTPS	Der Lizenzserver, der den Lizenzverwaltungsdienst hostet. Die Kommunikation erfolgt über https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx	Das Aktivieren von Lizenzen.

Server-Dienst

Portnummer	Protokoll	Verbindungen zu...	Zweck
80	HTTP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Authentifizierung, Konfiguration und Datenstreams; Video und Audio.
443	HTTPS	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Authentifizierung, Konfiguration und Datenstreams; Video und Audio.
554	RTSP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Datenstreams; Video und Audio.
11000	TCP	Failover-Aufzeichnungsserver	Abfrage des Status der Aufzeichnungsserver.
40001 – 40099	HTTP	Mobil-Server-Dienst	Push-Video auf dem Mobile Server. Dieser Portbereich ist standardmäßig abgeschaltet.

Failover Server-Dienst und Failover Recording Server-Dienst

Portnummer	Protokoll	Verbindungen zu...	Zweck
11000	TCP	Failover-Aufzeichnungsserver	Abfrage des Status der Aufzeichnungsserver.

Ereignisserver-Dienst

Portnummer	Protokoll	Verbindungen zu...	Zweck
443	HTTPS	Milestone Customer Dashboard über https://service.milestonesys.com/	Senden Sie Status, Ereignisse und Fehlermeldungen vom XProtect-System an Milestone Customer Dashboard.

Protokollserver-Dienst

Portnummer	Protokoll	Verbindungen zu...	Zweck
443	HTTP	Protokollserver	Weiterleitung von Nachrichten an den Log-Server.

Kameras, Encoder und I/O-Geräte (eingehende Verbindungen)

Portnummer	Protokoll	Verbindungen von...	Zweck
80	TCP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Authentifizierung, Konfiguration und Datenstreams; Video und Audio.
443	HTTPS	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Authentifizierung, Konfiguration und Datenstreams; Video und Audio.
554	RTSP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Datenstreams; Video und Audio.

Kameras, Encoder und I/O-Geräte (ausgehende Verbindungen)

Portnummer	Protokoll	Verbindungen zu...	Zweck
25	SMTP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Senden von Ereignis-Mitteilungen (veraltet).
5432	TCP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Senden von Ereignis-Mitteilungen. Der Port ist standardmäßig abgeschaltet.
22337	HTTP	Protokollserver	Weiterleitung von Nachrichten an den Log-Server.

Nur einige wenige Kameramodelle können ausgehende Verbindungen aufbauen.

Clientkomponenten (ausgehende Verbindungen)

XProtect Smart Client, XProtect Management Client XProtect Mobile, -Server

Portnummer	Protokoll	Verbindungen zu...	Zweck
80	HTTP	Managementserver-Dienst	Authentifizierung
443	HTTPS	Managementserver-Dienst	Authentifizierung von Basis-Benutzern.
7563	TCP	Aufzeichnungsserver Dienst	Abrufen von Video- und Audiostreams, PTZ-Befehlen.
22331	TCP	Ereignisserver Dienst	Alarme.

XProtect Web Client, XProtect Mobile Client

Portnummer	Protokoll	Verbindungen zu...	Zweck
8081	HTTP	XProtect Mobile-Server	Abrufen von Video- und Audiostreams.
8082	HTTPS	XProtect Mobile-Server	Abrufen von Video- und Audiostreams.

Produktvergleichstabelle

XProtect VMS umfasst folgende Produkte:

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

Die vollständige Funktionsliste finden Sie auf der Produktüberblickseite auf der Milestone-Website (https://www.milestonesys.com/solutions/platform/product-index/).

Nachfolgend finden Sie eine Liste der Hauptunterschiede zwischen den Produkten:

Name	XProtect Essential+	XProtect Express+	XProtect Professional +	XProtect Expert	XProtect Corporate
Standorte pro SLC	1	1	Mehrere Standorte	Mehrere Standorte	Mehrere Standorte
Aufzeichnungsserver pro SLC	1	1	Unbegrenzt	Unbegrenzt	Unbegrenzt
Geräte pro Aufzeichnungsserver	8	48	Unbegrenzt	Unbegrenzt	Unbegrenzt
Milestone	-	Remote-	Remote-	Remote-	Zentraler/Rem

Name	XProtect Essential+	XProtect Express+	XProtect Professional +	XProtect Expert	XProtect Corporate
Interconnect™		System	System	System	ote-System
Milestone Federated Architecture™	-	-	-	Remote-System	Zentraler/Remote-System
Aufzeichnungsserver-Failover	-	-	-	Cold- und Hot-Standby	Cold- und Hot-Standby
Fernzugriffsdienste	-	-	-	-	✓
Edge-Speicher-Unterstützung	-	-	✓	✓	✓
Mehrschichtige Videospeicherarchitektur	Live-Datenbanken + 1 Archiv	Live-Datenbanken + 1 Archiv	Live-Datenbanken + 1 Archiv	Live-Datenbanken + unbegrenzte Archive	Live-Datenbanken + unbegrenzte Archive
SNMP-Benachrichtigung	-	-	-	✓	✓
Zeitgesteuerte Benutzerzugriffsrechte	-	-	-	-	✓
Bildrate reduzieren (Ausdünnung)	-	-	-	✓	✓
Videodatenverschlüsselung (Aufzeichnungsserver)	-	-	-	✓	✓
Datenbanksignatur (Recording-Server)	-	-	-	✓	✓

Name	XProtect Essential+	XProtect Express+	XProtect Professional +	XProtect Expert	XProtect Corporate
PTZ-Prioritätsstufen	1	1	3	32000	32000
Erweitertes PTZ (PTZ-Sitzung und Wachrundgang über XProtect Smart Client reservieren)	-	-	-	✓	✓
Beweissicherung	-	-	-	-	✓
Lesezeichenfunktion	-	-	Nur manuell	Manuell und regelbasiert	Manuell und regelbasiert
Live-Multi-Streaming oder Multicasting / Adaptives Streaming	-	-	-	✓	✓
Direktes Streaming	-	-	-	✓	✓
Gesamtsicherheit	Client-Benutzerrechte	Client-Benutzerrechte	Client-Benutzerrechte	Client-Benutzerrechte	Client-Benutzerrechte/ Administrator-Benutzerrechte
XProtect Management Client-Profile	-	-	-	-	✓
XProtect Smart Client-Profile	-	-	3	3	Unbegrenzt
XProtect Smart Wall	-	-	-	Optional	✓
Systemmonitor	-	-	-	✓	✓

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

Lizenzierung

Lizenzen (Erklärung)

Wenn Sie ein XProtect Essential+-System installiert haben, können Sie das System und acht Gerätelizenzen kostenlos ausführen. Automatische Lizenzaktivierung ist aktiviert und Geräte werden aktiviert, sobald Sie sie zum System hinzufügen.
Nur wenn Sie ein Upgrade (siehe Softwarelizenzcode ändern auf Seite 51) auf ein erweitertes XProtect-Produkt vornehmen, ist der übrige Teil dieses Themas und sind die anderen lizenzbezogenen Themen in dieser Dokumentation relevant.

Wenn Sie Ihre Software und Lizenzen kaufen, erhalten Sie:

- Eine Bestellbestätigung
- Eine Softwarelizenzdatei mit der Endung „.lic“, deren Namen Ihrem SLC (Software-Lizenzcode) entspricht

Ihr SLC ist auch auf Ihrer Bestellbestätigung gedruckt und besteht aus mehreren Nummern und Buchstaben, die mit Bindestrichen angeordnet sind, wie im Folgenden dargestellt:

- Produktversion 2014 oder früher: xxx-xxxx-xxxx
- Produktversion 2016 oder später: xxx-xxx-xxx-xx-xxxxxx

Die Softwarelizenzdatei enthält alle Informationen über Ihre erworbenen VMS-Produkte und -Lizenzen. Milestone empfiehlt, dass Sie die Informationen über Ihren SLC und eine Kopie Ihrer Softwarelizenzdatei an einem sicheren Ort lagern, an dem Sie sie wieder finden können. Im Navigationsbaum können Sie außerdem Ihren SLC anzeigen, indem Sie **Basis** > **Lizenzinformationen** auswählen. Möglicherweise benötigen Sie die Softwarelizenzdatei oder Ihren SLC, wenn Sie zum Beispiel ein My Milestone-Benutzerkonto einrichten, sich aus Supportgründen an Ihren Vertriebspartner wenden oder Änderungen am System vornehmen möchten.

Laden Sie zunächst die Software von unserer Website (https://www.milestonesys.com/downloads/) herunter. Wenn Sie die Software installieren (siehe Installation eines neuen XProtect-Systems auf Seite 78), werden Sie aufgefordert, die Softwarelizenzdatei bereitzustellen.

Nach Abschluss der Installation und Aktivierung Ihrer Lizenzen können Sie auf der Seite **Grundlagen** > **Lizenzinformationen** eine Übersicht über Ihre Lizenzen für alle Installationen mit dem selben SLC sehen.

Sie haben mindestens zwei Arten von Lizenzen gekauft:

Basislizenzen: Als Minimum verfügen Sie über eine Basislizenz für eines der XProtect-Produkte. Außerdem können Sie über eine oder mehrere Basislizenzen für XProtect-Zusatzprodukte verfügen.

Hardware-Gerätelizenzen: Jedes Gerät, das Sie Ihrem XProtect-System hinzufügen, setzt eine entsprechende Gerätelizenz voraus. Für Lautsprecher, Mikrofone oder Eingangs- und Ausgangsgeräte, die mit Ihren Kameras verbunden sind, benötigen Sie keine zusätzlichen Gerätelizenzen. Sie brauchen lediglich eine Gerätelizenz pro Videoencoder-IP-Adresse – selbst dann, wenn Sie an den Videoencoder mehrere Kameras anschließen. Ein Videoencoder kann eine oder mehrere IP-Adressen aufweisen.

Weitere Informationen finden Sie in der Liste unterstützter Hardware auf der Milestone-Website (https://www.milestonesys.com/supported-devices/). Wenn Sie in XProtect Mobile die Video Push-Funktion verwenden möchten, benötigen Sie zudem eine Gerätelizenz pro Mobilgerät oder Tablet, das in der Lage sein soll, Video auf Ihr System zu pushen. Wenn Sie nicht genug Gerätelizenzen besitzen, können Sie weniger wichtige Geräte deaktivieren (siehe Deaktivieren/Aktivieren von Hardware auf Seite 200), damit sich stattdessen neue Geräte ausführen lassen können.

Wenn Ihr Überwachungssystem der zentrale Standort in einer größeren Systemhierarchie ist, in der Milestone Interconnect zum Einsatz kommt, benötigen Sie Milestone Interconnect-Kameralizenzen, um Videos von Geräten an Remote-Systemen anzeigen zu können. Beachten Sie, dass ausschließlich XProtect Corporate als zentraler Standort agieren kann.

Die meisten XProtect-Zusatzprodukte setzen weitere Lizenztypen voraus. Die Softwarelizenzdatei kann auch Informationen über Ihre Lizenzen für Zusatzprodukte umfassen. Manche Zusatzprodukte verfügen über eigene separate Softwarelizenzdateien.

Softwarelizenzcode ändern

Wenn Sie Ihre Installation während des ersten Zeitraums mit einem temporären Softwarelizenzcode (SLC) durchführen, oder wenn Sie ein Upgrade auf ein erweitertes XProtect-Produkt durchgeführt haben, können Sie Ihren SLC ohne De- oder Neuinstallation ändern, wenn Sie Ihre neue Softwarelizenzdatei erhalten haben.

> ⚠ Dies muss lokal auf dem Management-Server erfolgen. Sie können dies **nicht** vom Management Client aus tun.

1. Auf dem Management-Server gehen Sie zum Benachrichtigungsbereich der Taskleiste.

2. Klicken Sie mit der rechten Maustaste auf das **Management-Server**-Symbol und wählen Sie **Lizenz ändern** aus.
3. Klicken Sie auf **Lizenz importieren**.
4. Wählen Sie als nächstes die Softwarelizenzdatei aus, die zu diesem Zweck gespeichert wurde. Wenn Sie fertig sind, wird der Speicherort der ausgewählten Softwarelizenzdatei direkt unter der Schaltfläche **Lizenz importieren** hinzugefügt.
5. Klicken Sie auf **OK** und Sie sind nun bereit, den SLC zu registrieren. Siehe Softwarelizenzcode registrieren auf Seite 68 registrieren.

Anforderungen und Hinweise

Sommerzeit (Erklärung)

Während der Sommerzeit werden die Uhren um eine Stunde nach vorne gestellt, damit es abends länger hell ist und morgens noch dunkler ist. Länder/Regionen verwenden die Sommerzeit unterschiedlich.

Wenn Sie mit einem Überwachungssystem arbeiten, das von sich aus zeitempfindlich ist, ist es wichtig, zu wissen, wie es mit der Sommerzeit umgeht.

> Ändern Sie die Sommerzeit-Einstellung nicht während der Sommerzeit, oder wenn Sie Aufnahmen aus der Sommerzeit haben.

Frühling: Umschalten von Standardzeit auf Sommerzeit

Die Umstellung von der Standard- auf die Sommerzeit ist einfach, da die Uhr lediglich eine Stunde nach vorne gestellt wird.

Beispiel:

Die Uhr springt von 02:00 Uhr Standardzeit auf 03:00 Uhr Sommerzeit und der Tag hat nur 23 Stunden. In diesem Fall gibt es für die Zeit zwischen 02:00 Uhr und 03:00 Uhr morgens keine Daten, da diese Stunde an diesem Tag nicht existierte.

Herbst: Umschalten von Sommerzeit auf Standardzeit

Wenn Sie im Herbst von Sommerzeit auf Standardzeit umschalten, springt die Uhr eine Stunde zurück.

Beispiel:

Die Uhr springt von 02:00 Uhr Sommerzeit auf 01:00 Uhr Standardzeit zurück. Die Stunde wiederholt sich somit und der Tag hat 25 Stunden. Nach 01:59:59 springt die Uhrzeit auf 01:00:00 zurück. Würde das System nicht reagieren, würde die Stunde erneut aufgezeichnet werden, sodass die erste Instanz von 01:30 Uhr durch die zweite Instanz von 01:30 Uhr überschrieben würde.

Um dies zu verhindern, archiviert das System das aktuelle Video für den Fall, dass sich die Systemzeit um mehr als fünf Minuten ändert. Sie können sich die erste Instanz von 01:00 Uhr nicht direkt in Clients ansehen, die Daten werden jedoch aufgezeichnet und sind sicher. Sie können sich das Video in XProtect Smart Client ansehen, indem Sie die archivierte Datenbank direkt öffnen.

Zeitserver (Erklärung)

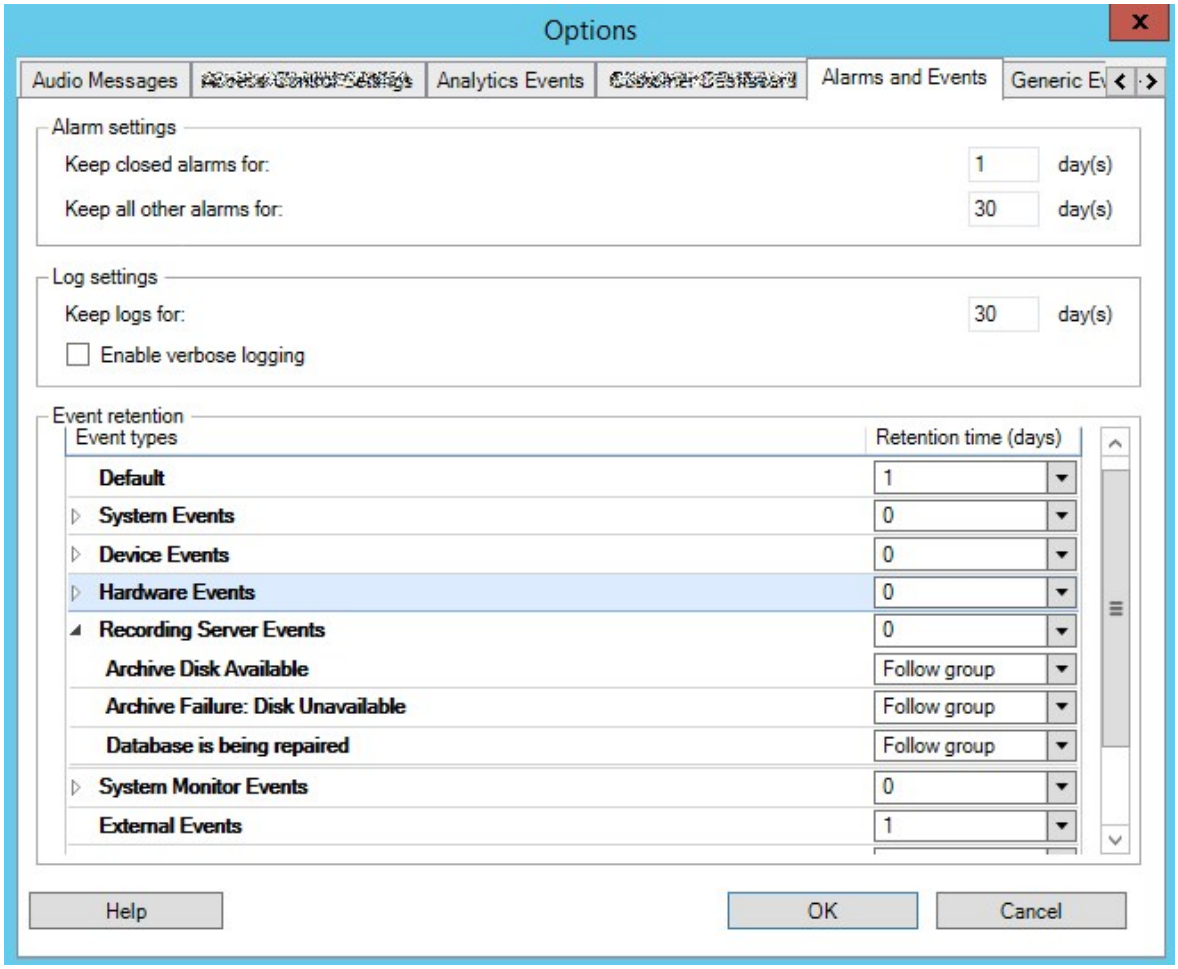
Sobald Ihr System Bilder empfängt, werden diese umgehend mit einem Zeitstempel versehen. Da es sich bei Kameras um separate Einheiten handelt, die über eigene Zeitmessgeräte verfügen können, stimmen die Kamerazeit und die Systemzeit nicht immer überein. Dies kann hin und wieder zu Verwirrung führen. Falls Ihre Kamera Zeitstempel unterstützt, empfiehlt Milestone, die Kamera- und Systemzeit über einen Zeitserver automatisch zu synchronisieren, um konsistente Zeitangaben zu erhalten.

Wenn Sie weitere Informationen zur Konfiguration eines Zeitservers benötigen, suchen Sie auf der Microsoft-Website (https://www.microsoft.com/) nach **„Zeitserver“**, **„Zeitdienst“** oder ähnlichen Begriffen.

Größenbegrenzung für die Datenbank

Um zu vermeiden, dass die SQL-Datenbank (siehe SQL Servers und Datenbanken auf Seite 24) auf eine Größe anwächst, die die Leistung des Systems beeinträchtigt, können Sie angeben, für wie viele Tage die verschiedenen Ereignistypen und Alarme in der Datenbank gespeichert werden sollen.

1. Öffnen Sie das Menü **Extras**.
2. Klicken Sie auf **Optionen**, und dann auf die Registerkarte **Alarme und Ereignisse**.



3. Nehmen Sie die erforderlichen Einstellungen vor. Weitere Informationen finden Sie auf der Registerkarte Registerkarte „Alarme und Ereignisse“ (Optionen) auf Seite 132.

IPv6 und IPv4 (Erklärung)

Ihr System unterstützt sowohl IPv6 als auch IPv4. Ebenso wie bei XProtect Smart Client.

IPv6 ist die aktuelle Version des Internet Protocols (IP). Das Internet Protocol bestimmt das Format und die Verwendung von IP-Adressen. IPv6 besteht zusätzlich zur weiter verbreiteten IP-Version IPv4. IPv6 wurde als Lösung der Adressenausschöpfung von IPv4 entwickelt. IPv6-Adressen sind 128-Bit lang, wo hingegen IPv4-Adressen nur 32-Bit lang sind.

Letztendlich bedeutet dies, dass das Anschriftenverzeichnis des Internets von 4,3 Milliarden einzigartigen Adressen auf 340 Sextillionen (340 Billionen Billionen) Adressen angewachsen ist. Ein Wachstumsfaktor von 79 Quadrilliarden (Milliarden Milliarden Milliarden).

Immer mehr Unternehmen nehmen eine Implementierung von IPv6 in ihren Netzwerken vor. Beispielsweise sind alle Gebäude der Bundesbehörden in den Vereinigten Staaten dazu verpflichtet, IPv6-Kompatibel zu sein. Beispiele und Abbildungen in dieser Anleitung setzen jedoch die Verwendung von IPv4 voraus, da diese IP-Version noch immer weiter verbreitet ist. IPv6 funktioniert aber ebenso gut im System.

Gebrauch des Systems mit IPv6 (Erklärung)

Bei der Verwendung des Systems mit IPv6 treffen folgende Bedingungen zu:

Server

Server können oftmals sowohl IPv4 als auch IPv6 verwenden. Wenn allerdings ein Server in Ihrem System (beispielsweise ein Management-Server oder Aufzeichnungsserver) eine bestimmte IP-Version benötigt, müssen alle anderen Server in ihrem System ebenfalls über die selbe IP-Version verbunden werden.

Beispiel: Bis auf einen Server in Ihrem System können alle Server sowohl IPv4 als auch IPv6 verwenden. Die Ausnahme stellt ein Server dar, der nur IPv6 nutzen kann. Dies hat zur Folge, dass alle Server über IPv6 kommunizieren müssen.

Geräte

Sie können Geräte (z. B. Kameras, Eingänge, Ausgänge, Mikrofone, Lautsprecher) verwenden, die eine andere IP-Version als die der Serverkommunikation nutzen, vorausgesetzt Ihre Netzwerkgeräte und die Aufzeichnungsserver unterstützen die IP-Version des Geräts. Siehe auch Abbildung unten.

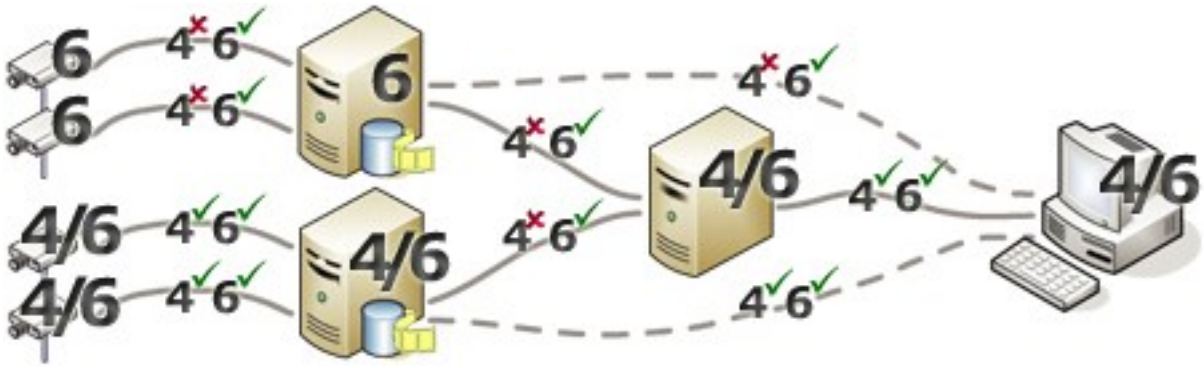
Clients

Wenn Ihr System IPv6 verwendet, sollten sich Benutzer mit dem XProtect Smart Client verbinden. Das XProtect Smart Client unterstützt sowohl IPv6 als auch IPv4.

Wenn einer oder mehrere Server in Ihrem System **nur** IPv6 verwenden können, **müssen** XProtect Smart Client-Benutzer IPv6 für die Verbindung dieser Server benutzen. In diesem Zusammenhang ist es wichtig, dass sich XProtect Smart Client-Installationen zuerst mit einem Management-Server für die erste Authentifizierung verbinden und dann mit den erforderlichen Aufzeichnungsservern für den Zugriff auf die Aufzeichnungen.

Allerdings müssen die XProtect Smart Client-Benutzer nicht selbst in einem IPv6-Netzwerk sein, wenn Ihre Netzwerkgeräte die Kommunikation zwischen verschiedenen IP-Versionen unterstützen, und das IPv6-Protokoll auf Ihren Computern installiert haben. Siehe auch Abbildung. Zur Installation von IPv6 auf einem Client-Computer, öffnen Sie die Eingabeaufforderung, geben Sie ***Ipv6 install*** ein, und drücken Sie anschließend **ENTER**.

Beispielabbildung



Beispiel: Da ein Server im System nur IPv6 verwenden kann, muss sämtliche Kommunikation mit diesem Server IPv6 verwenden. Allerdings bestimmt dieser Server auch die IP-Version für die Kommunikation zwischen allen anderen Servern im System.

Keine Matrix Monitor Kompabilität

Bei Verwendung von IPv6 können Sie die Matrix Monitor-Anwendung in Ihrem System nicht benutzen. Matrix Funktionalität in XProtect Smart Client ist nicht betroffen.

Schreiben von IPv6-Adressen (Erklärung)

Eine IPv6 wird üblicherweise in acht Blöcken aus vier hexadezimalen Ziffern geschrieben, wobei jeder Block von einem Doppelpunkt getrennt wird.

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

Durch Auslassen der ersten Nullen in einem Block, können Sie die Adressen kürzen. Beachten Sie auch, dass einige der vierstelligen Blöcke möglicherweise nur aus Nullen bestehen. Wenn solche 0000-Blöcke aufeinanderfolgen, können Sie die Adressen verkürzen, indem Sie die 0000-Blöcke mit zwei Doppelpunkten ersetzen, sofern nur einer dieser doppelten Doppelpunkte in der Adresse auftauchen.

Beispiel:
2001:0B80:0000:0000:0000:0F80:3FA8:18AB kann verkürzt werden zu

2001:B80:0000:0000:0000:F80:3FA8:18AB, wenn die ersten Nullen entfernt werden, oder zu

2001:0B80::0F80:3FA8:18AB, wenn die 0000-Blöcke entfernt werden, oder sogar zu

2001:B80::F80:3FA8:18AB, wenn sowohl die ersten Nullen als auch die 0000-Blöcke entfernt werden.

Verwendung von IPv6-Adressen in URLs

IPv6-Adressen enthalten Doppelpunkte. Doppelpunkte werden jedoch auch in anderen Syntaxtypen von Netzwerkadressen verwendet. Beispielsweise verwendet IPv4 einen Doppelpunkt, um IP-Adressen und Portnummern zu trennen, wenn beide in einer URL genutzt werden. IPv6 hat dieses Prinzip übernommen. Zur Vermeidung von Missverständnissen werden eckige Klammern um IPv6-Adressen geschrieben, wenn sie in URLs verwendet werden.

Beispiel einer URL mit einer IPv6-Adresse:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB], die wiederum auf *http://[2001:B80::F80:3FA8:18AB]* verkürzt werden kann.

Beispiel einer URL mit einer IPv6-Adresse und einer Portnummer:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234, die natürlich gekürzt werden kann auf zum Beispiel *http://[2001:B80::F80:3FA8:18AB]:1234*

Weitere Informationen über IPv6 bekommen Sie zum Beispiel auf der IANA-Website (https://www.iana.org/numbers/). IANA (Internet Assigned Numbers Authority) ist die zuständige Organisation für die weltweite Koordination der IP-Adressverteilung.

Virtuelle Server

Sie können alle Systemkomponenten auf virtualisierten Windows®-Servern wie VMware® und Microsoft® Hyper-V® laufen lassen.

Die Virtualisierung wird oft bevorzugt, um die Hardware-Ressourcen besser auszunutzen. Im Normalfall belasten virtuelle Server, die auf dem Hardware-Hostserver ausgeführt werden, den virtuellen Server nicht übermäßig – und oft auch nicht zur selben Zeit. Die Aufzeichnungsserver zeichnen jedoch alle Kamerabilder und Video-Streams auf. Dies belastet die CPU, den Arbeitsspeicher, das Netzwerk und das Speichersystem. Bei Ausführung auf einem virtuellen Server werden die üblichen Vorteile von Virtualisierung also zu einem Großteil neutralisiert, da Aufzeichnungsserver in vielen Fällen alle verfügbaren Ressourcen belegen.

Bei der Ausführung in einer virtuellen Umgebung muss der physische Speicher des Hardware-Hosts dieselbe Größe aufweisen wie der, der den virtuellen Servern zugewiesen ist. Darüber hinaus muss sichergestellt sein, dass der virtuelle Server, auf dem der Aufzeichnungsserver ausgeführt wird, über genügend CPU und Arbeitsspeicher verfügt – standardmäßig ist das nicht der Fall. Üblicherweise benötigt der Aufzeichnungsserver je nach Konfiguration 2 bis 4 GB. Weitere Engpässe sind die Netzwerkadapter-Zuweisung sowie die Festplattenleistung. Sie sollten in Erwägung ziehen, auf dem Hostserver des virtuellen Servers, auf dem der Aufzeichnungsserver ausgeführt wird, einen physischen Netzwerkadapter zuzuweisen. Dadurch lässt sich leichter sicherstellen, dass der Netzwerkadapter nicht mit dem Datenverkehr zu anderen virtuellen Servern überlastet wird. Wenn der Netzwerkadapter für verschiedene virtuelle Server verwendet wird, kann hoher Netzwerkverkehr dazu führen, dass der Aufzeichnungsserver die konfigurierte Zahl der Bilder nicht abruft und aufzeichnet.

Mehrere Management-Server (Cluster) (Erklärung)

Die Management-Server kann auf mehreren Servern innerhalb eines Server-Clusters installiert werden. Dies gewährleistet sehr geringe Ausfallzeiten des Systems. Falls ein Server in einem Cluster ausfällt, übernimmt ein anderer Server in dem Cluster automatisch die Aufgabe des ausgefallenen Servers und der Management-Server kann über ihn ausgeführt werden. Der automatische Prozess, den Managementserverdienst auf einen anderen Server im Cluster umzuschalten, dauert bis zu 30 Sekunden.

Es ist nur möglich einen aktiven Management-Server pro Überwachungseinrichtung zu haben. Es können allerdings weitere Management-Server aufgesetzt werden, die bei Ausfällen einspringen.

Die Anzahl der erlaubten Failovers ist auf zwei innerhalb eines sechsstündigen Zeitraums begrenzt. Bei Überschreitung werden Managementserverdienste nicht automatisch vom Clustering-Dienst gestartet. Die Anzahl erlaubter Failovers kann Ihren Bedürfnissen angepasst werden.

Anforderungen für Cluster

- Zwei Maschinen mit Microsoft Windows Server 2012 oder neuer. Achten Sie bitte darauf, dass:
  - Alle Server, die Sie als Clusterknoten hinzufügen möchten, mit derselben Version von Windows Server laufen
  - Alle Server, die Sie als Clusterknoten hinzufügen möchten, mit derselben Domäne verbunden sind
  - Sie sich als lokaler Administrator am Windows-Konto anmelden können

  Weitere Informationen zu Clustern in Microsoft-Windows-Servern finden Sie unter Ausfallsichere Cluster https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster.
- Eine Microsoft SQL Server Installation

  Entweder eine externe SQL Server und eine Datenbank, die **außerhalb** des Server-Clusters installiert wird, **oder** ein **interner** SQL Server (geclusterter) Dienst innerhalb des Server-Clusters (zur Erstellung eines internen SQL Server Dienstes ist die Verwendung des SQL Server oder der Microsoft® SQL Server® Standard Version erforderlich, die als geclusterter Microsoft® SQL Server® Enterprise fungieren kann).

  Beim Herstellen der Verbindung zwischen dem Management Server und der Datenbank werden Sie, je nach den Passworteinstellungen in Ihrer Systemkonfiguration, ggf. dazu aufgefordert, das aktuelle Passwort für die Systemkonfiguration einzugeben. Siehe auch Passwort für die Systemkonfiguration (Erklärung) auf Seite 497.

Schützen von Aufzeichnungsdatenbanken vor Beschädigungen

Kamera-Datenbanken können beschädigt werden Es gibt verschiedene Datenbank-Reparatur-Optionen, um ein solches Problem zu lösen. Aber Milestone empfiehlt, dass Sie Maßnahmen ergreifen, um sicherzustellen, dass Ihre Kamera-Datenbanken nicht beschädigt werden.

Festplattenfehler: Schützen Sie Ihre Laufwerke

Festplattenlaufwerke sind mechanische Geräte, die anfällig für externe Einwirkungen sind. Beispiele für externe Einwirkungen, die zu einer Beschädigung von Festplattenlaufwerken und Kameradatenbanken führen können, sind:

- Erschütterungen (sorgen Sie dafür, dass das Überwachungssystem inklusive seiner Umgebung stabil ist)
- Starke Hitze (sorgen Sie dafür, dass der Server ausreichend Belüftung erhält)
- Starke magnetische Felder (verhindern)
- Stromausfälle (nutzen Sie eine unabhängige Stromversorgung (USV))
- Statische Elektrizität (sorgen Sie dafür, dass Sie sich erden, bevor Sie ein Festplattenlaufwerk anfassen)
- Feuer, Wasser usw. (verhindern)

Windows Task-Manager: Passen Sie auf beim Beenden von Prozessen

Bei Verwendung des Windows Task-Managers müssen Sie darauf achten, keine Prozesse zu beenden, die Folgen für das Überwachungssystem haben. Wenn Sie eine Anwendung oder einen Systemdienst beenden, indem Sie im Windows Task-Manager auf **Prozess beenden** klicken, kann der Prozess vor der Beendigung weder seinen Status noch seine Daten speichern. Dies kann zu einer Beschädigung von Kameradatenbanken führen.

Wenn Sie versuchen, einen Prozess zu beenden, zeigt der Windows Task-Manager in der Regel eine Warnung an. Falls Sie in der Warnnachricht gefragt werden, ob Sie den Prozess wirklich beenden möchten, klicken Sie auf **Nein** – es sei denn, Sie sind sich ganz sicher, dass das Beenden des Prozesses keine Auswirkungen auf das Überwachungssystem haben wird.

Stromausfälle: Nutzen Sie eine USV

Der häufigste Grund für beschädigte Datenbanken ist ein plötzliches Herunterfahren des Aufzeichnungsservers, wobei Dateien nicht gespeichert werden und das Betriebssystem nicht ordnungsgemäß heruntergefahren wird. Ursache dafür können Stromausfälle, Personen, die aus Versehen Stromkabel von Servern herausziehen, oder ähnliche Motive sein.

Die beste Methode, um Aufzeichnungsserver vor einem plötzlichen Herunterfahren zu schützen, besteht darin, jeden von ihnen mit einer USV (unabhängigen Stromversorgung) auszustatten.

Die USV dient als batteriebetriebene sekundäre Stromquelle, die bei Problemen mit der Stromversorgung genug Energie für das Speichern geöffneter Dateien und das sichere Herunterfahren Ihres Systems liefert. USVs bieten unterschiedliche Leistungsmerkmale, viele USVs beinhalten jedoch Software für ein automatisches Speichern geöffneter Dateien, für eine Benachrichtigung der Systemadministratoren usw.

Die Auswahl des richtigen USV-Typs hängt von den individuellen Anforderungen Ihres Unternehmens ab. Bei der Evaluierung Ihrer Anforderungen sollten Sie allerdings die Laufzeitlänge beachten, die Ihre USV unterstützen muss, falls es zu einem Stromausfall kommt. Das Speichern geöffneter Dateien und das Herunterfahren eines Betriebssystems können einige Minuten dauern.

SQL-Datenbanktransaktionsprotokoll (Erläuterung)

Jedes Mal, wenn in eine SQL-Datenbank eine Änderung geschrieben wird, protokolliert die SQL-Datenbank diese Änderung in ihrem Transaktionsprotokoll.

Mit dem Transaktionsprotokoll können Sie Änderungen in der SQL durch Microsoft® SQL Server Management Studio rückgängig machen. Die SQL-Datenbank speichert standardmäßig ihr Transaktionsprotokoll auf unbegrenzte Zeit, was bedeutet, dass das Transaktionsprotokoll mit der Zeit immer mehr Einträge enthält. Das Transaktionsprotokoll befindet sich standardmäßig auf dem Systemlaufwerk, und wenn es sich stetig vergrößert, kann es die ordnungsgemäße Ausführung von Windows beeinträchtigen.

Das gelegentliche Löschen des Transaktionsprotokolls ist eine gute Methode, um ein solches Szenario zu vermeiden. Allerdings macht die Löschung allein das Transaktionsprotokoll nicht kleiner, bereinigt jedoch dessen Inhalt und verhindert so ein unkontrolliertes Wachstum. Ihr VMS-System löscht keine Transaktionsprotokolle. In SQL Server gibt es Methoden zum Löschen des Transaktionsprotokolls. Weitere Informationen finden Sie auf der Microsoft-Support-Seite (https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017), wenn Sie nach *Abschneiden des Transaktionsprotokolls* suchen.

Mindestsystemanforderungen

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

Vor dem Start der Installation

Milestone empfiehlt Ihnen, die im nächsten Abschnitt beschriebenen Voraussetzungen zu lesen, bevor Sie die tatsächliche Installation beginnen.

Server und Netzwerk vorbereiten

Betriebssystem

Achten Sie darauf, dass auf allen Servern eine saubere Installation eines Microsoft Windows-Betriebssystems installiert ist und das Betriebssystem mit den neuesten Windows-Updates aktualisiert wurde.

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

Microsoft® .NET Framework

Prüfen Sie, ob Microsoft .NET Framework 4.7 oder höher auf allen Servern installiert ist.

Netzwerk

Weisen Sie statische IP-Adressen zu oder nehmen Sie DHCP-Reservierungen an allen Systemkomponenten und Kameras vor. Sie müssen verstehen, wie und wann das System Bandbreite verbraucht, um sicherzustellen, dass im Netzwerk ausreichend Bandbreite zur Verfügung steht. Die Hauptlast in Ihrem Netzwerk besteht aus drei Elementen:

- Kamera-Videostreams
- Clients zeigen Video an
- Archivierung von aufgezeichneten Videos

Der Aufzeichnungsserver ruft Videostreams von den Kameras ab, eine konstante Last im Netzwerk nach sich zieht. Clients, die Video anzeigen, verbrauchen Netzwerkbandbreite. Wenn im Inhalt der Client-Ansichten keine Änderungen auftreten, ist die Last konstant. Änderungen im Ansichtsinhalt, Videosuche oder Wiedergabe lassen die Last dynamisch werden.

Die Archivierung von aufgezeichnetem Video ist eine optionale Funktion, die es dem System ermöglicht Aufzeichnungen in einen Netzwerkspeicher zu verschieben, wenn nicht genug Speicherplatz im internen Speicher des Computers vorhanden ist. Dies ist ein geplanter Auftrag, den Sie definieren müssen. Üblicherweise archivieren Sie in einem Netzlaufwerk, wodurch er zu einer geplanten dynamischen Last im Netzwerk wird.

Ihr Netzwerk muss über Bandbreiten-Spielraum verfügen, um diese Spitzen im Datenverkehr zu bewältigen. Damit werden die Reaktionsfähigkeit des Systems und die allgemeine Benutzererfahrung optimiert.

Active Directory vorbereiten

Wenn Sie Benutzer über den Active Directory-Dienst hinzufügen möchten, muss in Ihrem Netzwerk ein Server vorhanden sein, auf dem Active Directory installiert ist und der als Domänen-Controller fungiert.

Zur einfachen Verwaltung von Benutzern und Gruppen empfiehlt Milestone Ihnen, Microsoft Active Directory® zu installieren und zu konfigurieren, bevor Sie Ihr XProtect-System installieren. Wenn Sie den Management-Server nach der Installation Ihres Systems zum Active Directory hinzufügen, müssen Sie den Management-Server neu installieren und die Benutzer durch die im Active Directory neu definierten Windows-Benutzer ersetzen.

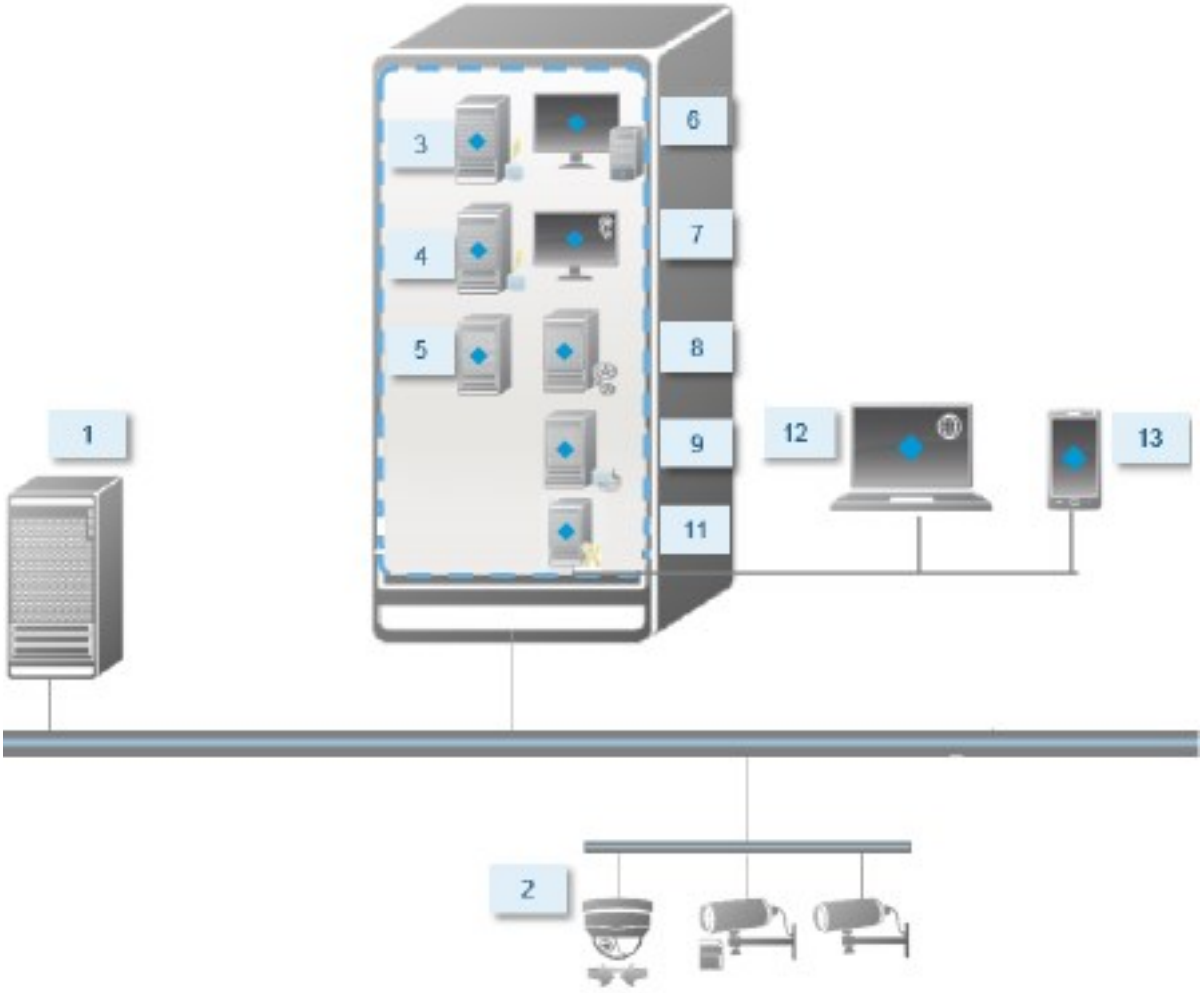
Basisbenutzer werden in Milestone Federated Architecture-Systemen nicht unterstützt. Wenn Sie also beabsichtigen, Milestone Federated Architecture zu verwenden, müssen Sie Benutzer als Windows-Benutzer über den Dienst Active Directory hinzufügen. Wenn Sie Active Directory nicht installieren, befolgen Sie die Schritte in Installation für Arbeitsgruppen auf Seite 103, wenn Sie eine Installation ausführen.

Installationsmethode

Im Installationsassistenten müssen Sie festlegen, welche Installationsmethode Sie verwenden. Sie müssen Ihre Auswahl auf den Anforderungen Ihrer Organisation basieren, aber wahrscheinlich haben Sie die Methode bereits gewählt, als Sie das System kauften.

Optionen	Beschreibung
Einzelcomputer	Installiert alle Server- und Clientkomponenten sowie SQL Server auf dem aktuellen Computer. Nach Abschluss der Installation haben Sie die Möglichkeit, das System mithilfe eines Assistenten zu konfigurieren. Wenn Sie der Fortsetzung zustimmen, durchsucht der Aufzeichnungsserver Ihr Netzwerk nach Hardware, und Sie können auswählen, welche Hardwaregeräte Sie zu Ihrem System hinzufügen möchten. Die maximale Anzahl von Hardwaregeräten, die im Konfigurationsassistenten hinzugefügt werden können, hängt von Ihrer Basislizenz ab. Die Kameraansichten sind außerdem in Ansichten vorkonfiguriert, und eine Standard-Anwenderrolle wird erstellt. Nach der Installation öffnet sich XProtect Smart Client, und das System ist einsatzbereit.
Benutzerdefiniert	Der Managementserver wird immer von der Liste der Systemkomponenten ausgewählt und wird stets installiert; Sie können jedoch frei auswählen, was auf dem aktuellen Computer zusätzlich zu den übrigen Server- und Client-Komponenten noch installiert werden soll. Standardmäßig ist der Aufzeichnungsserver auf der Liste der Komponenten nicht ausgewählt, dies können Sie jedoch ändern. Sie können die nicht ausgewählten Komponenten anschließend auf anderen Computern installieren.

Einzelne Computer-Installation

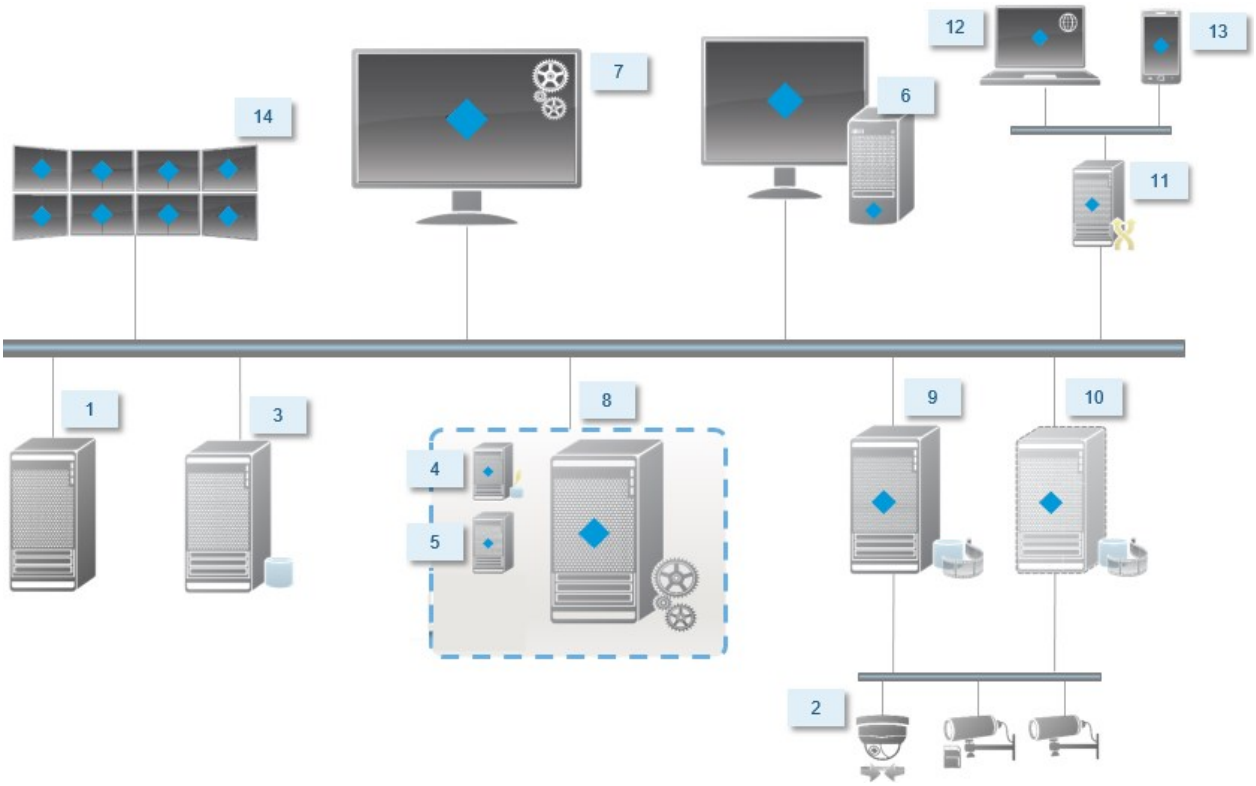


Normalerweise besteht ein System aus folgenden Systemkomponenten:

1. **Active Directory**
2. **Geräte**
3. **Server mit SQL Server**
4. **Ereignisserver**
5. **Protokollserver**
6. **XProtect Smart Client**
7. **Management Client**
8. **Managementserver**

9. **Aufzeichnungsserver**
10. **Failover-Aufzeichnungsserver**
11. **XProtect Mobile-Server**
12. **XProtect Web Client**
13. **XProtect Mobile Client**
14. **XProtect Smart Client mit XProtect Smart Wall**

Benutzerdefinierte Installation - Beispiel für verteilte Systemkomponenten



Entscheiden Sie sich für eine Version von SQL Server

Microsoft® SQL Server® Express ist eine kostenlose Version von SQL Server, die verglichen mit anderen Versionen von SQL Server leicht zu installieren und für den Gebrauch vorzubereiten ist. Während der Installation auf einem **Einzelnen Computer** wird Microsoft SQL Server Express installiert, es sei denn, SQL Server ist auf dem betreffenden Computer bereits installiert.

Die XProtect VMS Installation beinhaltet Microsoft SQL Server Express Version 2019. Nicht alle Windows-Betriebssysteme unterstützen diese Version von SQL Server. Bevor Sie XProtect VMS installieren, überprüfen Sie, ob Ihr Betriebssystem SQL Server 2019 unterstützt. Sollte Ihr Betriebssystem diese Version von SQL Server nicht

unterstützen, installieren Sie eine unterstützte Version von SQL Server, bevor sie mit der XProtect VMS-Installation beginnen. Weitere Angaben zu den unterstützten Ausgaben von SQL Server siehe https://www.milestonesys.com/systemrequirements/ .

Für sehr große Systeme, oder für Systeme mit vielen Transaktionen zu und von den SQL-Datenbanken, empfiehlt Milestone Ihnen, eine Microsoft® SQL Server® Standard oder Microsoft® SQL Server® Enterprise-Ausgabe von SQL Server auf einem eigenen Computer im Netzwerk und auf einem bestimmten Festplattenlaufwerk zu verwenden, das für keine anderen Zwecke verwendet wird. Die Installation von SQL Server auf einem eigenen Laufwerk verbessert die Leistung des gesamten Systems.

Dienstkonto auswählen

Sie werden im Rahmen der Installation aufgefordert, ein Konto anzugeben, um die Milestone-Dienste auf diesem Computer auszuführen. Die Dienste werden immer in diesem Konto ausgeführt, unabhängig davon, welcher Benutzer angemeldet ist. Achten Sie darauf, dass das Konto über alle erforderlichen Benutzerrechte verfügt, beispielsweise die entsprechenden Rechte zum Ausführen von Aufgaben, ausreichender Netzwerk- und Dateizugriff und Zugriff auf die im Netzwerk freigegebenen Ordner.

Sie können zwischen einem vorab definierten Konto und einem Benutzerkonto wählen. Treffen Sie Ihre Entscheidung basierend auf der Umgebung, in der Sie Ihr System installieren möchten:

Domänenumgebung

In einer Domänenumgebung:

- Milestone empfiehlt, dass Sie das eingebaute Netzwerkkonto verwenden

  Es ist einfacher zu verwenden, auch wenn Sie das System auf mehrere Computer erweitern müssen.

- Sie können auch Domänenbenutzerkonten verwenden, aber sie sind möglicherweise schwerer zu konfigurieren

Arbeitsgruppenumgebung

In einer Arbeitsgruppenumgebung empfiehlt Milestone, dass Sie ein lokales Benutzerkonto verwenden, das über alle erforderlichen Rechte verfügt. Hierbei handelt es sich häufig um das Administratorkonto.

> ⚠ Wenn sich die Installationen über mehrere Computer erstrecken, muss das ausgewählte Benutzerkonto auf allen Computern in Ihren Installationen mit identischem Benutzernamen, Kennwort und Zugriffsrechten konfiguriert werden.

Kerberos Authentifizierung (Erklärung)

Kerbero ist ein auf Tickets basierendes Netzwerkauthentifizierungsprotokoll. Es wurde als eine starke Authentifizierung für Client/Server oder Server/Server Anwendungen entwickelt.

Nutzen Sie die Kerberos-Authentifizierung als Alternative zum älteren Microsoft NT LAN-Authentifizierungsprotokoll (NTLM).

Eine Kerbero-Authentifizierung erfordert eine gegenseitige Authentifizierung, bei der der Client den Dienst und der Dienst wiederum den Client authentifiziert. Auf diese Weise können Sie eine sicherere Authentifizierung von XProtect-Clients zu XProtect-Servern sicherstellen, ohne Ihr Passwort preiszugeben.

Sie müssen die Service Principal Names (SPN) im Active Directory registrieren, um eine gegenseitige Authentifizierung in Ihrem XProtect VMS zu ermöglichen. Ein SPN ist ein Pseudonym, das auf eine Entität, wie einen XProtect-Serverdienst eindeutig identifiziert. Jeder Dienst, der gegenseitige Authentifizierung verwendet, muss einen registrierten SPN besitzen, damit Clients den Dienst im Netzwerk identifizieren können. Eine gegenseitige Authentifizierung ist ohne ordnungsgemäße registrierte SPN nicht möglich.

Die nachfolgende Tabelle listet die verschiedenen Milestone-Dienste mit den korrespondierenden Portnummern auf, die für eine Registrierung benötigt werden:

Dienst	Portnummer
Managementserver – IIS	80 - Konfigurierbar
Managementserver – Intern	8080
Aufzeichnungsserver - Data Collector	7609
Failover Server	8990
Ereignisserver	22331
LPR Server	22334

Die Anzahl der Dienste, die Sie im Active Directory ihrer gegenwärtigen Installation registrieren müssen. Data Collector wird bei der Installation des Managementserver, Aufzeichnungsserver, Ereignisserver oder Failover Server Dienstes automatisch installiert.

Sie müssen für den Benutzer, der den Dienst ausführt, zwei SPNs registrieren: einen mit dem Hostnamen und einen mit dem voll qualifizierten Domainnamen.

Wenn Sie den Dienst unter einem Netzwerkdienstkonto ausführen, müssen Sie die zwei SPN für jeden Computer registrieren, die den Dienst ausführen.

Dies ist das Milestone SPN-Benennungsschema:

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[vollständig qualifizierten Domainamen]:[Port]
```

Hier ein Beispiel für SPNs für den Aufzeichnungsserver-Dienst, der auf einem Computer mit den folgenden Spezifikationen ausgeführt wird:

```
Hostname: Record-Server1
Domäne: Surveillance.com
```

Zu registrierende SPNs:

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

Virus scanning exclusions (Erläuterung)

Wenn ein Antivirus-Programm wie im Fall anderer Datenbanksoftware auf einem Computer installiert wird, auf dem XProtect-Software ausgeführt wird, ist es wichtig, dass sie spezifische Dateitypen und Ordner und bestimmte Arten von Netzwerkverkehr ausschließen. Wenn Sie diese Ausnahme nicht einrichten, werden Virenscans einen erheblichen Anteil der Systemressourcen beanspruchen. Darüber hinaus kann der Scanprozess vorübergehend Dateien sperren, was zu einer Unterbrechung im Aufzeichnungsprozess oder sogar einer Beschädigung der Datenbanken führen würde.

Wenn Sie den Virenscan ausführen müssen, scannen Sie keine Aufzeichnungsserver-Verzeichnisse, die Aufzeichnungsdatenbanken enthalten (standardmäßig C:\mediadatabase\, sowie alle Unterordner). Vermeiden Sie auch den Virenscan in Archivspeicher-Verzeichnissen.

Erstellen Sie die folgenden zusätzlichen Ausschlüsse:

- Dateitypen: .blk, .idx, .pic
- Ordner und Unterordner:
  - C:\Program Files\Milestone oder C:\Program Files (x86)\Milestone
  - C:\Programdaten\Milestone\MIPSDK
  - C:\Programdaten\Milestone\XProtect Mobile Server\Logs
  - C:\Programmdaten\Milestone\XProtect Data Collector Server\Logs
  - C:\ProgramData\Milestone\XProtect Event Server\Logs
  - C:\Programmdaten\Milestone\XProtect Log Server
  - C:\Programmdaten\Milestone\XProtect Management Server\Logs
  - C:\Programmdaten\Milestone\XProtect Recording Server\Logs
  - C:\Programmdaten\Milestone\XProtect Report Web Server\Logs
- Netzwerkscans an den folgenden TCP-Ports ausschließen:

Produkt	TCP-Ports
XProtect VMS	80, 8080, 7563, 25, 21, 9000
XProtect Mobile	8081

oder

- Netzwerkscans der folgenden Prozesse ausschließen:

Produkt	Prozesse
XProtect VMS	VideoOS.Recorder.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe

Ihre Organisation hat möglicherweise strenge Richtlinien in Bezug auf Virenscans, es ist jedoch wichtig, dass die oben aufgeführten Ordner und Dateien von Virenscans ausgenommen werden.

Wie ist XProtect VMS so zu konfigurieren, dass es im FIPS 140-2-konformen Modus läuft?

Um XProtect VMS in einem FIPS 140-2-Betriebsmodus auszuführen, müssen Sie:

- Das Windows-Betriebssystem in einem FIPS 140-2-genehmigten Betriebsmodus ausführen. Siehe die Microsoft-Internetseite zu Informationen dazu, wie FIPS aktiviert wird.
- Achten Sie darauf, dass eigenständige Dritt-Integrationen auf einem FIPS-fähigen Windows-Betriebssystem laufen können
- Stellen Sie Verbindungen zu Geräten so her, dass ein FIPS 140-2-konformer Betriebsmodus gewährleistet ist
- Achten Sie darauf, dass Daten in Mediendatenbanken mithilfe von FIPS 140-2-konformen Chiffren verschlüsselt werden

  Dies erfolgt durch Ausführung des Upgrade-Tools für Mediendatenbanken. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

Bevor Sie XProtect VMS auf einem FIPS-fähigen System installieren

Während neue Installation von XProtect VMS auf Computern erfolgen können, die FIPS-fähig sind, können Sie kein Upgrade von XProtect VMS durchführen, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist.

Wenn Sie ein Upgrade vornehmen, deaktivieren Sie vor der Installation die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem der SQL-Server gehosted wird.

Das Installationsprogramm für XProtect VMS prüft die FIPS-Sicherheitsrichtlinie und verhindert die Installation, wenn FIPS aktiviert ist.

Wenn Sie allerdings ein Upgrade von XProtect VMS Version 2020 R3 oder später vornehmen, brauchen Sie FIPS nicht zu deaktivieren.

Wenn Sie die Komponenten von XProtect VMS auf allen Computern installiert und das System für FIPS vorbereitet haben, können Sie die FIPS-Sicherheitsrichtlinie auf Windows auf allen Computern in Ihrem VMS aktivieren.

Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

Softwarelizenzcode registrieren

Vor der Installation müssen Sie über den Namen und den Speicherort der Softwarelizenzdatei verfügen, die Sie von Milestone erhalten haben.

Sie können eine kostenlose Version von XProtect Essential+ installieren. Diese Version bietet eingeschränkte Funktionen von XProtect VMS für eine begrenzte Zahl von Kameras. Zum Installieren von XProtect Essential+ benötigen Sie eine Internetverbindung.

Der Softwarelizenzcode (SLC) ist auf Ihrer Bestellbestätigung gedruckt und die Softwarelizenzdatei ist nach Ihrer SLC benannt.

Milestone empfiehlt, dass Sie Ihren SLC vor der Installation auf unserer Website (https://online.milestonesys.com/) registrieren. Ihr Händler hat dies gegebenenfalls bereits für Sie erledigt.

Gerätetreiber (Erklärung)

Ihr System verwendet Videogerätetreiber, um die mit einem Aufzeichnungsserver verbundenen Kameras zu steuern und mit ihnen zu kommunizieren. Die Gerätetreiber müssen auf jeden Aufzeichnungsserver Ihres System installiert werden.

Ab der Ausgabe 2018 R1 sind die Gerätetreiber in zwei Gerätepacks aufgeteilt: das reguläre Gerätepaket mit neueren Treibern und ein Stamm-Gerätepaket mit älteren Treibern.

Das reguläre Gerätepaket wird automatisch installiert, wenn Sie den Aufzeichnungsserver installieren. Später können Sie die Treiber aktualisieren, indem Sie eine neuere Version des Gerätepakets herunterladen und installieren. Milestone veröffentlicht regelmäßig neue Versionen von Gerätetreibern und stellt diese als Treiberpaket auf der Download-Seite (https://www.milestonesys.com/downloads/) unserer Webseite zur Verfügung. Bei der Aktualisierung eines Gerätepakets können Sie die neueste Version über jede zuvor installierte Version installieren.

Das Stammgerätepaket kann nur installiert werden, wenn ein reguläres Gerätepaket im System installiert ist. Die Treiber aus dem Stammgerätepaket werden automatisch installiert, wenn eine vorige Version bereits auf Ihrem System installiert ist. Es steht zur Verfügung zum manuellen Herunterladen und Installieren auf der Software-Download-Seite (https://www.milestonesys.com/downloads/).

Stoppen Sie den Aufzeichnungsserver-Dienst vor der Installation, andernfalls müssen Sie den Computer neu starten.

Damit eine optimale Leistung garantiert ist, sollten Sie immer die neuesten Gerätetreiber verwenden.

Anforderungen für Offline-Installationen

Wenn Sie das System auf einem Server installieren, der offline ist, benötigen Sie Folgendes:

- Die `Milestone XProtect VMS-Produkte 2020 R3 System Installer.exe`-Datei
- Die Softwarelizenzdatei (SLC) für Ihr XProtect-System
- Ein Medium zur Installation eines Betriebssystems, einschließlich der erforderlichen .NET-Version (https://www.milestonesys.com/systemrequirements/)

Sichere Kommunikation (Erläuterung).

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

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

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

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

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

> Zertifikate haben ein Verfalldatum. XProtect VMS gibt Ihnen keine Wawrnung, wenn das Zertifikat in Kürze abläuft. Wenn ein Zertifikat abläuft:
> - Die Clients vertrauen dann nicht mehr dem Aufzeichnungsserver mit dem abgelaufenen Zertifikat und können daher auch nicht mehr mit ihm kommunizieren.
> - Die Aufzeichnungsserver vertrauen dann nicht mehr dem Managementserver mit dem abgelaufenen Zertifikat und können daher auch nicht mehr mit ihm kommunizieren.
> - Die mobilen Geräte vertrauen dann nicht mehr dem Mobile Server mit dem abgelaufenen Zertifikat und können daher auch nicht mehr mit ihm kommunizieren
>
> Um die Zertifikate zu erneuern, folgen Sie den Schritten in dieser Anleitung, wie Sie es bereits getan haben, als Sie Zertifikate erstellt haben.

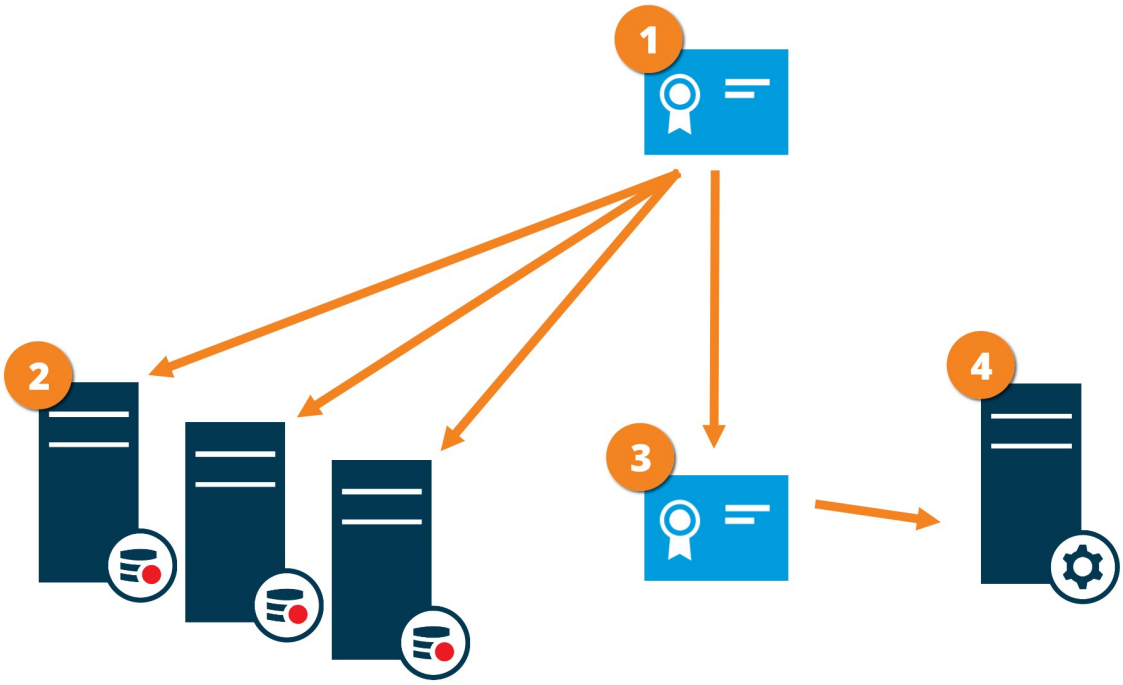
Wenn Sie ein Zertifikat mit demselben Themennamen erneuern und es zum Windows Certificate Store hinzufügen, so übernehmen die Server automatisch das neue Zertifikat. Dies erleichtert das Erneuern für viele Server, ohne dass das Zertifikat für jeden Aufzeichnungsserver erneut ausgewählt werden muss und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

Verschlüsselung des Managementservers (Erläuterung):

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

Verteilung von Zertifikaten für Managementserver

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



❶ Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl das Thema/der Eigentümer (Managementserver) vertraut, als auch die Partei, die das Zertifikat überprüft (Aufzeichnungsserver)

❷ Dem CA-Zertifikat muss auf allen Aufzeichnungsservern vertraut werden. So überprüfen die Aufzeichnungsserver die Gültigkeit der von der CA ausgegebenen Zertifikate

❸ Das CA-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen dem Managementserver und den Aufzeichnungsservern

❹ Das CA-Zertifikat muss auf dem Computer installiert werden, auf dem der Managementserver läuft

Anforderungen für das private Zertifikat des Managementservers:

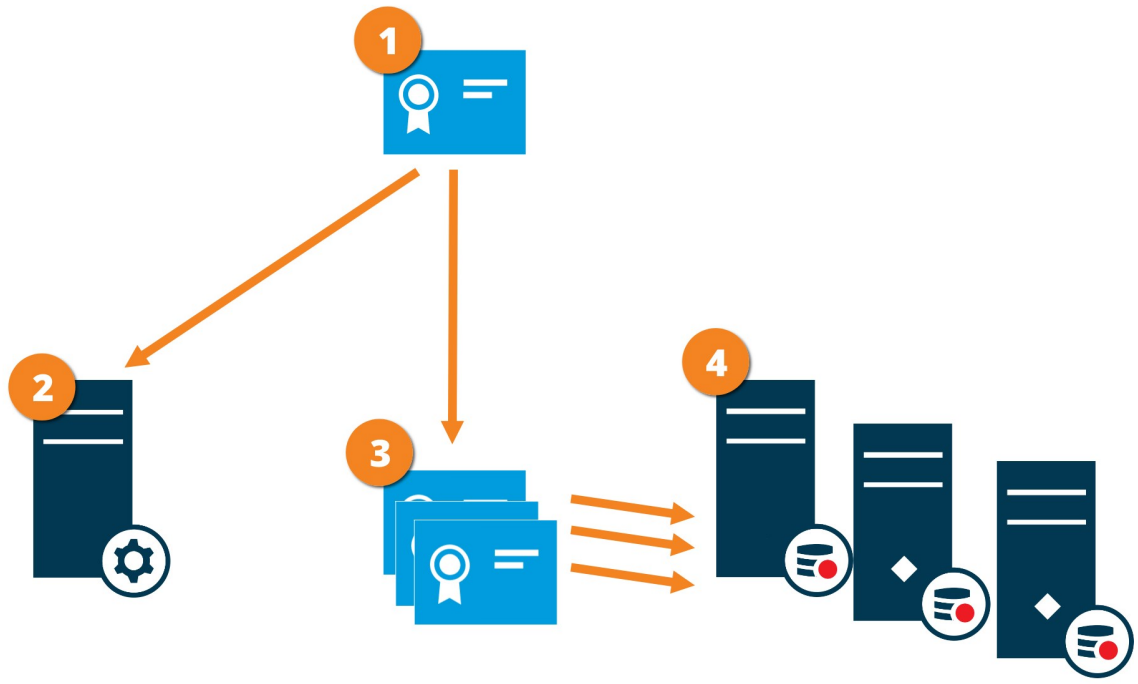
- Wird dem Aufzeichnungsserver ausgestellt, damit der Hostname des Aufzeichnungsservers im Namen des Zertifikates enthalten ist, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, an die das Zertifikat ausgegeben wird
- Wird auf dem Managementserver selbst vertraut, indem dem CA-Zertifikat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

Verschlüsselung vom Management-Server zum Aufzeichnungsserver (Erläuterung)

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

Verteilung von Zertifikaten

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



❶ Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl Thema/Eigentümer (Aufzeichnungsserver) vertraut, als auch die Partei, die das Zertifikat überprüft (Management-Server)

❷ Dem öffentlichen CA-Zertifikat muss auf dem Management-Server vertraut werden. So überprüft der Management Server die Gültigkeit der von der CA ausgegebenen Zertifikate

❸ Das CA-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen den Aufzeichnungsservern und dem Management-Server

❹ Das CA-Zertifikat muss auf den Computern installiert werden, auf denen die Aufzeichnungsserver laufen

Anforderungen für das Zertifikat des privaten Aufzeichnungsservers:

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

Verschlüsselung zwischen dem Management Server und den Data Collector Server (Erläuterung)

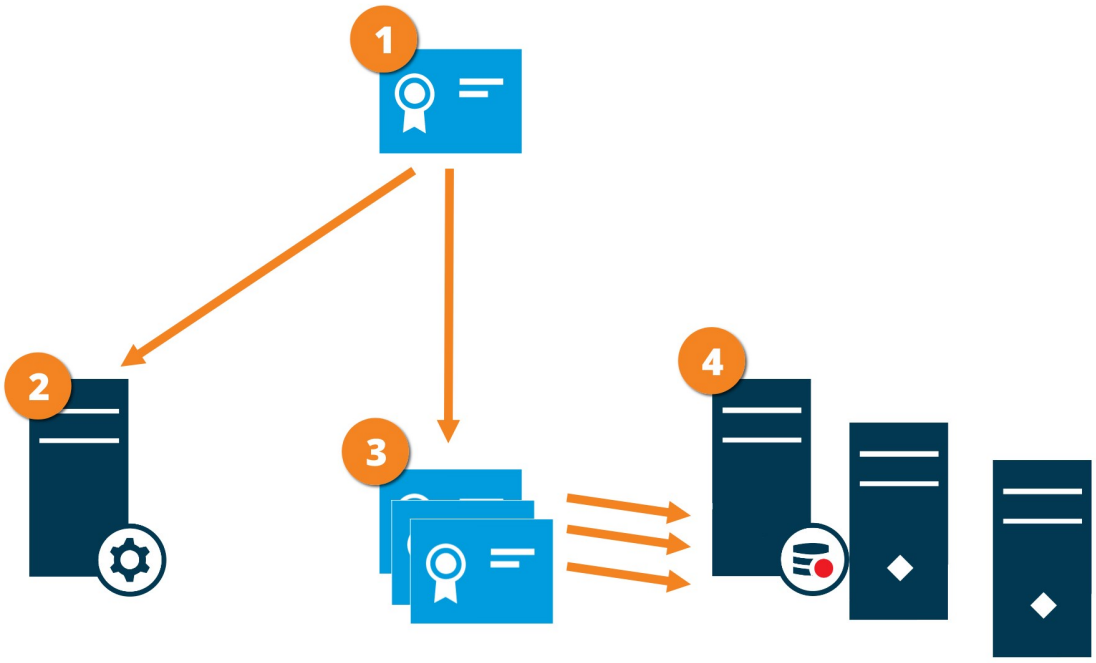
Sie können die wechselseitige Verbindung zwischen dem Managementserver und dem davon abhängigen Data Collector verschlüsseln, wenn Sie einen Remote Server des folgenden Typs haben:

- Aufzeichnungsserver
- Ereignisserver
- Protokollserver
- LPR Server
- Mobile Server

Wenn Sie die Verschlüsselung auf dem Managementserver aktivieren, so gilt diese für die Verbindungen von allen Data Collector-Servern, die eine Verbindung zum Managementserver herstellen. Die Verschlüsselung dieser Kommunikation muss nach den Einstellungen für die Verschlüsselung auf dem Management-Server erfolgen. Ist daher die Verschlüsselung auf dem Management Server aktiviert, so muss sie auch auf den Data Collector-Servern aktiviert werden, die mit jedem der Remote Server verknüpft sind, und umgekehrt. Bevor Sie die Verschlüsselung aktivieren, müssen Sie auf dem Managementserver und auf allen Data Collector-Servern, die mit Remote Servern verknüpft sind, Sicherheitszertifikate installieren.

Verteilung von Zertifikaten

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



❶ Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl Thema/Eigentümer (Datensammlerserver) vertrauen als auch die Partei, die das Zertifikat überprüft (Management Server)

❷ Dem öffentlichen CA-Zertifikat muss auf dem Management-Server vertraut werden. So überprüft der Management Server die Gültigkeit der von der CA ausgegebenen Zertifikate

❸ Das CA-Zertifikat dient zur Herstellung einer sicheren Verbindung zwischen den Datensammlerservern und dem Management Server

❹ Das CA-Zertifikat muss auf den Computern installiert werden, auf denen die Datensammlerserver laufen

Anforderungen für das Zertifikat des privaten Datensammlerserver:

- Es wird dem Server ausgestellt, damit der Hostname des Datensammlerservers im Zertifikat enthalten ist, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, denen das Zertifikat ausgestellt wird
- Wird auf dem Managementserver vertraut, indem dem CA-Zertifikat vertraut wird, das zur Ausstellung des Datensammlerserverzertifikates verwendet wurde

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

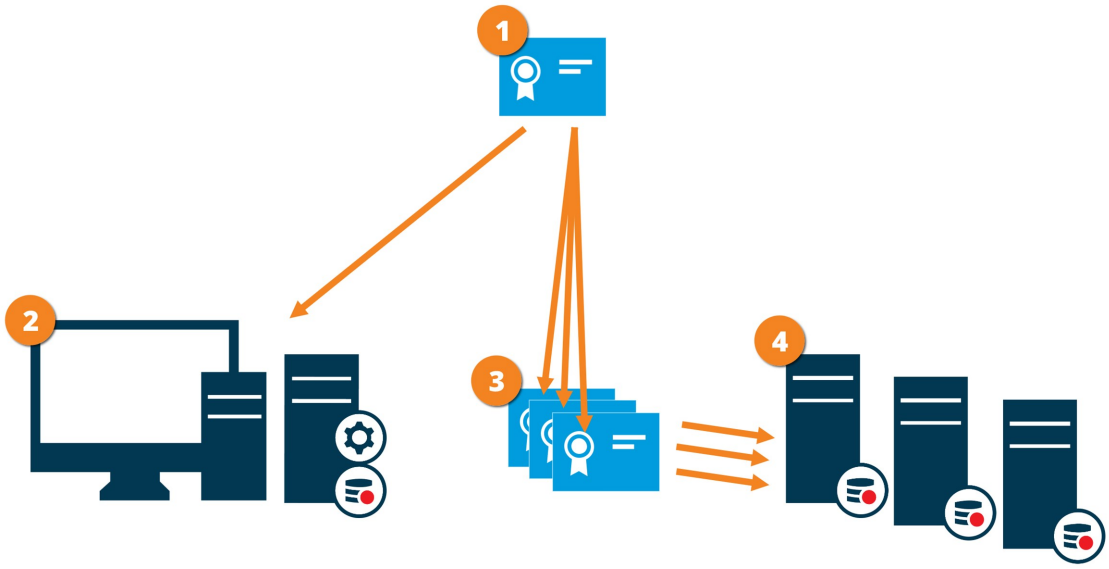
Wenn Sie auf einem Aufzeichnungsserver die Verschlüsselung aktivieren, wird die Kommunikation aller Clients, Server und Integrationen verschlüsselt, die Datenstreams vom Aufzeichnungsserver abrufen. Diese werden in diesem Dokument als 'Clients' bezeichnet:

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

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

Verteilung von Zertifikaten

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



❶ Ein CA fungiert als vertrauenswürdiger Dritter, dem sowohl Thema/Eigentümer (Aufzeichnungsserver) vertrauen, als auch die Partei, die das Zertifikat überprüft (alle Clients)

❷ Dem öffentlichen CA-Zertifikat muss auf allen Clientcomputern vertraut werden. So überprüfen die Clients die Gültigkeit der von der CA ausgegebenen Zertifikate

❸ Das CA-Zertifikat dient zum Aufbau einer sicheren Verbindung zwischen den Aufzeichnungsservern und allen Clients und Diensten

❹ Das CA-Zertifikat muss auf den Computern installiert werden, auf denen die Aufzeichnungsserver laufen

Anforderungen für das Zertifikat des privaten Aufzeichnungsservers:

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

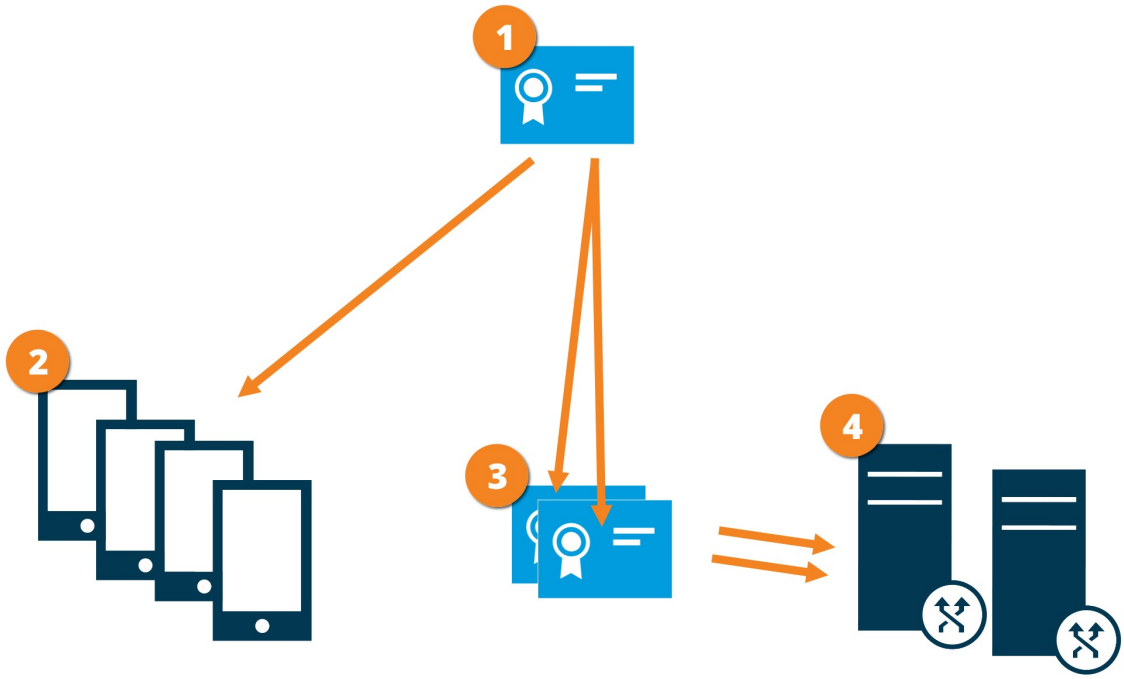
Wenn Sie auf den Aufzeichnungsservern die Verschlüsselung aktivieren, und Ihr System verwendet Failover-Aufzeichnungsserver, so empfiehlt Milestone, dass Sie die Failover-Aufzeichnungsserver ebenfalls dafür vorbereiten, dass sie eine Verschlüsselung verwenden.

Datenverschlüsselung des mobilen Servers (Erläuterung)

In XProtect VMS wird die Verschlüsselung für jeden mobilen Server aktiviert oder deaktiviert. Wenn Sie die Verschlüsselung auf einem mobilen Server aktivieren, so können Sie sich aussuchen, ob Sie die verschlüsselte Kommunikation mit allen Clients, Diensten und Integrationen verwenden wollen, die Datenstreams abrufen.

Verteilung von Zertifikaten für mobile Server

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



1 Eine CA fungiert als vertrauenswürdiger Dritter, dem sowohl das Thema/der Eigentümer (mobiler Server) vertraut, als auch die Partei, die das Zertifikat überprüft (alle Clients).

2 Dem öffentlichen CA-Zertifikat muss auf allen Clientcomputern vertraut werden. So überprüfen die Clients die Gültigkeit der von der CA ausgegebenen Zertifikate

3 Das CA-Zertifikat dient zur sicheren Verbindung zwischen dem mobilen Server und Clients und Diensten

4 Das CA-Zertifikat muss auf dem Computer installiert werden, auf dem der mobile Server läuft

Anforderungen für das CA-Zertifikat:

- Der Hostname des mobilen Servers muss im Zertifikates enthalten sein, entweder als Thema (Besitzer) oder in der Liste der DNS-Namen, an die das Zertifikat ausgegeben wird
- Dem Zertifikat muss von allen Computern vertraut werden, die Dienste ausführen, die Datenstreams vom mobilen Server abrufen
- Das Dienstkonto, auf dem der Aufzeichnungsserver läuft, muss Zugriff zum privaten Schlüssel des CA-Zertifikates haben.

Anforderungen zur Verschlüsselung mobiler Server für Clients

Wenn Sie die Verschlüsselung nicht aktivieren und keine HTTP-Verbindung verwenden, so steht die Push-to-Talk-Funktion in XProtect Web Client später nicht zur Verfügung.

Installation

Installation eines neuen XProtect-Systems

Installieren Sie XProtect Essential+

Sie können eine kostenlose Version von XProtect Essential+ installieren. Diese Version bietet eingeschränkte Funktionen von XProtect VMS für eine begrenzte Zahl von Kameras. Zum Installieren von XProtect Essential+ benötigen Sie eine Internetverbindung.

Diese Version wird unter Nutzung der Installationsoption **Einzelcomputer** auf einem einzigen Computer installiert. Die Option **Einzelcomputer** installiert alle Server- und Client-Komponenten auf dem aktuellen Rechner.

Milestone empfiehlt Ihnen, vor der Installation den folgenden Abschnitt sorgfältig durchzulesen: Vor dem Start der Installation auf Seite 59.

Für FIPS-Installationen können Sie kein Upgrade von XProtect VMS durchführen, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist. Deaktivieren Sie vor der Installation die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem der SQL-Server gehosted wird. Wenn Sie allerdings ein Upgrade von XProtect VMS Version 2020 R3 oder später vornehmen, brauchen Sie FIPS nicht zu deaktivieren. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

Nach der Erstinstallation können Sie mit dem Konfigurationsassistenten fortfahren. Je nach Hardware und Konfiguration scannt der Aufzeichnungsserver Ihr Netzwerk nach Hardware. Sie können dann die Hardwaregeräte auswählen, die zu Ihrem System hinzugefügt werden sollen. Kameras sind in Ansichten vorkonfiguriert, und Sie haben die Option zum Aktivieren anderer Geräte wie Mikrofone und Lautsprecher. Sie haben auch die Option, Benutzer entweder mit einer Bedienerrolle oder mit einer Administratorrolle zum System hinzuzufügen. Nach der Installation öffnet sich XProtect Smart Client, und das System ist einsatzbereit.

Andernfalls, wenn Sie den Installationsassistenten schließen, wird XProtect Management Client geöffnet, wo Sie manuelle Konfigurationen vornehmen können, wie z.B. zum Hinzufügen von Hardwaregeräten und Benutzern zum System.

Wenn Sie Aktualisierungen von einer vorherigen Version des Produkts durchführen, sucht das System nicht nach Hardware oder erzeugt neue Ansichten und Benutzerprofile.

1. Sie können die Software kostenlos aus dem Internet herunterladen (https://www.milestonesys.com/downloads/) und die Datei `Milestone XProtect VMS-Produkte 2020 R3 System Installer.exe` ausführen.
2. Die Installationsdateien werden entpackt. Abhängig von Ihren Sicherheitsseinstellungen erscheinen eine oder mehrere Windows® Sicherheitswarnungen. Akzeptieren Sie diese, um mit dem Entpacken fortzufahren.
3. Nach Abschluss dieses Vorganges erscheint der **Milestone XProtect VMS** Installationsassistent.
    1. Wählen Sie die während der Installation zu verwendende **Sprache** aus (dies ist nicht die Sprache, die Ihr System nach erfolgter Installation verwendet; diese Einstellung erfolgt später). Klicken Sie auf **Weiter**.
    2. Lesen Sie den *Milestone Endbenutzer-Lizenzvertrag*. Wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen dieser Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
    3. Klicken Sie auf das Link **XProtect Essential+**, um eine kostenlose Lizenzdatei herunterzuladen.

       Die kostenlose Lizenz wird heruntergeladen und erscheint dann im Feld **Speicherort für die Lizenzdatei eingeben oder suchen**. Klicken Sie auf **Weiter**.
4. Wählen Sie **Einzelcomputer** aus.

   Eine Liste der zu installierenden Komponenten wird angezeigt (Sie können diese Liste nicht bearbeiten). Klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Passwort für Systemkonfiguration zuweisen** ein Passwort ein, das Ihre Systemkonfiguration schützt. Dieses Passwort benötigen Sie, falls eine Systemwiederherstellung erforderlich wird oder wenn Sie Ihr System erweitern, z.B. indem Sie Cluster hinzufügen.

   > Es ist wichtig, dass Sie dieses Passwort sicher aufbewahren. Wenn Sie dieses Passwort verlieren, sind Sie ggf. nicht mehr in der Lage, Ihre Systemkonfiguration wiederherzustellen.

   Wenn Sie Ihre Systemkonfiguration nicht mit einem Passwort schützen wollen, wählen Sie **Ich möchte kein Passwort zum Schutz der Systemkonfiguration verwenden, und mir ist klar, dass die Systemkonfiguration dann nicht verschlüsselt ist**.

   Klicken Sie auf **Weiter**.

6. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an:
    1. Geben Sie den Namen des Aufzeichnungsservers im Feld **Aufzeichnungsserver-Name** ein. Der Standardwert ist der Name des Computers.
    2. Das Feld für die **Management-Server-Adresse** zeigt die Adresse und Port-Nummer des Management-Servers: localhost:80.
    3. Wählen Sie im Feld **Wahl des Speicherorts für die Medien-Datenbank** den Speicherort aus, an dem Sie Ihre Video-Aufzeichnungen speichern möchten. Milestone empfiehlt, einen anderen Speicherort für Ihre Videoaufnahmen zu wählen als den Ort der Programminstallation oder das System-Laufwerk. Der Standard-Speicherort ist das Laufwerk mit der höchsten freien Speicherkapazität.
    4. Geben Sie in dem Feld **Speicherdauer für Video-Aufnahmen** an, wie lange die Videoaufnahmen gespeichert werden sollen. Sie können von 1 bis 999 Tage eingeben, wobei die Standard-Retentionszeit 7 Tage beträgt.
    5. Klicken Sie auf **Weiter**.

7. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

   - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

     Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

     > Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

   - Zwischen den Aufzeichnungsservern und den Clients

     Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

   - Zwischen dem Mobile Server und den Clients

     Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

   Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

   Weitere Informationen zur Vorbereitung Ihres System für die sichere Kommunikation finden Sie unter Sichere Kommunikation (Erläuterung). auf Seite 69 sowie im Milestone Leitfaden zu Zertifikaten.

   Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.

8. Tun Sie im Fenster **Auswahl des Dateispeicherorts und der Produktsprache** folgendes:

   1. Wählen Sie im Feld **Dateispeicherort** den Speicherort, an dem Sie die Software installieren wollen.

      > Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

   2. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll.
   3. Klicken Sie auf **Installieren**.

   Die Software wird nun installiert. Microsoft® SQL Server® Express und Microsoft IIS werden während der Installation automatisch installiert, falls dies auf dem betreffenden Computer noch nicht erfolgt ist.

9. Sie werden ggf. aufgefordert, Ihren Computer neu zu starten. Nach dem Neustart erscheinen je nach Ihren Sicherheitseinstellungen möglicherweise eine oder mehrere Windows-Sicherheitswarnungen. Akzeptieren Sie diese, um die Installation abzuschließen.
10. Wenn die Installation abgeschlossen ist, wird eine Liste der auf dem Rechner installierten Komponenten angezeigt.

    Klicken Sie auf **Fortfahren**, um Hardware und Benutzer zum System hinzuzufügen.

    > Wenn Sie jetzt auf **Schließen** klicken, umgehen Sie den Konfigurationsassistenten, und XProtect Management Client wird geöffnet. Sie können das System konfigurieren, z.B. um in Management Client Hardware und Benutzer hinzuzufügen.

11. Geben Sie auf der Seite **Benutzernamen und Passwörter für Hardware eingeben** die Benutzernamen und Passwörter für die Hardware ein, in die Sie die vom Hersteller vorgegebenen geändert haben.

    Das Installationsprogramm sucht im Netzwerk nach dieser Hardware sowie nach Hardware mit Standardanmeldeinformationen des Herstellers.

    Klicken Sie auf **Weiter** und warten Sie ab, während das System nach der Hardware sucht.
12. Wählen Sie auf der Seite **Auswahl der zum System hinzuzufügenden Hardware** die Hardware aus, die Sie zum System hinzufügen wollen. Klicken Sie auf **Weiter** und warten Sie ab, während das System die Hardware hinzufügt.
13. Auf der Seite **Konfiguration der Geräte** können Sie die Hardware beschreibende Namen eingeben, indem Sie auf das Bearbeitungssymbol neben dem Hardwarenamen klicken. Dieser Name wird dann den Hardwaregeräten vorangestellt.

    Erweitern Sie den Hardware-Knoten, um Hardwaregeräte wie Kameras, Lautsprecher und Mikrofone zu aktivieren oder zu deaktivieren.

    > Kameras werden standardmäßig aktiviert, und Lautsprecher und Mikrofone werden standardmäßig deaktiviert.

    Klicken Sie auf **Weiter** und warten Sie ab, während das System die Hardware konfiguriert.
14. Auf der Seite **Benutzer hinzufügen** können Sie zum System Benutzer als Windows-Benutzer oder als Basisbenutzer hinzufügen. Diese Benutzer können entweder die Rolle des Administrators oder die eines Benutzers spielen.

    Definieren Sie den Benutzer und klicken Sie auf **Hinzufügen**.

    Wenn Sie das Hinzufügen von Benutzern beenden, klicken Sie auf **Fortfahren**.

15. Wenn die Installation und Erstkonfiguration beendet sind, erscheint die Seite **Konfiguration ist beendet**, auf der Folgendes angezeigt wird:
    - Eine Liste der zum System hinzugefügten Hardwaregeräte
    - Eine Liste von zum System hinzugefügten Benutzern
    - Die Adressen zum XProtect Web Client und XProtect Mobile-Client, die Sie an Ihre Benutzer weitergeben können

    Wenn Sie auf **Schließen** klicken, wird XProtect Smart Client geöffnet und steht zur Benutzung bereit.

Systeminstallation - Einzel-Computer-Option

Die Option **Einzelcomputer** installiert alle Server- und Client-Komponenten auf dem aktuellen Rechner.

Milestone empfiehlt Ihnen, vor der Installation den folgenden Abschnitt sorgfältig durchzulesen: Vor dem Start der Installation auf Seite 59.

Für FIPS-Installationen können Sie kein Upgrade von XProtect VMS durchführen, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist. Deaktivieren Sie vor der Installation die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem der SQL-Server gehosted wird. Wenn Sie allerdings ein Upgrade von XProtect VMS Version 2020 R3 oder später vornehmen, brauchen Sie FIPS nicht zu deaktivieren. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

Nach der Erstinstallation können Sie mit dem Konfigurationsassistenten fortfahren. Je nach Hardware und Konfiguration scannt der Aufzeichnungsserver Ihr Netzwerk nach Hardware. Sie können dann die Hardwaregeräte auswählen, die zu Ihrem System hinzugefügt werden sollen. Kameras sind in Ansichten vorkonfiguriert, und Sie haben die Option zum Aktivieren anderer Geräte wie Mikrofone und Lautsprecher. Sie haben auch die Option, Benutzer entweder mit einer Bedienerrolle oder mit einer Administratorrolle zum System hinzuzufügen. Nach der Installation öffnet sich XProtect Smart Client, und das System ist einsatzbereit.

Andernfalls, wenn Sie den Installationsassistenten schließen, wird XProtect Management Client geöffnet, wo Sie manuelle Konfigurationen vornehmen können, wie z.B. zum Hinzufügen von Hardwaregeräten und Benutzern zum System.

Wenn Sie Aktualisierungen von einer vorherigen Version des Produkts durchführen, sucht das System nicht nach Hardware oder erzeugt neue Ansichten und Benutzerprofile.

1. Sie können die Software kostenlos aus dem Internet herunterladen (https://www.milestonesys.com/downloads/) und die Datei `Milestone XProtect VMS-Produkte 2020 R3 System Installer.exe` ausführen.
2. Die Installationsdateien werden entpackt. Abhängig von Ihren Sicherheitsseinstellungen erscheinen eine oder mehrere Windows® Sicherheitswarnungen. Akzeptieren Sie diese, um mit dem Entpacken fortzufahren.
3. Nach Abschluss dieses Vorganges erscheint der **Milestone XProtect VMS** Installationsassistent.
    1. Wählen Sie die während der Installation zu verwendende **Sprache** aus (dies ist nicht die Sprache, die Ihr System nach erfolgter Installation verwendet; diese Einstellung erfolgt später). Klicken Sie auf **Weiter**.
    2. Lesen Sie den *Milestone Endbenutzer-Lizenzvertrag*. Wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen dieser Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
    3. Geben Sie im Feld **Geben Sie den Speicherort der Lizenzdatei ein bzw. navigieren Sie dort hin** die Lizenzdatei an, die Sie von Ihrem XProtect-Anbieter erhalten haben. Alternativ können Sie auch zum Dateispeicherort navigieren , oder Sie klicken auf das Link **XProtect Essential+** um eine kostenlose Lizenzdatei herunterzuladen. Zu den Einschränkungen des kostenlosen XProtect Essential+ Produktes siehe die Produktvergleichstabelle auf Seite 46. Das System überprüft Ihre Lizenzdatei, bevor Sie fortfahren können. Klicken Sie auf **Weiter**.
4. Wählen Sie **Einzelcomputer** aus.

    Eine Liste der zu installierenden Komponenten wird angezeigt (Sie können diese Liste nicht bearbeiten). Klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Passwort für Systemkonfiguration zuweisen** ein Passwort ein, das Ihre Systemkonfiguration schützt. Dieses Passwort benötigen Sie, falls eine Systemwiederherstellung erforderlich wird oder wenn Sie Ihr System erweitern, z.B. indem Sie Cluster hinzufügen.

    > Es ist wichtig, dass Sie dieses Passwort sicher aufbewahren. Wenn Sie dieses Passwort verlieren, sind Sie ggf. nicht mehr in der Lage, Ihre Systemkonfiguration wiederherzustellen.

    Wenn Sie Ihre Systemkonfiguration nicht mit einem Passwort schützen wollen, wählen Sie **Ich möchte kein Passwort zum Schutz der Systemkonfiguration verwenden, und mir ist klar, dass die Systemkonfiguration dann nicht verschlüsselt ist**.

    Klicken Sie auf **Weiter**.

6. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an:
    1. Geben Sie den Namen des Aufzeichnungsservers im Feld **Aufzeichnungsserver-Name** ein. Der Standardwert ist der Name des Computers.
    2. Das Feld für die **Management-Server-Adresse** zeigt die Adresse und Port-Nummer des Management-Servers: localhost:80.
    3. Wählen Sie im Feld **Wahl des Speicherorts für die Medien-Datenbank** den Speicherort aus, an dem Sie Ihre Video-Aufzeichnungen speichern möchten. Milestone empfiehlt, einen anderen Speicherort für Ihre Videoaufnahmen zu wählen als den Ort der Programminstallation oder das System-Laufwerk. Der Standard-Speicherort ist das Laufwerk mit der höchsten freien Speicherkapazität.
    4. Geben Sie in dem Feld **Speicherdauer für Video-Aufnahmen** an, wie lange die Videoaufnahmen gespeichert werden sollen. Sie können von 1 bis 999 Tage eingeben, wobei die Standard-Retentionszeit 7 Tage beträgt.
    5. Klicken Sie auf **Weiter**.

7. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

   - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

     Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

     > Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

   - Zwischen den Aufzeichnungsservern und den Clients

     Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

   - Zwischen dem Mobile Server und den Clients

     Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

   Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

   Weitere Informationen zur Vorbereitung Ihres System für die sichere Kommunikation finden Sie unter Sichere Kommunikation (Erläuterung). auf Seite 69 sowie im Milestone Leitfaden zu Zertifikaten.

   Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.

8. Tun Sie im Fenster **Auswahl des Dateispeicherorts und der Produktsprache** folgendes:

   1. Wählen Sie im Feld **Dateispeicherort** den Speicherort, an dem Sie die Software installieren wollen.

      > Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

   2. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll.
   3. Klicken Sie auf **Installieren**.

   Die Software wird nun installiert. Microsoft® SQL Server® Express und Microsoft IIS werden während der Installation automatisch installiert, falls dies auf dem betreffenden Computer noch nicht erfolgt ist.

9. Sie werden ggf. aufgefordert, Ihren Computer neu zu starten. Nach dem Neustart erscheinen je nach Ihren Sicherheitseinstellungen möglicherweise eine oder mehrere Windows-Sicherheitswarnungen. Akzeptieren Sie diese, um die Installation abzuschließen.
10. Wenn die Installation abgeschlossen ist, wird eine Liste der auf dem Rechner installierten Komponenten angezeigt.

    Klicken Sie auf **Fortfahren**, um Hardware und Benutzer zum System hinzuzufügen.

    > Wenn Sie jetzt auf **Schließen** klicken, umgehen Sie den Konfigurationsassistenten, und XProtect Management Client wird geöffnet. Sie können das System konfigurieren, z.B. um in Management Client Hardware und Benutzer hinzuzufügen.

11. Geben Sie auf der Seite **Benutzernamen und Passwörter für Hardware eingeben** die Benutzernamen und Passwörter für die Hardware ein, in die Sie die vom Hersteller vorgegebenen geändert haben.

    Das Installationsprogramm sucht im Netzwerk nach dieser Hardware sowie nach Hardware mit Standardanmeldeinformationen des Herstellers.

    Klicken Sie auf **Weiter** und warten Sie ab, während das System nach der Hardware sucht.
12. Wählen Sie auf der Seite **Auswahl der zum System hinzuzufügenden Hardware** die Hardware aus, die Sie zum System hinzufügen wollen. Klicken Sie auf **Weiter** und warten Sie ab, während das System die Hardware hinzufügt.
13. Auf der Seite **Konfiguration der Geräte** können Sie die Hardware beschreibende Namen eingeben, indem Sie auf das Bearbeitungssymbol neben dem Hardwarenamen klicken. Dieser Name wird dann den Hardwaregeräten vorangestellt.

    Erweitern Sie den Hardware-Knoten, um Hardwaregeräte wie Kameras, Lautsprecher und Mikrofone zu aktivieren oder zu deaktivieren.

    > Kameras werden standardmäßig aktiviert, und Lautsprecher und Mikrofone werden standardmäßig deaktiviert.

    Klicken Sie auf **Weiter** und warten Sie ab, während das System die Hardware konfiguriert.
14. Auf der Seite **Benutzer hinzufügen** können Sie zum System Benutzer als Windows-Benutzer oder als Basisbenutzer hinzufügen. Diese Benutzer können entweder die Rolle des Administrators oder die eines Benutzers spielen.

    Definieren Sie den Benutzer und klicken Sie auf **Hinzufügen**.

    Wenn Sie das Hinzufügen von Benutzern beenden, klicken Sie auf **Fortfahren**.

15. Wenn die Installation und Erstkonfiguration beendet sind, erscheint die Seite **Konfiguration ist beendet**, auf der Folgendes angezeigt wird:
    - Eine Liste der zum System hinzugefügten Hardwaregeräte
    - Eine Liste von zum System hinzugefügten Benutzern
    - Die Adressen zum XProtect Web Client und XProtect Mobile-Client, die Sie an Ihre Benutzer weitergeben können

    Wenn Sie auf **Schließen** klicken, wird XProtect Smart Client geöffnet und steht zur Benutzung bereit.

Systeminstallation - Benutzerdefiniert

Mit der Option **Benutzerdefiniert** wird der Managementserver installiert. Sie können jedoch auswählen, welche sonstigen Server- und Client-Komponenten Sie auf dem aktuellen Computer installieren wollen. Standardmäßig ist der Aufzeichnungsserver auf der Liste der Komponenten nicht ausgewählt. Abhängig von Ihrer Auswahl können Sie die nicht ausgewählten Komponenten anschließend auf anderen Computern installieren. Weitere Informationen zu jeder der Systemkomponenten und deren jeweilige Rollen, siehe Haupt-Systemkomponenten auf Seite 22. Die Installation auf anderen Computern erfolgt über die Downloadseite des Managementservers, mit dem Namen Download Manager. Weitere Informationen zur Installation über den Download Manager, siehe Installation neuer XProtect-Komponenten auf Seite 93.

Milestone empfiehlt Ihnen, vor der Installation den folgenden Abschnitt sorgfältig durchzulesen: Vor dem Start der Installation auf Seite 59.

Für FIPS-Installationen können Sie kein Upgrade von XProtect VMS durchführen, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist. Deaktivieren Sie vor der Installation die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem der SQL-Server gehosted wird. Wenn Sie allerdings ein Upgrade von XProtect VMS Version 2020 R3 oder später vornehmen, brauchen Sie FIPS nicht zu deaktivieren. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

1. Sie können die Software kostenlos aus dem Internet herunterladen (https://www.milestonesys.com/downloads/) und die Datei `Milestone XProtect VMS-Produkte 2020 R3 System Installer.exe` ausführen.
2. Die Installationsdateien werden entpackt. Abhängig von Ihren Sicherheitsseinstellungen erscheinen eine oder mehrere Windows® Sicherheitswarnungen. Akzeptieren Sie diese, um mit dem Entpacken fortzufahren.
3. Nach Abschluss dieses Vorganges erscheint der **Milestone XProtect VMS** Installationsassistent.

1. Wählen Sie die während der Installation zu verwendende **Sprache** aus (dies ist nicht die Sprache, die Ihr System nach erfolgter Installation verwendet; diese Einstellung erfolgt später). Klicken Sie auf **Weiter**.
2. Lesen Sie den *Milestone Endbenutzer-Lizenzvertrag*. Wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen dieser Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
3. Geben Sie im Feld **Geben Sie den Speicherort der Lizenzdatei ein bzw. navigieren Sie dort hin** die Lizenzdatei an, die Sie von Ihrem XProtect-Anbieter erhalten haben. Alternativ können Sie auch zum Dateispeicherort navigieren , oder Sie klicken auf das Link **XProtect Essential+** um eine kostenlose Lizenzdatei herunterzuladen. Zu den Einschränkungen des kostenlosen XProtect Essential+ Produktes siehe die Produktvergleichstabelle auf Seite 46. Das System überprüft Ihre Lizenzdatei, bevor Sie fortfahren können. Klicken Sie auf **Weiter**.

4. Wählen Sie **Benutzerdefiniert**. Eine Liste der zu installierenden Komponenten wird angezeigt. Mit Ausnahme des Management-Servers sind alle Komponenten in der Liste optional. Standardmäßig ist der Aufzeichnungsserver nicht ausgewählt. Klicken Sie auf **Weiter**.

   In den unten aufgeführten Schritten werden alle Systemkomponenten installiert. Installieren Sie für ein stärker verteiltes System weniger Systemkomponenten auf diesem Computer, und die übrigen Komponenten auf anderen Computern. Wenn Sie einen Installationsschritt nicht wiedererkennen, so liegt dies wahrscheinlich daran, dass Sie die Installation der Systemkomponente, zu der diese Seite gehört, nicht ausgewählt haben. Fahren Sie in diesem Fall mit dem nächsten Schritt fort. Siehe auch Installation neuer XProtect-Komponenten auf Seite 93, Installation neuer XProtect-Komponenten auf Seite 93, und Installation neuer XProtect-Komponenten auf Seite 93.

5. Nur wenn auf dem Computer mehr als eine IIS-Website zur Verfügung steht, wird die Seite **Wählen Sie eine Website auf dem IIS aus, die Sie mit Ihrem XProtect System verwenden möchten** angezeigt. Sie müssen auswählen, welche Website Sie mit Ihrem XProtect System verwenden wollen. Wählen Sie wenn möglich eine Website mit HTTPS-Bindung aus, da dieses Protokoll eine erweiterte und sicherere Version von HTTP ist. Klicken Sie auf **Weiter**.

   Falls Microsoft® IIS auf dem Computer noch nicht installiert ist, wird es installiert.

6. Wählen Sie auf der Seite **Auswählen Microsoft SQL Server** die SQL Server aus, die Sie verwenden möchten. Siehe auch SQL Server Optionen während der benutzerdefinierten Installation auf Seite 93. Klicken Sie auf **Weiter**.

> Wenn Sie auf Ihrem lokalen Computer keine SQL Server haben, können Sie Microsoft SQL Server Express installieren; auf einem größeren, verteilten Systemen würden Sie in Ihrem Netzwerk jedoch typischerweise einen eigenen SQL Server verwenden.

7. Wählen oder erstellen Sie auf der Seite **Datenbank auswählen** (die nur angezeigt wird, wenn Sie einen vorhandenen SQL Server ausgewählt haben), eine SQL-Datenbank zum Speichern Ihrer Systemkonfiguration. Wenn Sie sich für eine vorhandene SQL-Datenbank entscheiden, entscheiden Sie, ob vorhandene Daten **Beibehalten** oder **Überschrieben** werden sollen. Falls Sie ein Upgrade durchführen, wählen Sie die Option die vorhandenen Daten beizubehalten, damit Sie Ihre Systemkonfiguration nicht verlieren. Siehe auch SQL Server Optionen während der benutzerdefinierten Installation auf Seite 93. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite **Passwort für Systemkonfiguration zuweisen** ein Passwort ein, das Ihre Systemkonfiguration schützt. Dieses Passwort benötigen Sie, falls eine Systemwiederherstellung erforderlich wird oder wenn Sie Ihr System erweitern, z.B. indem Sie Cluster hinzufügen.

   > Es ist wichtig, dass Sie dieses Passwort sicher aufbewahren. Wenn Sie dieses Passwort verlieren, sind Sie ggf. nicht mehr in der Lage, Ihre Systemkonfiguration wiederherzustellen.

   Wenn Sie Ihre Systemkonfiguration nicht mit einem Passwort schützen wollen, wählen Sie **Ich möchte kein Passwort zum Schutz der Systemkonfiguration verwenden, und mir ist klar, dass die Systemkonfiguration dann nicht verschlüsselt ist**.

   Klicken Sie auf **Weiter**.
9. Wählen Sie auf der Seite **Dienstkonto auswählen** entweder **Dieses vorgegebene Konto** aus, oder **Dieses Konto**, um das Dienstkonto für alle Systemkomponenten außer des Aufzeichnungsservers auszuwählen. Geben Sie ggf. ein Passwort ein. Klicken Sie auf **Weiter**.
10. Wählen Sie auf **Auswahl des Dienstkontos für den Aufzeichnungsserver** entweder **Dieses vorgegebene Konto** aus, oder **Dieses Konto**, um das Dienstkonto für den Aufzeichnungsserver auszuwählen.

    Geben Sie ggf. ein Passwort ein.

    > Der Benutzername für das Konto muss aus einem einzigen Wort bestehen. Es darf keine Leerzeichen enthalten.

    Klicken Sie auf **Weiter**.

11. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an:
    1. Geben Sie den Namen des Aufzeichnungsservers im Feld **Aufzeichnungsserver-Name** ein. Der Standardwert ist der Name des Computers.
    2. Das Feld für die **Management-Server-Adresse** zeigt die Adresse und Port-Nummer des Management-Servers: localhost:80.
    3. Wählen Sie im Feld **Wahl des Speicherorts für die Medien-Datenbank** den Speicherort aus, an dem Sie Ihre Video-Aufzeichnungen speichern möchten. Milestone empfiehlt, einen anderen Speicherort für Ihre Videoaufnahmen zu wählen als den Ort der Programminstallation oder das System-Laufwerk. Der Standard-Speicherort ist das Laufwerk mit der höchsten freien Speicherkapazität.
    4. Geben Sie in dem Feld **Speicherdauer für Video-Aufnahmen** an, wie lange die Videoaufnahmen gespeichert werden sollen. Sie können von 1 bis 999 Tage eingeben, wobei die Standard-Retentionszeit 7 Tage beträgt.
    5. Klicken Sie auf **Weiter**.

12. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

    - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

      Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

      > Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

    - Zwischen den Aufzeichnungsservern und den Clients

      Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

    - Zwischen dem Mobile Server und den Clients

      Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

    Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

    Weitere Informationen zur Vorbereitung Ihres System für die sichere Kommunikation finden Sie unter Sichere Kommunikation (Erläuterung). auf Seite 69 sowie im Milestone Leitfaden zu Zertifikaten.

    Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.

13. Wählen Sie auf der Seite **Dateispeicherort und Produktsprache auswählen** den **Speicherort** für die Programmdateien aus.

    > Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

14. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll. Klicken Sie auf **Installieren**.

    Die Software wird nun installiert. Nach Abschluss der Installation wird Ihnen eine Liste mit den erfolgreich installierten Systemkomponenten angezeigt. Klicken Sie auf **Schließen**.

15. Sie werden ggf. aufgefordert, Ihren Computer neu zu starten. Nach dem Neustart erscheinen je nach Ihren Sicherheitseinstellungen möglicherweise eine oder mehrere Windows-Sicherheitswarnungen. Akzeptieren Sie diese, um die Installation abzuschließen.
16. Konfigurieren Sie Ihr System in Management Client. Siehe Aufgabenliste für die Erstkonfiguration auf Seite 136.
17. Installieren Sie, je nach Ihrer Auswahl, die sonstigen Systemkomponenten auf den übrigen Computern durch den Download Manager. Siehe Installation neuer XProtect-Komponenten auf Seite 93.

SQL Server Optionen während der benutzerdefinierten Installation

Entscheiden Sie sich, welche SQL Server und Datenbank in Verbindung mit den u.a. Optionen verwendet werden soll.

SQL Server Optionen:

- **Installieren Sie Microsoft® SQL Server® Express auf diesem Computer**: Diese Option wird nur angezeigt, wenn SQL Server auf diesem Computer nicht installiert ist
- **Verwenden Sie SQL Server auf diesem Computer**: Diese Option wird nur angezeigt, wenn SQL Server bereits auf dem Computer installiert ist
- **Wählen Sie einen SQL Server in Ihrem Netzwerk aus, indem Sie folgende Suche ausführen**: Hiermit können Sie nach allen SQL Server suchen, die im Subnet Ihres Netzwerks sichtbar sind
- **Wählen Sie einen SQL Server in Ihrem Netzwerk aus**: Hiermit können Sie die Adresse (den Hostnamen oder die IP-Adresse) eines SQL Server eingeben, den Sie mithilfe einer Suche ggf. nicht finden können

SQL-Datenbankoptionen:

- **Neue Datenbank erstellen**: Vor allem für Neuinstallationen
- **Vorhandene Datenbank verwenden**: Vor allem für Upgrades bestehender Installationen. Milestone empfiehlt Ihnen, die vorhandene SQL-Datenbank beizubehalten und die darin enthaltenen Daten dort zu belassen, damit Sie Ihre Systemkonfiguration nicht verlieren. Sie können auch auswählen, ob Sie die Daten in der SQL-Datenbank überschreiben wollen

Installation neuer XProtect-Komponenten

Installation über Download Manager (Erläuterung)

Falls Sie Systemkomponenten auf anderen Computern installieren wollen als auf dem, auf dem der Managementserver installiert ist, müssen Sie diese Systemkomponenten über die Downloadseite des Managementserver installieren Download Manager.

1. Gehen Sie von dem Computer, auf dem Managementserver installiert ist, zur Downloadseite des Managementserver. Wählen Sie im Windows **Startmenü Programme** > **Milestone** > **Administrative Installationsseite** und schreiben Sie sich die Internetadresse zum späteren Gebrauch bei der Installation der Systemkomponenten auf anderen Computern auf oder kopieren Sie sie. Die Adresse hat

typischerweise die Form *http://[management server address]/installation/Admin/default-en-US.htm*.

2. Melden Sie sich bei jedem der übrigen Computer an, um eine oder mehrere der sonstigen Systemkomponenten zu installieren:
   - Aufzeichnungsserver (siehe auch Installation eines Aufzeichnungsserver über Download Manager auf Seite 94 oder Automatische Installation eines Aufzeichnungsservers auf Seite 100).
   - Management Client
   - Smart Client
   - Ereignisserver

     Wenn Sie die Ereignisserver in einer FIPS-konformen Umgebung installieren, müssen Sie den Windows-FIPS 140-2-Modus vor der Installation deaktivieren.

   - Protokollserver
   - Mobile Server
3. Öffnen Sie einen Internetbrowser, geben Sie die Adresse der Downloadseite des Managementserver in das Adressfeld ein und laden Sie das jeweilige Installationsprogramm herunter.
4. Führen Sie das Installationsprogramm aus.

Siehe Systeminstallation - Benutzerdefiniert auf Seite 88, wenn Sie im Zweifel sind, welche Auswahl und welche Einstellungen bei den verschiedenen Installationsschritten erforderlich sind.

Installation eines Aufzeichnungsserver über Download Manager

Wenn Ihre Systemkomponenten auf separate Computer verteilt sind, können Sie die Aufzeichnungsserver installieren, indem Sie den untenstehenden Anweisungen folgen.

Der Aufzeichnungsserver ist bereits installiert, wenn Sie eine **Einzelcomputer**-Installation vorgenommen haben. Aber Sie können die gleichen Anweisungen befolgen, um weitere Aufzeichnungsserver hinzuzufügen, wenn Sie mehr Kapazität benötigen.

Wenn Sie einen Failover-Server installieren müssen, siehe hierzu Installation neuer XProtect-Komponenten auf Seite 93.

1. Gehen Sie von dem Computer, auf dem Managementserver installiert ist, zur Downloadseite des Managementserver. Wählen Sie im Windows **Startmenü Programme** > **Milestone** > **Administrative Installationsseite** und schreiben Sie sich die Internetadresse zum späteren Gebrauch bei der Installation

der Systemkomponenten auf anderen Computern auf oder kopieren Sie sie. Die Adresse hat typischerweise die Form *http://[management server address]/installation/Admin/default-en-US.htm*.

2. Melden Sie sich an dem Computer an, auf dem der Aufzeichnungsserver installiert werden soll.
3. Öffnen Sie einen Internetbrowser und geben Sie die Adresse der Download-Webseite des Managementserver in das Adressfeld ein und drücken Sie die Eingabetaste.
4. Laden Sie das Installationsprogramm für den Aufzeichnungsserver herunter, indem Sie **Alle Sprachen** unter dem **Installationsprogramm für den Aufzeichnungsserver** auswählen. Speichern Sie das Installationsprogramm, oder führen Sie es direkt von der Webseite aus aus.
5. Wählen Sie die **Sprache**, die Sie für die Installation verwenden wollen. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Wählen Sie einen Installationstyp aus**:

   Typisch, um einen Aufzeichnungsserver mit den Standardwerten zu installieren, oder

   Benutzerdefiniert, um einen Aufzeichnungsserver mit benutzerdefinierten Werten zu installieren.
7. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an:
   1. Geben Sie den Namen des Aufzeichnungsservers im Feld **Aufzeichnungsserver-Name** ein. Der Standardwert ist der Name des Computers.
   2. Das Feld für die **Management-Server-Adresse** zeigt die Adresse und Port-Nummer des Management-Servers: localhost:80.
   3. Wählen Sie im Feld **Wahl des Speicherorts für die Medien-Datenbank** den Speicherort aus, an dem Sie Ihre Video-Aufzeichnungen speichern möchten. Milestone empfiehlt, einen anderen Speicherort für Ihre Videoaufnahmen zu wählen als den Ort der Programminstallation oder das System-Laufwerk. Der Standard-Speicherort ist das Laufwerk mit der höchsten freien Speicherkapazität.
   4. Geben Sie in dem Feld **Speicherdauer für Video-Aufnahmen** an, wie lange die Videoaufnahmen gespeichert werden sollen. Sie können von 1 bis 999 Tage eingeben, wobei die Standard-Retentionszeit 7 Tage beträgt.
   5. Klicken Sie auf **Weiter**.
8. Die Seite **IP-Adressen der Aufzeichnungsserver** wird nur angezeigt, wenn Sie **Benutzerdefiniert** ausgewählt haben. Geben Sie die Anzahl der Aufzeichnungsserver an, die Sie auf diesem Computer installieren wollen. Klicken Sie auf **Weiter**.

9. Wählen Sie auf **Auswahl des Dienstkontos für den Aufzeichnungsserver** entweder **Dieses vorgegebene Konto** aus, oder **Dieses Konto**, um das Dienstkonto für den Aufzeichnungsserver auszuwählen.

   Geben Sie ggf. ein Passwort ein.

   > Der Benutzername für das Konto muss aus einem einzigen Wort bestehen. Es darf keine Leerzeichen enthalten.

   Klicken Sie auf **Weiter**.

10. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:

    - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

      Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

      > Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

    - Zwischen den Aufzeichnungsservern und den Clients

      Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

    - Zwischen dem Mobile Server und den Clients

      Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

    Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

    Weitere Informationen zur Vorbereitung Ihres System für die sichere Kommunikation finden Sie unter Sichere Kommunikation (Erläuterung). auf Seite 69 sowie im Milestone Leitfaden zu Zertifikaten.

    Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.

11. Wählen Sie auf der Seite **Dateispeicherort und Produktsprache auswählen** den **Speicherort** für die Programmdateien aus.

> Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

12. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll. Klicken Sie auf **Installieren**.

    Die Software wird nun installiert. Nach Abschluss der Installation wird Ihnen eine Liste mit den erfolgreich installierten Systemkomponenten angezeigt. Klicken Sie auf **Schließen**.

13. Sobald der Aufzeichnungsserver installiert wurde, können Sie dessen Betriebszustand dem Recording Server Manager-Task-Leistensymbol entnehmen und diesen in Management Client konfigurieren. Für weitere Informationen, siehe Aufgabenliste für die Erstkonfiguration auf Seite 136.

Installation eines Failover-Aufzeichnungsservers Download Manager

> Wenn Sie Arbeitsgruppen ausführen, müssen Sie die alternative Installationsmethode für Failover-Aufzeichnungsserver verwenden, (siehe Installation für Arbeitsgruppen auf Seite 103).

1. Gehen Sie von dem Computer, auf dem Managementserver installiert ist, zur Downloadseite des Managementserver. Wählen Sie im Windows **Startmenü Programme** > **Milestone** > **Administrative Installationsseite** und schreiben Sie sich die Internetadresse zum späteren Gebrauch bei der Installation der Systemkomponenten auf anderen Computern auf oder kopieren Sie sie. Die Adresse hat typischerweise die Form *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Melden Sie sich an dem Computer an, auf dem der Failover-Aufzeichnungsserver installiert werden soll.
3. Öffnen Sie einen Internetbrowser, geben Sie die Adresse der Download-Webseite des Managementserver in das Adressfeld ein und laden Sie das Installationsprogramm für den Aufzeichnungsserver herunter. Speichern Sie das Installationsprogramm, oder führen Sie es direkt von der Webseite aus aus.
4. Laden Sie das Installationsprogramm für den Aufzeichnungsserver herunter, indem Sie **Alle Sprachen** unter dem **Installationsprogramm für den Aufzeichnungsserver** auswählen. Speichern Sie das Installationsprogramm, oder führen Sie es direkt von der Webseite aus aus.
5. Wählen Sie die **Sprache**, die Sie für die Installation verwenden wollen. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Installationstyp auswählen Failover** aus, um einen Aufzeichnungsserver als Failover-Server zu installieren.

7. Geben Sie auf der Seite **Einstellungen für den Aufzeichnungsserver angeben** die verschiedenen Einstellungen für den Aufzeichnungsserver an. Den Namen des ausfallsicheren Aufzeichnungsservers, die Adresse des Managementservers und den Pfad zur Mediendatenbank. Klicken Sie auf **Weiter**.
8. Auf der Seite **Dienstkonto für den Aufzeichnungsserver auswählen** müssen Sie beim Installieren eines ausfallsicheren Aufzeichnungsservers dasjenige Benutzerkonto verwenden, das den Namen **Dieses Konto** trägt. Hiermit wird das Failover-Benutzerkonto erstellt. Geben Sie ggf. ein Passwort ein und bestätigen Sie es. Klicken Sie auf **Weiter**.
9. Auf der Seite **Verschlüsselung auswählen** können Sie die Kommunikationsflüsse sichern:
   - Zwischen den Aufzeichnungsservern, Datensammlern und dem Management Server

     Um die Verschlüsselung für interne Kommunikationsflüsse zu aktivieren, wählen Sie im Abschnitt **Serverzertifikat** ein Zertifikat aus.

     > Wenn Sie die Verbindung vom Aufzeichnungsserver zum Management Server verschlüsseln, fordert das System, dass Sie auch die Verbindung vom Management Server zum Aufzeichnungsserver verschlüsseln.

   - Zwischen den Aufzeichnungsservern und den Clients

     Um die Verschlüsselung zwischen Aufzeichnungsservern und Client-Komponenten zu aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, wählen Sie im Abschnitt **Streamingmedienzertifikat** ein Zertifikat aus.

   - Zwischen dem Mobile Server und den Clients

     Um die Verschlüsselung zwischen Client-Komponenten zu aktivieren, die Datenstreams vom Mobile Server abrufen, wählen Sie im Abschnitt **Mobil-Streamingmedienzertifikat** ein Zertifikat aus.

   Sie können für alle Systemkomponenten dieselbe oder verschiedene Zertifikatsdateien verwenden, abhängig von den Systemkomponenten.

   Weitere Informationen zur Vorbereitung Ihres System für die sichere Kommunikation finden Sie unter Sichere Kommunikation (Erläuterung). auf Seite 69 sowie im Milestone Leitfaden zu Zertifikaten.

   Nach der Installation vom Server Configurator im Taskleistensymbol Management Server Manager können Sie außerdem die Verschlüsselung aktivieren.
10. Wählen Sie auf der Seite **Dateispeicherort und Produktsprache auswählen** den **Speicherort** für die Programmdateien aus.

    > Ist auf dem Computer bereits ein Milestone XProtect VMS-Produkt installiert, so ist dieses Feld deaktiviert. Das Feld zeigt den Ort, an dem die Komponente installiert wird.

11. Wählen Sie in dem Feld **Produktsprache** die Sprache aus, in der das XProtect-Produkt installiert werden soll. Klicken Sie auf **Installieren**.

    Die Software wird nun installiert. Nach Abschluss der Installation wird Ihnen eine Liste mit den erfolgreich installierten Systemkomponenten angezeigt. Klicken Sie auf **Schließen**.

12. Sobald der ausfallsichere Aufzeichnungsserver installiert wurde, können Sie dessen Betriebszustand dem Failover Server-Symbol Aufzeichnungsserver-Dienst entnehmen und diesen in Management Client konfigurieren. Für weitere Informationen, siehe Aufgabenliste für die Erstkonfiguration auf Seite 136.

Stille Installation über eine Befehlszeilenoberfläche (Erläuterung)

Mit der stillen Installation können Systemadministratoren den Aufzeichnungsserver und die Smart Client-Software über ein großes Netzwerk ohne Mitwirkung der Anwender und mit möglichst wenig Störung für den Endanwender installieren und aktualisieren.

Die Installationsdateien Smart Client und Aufzeichnungsserver (.exe-Dateien) haben unterschiedliche Befehlszeilenargumente. Sie haben jeweils einen eigenen Satz Befehlszeilenparameter, die in einer Befehlszeilenoberfläche direkt oder über eine Datei mit Argumenten aktiviert werden können. In der Befehlszeilenoberfläche können Sie zusammen mit den Installationsdateien auch Befehlszeilenoptionen verwenden.

Sie können die Installationsdateien für XProtect, ihre Befehlszeilenparameter und ihre Befehlszeilenoptionen mit Tools für die stille Verteilung und Installation mit Software wie Microsoft System Center Configuration Manager (SCCM, auch als ConfigMgr bekannt) kombinieren. Weitere Informationen zu solchen Tools finden Sie auf der Internetseite des Herstellers. Sie können Milestone Software Manager auch für die Ferninstallation und für die Aktualisierung von Aufzeichnungsserver, Device-Packs und Smart Client verwenden. Weitere Informationen finden Sie in der Milestone Software Manager-Dokumentation.

Dateien mit Befehlszeileparametern und -argumenten

Bei der stillen Installationen können Sie Einstellungen angeben, die mit den verschiedenen Komponenten des VMS-Systems verknüpft sind sowie mit deren interner Kommunikation, mit Dateien mit Befehlszeilenparametern und -Argumenten. Dateien mit Befehlszeilenparametern und -Argumenten sollten nur für Neuinstallationen verwendet werden, da Sie die Einstellungen, die die Befehlszeilenparameter darstellen, während eines Upgrades nicht ändern können.

Um die verfügbaren Befehlszeilenparameter anzusehen und Dateien mit Argumenten für ein Installationsprogramm zu erzeugen, navigieren Sie in der Befehlszeilenoberfläche zu dem Verzeichnis, in dem sich das Installationsprogramm befindet, und geben Sie den folgenden Befehl ein:

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

Beispiel:

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

In der gespeicherten Datei mit den Argumenten (Arguments.xml) hat jeder Befehlszeilenparameter eine Beschreibung, die dessen Zweck angibt. Sie können die Datei mit den Argumenten verändern und abspeichern, damit die Werte der Befehlszeilenparameter die Bedürfnisse Ihrer Installation erfüllen.

Wenn Sie eine Datei mit Argumenten gemeinsam mit deren Installationsprogramm verwenden wollen, verwenden Sie die Befehlszeilenoption `--arguments`, indem Sie den folgenden Befehl eingeben:

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

Beispiel:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=C:\temp\arguments.xml
```

Befehlszeilenoptionen

In der Befehlszeilenoberfläche können Sie Installationsdateien auch mit Befehlszeilenoptionen kombinieren. Die Befehlszeilenoptionen verändern allgemein das Verhalten eines Befehls.

Um eine vollständige Liste der Befehlszeilenoptionen angezeigt zu bekommen, navigieren Sie in der Befehlszeilenoberfläche zu dem Verzeichnis, in dem sich das Installationsprogramm befindet, und geben Sie `[NameOfExeFile].exe --help` ein. Damit die Installation erfolgreich ist, müssen Sie für Befehlszeilenoptionen, die einen Wert erfordern, einen solchen angeben.

Sie können sowohl Befehlszeilenparameter als auch Befehlszeilenoptionen im selben Befehl verwenden. Verwenden Sie die Befehlszeilenoption `--parameters` und trennen Sie die einzelnen Befehlszeilenparameter mit einem Doppelpunkt (:). In dem Beispiel weiter unten sind `--quiet`, `--showconsole` und `--parameters` Befehlszeilenoptionen, und `ISFAILOVER` und `RECORDERNAME` sind Befehlszeilenparameter:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

Automatische Installation eines Aufzeichnungsservers

Bei der stillen Installation werden Sie nicht benachrichtigt, wenn die Installation abgeschlossen ist. Um benachrichtigt zu werden, fügen Sie zu dem Befehl die Befehlszeilenoption `--showconsole` hinzu. Das Taskleistensymbol Milestone XProtect Recording Server erscheint, wenn die Installation abgeschlossen ist.

In dem Beispielbefehl weiter unten müssen der Text in den eckigen Klammern ([ ]) und auch die eckigen Klammern selbst durch echte Werte ersetzt werden. Beispiel: anstatt "[path]" könnten Sie eingeben **"d:\program files\"**, **d:\record** oder **\\network-storage-02\surveillance**. Verwenden Sie die Befehlszeilenoption `--help`, um etwas zu den zulässigen Formaten für den Wert jeder Befehlszeileoption zu lesen.

1. Melden Sie sich an dem Computer an, auf dem die Komponente Aufzeichnungsserver installiert werden soll.
2. Managementserver Öffnen Sie einen Internetbrowser und geben Sie die Adresse der Download-Webseite des ein, die das Ziel des Administrators sein soll, und drücken Sie die Eingabetaste.

   Diese Adresse hat typischerweise die Form http://[management server address]/installation/Admin/default-en-US.htm.
3. Laden Sie das Installationsprogramm für den Aufzeichnungsserver herunter, indem Sie **Alle Sprachen** unter dem **Installationsprogramm für den Recording Server** auswählen.
4. Öffnen Sie die von Ihnen gewünschte Befehlszeilenoberfläche. Zum Öffnen von Windows Command Prompt, öffnen Sie das Startmenü von Windows und geben Sie **cmd** ein.
5. Navigieren Sie zu dem Verzeichnis, in dem sich die heruntergeladene Installationsdatei befindet.
6. Setzen Sie die Installation nach einem der beiden weiter unten aufgeführten Szenarien fort:

Szenario 1: Upgrade einer vorhandenen Installation, oder Installation auf einem Server mit der Managementserver-Komponente mit Standardwerten

- Geben Sie den folgenden Befehl ein, dann beginnt die Installation.

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

Szenario 2: Installation in einem verteilten System

1. Geben Sie den folgenden Befehl ein, um eine Datei mit Argumenten mit Befehlszeilenparametern zu erzeugen.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=
[path]
```

2. Öffnen Sie die Datei mit den Argumenten (Arguments.xml) von dem angegebenen Pfad aus und ändern Sie ggf. die Werte der Befehlszeilenparameter.

   Achten Sie darauf, den Befehlszeilenparametern SERVERHOSTNAME und SERVERPORT gültige Werte zuzuordnen. Andernfalls kann die Installation nicht abgeschlossen werden.

4. Speichern Sie die Datei mit den Argumenten.
5. Kehren Sie zur Befehlszeilenoberfläche zurück und geben Sie den u.a. Befehl ein, um die Installation mit den in der Datei mit den Argumenten angegebenen Werte für die

Befehlszeilenparameter vorzunehmen.

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

Stille Installation von XProtect Smart Client

Bei der stillen Installation werden Sie nicht benachrichtigt, wenn die Installation abgeschlossen ist. Um benachrichtigt zu werden, fügen Sie zu dem Befehl die Befehlszeilenoption `--showconsole` hinzu. Auf dem Desktop erscheint ein Link zu XProtect Smart Client, wenn die Installation abgeschlossen ist.

In dem Beispielbefehl weiter unten müssen der Text in den eckigen Klammern ([ ]) und auch die eckigen Klammern selbst durch echte Werte ersetzt werden. Beispiel: anstatt "[path]" könnten Sie eingeben **"d:\program files\"**, **d:\record** oder **\\network-storage-02\surveillance**. Verwenden Sie die Befehlszeilenoption `--help`, um etwas zu den zulässigen Formaten für den Wert jeder Befehlszeileoption zu lesen.

1. Managementserver Öffnen Sie einen Internetbrowser und geben Sie die Adresse der Download-Webseite des in die Adresszeile ein, die das Ziel beim Endbenutzer sein soll, und drücken Sie die Eingabetaste.

   Diese Adresse hat typischerweise die Form http://[management server address]:[port]/installation/default-en-US.htm.

2. Laden Sie das Installationsprogramm XProtect Smart Client herunter, indem Sie **Alle Sprachen** unter dem Installationsprogramm **XProtect Smart Client** auswählen.

3. Öffnen Sie die von Ihnen gewünschte Befehlszeilenoberfläche. Zum Öffnen von Windows Command Prompt, öffnen Sie das Startmenü von Windows und geben Sie **cmd** ein.

4. Navigieren Sie zu dem Verzeichnis, in dem sich die heruntergeladene Installationsdatei befindet.

5. Setzen Sie die Installation nach einem der beiden weiter unten aufgeführten Szenarien fort:

Szenario 1: Upgrade einer vorhandenen Installation, oder Installation mit Standardwerten für die Befehlszeilenparameter

- Geben Sie den folgenden Befehl ein, dann beginnt die Installation.

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

Szenario 2: Installation mit benutzerdefinierten Werten für die Befehlszeilenparameter mithilfe einer xml-Argumentdatei als Eingabe

1. Geben Sie den folgenden Befehl ein, um eine XML-Datei mit Argumenten mit Befehlszeilenparametern zu erzeugen.

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

2. Öffnen Sie die Datei mit den Argumenten (Arguments.xml) von dem angegebenen Pfad aus und ändern Sie ggf. die Werte der Befehlszeilenparameter.
3. Speichern Sie die Datei mit den Argumenten.
4. Kehren Sie zur Befehlszeilenoberfläche zurück und geben Sie den u.a. Befehl ein, um die Installation mit den in der Datei mit den Argumenten angegebenen Werte für die Befehlszeilenparameter vorzunehmen.

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

Installation für Arbeitsgruppen

Wenn Sie kein Domänen-Setup, sondern ein Active Directory-Setup verwenden, führen Sie bei der Installation folgende Schritte aus:

1. Melden Sie sich mit einem allgemeinen Administratorkonto bei Windows an.

   Achten Sie darauf, das gleiche Konto auf allen Computern im System zu verwenden.

2. Starten Sie abhängig von Ihren Anforderungen die Installation des Management- oder des Aufzeichnungsservers und klicken Sie auf **Benutzerdefiniert**.
3. Entsprechend Ihrer Auswahl in Schritt 2 wählen Sie die Option zur Installation des Managementserver- oder des Aufzeichnungsserver-Dienstes aus, wobei Sie ein allgemeines Administratorkonto benutzen können.
4. Beenden Sie die Installation.
5. Wiederholen Sie die Schritte 1-4, um weitere, zu verbindende Systeme zu installieren. Sie müssen alle unter Verwendung eines allgemeinen Administratorkontos installiert werden.

Sie können diesen Ansatz nicht verwenden, wenn Sie eine Aktualisierung von Arbeitsgruppeninstallationen vornehmen. Beachten Sie stattdessen Upgrade in einem Arbeitsgruppen-Setup auf Seite 537.

Installation in einem Cluster

Vor der Installation in einem Cluster, siehe Mehrere Management-Server (Cluster) (Erklärung) auf Seite 57 und Anforderungen für Cluster auf Seite 57.

Die Beschreibungen und Illustrationen unterscheiden sich ggf. von dem, was auf Ihren Bildschirm angezeigt wird.

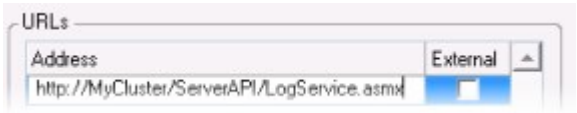
Installation und Ändern der URL-Adresse:

1. Installieren Sie den Managementserver und alle seine Unterkomponenten auf dem ersten Server im Cluster.

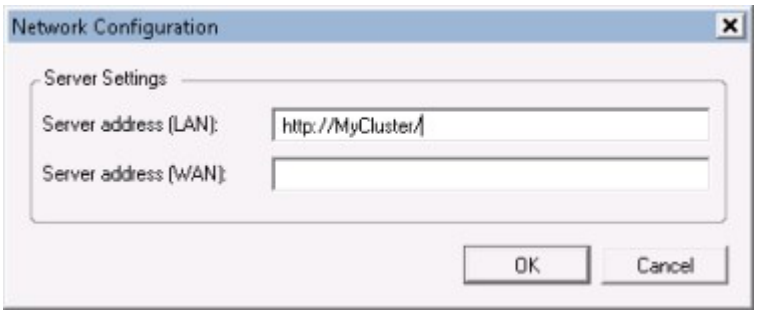
   Der Managementserver muss mit einem bestimmten Benutzer installiert werden und nicht als Netzwerkdienst. Hierfür ist es erforderlich, dass Sie zur Installation die Option **Benutzerdefiniert** verwenden. Der spezifische Benutzer muss außerdem Zugriff zum gemeinsamen Netzlaufwerk haben, und vorzugsweise ein Passwort, das nicht abläuft.

2. Nach der Installation des Managementservers Management Client öffnen Sie auf dem ersten Server im Cluster Management Client und wählen Sie im Menü **Extras Registrierte Dienste** aus.

   1. Wählen Sie in dem Fenster **Registrierte Dienste hinzufügen/entfernen Protokolldienst** von der Liste und klicken Sie auf **Bearbeiten**.
   2. Ändern Sie in dem Fenster **Registrierten Dienst ändern** die URL- Adresse des Protokolldienstes in die URL-Adresse des Clusters.

   3. Wiederholen Sie diese Schritte für alle Dienste, die in dem Fenster **Registrierte Dienste hinzufügen/entfernen** aufgeführt sind. Klicken Sie auf **Netzwerk**.
   4. Ändern Sie in dem Fenster **Netzwerkkonfiguration** die URL- Adresse des Servers in die URL-Adresse des Clusters. (Dieser Schritt gilt nur für den ersten Server im Cluster.) Klicken Sie auf **OK**.

   5. Klicken Sie in dem Fenster **Registrierte Dienste hinzufügen/entfernen** auf **Schließen**. Schließen Sie das Management Client.
   6. Stoppen Sie den Managementserver-Dienst und den IIS. Lesen Sie auf der Internetseite von Microsoft nach, wie der IIS angehalten wird (https://technet.microsoft.com/library/cc732317(WS.10).aspx/).

7. Wiederholen Sie diese Schritte für alle weiteren Server im Cluster, diesmal mit dem Hinweis auf die vorhandene SQL Server und Datenbank. Für den letzten Server im Cluster, auf dem Sie den Management-Server installieren, halten Sie den Dienst Managementserver jedoch nicht an.

Konfigurieren Sie als nächstes den Dienst Managementserver als allgemeinen Dienst im ausfallsicheren Cluster:

1. Gehen Sie auf dem letzten Server, auf dem Sie den Managementserver installiert haben, auf **Start** > **Administrative Hilfsmittel**, öffnen Sie das **Failover Cluster Management** von Windows. Erweitern Sie in dem Fenster **Failover Cluster Management** Ihren Cluster, klicken Sie mit der rechten Maustaste auf **Dienste und Anwendungen** und wählen Sie **Als Dienst oder Anwendung konfigurieren**.

2. Klicken Sie in der Dialogbox **Hohe Verfügbarkeit** auf **Weiter**.
3. Wählen Sie den **Allgemeinen Dienst** aus und klicken Sie dann auf **Weiter**.
4. Machen Sie auf der dritten Seite der Dialogbox keinerlei Angaben und klicken Sie dann auf **Weiter**.
5. Wählen Sie den **Milestone XProtect Management Server**-Dienst aus, und klicken Sie dann auf **Weiter**. Geben Sie den Namen an (Host-Name des Clusters), den die Clients verwenden, wenn sie auf den Dienst zugreifen, und klicken Sie dann auf **Weiter**.
6. Für den Dienst ist kein Speicherplatz erforderlich, klicken Sie auf **Weiter**. Für die Registrierung sollten keine Einstellungen repliziert werden, klicken Sie auf **Weiter**. Überprüfen Sie, ob der Cluster-Dienst Ihren Bedürfnissen entsprechend konfiguriert ist, und klicken Sie dann auf **Weiter**. Der Managementserver ist nun im ausfallsicheren Cluster als allgemeiner Dienst konfiguriert. Klicken Sie auf **Fertigstellen**.
7. In der Einrichtung des Clusters sollten der Ereignisserver und der Data Collector als abhängiger Dienst des Management-Servers eingestellt werden, so dass der Ereignisserver anhält, wenn der Management-Server angehalten wird.
8. Zum Hinzufügen des **Milestone XProtect Event Server**-Dienstes als Ressource zum **Milestone XProtect Management Server Cluster**-Dienst klicken Sie mit der rechten Maustaste auf den Cluster-Dienst und klicken Sie auf **Ressource hinzufügen** > **4 - Allgemeiner Dienst** und wählen Sie **Milestone XProtect Event Server** aus.

Ändern Sie die folgenden Konfigurationsseinstellungen:

An den Managementserver Knoten:

- In C:\ProgramData\Milestone\XProtectManagementserver**ServerConfig.xml**:

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

- In C:\Program Files\Milestone\XProtectManagementserver\IIS\IDP**appsettings.json**:

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

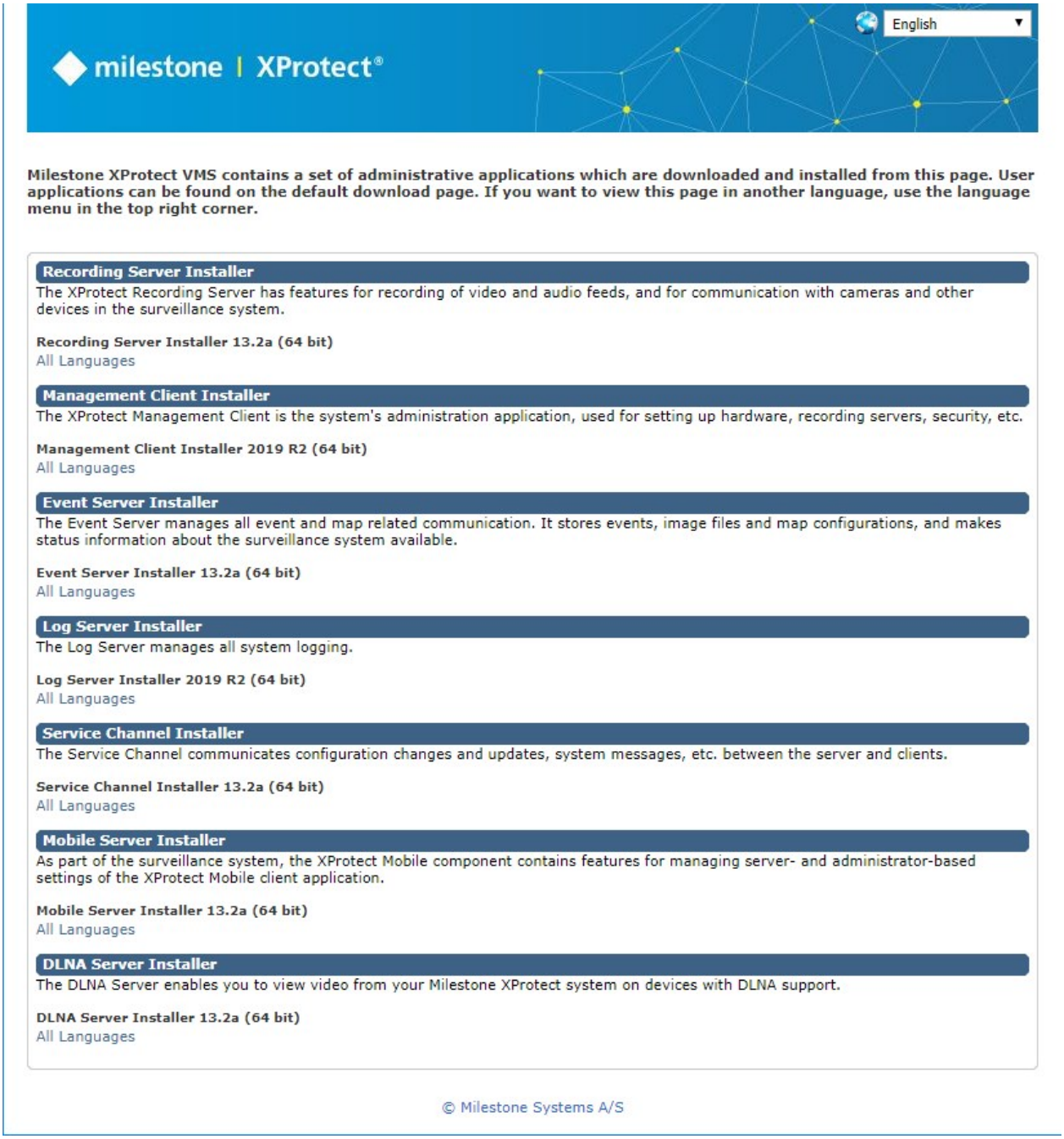
Überprüfen Sie an den Aufzeichnungsservers ob die Adresse des Autorisierungsservers auch auf der Adresse der Clusterrolle steht:

In C:\ProgramData\Milestone\XProtectAufzeichnungsserver**RecorderConfig.xml**:

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

Download Manager/Download-Webseite

Der Management-Server verfügt über eine integrierte Webseite. Über diese Webseite können Administratoren und Endbenutzer die benötigten XProtect-Systemkomponenten von einem beliebigen Speicherort – lokal oder remote – herunterladen und installieren.



Die Webseite kann zwei Gruppen von Inhalt anzeigen und zwar standardmäßig in der Sprache, die der Sprache der Systeminstallation entspricht:

- Eine Webseite richtet sich an **Administratoren**, die so wichtige Systemkomponenten herunterladen und installieren können. In den meisten Fällen wird die Webseite am Ende der Management-Server-Installation automatisch geladen. Sie zeigt den Standardinhalt an. Auf dem Management-Server (Sie können über das Windows **Startmenü** auf die Webseite zugreifen) wählen Sie **Programme** > **Milestone** > **Administrative Installationsseite** aus. Andernfalls können Sie die URL eingeben:

http://[Management-Server-Adresse]:[Port]/installation/admin/

[Management-Server-Adresse] ist die IP-Adresse oder der Hostname des Management-Servers und [Port] ist die Portnummer, auf deren Nutzung das ILS auf dem Management-Server konfiguriert ist.

- Eine Webseite richtet sich an die **Endbenutzer**, um ihnen den Zugriff auf Client-Anwendungen per Standardkonfiguration zu ermöglichen. Auf dem Management-Server (Sie können über das Windows **Startmenü** auf die Webseite zugreifen) wählen Sie **Programme** > **Milestone** > **Öffentliche Installationsseite** aus. Andernfalls können Sie die URL eingeben:

  http://[Management-Server-Adresse]:[Port]/installation/

  [Management-Server-Adresse] ist die IP-Adresse oder der Hostname des Management-Servers und [Port] ist die Portnummer, auf deren Nutzung das ILS auf dem Management-Server konfiguriert ist.

Die zwei Webseiten haben einige standardmäßige Inhalte, also können Sie sie sofort nach der Installation nutzen. Als Administrator können Sie jedoch mit dem Download Manager anpassen, was auf den Webseiten angezeigt werden soll. Sie können auch Komponenten zwischen den beiden Versionen der Webseite verschieben. Zum Verschieben einer Komponente klicken Sie mit der rechten Maustaste darauf. Dann wählen Sie die Webseiten-Version aus, in die Sie die Komponente verschieben wollen.

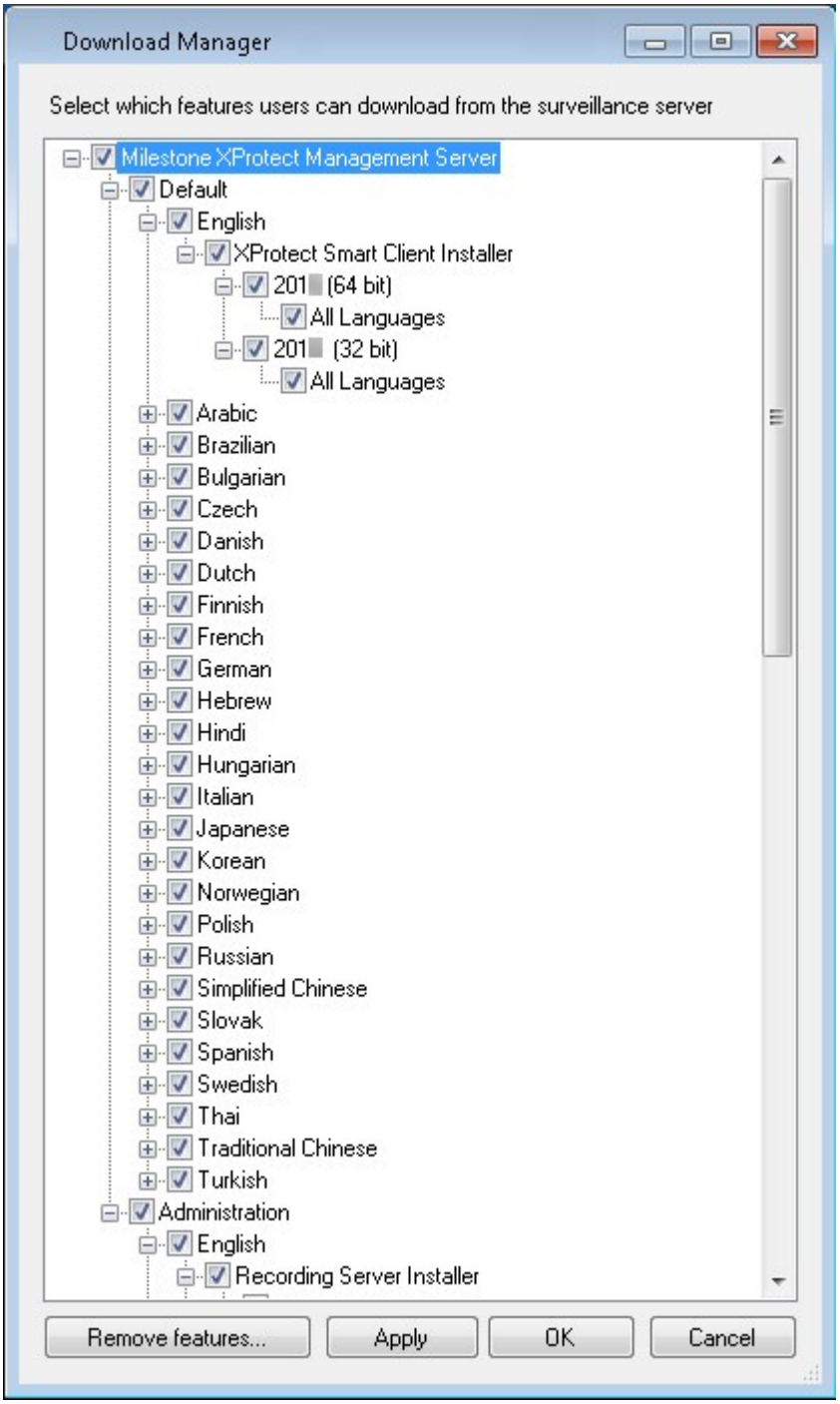
Auch wenn Sie mit dem Download Manager steuern können, welche Komponenten von den Benutzern heruntergeladen und installiert werden können, ist er kein Verwaltungstool für Benutzerrechte. Diese Rechte werden von Rollen definiert, die im Management Client festgelegt werden.

Auf dem Management-Server (Sie können XProtect Download Manager über das Windows **Startmenü** auf die Webseite zugreifen) wählen Sie **Programme** > **Milestone** > **XProtect Download Manager** aus.

Download Manager Standardkonfiguration

Das Download Manager besitzt eine Standardkonfiguration. Dies gewährleistet, dass die Benutzer Ihres Unternehmens von Beginn an auf die Standardkomponenten zugreifen können.

Die Standardkonfiguration besitzt ein Standard-Setup mit der Möglichkeit, zusätzliche oder optionale Komponenten herunterzuladen. Üblicherweise erreichen Sie die Webseite vom Computer des Management-Servers, Sie können jedoch auch von anderen Computern auf sie zugreifen.



- Die erste Ebene: Bezieht sich auf Ihr XProtect Produkt
- Die zweite Ebene: Bezieht sich auf die zwei Versionen der Webseite. **Standard** bezieht sich auf die Webseitenversion, die von den Endbenutzern gesehen wird. **Administration** bezieht sich auf die Webseitenversion, die von den Systemadministratoren gesehen wird
- Die dritte Ebene: Bezieht sich auf die Sprachen, in der die Webseite verfügbar ist

- Die vierte Ebene: Bezieht sich auf die Komponenten, die den Benutzern bereitgestellt sind oder werden können
- Die fünfte Ebene: Bezieht sich auf bestimmte Versionen jeder Komponente, die den Benutzern bereitgestellt sind oder werden können
- Die sechste Ebene: Bezieht sich auf die Sprachversionen der Komponenten, die den Benutzern bereitgestellt sind oder werden können

Die Tatsache, dass anfänglich nur Standardkomponenten verfügbar sind und nur in derselben Sprachversion wie das System an sich, hilft die Installationszeit zu verringern und auf dem Server Platz zu sparen. Es besteht keine Notwendigkeit für eine Komponente oder eine Sprachversion auf dem Server, wenn sie von niemandem verwendet wird.

Falls erforderlich, können Sie weitere Komponenten oder Sprachen hinzufügen und ungewollte Sprachen oder Komponenten verbergen oder entfernen.

Download Manager Standardinstallationsprogramme (Benutzer)

Standardmäßig stehen die folgenden Komponenten für eine separate Installation auf der Download-Webseite des Management-Servers, die sich an Endbenutzer richtet, zur Verfügung (gesteuert vom Download Manager):

- Aufzeichnungsserver, einschließlich Failover-Aufzeichnungsservern. Failover-Aufzeichnungsserver werden zunächst als Aufzeichnungsserver heruntergeladen und installiert. Während der Installation legen Sie dann fest, dass Sie einen Failover-Aufzeichnungsserver benötigen.
- Management Client
- XProtect Smart Client
- Event Server, wird in Verbindung mit der Kartenfunktionalität verwendet
- Log-Server, wird zur Bereitstellung der zum Protokollieren der Systemdaten erforderlichen Funktionalität verwendet
- XProtect Mobile-Server
- Innerhalb Ihrer Organisation sind möglicherweise weitere Optionen verfügbar.

Zur Installation von Treiberpaketen, siehe Installationsprogramm für Treiberpaket - muss heruntergeladen werden auf Seite 112.

Hinzufügen/Veröffentlichen von Komponenten des Download Manager-Installationsprogramms

Sie müssen zwei Verfahrensschritte abschließen, um Nicht-Standard-Komponenten und neue Versionen auf der Download-Seite des Management-Servers verfügbar zu machen.

Als Erstes müssen Sie neue und/oder Nicht-Standard-Komponenten zum Download Manager hinzufügen. Dann nutzen Sie ihn zum Abgleich, welche Komponenten in den jeweiligen Sprachversionen der Webseite verfügbar sein sollen.

Falls der Download Manager geöffnet ist, schließen Sie ihn vor der Installation neuer Komponenten.

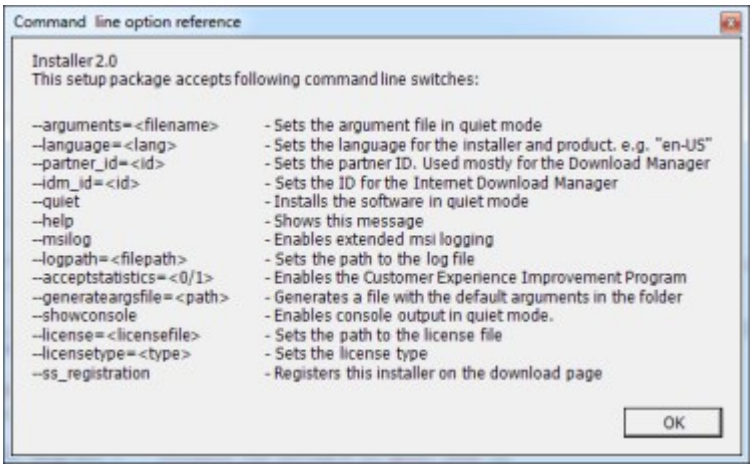
Hinzufügen neuer Dateien bzw. Nicht-Standard-Dateien zum Download Manager:

1. Gehen Sie auf dem Computer, auf den Sie die Komponente(n) heruntergeladen haben, zum Windows-**Startmenü** und öffnen Sie die *Eingabeaufforderung*
2. Geben Sie in der *Eingabeaufforderung* den Namen der Datei (*.exe*) mit dem Zusatz [space]*--ss_registration* ein und führen Sie den Befehl aus

   Beispiel: *MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

   Die Datei wird nun zum Download Manager hinzugefügt, aber nicht auf dem aktuellen Computer installiert.

Wenn Sie eine Übersicht über die Befehle des Installationsprogramms benötigen, geben Sie in der *Eingabeaufforderung* [Leertaste]*--help* ein. Dann wird das folgende Fenster angezeigt:



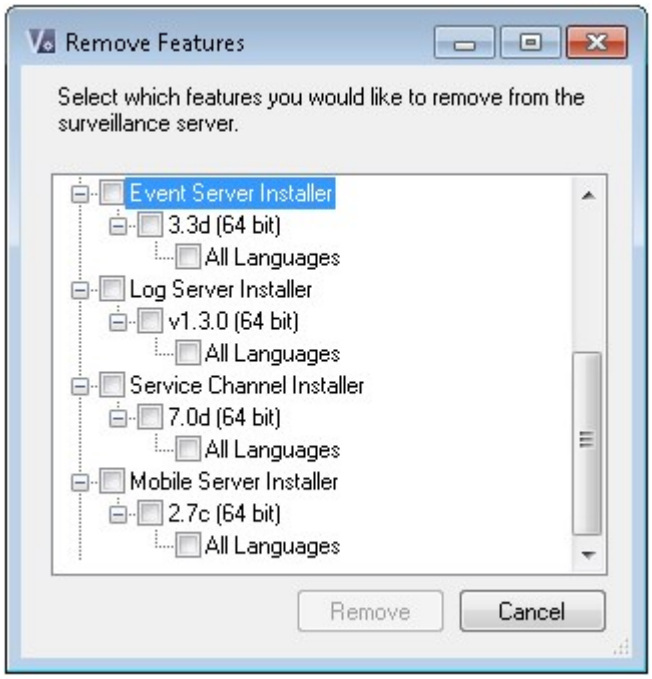
Wenn Sie neue Komponenten installiert haben, werden sie standardmäßig im Download Manager ausgewählt. Sie sind sofort über die Webseite für die Benutzer zugänglich. Sie können die Funktionen auf der Webseite stets ein- oder ausblenden. Dazu markieren Sie die Kontrollkästchen in der Baumstruktur des Download Managers bzw. Sie heben deren Auswahl auf.

Sie können die Abfolge ändern, in der die Komponenten auf der Webseite angezeigt werden. Ziehen Sie die Komponentenelemente in der Baumstruktur des Download Managers einfach per Drag-&-Drop in die gewünschte Position.

Ausblenden/Entfernen der Download Manager Installationsprogrammkomponenten

Sie haben drei Möglichkeiten:

- **Komponenten** auf der Webseite ausblenden. Dazu heben Sie die Auswahl der Kontrollkästchen in der Baumstruktur des Download Managers auf. Die Komponenten auf dem Management-Server installiert und durch die Markierung der Kontrollkästchen in der Baumstruktur des Download Managers können Sie die Komponenten schnell wieder zugänglich machen
- **Verschieben Sie die Installation der Komponenten** auf den Management-Server. Die Komponenten werden vom Download Manager entfernt, aber die Installationsdateien für die Komponenten sind in *C:\Program Files (x86)\Milestone\ XProtect Download Manager* verfügbar, sodass Sie diese bei Bedarf später neu installieren können
  1. Im Download Manager, klicken Sie auf **Funktionen entfernen**.
  2. Wählen Sie im Fenster **Funktionen entfernen** die Funktion(en), die Sie entfernen wollen.



  3. Klicken Sie auf **OK** und dann auf **Ja**.
- **Installationsdateien für nicht benötigte Funktionen** vom Management-Server entfernen. Dadurch können Sie Speicherplatz auf dem Server sparen, wenn Sie wissen, dass Ihre Organisation bestimmte Funktionen nicht verwenden wird

Installationsprogramm für Treiberpaket - muss heruntergeladen werden

Das Treiberpaket (enthält Gerätetreiber), das in Ihrer ursprünglichen Installation beinhaltet ist, ist nicht in Download Manager enthalten. Wenn Sie das Treiberpaket neu installieren müssen oder das Installationsprogramm des Treiberpakets verfügbar machen möchten, müssen Sie zuerst die aktuellste Version zum Download Manager hinzufügen oder veröffentlichen:

1. Sie erhalten das neueste reguläre Treiberpaket auf der Download-Seite auf der Milestone-Website (https://www.milestonesys.com/downloads/).
2. Auf der gleichen Seite können Sie auch das Stammtreiberpaket mit älteren Treibern herunterladen. Um zu prüfen, ob Ihre Kameras Treiber aus dem Legacy-Treiberpaket verwenden, besuchen Sie diese Website (https://www.milestonesys.com/community/business-partner-tools/device-packs/).
3. Download ManagerVeröffentlichen/Fügen Sie es zum hinzu, indem Sie den --ss_registration-Befehl verwenden.

Wenn Sie keine Verbindung zum Netzwerk haben, können Sie den gesamten Aufzeichnungsserver vom Download Manager aus erneut installieren. Die Installationsdateien für den Aufzeichnungsserver sind lokal auf Ihrem Computer gespeichert, wodurch Sie automatisch eine erneute Installation des Treiberpakets vornehmen können.

Installationsprotokolldateien und Fehlersuche

Während einer Installation, eines Upgrades oder einer Deinstallation werden Protokolleinträge in verschiedenen Installationsprotokolldateien vorgenommen: Zur Hauptprotokolldatei für die Installation installer.log und zu den Protokolldateien zu den verschiedenen Systemkomponenten, die Sie installieren. Alle Protokolleinträge haben Zeitstempel, und die neuesten Protokolleinträge befinden sich am Ende der Protokolldateien.

Sie können alle Installationsprotokolldateien in dem Verzeichnis C:\ProgramData\Milestone\Installer\ finden. Protokolldateien mit Bezeichnungen wie *I.log oder *I[integer].log sind Protokolldateien zu neuen Installationen oder Upgrades, deren Protokolldateien mit Bezeichnungen wie *U.log oder *U[integer].log Deinstallationen betreffen. Wenn Sie einen Server mit bereits installiertem XProtect-System von einem Milestone-Partner erworben haben, sind vielleicht keine Installationsprotokolldateien vorhanden.

Die Protokolldateien enthalten Informationen zu den Befehlszeilenparametern und Befehlszeilenoptionen und deren Werten, die während einer Installation, für ein Upgrade oder zur Deinstallation verwendet wurden. Um die Befehlszeilenparameter in den Protokolldateien zu finden, suchen Sie nach **Befehlszeile:** oder **Parameter '**, je nach der Protokolldateien.

Zur Fehlersuche sollten Sie zuerst in der Hauptprotokolldatei der Installation nachschauen. Wenn es während der Installation zu Ausnahmen, Fehlern oder Warnungen bekommen ist, wurden diese protokolliert. Probieren Sie eine Suche nach **Ausnahme**, **Fehler** oder **Warnung**. "Exitcode: 0" bedeutet eine erfolgreiche Installation, und "Exitcode: 1" das Gegenteil. Anhand der Ergebnisse Ihrer Suche in den Protokolldateien können Sie evtl. auf https://supportcommunity.milestonesys.com/s/knowledgebase?language=en_US/ eine Lösung finden. Wenn nicht, wenden Sie sich an Ihren Milestone-Partner, und stellen Sie ihm die entsprechenden Installationsprotokolldateien zur Verfügung.

Konfiguration

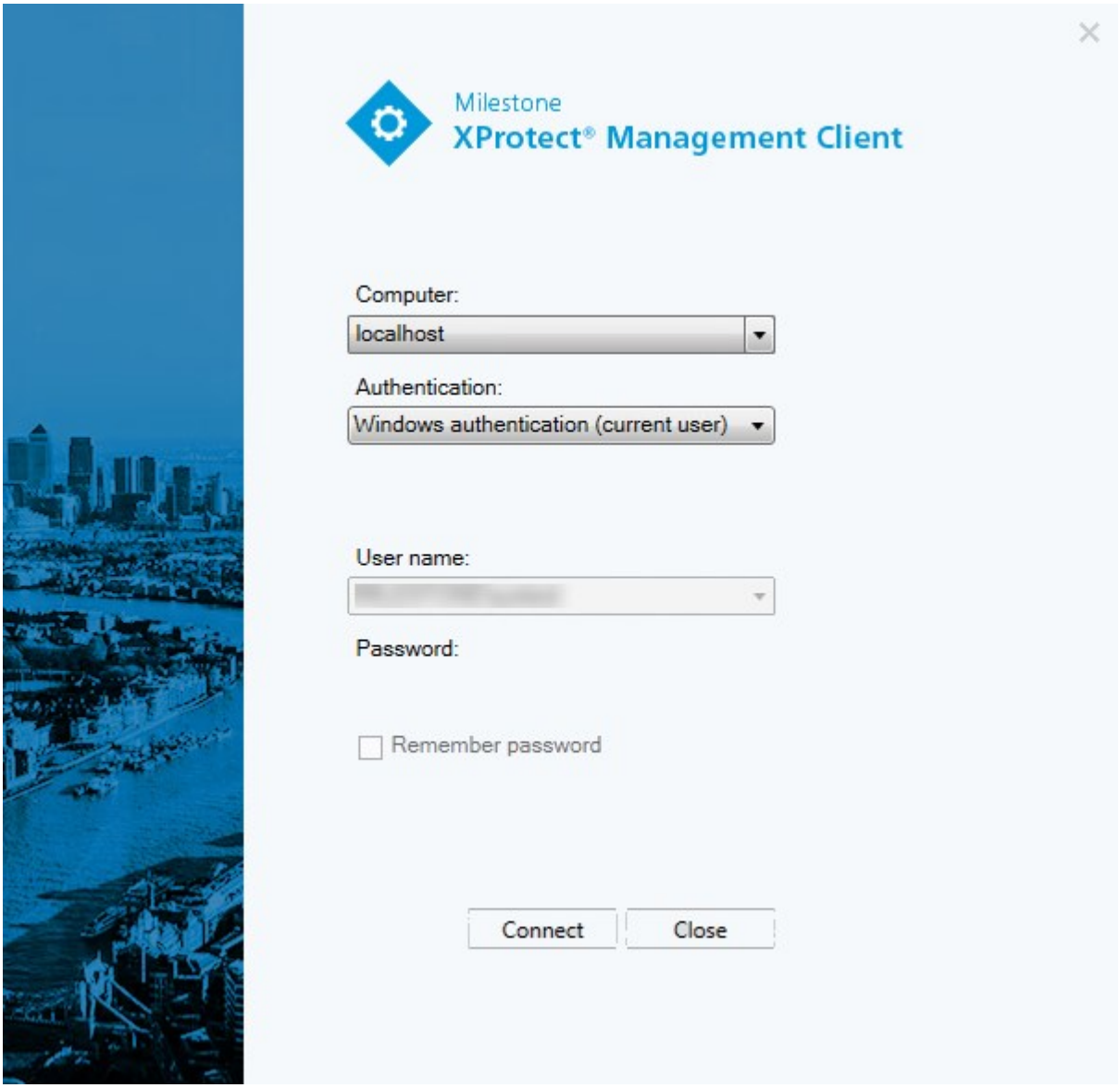
Navigation in Management Client

Dieser Abschnitt gibt eine Einführung in die Management Client Benutzeroberfläche.

Übersicht über das Anmeldeverfahren

Wenn Sie den Management Client starten, müssen Sie zuerst Ihre Anmeldeinformationen eingeben, um eine Verbindung zu einem System herstellen zu können.

Mit installiertem XProtect Corporate 2016 oder XProtect Expert 2016 oder einer neueren Version, können Sie sich nach der Installation eines Patches an Systemen anmelden, auf denen eine ältere Version des Produkts läuft. Die unterstützten Versionen sind XProtect Corporate 2013 und XProtect Expert 2013 oder neuer.



Anmeldungsautorisierung (Erklärung)

Mit dem System können Administratoren Benutzer so konfigurieren, dass diese sich bei einem System nur dann anmelden können, wenn ein zweiter Benutzer mit ausreichenden Berechtigungen die Anmeldung autorisiert. In diesem Fall fragen der XProtect Smart Client oder der Management Client während der Anmeldung nach der zweiten Autorisierung.

Benutzer, die mit der integrierten Rolle **Administratoren** verknüpft sind, verfügen stets über eine Berechtigung zur Autorisierung und werden nicht um eine zweite Anmeldung gebeten, es sei denn, der Benutzer ist mit einer weiteren Rolle verknüpft, die eine zweite Anmeldung voraussetzt.

So verknüpfen Sie eine Anmeldungsautorisierung mit einer Rolle:

- Richten Sie für die ausgewählte Rolle die Option **Anmelde-Autorisierung erforderlich** ein (auf der Registerkarte **Informationen** (siehe Rolleneinstellungen auf Seite 379) unter **Rollen**, damit der Benutzer bei der Anmeldung nach einer zusätzlichen Autorisierung gefragt wird.
- Richten Sie für die ausgewählte Rolle die Option **Benutzer autorisieren** auf der Registerkarte **Gesamtsicherheit** ein (siehe Rolleneinstellungen auf Seite 379) unter **Rollen**, damit der Benutzer Anmeldungen anderer Benutzer genehmigen kann

Für einen Benutzer lassen sich beide Optionen auswählen. Das bedeutet, dass der Benutzer bei der Anmeldung nach einer zusätzlichen Autorisierung gefragt wird, er jedoch auch Anmeldungen anderer Benutzer autorisieren kann (außer seiner eigenen).

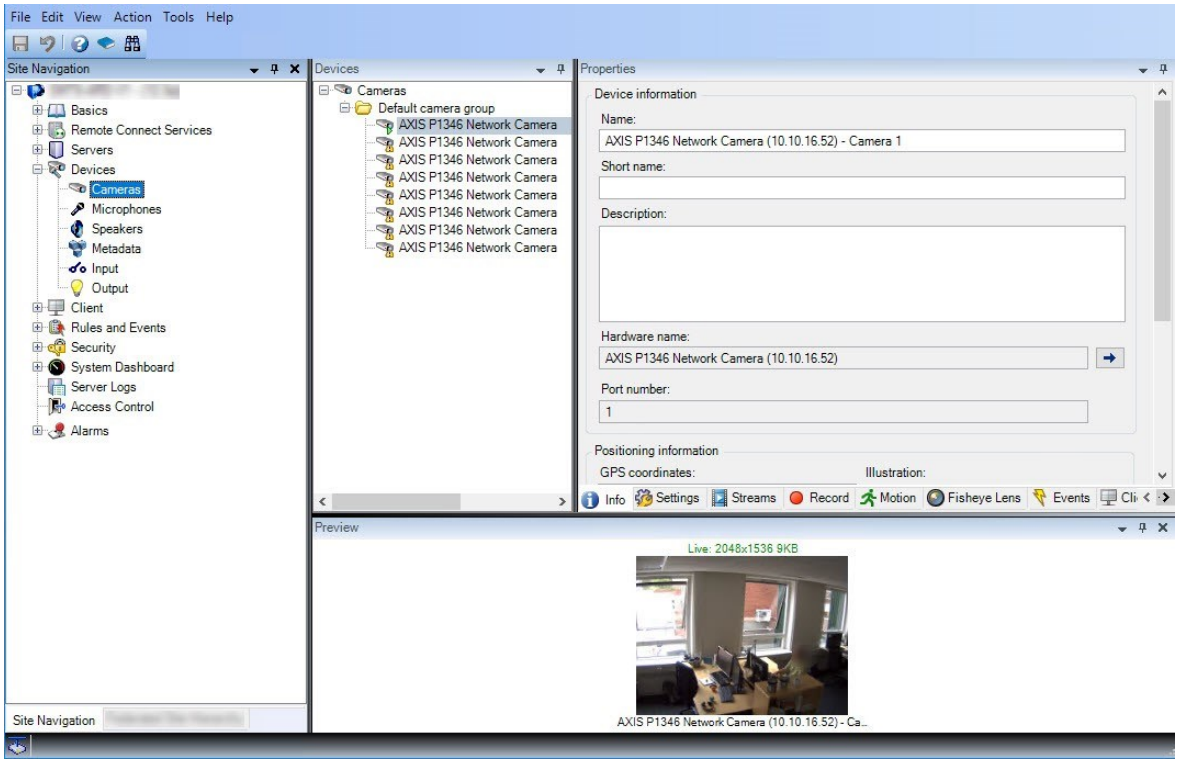
Management Client Fenster-Übersicht

Das Management Client-Fenster ist in Bereiche unterteilt. Die Anzahl der Bereiche und Layouts hängt ab von Ihren:

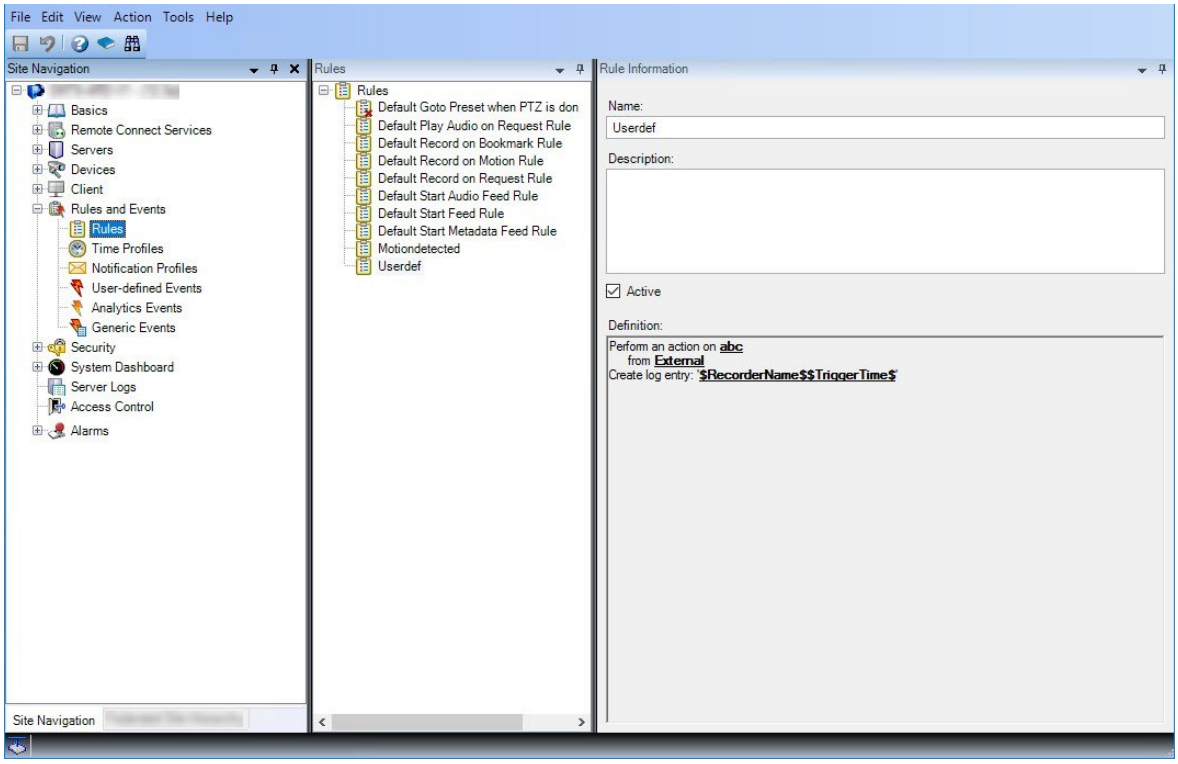
- Systemkonfiguration
- Aufgabe
- Verfügbare Funktionen

Unten finden Sie einige Beispiele typischer Layouts:

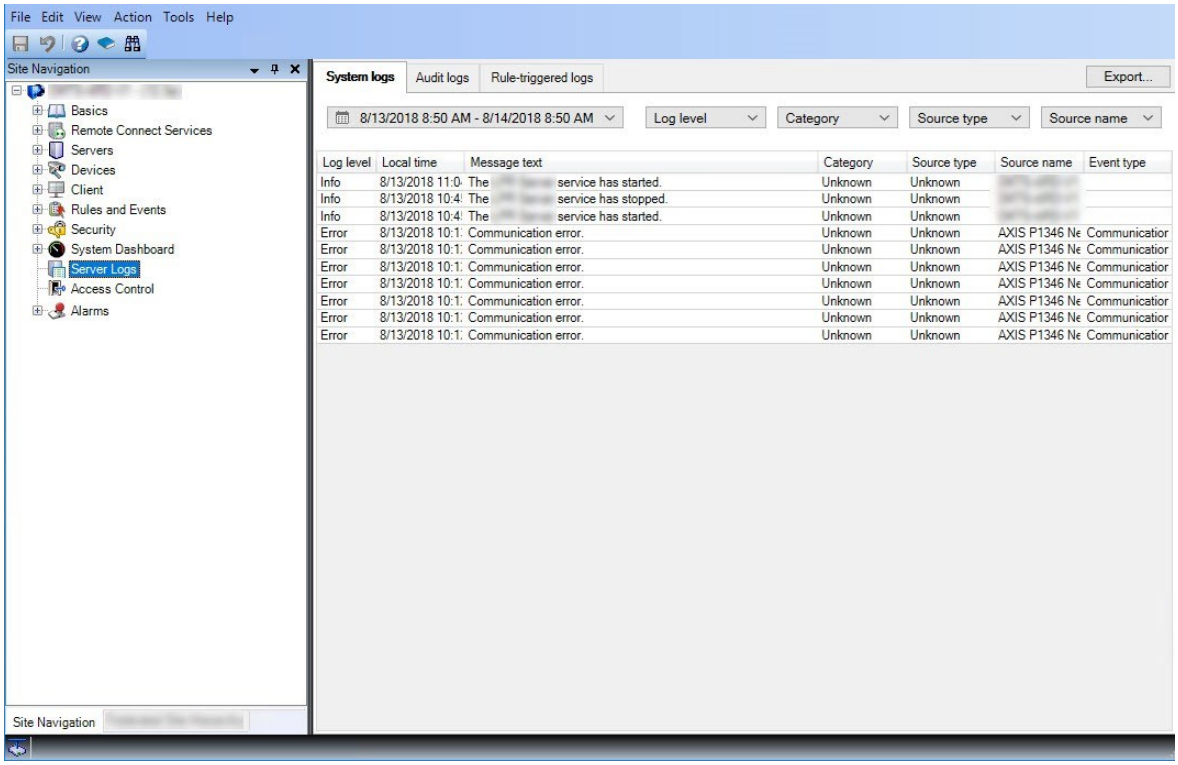
- Wenn Sie mit Aufzeichnungsservern und Geräten arbeiten:



- Wenn Sie mit Regeln, Zeit und Benachrichtigungsprofilen, Benutzern, Rollen arbeiten:

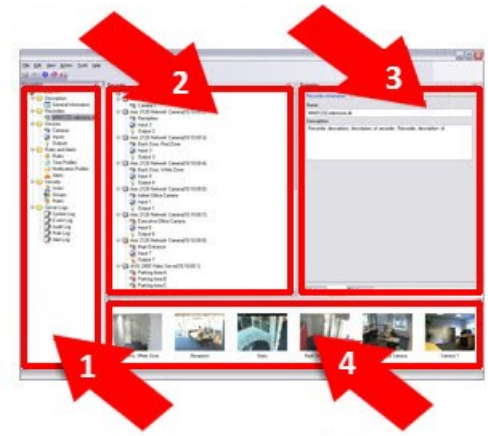


- Wenn Sie sich Protokolle ansehen:



Fensterübersicht

In dieser Darstellung sehen Sie ein typisches Fensterlayout. Da Sie das Layout anpassen können, ist es möglich, dass es auf Ihrem Computer anders aussieht.



1. Fenster „Standort-Navigation“ und „Hierarchie der föderalen Standorte“
2. Übersichtsbereich
3. Eigenschaftenfenster
4. Vorschaufenster

Fenster „Standort-Navigation“: Dies ist Ihr wichtigstes Navigationselement im Management Client. Es spiegelt den Namen sowie die Einstellungen und Konfigurationen des Standorts wider, an dem Sie sich angemeldet haben. Der Standortname wird oben im Fenster angezeigt. Die Funktionen sind in Kategorien angeordnet, welche der Funktionalität der Software entsprechen.

Fenster „Hierarchie der föderalen Standorte“: Dies ist das Navigationselement, in dem alle Milestone Federated Architecture-Standorte in einer Hierarchie mit über- und untergeordneten Standorten angezeigt werden.

Sie können einen beliebigen Standort auswählen und sich dort anmelden. Daraufhin wird der Management Client für den Standort gestartet. Derjenige Standort, bei dem Sie sich angemeldet haben, befindet sich stets oben in der Hierarchie.

Übersichtsbereich: Liefert eine Übersicht über das Element, das Sie im Fenster **Standort-Navigation** ausgewählt haben, zum Beispiel in Form einer detaillierten Liste. Wenn Sie im Fenster **Übersicht** ein Element auswählen, werden dessen Eigenschaften meist im Fenster **Eigenschaften** angezeigt. Wenn Sie im Fenster **Übersicht** mit der rechten Maustaste auf ein Element klicken, erhalten Sie Zugriff auf dessen Verwaltungsfunktionen.

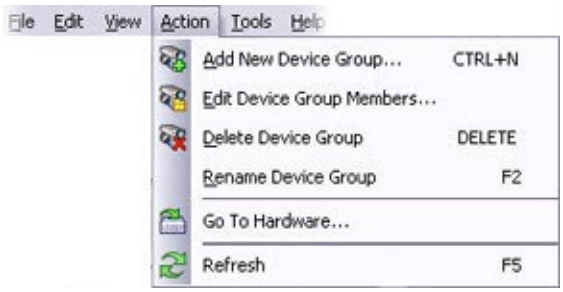
Eigenschaftenfenster: Zeigt die Eigenschaften des Elements an, das im Fenster **Übersicht** ausgewählt wurde. Die Eigenschaften werden auf verschiedenen zugehörigen Registerkarten angezeigt:

Vorschaufenster: Das Fenster **Vorschau** wird angezeigt, wenn Sie mit Aufzeichnungsservern und Geräten arbeiten. Es präsentiert Vorschaubilder der ausgewählten Kameras bzw. Informationen über den Status des aktuellen Geräts. Im Beispiel ist ein Vorschaubild der Kamera dargestellt, inkl. Informationen zur Auflösung und Datenrate des Live-Streams der Kamera:

Standardmäßig beziehen sich die Informationen, die mit den Vorschaubildern einer Kamera angezeigt werden, auf die Live-Streams einer Kamera. Sie werden oberhalb der Vorschau als grüner Text dargestellt. Wenn Sie lieber Informationen zum Aufzeichnungsstream aufrufen möchten (als roter Text dargestellt), wählen Sie im Menü die Optionen **Ansicht** > **Aufzeichnungsstreams** anzeigen.

Wenn im **Vorschaufenster** Vorschaubilder verschiedener Kameras mit einer hohen Bildrate angezeigt werden, kann die Leistung darunter leiden. Falls Sie die Anzahl an Vorschaubildern sowie ihre Bildraten ändern möchten, wählen Sie im Menü **Optionen** > **Allgemein**.

Menü-Übersicht



Nur als Beispiel – einige Menüs ändern sich je nach Kontext.

Menü „Datei“

Sie können Änderungen an der Konfiguration speichern und die Anwendung verlassen. Sie können auch eine Sicherungskopie Ihrer Konfiguration anfertigen. Siehe dazu Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung) auf Seite 494.

Menü bearbeiten

Sie können Änderungen rückgängig machen.

Ansichtsmenü

Name	Beschreibung
Anwendungslayout zurücksetzen	Setzen Sie das Layout der verschiedenen Fenster im Management Client auf ihre Standardeinstellungen zurück.
Vorschaufenster	Aktivieren und deaktivieren Sie das Fenster **Vorschau**, wenn Sie mit Aufzeichnungsservern und Geräten arbeiten.
Aufzeichnungs-Streams anzeigen	Standardmäßig beziehen sich die Informationen, die mit den Vorschaubildern im Fenster **Vorschau** angezeigt werden, auf die Live-Streams der Kameras. Wenn Sie stattdessen lieber Informationen zu Aufzeichnungs-Streams aufrufen möchten, wählen Sie im Menü die Option **Aufzeichnungs-Streams zeigen** aus.
Hierarchie der föderalen Sites	Standardmäßig ist das Fenster **Hierarchie der föderalen Standorte** aktiviert.
Site-Navigation	Standardmäßig ist das Fenster **Standortnavigation** aktiviert.

Aktionsmenü

Der Inhalt des Menüs **Aktion** unterscheidet sich je nach im **Site-Navigationsfenster** ausgewähltem Element. Die Aktionen, die Sie auswählen können, auf die Sie auch per Klick mit der rechten Maustaste auf das Element zugreifen können. Die Elemente werden in Konfigurieren des Systems im Site-Navigationsfenster auf Seite 138 beschrieben.

Dem Voralarm-Puffer für jede Kamera, siehe Geräte, die Voralarm-Puffern unterstützen auf Seite 238

Name	Beschreibung
Aktualisieren	Steht immer zur Verfügung und lädt die angeforderten Informationen aus dem Management-Server neu.

Menü „Extras“

Name	Beschreibung
Registrierte Services	Verwaltung registrierter Dienste. Siehe Verwaltung registrierter Dienste auf Seite 525.
Effektive Rollen	Sehen Sie sich alle Funktionen eines ausgewählten Benutzers oder einer Gruppe an.
Optionen	Öffnet das Dialogfeld Optionen, das Ihnen ermöglicht, globale Systemeinstellungen zu definieren und zu bearbeiten.

Hilfe-Menü

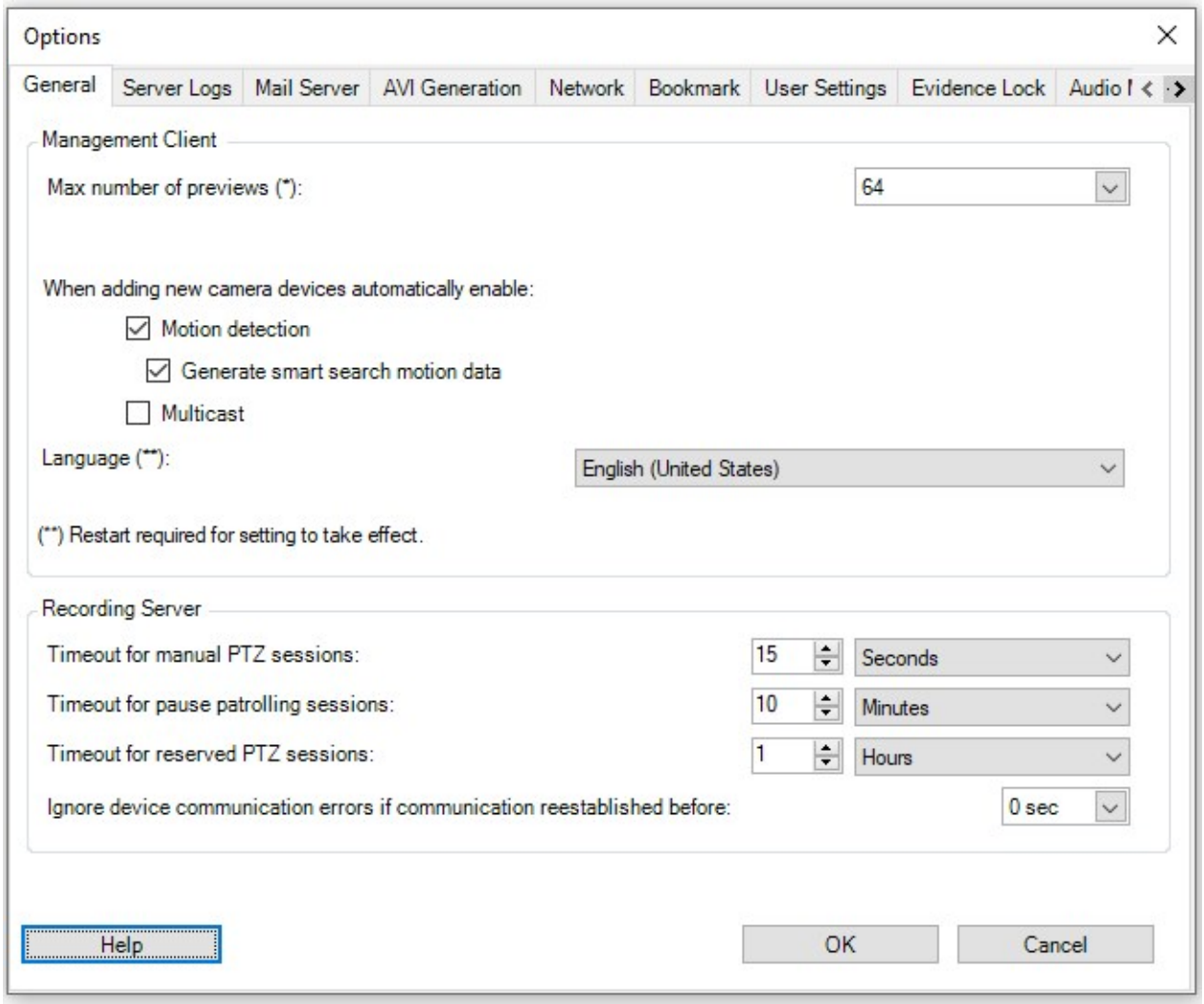
Sie können auf das Hilfesystem und Informationen über die Version von Management Client zugreifen.

Einstellen von Optionen für das System

Im Dialogfeld **Optionen** können Sie eine Reihe von Einstellungen bezüglich der allgemeinen Oberfläche und Funktionalität des Systems vornehmen.

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

Gehen Sie zu **Tools** > **Optionen**, um das Dialogfeld zu öffnen.



Registerkarte „Allgemein“ (Optionen)

Auf der Registerkarte „Allgemein“ können Sie allgemeine Einstellungen für den Management Client und den Aufzeichnungsserver festlegen.

Management Client

Name	Beschreibung
Maximale Anzahl von Vorschauen	Wählen Sie die Höchstzahl der Miniaturbilder, die im Bereich **Vorschau** angezeigt werden. Der Standardwert beträgt

Name	Beschreibung
	64 Miniaturbilder. Wählen Sie aus dem Menü **Aktion** > **Aktualisieren**, damit die Änderungen übernommen werden. Eine hohe Bildrate zusammen mit einer großen Anzahl an Miniaturbildern kann das System verlangsamen.
Beim Hinzufügen neuer Kamerageräte automatisch aktivieren: **Bewegungserkennung**	Aktivieren Sie das Kontrollkästchen, um die Bewegungserkennung auf neuen Kameras zu aktivieren, die Sie dem System mithilfe des Assistenten **Hardware hinzufügen** hinzufügen. Diese Einstellung beeinflusst nicht die Einstellungen für die Bewegungserkennung auf bestehenden Kameras. Sie können die Bewegungserkennung einer Kamera auf der Registerkarte **Bewegung** aktivieren und deaktivieren.
Beim Hinzufügen neuer Kamerageräte automatisch aktivieren: **Bewegungsdaten für Smart Search erzeugen**	Die Erstellung von Bewegungsdaten für Smart Search erfordert, dass die Bewegungserkennung für die Kamera aktiviert ist. Aktivieren Sie das Kontrollkästchen, um die Erstellung von Smart Search-Bewegungsdaten auf neuen Kameras zu aktivieren, die Sie dem System mithilfe des Assistenten **Hardware hinzufügen** hinzufügen. Diese Einstellung beeinflusst nicht die Einstellungen für die Bewegungserkennung auf bestehenden Kameras. Sie können die Erstellung von Smart Search-Bewegungsdaten für eine Kamera auf der Registerkarte **Bewegung** aktivieren und deaktivieren.
Beim Hinzufügen neuer Kamerageräte automatisch aktivieren: **Multicast**	Aktivieren Sie das Kontrollkästchen, um Multicast auf neuen Kameras zu aktivieren, die Sie mithilfe des Assistenten **Hardware hinzufügen** hinzufügen. Diese Einstellung beeinflusst nicht die Multicast-Einstellungen auf bestehenden Kameras. Sie können Live-Multicasting für eine Kamera auf der Registerkarte **Client** aktivieren und deaktivieren.
Sprache	Wählen Sie die Sprache des Management Client. Starten Sie den Management Client neu, um die neue Sprache zu verwenden.

Aufzeichnungsserver

Name	Beschreibung
Zeitüberschreitung für manuelle PTZ-Sitzungen	Client-Benutzer mit den erforderlichen Benutzerrechten können Wachrundgänge von PTZ-Kameras manuell unterbrechen. Wählen Sie aus, wie viel Zeit vergangen sein sollte, bis reguläre Wachrundgänge nach einer manuellen Unterbrechung wieder aufgenommen werden. Diese Einstellung betrifft alle PTZ-Kameras in Ihrem System. Die Standardeinstellung ist 15 Sekunden. Wenn Sie für die Kameras individuelle Zeitüberschreitungen möchten, bestimmten Sie diese auf der Registerkarte **Voreinstellungen** für die Kamera.
Zeitüberschreitung für Sitzungen „Wachrundgang anhalten“	Client-Benutzer mit einer ausreichenden PTZ-Priorität können Wachrundgänge auf PTZ-Kameras anhalten. Wählen Sie aus, wie viel Zeit vergangen sein sollte, bis reguläre Wachrundgänge nach dem Anhalten wieder aufgenommen werden. Diese Einstellung betrifft alle PTZ-Kameras in Ihrem System. Die Standardeinstellung ist 10 Minuten. Wenn Sie für die Kameras individuelle Zeitüberschreitungen möchten, bestimmten Sie diese auf der Registerkarte **Voreinstellungen** für die Kamera.
Zeitüberschreitung für reservierte PTZ-Sitzungen	Legen sie eine Standardzeitüberschreitung für reservierte PTZ-Sitzungen fest. Wenn ein Benutzer eine reservierte PTZ-Sitzung ausführt, kann die PTZ-Kamera nicht von anderen verwendet werden, bis sie entweder manuell freigegeben wurde oder die Zeit überschritten wurde. Die Standardeinstellung ist 1 Stunde. Wenn Sie für die Kameras individuelle Zeitüberschreitungen möchten, bestimmten Sie diese auf der Registerkarte **Voreinstellungen** für die Kamera.
Geräte-Verbindungsfehler ignorieren, wenn die Verbindung wiederhergestellt wird vor	Das System protokolliert alle Kommunikationsfehler auf Hardware und Geräten, hier wählen Sie jedoch aus, wie lange ein Kommunikationsfehler vorliegen muss, bevor der Regel-Engine das Ereignis **Kommunikationsfehler** auslöst.

Registerkarte „Serverprotokolle“ (Optionen)

Auf der Registerkarte **Serverprotokolle** können Sie Einstellungen für die Management-Server-Protokolle des Systems vornehmen.

Weitere Informationen finden Sie unter Protokolle (erklärt) auf Seite 437.

Name	Beschreibung
Protokolle	Wählen Sie einen Protokolltyp zum Konfigurieren aus: • Systemprotokolle • Auditprotokolle • Von Regel ausgelöste Protokolle
Einstellungen	Deaktivieren oder aktivieren Sie die Protokolle und legen Sie die Speicherzeit fest. Erlauben Sie es 2018 R2 und früheren Komponenten, Protokolle aufzuzeichnen. Für weitere Informationen siehe 2018 R2 und früheren Komponenten erlauben, Protokolle aufzuzeichnen auf Seite 439. Für **Systemprotokolle** können Sie die Nachrichtenstufen festlegen, die Sie protokollieren möchten: • Alle (schließt undefinierte Nachrichten mit ein) • Informationen, Warnungen und Fehler • Warnungen und Fehler • Fehler (Standardeinstellung) „Protokollierung der Benutzerzugriffe“ aktivieren für **Auditprotokolle**, wenn das System alle Benutzeraktionen im XProtect Smart Client protokollieren soll. Das sind z. B. Exporte, Aktivierung von Ausgängen und Ansehen von Live-Aufnahmen über Kameras oder die Wiedergabe einer Aufzeichnung. Festlegen: • Die Länge einer WiedergabeSequenz Das bedeutet, dass das System nur einen Protokolleintrag erstellt, solange die Wiedergabe durch den Benutzer innerhalb dieses Zeitraums bleibt. Wenn die Wiedergabe diesen Zeitraum überschreitet, erstellt das System einen neuen Protokolleintrag. • Die Anzahl von Aufzeichnungen (Bildern), die ein Benutzer angesehen hat, bis das System einen Protokolleintrag erstellt

Registerkarte „Mailserver“ (Optionen)

Auf der Registerkarte **Mailserver** können Sie die Einstellungen für den Mailserver Ihres Systems festlegen. Weitere Informationen finde Sie unter Benachrichtigungsprofile auf Seite 354.

Name	Beschreibung
E-Mail-Absenderadresse	Geben Sie die E-Mailadresse ein, die als Absender der E-Mailbenachrichtigungen für alle Benachrichtigungsprofile angezeigt werden soll. Beispiel: **sender@unternehmen.org**.
Mail-Server-Adressen	Geben Sie den Namen des SMTP-Mailservers ein, der e-Mail-Benachrichtigungen sendet. Beispiel: **mailserver.unternehmen.org**.
Mail-Server-Port	Der für Verbindungen zum Server verwendete TCP-Port. Der Standardport ist 25 für unverschlüsselte Verbindungen, verschlüsselte Verbindungen verwenden typischerweise den Port 465 oder 587.
Die Verbindung zum Server verschlüsseln	Wenn Sie die Kommunikation zwischen dem Management Server und dem SMTP-Mailserver sichern wollen, aktivieren Sie dieses Kontrollkästchen. Die Verbindung wird mithilfe des E-Mail-Protokollbefehls STARTTLS gesichert. In dieser Betriebsart beginnt die Sitzung mit einer unverschlüsselten Verbindung, dann erfolgt ein STARTTLS-Befehl vom SMTP-Mailserver an den Management-Server, auf die sichere Kommunikation mithilfe von SSL umzuschalten.
Server erfordert Login	Wenn diese Option aktiviert ist, müssen Sie einen Benutzernamen und ein Passwort für die Benutzer zur Anmeldung beim Mailserver festlegen.

Registerkarte „AVI-Generierung“ (Optionen)

Auf der Registerkarte **AVI-Generierung** können Sie Komprimierungseinstellungen für die Generierung von AVI-Videoclipdateien festlegen. Diese Einstellungen sind erforderlich, wenn Sie AVI-Dateien an E-Mailbenachrichtigungen anhängen möchten, die von durch Regeln ausgelösten Benachrichtigungsprofilen gesendet werden.

Siehe auch Benachrichtigungsprofile auf Seite 354.

Name	Beschreibung
Komprimierer	Wählen Sie den Codec (Komprimierungs-/Dekomprimierungstechnologie) aus, den Sie anwenden möchten. Sollten Sie mehr Codecs auf der Liste zur Auswahl haben wollen, installieren Sie diese auf dem Management-Server. Nicht alle Kameras unterstützen alle Codecs.

Name	Beschreibung
Komprimierungsqualität	(Nicht verfügbar für alle Codecs). Verwenden Sie den Schieberegler, um den Komprimierungsgrad zu wählen (**0** – **100**), der vom Codec durchgeführt werden soll. **0** bedeutet keine Komprimierung, wodurch im Allgemeinen die Bildqualität und die Dateigröße zunimmt. **100** bedeutet maximale Komprimierung, wodurch im Allgemeinen die Bildqualität und die Dateigröße abnimmt. Wenn der Schieberegler nicht verfügbar ist, wird die Komprimierungsqualität ausschließlich durch den ausgewählten Codec bestimmt.
Keyframe alle	(Nicht verfügbar für alle Codecs). Wenn Sie Keyframes verwenden möchten, aktivieren Sie das Kontrollkästchen und legen Sie die gewünschte Anzahl an Bildern zwischen den Keyframes fest. Keyframes sind einzelne Bilder, die in einem bestimmten Intervall gespeichert werden. Keyframes enthalten die gesamte Ansicht der Kamera, während die folgenden Bilder nur die geänderten Pixel enthalten. So kann die Größe von Dateien beträchtlich verringert werden. Wenn das Kontrollkästchen nicht verfügbar oder nicht aktiviert ist, enthält jedes Bild die gesamte Ansicht der Kamera.
Datenrate	(Nicht verfügbar für alle Codecs). Wenn Sie eine bestimmte Datenrate festlegen möchten, aktivieren Sie das Kontrollkästchen und legen Sie die Anzahl der Kilobytes pro Sekunde fest. Die Datenrate entscheidet über die Größe der angehängten AVI-Datei. Wenn das Kontrollkästchen nicht verfügbar oder nicht aktiviert ist, wird die Datenrate vom ausgewählten Codec bestimmt.

Netzwerk-Registerkarte (Optionen)

Auf der Registerkarte **Netzwerk** können Sie die IP-Adressen der lokalen Clients festlegen, wenn sich die Clients über das Internet mit dem Aufzeichnungsserver verbinden sollen. Das Überwachungssystem erkennt dann, dass sie vom lokalen Netzwerk kommen.

Sie können auch die IP-Version des Systems festlegen: IPv4 oder IPv6. Standardwert ist IPv4.

Lesezeichen-Registerkarte (Optionen)

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

Auf der Registerkarte **Lesezeichen** können Sie Einstellungen für Lesezeichen, ihre IDs und Funktionen in XProtect Smart Client festlegen.

Name	Beschreibung
Präfix der Lesezeichen-ID	Legen Sie ein Präfix für Lesezeichen fest, das von allen Benutzern von XProtect Smart Client erstellt wird.
Standardmäßige Lesezeichenzeit	Legen Sie die standardmäßige Start- und Endzeit für Lesezeichen fest, die in XProtect Smart Client erstellt werden. Diese Einstellung muss abgestimmt werden mit: • Die standardmäßige Lesezeichenregel finden Sie unter Regeln auf Seite 340 • Dem Voralarm-Puffer für jede Kamera, siehe Geräte, die Voralarm-Puffern unterstützen auf Seite 238

Zum Festlegen der Lesezeichenrechte einer Rolle, siehe Registerkarte „Geräte“ (Rollen) auf Seite 409.

Registerkarte „Benutzereinstellungen“ (Optionen)

Auf der Registerkarte **Benutzereinstellungen** können Benutzer ihre bevorzugten Einstellungen festlegen, z. B. ob eine Nachricht angezeigt werden soll, wenn Fernaufzeichnung aktiviert ist.

Registerkarte „Customer Dashboard" (Kunden-Dashboard) (Optionen)

Auf der Registerkarte **Customer Dashboard (Kunden Dashboard)** können Sie Milestone Customer Dashboard aktivieren oder deaktivieren.

Kunden Dashboard ist ein Online-Überwachungsdienst, der Systemadministratoren oder anderen Personen, die Zugriff auf Informationen zur Ihrer Systeminstallation haben, eine grafische Übersicht über den aktuellen Status Ihres Systems bietet, einschließlich mögliche technische Probleme wie Kameraausfälle.

Sie können das Kontrollkästchen jederzeit aktivieren oder deaktivieren, um Ihre Kunden–Dashboard-Einstellungen zu ändern.

Registerkarte Beweissicherung (Optionen)

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

Auf der Registerkarte **Beweissicherung** können Sie Beweissicherungsprofile bearbeiten und die Dauer festlegen, die Ihre Clientbenutzer auswählen können, um den Schutz der Daten zu gewährleisten.

Name	Beschreibung
Beweissicherungsprofile	Eine Liste mit angelegten Beweissicherungsprofilen. Sie können Beweissicherungsprofile hinzufügen und entfernen. Sie können das Standard-Beweissicherungsprofil nicht entfernen, aber Sie können die Zeitoptionen und den Namen des Profils ändern.
Sperrzeitoptionen	Die Beweissicherungsdauer, die Clientbenutzer auswählen können. Verfügbare Optionen sind Stunde(n), Tag(e), Woche(n), Monat(e), Jahr(e), unbestimmt oder benutzerdefiniert.

Zur Angabe der Zugriffsrechte einer Rolle für die Beweissicherung sehe die Registerkarte Registerkarte „Geräte“ (Rollen) auf Seite 409 für die Einstellungen für eine Rolle.

Registerkarte „Audionachrichten“ (Optionen)

Über die Registerkarte **Audionachrichten** können Sie Dateien mit Audionachrichten hochladen, deren Sendung durch bestimmte Regeln ausgelöst wird.

Es können maximal 50 Dateien hochgeladen werden und die maximale Größe beträgt 1 MB pro Datei.

Name	Beschreibung
Name	Zeigt den Namen einer Nachricht an. Sie geben den Namen beim Hinzufügen der Nachricht ein. Klicken Sie auf **Hinzufügen**, um eine Nachricht auf das System hochzuladen.
Beschreibung	Zeigt eine Beschreibung der Nachricht an.

Name	Beschreibung
	Sie geben die Beschreibung beim Hinzufügen der Nachricht ein. Sie können als Beschreibung den Verwendungszweck oder die Nachricht selbst angeben.
Hinzufügen	Damit können Sie Audionachrichten auf das System hochladen. Unterstützt werden die standardmäßigen Audiodateiformate von Windows: • .wav • .wma • .flac
Bearbeiten	Damit können Sie den Namen und die Beschreibung bearbeiten oder die jeweilige Datei ersetzen.
Entfernen	Damit löschen Sie die Audionachricht von der Liste.
Wiedergabe	Klicken Sie auf diese Schaltfläche, um sich die Audionachricht von dem Computer anzuhören, auf dem Management Client ausgeführt wird.

Zum Festlegen einer Regel, die die Wiedergabe von Audiodateien auslöst, siehe Regeln auf Seite 340.

Um mehr über Aktionen im Allgemeinen zu erfahren, die Sie in Regeln verwenden können, siehe Aktionen und Stopp-Aktionen (Erklärung) auf Seite 312.

Registerkarte „Zutrittskontrolleinstellungen“ (Optionen)

Zur Nutzung von XProtect Access müssen Sie eine Basislizenz erworben haben, die Ihnen den Zugriff auf diese Funktion erlaubt.

Name	Beschreibung
Fenster "Entwicklungseigenschaften" anzeigen	Wenn ausgewählt, erscheinen zusätzliche Entwicklerinformationen für **Zutrittskontrolle > Allgemeine Einstellungen**. Diese Einstellung sollte nur von Entwicklern verwendet werden, die Zutrittskontrollsysteme integrieren.

Registerkarte „Analyseereignisse“ (Optionen)

Auf der Registerkarte **Analyseereignisse** können Sie die Funktion Analyseereignisse aktivieren und genauer bestimmen.

Name	Beschreibung
Aktivieren	Legen Sie fest, ob Sie Analyseereignisse verwenden möchten. Standardmäßig ist diese Funktion deaktiviert.
Port	Legen Sie den Port fest, der von dieser Funktion verwendet werden soll. Die Standardeinstellung ist Port 9090. Stellen Sie sicher, dass die entsprechenden VCA-Tool-Hersteller auch diese Portnummer verwenden. Denken Sie beim Ändern der Portnummer daran, auch die Portnummer der Hersteller zu ändern.
Alle Netzwerkadressen oder Angegebenen Netzwerkadressen	Legen Sie fest, ob Ereignisse von allen IP-Adressen/Hostnamen zugelassen werden oder nur Ereignisse von IP-Adressen/Hostnamen, die auf der **Adressliste** (siehe unten) aufgeführt werden.
Adressliste	Legen Sie eine Liste vertrauenswürdiger IP-Adressen/Hostnamen an. Die Liste filtert eingehende Daten, sodass nur Ereignisse von bestimmten IP-Adressen/Hostnamen zugelassen werden. Sie können die Adressformate beider Domänen-Namen-Systeme (DNS), IPv4 und IPv6 verwenden. Sie können Adressen zu Ihrer Liste hinzufügen, indem Sie jede IP-Adresse oder jeden Hostnamen manuell eingeben oder eine externe Adressliste importieren. • **Manuelle Eingabe**: Geben Sie die IP-Adresse/den Hostnamen in die Adressliste ein. Wiederholen Sie diesen Schritt für alle Adressen • **Importieren**: Klicken Sie auf **Importieren** und öffnen Sie die externe Adressliste. Die externe Liste muss eine .txt-Datei sein und jede IP-Adresse oder jeder Hostname muss auf einer separaten Leitung sein

Registerkarte „Alarme und Ereignisse“ (Optionen)

Über die Registerkarte **Alarme und Ereignisse** können Sie Einstellungen für Alarme, Ereignisse und Protokolle festlegen. Für weitere Informationen bezogen auf diese Einstellungen siehe auch Größenbegrenzung für die Datenbank auf Seite 53.

Name	Beschreibung
Geschlossene Alarme beibehalten für	Legen Sie eine Anzahl an Tagen fest, für welche die Alarme mit dem Status **Geschlossen** in der Datenbank gespeichert bleiben. Wenn Sie den Wert auf **0** setzen, wird der Alarm gelöscht, nachdem er geschlossen wurde. Alarme besitzen immer einen Zeitstempel. Wird der Alarm von einer Kamera ausgelöst, dann wird mit dem Zeitstempel ein Bild vom Zeitpunkt des Alarms gespeichert. Die Alarminformation selbst wird auf dem Event Server gespeichert, während die Videoaufnahmen, die zu dem angehängten Bild gehören, auf dem Server des entsprechenden Überwachungssystems gespeichert werden. Behalten Sie die Videoaufnahmen mindestens so lange, wie Sie Ihre Alarme auf dem Event Server behalten wollen, damit Sie die Bilder des Alarms ansehen können.
Alle anderen Alarme beibehalten für	Legen Sie die Anzahl an Tagen fest, für welche die Alarme mit dem Status **Neu**, **Wird verarbeitet** oder **Zurückgestellt** gespeichert werden. Wenn Sie den Wert auf 0 festlegen, erscheint der Alarm im System, wird aber nicht gespeichert.

Name	Beschreibung
	Alarme besitzen immer einen Zeitstempel. Wird der Alarm von einer Kamera ausgelöst, dann wird mit dem Zeitstempel ein Bild vom Zeitpunkt des Alarms gespeichert. Die Alarminformation selbst wird auf dem Event Server gespeichert, während die Videoaufnahmen, die zu dem angehängten Bild gehören, auf dem Server des entsprechenden Überwachungssystems gespeichert werden. Behalten Sie die Videoaufnahmen mindestens so lange, wie Sie Ihre Alarme auf dem Event Server behalten wollen, damit Sie die Bilder des Alarms ansehen können.
Protokolle beibehalten für	Legen Sie die Anzahl an Tagen fest, für welche die Protokolle des Event-Servers beibehalten werden sollen. Sollten Sie die Protokolle für einen längeren Zeitraum beibehalten, so stellen Sie sicher, dass der Computer mit dem Event Server über ausreichend Speicherplatz verfügt.
Verbose-Protokollierung aktivieren	Markieren Sie das Kontrollkästchen, um ein detailliertes Protokoll der Event Server-Kommunikation aufzubewahren. Es wird für die Anzahl an Tagen gespeichert, die im Feld **Protokolle beibehalten für** festgelegt wurde.
Ereignistypen	Legen Sie die Anzahl an Tagen fest, für welche die Ereignisse in der Datenbank gespeichert werden sollen. Es gibt zwei Möglichkeiten, dies zu tun: • Sie können die Speicherzeit für eine gesamte Ereignisgruppe festlegen. Ereignistypen mit dem Wert **Gruppe folgen** übernehmen den Wert der Ereignisgruppe • Sie können die Speicherzeit für einzelne Ereignistypen auch dann festlegen, wenn Sie einen Wert für eine Ereignisgruppe bestimmen. Wenn der Wert **0** beträgt, werden die Ereignisse nicht in der Datenbank gespeichert.

Name	Beschreibung
	Externe Ereignisse (benutzerdefinierte Ereignisse, generische Ereignisse und Eingangsereignisse) werden standardmäßig auf **0** gesetzt und der Wert kann nicht geändert werden. Der Grund dafür ist, dass diese Ereignistypen so häufig auftreten, dass ihre Speicherung in der Datenbank Leistungsprobleme verursachen könnte.

Registerkarte „Generische Ereignisse“ (Optionen)

Auf der Registerkarte **Generische Ereignisse** können Sie generische Ereignisse und Einstellungen zu Datenquellen festlegen.

Für weitere Informationen zum Konfigurieren von generischen Ereignissen siehe Generische Ereignisse auf Seite 367.

Name	Beschreibung
Datenquelle	Sie können zwischen zwei standardmäßigen Datenquellen wählen und eine benutzerdefinierte Datenquelle einstellen. Die Wahl hängt von Ihrem Drittanbieterprogramm und/oder der Hardware oder Software ab, die Sie als Interface verwenden möchten: **Kompatibel**: Werkseinstellungen sind aktiviert, Echo bei allen Bytes, TCP und UDP, nur IPv4, Port 1234, kein Trennzeichen, nur lokaler Host, aktuelle Codepage-Verschlüsselung (ANSI). **International**: Werkseinstellungen sind aktiviert, Echo nur bei Statistiken, nur TCP, IPv4+6, Port 1235, <CR><LF> als Trennzeichen, nur lokaler Host, UTF-8-Kodierung. (<CR><LF> = 13,10). [Datenquelle A] [Datenquelle B] und so weiter.
Neu	Anklicken, um eine neue Datenquelle zu definieren.

Name	Beschreibung
Name	Name der Datenquelle.
Aktiviert	Datenquellen sind standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Datenquelle zu deaktivieren.
Zurücksetzen	Anklicken, um alle Einstellungen der ausgewählten Datenquelle zurückzusetzen. Der Name, der im Feld **Name** eingegeben wurde, bleibt.
Port	Die Portnummer der Datenquelle.
Protokolltypauswahl	Protokolle, die vom System beachtet und analysiert werden sollen, um generische Ereignisse zu erkennen: **Beliebig**: Sowohl TCP als auch UDP. **TCP**: Nur TCP. **UDP**: Nur UDP. TCP- und UDP-Pakete, die für generische Ereignisse verwendet werden, dürfen Sonderzeichen enthalten, wie z. B. @, #, +, ~ und andere.
IP-Typauswahl	Auswählbare IP-Adressentypen: IPv4, IPv6 oder beide.
Separator-Bytes	Wählen Sie die Separator-Bytes aus, um einzelne generische Ereignisaufzeichnungen zu trennen. Der Standardwert für den Datenquelltyp **International** (siehe **Datenquellen** oben) ist **13,10**. (13,10 = <CR><IF>).
Echotypauswahl	Verfügbare Formate für die Echorückstrahlung: • **Echo-Statistiken**: Echo für das folgende Format: **[X],[Y],[Z],[Name generisches Ereignis]** **[X]** = Anforderungsnummer. **[Y]** = Zeichenzahl. **[Z]** = Anzahl der Übereinstimmungen mit einem generischen Ereignis. **[Name generisches Ereignis]** = Name, der im Feld **Name** eingegeben wurde. • **Echo bei allen Bytes**: Echo bei allen Bytes

Name	Beschreibung
	• **Kein Echo**: Unterdrückt alle Echos
Kodierungstypauswahl	Standardmäßig zeigt die Liste nur die wichtigsten Optionen. Aktivieren Sie **Alle anzeigen**, um alle verfügbaren Kodierungen anzuzeigen.
Zulässige externe IPv4-Adressen	Bestimmen Sie die IP-Adressen, mit denen Management-Server kommunizieren können muss, um externe Ereignisse zu verwalten. Sie können damit auch IP-Adressen ausschließen, von denen Sie keine Daten möchten.
Zulässige externe IPv6-Adressen	Bestimmen Sie die IP-Adressen, mit denen Management-Server kommunizieren können muss, um externe Ereignisse zu verwalten. Sie können damit auch IP-Adressen ausschließen, von denen Sie keine Daten möchten.

Aufgabenliste für die Erstkonfiguration

Die folgende Checkliste enthält die ersten Aufgaben zur Konfiguration Ihres Systems. Einige davon haben Sie möglicherweise bereits während der Installation abgeschlossen.

Eine ausgefüllte Prüfliste an sich garantiert nicht, dass das System den genauen Anforderungen Ihrer Organisation entspricht. Damit das System mit den Anforderungen Ihrer Organisation übereinstimmt, empfiehlt Milestone, dass Sie das System kontinuierlich überwachen und anpassen.

Beispielsweise ist es ratsam, die Empfindlichkeitseinstellungen für die Bewegungserkennung durch einzelne Kameras unter unterschiedlichen, physischen Bedingungen zu testen, wenn das System ausgeführt wird, einschließlich von Tag/Nacht und bei windigem/ruhigem Wetter.

Das Einrichten der Regeln, die die meisten Aktionen festlegen, die Ihr System ausführt, einschließlich des Zeitpunkts der Aufzeichnung eines Videos, ist ein weiteres Beispiel für eine Konfiguration, die Sie gemäß den Anforderungen Ihrer Organisation ändern können.

Schritt	Beschreibung
☑	Sie haben die erste Installation Ihres Systems fertig gestellt. Siehe Installation eines neuen XProtect-Systems auf Seite 78.
☑	Ändern Sie den SLC in einen permanenten SLC (bei Bedarf).

Schritt	Beschreibung
	Siehe Softwarelizenzcode ändern auf Seite 51.
☑	Melden Sie sich bei Management Client an. Siehe Übersicht über das Anmeldeverfahren auf Seite 114.
☐	Prüfen Sie, ob die Speichereinstellungen jedes Aufzeichnungsservers Ihren Einstellungen entsprechen. Siehe Registerkarte „Speicher“ (Aufzeichnungsserver) auf Seite 157.
☐	Prüfen Sie, ob die Archivierungseinstellungen jedes Aufzeichnungsservers Ihren Einstellungen entsprechen. Siehe Registerkarte „Speicher“ (Aufzeichnungsserver) auf Seite 157.
☐	Erkennt die Hardware, Kameras oder Video-Encoder, die jedem Aufzeichnungsserver hinzugefügt werden. Beachten Sie Hardware hinzufügen auf Seite 197.
☐	Konfigurieren Sie die einzelnen Kameras jedes Aufzeichnungsservers. Siehe Kamerageräte (Erklärung) auf Seite 215.
☐	Aktivieren Sie die Speicherung und Archivierung für einzelne Kameras oder für eine Gruppe von Kameras. Dies erfolgt über einzelne Kameras oder über die Gerätegruppe. Beachten Sie Registerkarte „Speicher“ (Aufzeichnungsserver) auf Seite 157.
☐	Geräte aktivieren und konfigurieren. Beachten Sie Site-Navigation: Geräte: Arbeiten mit Geräten auf Seite 214.
☐	Das Verhalten des Systems wird in großem Umfang von Regeln festgelegt. In den zu erstellenden Regeln ist festgelegt, wann die Kameras aufzeichnen sollen, wann Pan-Tilt-Zoom-Kameras (PTZ) aufzeichnen und wann Benachrichtigungen verschickt werden sollen. Regeln erstellen. Siehe Regeln und Ereignisse (Erklärung) auf Seite 310.

Schritt	Beschreibung
☐	Rollen zum System hinzufügen. Siehe Regeln (Erklärung) auf Seite 373.
☐	Fügen Sie zu jeder der Rollen Benutzer oder Gruppen von Benutzern hinzu. Beachten Sie Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen auf Seite 377.
☐	Lizenzen aktivieren. Siehe Lizenzinformationen auf Seite 138oder Lizenzinformationen auf Seite 138.

Siehe auch Konfigurieren des Systems im Site-Navigationsfenster auf Seite 138.

Konfigurieren des Systems im Site-Navigationsfenster

Im **Site-Navigationsfenster** können Sie Ihr System konfigurieren und verwalten, sodass es Ihren Bedürfnissen entspricht. Wenn Ihr System kein Einzelstandortsystem ist, aber föderale Standorte beinhaltet, beachten Sie, dass Sie diesen Standort im Fenster **Hierarchie der föderalen Standorte** verwalten können.

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

Site-Navigation: Grundlagen

Dieser Abschnitt beschreibt, wie Lizenzen angezeigt und verwaltet und wie Informationen über die Seite hinzugefügt werden.

Lizenzinformationen

Sie können alle Lizenzen, die dieselbe Softwarelizenzdatei an diesem und an allen anderen Standorten nutzen, sowie Ihre Milestone Care-Abonnements nachverfolgen und entscheiden, wie Sie Lizenzen aktivieren möchten. Grundlegende Informationen zu den verschiedenen XProtect-Lizenzen finden Sie unter Lizenzen (Erklärung) auf Seite 50.

Lizenziert für

Auflistung der Kontaktangaben des Lizenzinhabers, die während der Softwareregistrierung eingegeben wurden. Klicken Sie auf **Details bearbeiten**, um die Angaben zum Lizenzinhaber zu bearbeiten. Hier finden Sie auch einen Link zu dem Endbenutzer-Lizenzvertrag, den Sie vor der Installation akzeptiert haben.

Milestone Care

Hier finden Sie Informationen über Ihre aktuelle Milestone Care™-Einstufung. Beim Kauf Ihres Systems haben Sie auch ein zweijähriges Milestone Care Plus-Abonnement eingegeben. Ihre Installation ist immer von Milestone Care Basic abgedeckt. Zudem erhalten Sie Zugriff auf unterschiedliche Selbsthilfematerialien wie Wissensdatenbank-Artikel, Handbücher und Tutorials auf der Support-Website (https://www.milestonesys.com/support/). Das Ablaufdatum Ihres Milestone Care Plus-Abonnements ist in der Tabelle **Installierte Produkte** ersichtlich.Wenn Sie sich entscheiden, nach der Installation Ihres Systems ein Milestone Care-Abonnement zu kaufen oder zu verlängern, müssen Sie die Lizenzen aktivieren, bevor die korrekten Milestone Care-Informationen angezeigt werden.

Ein Milestone Care Plus-Abonnement gibt Ihnen Zugriff auf Upgrades. Sie erhalten auch Zugriff auf den Kunden Dashboard-Dienst (Kunden Dashboard), die Smart-Connect-Funktion und die vollständige PushBenachrichtigungs-Funktionalität Wenn Sie ein Milestone Care Premium-Abonnement besitzen, können Sie auch den Milestone-Support kontaktieren, um Hilfe zu erhalten. Denken Sie daran, Informationen über Ihre Milestone Care-ID anzugeben, wenn Sie Milestone kontaktieren. Das Ablaufdatum für Ihr Milestone Care Premium ist erneut sichtbar. Wenn Sie mehr über Milestone Care erfahren möchten, folgen Sie den Links.

Installierte Produkte

Listet folgende Angaben über alle installierten Basislizenzen für XProtect VMS und Zusatzprodukte auf, die dieselbe Softwarelizenzdatei nutzen:

- Produkte und Versionen
- Dem Softwarelizenzcode (SLC) der Produkte
- Das Ablaufdatum des SLC. Normalerweise unbegrenzt
- Das Ablaufdatum Ihres Milestone Care Plus-Abonnements
- Das Ablaufdatum Ihres Milestone Care Premium-Abonnements

Manche Lizenzen, wie XProtect Essential+, werden mit aktivierter automatischer Lizenzaktivierung installiert, sodass die Einstellung nicht deaktiviert werden kann.

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	

Lizenzübersicht - Alle Sites

Führt die Zahl der aktivierten Gerätelizenzen oder anderer Lizenzen in der Softwarelizenzdatei und die Gesamtzahl der für das System verfügbaren Lizenzen auf. Hier erkennen Sie mit einem Blick, ob Sie Ihr System noch erweitern können, ohne zusätzliche Lizenzen zu erwerben.

Für eine detaillierte Übersicht des Status Ihrer an anderen Standorten aktivierten Lizenzen klicken Sie auf den Link **Lizenzdetails – alle Standorte**. Im Bereich **Lizenzdetails – aktueller Standort** unten sehen Sie die verfügbaren Informationen.

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

Wenn Sie Lizenzen für Zusatzprodukte haben, finden Sie weitere Details zu diesen unter den Zusatzprodukt-spezifischen Punkten im **Bereich „Standort-Navigation“**.

Lizenzdetails – aktueller Standort

In der Spalte **Aktiviert** ist die Anzahl aktivierter Gerätelizenzen oder anderer Lizenzen an diesem Standort aufgeführt.

In der Spalte **Geräteänderungen ohne Aktivierung** sehen Sie außerdem die Anzahl verwendeter Geräteänderungen ohne Aktivierung (siehe Geräteänderungen ohne Aktivierung (Erklärung) auf Seite 141) und die Anzahl der jährlich verfügbaren Änderungen.

Wenn Sie Lizenzen haben, die noch nicht aktiviert sind und deshalb im Übergangszeitraum laufen, sind diese in der Spalte **Im Übergangszeitraum** aufgeführt. Das Ablaufdatum der ersten Lizenz, die abläuft, wird unter der Tabelle in Rot angezeigt.

Wenn Sie vergessen, Lizenzen vor Ablauf des Übergangszeitraums zu aktivieren, senden sie keine Videodaten mehr an das System. Diese Lizenzen sind in der Spalte **Übergangszeitraum abgelaufen** aufgeführt. Für weitere Informationen siehe Lizenzen nach Übergangszeitraum aktivieren auf Seite 145.

Wenn Sie mehr Lizenzen verwendet haben, als verfügbar sind, sind diese in der Spalte **Ohne Lizenz** aufgeführt. Sie können im System nicht verwendet werden. Für weitere Informationen siehe Erhalten zusätzlicher Lizenzen auf Seite 146.

Wenn Sie Lizenzen haben, die sich in einem Übergangszeitraum befinden, bei denen der Übergangszeitraum abgelaufen ist oder für die keine Lizenzen vorhanden sind, wird bei jedem Anmelden bei Management Client eine entsprechende Erinnerungsmeldung angezeigt.

License Details - Current Site: SYS

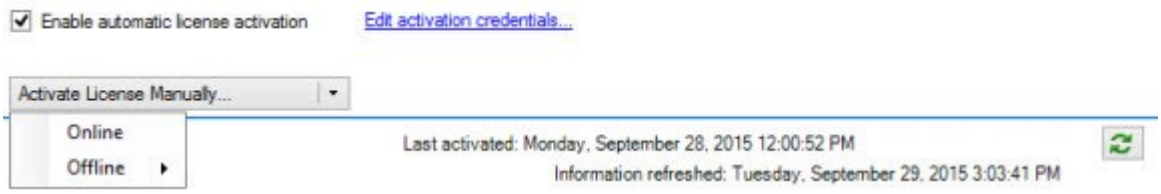
License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Hardware Device	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

Geräte ohne Lizenzen sind in Management Client durch ein Ausrufezeichen gekennzeichnet. Das Ausrufezeichen wird auch für andere Zwecke verwendet. Bewegen Sie den Mauszeiger auf das Ausrufezeichen, um die Bedeutung anzuzeigen.

Funktionen zur Lizenzaktivierung

Unter den drei Tabellen befinden sich folgende Elemente:

- Ein Kontrollkästchen zum Aktivieren der automatischen Lizenzaktivierung und ein Link zum Bearbeiten der Benutzeranmeldedaten zur automatischen Aktivierung. Weitere Informationen finden Sie unter Automatische Lizenzaktivierung (Erklärung) auf Seite 143 und Automatische Lizenzaktivierung aktivieren auf Seite 144. Wenn die automatische Aktivierung fehlgeschlagen ist, wird eine Fehlermeldung in Rot angezeigt. Für weitere Informationen klicken Sie auf den Link **Details**
- Eine Dropdown-Liste zur manuellen Aktivierung von Lizenzen (online oder offline). Weitere Informationen finden Sie unter Lizenzen online aktivieren auf Seite 144 und Lizenzen offline aktivieren auf Seite 145
- Rechts unten auf der Seite sehen Sie, wann Ihre Lizenzen zuletzt aktiviert wurden (automatisch oder manuell) und wann die Informationen auf der Seite aktualisiert wurden. Die Zeitstempel stammen vom Server, nicht vom lokalen Computer



Geräteänderungen ohne Aktivierung (Erklärung)

Auf der Seite **Grundlagen** > **Lizenzinformationen** wird in der Spalte **Änderungen ohne Aktivierung** die Zahl der Geräte angezeigt, die Sie austauschen oder hinzufügen können, ohne Ihre Gerätelizenzen aktivieren zu müssen. Außerdem können Sie sehen, wie viele Änderungen Sie seit der letzten Aktivierung vorgenommen haben. Geräte, die Sie im Rahmen Ihrer Geräteänderungen ohne Aktivierung hinzufügen, werden als vollständig aktivierte Gerätelizenzen ausgeführt.

Ein Jahr nach Ihrer letzten Lizenzaktivierung wird Ihre Zahl der **Geräteänderungen ohne Aktivierung** automatisch auf null zurückgesetzt. Nach dem Zurücksetzen können Sie weiter Geräte hinzufügen und austauschen, ohne die Lizenzen aktivieren zu müssen.

Die Zahl der Geräteänderungen ohne Aktivierung unterscheidet sich von Installation zu Installation und wird anhand verschiedener Variablen berechnet. Eine genaue Beschreibung dazu finden Sie unter Lizenzinformationen auf Seite 138.

Wenn Ihr Überwachungssystem für längere Zeit offline ist (zum Beispiel ein Überwachungssystem auf einem Schiff, das sich auf großer Fahrt befindet, oder an einem sehr entlegenen Ort ohne Internetzugriff), können Sie sich an Ihren Milestone-Vertriebspartner wenden und um eine höhere Zahl von Geräteänderungen ohne Aktivierung bitten.

Ihrem Distributor müssen Sie erklären, warum Sie meinen, für eine höhere Zahl von Geräteänderungen ohne Aktivierung qualifiziert zu sein. Milestone entscheidet jede Anfrage auf individueller Basis. Wenn Ihnen mehr Geräteänderungen ohne Aktivierung gewährt werden, müssen Sie Ihre Lizenzen aktivieren, um die höhere Zahl im XProtect-System zu registrieren.

So berechnet sich die Zahl der Geräteänderungen ohne Aktivierung

Die Geräteänderungen ohne Aktivierung werden anhand von drei Variablen berechnet. Wenn Sie über mehrere Installationen der Milestone-Software verfügen, gelten die Variablen für jede von ihnen separat. Die Variablen umfassen:

- **C%** ist ein fester Prozentsatz der Gesamtmenge aktivierter Lizenzen
- **Cmin** ist ein fester Minimalwert der Zahl von Geräteänderungen ohne Aktivierung
- **Cmax** ist ein fester Maximalwert der Zahl von Geräteänderungen ohne Aktivierung

Die Zahl der Geräteänderungen ohne Aktivierung kann nie unter dem **Cmin**-Wert bzw. über dem **Cmax**-Wert liegen. Der anhand der **C%**-Variable errechnete Wert hängt davon ab, wie viele aktivierte Geräte sich in den einzelnen Installationen Ihres Systems befinden. Geräte, die mittels Geräteänderungen ohne Aktivierung hinzugefügt wurden, werden von der **C%**-Variable nicht als aktiviert gezählt.

Milestone definiert die Werte aller drei Variablen, wobei sich die Werte ohne Ankündigung ändern können. Die Werte der Variablen hängen vom jeweiligen Produkt ab.

Weitere Informationen über die aktuellen Standardwerte für Ihr Produkt finden Sie unter My Milestone (https://www.milestonesys.com/device-change-calculation/).

Beispiele basieren auf folgenden Werten: C% = 15 %, Cmin = 10 und Cmax = 100

Ein Kunde kauft 100 Gerätelizenzen. Er fügt seinem System 100 Kameras hinzu. Solange er keine automatische Lizenzaktivierung gewählt hat, betragen seine Geräteänderungen ohne Aktivierung weiterhin null. Der Kunde aktiviert seine Lizenzen und weist nun 15 Geräteänderungen ohne Aktivierung auf.

Ein Kunde kauft 100 Gerätelizenzen. Er fügt seinem System 100 Kameras hinzu und aktiviert seine Lizenzen. Die Geräteänderungen ohne Aktivierung des Kunden belaufen sich nun auf 15. Der Kunde entscheidet sich, ein Gerät aus seinem System zu löschen. Er weist nun 99 aktivierte Geräte auf, während die Zahl der Geräteänderungen ohne Aktivierung auf 14 sinkt.

Ein Kunde kauft 1.000 Gerätelizenzen. Er fügt seinem System 1.000 Kameras hinzu und aktiviert seine Lizenzen. Die Geräteänderungen ohne Aktivierung des Kunden belaufen sich nun auf 100. Gemäß der **C%**-Variable sollte er nun über 150 Geräteänderungen ohne Aktivierung verfügen, die **Cmax**-Variable lässt jedoch nur 100 Geräteänderungen ohne Aktivierung zu.

Ein Kunde kauft 10 Gerätelizenzen. Er fügt seinem System 10 Kameras hinzu und aktiviert seine Lizenzen. Die Zahl der Geräteänderungen ohne Aktivierung des Kunden beläuft sich aufgrund der **Cmin**-Variable nun auf 10. Wenn die Zahl ausschließlich anhand der **C%**-Variable berechnet worden wäre, würde sie lediglich 1 betragen (15 % von 10 = 1,5 – abgerundet auf 1).

Ein Kunde kauft 115 Gerätelizenzen. Er fügt seinem System 100 Kameras hinzu und aktiviert seine Lizenzen. Die Geräteänderungen ohne Aktivierung des Kunden belaufen sich nun auf 15. Er fügt weitere 15 Kameras hinzu, ohne sie zu aktivieren, indem er 15 seiner 15 Geräteänderungen ohne Aktivierung nutzt. Der Kunde entfernt 50 der Kameras aus dem System; seine Geräteänderungen ohne Aktivierung sinken auf 7. Das bedeutet, dass 8 der zuvor hinzugefügten Kameras innerhalb der 15 Geräteänderungen ohne Aktivierung in einen Übergangszeitraum eingehen. Nun fügt der Kunde 50 neue Kameras hinzu. Da der Kunde bei der letzten Aktivierung von Lizenzen in seinem System 100 Kameras aktiviert hat, reduzieren sich die Geräteänderungen ohne Aktivierung wieder auf 15 und die 8 Kameras, die in den Übergangszeitraum verschoben wurden, werden wieder zu Geräteänderungen ohne Aktivierung. Die 50 neuen Kameras befinden sich nun in einem Übergangszeitraum.

Anzeigen der Lizenzübersicht

Für alle Standorte, die mit der gleichen Softwarelizenzdatei lizenziert wurden, können Sie eine Lizenzübersicht aufrufen, in der Lizenzen angezeigt werden, die aktiviert sind, sich in einem Übergangszeitraum befinden, abgelaufen sind oder fehlen.

- Klicken Sie auf **Lizenzübersicht**

Wenn die Verbindung unterbrochen wurde, können Sie lediglich die Zahl der aktivierten Lizenzen anzeigen. Für Lizenzen in einem Übergangszeitraum, abgelaufene Lizenzen und fehlende Lizenzen wird „N/A“ angezeigt.

Automatische Lizenzaktivierung (Erklärung)

Für eine einfache Wartung und hohe Flexibilität empfiehlt Milestone die Verwendung einer automatischen Lizenzaktivierung (siehe Automatische Lizenzaktivierung aktivieren auf Seite 144), da sich dadurch der Wartungsaufwand für Sie reduziert. Die automatische Aktivierung von Lizenzen setzt voraus, dass der Management-Server online ist.

Wenn die obigen Anforderungen erfüllt sind, aktiviert das System Ihre Geräte oder andere Lizenzen nur wenige Minuten nachdem Sie Geräte hinzugefügt, entfernt oder ausgetauscht bzw. andere Änderungen vorgenommen haben, welche sich auf die Verwendung Ihrer Lizenzen auswirken. Daher brauchen Sie nie eine Lizenzaktivierung manuell starten. Die Anzahl der verwendeten Geräteänderungen ohne Aktivierung ist immer Null. Keine Hardwaregeräte befinden sich innerhalb einer Probezeit und haben das Risiko abzulaufen. Wenn eine Ihrer Basislizenzen innerhalb von 14 Tagen abläuft, wird Ihr XProtect-System als Vorsichtsmaßnahme jede Nacht automatisch versuchen, Ihre Lizenzen zu aktivieren.

Das einzige Mal, dass Sie Ihre Lizenzen manuell aktivieren müssen ist, wenn Sie:

- Kaufen Sie zusätzliche Lizenzen (siehe Erhalten zusätzlicher Lizenzen auf Seite 146)
- Möchten Sie ein Upgrade vornehmen (siehe Upgrade-Anforderungen auf Seite 532)
- Kaufen oder erneuern Sie ein Milestone Care-Abonnement (siehe Automatische Lizenzaktivierung (Erklärung))
- Erhalten Sie eine Genehmigung für mehr Geräteänderungen ohne Aktivierung (siehe Geräteänderungen ohne Aktivierung (Erklärung) auf Seite 141)

Automatische Lizenzaktivierung aktivieren

1. Wählen Sie auf der Seite **Lizenzinformationen** die Option **Automatische Lizenzaktivierung aktivieren**.
2. Geben Sie den Benutzernamen und das Passwort ein, die Sie für die automatische Lizenzaktivierung verwenden möchten:
   - Wenn Sie ein bereits vorhandener Benutzer sind, geben Sie Ihren Benutzernamen und das Passwort ein, um sich im Software-Registrierungssystem anzumelden
   - Wenn Sie ein neuer Benutzer sind, klicken Sie zur Einrichtung eines neuen Benutzerkontos auf den Link **Neuen Benutzer erstellen** und befolgen Sie das Registrierungsverfahren. Wenn Sie Ihren Softwarelizenzcode (SLC) noch nicht registriert haben, müssen Sie das nun tun

     Die Anmeldeinformationen werden in einer Datei auf dem Management-Server gespeichert.
3. Klicken Sie auf **OK**.

Wenn Sie Ihren Benutzernamen und/oder das Passwort für die automatische Aktivierung später ändern möchten, klicken Sie auf den Link **Aktivierungs-Anmeldeinformationen bearbeiten**.

Automatische Lizenzaktivierung deaktivieren

Deaktivieren der automatischen Lizenzaktivierung, jedoch unter Beibehaltung des Passworts zur späteren Verwendung:

1. Löschen Sie auf der Seite **Lizenzinformationen** die Auswahl **Automatische Lizenzaktivierung aktivieren**. Das Passwort und der Benutzername bleiben weiterhin auf dem Management-Server gespeichert.

Deaktivieren der automatischen Lizenzaktivierung und Löschen des Passworts:

1. Klicken Sie auf der Seite **Lizenzinformationen** auf **Aktivierungs-Anmeldeinformationen bearbeiten**.
2. Klicken Sie auf **Passwort löschen**.
3. Bestätigen Sie, dass Sie das Passwort und den Benutzernamen vom Management-Server löschen möchten.

Lizenzen online aktivieren

Aktivieren Sie Ihre Lizenzen online, wenn der Computer, auf dem der Management-Server ausgeführt wird, über einen InternetZugriff verfügt.

1. Wählen Sie im Knoten **Lizenzinformationen** die Option **Lizenz manuell aktivieren** und dann **Online** aus.
2. Das Dialogfeld **Online aktivieren** wird angezeigt:
   - Wenn Sie ein bereits vorhandener Benutzer sind, geben Sie Ihren Benutzernamen und das Passwort ein
   - Wenn Sie ein neuer Benutzer sind, klicken Sie zur Einrichtung eines neuen Benutzerkontos auf den Link **Neuen Benutzer erstellen**. Wenn Sie Ihren Softwarelizenzcode (SLC) noch nicht registriert haben, müssen Sie das nun tun
3. Klicken Sie auf **OK**.

Wenn Sie bei der Online-Aktivierung eine Fehlermeldung erhalten, folgen Sie den Anweisungen auf dem Bildschirm, um das Problem zu beheben oder wenden Sie sich an den Milestone-Support.

Lizenzen offline aktivieren

Wenn der Computer, auf dem der Management-Server ausgeführt wird, keinen InternetZugriff hat, können Sie Lizenzen offline aktivieren.

1. Wählen Sie dazu im Knoten **Lizenzinformationen** die Optionen **Lizenz manuell aktivieren** > **Offline** > **Lizenz zur Aktivierung exportieren**, um eine Lizenzanforderungsdatei (.lrq) mit Informationen zu den hinzugefügten Geräten zu exportieren.
2. Die Lizenzanforderungsdatei (.lrq) erhält automatisch den gleichen Namen wie Ihr SLC. Wenn Sie über mehrere Standorte verfügen, müssen Sie sicherstellen, dass der Name eindeutig ist, damit Sie leichter erkennen können, welche Datei zu welchem Standort gehört.
3. Kopieren Sie die Lizenzanforderungsdatei auf einen Computer mit Internetzugriff, und melden Sie sich bei unserer Website (https://online.milestonesys.com/) an, um die aktivierte Software-Lizenzdatei (.lic) abzurufen.
4. Kopieren Sie die .lic-Datei, die den gleichen Namen trägt wie Ihre Lizenzanforderungsdatei, mit Management Client auf Ihren Computer.
5. Wählen Sie auf der Seite Management Client **Lizenzinformationen** die Optionen **Lizenz offline aktivieren** > **Aktivierte Lizenz importieren** und dann die aktivierte Software-Lizenzdatei aus, um sie zu importieren und so Ihre Lizenzen zu aktivieren.
6. Klicken Sie auf **Fertig stellen**, um den Aktivierungsvorgang zu beenden.

Lizenzen nach Übergangszeitraum aktivieren

Wenn Sie eine Lizenz (für Geräte, Milestone Interconnect-Kamera oder Zutrittskontrolltüren) nicht während der Probezeit aktivieren, ist das entsprechende Gerät nicht mehr verfügbar, sodass es sich im Überwachungssystem auch nicht mehr nutzen lässt:

- Die Konfiguration der Kamera und andere Einstellungen werden nicht aus dem Management Client entfernt
- Die Lizenz wird nicht aus der Systemkonfiguration entfernt
- Um die nicht verfügbaren Geräte erneut zu aktivieren, aktivieren Sie die Lizenzen wie gewohnt. Weitere Informationen dazu finden Sie unter Lizenzen offline aktivieren auf Seite 145 oder Lizenzen online aktivieren auf Seite 144

Erhalten zusätzlicher Lizenzen

Wenn Sie mehr Geräte, Milestone Interconnect-Systeme oder Türen hinzufügen möchten bzw. bereits hinzugefügt haben, als Sie Lizenzen haben, müssen Sie zusätzliche Lizenzen kaufen, damit die entsprechenden Geräte Daten an Ihr System senden können:

- Wenn Sie zusätzliche Lizenzen für Ihr System benötigen, wenden Sie sich an Ihren XProtect Produktpartner

Neue Lizenzen für die aktuelle Version Ihres Überwachungssystems:

- Sorgen Sie einfach für eine manuelle Aktivierung Ihrer Lizenzen, um Zugriff auf die neuen Lizenzen zu erhalten. Weitere Informationen dazu finden Sie unter Lizenzen offline aktivieren auf Seite 145 oder Lizenzen online aktivieren auf Seite 144

Neue Lizenzen für eine aktualisierte Version des Überwachungssystems:

- Sie erhalten eine aktualisierte Software-Lizenzdatei (.**lic**) (siehe Lizenzen (Erklärung) auf Seite 50) inklusive der neuen Lizenzen und der neuen Version. Bei der Installation der neuen Version müssen Sie die neue Software-Lizenzdatei verwenden. Weitere Informationen finden Sie unter Upgrade-Anforderungen auf Seite 532.

Lizenzen für einen Austausch von Geräten

Ein Gerät (z. B. eine Kamera), das in Ihrem System lizenziert ist, können Sie gegen ein neues Gerät austauschen, das an dessen Stelle aktiviert und lizenziert wird.

Wenn Sie ein Gerät von einem Aufzeichnungsserver entfernen, wird eine Gerätelizenz frei.

Wenn Sie eine Kamera gegen eine ähnliche Kamera (Hersteller, Marke und Modell) austauschen und der neuen Kamera die gleiche IP-Adresse zuweisen, haben Sie weiter vollständigen Zugriff auf alle Datenbanken der Kamera. In diesem Fall können Sie das Netzwerkkabel aus der alten Kamera einfach in die neue Kamera stecken, ohne Einstellungen im Management Client ändern zu müssen.

Wenn Sie ein Gerät gegen ein anderes Modell austauschen, müssen Sie den Assistenten **Hardware ersetzen** (siehe Hardware ersetzen auf Seite 510) verwenden, um alle relevanten Kameradatenbanken, Mikrofone, Eingänge, Ausgänge und Einstellungen richtig zuordnen zu können.

Wenn Sie die automatische Lizenzaktivierung aktiviert haben (siehe Automatische Lizenzaktivierung aktivieren auf Seite 144), wird das neue Gerät automatisch aktiviert.

Wenn Sie alle Ihre Geräteänderungen ohne Aktivierung (siehe Geräteänderungen ohne Aktivierung (Erklärung) auf Seite 141) bereits verwendet haben, müssen Sie Ihre Lizenzen manuell aktivieren. Weitere Informationen zum Aktivieren von Lizenzen finden Sie unter Lizenzen offline aktivieren auf Seite 145 oder Lizenzen online aktivieren auf Seite 144.

Site-Informationen

Für eine einfachere Identifikation jedes Standortes können Sie weitere Informationen zu einem Standort hinzufügen, beispielsweise in einer großen Milestone Federated Architecture Einrichtung. Neben dem Standortnamen, können Sie auch folgendes beschreiben:

- Adresse/Standort
- Administrator(en)
- Weitere Informationen

Site-Informationen bearbeiten

Zur Aktualisierung der Standortinformationen:

1. Wählen Sie **Bearbeiten**.
2. Wählen Sie ein Tag.
3. Geben Sie die Informationen im Feld **Werte** ein.
4. Klicken Sie auf **OK**.

Site-Navigation: Server und Hardware

Dieser Abschnitt beschreibt, wie Aufzeichnungsserver und Failover-Aufzeichnungsserver installiert und konfiguriert werden. Sie lernen außerdem, wie Hardware zum System hinzugefügt und andere Seiten miteinander verbunden werden.

- Site-Navigation: Server und Hardware: Aufzeichnungsserver auf Seite 147
- Site-Navigation: Server und Hardware: Failover-Server auf Seite 184
- Site-Navigation: Server und Hardware: Hardware auf Seite 197
- Site-Navigation: Server und Hardware: Verwalten von Remote-Servern auf Seite 212

Site-Navigation: Server und Hardware: Aufzeichnungsserver

Aufzeichnungsserver (Erklärung)

Das System verwendet Aufzeichnungsserver zum aufnehmen von Videofeeds und für die Kommunikation mit Kameras und anderen Geräten. Ein Überwachungssystem besteht typischerweise aus mehreren Aufzeichnungsservern.

Aufzeichnungsserver sind Computer, auf denen Sie die Software Aufzeichnungsserver installiert und sie so konfiguriert haben, dass sie mit dem Management-Server kommuniziert. Aufzeichnungsserver werden im Bereich **Übersicht** angezeigt, wenn Sie den **Server**-Ordner ausklappen und dann **Aufzeichnungsserver** auswählen.

Abwärtskompatibilität mit Aufzeichnungsservern älterer Versionen als diese Version des Management-Servers sind eingeschränkt. Sie können mit älteren Versionen immer noch auf Aufzeichnungen der Aufzeichnungsserver zugreifen, allerdings muss für eine Änderung der Konfiguration die Version mit der des Management-Servers übereinstimmen. Milestone empfiehlt ein Upgrade aller Aufzeichnungsserver in Ihrem System auf die gleiche Version, die auf Ihrem Management-Server läuft.

Der Aufzeichnungsserver unterstützt die Verschlüsselung von Datenstreams an Clients und Dienste. Weitere Informationen finden Sie unter Vor dem Start der Installation auf Seite 59:

- Verschlüsselung zu Clients und Servern aktivieren auf Seite 456
- Verschlüsselungsstatus an Clients anzeigen auf Seite 153

Der Aufzeichnungsserver unterstützt auch die Verschlüsselung der Verbindung mit dem Managementserver Weitere Informationen finden Sie unter Vor dem Start der Installation auf Seite 59:

- Verschlüsselung aktivieren auf Seite 453
- Verschlüsselung für Aufzeichnungsserver oder Remote Server aktivieren auf Seite 455

Sie haben mehrere Optionen bei der Verwaltung Ihres Aufzeichnungsservers:

- Hardware hinzufügen auf Seite 197
- Hardware verschieben auf Seite 506
- Löschen sämtlicher Hardware auf einem Aufzeichnungsserver auf Seite 528
- Deinstallieren eines Aufzeichnungsservers auf Seite 528

Wenn der Aufzeichnungsserver-Dienst ausgeführt wird, ist es äußerst wichtig, dass weder der Windows Explorer noch andere Programme auf Mediendatenbank-Ordner oder -Dateien zugreifen, die Ihrer Systemkonfiguration zugewiesen sind. Wenn sie es dennoch tun, ist es wahrscheinlich, dass der Aufzeichnungsserver wichtige Mediendaten nicht umbenennen oder verschieben kann. Dies könnte den Aufzeichnungsserver stoppen. Um einen gestoppten Aufzeichnungsserver neu zu starten, halten Sie den Aufzeichnungsserver-Dienst an, schließen Sie das Programm, das auf die Mediendaten oder Ordner zugreift und starten Sie den Aufzeichnungsserver-Dienst neu.

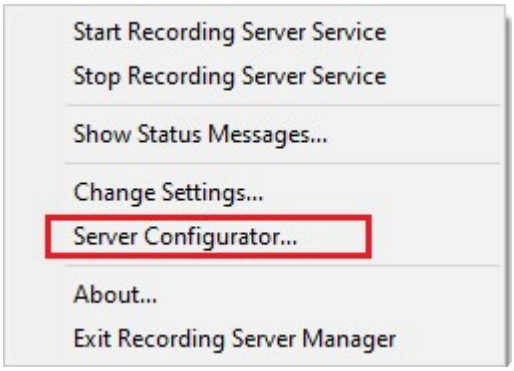
Registrieren eines Aufzeichnungsservers

Bei der Installation eines Aufzeichnungsserver wird dieser meist automatisch registriert. Die Registrierung müssen Sie jedoch manuell vornehmen, wenn:

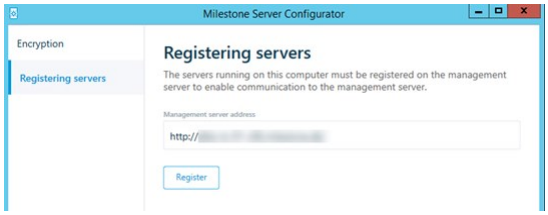
- Sie haben den Aufzeichnungsserver ersetzt
- Der Aufzeichnungsserver wurde offline installiert und hinterher zum Managementserver hinzugefügt
- Ihr Managementserver verwendet nicht die Standardports. Die Portnummern sind von der Konfiguration der Verschlüsselung abhängig. Weitere Informationen finden Sie unter Vom System verwendete Ports auf Seite 33
- Eine automatische Registrierung ist fehlgeschlagen, z.B. nach Änderung der Adresse des Management Servers, oder nach der Aktivierung oder Deaktivierung der Verschlüsselungseinstellungen für die Serverkommunikation

Bei der Registrierung eines Aufzeichnungsservers wird dieser für eine Verbindung mit Ihrem Management-Server konfiguriert. Der Teil des Management-Servers, der sich um Registrierungen kümmert, ist der Authorization Server-Dienst.

1. Öffnen Sie Server Configurator entweder vom Windows-Startmenü oder vom Taskleistensymbol für den Aufzeichnungsserver aus.



2. Wählen Sie unter Server Configurator **Serverregistrierung**.



3. Überprüfen Sie die Adresse des Managementservers sowie das Schema (http oder https), zu dem die Server auf dem Computer eine Verbindung herstellen sollen, und klicken Sie dann auf **Registrieren**.

Dann erscheint eine Bestätigung, die besagt, dass die Registrierung auf dem Management Server erfolgreich war.

Siehe auch Ersetzen eines Aufzeichnungsservers auf Seite 505.

Ändern oder überprüfen Sie die Basiskonfiguration eines Aufzeichnungsservers

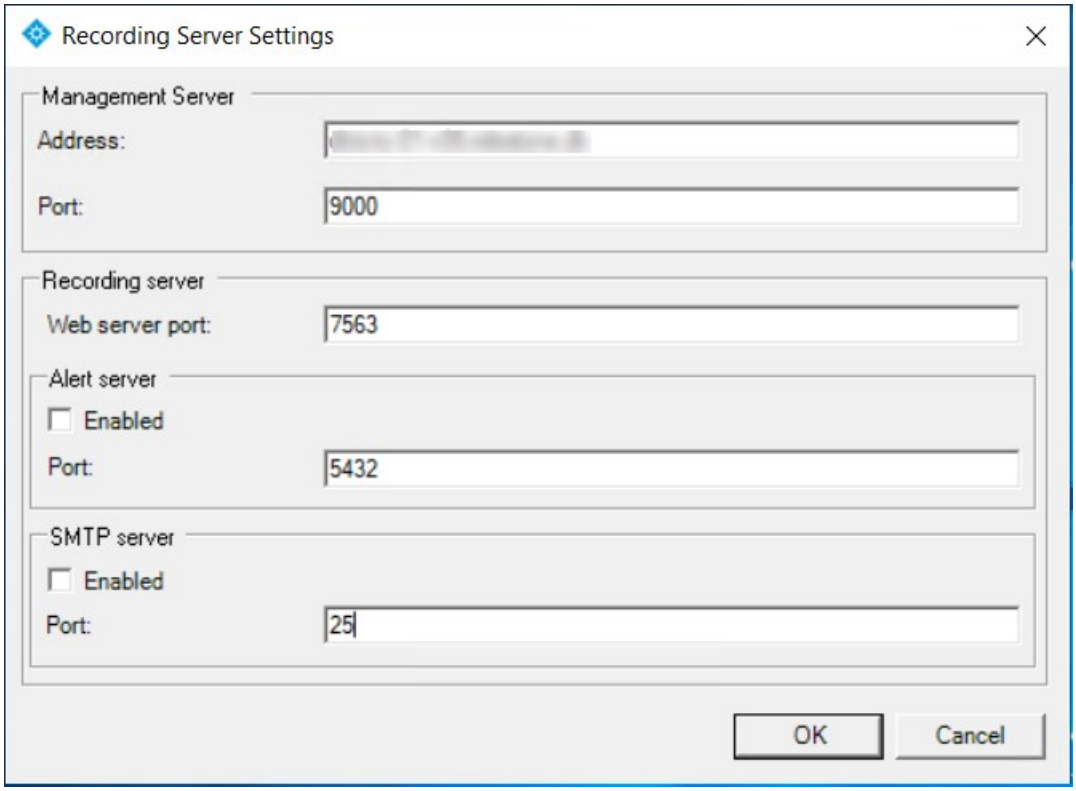
Wenn Management Client nicht alle installierten Aufzeichnungsserver auflistet, wurden wahrscheinlich die Einstellungsparameter (zum Beispiel: IP-Adresse oder Hostname des Management-Servers) während der Installation falsch konfiguriert.

Sie müssen die Aufzeichnungsserver nicht neu installieren, um die Parameter des Management-Servers festzulegen, aber Sie können seine Grundeinstellungen ändern/bestätigen:

1. Auf dem ausführendem Computer des Aufzeichnungsservers, klicken Sie mit der rechten Maustaste auf das **Aufzeichnungsserver**-Symbol im Benachrichtigungsbereich.
2. Wählen Sie **Aufzeichnungsserver Service stoppen** aus.

3. Klicken Sie nochmals auf das **Aufzeichnungsserver**-Symbol und wählen Sie **Einstellungen ändern**.

   Das Fenster **Aufzeichnungsserver-Einstellungen** wird angezeigt.



4. Überprüfen oder ändern Sie z.B. die folgenden Einstellungen:
   - **Management Server**: **Adresse**: Geben Sie die IP-Adresse oder den Hostnamen des Management Servers an, mit dem der Aufzeichnungsserver verbunden sein soll.
   - **Management Server**: **Port**: Geben Sie die bei der Kommunikation mit dem Management-Server zu verwendende Portnummer an. Sie können dies ggf. ändern, die Portnummer muss jedoch stets der Portnummer entsprechen, die auf dem Management Server eingerichtet wurde. Siehe Vom System verwendete Ports auf Seite 33.
   - **Aufzeichnungsserver**: **Web-Server-Port**: Geben Sie die bei der Kommunikation mit dem Aufzeichnungsserver zu verwendende Portnummer an. Siehe Vom System verwendete Ports auf Seite 33.
   - **Aufzeichnungsserver**: **Alarm-Server-Port** Aktivieren Sie die Portnummer und geben Sie die bei der Kommunikation mit dem Alarm-Server des Aufzeichnungsservers zu verwendende Portnummer an, der auf Ereignismeldungen von Geräten wartet. Siehe Vom System verwendete Ports auf Seite 33.
   - **SMTP-Server**: **Port**: Aktivieren Sie die Portnummer und geben Sie die bei der Kommunikation mit dem Dienst Simple Mail Transfer Protocol (SMTP) des Aufzeichnungsservers zu verwendende Portnummer an. Siehe Vom System verwendete Ports auf Seite 33.

5. Klicken Sie auf **OK**.
6. Um den Aufzeichnungsserver-Dienst wieder zu starten, klicken Sie mit der rechten Maustaste auf das **Aufzeichnungsserver**-Symbol und wählen Sie **Aufzeichnungsserver Dienst** starten aus.

Ein Anhalten des Aufzeichnungsserver-Dienstes hat zur Folge, dass Sie kein Live-Video aufzeichnen oder anschauen können, während Sie die Grundeinstellungen des Aufzeichnungsservers bestätigen/ändern.

Das Fenster mit den Einstellungen des Aufzeichnungsservers

Wenn Sie mit der rechten Maustaste auf das Taskleistensymbol Recording Server Manager klicken und **Einstellungen ändern** auswählen, können Sie folgende Angaben vornehmen:

Name	Beschreibung
Adresse	IP -Adresse (z.B.: 123.123.123.123) oder Hostname (z.B. "ourserver") des Management Servers, mit dem der Aufzeichnungsserver verbunden sein soll. Diese Angaben sind notwendig, damit der Aufzeichnungsserver mit dem Management Server kommunizieren kann.
Port	Die bei der Kommunikation mit dem Management-Server zu verwendende Portnummer. Der Standardport ist 9000. Bei Bedarf können Sie dies ändern.
Web-Server-Port	Zur Bearbeitung von Anfragen vom Webserver zu verwendende Portnummer, z.B. zur Bearbeitung der PTZ-Kamerasteuerungsbefehle und für Browsing- und Live-Anfragen von XProtect Smart Client. Der Standardport ist 7563. Bei Bedarf können Sie dies ändern.
Alarmserverport	Die zu verwendende Portnummer, wenn der Aufzeichnungsserver auf TCP-Informationen wartet (manche Geräte verwenden TCP zum Versenden von Ereignismeldungen). Der Standardport ist 5432 (standardmäßig deaktiviert). Bei Bedarf können Sie dies ändern.
SMTP-Server-Port	Die zu verwendende Portnummer, wenn der Aufzeichnungsserver auf Simple Mail Transfer Protocol (SMTP)-Informationen wartet. SMTP ist ein Standard zum Versenden von Benachrichtigungen zwischen Servern per E-Mail. Manche Geräte verwenden SMTP zum Versenden von Ereignismeldungen oder Bildern an den Überwachungssystemserver per E-Mail. Der Standardport ist 25; diesen können Sie

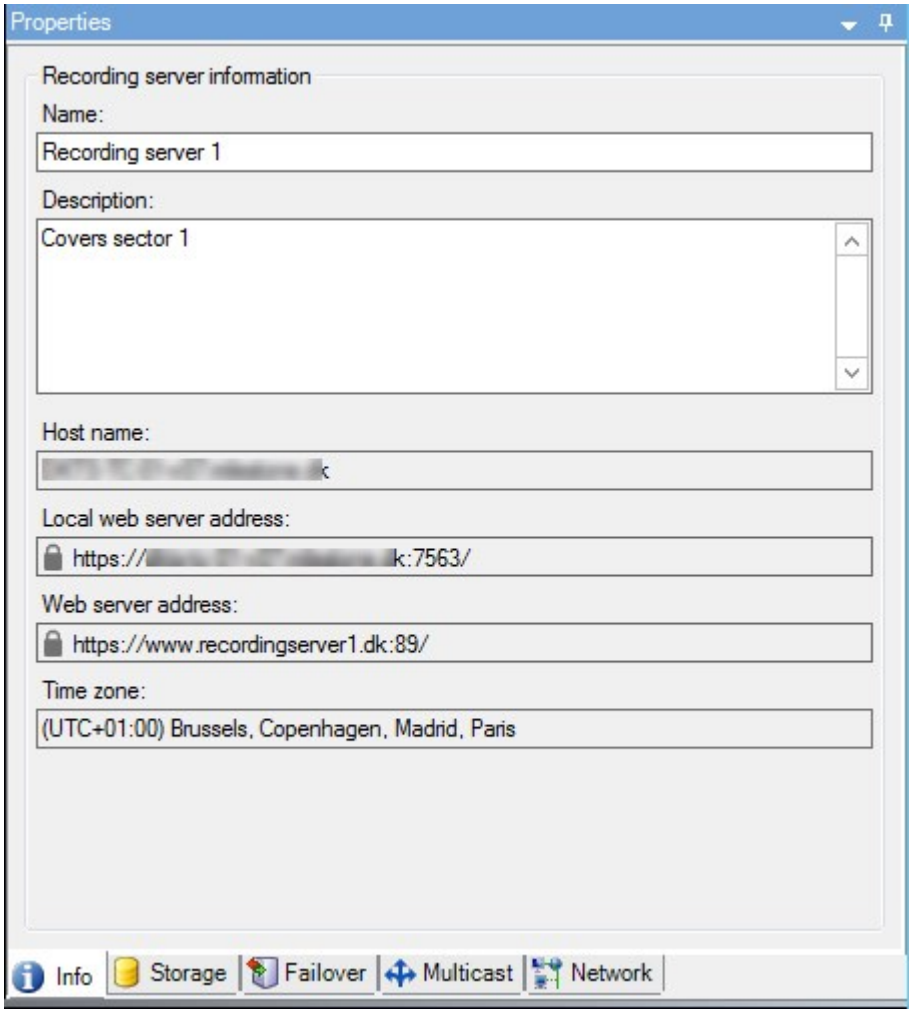
Name	Beschreibung
	aktivieren und deaktivieren. Bei Bedarf können Sie die Portnummer ändern.
Verschlüsselung der Verbindungen vom Management Server zum Aufzeichnungsserver	Bevor Sie die Verschlüsselung aktivieren und ein Zertifikat zur Serverauthentifizierung von der Liste auswählen, vergewissern Sie sich, dass Sie die Verschlüsselung auf dem Management Server zuerst aktivieren und dass dem Zertifikat des Management Servers auf den Aufzeichnungsservern vertraut wird. Weitere Informationen finden Sie unter Vor dem Start der Installation auf Seite 59:
Verschlüsseln Sie die Verbindungen zu Clients und Diensten, die Daten streamen	Bevor Sie die Verschlüsselung aktivieren und ein Zertifikat zur Authentifizierung des Servers von der Liste auswählen, vergewissern Sie sich, dass dem Zertifikat auf allen Computern vertraut wird, auf denen Dienste laufen, die Datenstreams vom Aufzeichnungsserver abrufen. XProtect Smart Client und alle Dienste, die Datenstreams vom Aufzeichnungsserver abrufen, müssen auf die Version 2019 R1 oder höher aktualisiert werden. Manche Lösungen von Drittanbietern, die mit Hilfe von Versionen von MIP SDK erstellt wurden, die älter sind als die Version 2019 R1, müssen ggf. aktualisiert werden. Weitere Informationen finden Sie unter Vor dem Start der Installation auf Seite 59. Um zu überprüfen, ob Ihr Aufzeichnungsserver eine Verschlüsselung verwendet, siehe Verschlüsselungsstatus an Clients anzeigen auf Seite 153.
Details	Angaben aus dem Windows Certificate Store zu dem ausgewählten Zertifikat anzeigen.

Verschlüsselungsstatus an Clients anzeigen

Um zu überprüfen, ob Ihr Aufzeichnungsserver eine Verschlüsselung verwendet:

1. Öffnen Sie den Management Client.
2. Wählen Sie im Bereich **Standort-Navigation** die Optionen **Server** > **Aufzeichnungsserver**. Daraufhin wird eine Liste mit Aufzeichnungsservern geöffnet.

3. Wählen Sie in dem Fenster **Übersicht** den jeweiligen Aufzeichnungsserver aus und gehen Sie auf die Registerkarte **Info**.
   Wenn die Verschlüsselung zu Clients und Servern, die Datenstreams vom Aufzeichnungsserver abrufen, aktiviert ist, erscheint ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der des optionalen Webservers.



Aufzeichnungsserver-Statussymbole

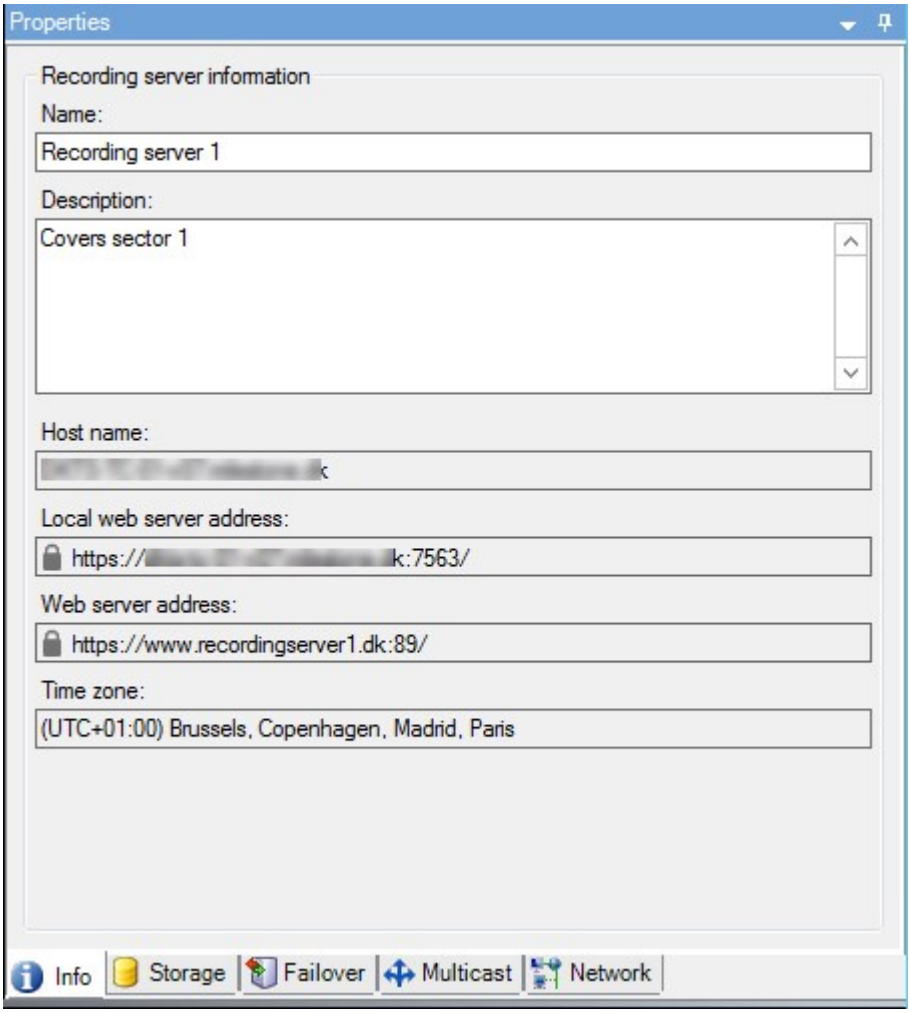
Management Client verwendet die folgenden Symbole, um den Status der einzelnen Aufzeichnungsserver anzuzeigen:

Symbol	Beschreibung
	**Aufzeichnungsserver wird ausgeführt**
	**Aufzeichnungsserver benötigt Aufmerksamkeit**: Entweder wird der Aufzeichnungsserver nicht ausgeführt oder er läuft mit Fehlern. 1. Bewegen Sie den Cursor über das Symbol des Aufzeichnungsservers, um die Statusmeldung anzuzeigen. 2. Wenn Sie den Aufzeichnungsserver starten oder stoppen müssen, klicken Sie mit der rechten Maustaste auf das Recording Server Manager-Taskleistensymbol.
	**Anhaltende Datenbankwiederherstellung**: Erscheint wenn z. B. aufgrund eines Stromausfalls Fehler in den Datenbanken auftreten, und der Aufzeichnungsserver diese repariert. Der Wiederherstellungsprozess kann je nach Größe der Datenbanken einige Zeit in Anspruch nehmen. Weitere Informationen zur Vermeidung von Datenbankfehlern, finden Sie unter Schützen von Aufzeichnungsdatenbanken vor Beschädigungen auf Seite 58.  Während eine Wiederherstellung einer Datenbank bei Systemstart durchgeführt wird, können Sie kein Video mit den zum Aufzeichnungsserver verbundenen Kameras aufzeichnen. Nur die Live-Ansicht steht zur Verfügung.  Eine Datenbankwiederherstellung bei normalem Betrieb beeinflusst die Aufzeichnungen nicht.

Registerkarte „Info“ (Aufzeichnungsserver)

Auf der Registerkate **Info** können Sie den Namen und die Beschreibung des Aufzeichnungsservers überprüfen oder bearbeiten.

Sie können den Host-Namen und die Adressen anschauen. Das Vorhängeschloss-Symbol vor der Adresse des Webservers zeigt die Verschlüsselung der Kommunikation mit den Clients und Diensten an, die Datenstreams von diesem Aufzeichnungsserver abrufen.



Eigenschaften der Registerkarte Info (Aufzeichnungsserver)

Name	Beschreibung
Name	Sie können sich aussuchen, ob Sie für den Aufzeichnungsserver einen Namen eingeben wollen. Der Name wird im System und von den Clients verwendet, wenn der Aufzeichnungsserver aufgeführt ist. Der Name muss nicht einzigartig sein. Wenn Sie einem Aufzeichnungsserver einen neuen Namen geben, wird der Name in Management Client global geändert.
Beschreibung	Sie können sich aussuchen, ob sie eine Beschreibung auswählen möchten, die in mehreren

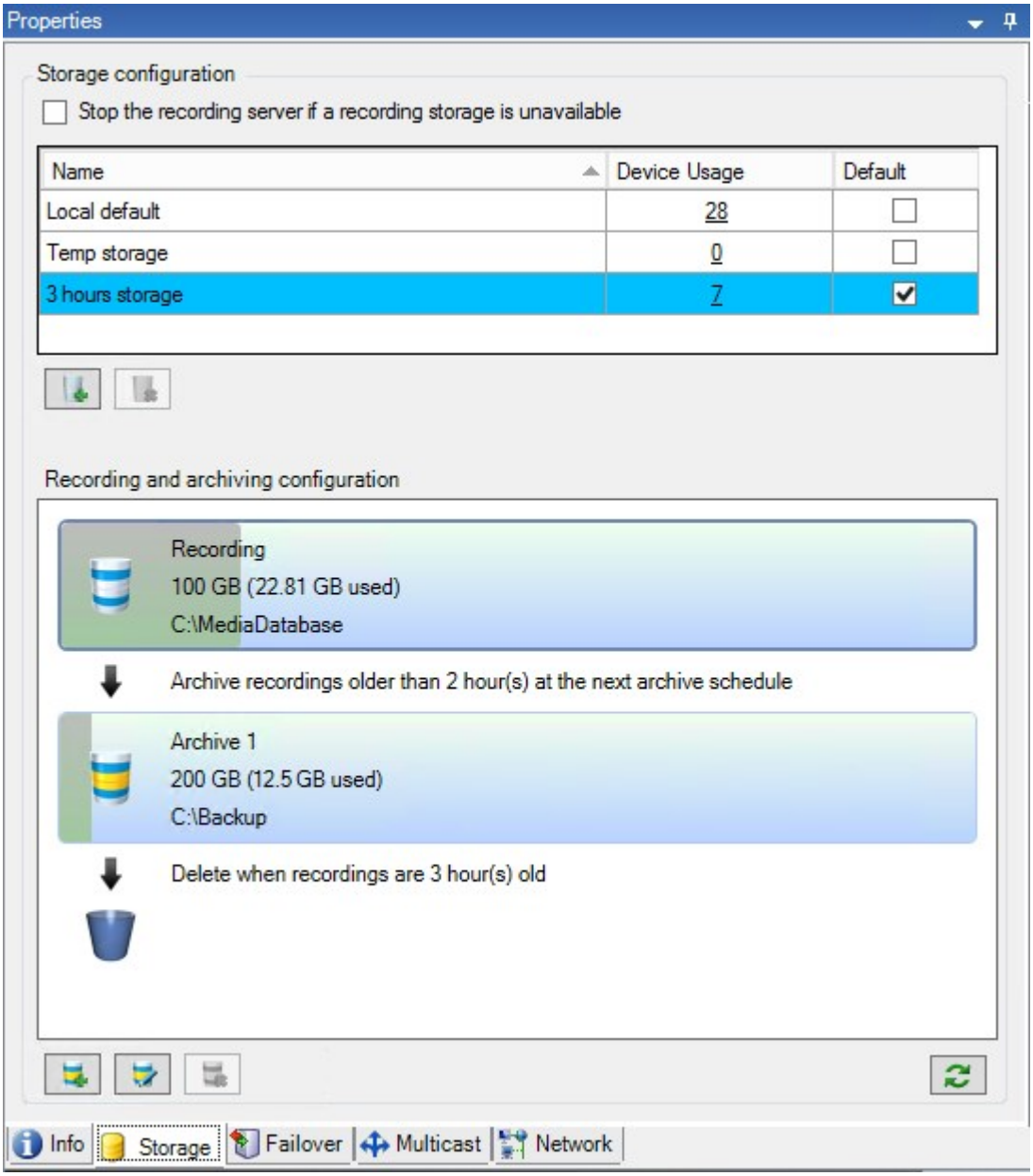
Name	Beschreibung
	Listen im System auftaucht. Beschreibungen sind nicht obligatorisch.
Hostname	Zeigt den Hostnamen des Aufzeichnungsservers an.
Adresse des lokalen Webservers	Zeigt die lokale Adresse des Webservers des Aufzeichnungsservers an. Sie verwenden die lokale Adresse, zum Beispiel zur Handhabung der PTZ-Kamerasteuerungsbefehle, sowie zur Handhabung von Browsing- und Live-Anforderungen von XProtect Smart Client. Die Adresse enthält die Portnummer, die für die Kommunikation mit dem Webserver verwendet wird (typischerweise Port 7563). Wenn Sie die Verschlüsselung zu Clients und Servern aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, erscheint ein Vorhängeschloss-Symbol, und die Adresse enthält **https** anstelle von **http**.
Adresse des Web-Servers	Zeigt die öffentliche Adresse des Webservers des Aufzeichnungsservers über das Internet an. Falls Ihre Installation eine Firewall oder einen NAT-Router verwendet, geben Sie bitte die Adresse der Firewall oder des NAT-Routers ein, damit die Clients, die auf das Überwachungssystem im Internet zugreifen, sich mit dem Aufzeichnungsserver verbinden können. Die öffentliche Adresse und die Portnummer geben Sie auf der Registerkarte **Netzwerk** an. Wenn Sie die Verschlüsselung zu Clients und Servern aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, erscheint ein Vorhängeschloss-Symbol, und die Adresse enthält **https** anstelle von **http**.
Zeitzone	Zeigt die Zeitzone an, in der sich der Aufzeichnungsserver befindet.

Registerkarte „Speicher“ (Aufzeichnungsserver)

Auf der Registerkarte **Speicher** können Sie Aufzeichnungen für einen ausgewählten Aufzeichnungsserver einrichten, verwalten und anzeigen.

Zur Aufzeichnung von Speicher und Archiven zeigt die horizontale Leiste die aktuelle Menge an Speicherplatz an. Sie können das Verhalten des Aufzeichnungsservers für den Fall angeben, dass Aufzeichnungsspeicher nicht mehr verfügbar sind. Dies ist vor allem wichtig, wenn Ihr System Failover-Server beinhaltet.

Bei Verwendung von **Beweissicherung** zeigt eine vertikale rote Linie an, welcher Speicherplatz für Aufnahmen mit Beweissicherung verwendet wird.



Lagerung und Archivierung (Erklärung)

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

Wenn eine Kamera Video- oder Audiodaten aufzeichnet, werden alle ausgewählten Aufzeichnungen standardmäßig in dem für das Gerät definierten Speicher gespeichert. Jeder Speicher besteht aus einem Aufzeichnungsspeicher, der Aufzeichnungen in der **Aufzeichnungs**-Datenbank speichert. Ein Speicher hat keine Standardarchive; Sie können jedoch Archive erstellen.

Um zu vermeiden, dass eine Aufzeichnungsdatenbank vollläuft, können Sie zusätzliche Speichergeräte erstellen (siehe Neues Speichergerät hinzufügen). Außerdem können Sie in jedem Speicher Archive erstellen (siehe Archiv auf einem Speicherlaufwerk anlegen) und ein Archivierungsverfahren zum Speichern von Daten starten.

Bei der Archivierung handelt es sich um die automatische Übertragung von Aufzeichnungen beispielsweise von der Aufzeichnungsdatenbank einer Kamera an einen anderen Speicherort. Das bedeutet, dass die Menge der Aufzeichnungen, die Sie speichern können, nicht auf die Größe der Aufzeichnungsdatenbank beschränkt ist. Bei der Archivierung können Sie Ihre Aufzeichnungen auch auf anderen Medien sichern.

Speicherung und Archivierung lassen sich auf jedem Aufzeichnungsserver konfigurieren.

Solange Sie archivierte Aufzeichnungen lokal oder in aufrufbaren Netzwerklaufwerken speichern, können Sie XProtect Smart Client zu ihrer Ansicht verwenden.

Wenn ein Laufwerk ausfällt und der Aufzeichnungsspeicher nicht länger verfügbar ist, wechselt der horizontale Balken auf Rot. Es ist zwar noch möglich, Live-Video in XProtect Smart Client anzuzeigen, aber die Aufzeichnung und Archivierung wird gestoppt, bis das Festplattenlaufwerk wiederhergestellt wird. Wenn Ihr System mit ausfallsicheren Aufzeichnungsservern konfiguriert ist, können Sie bestimmen, dass der Aufzeichnungsserver nicht mehr ausgeführt werden soll, damit die ausfallsicheren Server übernehmen (siehe Verhalten festlegen, wenn kein Speichergerät für die Aufzeichnungen zur Verfügung steht).

Im Folgenden werden hauptsächlich Kameras und Video erwähnt, das Gleiche gilt jedoch auch für Lautsprecher, Mikrofone, Audio und Ton.

Milestone empfiehlt die Verwendung einer dedizierten Festplatte für die Aufzeichnung-Speicher und -Archive, um eine beeinträchtigte Leistung der Festplatte zu vermeiden. Bei der Formatierung der Festplatte muss die Einstellung **Größe der Zuweisungseinheiten** von 4 auf 64 Kilobyte geändert werden. Dadurch lässt sich die Aufzeichnungsleistung der Festplatte maßgeblich verbessern. Mehr Informationen und Hilfestellungen zur Größe der Zuweisungseinheiten finden Sie auf der Microsoft-Website (https://support.microsoft.com/help/140365/default-cluster-size-for-ntfs-fat-and-exfat/).

Wenn weniger als 5 GB Speicherplatz frei sind, werden immer die ältesten Daten in einer Datenbank automatisch archiviert (oder gelöscht, wenn kein nächstes Archiv festgelegt ist). Wenn weniger als 1 GB frei ist, werden die Daten gelöscht. Eine Datenbank erfordert 250 MB an freiem Speicherplatz. Wenn dieser Grenzwert erreicht wird (da Daten nicht schnell genug gelöscht werden), werden erst dann wieder Daten in die Datenbank geschrieben, wenn Sie genügend Platz freigegeben haben. Die tatsächliche Maximalgröße Ihrer Datenbank ist die Anzahl der angegebenen Gigabyte minus 5 GB.

Für Systeme, die FIPS 140-2 erfüllen, mit Exports und archivierten Mediendatenbanken aus XProtect VMS-Versionen vor 2017 R3, die mithilfe von nicht FIPS-konformen Chiffren verschlüsselt sind, müssen die Daten an einem Ort archiviert werden, wo sie nach Aktivierung von FIPS weiterhin zugänglich sind.
Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

Anbinden von Geräten an einen Speicher

Sobald Sie die Speicher- und Archivierungseinstellungen für einen Aufzeichnungsserver konfiguriert haben, können Sie die Speicherung und Archivierung für einzelne Kameras oder eine Kameragruppe aktivieren. Sie können dies über die einzelnen Geräte oder über die Gerätegruppe ausführen. Beachten Sie Ein Gerät oder eine Gruppe von Geräten an einem Speicher anbringen.

Effektive Archivierung

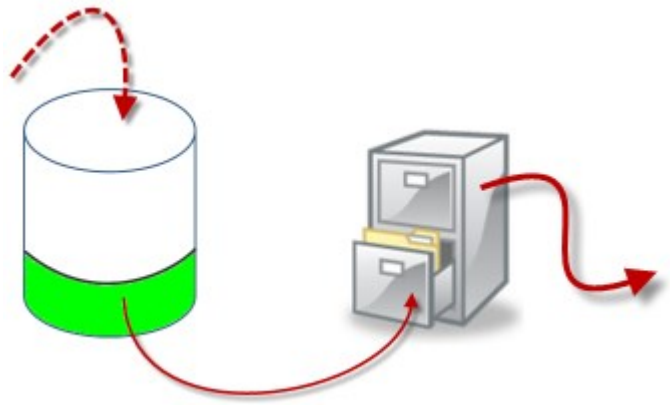
Wenn Sie die Archivierung für eine Kamera oder eine Kameragruppe aktivieren, wird der Inhalt des Aufnahmespeichers in von Ihnen festgelegten Abständen automatisch in das erste Archiv verschoben.

Je nach Anforderungen können Sie für jeden Ihrer Speicher ein oder mehrere Archive konfigurieren. Archive lassen sich entweder lokal auf dem Computer des Aufzeichnungsservers selbst oder an einem anderen Speicherort platzieren, den das System aufrufen kann (z. B. in einem Netzwerklaufwerk).

Indem Sie Ihre Archivierung effektiv einrichten, können Sie den Speicherbedarf optimieren. In vielen Fällen wünschen Sie, dass archivierte Aufzeichnungen so wenig Speicherplatz belegen wie möglich – vor allem auf lange Sicht, wenn unter Umständen auch Abstriche an der Bildqualität hingenommen werden können. Auf der Registerkarte **Speicher** eines Aufzeichnungsservers nehmen Sie effektive Archivierungen vor, indem Sie verschiedene voneinander abhängige Einstellungen anpassen:

- Aufzeichnung der Speichererhaltung
- Aufzeichnung der Speichergröße
- Speicherzeit von Archiven
- Größe von Archiven
- Archiv-Zeitplan
- Verschlüsselung
- Bilder pro Sekunde (FPS).

Mit den Größenfeldern lässt sich die Größe des Aufzeichnungsspeichers, veranschaulicht durch den Zylinder, und seiner Archive festlegen:



Durch Einstellung der Speicherzeit und Größe für die Aufzeichnungsspeicher (veranschaulicht durch den weißen Bereich im Zylinder) können Sie festlegen, wie alt Aufzeichnungen sein müssen, bevor sie archiviert werden. In unserem dargestellten Beispiel archivieren Sie die Aufzeichnungen, wenn sie alt genug sind, um archiviert zu werden.

Die Einstellung der Speicherzeit und Größe für Archive bestimmt darüber, wie lange die Aufzeichnungen im Archiv verbleiben. Aufzeichnungen bleiben für die angegebene Zeit bzw. solange im Archiv, bis das Archiv das festgelegte Größenlimit erreicht hat. Wenn diese Einstellungen erfüllt sind, beginnt das System damit, alte Aufzeichnungen im Archiv zu überschreiben.

Der Archiv-Zeitplan bestimmt darüber, wie oft und zu welchen Zeiten Archivierungen vorgenommen werden.

Die Bilder pro Sekunde bestimmen über die Größe der Daten in den Datenbanken.

Für eine effektive Archivierung Ihrer Aufzeichnungen müssen Sie alle der Parameter passend zueinander konfigurieren. Das bedeutet, dass die Speicherzeit des nächsten Archivs stets länger sein muss als die Speicherzeit des aktuellen Archivs bzw. der aktuellen Aufzeichnungsdatenbank. Der Grund dafür ist, dass die Zahl der Speichertage, die für ein Archiv angegeben sind, alle Speicherzeiten beinhaltet, die früher im Prozess angegeben wurden. Außerdem muss die Archivierung in kürzeren Abständen erfolgen als die Speicherzeit; ansonsten drohen Datenverluste. Wenn Sie eine Speicherzeit von 24 Stunden eingerichtet haben, werden alle Daten gelöscht, die älter als 24 Stunden sind. Wenn Sie Ihre Daten stets sicher ins nächste Archiv verschieben wollen, müssen Sie die Archivierung häufiger als einmal alle 24 Stunden ausführen.

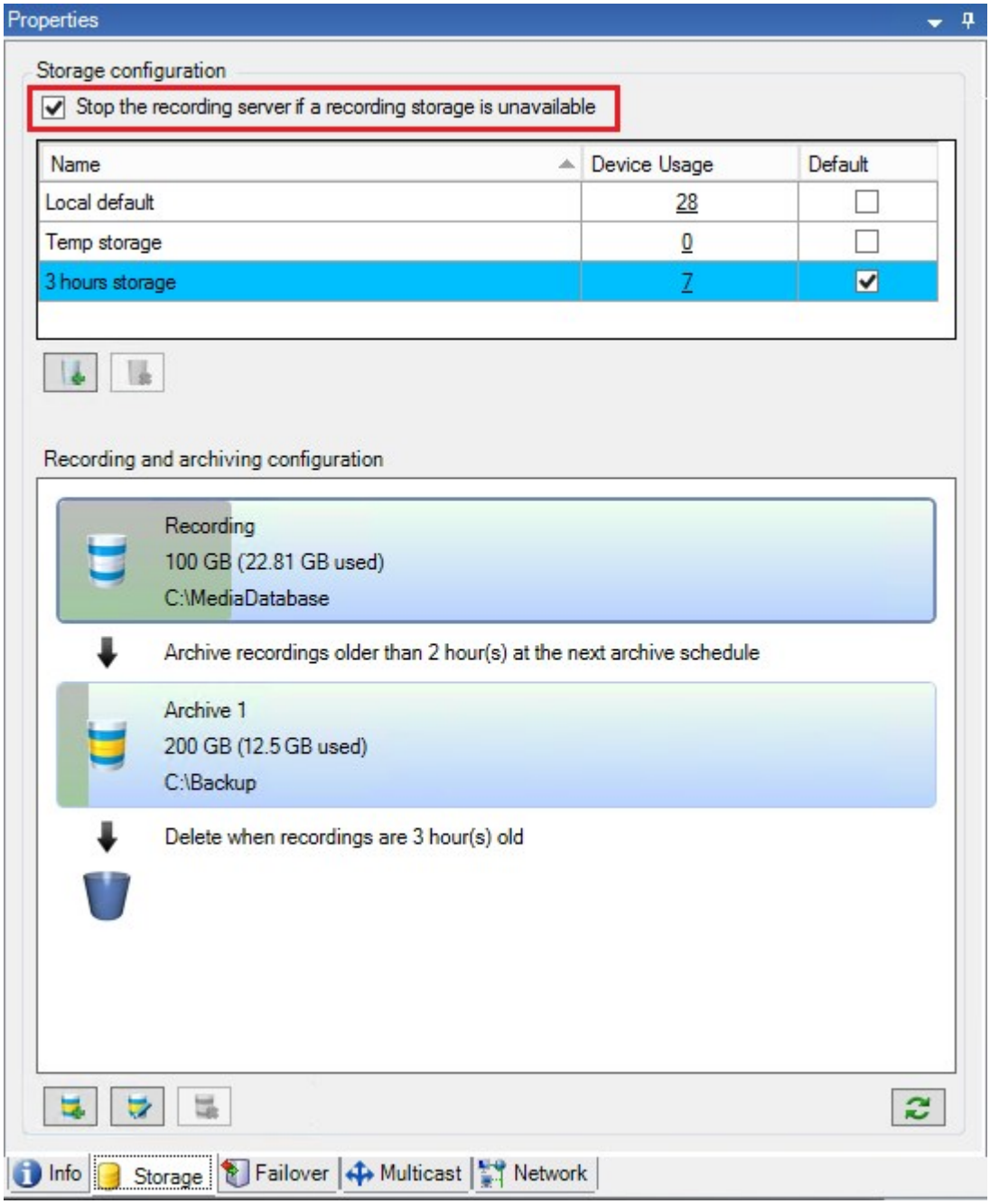
Beispiel: Diese Speicher (Abbildung links) weisen eine Speicherzeit von 4 Tagen, das folgende Archiv (Abbildung rechts) eine Speicherzeit von 10 Tagen auf. Die Archivierung wurde so konfiguriert, dass sie jeden Tag um 10:30 Uhr stattfindet, sodass Archivierungen häufiger vorgenommen werden als die Speicherzeit lang ist.

Außerdem können Sie die Archivierung mithilfe von Regeln und Ereignissen steuern.

Geben Sie an, wie das System sich verhalten soll, wenn kein Speicherplatz für Aufzeichnungen verfügbar ist

Der Aufzeichnungsserver läuft standardmäßig weiter auch wenn der Speicher für die Aufzeichnungen nicht mehr zur Verfügung steht. Wenn Ihr System mit ausfallsicheren Aufzeichnungsservern konfiguriert wurde, können Sie bestimmen, dass der Aufzeichnungsserver nicht mehr ausgeführt werden soll, damit die ausfallsicheren Server übernehmen:

1. Gehen Sie auf dem jeweiligen Aufzeichnungsserver auf die Registerkarte **Speicher**.
2. Wählen Sie die Option **Aufzeichnungsserver anhalten, wenn kein Speicherplatz für Aufzeichnungen zur Verfügung steht** .



Einen neuen Speicher hinzufügen

Wenn Sie einen neuen Speicher hinzufügen, erstellen Sie stets einen Aufzeichnungsspeicher mit einer vordefinierten Aufzeichnungsdatenbank namens **Aufzeichnung**. Sie können die Datenbank nicht umbenennen. Neben der Aufzeichnungsdatenbank kann ein Speicher eine Reihe verschiedener Archive beinhalten.

1. Um einem ausgewählten Aufzeichnungsserver einen zusätzlichen Speicher hinzuzufügen, klicken Sie auf die Schaltfläche  unter der Liste **Speicherkonfiguration**. Das Dialogfeld **Speicher- und Aufzeichnungseinstellungen** wird angezeigt.
2. Geben Sie die relevanten Einstellungen an (siehe Speicher- und Aufzeichnungseinstellungen).
3. Klicken Sie auf **OK**.

Bei Bedarf können Sie in Ihrem neuen Speicher Archive erstellen.

Erstellen eines Archivs in einem Speicher

Ein Speicher hat kein Standardarchiv; Sie können jedoch je nach Bedarf Archive erstellen.

1. Wählen Sie den gewünschten Speicher in der Liste **Aufzeichnungs- und Archivierungskonfiguration** aus.
2. Klicken Sie auf die Schaltfläche  unter der Liste **Aufzeichnungs- und Archivierungskonfiguration**.
3. Nehmen Sie im Dialogfeld **Archiveinstellungen** die erforderlichen Einstellungen vor (siehe Eigenschaften der Archiveinstellungen).
4. Klicken Sie auf **OK**.

Anbinden eines Geräts oder eine Gruppe von Geräten an einen Speicher

Sobald ein Speicher für einen Aufzeichnungsserver konfiguriert wurde, können Sie ihn für einzelne Geräte wie Kameras, Mikrofone oder Lautsprecher bzw. eine Gruppe von Geräten aktivieren. Außerdem können Sie festlegen, welche Speicherbereiche eines Aufzeichnungsservers Sie für das bestimmte Gerät oder die Gruppe verwenden möchten.

1. Erweitern Sie **Geräte**, und wählen Sie je nach Bedarf **Kameras**, **Mikrofone** oder **Lautsprecher** aus.
2. Wählen Sie das Gerät oder eine Gerätegruppe aus.
3. Wählen Sie die Registerkarte **Aufzeichnung**.
4. Wählen Sie im Bereich **Speicher** die Option **Auswählen**.
5. Wählen Sie im angezeigten Dialogfeld die Datenbank aus, in der die Aufzeichnungen des Geräts gespeichert werden sollen, und klicken Sie auf **OK**.
6. Klicken Sie in der Symbolleiste auf **Speichern**.

Wenn Sie auf der Registerkarte „Speicher“ des Aufzeichnungsservers auf die Gerätenutzungszahl klicken, ist das Gerät im angezeigten Nachrichtenbericht sichtbar.

Bearbeiten der Einstellungen für einen ausgewählten Speicher oder ein ausgewähltes Archiv

1. Wählen Sie zur Bearbeitung eines Speichers dessen Aufzeichnungsdatenbank in der Liste **Aufzeichnungs- und Archivierungskonfiguration** aus. Wählen Sie die Archivdatenbank aus, um ein Archiv zu bearbeiten.
2. Klicken Sie auf die Schaltfläche **Aufzeichnungsspeicher bearbeiten** unter  der Liste **Aufzeichnungs- und Archivierungskonfiguration**.
3. Bearbeiten Sie entweder eine Aufzeichnungsdatenbank oder ein Archiv.

Wenn Sie die maximale Größe einer Datenbank ändern, sorgt das System für eine automatische Archivierung aller Aufzeichnungen, die das neue Limit überschreiten. Je nach den Archivierungseinstellungen werden die Aufzeichnungen automatisch im nächsten Archiv archiviert bzw. gelöscht.

Digitale Signaturen für Export aktivieren

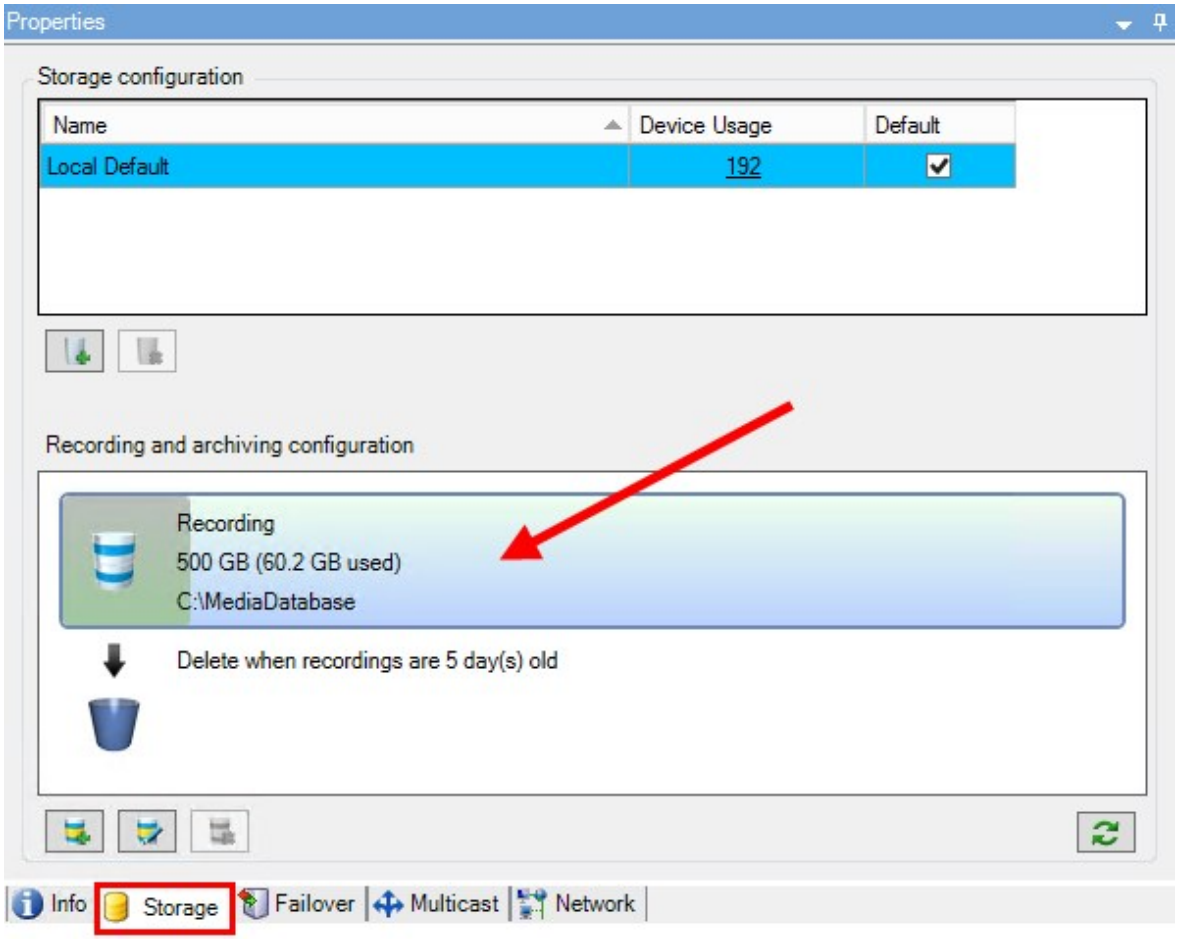
Verfügbare Funktionalität hängt vom verwendeten System ab. Weitere Informationen finden Sie unter https://www.milestonesys.com/solutions/platform/product-index/.

Sie können digitale Signatur für aufgezeichnete Videos aktivieren, sodass Client-Benutzer überprüfen können, dass das aufgezeichnete Video seit seiner Aufnahme nicht manipuliert wurde. Das Verifizieren der Echtzeit des Videos führt der Benutzer in XProtect Smart Client – Player durch, nachdem das Video exportiert wurde.

Im Dialogfeld **Exportieren** in XProtect Smart Client muss außerdem Signatur aktiviert sein. Anderenfalls wird die Schaltfläche **Signaturen verifizieren** in XProtect Smart Client – Player nicht angezeigt.

1. Erweitern Sie im Bereich **Standort-Navigation** den Knoten **Server**.
2. Klicken Sie auf **Aufzeichnungsserver**.
3. Klicken Sie im Übersichtsfenster auf den Aufzeichnungsserver, für den Sie die Signatur aktivieren möchten.

4. Klicken Sie unten im Bereich **Eigenschaften** auf die Registerkarte **Speicher**.



5. Doppelklicken Sie im Bereich **Aufzeichnungs- und Archivierungskonfiguration** auf den horizontalen Balken, der die Aufzeichnungsdatenbank repräsentiert. Das Fenster **Speicher- und Aufzeichnungseinstellungen** wird geöffnet.
6. Aktivieren Sie das Kontrollkästchen **Signatur**.
7. Klicken Sie auf **OK**.

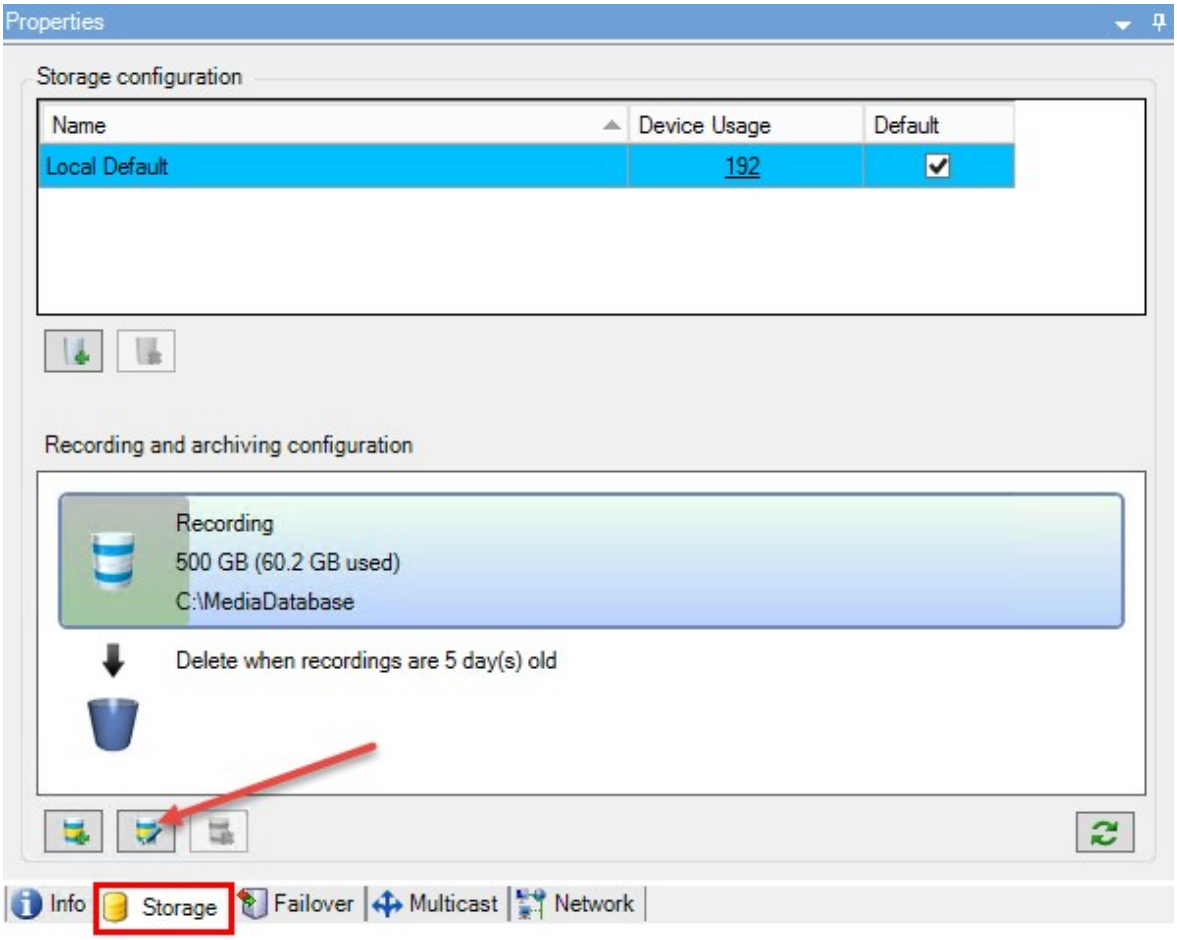
Verschlüsseln Sie Ihre Aufzeichnungen

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

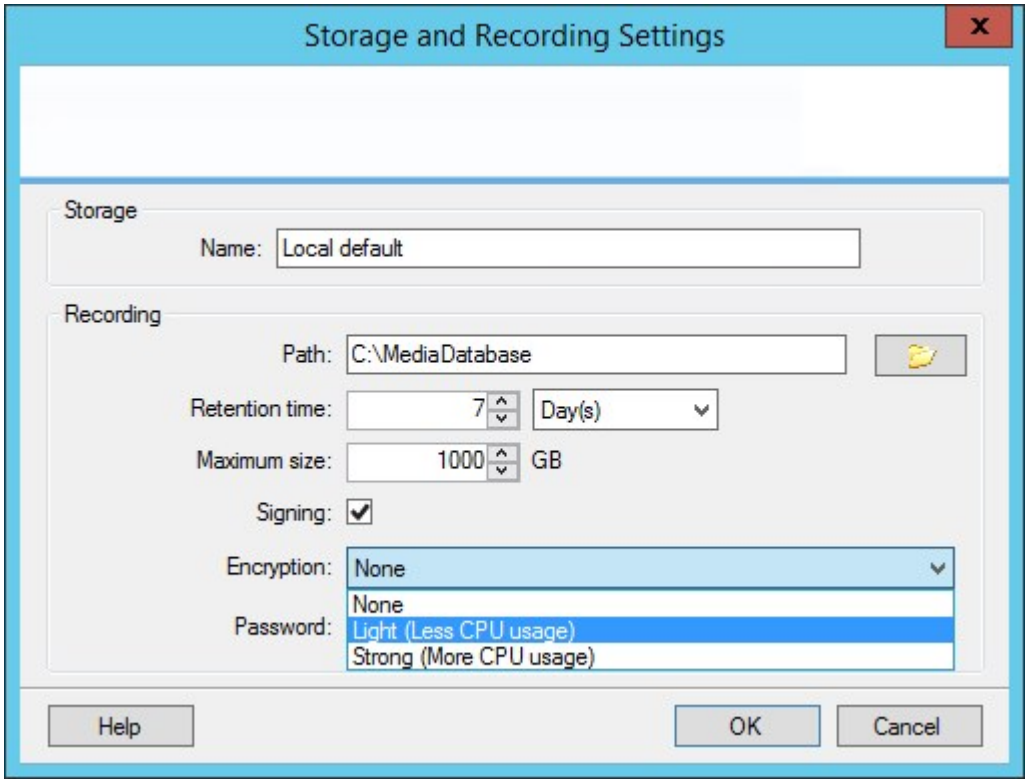
Sie können Ihre Aufzeichnungen sichern, indem Sie im Speicher und in den Archiven Ihres Aufzeichnungsservers die Verschlüsselung aktivieren. Sie können zwischen leichter und starker Verschlüsselung wählen. Wenn Sie die Verschlüsselung aktivieren, müssen Sie auch ein Passwort angeben.

Die Aktivierung oder Änderung von Verschlüsselungseinstellungen oder Passwort kann zeitraubend sein, abhängig von der Größe der Datenbank und der Leistungsfähigkeit des Laufwerks. Sie können die Fortschritte unter **Laufende Aufgaben** verfolgen.
Stoppen Sie den Aufzeichnungsserver nicht, während diese Aufgabe läuft.

1. Klicken Sie auf die Schaltfläche **Aufzeichnungsspeicher bearbeiten** unter der Liste **Konfiguration der Aufzeichnung und Archivierung**.



2. Geben Sie in dem eingeblendeten Dialogfeld das Verschlüsselungsniveau an.



3. Sie werden automatisch zum Dialogfeld **Passwort einrichten** geleitet. Geben Sie ein Passwort ein und klicken Sie auf **OK**.

Sichern archivierter Aufzeichnungen

Viele Unternehmen wollen Aufzeichnungen mithilfe von Bandlaufwerken oder ähnlichen Medien sichern. Wie Sie das genau machen, hängt von den individuellen Anforderungen und den im Unternehmen verwendeten Sicherungsmedien ab. Berücksichtigen Sie jedoch folgende Hinweise:

Sichern von Archiven anstelle von Kameradatenbanken

Erstellen Sie Sicherungen stets anhand des Inhalts von Archiven, nicht anhand der einzelnen Kameradatenbanken. Wenn Sie Sicherungen auf Grundlage des Inhalts einzelner Kameradatenbanken erzeugen, können Freigabeverletzungen und andere Fehlfunktionen auftreten.

Sorgen Sie bei der Planung von Sicherungen dafür, dass sich der Sicherungsauftrag nicht mit den festgelegten Archivierungszeiten überschneidet. Um die Archiv-Zeitpläne der einzelnen Aufzeichnungsserver in jedem der Speicherbereiche eines Aufzeichnungsservers anzuzeigen, rufen Sie die Registerkarte „Speicher“ auf.

Kennenlernen der Archivstruktur für gezielte Sicherungen

Bei der Archivierung von Aufzeichnungen speichern Sie diese in einer bestimmten Struktur des Archivs, die verschiedene Unterverzeichnisse umfasst.

Bei der gesamten regulären Nutzung Ihres Systems ist die Struktur mit Unterverzeichnissen für die Benutzer des Systems vollkommen transparent, wenn sie Aufzeichnungen mit XProtect Smart Client durchsuchen. Dies gilt sowohl für archivierte als auch für nicht archivierte Aufzeichnungen. Es ist wichtig, die Unterverzeichnis-Struktur (siehe Archivstruktur (Erklärung) zu kennen, wenn Sie Ihre archivierten Aufzeichnungen sichern möchten (siehe Sicherung und Wiederherstellung einer Systemkonfiguration auf Seite 494).

Archivstruktur (Erklärung)

Bei der Archivierung von Aufzeichnungen speichern Sie diese in einer bestimmten Struktur des Archivs, die verschiedene Unterverzeichnisse umfasst.

> Bei der gesamten regulären Nutzung Ihres Systems ist die Struktur mit Unterverzeichnissen für die Benutzer des Systems vollkommen transparent, wenn sie sämtliche Aufzeichnungen mit dem XProtect Smart Client durchsuchen. Dabei ist es egal, ob die Aufzeichnungen archiviert sind oder nicht. Wenn Sie Ihre archivierten Aufzeichnungen effektiv sichern möchten, ist es wichtig, dass Sie die Struktur mit Unterverzeichnissen gut kennen.

In jedem der Archivverzeichnisse des Aufzeichnungsservers erstellt das System automatisch separate Unterverzeichnisse. Diese Unterverzeichnisse werden nach dem Namen des Geräts und der Archivdatenbank benannt.

Da Sie Aufzeichnungen aus verschiedenen Kameras im gleichen Archiv speichern können und die Archivierung für die einzelnen Kameras wahrscheinlich in regelmäßigen Abständen vorgenommen wird, werden automatisch Unterverzeichnisse hinzugefügt.

Diese Unterverzeichnisse stehen für je eine Stunde Aufzeichnungen. Dank dieser stundenweisen Aufteilung werden nur relativ kleine Teile von Daten in einem Archiv verschoben, wenn Sie die zulässige Maximalgröße des Archivs erreichen.

Die Unterverzeichnisse werden nach dem Gerät benannt, gefolgt von einem Hinweis darauf, woher die Aufzeichnungen stammen (lokaler Speicher oder SMTP), **plus** Datum und Uhrzeit des aktuellsten Datensatzes in der Datenbank, der im Unterverzeichnis enthalten ist.
Namensstruktur

```
...[Speicherpfad]\[Speichername]\[Gerätename] – plus Datum und Uhrzeit der letzten Aufzeichnung]\
```

Wenn vom lokalen Speicher:

```
...[Speicherpfad]\[Speichername]\[Gerätename] (Edge) – plus Datum und Uhrzeit der letzten Aufzeichnung]\
```

Falls via SMTP:

```
...[Speicherpfad]\[Speichername]\[Gerätename] (SMTP) - plus Datum und Uhrzeit der
letzten Aufzeichnung]\
```

Praktisches Beispiel

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

Unterverzeichnisse

Außerdem werden automatisch weitere Unterverzeichnisse hinzugefügt. Zahl und Art der Unterverzeichnisse hängen von der Art der jeweiligen Aufzeichnungen ab. So werden zum Beispiel separate Unterverzeichnisse hinzugefügt, wenn Aufzeichnungen technisch in Sequenzen aufgeteilt werden. Dies kommt häufig vor, wenn Sie zur Auslösung von Aufzeichnungen eine Bewegungserkennung nutzen.

- **Medien**: Dieser Ordner enthält die tatsächlichen Medien, bei denen es sich um entweder Video- oder Audioinhalte handelt (nicht aber beides)
- **MotionLevel**: Dieser Ordner enthält Raster mit Bewegungsraten, die aus den Videodaten mit unserem Bewegungserkennungsalgorithmus erstellt wurden. Auf Grundlage dieser Daten kann die Smart Search-Funktion in XProtect Smart Client extrem schnelle Suchen durchführen.
- **Bewegung**: In diesem Ordner werden BewegungsSequenzen gespeichert. Eine BewegungsSequenz ist ein zeitlicher Abschnitt, in dem eine Bewegung in den Videodaten erkannt wurde. Diese Informationen werden zum Beispiel in der Zeitachse in XProtect Smart Client verwendet
- **Aufzeichnung**: In diesem Ordner werden AufzeichnungsSequenzen gespeichert. Eine AufzeichnungsSequenz ist ein Zeitintervall, für das es kohärente Aufzeichnungen mit Mediendaten gibt. Diese Informationen werden zum Beispiel zum Zeichnen der Zeitachse in XProtect Smart Client verwendet
- **Signatur**: Dieser Ordner enthält die für die Mediendaten (im Medienordner) erstellten Signaturen. Mit diesen Informationen können Sie sicherstellen, dass die Mediendaten seit ihrer Aufzeichnung nicht manipuliert wurden.

Falls Sie Ihre Archive sichern möchten, können Sie Sicherungen gezielt vornehmen, wenn Sie die Grundlagen der Struktur mit Unterverzeichnissen gut kennen.

Sicherungsbeispiele

Wenn Sie den Inhalt eines gesamten Archivs sichern möchten, sichern Sie das entsprechende Archivverzeichnis mit all seinen Inhalten. Zum Beispiel alles unterhalb von:

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

Um die Aufzeichnungen einer bestimmten Kamera aus einem bestimmten Zeitraum zu sichern, sichern Sie ausschließlich die entsprechenden Unterverzeichnisse. Zum Beispiel alles unterhalb von:

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

Löschen eines Archivs aus einem Speicher

1. Wählen Sie das gewünschte Archiv in der Liste **Aufzeichnungs- und Archivierungskonfiguration** aus.

   Sie können lediglich das letzte Archiv in der Liste löschen. Das Archiv muss nicht leer sein.

2. Klicken Sie auf die Schaltfläche  unter der Liste **Aufzeichnungs- und Archivierungskonfiguration**.
3. Klicken Sie auf **Ja**.

   Wenn das Archiv nicht verfügbar ist, z.B. offline, müssen Sie zunächst die Verbindung wiederherstellen, bevor Sie das Archiv löschen können.

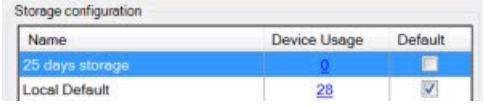
Löschen eines Speichers

Sie können den/die Standardspeicher, den/die Geräte als Aufzeichnungsspeicher für Live-Aufzeichnungen verwenden, nicht löschen.
Dies bedeutet, dass Sie eventuell Geräte und alle noch nicht archivierten Aufzeichnungen an einen anderen Speicher verschieben müssen (siehe Hardware verschieben auf Seite 506), bevor Sie den Speicher löschen.

1. Zur Anzeige einer Liste der Geräte, die den Speicher verwenden, klicken Sie auf die Gerätenutzungszahl.

   Wenn der Speicher Daten von Geräten aufweist, die auf einen anderen Aufzeichnungsserver verschoben wurden, wird eine Warnung angezeigt. Klicken Sie auf den Link, um die Liste mit Geräten anzuzeigen.

2. Führen Sie die Schritte in Verschieben nicht archivierter Aufzeichnungen von einem Speicher in einen anderen aus.
3. Fahren Sie fort, bis Sie alle Geräte verschoben haben.
4. Wählen Sie den Speicher aus, den Sie löschen möchten.



5. Klicken Sie auf die Schaltfläche  unter der Liste **Speicherkonfiguration**.
6. Klicken Sie auf **Ja**.

Verschieben nicht archivierter Aufzeichnungen von einem Speicher in einen anderen

Auf der Registerkarte **Aufzeichnung** des Geräts können Sie Aufzeichnungen von einer Live-Aufzeichnungsdatenbank in eine andere verschieben.

1. Wählen Sie den Gerätetyp aus. Wählen Sie im Fenster **Übersicht** das gewünschte Gerät aus.
2. Klicken Sie auf die Registerkarte **Aufzeichnung**. Klicken Sie oben im Bereich **Speicher** auf **Auswählen**.
3. Wählen Sie die Datenbank im Dialogfeld **Speicher auswählen** aus.
4. Klicken Sie auf **OK**.
5. Wählen Sie im Dialogfeld **Aufzeichnungsaktion**, ob Sie bereits vorhandene – aber noch **nicht archivierte** – Aufzeichnungen in den neuen Speicher verschieben bzw. löschen möchten.
6. Klicken Sie auf **OK**.

Speicher- und Aufzeichnungseinstellungen (Eigenschaften)

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

Geben Sie im Dialogfeld **Speicher- und Aufzeichnungseinstellungen** Folgendes an:

Name	Beschreibung
Name	Benennen Sie den Speicher um, falls erforderlich. Die Namen müssen eindeutig sein.
Pfad	Geben Sie den Pfad zu dem Verzeichnis an, in dem Sie Aufzeichnungen in diesem Speicher speichern. Der Speicher muss sich nicht unbedingt auf dem Aufzeichnungsserver-Computer befinden. Wenn das Verzeichnis nicht vorhanden ist, können Sie es erstellen. Netzwerklaufwerke müssen mit dem UNC-Format (Universal Naming Convention) benannt werden, beispielsweise: *server**volume**directory*\.
Speicherzeit	Geben Sie an, wie lange Aufzeichnungen im Archiv bleiben sollen, bevor sie gelöscht oder ins nächste Archiv verschoben werden (je nach Archiveinstellungen). Die Speicherzeit muss immer länger als die Speicherzeit des bisherigen Archivs oder

Name	Beschreibung
	der Standard-Aufzeichnungsdatenbank sein. Der Grund dafür ist, dass die Zahl der Speichertage, die für ein Archiv angegeben sind, alle Speicherzeiten beinhaltet, die früher im Prozess angegeben wurden.
Maximale Größe	Wählen Sie die maximale Gigabyte-Anzahl an Aufzeichnungsdaten aus, die in der Aufzeichnungsdatenbank gespeichert werden sollen. Aufzeichnungsdaten, die die angegebene Gigabyte-Anzahl überschreiten, werden automatisch ins erste Archiv auf der Liste verschoben – sofern eines angegeben ist – oder gelöscht. Wenn weniger als 5 GB Speicherplatz frei sind, archiviert das System immer die ältesten Daten in einer Datenbank bzw. löscht diese, wenn kein nächstes Archiv angegeben ist. Wenn weniger als 1 GB frei ist, werden die Daten gelöscht. Eine Datenbank erfordert 250 MB an freiem Speicherplatz. Wenn dieser Grenzwert erreicht wird (wenn Daten nicht schnell genug gelöscht werden), werden erst dann wieder Daten in die Datenbank geschrieben, wenn Sie genügend Platz freigegeben haben. Die tatsächliche Maximalgröße Ihrer Datenbank entspricht der Anzahl der angegebenen Gigabyte minus 5 GB.
Wird signiert	Ermöglicht eine digitale Signatur für die Aufzeichnungen. Das heißt beispielsweise, dass das System bestätigt, dass das exportierte Video nicht verändert oder bei der Wiedergabe manipuliert wurde. Das System verwendet den SHA-2-Algorithmus für digitale Signaturen.
Verschlüsselung	Wählen Sie den Verschlüsselungsgrad der Aufnahmen aus: • Keine • Schwach (weniger CPU-Auslastung) • Stark (Höhere CPU-Auslastung) Das System verwendet den AES-256-Algorithmus zur Verschlüsselung. Bei Auswahl von **Schwach** wird ein Teil der Aufzeichnung verschlüsselt. Bei Auswahl von **Stark** wird die gesamte Aufzeichnung verschlüsselt. Wenn Sie Verschlüsselung aktivieren, müssen Sie nachfolgend auch ein Passwort

Name	Beschreibung
	angeben.
Passwort	Geben Sie ein Passwort für die Benutzer an, die verschlüsselte Daten anzeigen dürfen. Milestone empfiehlt die Nutzung sicherer Passwörter. Sichere Passwörter enthalten keine Wörter, die in Wörterbüchern zu finden sind oder Bestandteil des Namens des Benutzers sind. Sie umfassen acht oder mehr alphanumerische Zeichen, Groß- und Kleinbuchstaben und Sonderzeichen.

Eigenschaften der Archiveinstellungen

Geben Sie im Dialogfeld **Archiveinstellungen** Folgendes an:

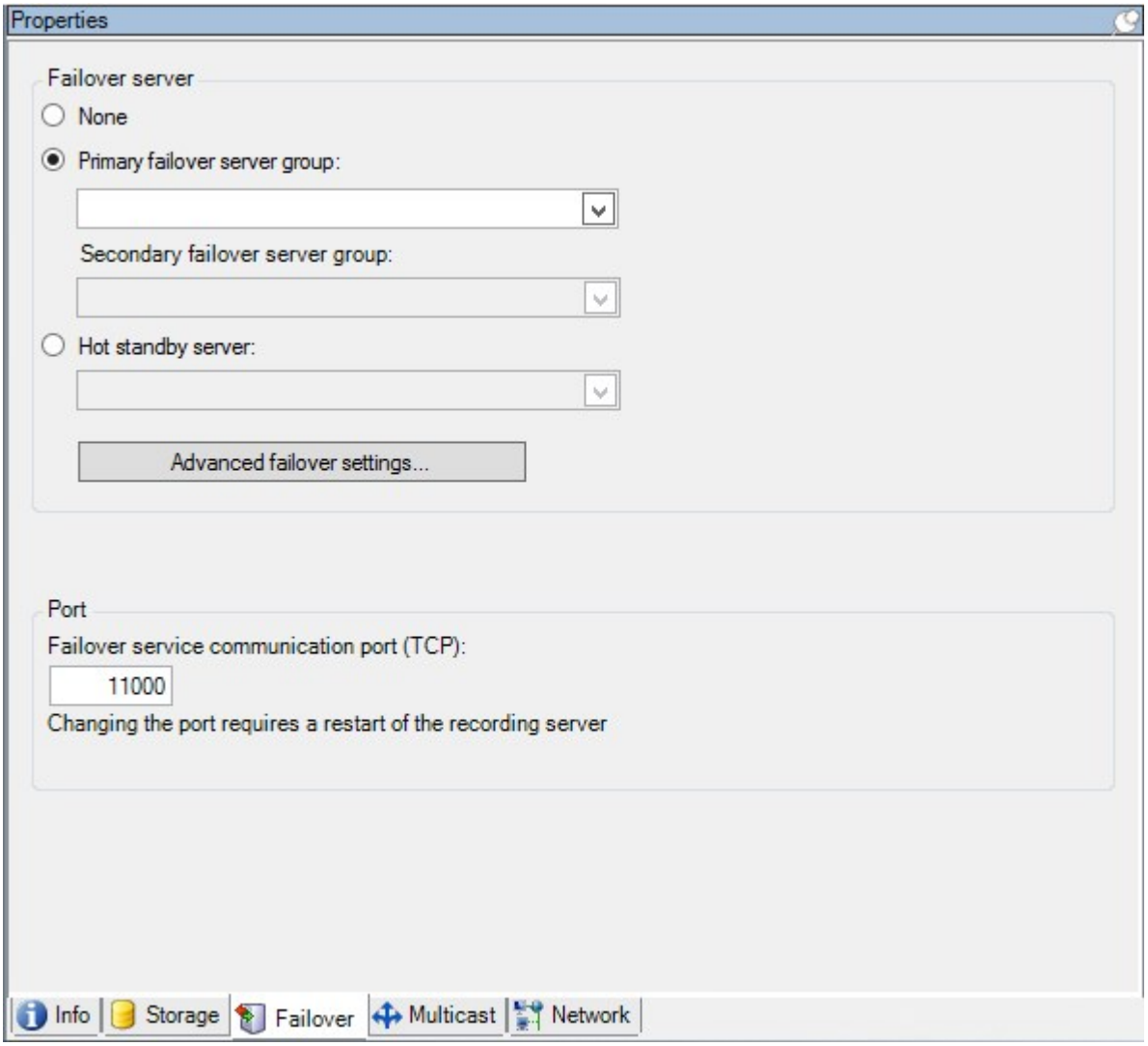
Name	Beschreibung
Name	Benennen Sie den Speicher um, falls erforderlich. Die Namen müssen eindeutig sein.
Pfad	Geben Sie den Pfad zu dem Verzeichnis an, in dem Sie Aufzeichnungen in diesem Speicher speichern. Der Speicher muss sich nicht unbedingt auf dem Aufzeichnungsserver-Computer befinden. Wenn das Verzeichnis nicht vorhanden ist, können Sie es erstellen. Netzwerklaufwerke müssen mit dem UNC-Format (Universal Naming Convention) benannt werden, beispielsweise: *server**volume**directory*\.
Speicherzeit	Geben Sie an, wie lange Aufzeichnungen im Archiv bleiben sollen, bevor sie gelöscht oder ins nächste Archiv verschoben werden (je nach Archiveinstellungen). Die Speicherzeit muss immer länger als die Speicherzeit des bisherigen Archivs oder der Standard-Aufzeichnungsdatenbank sein. Der Grund dafür ist, dass die Zahl der Speichertage, die für ein Archiv angegeben sind, alle Speicherzeiten beinhaltet, die früher im Prozess angegeben wurden.
Maximale	Wählen Sie die maximale Gigabyte-Anzahl an Aufzeichnungsdaten aus, die in der

Name	Beschreibung
Größe	Aufzeichnungsdatenbank gespeichert werden sollen. Aufzeichnungsdaten, die die angegebene Gigabyte-Anzahl überschreiten, werden automatisch ins erste Archiv auf der Liste verschoben – sofern eines angegeben ist – oder gelöscht. ⚠ Wenn weniger als 5 GB Speicherplatz frei sind, archiviert das System immer die ältesten Daten in einer Datenbank bzw. löscht diese, wenn kein nächstes Archiv angegeben ist. Wenn weniger als 1 GB frei ist, werden die Daten gelöscht. Eine Datenbank erfordert 250 MB an freiem Speicherplatz. Wenn dieser Grenzwert erreicht wird (wenn Daten nicht schnell genug gelöscht werden), werden erst dann wieder Daten in die Datenbank geschrieben, wenn Sie genügend Platz freigegeben haben. Die tatsächliche Maximalgröße Ihrer Datenbank entspricht der Anzahl der angegebenen Gigabyte minus 5 GB.
Zeitplan	Legen Sie einen Archiv-Zeitplan fest, der die zeitlichen Abstände enthält, in denen der Archivierungsprozess gestartet wird. Sie können sehr häufig (im Allgemeinen einmal pro Stunde an 365 Tagen im Jahr) oder sehr selten (zum Beispiel an jedem ersten Montag alle 36 Monate) archivieren.
Bildrate reduzieren	Wenn Sie bei der Archivierung die Bildrate verringern möchten, wählen Sie die Option **Bildrate reduzieren** und legen Sie die Bilder pro Sekunde (FPS) fest. Durch eine Reduzierung der Bildraten mit einem bestimmten FPS-Wert nehmen Ihre Aufzeichnungen im Archiv weniger Platz in Anspruch. Gleichzeitig verringert sich jedoch auch die Bildqualität im Archiv. MPEG-4/H.264/H.265 sorgt für eine automatische Minimierung auf Keyframes. 0,1 = 1 Bild pro 10 Sekunden.

Registerkarte „Failover“ (Aufzeichnungsserver)

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

Wenn Ihr Unternehmen Failover-Aufzeichnungsserver nutzt, können Sie die Registerkarte **Failover** verwenden, um Aufzeichnungsservern Failover-Server zuzuweisen. Siehe Eigenschaften der Registerkarte „Failover“.



Details zu Failover-Aufzeichnungsservern, Installation und Einstellungen, Failover-Gruppen und ihren Einstellungen finden Sie unter Failover-Aufzeichnungsserver (Erklärung) auf Seite 184.

Zuweisen von Failover-Aufzeichnungsservern

Auf der Registerkarte **Failover** eines Aufzeichnungsservers können Sie zwischen drei Failover-Einrichtungsarten wählen:

- Keine Failover-Einrichtung
- Einrichtung primärer/sekundärer Failover-Gruppen (Cold-Standby)
- Eine Hot-Standby-Einrichtung

Wenn Sie sich für **b** und **c** entscheiden, müssen Sie den gewünschten Server/die gewünschten Gruppen auswählen. Bei **b** können Sie außerdem eine sekundäre Failover-Gruppe einrichten. Sollte der Aufzeichnungsserver nicht mehr verfügbar sein, übernimmt ein Failover-Aufzeichnungsserver aus der primären Failover-Gruppe. Wenn Sie zudem eine sekundäre Failover-Gruppe ausgewählt haben, übernimmt ein Failover-Aufzeichnungsserver aus der sekundären Gruppe in dem Fall, dass alle Failover-Aufzeichnungsserver in der primären Failover-Gruppe ausgelastet sind. So riskieren Sie nur für den seltenen Fall, dass alle Failover-Aufzeichnungsserver in der primären als auch in der sekundären Failover-Gruppe ausgelastet sind, dass es keine Failover-Lösung gibt.

1. Wählen Sie im Bereich **Standort-Navigation** die Optionen **Server** > **Aufzeichnungsserver**. Daraufhin wird eine Liste mit Aufzeichnungsservern geöffnet.
2. Wählen Sie im Fenster **Übersicht** den gewünschten Aufzeichnungsserver aus, und öffnen Sie die Registerkarte **Failover**.
3. Wählen Sie zur Auswahl der Failover-Einrichtungsart zwischen folgenden Optionen aus:
   - **Keine**
   - **Primäre Failover-Servergruppe/Sekundäre Failover-Servergruppe**
   - **Hot-Standby-Server**

   Sie können eine Failover-Gruppe nicht als primäre und auch als sekundäre Failover-Gruppe festlegen und ebenso nicht reguläre Failover-Server, die bereits Teil einer Failover-Gruppe sind, als Hot-Standby-Server auswählen.
4. Klicken Sie als Nächstes auf **Erweiterte Failover-Einstellungen**. Daraufhin öffnet sich das Fenster **Erweiterte Failover-Einstellungen**, in dem alle mit dem ausgewählten Aufzeichnungsserver verbundenen Geräte aufgelistet werden. Wenn Sie die Option **Keine** gewählt haben, sind außerdem die erweiterten Failover-Einstellungen verfügbar. Das System speichert alle Einstellungen für spätere Failover-Einrichtungen.
5. Um die Stufe der Failover-Unterstützung zu ermitteln, wählen Sie für jedes Gerät in der Liste **Vollständiger Support**, **Nur live** oder **Deaktiviert** aus. Klicken Sie auf **OK**.
6. Bearbeiten Sie die Portnummer, wenn erforderlich, im Feld **Kommunikationsport des Failover-Dienstes (TCP)**.

Wenn Sie Failover-Support aktivieren und der Aufzeichnungsserver so konfiguriert ist, dass er weiterläuft, wenn kein Aufzeichnungsspeicher verfügbar ist, übernimmt der Failover-Aufzeichnungsserver nicht. Damit der Failover-Support funktioniert, müssen Sie auf der Registerkarte **Speicher** die Option **Aufzeichnungsserver stoppen, wenn ein Aufzeichnungsspeicher nicht verfügbar ist** auswählen.

Eigenschaften der Registerkarte „Failover“

Name	Beschreibung
Keine	Wählen Sie eine Einrichtung ohne Failover-Aufzeichnungsserver aus.
Primäre Failover-Servergruppe/Sekundäre Failover-Servergruppe	Wählen Sie eine reguläre Failover-Einrichtung mit einer primären und möglicherweise einer zweiten Failover-Servergruppe aus.
Hot-Standby-Server	Wählen Sie eine Hot-Standby-Einrichtung mit einem dedizierten Aufzeichnungsserver als Hot-Standby-Server aus.
Erweiterte Failover-Einstellungen	Öffnet das Fenster **Erweiterte Failover-Einstellungen**: • **Vollständiger Support**: Aktiviert vollständige Failover-Unterstützung für das Gerät • **Nur live**: Aktiviert Failover-Unterstützung ausschließlich für Live-Streams auf dem Gerät • **Deaktiviert**: Deaktiviert Failover-Unterstützung für das Gerät
Kommunikationsport des Failover-Dienstes (TCP)	Die standardmäßige Portnummer lautet 11000. Dieser Port wird für die Kommunikation zwischen Aufzeichnungsservern und Failover-Aufzeichnungsservern verwendet. Wenn Sie den Port ändern, **muss** der Aufzeichnungsserver ausgeführt werden und **muss** mit dem Management-Server verbunden sein.

Registerkarte „Multicast“ (Aufzeichnungsserver)

Ihr System unterstützt Multicasting von Live-Streams über Ihre Aufzeichnungsserver. Falls mehrere XProtect Smart Client-Benutzer das Live-Video von derselben Kamera sehen möchten, können mit Hilfe von Multicast wertvolle Systemressourcen eingespart werden. Multicast ist besonders bei der Nutzung der Matrix Funktionalität von großer Bedeutung, da hierbei mehrere Clients Live-Videodaten von derselben Kamera erfordern.

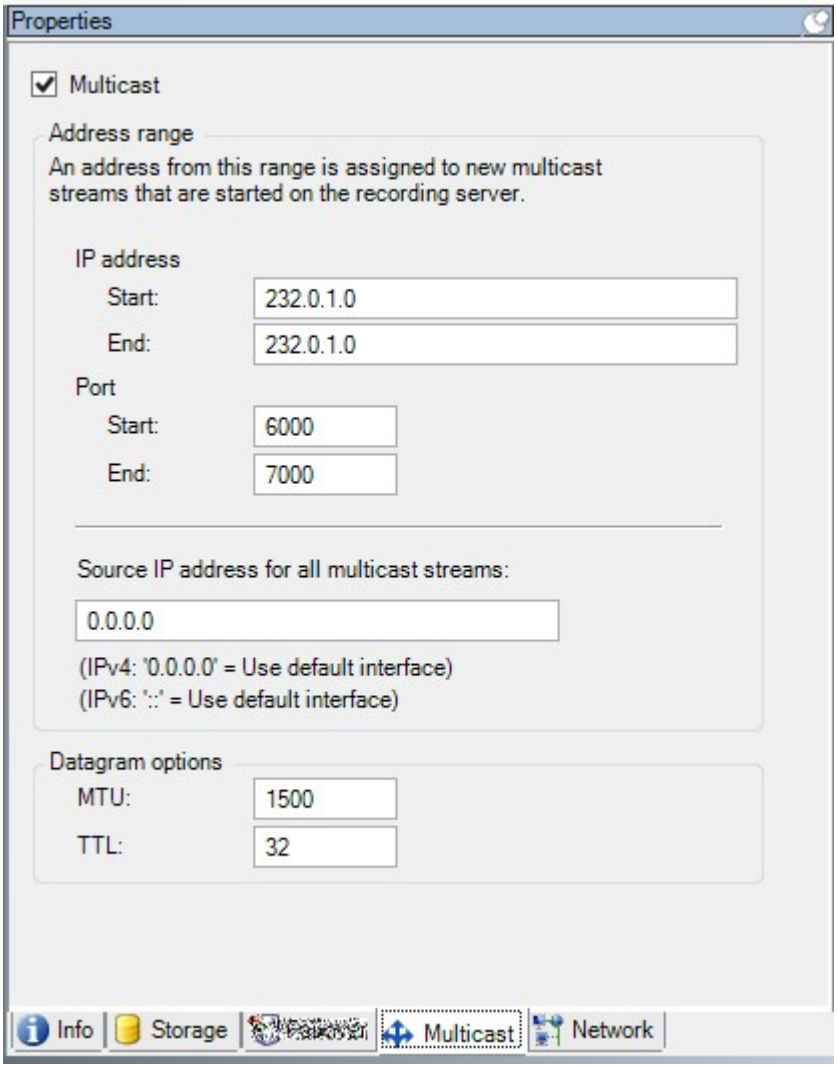
Multicast ist nur möglich für Live-Streams, nicht jedoch für aufgezeichnete Video-/Audio-Dateien.

Wenn ein Aufzeichnungsserver über mehr als eine Netzwerkkarte verfügt, kann Multicast nur auf einer von ihnen aktiviert werden. Im Management Client können Sie festlegen,

welche Karte Sie verwenden möchten.

Wenn Sie Failover-Server verwenden, müssen Sie auch die IP-Adresse der Netzwerkkarte auf den Failover-Servern bestimmen (siehe Registerkarte Multicast (Failover-Server) auf Seite 191).

Eine erfolgreiche Implementierung von Multicasting setzt zudem voraus, dass Sie Ihre Netzwerkausrüstung so einrichten, dass Multicast-Datenpakete ausschließlich an die gewünschte Gruppe von Empfängern übertragen werden. Wenn nicht, kann es vorkommen, dass sich Multicasting nicht von Broadcasting unterscheidet, wodurch sich die Geschwindigkeit im Netzwerk möglicherweise deutlich reduziert.



Multicasting (Erklärung)

Bei der herkömmlichen Netzwerkkommunikation wird jedes Datenpaket von genau einem Absender an genau einen Empfänger gesendet. Dieser Prozess wird als „Unicasting" bezeichnet. Mit Multicasting können Sie jedoch ein Datenpaket (von einem Server) an mehrere Empfänger (Clients) in einer Gruppe senden. Multicasting kann dabei helfen, den Bandbreitenbedarf zu reduzieren.

- Wenn Sie **Unicasting** nutzen, muss die Quelle einen Datenstream pro Empfänger übertragen
- Bei Verwendung von **Multicasting** wird für jedes Netzwerksegment hingegen nur ein Datenstream benötigt

Beim hier beschriebenen Multicasting handelt es sich **nicht** um ein Streaming von Videodaten von einer Kamera an Server, sondern von Servern an Clients.

Beim Multicasting arbeiten Sie mit einer definierten Gruppe von Empfängern, je nach Optionen wie IP-Adressbereichen, der Fähigkeit zum Aktivieren/Deaktivieren von Multicasts für einzelne Kameras, der Fähigkeit zum Festlegen der maximal akzeptablen Datenpaketgröße (MTU), der Maximalzahl an Routern, zwischen denen ein Datenpaket übertragen werden muss (TTL) usw.

Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet.

Multicasting sollte nicht mit **Broadcasting** verwechselt werden, bei dem Daten an alle gesendet werden, die mit dem Netzwerk verbunden sind, selbst wenn die Daten möglicherweise nicht für alle relevant sind:

Name	Beschreibung
Unicasting	Sendet Daten von genau einer Quelle an genau einen Empfänger.
Multicasting	Sendet Daten von einer einzelnen Quelle an verschiedene Empfänger in einer klar definierten Gruppe.
Broadcasting	Sendet Daten von einer einzelnen Datenquelle an alle im Netzwerk. Somit kann Broadcasting die Geschwindigkeit im Netzwerk deutlich reduzieren.

Aktivieren Sie Multicasting für den Recording-Server

Wenn Sie Multicasting verwenden möchten, muss Ihre Netzwerkinfrastruktur den IP-Multicasting-Standard IGMP (Internet Group Management Protocol) unterstützen.

- Aktivieren Sie auf der Registerkarte **Multicast** das Kontrollkästchen **Multicast**

Wenn auf einem oder mehr Servern bereits der gesamte IP-Adressbereich für Multicast genutzt wird, müssen Sie zunächst einige IP-Adressen für Multicast freigeben, bevor Sie Multicasting auf zusätzlichen Aufzeichnungsservern aktivieren können.

Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet.

Zuweisen eines IP-Adressbereichs

Legen Sie den Bereich fest, den Sie als Adressen für Multicast-Streams des ausgewählten Aufzeichnungsservers zuweisen möchten. Wenn Benutzer Multicast-Video von diesem Aufzeichnungsserver anzeigen, stellen die Clients Verbindungen mit diesen Adressen her.

Für jeden Multicast-Kamera-Feed müssen die IP-Adresse und die Port-Kombination eindeutig sein (Beispiel für IPv4: 232.0.1.0:6000). Sie können entweder eine IP-Adresse und viele Ports oder viele IP-Adressen und weniger Ports verwenden. Standardmäßig schlägt das System eine einzelne IP-Adresse und einen Bereich von 1.000 Ports vor; Sie können die Einstellungen jedoch bei Bedarf ändern.

IP-Adressen für Multicasting müssen sich im von IANA für dynamische Hostzuordnung definierten Bereich befinden. IANA ist die Organisation, die für die Überwachung der globalen Vergabe von IP-Adressen zuständig ist.

Name	Beschreibung
IP-Adresse	Geben Sie im Feld **Start** die erste IP-Adresse des gewünschten Bereichs an. Geben Sie dann im Feld **Ende** die letzte IP-Adresse des gewünschten Bereichs an.
Port	Geben Sie im Feld **Start** die erste Portnummer des gewünschten Bereichs an. Geben Sie dann im Feld **Ende** die letzte Portnummer des gewünschten Bereichs an.
Quell-IP-Adresse für alle Multicast-Streams	Sie können Multicast nur auf einer Netzwerkkarte aktivieren. Dieses Feld ist also relevant, wenn Ihr Aufzeichnungsserver über mehr als eine Netzwerkkarte verfügt oder eine Netzwerkkarte mit mehr als einer IP-Adresse aufweist. Wenn Sie die Standardschnittstelle des Aufzeichnungsservers verwenden möchten, belassen Sie den Wert im Feld bei 0.0.0.0 (IPv4) oder :: (IPv6). Wenn Sie eine andere Netzwerkkarte bzw. eine andere IP-Adresse auf der gleichen Netzwerkkarte nutzen möchten, geben Sie die IP-Adresse der gewünschten Schnittstelle an. • IPv4: 224.0.0.0 bis 239.255.255.255. • IPv6, der Bereich wird auf der Website von IANA (https://www.iana.org/) beschrieben.

Festlegen von Datagramm-Optionen

Legen Sie die Einstellungen für Datenpakete (Datagramme) fest, die über Multicasting übertragen werden sollen.

Name	Beschreibung
MTU	Maximale Übertragungseinheit, also die maximal zulässige physische Datenpaketgröße (gemessen in Byte). Nachrichten, die größer als der angegebene MTU-Wert sind, werden vor dem Senden in kleinere Pakete aufgeteilt. Der Standardwert lautet 1500; dies ist auch bei den meisten Windows-Computern und Ethernet-Netzwerken der Standardwert.
TTL	Gültigkeitsdauer (Time To Live), also die maximal zulässige Zahl an Hops, die ein Datenpaket zurücklegen darf, bevor es verworfen oder zurückgesendet wird. Ein Hop ist ein Punkt zwischen zwei Netzwerkgeräten (meist ein Router). Der Standardwert ist 128.

Aktivieren von Multicasting für einzelne Kameras

Multicasting funktioniert nur, wenn Sie die Option für die entsprechenden Kameras aktivieren:

1. Wählen Sie im Fenster **Übersicht** den Aufzeichnungsserver und die gewünschte Kamera aus.
2. Aktivieren Sie auf der Registerkarte **Client** das Kontrollkästchen **Live-Multicast**. Wiederholen Sie diesen Schritt für alle entsprechenden Kameras.

Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet.

Registerkarte „Netzwerk“ (Aufzeichnungsserver)

Die öffentliche IP-Adresse eines Aufzeichnungsservers legen Sie auf der Registerkarte **Netzwerk** fest.

Wozu dient eine öffentliche Adresse?

Wenn ein Zugriffs-Client wie XProtect Smart Client eine Verbindung mit einem Überwachungssystem herstellt, erfolgt ein Teil der anfänglichen Datenkommunikation (inkl. des Austauschs der Kontaktadressen) gemeinsam im Hintergrund. Dies geschieht automatisch und ist für Benutzer vollkommen transparent.

Clients können Verbindungen über das lokale Netzwerk oder das Internet herstellen. In beiden Fällen muss das Überwachungssystem dazu in der Lage sein, geeignete Adressen bereitzustellen, damit Clients auf Live-Videos und Videoaufzeichnungen der Aufzeichnungsserver zugreifen können:

- Wenn Clients eine lokale Verbindung herstellen, muss das Überwachungssystem mit lokalen Adressen und Portnummern antworten
- Wenn Clients eine Verbindung über das Internet herstellen, muss das Überwachungssystem mit der öffentlichen Adresse des Aufzeichnungsservers antworten. Dies ist die Adresse der Firewall oder des NAT-Routers (Network Address Translation) und oftmals auch eine andere Portnummer. Die Adresse und der Port können dann an die lokale Adresse und den lokalen Port des Servers weitergeleitet werden.

  Wenn Sie von außerhalb einer NAT-Firewall auf das Überwachungssystem zugreifen möchten, können Sie öffentliche Adressen und Port-Forwarding verwenden. So können Clients von außerhalb der Firewall ohne VPN-Verbindungen (Virtual Private Network) mit Aufzeichnungsservern herstellen. Jeder Aufzeichnungsserver lässt sich einem bestimmten Port zuordnen; dieser Port kann durch die Firewall an die interne IP-Adresse des Servers weitergeleitet werden

Festlegen von öffentlichen Adressen und Ports

1. Zum Aktivieren des öffentlichen Zugriffs wählen Sie das Kontrollkästchen **Öffentlichen Zugriff ermöglichen** aus.
2. Legen Sie die öffentliche Adresse des Aufzeichnungsservers fest. Geben Sie die Adresse der Firewall oder des NAT-Routers ein, damit Clients, die über das Internet auf das Überwachungssystem zugreifen, eine Verbindung zu den Aufzeichnungsservern herstellen können.
3. Geben Sie eine öffentliche Portnummer an. Es wird empfohlen, für die Firewall oder den NAT-Router andere Portnummern als für die Lokalen zu verwenden.

Wenn Sie einen öffentlichen Zugriff nutzen, konfigurieren Sie die Firewall oder den NAT-Router so, dass an die öffentliche Adresse gesendete Anfragen an die lokale Adresse und Ports von relevanten Aufzeichnungsservern weitergeleitet werden.

Zuweisen lokaler IP-Bereiche

Sie definieren eine Liste lokaler IP-Bereiche, deren Ursprung vom Überwachungssystem als lokales Netzwerk erkannt werden sollte:

- Klicken Sie auf der Registerkarte **Netzwerk** auf **Konfigurieren**

Site-Navigation: Server und Hardware: Failover-Server

Failover-Aufzeichnungsserver (Erklärung)

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

Ein Failover-Aufzeichnungsserver ist ein zusätzlicher Aufzeichnungsserver, der die Arbeit des eigentlichen Aufzeichnungsservers übernimmt, falls dieser nicht mehr verfügbar ist. Sie können einen Failover-Aufzeichnungsserver in zwei Modi konfigurieren, als **Cold-Standby-Server** oder als **Hot-Standby-Server**.

Die Installation eines Failover-Aufzeichnungsservers läuft wie bei Standard-Aufzeichnungsservern ab (siehe Installation neuer XProtect-Komponenten auf Seite 93). Sobald Sie Failover-Aufzeichnungsserver installiert haben, werden diese im Management Client angezeigt. Milestone empfiehlt die Installation aller Failover-Aufzeichnungsserver auf separaten Computern. Achten Sie darauf, dass sie Failover-Aufzeichnungsserver mit der korrekten IP-Adresse/dem korrekten Hostnamen des Management-Servers konfigurieren. Während des Installationsprozesses werden die Benutzerrechte für das Benutzerkonto, unter dem der ausfallsichere Serverdienst laufen soll, bereitgestellt. Dies sind:

- Start-/Stopp- Berechtigungen zu starten oder stoppen des ausfallsicheren Aufzeichnungsservers
- Lesende und schreibende Zutrittsberechtigung zum Lesen und Schreiben in der Datei RecorderConfig.xml

Wird für die Verschlüsselung ein Zertifikat ausgewählt, so muss der Administrator dem Benutzer auf dem ausgewählten Zertifikate-Privatschlüssel des Failover-Servers die Lesezugriffsberechtigung geben.

Wenn der Failover-Aufzeichnungsserver von einem Aufzeichnungsserver übernimmt, der eine Verschlüsselung verwendet, so empfiehlt Milestone, dass Sie den Failover-Aufzeichnungsserver ebenfalls dafür vorbereiten, dass er eine Verschlüsselung verwendet. Weitere Informationen finden Sie unter Vor dem Start der Installation auf Seite 59 und Installation neuer XProtect-Komponenten auf Seite 93.

Sie können bestimmen, welche Art von Failover-Unterstützung Sie auf Geräteebene möchten. Für jedes Gerät auf einem Aufzeichnungsserver können Sie vollständige, teilweise oder keine Failover-Unterstützung auswählen. So können Sie Ihren Failover-Ressourcen Prioritäten zuweisen und Failover beispielsweise nur für Video- und nicht für Audiokanäle einrichten oder Failover nur auf wichtigen Kameras haben.

Während ihr System im Failover-Modus ist, können Sie keine Hardware ersetzen oder umziehen, den Aufzeichnungsserver aktualisieren oder Gerätekonfigurationen ändern, wie zum Beispiel Speicherungseinstellungen oder Einstellungen für Videostreams.

Cold-Standby-Failover-Aufzeichnungsserver

Bei einem Cold-Standby-Failover-Aufzeichnungsserver gruppieren Sie mehrere Failover-Aufzeichnungsserver in einer Failover-Gruppe. Die gesamte Failover-Gruppe dient dem Zweck, mehrere vorab ausgewählte Aufzeichnungsserver abzulösen, wenn einer von ihnen nicht mehr verfügbar sein sollte. Sie können so viele Gruppen erstellen, wie Sie möchten (siehe Failover-Aufzeichnungsserver für Cold-Standby gruppieren (Erklärung)).

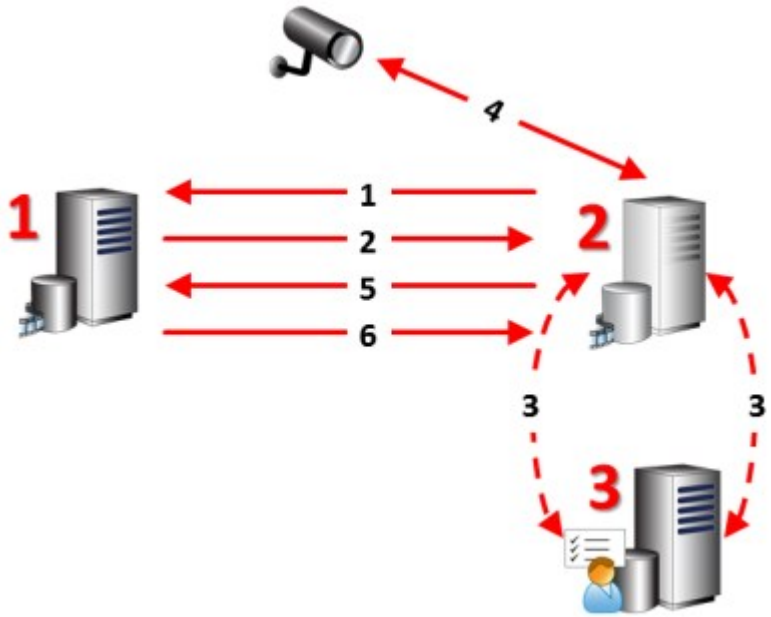
Gruppen haben einen klaren Vorteil: Wenn Sie später bestimmen, welche Failover-Aufzeichnungsserver einen Aufzeichnungsserver ablösen sollen, wählen Sie einfach eine Gruppe von Failover-Aufzeichnungsservern aus. Falls die ausgewählte Gruppe aus mehr als einem Failover-Aufzeichnungsserver besteht, haben Sie zur Sicherheit mehr als einen Failover-Aufzeichnungsserver zur Ablösung in Bereitschaft, falls ein Aufzeichnungsserver nicht mehr verfügbar sein sollte. Sie können eine sekundäre Failover-Server-Gruppe bestimmen, welche die Aufgaben der primären Gruppe übernimmt, sollten alle Aufzeichnungsserver der primären Gruppe ausgelastet sein. Ein Failover-Aufzeichnungsserver kann nicht Teil mehrerer Gruppen sein.

Failover-Aufzeichnungsserver in einer Failover-Gruppe sind in einer Sequenz angeordnet. Die Sequenz bestimmt die Reihenfolge, in der die Failover-Aufzeichnungsserver einen Aufzeichnungsserver ablösen. Standardmäßig entspricht die Sequenz der Reihenfolge, in der Sie die Failover-Aufzeichnungsserver in die Failover-Gruppe aufgenommen haben: Der zuerst aufgenommene Server ist der erste in der Sequenz. Bei Bedarf können Sie dies ändern.

Hot-Standby-Failover-Aufzeichnungsserver

Bei einem Hot-Standby-Failover-Aufzeichnungsserver bestimmen Sie einen Failover-Aufzeichnungsserver, der nur **einen** Aufzeichnungsserver ablöst. So kann das System diesen Failover-Aufzeichnungsserver im „Standby"-Modus behalten, sodass er mit der korrekten/aktuellen Konfiguration des ihm zugewiesenen Aufzeichnungsservers synchronisiert wird und viel schneller zur Ablösung bereit ist als ein Cold-Standby-Failover-Aufzeichnungsserver. Wie bereits erwähnt, weisen Sie Hot-Standby-Server nur einem Aufzeichnungsserver zu und können sie nicht gruppieren. Sie können Failover-Server, die bereits Teil einer Failover-Gruppe sind, nicht zu Hot-Standby-Aufzeichnungsservern machen.

Failover-Schritte (Erklärung)



Beschreibung
Beteiligte Server (Zahlen in rot): 1. Aufzeichnungsserver 2. Failover Recording Server 3. Managementserver
Failover-Schritte für **Cold-Standby**: 1. Um zu prüfen, ob er läuft oder nicht, steht ein Failover-Server in ständiger TCP-Verbindung mit einem Aufzeichnungsserver. 2. Diese Verbindung wird unterbrochen. 3. Der Failover-Aufzeichnungsserver erfragt die aktuelle Konfiguration des Aufzeichnungsservers vom Management-Server. Der Management-Server sendet die angefragte Konfiguration, der Failover-Aufzeichnungsserver erhält sie, startet und beginnt dann anstelle des Aufzeichnungsservers aufzuzeichnen. 4. Der Failover-Aufzeichnungsserver und die relevante(n) Kamera(s) tauschen Videodaten aus. 5. Der Failover-Aufzeichnungsserver versucht kontinuierlich, die Verbindung mit dem Aufzeichnungsserver wiederherzustellen. 6. Wenn die Verbindung zum Aufzeichnungsserver wiederhergestellt wurde, schaltet sich der Failover-Aufzeichnungsserver ab und der Aufzeichnungsserver erhält (ggf.) Videodaten, die während der Ausfallzeit aufgenommen wurden. Diese werden in seiner Datenbank zusammengeführt.
Failover-Schritte für **Hot-Standby**: 1. Um zu prüfen, ob er läuft oder nicht, steht ein Hot-Standby-Server in ständiger TCP-Verbindung mit dem zugewiesenen Aufzeichnungsserver. 2. Diese Verbindung wird unterbrochen. 3. Der Hot-Standby-Server kennt die aktuelle Konfiguration des zugewiesenen Aufzeichnungsservers bereits und beginnt an seiner Stelle aufzuzeichnen. 4. Der Hot-Standby-Server und die relevante(n) Kamera(s) tauschen Videodaten aus. 5. Der Hot-Standby-Server versucht kontinuierlich, die Verbindung mit dem Aufzeichnungsserver wiederherzustellen. 6. Wenn die Verbindung zum Aufzeichnungsserver wiederhergestellt wurde, kehrt der Hot-Standby-Server in den Hot-Standby-Modus zurück und der Aufzeichnungsserver erhält (ggf.) Videodaten, die während der Ausfallzeit aufgenommen wurden. Diese werden in seiner Datenbank zusammengeführt.

Die Funktionalität der Failover-Aufzeichnungsserver (Erklärung)

- Ein Failover-Aufzeichnungsserver überprüft den Status relevanter Aufzeichnungsserver alle 0,5 Sekunden. Falls ein Aufzeichnungsserver 2 Sekunden lang nicht reagiert, wird er als nicht verfügbar eingestuft und der Failover-Aufzeichnungsserver übernimmt
- Ein Cold-Standby-Failover-Aufzeichnungsserver übernimmt die Aufzeichnung für den nicht mehr verfügbaren Server nach fünf Sekunden sowie dem Zeitraum, in dem der Aufzeichnungsserver-Dienst des Failover-Aufzeichnungsservers startet und in dem die Verbindung zu den Kameras aufgebaut wird. Ein Hot-Standby-Failover-Aufzeichnungsserver hingegen übernimmt schneller, da der Aufzeichnungsserver-Dienst bereits über die korrekte Konfiguration verfügt und nur die Kameras starten muss, um Feeds zu liefern. Während des Systemstarts können Sie weder Aufzeichnungen speichern noch Live-Video von betroffenen Kameras sehen
- Sobald ein Aufzeichnungsserver wieder verfügbar ist, übernimmt er automatisch für den Failover-Aufzeichnungsserver. Vom Failover-Aufzeichnungsserver gespeicherte Aufzeichnungen werden automatisch in den Datenbanken des Standard-Aufzeichnungsservers zusammengeführt. Die Dauer dieses Vorgangs hängt von der Aufzeichnungsmenge, Netzwerkkapazität und weiteren Faktoren ab. Während der Zusammenführung können Sie keine Aufzeichnungen aus dem Zeitraum der Übernahme durch den Failover-Aufzeichnungsserver einsehen
- Wenn ein Cold-Standby-Failover-Aufzeichnungsserver während der Zusammenführung einen anderen Aufzeichnungsserver ablösen muss, verschiebt er den Zusammenführungsprozess mit Aufzeichnungsserver A und übernimmt die Aufzeichnungen für Aufzeichnungsserver B. Wenn Aufzeichnungsserver B wieder verfügbar ist, übernimmt der Failover-Aufzeichnungsserver den Zusammenführungsprozess für Aufzeichnungsserver A und danach für Aufzeichnungsserver B.
- In einer Hot-Standby-Konfiguration kann ein Hot-Standby-Server nicht für einen zusätzlichen Aufzeichnungsserver übernehmen, da er nur Hot Standby für einen einzigen Aufzeichnungsserver sein kann. Fällt dieser Aufzeichnungsserver jedoch wieder aus, übernimmt der Hot-Standby-Server abermals und behält die zuvor gemachten Aufzeichnungen. Der Aufzeichnungsserver behält Aufzeichnungen, bis sie wieder im primären Recorder zusammengeführt werden oder dem Failover-Aufzeichnungsserver kein Festplattenspeicher mehr zur Verfügung steht
- Eine Failover-Lösung bietet keine vollständige Redundanz. Sie ist nur eine zuverlässige Methode, um Ausfallzeiten zu minimieren. Wenn ein Aufzeichnungsserver wieder verfügbar ist, stellt der Failover Server-Dienst sicher, dass der Aufzeichnungsserver wieder Aufzeichnungen speichern kann. Erst dann ist der eigentliche Aufzeichnungsserver wieder für die Speicherung von Aufzeichnungen zuständig. Daher ist ein Aufzeichnungsverlust in diesem Teil des Prozesses sehr unwahrscheinlich

- Für Clientbenutzer ist die Ablösung durch den Failover-Aufzeichnungsserver fast unmerklich. Eine kurze Pause tritt auf, die meistens nur ein paar Sekunden dauert, wenn der Failover-Aufzeichnungsserver übernimmt. Während dieser Pause können Benutzer nicht auf Videoaufnahmen des betroffenen Aufzeichnungsservers zugreifen. Clientbenutzer können wieder Live-Video ansehen, sobald der Failover-Aufzeichnungsserver übernommen hat. Da neue Aufzeichnungen auf dem Failover-Aufzeichnungsserver gespeichert werden, können Sie Aufzeichnungen aus der Zeit abspielen, nachdem der Failover-Aufzeichnungsserver übernommen hat. Clients können keine älteren, nur auf dem betroffenen Aufzeichnungsserver gespeicherten Aufzeichnungen abspielen, bis dieser Aufzeichnungsserver wieder funktioniert und für den Failover-Aufzeichnungsserver übernommen hat. Sie haben keinen Zugriff auf archivierte Aufzeichnungen. Wenn der Aufzeichnungsserver wieder funktioniert, findet eine Zusammenführung statt, bei der die Failover-Aufzeichnungen wieder mit der Datenbank des Aufzeichnungsservers zusammengeführt werden. Während dieses Vorgangs können Sie keine Aufzeichnungen aus dem Zeitraum abspielen, in dem der Failover-Aufzeichnungsserver übernommen hat
- In einer Cold-Standby-Konfiguration ist es nicht notwendig, einen Failover-Aufzeichnungsserver als Backup für einen anderen Failover-Aufzeichnungsserver einzurichten. Dies liegt daran, dass Sie Failover-Gruppen und keine bestimmten Failover-Aufzeichnungsserver für die Ablösung bestimmter Aufzeichnungsservers zuweisen. Eine Failover-Gruppe muss mindestens einen Failover-Aufzeichnungsserver enthalten, doch Sie können so viele wie notwendig hinzufügen. Falls eine Failover-Gruppe mehr als einen Failover-Aufzeichnungsserver enthält, steht mehr als ein Failover-Aufzeichnungsserver zur Ablösung bereit.
- In einer Hot-Standby-Konfiguration können Sie keine Failover-Aufzeichnungsserver oder Hot-Standby-Server als Failover für einen Hot-Standby-Server einrichten

Failover-Aufzeichnungsserver einrichten und aktivieren

> Wenn Sie den Failover-Aufzeichnungsserver deaktiviert haben, müssen Sie ihn aktivieren, bevor er von den Standard-Aufzeichnungsservern übernehmen kann.

Tun Sie das Folgende, um einen Failover-Aufzeichnungsserver zu aktivieren und dessen grundlegenden Eigenschaften zu bearbeiten:

1. Wählen Sie im Fenster **Standort-Navigation** die Optionen **Server** > **Failover-Server** aus. Dadurch öffnet sich eine Liste von installierten Failover-Aufzeichnungsserver und Failover-Gruppen.
2. Wählen Sie im Fenster **Übersicht** den erwünschten Failover-Aufzeichnungsserver aus.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Aktiviert**. Der Failover-Aufzeichnungsserver ist nun aktiviert.
4. Um die Eigenschaften des Failover-Aufzeichnungsservers zu bearbeiten, gehen Sie auf die Registerkarte **Info**.

5. Wenn Sie fertig sind, gehen Sie auf die Registrierkarte **Netzwerk**. Hier können Sie die öffentliche IP-Adresse des Failover-Aufzeichnungsservers und mehr definieren. Dies ist wichtig, wenn Sie NAT (Network Address Translation) und Portweiterleitung verwenden. Weitere Informationen finden Sie auf der Registerkarte **Netzwerk** des Standard-Aufzeichnungsservers.
6. Wählen Sie im Bereich **Standort-Navigation** die Optionen **Server** > **Aufzeichnungsserver** aus. Wählen Sie den Aufzeichnungsserver aus, für den die Failover-Unterstützung aktiviert werden soll, und Registerkarte „Failover" (Aufzeichnungsserver) auf Seite 175).

Um den Status eines Failover-Aufzeichnungsservers anzuzeigen, halten Sie die Maus über das Failover Recording Server Manager-Taskleistensymbol im Benachrichtigungsbereich. Ein Tooltip wird angezeigt, der den Text enthält, der im Feld Beschreibung des Failover-Aufzeichnungsservers eingegeben wurde. Dies kann Ihnen dabei helfen festzustellen, für welchen Aufzeichnungsserver der Failover-Aufzeichnungsserver zur Übernahme konfiguriert wurde.

Der Failover-Aufzeichnungsserver pingt den Management-Server regelmäßig, um sicherzustellen, dass er online ist und bei Bedarf die Konfiguration der Standard-Aufzeichnungsserver anfordern und empfangen kann. Wenn Sie das Pingen blockieren, kann der Failover-Aufzeichnungsserver nicht von Standard-Aufzeichnungsserver übernehmen.

Gruppieren von Failover-Aufzeichnungsservern für Cold-Standby

1. Wählen Sie **Server** > **Failover-Server**. Dadurch öffnet sich eine Liste von installierten Failover-Aufzeichnungsserver und Failover-Gruppen.
2. Klicken Sie im Bereich **Übersicht** mit der rechten Maustaste auf **Failover-Gruppen** und wählen Sie **Gruppe hinzufügen**.
3. Geben Sie einen Namen (in diesem Beispiel *Failover-Gruppe 1*) und eine Beschreibung (optional) Ihrer neuen Gruppe an. Klicken Sie auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf die gerade erstellte Gruppe (*Failover-Gruppe 1*). Wählen Sie **Gruppenmitglieder bearbeiten**. Dadurch öffnet sich das Fenster **Gruppenmitglieder auswählen**.
5. Nutzen Sie Drag-and-Drop oder die Tasten, um den/die ausgewählten Failover-Aufzeichnungsserver von links nach rechts zu bewegen. Klicken Sie auf **OK**. Der/die ausgewählten Failover-Aufzeichnungsserver sind jetzt Teil der neu erstellten Gruppe (*Failover-Gruppe 1*).
6. Gehen Sie zur Registerkarte **Sequenz**. Klicken Sie auf **Nach oben** und **Nach unten**, um die interne Sequenz der regulären Failover-Aufzeichnungsserver in der Gruppe zu bestimmen.

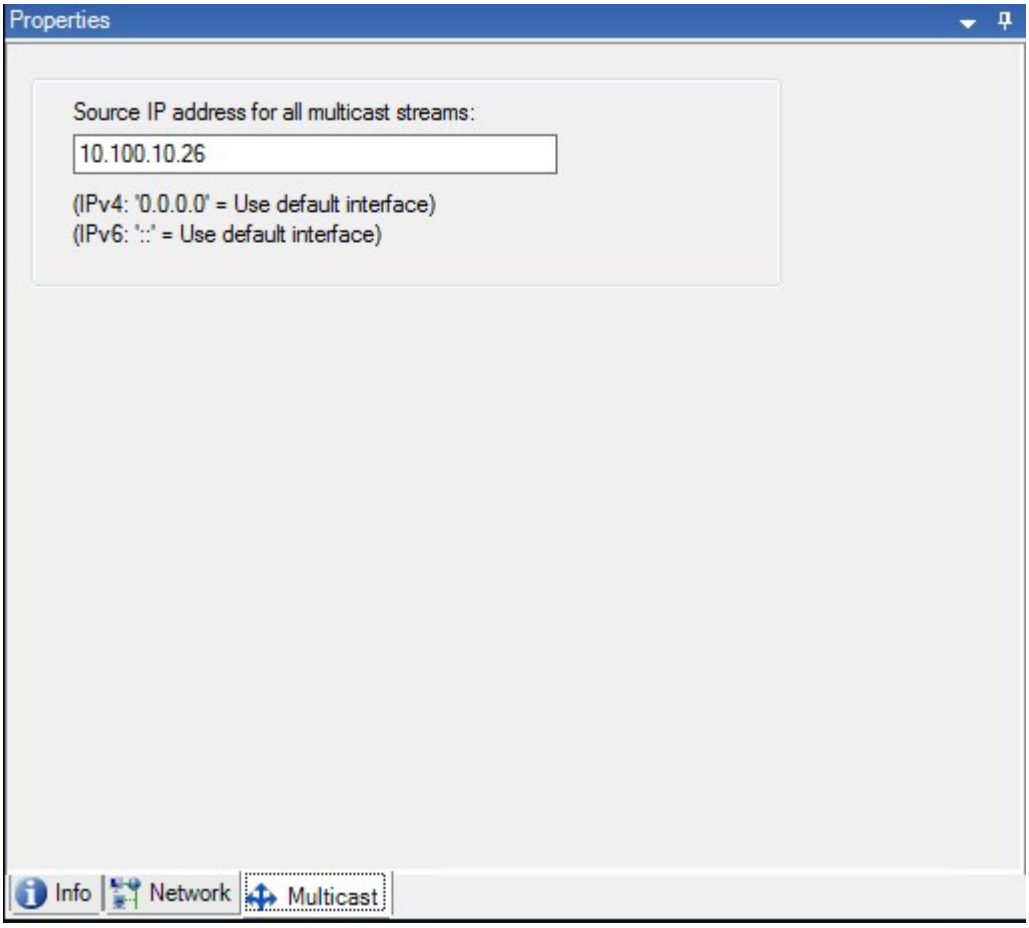
Bedeutung von Failover-Aufzeichnungsserver-Statussymbolen

Folgende Symbole repräsentieren den Status von Failover-Aufzeichnungsserver (Symbole sind im Bereich **Übersicht** zu sehen):

Symbol	Beschreibung
	Der Failover-Aufzeichnungsserver wartet oder ist in Bereitschaft. Wenn er wartet, ist der Failover-Aufzeichnungsserver noch nicht dazu konfiguriert, einen anderen Aufzeichnungsserver abzulösen. In Bereitschaft ist der Failover-Aufzeichnungsserver auf die Beobachtung eines oder mehrerer Aufzeichnungsserver konfiguriert.
	Der Failover-Aufzeichnungsserver hat für den bezeichneten Aufzeichnungsserver übernommen. Wenn Sie Ihren Cursor über dem Server-Symbol platzieren, erscheint ein Tooltip. Sehen Sie anhand des Tooltips für welchen Aufzeichnungsserver der Failover-Aufzeichnungsserver übernommen hat.
	Die Verbindung zum Failover-Aufzeichnungsserver wurde unterbrochen.

Registerkarte Multicast (Failover-Server)

Wenn Sie Failover-Server verwenden und Multicasting von Live-Streaming aktiviert wurde, müssen Sie die IP-Adressen der Netzwerkkarten sowohl auf den Aufzeichnungsserver und den Failover-Server festlegen.



Weitere Informationen über Multicasting finden Sie unter Registerkarte „Multicast“ (Aufzeichnungsserver) auf Seite 178 oder Registerkarte „Multicast“ (Aufzeichnungsserver) auf Seite 178.

Eigenschaften der Registerkarte "Info" (Failover-Server)

Geben Sie die folgenden Eigenschaften von Failover-Aufzeichnungsservern an:

Name	Beschreibung
Name	Der Name des Failover-Aufzeichnungsservers, wie er in Management Client, Protokollen und andernorts auftaucht.

Name	Beschreibung
Beschreibung	Ein optionales Feld, in dem Sie den Failover-Aufzeichnungsserver beschreiben können, z. B. für welchen Aufzeichnungsserver er übernimmt.
Hostname	Zeigt den Hostnamen des Failover-Aufzeichnungsservers an. Sie können diese nicht ändern.
Adresse des lokalen Webservers	Zeigt die lokale Adresse des Webservers des Failover-Aufzeichnungsservers an. Sie verwenden die lokale Adresse, zum Beispiel zur Handhabung der PTZ-Kamerasteuerungsbefehle, sowie zur Handhabung von Browsing- und Live-Anforderungen von XProtect Smart Client. Die Adresse enthält die Portnummer, die für die Kommunikation mit dem Webserver verwendet wird (typischerweise Port 7563). Wenn der Failover-Aufzeichnungsserver von einem Aufzeichnungsserver übernimmt, der eine Verschlüsselung verwendet, müssen Sie auch den Failover-Aufzeichnungsserver so vorbereiten, dass er eine Verschlüsselung verwendet. Wenn Sie die Verschlüsselung zu Clients und Servern aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, erscheint ein Vorhängeschloss-Symbol, und die Adresse enthält **https** anstelle von **http**.
Adresse des Web-Servers	Zeigt die öffentliche Adresse des Webservers des Failover-Aufzeichnungsservers im Internet an. Wenn Ihre Installation eine Firewall oder einen NAT-Router verwendet, geben Sie die Adresse der Firewall oder des NAT-Routers ein, damit Clients, die über das Internet auf das Überwachungssystem zugreifen, sich mit dem Failover-Aufzeichnungsserver verbinden können. Die öffentliche Adresse und die Portnummer geben Sie auf der Registerkarte **Netzwerk** an. Wenn Sie die Verschlüsselung zu Clients und Servern aktivieren, die Datenstreams vom Aufzeichnungsserver abrufen, erscheint ein Vorhängeschloss-Symbol, und die Adresse enthält **https** anstelle von **http**.
UDP-Port	Über diese Portnummer kommunizieren die Failover-Aufzeichnungsserver. Die Standardeinstellung ist Port 8844.
Speicherort der Datenbank	Bestimmen Sie den vom Failover-Aufzeichnungsserver zur Speicherung von Aufzeichnungen verwendeten Pfad zur Datenbank.

Name	Beschreibung
	Sie können den Datenbankpfad nicht ändern, während der Failover-Aufzeichnungsserver für einen Aufzeichnungsserver übernimmt. Das System wendet die Änderungen an, wenn der Failover-Aufzeichnungsserver nicht mehr für einen Aufzeichnungsserver übernimmt.
Diesen Failover-Server aktivieren	Abwählen, um den Failover-Aufzeichnungsserver zu deaktivieren (standardmäßig ausgewählt). Sie müssen Failover-Aufzeichnungsserver deaktivieren, bevor sie Aufzeichnungsserver ablösen können.

Eigenschaften der Registerkarte "Info" (Failover-Gruppe)

Feld	Beschreibung
Name	Der Name der Failover-Gruppe, wie er im Management Client, Protokollen und andernorts auftaucht.
Beschreibung	Eine optionale Beschreibung, z. B. der physische Serverstandort.

Eigenschaften der Registerkarte "Sequenz" (Failover-Gruppe)

Feld	Beschreibung
Failover-Sequenz angeben	Verwenden Sie **Nach oben** und **Nach unten**, um die gewünschte Sequenz der regulären Failover-Aufzeichnungsserver in der Gruppe festzulegen.

Failover-Aufzeichnugnsserver-Dienst (Erklärung)

Ein Failover-Aufzeichnungsserver verfügt über zwei installierte Dienste:

- Ein Failover Server-Dienst, der die Abläufe für die Übernahme vom Aufzeichnungsserver übernimmt. Dieser Dienst ist immer aktiv und überprüft konstant den Status relevanter Aufzeichnungsserver
- Ein Failover Recording Server-Dienst, durch den der Failover-Aufzeichnungsserver als Aufzeichnungsserver agieren kann.

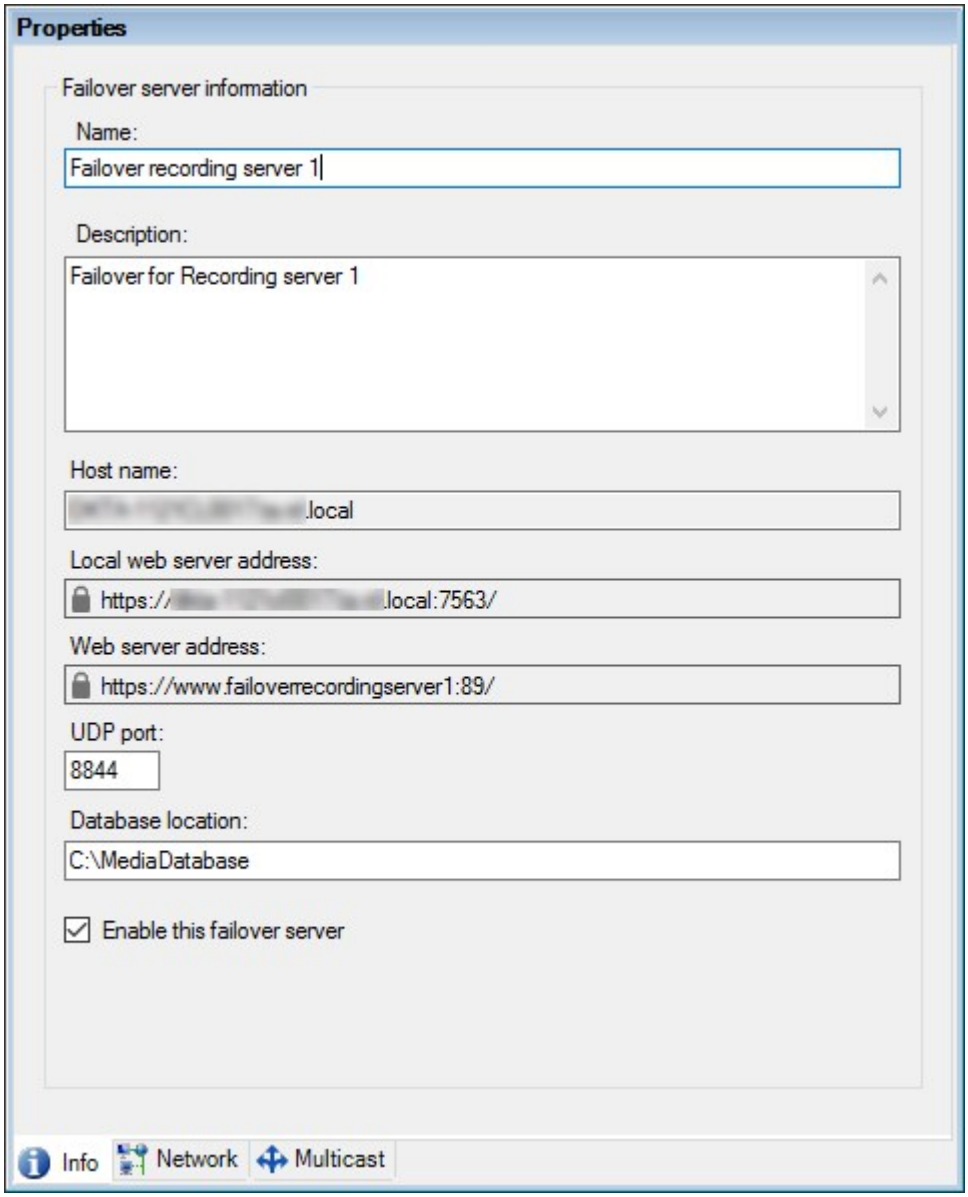
  In einer Cold-Standby-Konstellation wird dieser nur bei Bedarf gestartet, wenn also der Cold-Standby-Failover-Aufzeichnungsserver den Aufzeichnungsserver ablöst. Das Starten dieses Dienstes dauert in der Regel ein paar Sekunden, kann aber länger dauern, je nach lokalen Sicherheitseinstellungen usw.
  In einer Hot-Standby-Einrichtung. Dieser Dienst läuft immer, sodass der Hot-Standby-Server schneller übernimmt als der Cold-Standby-Failover-Aufzeichnungsserver.

Verschlüsselungsstatus auf einem Failover-Aufzeichnungsserver anzeigen

Um zu prüfen, ob Ihr Failover-Aufzeichnungsserver eine Verschlüsselung verwendet, tun Sie bitte folgendes:

1. Wählen Sie auf der Tafel **Seitennavigation Server** > **Failover-Server** aus. Daraufhin wird eine Liste mit Failover-Aufzeichnungsservern geöffnet.
2. Wählen Sie in dem Fenster **Übersicht** den jeweiligen Aufzeichnungsserver aus und gehen Sie auf die Registerkarte **Info**.
   Wenn die Verschlüsselung zu Clients und Servern, die Datenstreams vom Aufzeichnungsserver abrufen, aktiviert ist, erscheint ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der des

optionalen Webservers.



Anzeigen von Statusmeldungen

1. Klicken Sie auf dem Failover-Aufzeichnungsserver mit der rechten Maustaste auf das **Milestone Failover Recording Server-Dienst**-Symbol.
2. Wählen Sie **Statusmeldungen anzeigen**. Das Fenster **Failover-Server-Statusmeldungen** wird mit Zeitstempel-Statusmeldungen eingeblendet.

Anzeigen von Versionsinformationen

Die Kenntnis der genauen Version Ihres **Failover Recording Server-Dienstes** ist hilfreich, wenn Sie sich an den Produktsupport wenden wollen.

1. Klicken Sie auf dem Failover-Aufzeichnungsserver mit der rechten Maustaste auf das **Milestone Failover Recording Server-Dienst**-Symbol.
2. Wählen Sie **Info**.
3. Ein kleines Dialogfeld öffnet sich und zeigt die exakte Version Ihres **Failover Recording Server-Dienstes** an.

Site-Navigation: Server und Hardware: Hardware

Hardware (Erklärung)

Hardware steht entweder für:

- Die physische Einheit, die mit dem Aufzeichnungsserver des Überwachungssystems direkt über IP verbunden ist, beispielsweise eine Kamera, ein Videoencoder, ein I/O-Modul
- Ein Aufzeichnungsserver an einem Remote-System in einer Milestone Interconnect-Einrichtung

Weitere Informationen dazu, wie Sie Hardware zu Ihrem System hinzufügen können, finden Sie unter Hardware hinzufügen auf Seite 197.

Hardware hinzufügen

Sie haben mehrere Optionen, um zu den Aufzeichnungsservern in Ihrem System Hardware hinzuzufügen.

> ⚠ Wenn Ihre Hardware sich hinter einem NAT-fähigen Router oder einer Firewall befindet, müssen Sie möglicherweise eine andere Portnummer bestimmen und den Router/die Firewall so konfigurieren, dass die von der Hardware genutzten Port- und IP-Adressen zugewiesen werden.

Der Assistent zum **Hardware hinzufügen** hilft Ihnen dabei, in Ihrem Netzwerk Hardware wie etwa Kameras und Videoencoder zu finden und diese den Aufzeichnungsservern in Ihrem System hinzuzufügen. Mit dem Assistenten können Sie auch Remote-Server für Milestone Interconnect-Einrichtungen hinzufügen. Fügen Sie jeweils nur bei **einem Aufzeichnungsserver** zur selben Zeit Hardware hinzu.

1. Um auf **Hardware hinzufügen** zuzugreifen, klicken Sie mit der rechten Maustaste auf den notwendigen Aufzeichnungsserver und wählen Sie **Hardware hinzufügen**.
2. Wählen Sie eine der Assistentenoptionen (siehe unten) und folgen Sie den Anweisungen auf dem Bildschirm.
3. Nach der Installation können Sie die Hardware und Geräte im Fenster **Übersicht** sehen.

Bestimmte Hardwaregeräte müssen vorkonfiguriert werden, wenn die Hardware zum ersten Mal hinzugefügt wird. Ein zusätzlicher Assistent zur **Vorkonfiguration von Hardwaregeräten** erscheint, wenn solche Hardwaregeräte hinzugefügt werden. Weitere Informationen finden Sie unter Hardwarevorkonfiguration (Erklärung) auf Seite 199.

Name	Beschreibung
Express (empfohlen)	Das System scannt das lokale Netzwerk des Aufzeichnungsservers automatisch nach neuer Hardware. Wählen Sie das Kontrollkästchen **Hardware auf anderen Aufzeichnungsservern anzeigen** aus, um zu erfahren, ob erkannte Hardware auf anderen Aufzeichnungsservern läuft. Sie können diese Option jedes Mal auswählen, wenn Sie Ihrem Netzwerk neue Hardware hinzufügen und diese in Ihrem System verwenden wollen. Sie können diese Option nicht verwenden, um Remote-Systeminstallationen in Milestone Interconnect-Einstellungen hinzuzufügen. Zum Hinzufügen von sowohl HTTP- als auch HTTPS-Hardware führen Sie die **Express**-Erkennung mit ausgewählter Optionsschaltfläche **HTTPS (Sicher)** aus, und dann mit ausgewählter Optionsschaltfläche **HTTP (Unsicher)**.
Adressbereich scannen	Das System scannt Ihr Netzwerk nach relevanter Hardware und Milestone Interconnect-Remote-Systeminstallationen auf Basis Ihrer Angaben zu: • Hardware-Benutzernamen und Passwörtern. Dies ist nicht nötig, wenn Ihre Hardware die werksseitig voreingestellten Benutzernamen und Passwörter verwendet • Treiber • IP-Bereiche (nur IPv4) • Portnummer (Standardport 80) Sie können diese Option auswählen, wenn Sie nur einen Teil Ihres Netzwerks scannen möchten, beispielsweise bei einer Systemerweiterung.
Handbuch	Bestimmen Sie die Einzelheiten zu allen Hardware- und Milestone Interconnect-

Name	Beschreibung
	Remote-Systeminstallationen separat. Dies kann eine gute Vorgehensweise sein, wenn Sie nur wenige Hardware-Einheiten hinzufügen möchten und ihre IP-Adressen, relevanten Benutzernamen und Passwörter kennen oder eine Kamera die automatische Erkennungsfunktion nicht unterstützt.
Fernverbindungs-Hardware	Das System scannt nach Hardware, die über einen über Fernzugriff verbundenen Server verbunden ist. Sie können diese Option nutzen, wenn Sie beispielsweise Server für die Axis One-click Camera Connection installiert haben. Sie können diese Option nicht verwenden, um Remote-Systeminstallationen in Milestone Interconnect-Einstellungen hinzuzufügen.

Hardwarevorkonfiguration (Erklärung)

Manche Hersteller fordern, dass auf Hardware im Auslieferungszustand Benutzerdaten eingerichtet werden, bevor die Hardware erstmals zu einem VMS-System hinzugefügt wird. Dies wird als Hardwarevorkonfiguration bezeichnet und erfolgt mithilfe des Assistenten **Hardwaregeräte vorkonfigurieren**, der erscheint, wenn solche Hardwaregeräte durch den Assistenten Hardware hinzufügen auf Seite 197 erkannt werden.

Einige wichtige Informationen zum Assistenten **Hardwaregeräte vorkonfigurieren**:

- Hardware, für die Benutzerdaten erforderlich sind, bevor sie zu einem VMS-System hinzugefügt wird, kann nicht unter Verwendung der typischen Standard-Benutzerdaten hinzugefügt werden und muss über den Assistenten konfiguriert werden, oder indem die Hardware direkt angeschlossen wird
- Benutzerdaten (Benutzername oder Passwort) können Sie nur auf Felder anwenden, die als **nicht festgelegt** gekennzeichnet sind
- Sobald der Hardware-**Status** auf **konfiguriert** lautet, können Sie die Benutzerdaten (Benutzername oder Passwort) nicht mehr ändern
- Die Vorkonfiguration gilt für Hardware im Auslieferungszustand und muss nur einmal erfolgen. Sobald die Hardware vorkonfiguriert wurde, kann sie wie jede andere Hardware verwaltet werden in Management Client
- Sobald Sie den Assistenten **Hardwaregeräte vorkonfigurieren** schließen, erscheint die vorkonfigurierte Hardware in dem Assistenten Hardware hinzufügen auf Seite 197 und kann jetzt zu Ihrem System hinzugefügt werden

Es wird unbedingt empfohlen, dass Sie die vorkonfigurierte Hardware zu Ihrem System hinzufügen, indem Sie den Assistenten Hardware hinzufügen auf Seite 197 abschließen sobald Sie den Assistenten **Hardwaregeräte vorkonfigurieren** geschlossen haben. Management Client speichert die vorkonfigurierten Benutzerdaten nicht ab, wenn Sie die Hardware nicht zu Ihrem System hinzufügen.

Deaktivieren/Aktivieren von Hardware

Hinzugefügte Hardware ist standardmäßig **aktiviert**.

So können Sie erkennen, ob Hardware aktiviert oder deaktiviert ist:

verwenden
Deaktiviert

Um hinzugefügte Hardware zu deaktivieren, z.B. aus Lizenz- oder Leistungsgründen

1. Erweitern Sie den Aufzeichnungsserver und klicken Sie mit der rechten Maustaste auf die Hardware, die Sie deaktivieren möchten.
2. Wählen Sie **Aktiviert**, um die Option zu aktivieren oder zu deaktivieren.

Hardware bearbeiten

Klicken Sie mit der rechten Maustaste auf die hinzugefügte Hardware und wählen Sie **Hardware bearbeiten** aus, um die Netzwerkkonfiguration und die Einstellungen für die Benutzerberechtigungen der Hardware in Management Client zu ändern.

Für manche Hardwaregeräte erlaubt Ihnen der Dialog **Hardware bearbeiten** auch, Einstellungen direkt auf das jeweilige Hardwaregerät anzuwenden.

Wenn die Optionsschaltfläche **Einstellungen Management Client bearbeiten ausgewählt ist**, zeigt der Dialog **Hardware bearbeiten** die Einstellungen, die Management Client für die Verbindung zur Hardware verwendet. Damit das Hardwaregerät korrekt zum System hinzugefügt wird, nehmen Sie die gleichen Einstellungen vor, die Sie auch für die Verbindung zur Hardwarekonfigurationsoberfläche des Herstellers verwenden:

Name	Beschreibung
Name	Zeigt den Namen der Hardware neben der ermittelten IP-Adresse an (in Klammern).
URL der	Die Webadresse der Konfigurationsoberfläche des Herstellers, die typischerweise die IP-

Name	Beschreibung
Hardware	Adresse der Hardware enthält.
Benutzername	Der für die Verbindung zur Hardware verwendete Benutzername. Der Benutzername, den Sie hier eingeben, ändert nicht den Benutzernamen auf dem Hardwaregerät selbst. Wählen Sie Optionsschaltflächen **Bearbeiten Management Client und Hardwareeinstellungen** aus, um auf unterstützten Hardwaregeräten die Einstellungen zu ändern.
Passwort	Das für die Verbindung zur Hardware verwendete Passwort. Das Passwort, das Sie hier eingeben, ändert nicht das Passwort auf dem Hardwaregerät selbst. Wählen Sie Optionsschaltflächen **Bearbeiten Management Client und Hardwareeinstellungen** aus, um auf unterstützten Hardwaregeräten die Einstellungen zu ändern. Informationen dazu, wie Passwörter für mehrere Hardwaregeräte geändert werden, siehe Passwörter auf Hardwaregeräten ändern auf Seite 209. Als Systemadministrator müssen Sie anderen Benutzern die Erlaubnis erteilen, das Passwort im Management Client einzusehen. Weitere Informationen finden Sie unter Rolleneinstellungen auf Seite 379 unter Hardware.

Wenn die Option Schaltfläche **Bearbeiten Management Client und Hardwareeinstellungen** ausgewählt ist (für unterstützte Hardware), zeigt der Dialog **Hardware bearbeiten** die Einstellungen, die auch direkt auf das jeweilige Hardwaregerät angewendet werden:

Wenn mit dieser Optionsschaltfläche die Einstellungen angewendet werden, werden die aktuellen Einstellungen auf dem Hardwaregerät überschrieben. Die Hardware verliert dann für einen Moment die Verbindung zum Aufzeichnungsserver, während die Einstellungen angewendet werden.

Name	Beschreibung
Name	Zeigt den Namen der Hardware neben der ermittelten IP-Adresse an (in Klammern).
Netzwerkkonfiguration	Die Netzwerkeinstellungen der Hardware. Zum Einstellen der Netzwerkeinstellungen wählen Sie Konfigurieren auf Seite 202.
Konfigurieren	Geben Sie (für unterstützte Hardwaregeräte) anhand der Auswahlliste für die **IP-Version** das Internetprotokoll an. • Für IPv4 müssen die Werte das folgende Format haben: **(0-999).(0-999).(0-999).(0-999)** • Für IPv6 müssen die Werte in acht Gruppen aus Hexadezimalzahlen angeordnet sein, die jeweils mit einem Doppelpunkt getrennt sind. Die Subnetzmaske muss eine Zahl zwischen **0-128** sein. Die Schaltfläche **Prüfen** testet, ob aktuell im System noch ein weiteres Hardwaregerät vorhanden ist, das die angegebene IP-Adresse verwendet. **Prüfen** kann keine Konflikte mit Hardwaregeräten erkennen, die ausgeschaltet sind, sich außerhalb des XProtect VMS-Systems befinden oder aus sonstigen Gründen momentan nicht reagieren.
Benutzername	Der für die Verbindung zur Hardware verwendete Benutzername und das dazugehörige Level. Wählen Sie von der Auswahlliste einen weiteren Benutzer aus und fügen Sie mithilfe des weiter unten beschriebenen Feldes **Passwort** ein neues Passwort hinzu. Mithilfe der unterstrichenen Aktionen unten im Abschnitt **Authentifizierung** (siehe **Benutzer hinzufügen auf Seite 203** oder **Benutzer löschen auf Seite 204**) können Sie Benutzer hinzufügen oder entfernen. Wenn Sie einen Benutzer auswählen, der nicht die höchste vom Hersteller vorgegebenen Benutzerebene besitzt, stehen manche Funktionen ggf. nicht zur Verfügung.
Passwort	Das für die Verbindung zur Hardware verwendete Passwort. Betrachten Sie den

Name	Beschreibung
	aktuell eingegebenen Text mithilfe des Symbols **Anzeige**. Wenn Sie das Passwort ändern, lesen Sie in der Dokumentation des Herstellers die Passwortregeln für das jeweilige Hardwaregerät nach, oder verwenden Sie die Schaltfläche **Passwort erzeugen**, um ein Passwort automatisch zu erzeugen, das die Anforderungen erfüllt. Informationen dazu, wie Passwörter für mehrere Hardwaregeräte geändert werden, siehe Passwörter auf Hardwaregeräten ändern auf Seite 209. Als Systemadministrator müssen Sie anderen Benutzern die Erlaubnis erteilen, das Passwort im Management Client einzusehen. Weitere Informationen finden Sie unter Rolleneinstellungen auf Seite 379 unter Hardware.
Benutzer hinzufügen	Wählen Sie das unterstrichene Link **Hinzufügen** aus, um den Dialog **Benutzer hinzufügen** zu öffnen und zum Hardwaregerät einen Benutzer hinzuzufügen. Wenn Sie einen Benutzer hinzufügen, wird dieser der aktuell aktive Benutzer, und die zuvor eingegebenen Anmeldedaten werden überschrieben. Wenn Sie das Passwort erstellen, lesen Sie in der Dokumentation des Herstellers die Passwortregeln für das jeweilige Hardwaregerät nach, oder verwenden Sie die Schaltfläche **Passwort erzeugen**, um automatisch ein Passwort zu erzeugen, das die Anforderungen erfüllt. Das höchste von dem Hardwaregerät erkannte Benutzerlevel wird automatisch vorausgewählt. Es wird empfohlen, das standardmäßig eingestellte **Benutzerlevel** zu ändern. Wenn Sie ein **Benutzerlevel** auswählen, das nicht das höchste vom Hersteller vorgegebene Benutzerlevel ist, stehen manche Funktionen ggf. nicht zur Verfügung.

Name	Beschreibung
Benutzer löschen	Wählen Sie das unterstrichene Link **Löschen** aus, um den Dialog **Benutzer löschen** zu öffnen und Benutzer vom Hardwaregerät zu löschen. Den aktuell aktiven Benutzer können Sie nicht löschen. Verwenden Sie den oben beschriebenen Dialog **Benutzer hinzufügen**, um einen neuen Benutzer einzustellen, und entfernen Sie dann den alten Benutzer mithilfe dieser Oberfläche.

Siehe auch Hardware verwalten.

Aktivieren/Deaktivieren einzelner Geräte

Kameras sind standardmäßig **aktiviert**.

Mikrofone, Lautsprecher, Metadaten, Eingänge und **Ausgänge** sind standardmäßig **deaktiviert**.

Dies bedeutet, dass Mikrofone, Lautsprecher, Metadaten, Eingänge und Ausgänge einzeln aktiviert werden müssen, bevor Sie diese im System nutzen können. Der Grund ist, dass Überwachungssysteme auf Kameras zurückgreifen, während die Nutzung von Mikrofonen usw. stark von den Bedürfnissen einer Organisation abhängt.

Sie können erkennen, ob Geräte aktiviert oder deaktiviert sind (hier am Beispiel eines Ausgangs):

Deaktiviert

Verwenden

Kameras, Mikrofone, Lautsprecher, Metadaten, Eingänge und Ausgänge werden auf dieselbe Weise aktiviert/deaktiviert.

1. Erweitern Sie den Aufzeichnungsserver und das Gerät. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie aktivieren möchten.
2. Wählen Sie **Aktiviert**, um die Option zu aktivieren oder zu deaktivieren.

Einrichten einer sicheren Verbindung zur Hardware

Sie können mithilfe von SSL (Secure Sockets Layer) eine sichere HTTPS-Verbindung zwischen der Hardware und dem Aufzeichnungsserver einrichten.

Wenden Sie sich an Ihren Kameraanbieter, um ein Hardware-Zertifikat zu erhalten und es hochzuladen, bevor Sie die unten angegebenen Schritte befolgen:

1. Klicken Sie im Bereich **Übersicht** mit der rechten Maustaste auf den Aufzeichnungsserver und wählen Sie die Hardware aus.

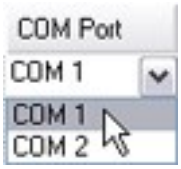
2. Aktivieren Sie HTTPS auf der Registerkarte **Einstellungen**. HTTPS ist standardmäßig nicht aktiviert.
3. Geben sie den Port auf dem Aufzeichnungsserver ein, zu dem die HTTPS-Verbindung besteht. Die Portnummer muss mit der Portnummer auf der Startseite des Geräts übereinstimmen.
4. Führen Sie nach Bedarf Veränderungen durch und speichern Sie.

Aktivieren von PTZ auf einem Videoencoder

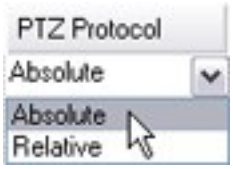
Um die Verwendung von PTZ-Kameras auf einem Videoencoder zu aktivieren, führen Sie in der Registerkarte **PTZ** folgende Schritte aus:

1. Wählen Sie in der Liste der mit dem Videoencoder verbundenen Geräte das Kästchen **PTZ aktivieren** für die relevanten Kameras aus:

2. Überprüfen Sie in der Spalte **PTZ-Geräte-ID** die ID jeder Kamera.
3. Wählen Sie in der Spalte **COM-Port** den Videoencoder, dessen COM-Ports (serielle Kommunikation) für die Steuerung der PTZ-Funktionalität verwendet werden soll:



4. Wählen Sie in der Spalte **PTZ-Protokoll**, welches Positionierungsschema Sie verwenden möchten:



   - **Absolut**: Wenn Benutzer für die Kamera PTZ-Steuerung verwenden, wird die Kamera relativ zu einer festen Position angebracht, oft als Home-Position bezeichnet
   - **Relativ**: Wenn Benutzer für die Kamera PTZ-Steuerung verwenden, wird die Kamera relativ zu einer festen Position angebracht

   Der Inhalt der Spalte **PTZ-Protokoll** variiert stark, abhängig von der Hardware. Einige verfügen über 5 bis 8 unterschiedliche Protokolle. Siehe auch Kameradokumentation.

5. Klicken Sie in der Symbolleiste auf **Speichern**.

   Nun können Sie die Preset-Positionen und Wachrundgänge für jede PTZ-Kamera konfigurieren:

   - Hinzufügen einer Preset-Position (Typ 1) auf Seite 253
   - Hinzufügen eines Wachrundgangprofils auf Seite 262

Hardware verwalten

Registerkarte „Info (Hardware)“

Informationen über die Registerkarte **Info** für Remote-Server finden Sie unter Registerkarte „Info (Remote-Server)“ auf Seite 212.

Registerkarte „Info (Hardware)“

Name	Beschreibung
Name	Geben Sie einen Namen ein. Das System verwendet den Namen, wenn die Hardware im System und den Clients aufgelistet wird. Der Name muss nicht einzigartig sein. Wenn Sie Hardware neu benennen, wird der Name im Management Client global geändert.
Beschreibung	Geben Sie eine Beschreibung der Hardware ein (optional). Die Beschreibung taucht in einer Anzahl Listen im System auf. Zum Beispiel, wenn Sie den Mauszeiger über den

Name	Beschreibung
	Hardware-Namen im Bereich **Übersicht** halten: 
Modell	Identifiziert das Hardware-Modell.
Seriennummer	Seriennummer der Hardware, wie vom Hersteller angegeben. Die Seriennummer ist oft, aber nicht immer, mit der MAC-Adresse identisch.
Treiber	Identifiziert den Treiber, der die Verbindung mit der Hardware verwaltet.
IE	Öffnet die Standard-Startseite des Hardware-Anbieters. Sie können diese Seite zur Administration der Hardware nutzen.
Adresse	Hostname oder IP-Adresse der Hardware.
MAC-Adresse	Legt die Media-Access-Control-Adresse (MAC) der Systemhardware fest. Eine MAC-Adresse ist eine zwölfstellige Hexadezimalzahl, die jedes Gerät in einem Netzwerk eindeutig identifiziert.
Letzte Passwortänderung	Das Feld **Zuletzt geändertes Passwort** zeigt den Zeitstempel der letzten Passwortänderung an, basierend auf den lokalen Zeiteinstellungen desjenigen Computers, von dem aus das Passwort geändert wurde.

Registerkarte Einstellungen (Hardware)

Auf der Registerkarte **Einstellungen** können Sie Einstellungen für die Hardware bestätigen oder bearbeiten.

Der Inhalt der Registerkarte **Einstellungen** wird durch die ausgewählte Hardware bestimmt und variiert je nach Hardware-Typ. Im Fall einiger Hardware-Typen enthält die Registerkarte **Einstellungen** keinen oder schreibgeschützten Inhalt.

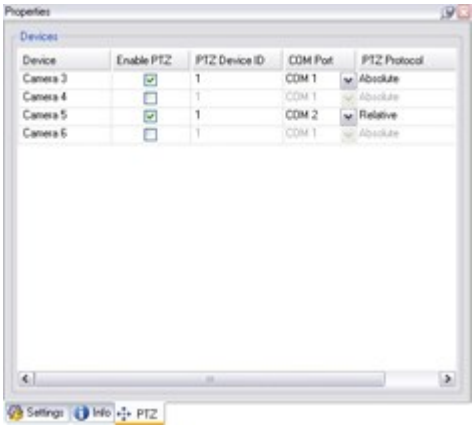
Informationen über die Registerkarte **Einstellungen** für Remote-Server finden Sie unter Registerkarte "Einstellungen" (Remote Server) auf Seite 213.

Registerkarte „PTZ (Videoencoder)“

Auf der Registerkarte **PTZ** können Sie PTZ (Pan/Tilt/Zoom) für Videoencoder aktivieren. Die Registerkarte ist verfügbar, wenn das ausgewählte Gerät ein Videoencoder ist oder der Treiber Kameras mit und ohne PTZ unterstützt.

Sie müssen die Verwendung von PTZ separat für jeden Kanal des Videoencoders auf der Registerkarte **PTZ** aktivieren, bevor Sie die PTZ-Funktionen der mit dem Videoencoder verbundenen PTZ-Kameras anwenden können.

Nicht alle Videoencoder unterstützen die Verwendung von PTZ-Kameras. Selbst Videoencoder, welche die Verwendung von PTZ-Kameras unterstützen, müssen möglicherweise konfiguriert werden, bevor diese Kameras benutzt werden können. Dies geschieht üblicherweise durch die Installation zusätzlicher Treiber über eine Browser-basierte Konfigurationsoberfläche auf der IP-Adresse des Geräts.



Die Registerkarte **PTZ** – PTZ ist für zwei Kanäle auf einem Videoencoder aktiviert.

Gerätepasswortverwaltung (Erklärung)

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

Sie können Passwörter für mehrere Hardwaregeräte auf einmal ändern.

Anfänglich sind die unterstützten Geräte Modelle von Canon, Axis, Bosch, Hanwa, Panasonic, Sony, Hikvision, sowie ONVIF-kompatible Hardwaregeräte; die Benutzeroberfläche zeigt Ihnen jedoch direkt an, ob ein Modell unterstützt wird oder nicht. Sie können auch auf unserer Webseite gehen, um herauszufinden, ob ein bestimmtes Modell unterstützt wird: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> Für Geräte, die keine Gerätepasswortverwaltung unterstützen, müssen Sie das Passwort eines Hardwaregerätes von dessen Webseite aus ändern und dann das neue Passwort von Hand in Management Client eingeben. Weitere Informationen siehe Hardware bearbeiten auf Seite 200.

Sie können sich aussuchen, ob das System einzelne Passwörter für jedes Hardwaregerät erzeugen oder ob für alle Hardwaregeräte ein einziges, benutzerdefiniertes Passwort verwendet werden soll. Für Passwörter können ausschließlich druckbare ASCII-Zeichen verwendet werden.

Das System erzeugt Passwörter auf der Grundlage der Anforderungen des Herstellers der Hardwaregeräte.

Wenn Sie die neuen Passwörter anwenden, verlieren die Hardwaregeräte vorübergehend die Verbindung zum Aufzeichnungsserver.

Nachdem Sie die neuen Passwörter angewendet haben, erscheint auf dem Bildschirm das Ergebnis für jedes Hardwaregerät. Bei fehlgeschlagenen Änderungen wird der Grund für das Fehlschlagen angezeigt, wenn das Hardwaregerät solche Informationen unterstützt. Aus dem Assistenten heraus können Sie einen Bericht über erfolgreiche und fehlgeschlagene Passwortänderungen erstellen, die Ergebnisse werden jedoch auch unter **Serverprotokolle** protokolliert.

> Für Hardwaregeräte mit ONVIF-Treibern und mehreren Benutzerkonten kann nur ein Administrator von XProtect mit Administratorrechten für die Hardwaregeräte Passwörter aus dem VMS heraus ändern.

Weitere Informationen dazu, wie Passwörter in einem Vorgang geändert werden, siehe Passwörter auf Hardwaregeräten ändern auf Seite 209.

Passwörter auf Hardwaregeräten ändern

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

Sie können die Passwörter auf mehreren Hardwaregeräten auf einmal ändern. Weitere Informationen zu dieser Funktion sowie zu den unterstützten Modellen finden Sie unter Gerätepasswortverwaltung (Erklärung) auf Seite 208.

Anforderungen:

- Das Hardwaregerätemodell unterstützt die Gerätepasswortverwaltung durch Milestone.

Schritte:

1. Wählen Sie in dem Fenster **Seitennavigation** den Knoten **Aufzeichnungsserver** aus.
2. Klicken Sie mit der rechten Maustaste im Bereich Übersicht auf den entsprechenden Aufzeichnungsserver oder auf die jeweilige Hardware.
3. Wählen Sie **Hardwarepasswort ändern** aus. Ein Assistent wird angezeigt.
4. Folgen Sie zum Abschluss des Änderungen den Anweisungen auf dem Bildschirm.

   Das Feld **Zuletzt geändertes Passwort** zeigt den Zeitstempel der letzten Passwortänderung an, basierend auf den lokalen Zeiteinstellungen desjenigen Computers, von dem aus das Passwort geändert wurde.

5. Die letzte Seite zeigt das Ergebnis. Wenn das System ein bestimmtes Passwort nicht aktualisieren konnte, klicken Sie auf **Fehlgeschlagen** neben dem Hardwaregerät, um die Begründung angezeigt zu bekommen.
6. Sie können auch auf die Schaltfläche **Bericht drucken** klicken, um die vollständige Liste der erfolgreichen und fehlgeschlagenen Aktualisierungen angezeigt zu bekommen.
7. Wenn Sie das Passwort auf den Hardwaregeräten ändern möchten, die versagt haben, klicken Sie auf **Erneut versuchen**, und der Assistent beginnt erneut mit den Hardwaregeräten, die versagt haben.

   Wenn Sie auf **Erneut versuchen** klicken, können Sie nicht mehr auf den Bericht vom ersten Versuch zugreifen, als sie den Assistenten ausgeführt haben.

   Aufgrund der Sicherheitseinschränkungen können manche Hardwaregeräte vorübergehend nicht zur Verfügung stehen, wenn die Passwortänderung mehrmals hintereinander fehlschlägt. Die Sicherheitsbeschränkungen sind von Hersteller zu Hersteller unterschiedlich.

Firmware Update für ein Gerät (Erläuterung)

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

Management Client erlaubt Ihnen, die Firmware zu einer Hardware zu aktualisieren, die zu Ihrem VMS-System zugefügt wurde. Sie können die Firmware für mehrere Hardwaregeräte gleichzeitig aktualisieren, wenn diese mit derselben Firmwaredatei kompatibel sind.

Die Benutzeroberfläche zeigt Ihnen direkt an, ob ein Modell Firmware Updates unterstützt. Sie können auch auf die Webseite Milestone gehen, um herauszufinden, ob ein bestimmtes Modell unterstützt wird: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> Für Geräte, die keine Firmware Updates unterstützen, müssen Sie die Firmware des jeweiligen Hardwaregerätes von dessen Internetseite aus aktualisieren.

Wenn Sie die Firmware aktualisieren, verlieren die Hardwaregeräte vorübergehend die Verbindung zum Aufzeichnungsserver.

Wenn Sie die Firmware aktualisiert haben, erscheint auf dem Bildschirm das Ergebnis für jedes Hardwaregerät. Bei fehlgeschlagenen Änderungen wird der Grund für das Fehlschlagen angezeigt, wenn das Hardwaregerät solche Informationen unterstützt. Die Ergebnisse werden auch unter **Serverprotokolle** protokolliert.

> Für Hardwaregeräte mit ONVIF-Treibern und mehreren Benutzerkonten kann nur ein Administrator von XProtect mit Administratorrechten für das Hardwaregerät die Firmware aus dem VMS heraus aktualisieren.

Weitere Informationen dazu, wie Passwörter in einem Vorgang geändert werden, finden Sie unter Firmware auf einem Hardwaregerät aktualisieren auf Seite 211.

Firmware auf einem Hardwaregerät aktualisieren

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

Sie können die Firmware für mehrere Hardwaregeräte auf einmal ändern aktualisieren. Weitere Informationen zu dieser Funktion sowie zu den unterstützten Modellen finden Sie unter Firmware Update für ein Gerät (Erläuterung) auf Seite 210.

Anforderungen:

- Das Hardwaregerät unterstützt Firmware Updates von Milestone.

Schritte:

1. Wählen Sie in dem Fenster **Seitennavigation** den Knoten **Aufzeichnungsserver** aus.
2. Klicken Sie mit der rechten Maustaste im Bereich Übersicht auf den entsprechenden Aufzeichnungsserver oder auf die jeweilige Hardware.
3. Wählen Sie **Hardware-Firmware aktualisieren**. Ein Assistent wird angezeigt.
4. Folgen Sie zum Abschluss des Änderungen den Anweisungen auf dem Bildschirm.

Sie können die Firmware für mehrere Hardwaregeräte nur dann gleichzeitig aktualisieren, wenn diese mit derselben Firmwaredatei kompatibel sind. Hardware, die über den ONVIF-Treiber hinzugefügt wird, finden Sie unter **Sonstige**, und nicht unter dem Namen ihres Herstellers.

6. Die letzte Seite zeigt das Ergebnis. Wenn das System die Firmware nicht aktualisieren konnte, klicken Sie auf **Fehlgeschlagen** neben dem Hardwaregerät, um die Begründung angezeigt zu bekommen.

Milestone übernimmt keine Verantwortung für Fehlfunktionen von Hardwaregeräten, wenn eine inkompatible Firmwaredatei bzw. ein inkompatibles Hardwaregerät ausgewählt wurde.

Site-Navigation: Server und Hardware: Verwalten von Remote-Servern

Registerkarte „Info (Remote-Server)“

Name	Beschreibung
Name	Das System verwendet den Namen, wenn der Remote-Server im System und den Clients aufgelistet wird. Der Name muss nicht einzigartig sein. Wenn Sie einen Server neu benennen, wird der Name im Management Client global geändert.
Beschreibung	Geben Sie eine Beschreibung des Remote-Servers ein (optional). Die Beschreibung taucht in einer Anzahl Listen im System auf. Zum Beispiel, wenn Sie den Mauszeiger über den Hardware-Namen im Bereich **Übersicht** halten.
Modell	Zeigt das am Remote-System installierte XProtect-Produkt an.
Version	Zeigt die Version des Remote-Systeminstallation an.
Softwarelizenzcode	Der Softwarelizenzcode des Remote-Systeminstallation.
Treiber	Identifiziert den Treiber, der die Verbindung mit dem Remote-Server verwaltet.
Adresse	Hostname oder IP-Adresse der Hardware.

Name	Beschreibung
IE	Öffnet die Standard-Startseite des Hardware-Anbieters. Sie können diese Seite zur Administration der Hardware oder des Systems nutzen.
Remote-Systeminstallation-ID	Die einzigartige System-ID des Remote-Systeminstallation, die von XProtect verwendet wird, um beispielsweise Lizenzen zu verwalten.
Windows-Benutzername	Geben Sie den Windows-Benutzernamen ein, um Zugriff über den Remote-Desktop zu erhalten.
Windows-Passwort	Geben Sie das Windows-Passwort ein, um Zugriff über den Remote-Desktop zu erhalten.
Verbinden	Stellt eine Verbindung zum Remote-System her (wenn Windows-Anmeldeinformationen akzeptiert werden).

Registerkarte "Einstellungen" (Remote Server)

Auf der Registerkarte **Einstellungen** können Sie den Namen des entfernten Systems sehen.

Registerkarte „Ereignisse (Remote-Server)“

Sie können Ereignisse aus dem Remote-System in Ihrem zentralen Standort hinzufügen, um Regeln zu erstellen und dadurch sofort auf Ereignisse im Remote-Systeminstallation zu reagieren. Die Anzahl der Ereignisse hängt von den konfigurierten Ereignissen im Remote-Systeminstallation ab. Sie können Standardereignisse nicht löschen.

Falls die Liste unvollständig sein sollte:

1. Klicken Sie mit der rechten Maustaste auf den relevanten Remote-Server im Bereich **Übersicht** und wählen Sie **Hardware aktualisieren**.
2. Das Dialogfeld listet alle Änderungen (deinstallierte, aktualisierte und hinzugefügte Geräte) im Remote-Systeminstallation seit der Einrichtung oder letzten Aktualisierung der Milestone Interconnect-Einrichtung auf. Klicken Sie auf **Bestätigen**, um Ihren zentralen Standort mit diesen Änderungen zu aktualisieren.

Registerkarte „Fernabfrage“

Auf der Registerkarte **Fernabfrage** können Sie Einstellungen für Abfragen von Fernaufzeichnungen für den Remote-System in einer Milestone Interconnect-Einrichtung verwalten:

Legen Sie folgende Eigenschaften fest:

Name	Beschreibung
Aufzeichnungen abfragen bei max.	Bestimmt das Maximum der Bandbreite in Kbits/s für das Abfragen von Aufzeichnungen von einem Remote-System. Wählen Sie das Kontrollkästchen aus, um die Beschränkung von Abfragen zu aktivieren.
Aufzeichnungen abfragen zwischen	Bestimmt, dass Abfragen von Aufzeichnungen von einem Remote-System auf ein spezifisches Zeitintervall beschränkt sind. Unvollendete Anfragen werden auch zur Endzeit fortgesetzt, bis sie vollendet wurden. Ist die Endzeit also kritisch, muss sie auf einen früheren Zeitpunkt gelegt werden, damit unvollendete Anfragen vollendet werden können. Wenn das System automatisch abgefragt wird oder eine Abfrageanfrage vom XProtect Smart Client außerhalb des Zeitintervalls erhält, wird sie akzeptiert, aber erst gestartet, wenn das ausgewählte Zeitintervall beginnt. Sie können ausstehende, von den Benutzern initiierte Remote-Aufzeichnungs-Abfrageanfragen über **System-Dashboard** -> **Aktuelle Aufgaben** anzeigen.
Parallel auf Geräten abfragen	Bestimmt die maximale Anzahl der Geräte, von denen Aufzeichnungen simultan abgefragt werden. Ändern Sie den Standardwert, wenn Sie mehr oder weniger Kapazität benötigen, abhängig von Ihren Systemkapazitäten.

Wenn Sie die Einstellungen ändern, dauert es möglicherweise mehrere Minuten, bis die Änderungen im System widergespiegelt werden.

Keine der obigen Aussagen trifft auf die direkte Wiedergabe von Fernaufzeichnungen zu. Alle Kameras, die direkt wiedergegeben werden sollen, sind zur direkten Wiedergabe verfügbar und nutzen Bandbreite nach Bedarf.

Site-Navigation: Geräte: Arbeiten mit Geräten

Die Geräte werden in der Management Client angezeigt, wenn Sie Hardware mit dem **Hardware hinzufügen**-Assistenten hinzufügen.

Sie können Geräte mittels Gerätegruppen verwalten, wenn diese die gleichen Eigenschaften besitzen. Siehe Site-Navigation: Geräte: Verwendung von Gerätegruppen auf Seite 224.

Sie können die Geräte auch einzeln verwalten:

- Kameras
- Mikrofone
- Lautsprecher
- Metadaten
- Eingänge
- Ausgaben

Geräte (Erklärung)

Hardware verfügt über eine Anzahl Geräte, die Sie einzeln verwalten können, wie zum Beispiel:

- Eine physische Kamera verfügt über Geräte, die den Kamerateil repräsentieren (Objektive), sowie Mikrofone, Lautsprecher, Metadaten, Eingang und Ausgang, ob angefügt oder eingebaut
- Ein Videoencoder ist mit mehreren analogen Kameras verbunden, die in einer Geräteliste auftauchen, welche den Kamerateil repräsentieren (Objektive), sowie Mikrofone, Lautsprecher, Metadaten, Eingang und Ausgang, ob angefügt oder eingebaut
- Ein I/O-Modul verfügt über Geräte, die die Eingangs- und Ausgangskanäle für beispielsweise Lampen repräsentieren
- Ein zugehöriges Audio-Modul verfügt über Geräte, die Mikrofone und Lautsprecher-Ein- und -Ausgänge repräsentieren
- In einer Milestone Interconnect-Einrichtung erscheint das System in einer einzigen Liste als Hardware mit allen Geräten aus der Remote-Systeminstallation-Liste

Das System fügt der Hardware zugehörige Geräte automatisch hinzu, wenn Sie die Hardware hinzufügen.

Informationen über unterstütze Hardware finden Sie auf der Seite für unterstützte Hardware auf der Milestone-Website (https://www.milestonesys.com/supported-devices/).

Die folgenden Abschnitte beschreiben alle Gerätetypen mit Links zu den Registerkarten, die Sie zu ihrer Verwaltung brauchen.

Kamerageräte (Erklärung)

Kamerageräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen, und sind standardmäßig aktiviert.

Kamerageräte senden Videostreams an das System, das die Clientbenutzer verwenden können, um Live-Video anzuzeigen oder damit das System für spätere Wiedergaben durch die Clientbenutzer aufzeichnen kann. Rollen bestimmen das Recht von Benutzern, Video anzuzeigen.

Informationen über unterstütze Hardware finden Sie auf der Seite für unterstützte Hardware auf der Milestone-Website (https://www.milestonesys.com/supported-devices/).

Das System wird mit einer Standardregel zum Start von Feeds geliefert, die sicherstellt, dass Videofeeds von allen verbundenen Kameras automatisch an das System übertragen werden. Genau wie andere Regeln kann die Standardregel deaktiviert und/oder nach Bedarf modifiziert werden.

Die Aktivierung/Deaktivierung und Umbenennung einzelner Geräte finden auf der Aufzeichnungsserver-Hardware statt. Siehe Aktivieren/Deaktivieren von Geräten über Gerätegruppen auf Seite 222.

Erweitern Sie für jegliche andere Konfiguration und Verwaltung von Kameras **Geräte** im Bereich „Standort-Navigation“ und wählen Sie **Kameras**. Gruppieren Sie im Bereich „Übersicht“ Ihre Kameras, um einen guten Überblick über sie zu erhalten. Die erste Gruppierung findet im Rahmen des Assistenten **Hardware hinzufügen** statt.

Befolgen Sie diese Konfigurationsreihenfolge, um die typischsten Aufgaben im Bereich der Konfiguration eines Kameragerätes auszuführen:

1. Konfigurieren von Kameraeinstellungen (siehe Registerkarte „Einstellungen“ (Geräte) auf Seite 230).
2. Konfigurieren von Streams (siehe Registerkarte „Streams“ (Geräte) auf Seite 232).
3. Bewegung konfigurieren (siehe die Registerkarte Registerkarte „Bewegung“ (Geräte) auf Seite 243).
4. Aufzeichnung konfigurieren (siehe die Registerkarte Registerkarte „Aufzeichnen“ (Geräte) auf Seite 235).
5. Konfigurieren Sie die restlichen Einstellungen nach Bedarf.

Mikrofongeräte (Erklärung)

An viele Geräte lassen sich externe Mikrofone anfügen. Einige Geräte verfügen über eingebaute Mikrofone.

Mikrofongeräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen. Sie sind standardmäßig nicht aktiviert, daher müssen Sie diese also vor Verwendung entweder während der Anwendung des **Hardware hinzufügen**-Assistenten oder danach aktivieren. Mikrofone benötigen keine separaten Lizenzen. Sie können so viele Mikrofone in Ihrem System anwenden wie nötig.

Sie können Mikrofone vollkommen unabhängig von Kameras verwenden.

Mikrofongeräte senden Audiostreams an das System, das die Clientbenutzer verwenden können, um Live-Audio anzuhören oder damit das System für spätere Wiedergaben durch die Clientbenutzer aufzeichnen kann. Sie können das System so einrichten, dass es mikrofonspezifische Ereignisse empfängt, die relevante Aktionen auslösen.

Informationen über unterstütze Hardware finden Sie auf der Seite für unterstützte Hardware auf der Milestone-Website (https://www.milestonesys.com/supported-devices/).

Rollen bestimmen das Recht von Benutzern, Mikrofone abzuhören. Sie können Mikrofone nicht vom Management Client abhören.

Das System wird mit einer Standardregel zum Start von Audiofeeds geliefert, die sicherstellt, dass Audiofeeds von allen verbundenen Mikrofonen automatisch an das System übertragen werden. Genau wie andere Regeln kann die Standardregel deaktiviert und/oder nach Bedarf modifiziert werden.

Die Aktivierung/Deaktivierung und Umbenennung einzelner Geräte finden auf der Aufzeichnungsserver-Hardware statt. Für weitere Informationen siehe Aktivieren/Deaktivieren von Geräten über Gerätegruppen auf Seite 222.

Erweitern Sie für jegliche andere Konfiguration und Verwaltung von Kameras **Geräte** im Bereich „Standort-Navigation“ und wählen Sie **Mikrofone**. Gruppieren Sie im Bereich „Übersicht“ Ihre Mikrofone, um einen guten Überblick über sie zu erhalten. Die erste Gruppierung findet im Rahmen des Assistenten **Hardware hinzufügen** statt.

Sie können Mikrofongeräte in den folgenden Registerkarten konfigurieren:

- Registerkarte Info (siehe Registerkarte „Info (Geräte)“ auf Seite 227)
- Registerkarte 'Einstellungen' (siehe die Registerkarte Registerkarte „Einstellungen“ (Geräte) auf Seite 230).
- Registerkarte 'Aufzeichnung' (siehe die Registerkarte Registerkarte „Aufzeichnen“ (Geräte) auf Seite 235)
- Registerkarte 'Ereignisse' (siehe die Registerkarte Registerkarte „Ereignisse“ (Geräte) auf Seite 268)

Lautsprecher-Geräte (Erklärung)

An viele Geräte lassen sich externe Lautsprecher anfügen. Einige Geräte verfügen über eingebaute Lautsprecher.

Lautsprechergeräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen. Sie sind standardmäßig nicht aktiviert, daher müssen Sie diese also vor Verwendung entweder während der Anwendung des **Hardware hinzufügen**-Assistenten oder danach aktivieren. Lautsprecher benötigen keine separaten Lizenzen. Sie können so viele Lautsprecher in Ihrem System nutzen wie nötig.

Sie können Lautsprecher vollkommen unabhängig von Kameras verwenden.

Informationen über unterstütze Hardware finden Sie auf der Seite für unterstützte Hardware auf der Milestone-Website (https://www.milestonesys.com/supported-devices/).

Das System versendet einen Audiostream an die Lautsprecher, wenn ein Benutzer im XProtect Smart Client die Sprechtaste drückt. Lautsprecheraudio wird nur aufgenommen, wenn ein Benutzer spricht. Rollen bestimmen das Recht von Benutzern, über Lautsprecher zu sprechen. Sie können vom Management Client nicht über Lautsprecher sprechen.

Wenn zwei Benutzer zum selben Zeitpunkt sprechen möchten, bestimmen ihre Rollen ihr Recht, über Lautsprecher zu sprechen. Sie können als Teil der Rollendefinierung Prioritäten für Sprecher festlegen, die von sehr hoch bis sehr niedrig reichen. Wenn zwei Benutzer zum selben Zeitpunkt sprechen möchten, erhält der Benutzer mit der Rolle, welche die höchste Priorität hat, die Gelegenheit zu sprechen. Wenn zwei Benutzer mit derselben Rolle gleichzeitig sprechen möchten, wird nach dem Windhundprinzip verfahren.

Das System wird mit einer Standardregel zum Start von Audiofeeds geliefert, durch die das Gerät gestartet wird, sodass es bereit ist, benutzeraktiviertes Audio an die Lautsprecher zu versenden. Genau wie andere Regeln kann die Standardregel deaktiviert und/oder nach Bedarf modifiziert werden.

Die Aktivierung/Deaktivierung und Umbenennung einzelner Geräte finden auf der Aufzeichnungsserver-Hardware statt. Siehe Aktivieren/Deaktivieren von Geräten über Gerätegruppen auf Seite 222.

Erweitern Sie für jegliche andere Konfiguration und Verwaltung von Kameras **Geräte** im Bereich Standort-Navigation und wählen Sie **Lautsprecher**. Gruppieren Sie im Bereich Übersicht Ihre Lautsprecher, um einen guten Überblick über sie zu haben. Die erste Gruppierung findet im Rahmen des Assistenten **Hardware hinzufügen** statt.

Sie können Lautsprechergeräte in den folgenden Registerkarten konfigurieren:

- Registerkarte „Info (Geräte)“ auf Seite 227
- Registerkarte „Einstellungen“ (Geräte) auf Seite 230
- Registerkarte „Aufzeichnen“ (Geräte) auf Seite 235

Metadaten-Geräte (Erklärung)

Metadatengeräte versenden Datenstreams an das System, das die Client-Benutzer verwenden können, um Daten zu Daten anzuzeigen, zum Beispiel Daten, die das Videobild, den Inhalt, Objekte im Bild oder den Ort beschreiben, an dem das Bild aufgezeichnet wurde. Metadaten können an Kameras, Mikrofone oder Lautsprecher angehängt werden.

Metadaten können erzeugt werden von:

- Das Gerät, das selbst die Daten liefert, z. B. eine Kamera, die Videoaufzeichnungen liefert
- Einem Drittsystem oder Integration über einen generischen Metadatentreiber

Die durch das Gerät erzeugten Metadaten werden automatisch mit einem oder mehreren Geräten derselben Hardware verknüpft.

Informationen über unterstütze Hardware finden Sie auf der Seite für unterstützte Hardware auf der Milestone-Website (https://www.milestonesys.com/supported-devices/).

Rollen bestimmen das Recht von Benutzern, Metadaten anzuzeigen.

Das System wird mit einer Standardregel zum Start von Feeds geliefert, die sicherstellt, dass Metadatenfeeds von Hardware, die Metadaten unterstützt, automatisch ins System übertragen werden. Genau wie andere Regeln kann die Standardregel deaktiviert und/oder nach Bedarf modifiziert werden.

Die Aktivierung/Deaktivierung und Umbenennung einzelner Geräte finden auf der Aufzeichnungsserver-Hardware statt. Für weitere Informationen siehe Aktivieren/Deaktivieren von Geräten über Gerätegruppen auf Seite 222.

Erweitern Sie für jegliche andere Konfiguration und Verwaltung von Metadatengeräten **Geräte** im Bereich „Standort-Navigation“ und wählen Sie **Metadaten**. Gruppieren Sie im Bereich „Übersicht“ Ihre Metadatengeräte, um einen guten Überblick über sie zu haben. Die erste Gruppierung findet im Rahmen des Assistenten **Hardware hinzufügen** statt.

Sie können Metadatengeräte in den folgenden Registerkarten konfigurieren:

- Registerkarte Info (siehe Registerkarte „Info (Geräte)“ auf Seite 227)
- Registerkarte 'Einstellungen' (siehe die Registerkarte Registerkarte „Einstellungen“ (Geräte) auf Seite 230).
- Registerkarte 'Aufzeichnung' (siehe die Registerkarte Registerkarte „Aufzeichnen“ (Geräte) auf Seite 235)

Eingabegeräte (Erklärung)

An viele Geräte lassen sich externe Einheiten an Eingangsports anfügen. Eingabegeräte sind normalerweise externe Sensoren. Solche externen Sensoren können beispielsweise genutzt werden, um zu registrieren, ob Türen, Fenster oder Tore geöffnet werden. Eingaben über diese externen Eingabegeräte werden vom System als Ereignisse angesehen.

Sie können diese Ereignisse in Regeln verwenden. Beispielsweise können Sie eine Regel erstellen, in der bestimmt wird, dass eine Kamera die Aufzeichnung startet, wenn eine Eingabe aktiviert wird, und 30 Sekunden nach Deaktivierung der Eingabe die Aufnahme beendet.

Sie können Eingabegeräte vollkommen unabhängig von Kameras verwenden.

> Überprüfen Sie vor der Verwendung eines externen Eingabegeräts mit einem Gerät, dass das Gerät den Sensorbetrieb erkennt. Bei den meisten Geräten wird dies auf der Konfigurationsoberfläche oder über Common-Gateway-Interface-Skriptbefehle (CGI) angezeigt.

Eingabegeräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen. Sie sind standardmäßig nicht aktiviert, daher müssen Sie diese also vor Verwendung entweder während der Anwendung des **Hardware hinzufügen**-Assistenten oder danach aktivieren. Eingabegeräte benötigen keine separaten Lizenzen. Sie können so viele Eingabegeräte in Ihrem System anwenden wie nötig.

> Informationen über unterstütze Hardware finden Sie auf der Seite für unterstützte Hardware auf der Milestone-Website (https://www.milestonesys.com/supported-devices/).

Die Aktivierung/Deaktivierung und Umbenennung einzelner Geräte finden auf der Aufzeichnungsserver-Hardware statt. Siehe Aktivieren/Deaktivieren von Geräten über Gerätegruppen auf Seite 222.

Erweitern Sie für jegliche andere Konfiguration und Verwaltung von Kameras **Geräte** im Bereich „Standort-Navigation“ und wählen Sie **Eingang**. Gruppieren Sie im Bereich „Übersicht“ Ihre Eingabegeräte, um einen guten Überblick über sie zu haben. Die erste Gruppierung findet im Rahmen des Assistenten **Hardware hinzufügen** statt.

Sie können Eingabegeräte in den folgenden Registerkarten konfigurieren:

- Registerkarte Info (siehe Registerkarte „Info (Geräte)“ auf Seite 227)
- Registerkarte 'Einstellungen' (siehe die Registerkarte Registerkarte „Einstellungen“ (Geräte) auf Seite 230).
- Registerkarte 'Ereignisse' (siehe die Registerkarte Registerkarte „Ereignisse“ (Geräte) auf Seite 268)

Manuelle Eingabeaktivierung zum Test

Mit der Regelfunktion können Sie Regeln definieren, die Eingaben automatisch aktivieren oder deaktivieren. Sie können sie aber auch manuell aktivieren und das Ergebnis im Management Client überprüfen:

1. Wählen Sie im Bereich **Übersicht** das relevante Eingabegerät.
2. Aktivieren Sie die Eingabe auf dem physischen Gerät.
3. Sehen Sie im Bereich **Vorschau** nach, ob die Anzeige grün aufleuchtet. Trifft dies zu, funktioniert das Eingabegerät.

Ausgabegeräte (Erklärung)

An viele Geräte lassen sich externe Einheiten an Ausgangsports anfügen. Hierdurch können Sie Lampen, Sirenen etc. über das System aktivieren/deaktivieren.

Sie können Ausgabe bei der Erstellung von Regeln nutzen. Sie können Regeln erstellen, die Ausgaben automatisch aktivieren oder deaktivieren, und Regeln, die Aktionen auslösen, wenn der Status einer Ausgabe verändert wird.

Ausgabe kann über Management Client und XProtect Smart Client manuell ausgelöst werden.

> Überprüfen Sie vor der Verwendung eines externen Ausgabegeräts mit einem Gerät, dass dieses Gerät das am Ausgang angebrachte Gerät steuern kann. Bei den meisten Geräten wird dies auf der Konfigurationsoberfläche oder über Common-Gateway-Interface-Skriptbefehle (CGI) angezeigt.

Ausgabegeräte werden automatisch hinzugefügt, wenn Sie Hardware zum System hinzufügen. Sie sind standardmäßig nicht aktiviert, daher müssen Sie diese also vor Verwendung entweder während der Anwendung des **Hardware hinzufügen**-Assistenten oder danach aktivieren. Ausgabegeräte benötigen keine separaten Lizenzen. Sie können so viele Ausgabegeräte in Ihrem System anwenden wie nötig.

Informationen über unterstütze Hardware finden Sie auf der Seite für unterstützte Hardware auf der Milestone-Website (https://www.milestonesys.com/supported-devices/).

Die Aktivierung/Deaktivierung und Umbenennung einzelner Geräte finden auf der Aufzeichnungsserver-Hardware statt. Siehe Aktivieren/Deaktivieren von Geräten über Gerätegruppen auf Seite 222.

Erweitern Sie für jegliche andere Konfiguration und Verwaltung von Kameras **Geräte** im Bereich „Standort-Navigation“ und wählen Sie **Ausgang**. Gruppieren Sie im Bereich „Übersicht“ Ihre Eingabegeräte, um einen guten Überblick über sie zu haben. Die erste Gruppierung findet im Rahmen des Assistenten **Hardware hinzufügen** statt.

Sie können Ausgabegeräte in den folgenden Registerkarten konfigurieren:

- Registerkarte „Info (Geräte)“ auf Seite 227
- Registerkarte „Einstellungen“ (Geräte) auf Seite 230

Manuelle Ausgabeaktivierung zum Test

Mit der Regelfunktion können Sie Regeln definieren, die Ausgaben automatisch aktivieren oder deaktivieren. Sie können sie aber auch manuell über einen Client aktivieren.

Sie können eine Ausgabe manuell über den Management Client aktivieren, um die Funktionalität zu testen:

1. Wählen Sie im Bereich **Übersicht** das relevante Ausgabegerät.
2. Im Bereich **Vorschau** werden üblicherweise folgende Elemente für jede Ausgabe angezeigt:

3. Wählen Sie das Kontrollkästchen an/ab, um die ausgewählte Ausgabe zu aktivieren/deaktivieren. Wenn eine Ausgabe aktiviert wird, leuchtet die Anzeige grün auf:

4. Alternativ können Sie auf die rechteckige Schaltfläche klicken, um die Ausgabe für die in der Einstellung **Ausgabe-Auslösungszeitpunkt** auf der Registerkarte **Einstellungen** festgelegte Dauer manuell zu aktivieren (diese Funktion/Einstellung ist möglicherweise nicht für alle Ausgaben verfügbar). Nach der festgelegten Dauer wird die Ausgabe automatisch deaktiviert.

Aktivieren/Deaktivieren von Geräten über Gerätegruppen

Sie können Geräte nur über die konfigurierte Hardware aktivieren/deaktivieren. Wenn sie nicht über den „Hardware hinzufügen"-Assistenten aktiviert/deaktiviert wurden, sind Kameragеräte standardmäßig aktiviert und alle anderen Geräte standardmäßig deaktiviert.

So finden Sie ein Gerät über die zu aktivierenden/deaktivierenden Gerätegruppen:

1. Wählen Sie im Bereich **Standort-Navigation** das Gerät aus.
2. Erweitern Sie im Bereich **Übersicht** die relevante Gruppe und suchen Sie das Gerät.
3. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie **Gehe zu Hardware**.
4. Klicken Sie auf den Plus-Knoten, um alle Geräte auf der Hardware anzuzeigen.
5. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie aktivieren/deaktivieren möchten, und wählen Sie **Aktiviert**.

Statussymbole von Geräten

Wenn Sie ein Gerät auswählen, werden Informationen zu seinem aktuellen Status im Bereich **Vorschau** angezeigt. Die folgenden Symbole zeigen den Status der Geräte an:

Kamera	Mikrofon	Sprecher	Metadaten	Eingang	Ausgang	Beschreibung
						Gerät aktiviert und empfängt Daten: Das Gerät

Kamera	Mikrofon	Sprecher	Metadaten	Eingang	Ausgang	Beschreibung
						ist aktiviert und Sie empfangen einen Live-Stream.
						**Gerät zeichnet auf**: Das Gerät zeichnet Daten im System auf.
						**Gerät temporär angehalten oder ohne Feed**: Es werden keine Informationen ans System übertragen. Bei einer Kamera können Sie kein Live-Video ansehen. Ein angehaltenes Gerät kann im Gegensatz zu einem deaktivierten Gerät noch mit dem Aufzeichnungsserver kommunizieren, um Ereignisse abzufragen, Einstellungen festzulegen usw.
						**Geräte deaktiviert**: Kann nicht automatisch durch eine Regel gestartet werden und kann nicht mit dem Aufzeichnungsserver kommunizieren. Wenn eine Kamera deaktiviert ist, können Sie keine Live-Videos oder Aufzeichnungen ansehen.
						**Gerätedatenbank wird repariert**.
						**Gerät benötigt Aufmerksamkeit**: Das Gerät

Kamera	Mikrofon	Sprecher	Metadaten	Eingang	Ausgang	Beschreibung
						funktioniert nicht richtig. Halten Sie den Mauszeiger über das Gerätesymbol, um eine Beschreibung des Problems im Tooltip zu erhalten.
						**Status unbekannt**: Status des Geräts ist unbekannt, wenn zum Beispiel der Aufzeichnungsserver offline ist.
						Einige Symbole können in Kombination auftreten, wie in folgendem Beispiel: **Gerät aktiviert und empfängt Daten** und **Gerät zeichnet auf**.

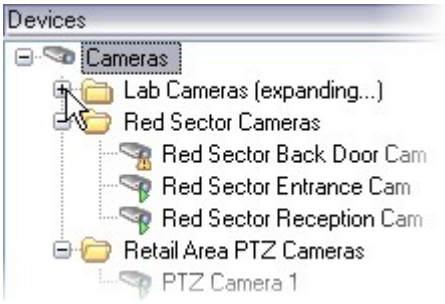
Site-Navigation: Geräte: Verwendung von Gerätegruppen

Das Zusammenfügen von Geräten in Gerätegruppen ist Teil des **Hardware hinzufügen**-Assistenten. Sie können allerdings die Gruppen jederzeit verändern oder bei Bedarf neue Gruppen hinzufügen.

Ein Zusammenfügen verschiedener Gerätetypen (Kameras, Mikrofone, Lautsprecher, Metadaten, Eingänge und Ausgänge) in Gruppen kann für Ihr System von Vorteil sein:

- Gerätegruppen bieten eine intuitive Übersicht der Geräte in Ihrem System
- Geräte können zu mehreren Gruppen gehören
- Sie können Untergruppen und Untergruppen innerhalb von Untergruppen erstellen
- Sie können allgemeine Eigenschaften für alle Geräte in einer Gerätegruppe gleichzeitig festlegen
- Geräteeigenschaften, die mittels der Gruppe festgelegt werden, gelten für die einzelnen Geräte und nicht für die Gruppe
- Bezüglich Rollen können Sie allgemeine Sicherheitseinstellungen für alle Geräte in einer Gerätegruppe gleichzeitig festlegen
- Sie können eine Regel für alle Geräte in einer Gerätegruppe gleichzeitig festlegen

Sie können so viele Gerätegruppen erstellen, wie Sie benötigen, jedoch nicht verschiedene Gerätetypen (z. B. Kameras und Lautsprecher) in einer Gerätegruppe vermischen.



Erstellen Sie Gerätegruppen mit **weniger** als 400 Geräten, um alle Eigenschaften anzeigen und bearbeiten zu können.

Wenn Sie eine Gerätegruppe löschen, entfernen Sie nur die Gerätegruppe selbst. Wenn Sie ein Gerät, beispielsweise eine Kamera, aus Ihrem System entfernen möchten, sollten Sie dies auf der Ebene des Aufzeichnungsservers tun.

Die folgenden Beispiele beziehen sich auf das Zusammenführen von Kameras in Gerätegruppen, aber das Prinzip gilt für alle Geräte:

Eine Gerätegruppe hinzufügen auf Seite 225

Bestimmen, welche Geräte die Gruppe beinhalten soll auf Seite 226

Bestimmen Sie die allgemeinen Eigenschaften für alle Geräte in einer Gerätegruppe auf Seite 226

Eine Gerätegruppe hinzufügen

1. Klicken Sie im **Übersicht** Fenster mit der rechten Maustaste auf den Gerätetypen unter dem Sie eine Gerätegruppe erstellen möchten.
2. Wählen Sie **Gerätegruppe hinzufügen**.
3. Im Dialogfenster **Gerätegruppe hinzufügen** können Sie Namen und Beschreibung der neuen Gerätegruppe festlegen:

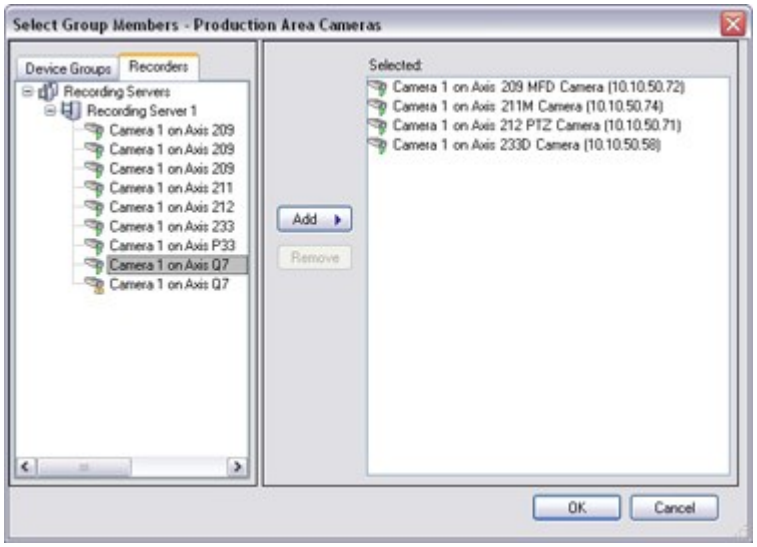
Die Beschreibung erscheint, wenn sie den Mauszeiger über die Gerätegruppe in der Gerätegruppenliste halten.

4. Klicken Sie auf **OK**. Ein Ordner für die neue Gerätegruppe erscheint in der Liste.
5. Fahren Sie damit fort, festzulegen, welche Geräte zu einer Gerätegruppe gehören sollen (siehe Bestimmen, welche Geräte die Gruppe beinhalten soll auf Seite 226).

Bestimmen, welche Geräte die Gruppe beinhalten soll

1. Klicken Sie im **Übersicht** Fenster mit der rechten Maustaste auf den zugehörigen Gerätegruppen-Ordner.
2. Wählen Sie **Mitglieder der Gerätegruppe bearbeiten**.
3. Im Fenster **Gruppenmitglieder auswählen**, wählen Sie eine der Registerkarten, um den Standort des Geräts festzustellen.

   Ein Gerät kann Mitglied mehrerer Gerätegruppen sein.
4. Wählen Sie die einzuschließenden Geräte aus, und klicken Sie auf **Hinzufügen** oder machen Sie einen Doppelklick auf das Gerät:



5. Klicken Sie auf **OK**.
6. Wenn Sie die Begrenzung von 400 Geräten in einer Gruppe überschreiten, können Sie Untergruppen zu den Gerätegruppen hinzufügen:

Bestimmen Sie die allgemeinen Eigenschaften für alle Geräte in einer Gerätegruppe

Bei Gerätegruppen können Sie allgemeine Eigenschaften für alle Geräte in einer Gerätegruppe festlegen:

1. Klicken Sie auf die Gerätegruppe im **Übersicht** Bereich.

   Unter **Eigenschaften** sind alle Eigenschaften, **die für alle Geräte der Gruppe verfügbar sind** aufgelistet und in Registerkarten unterteilt.

2. Bestimmen Sie die allgemeinen Eigenschaften.

   In der **Einstellungen**-Registerkarte können Sie zwischen den Einstellungen für **alle** Geräte und Einstellungen für einzelne Geräte wechseln.

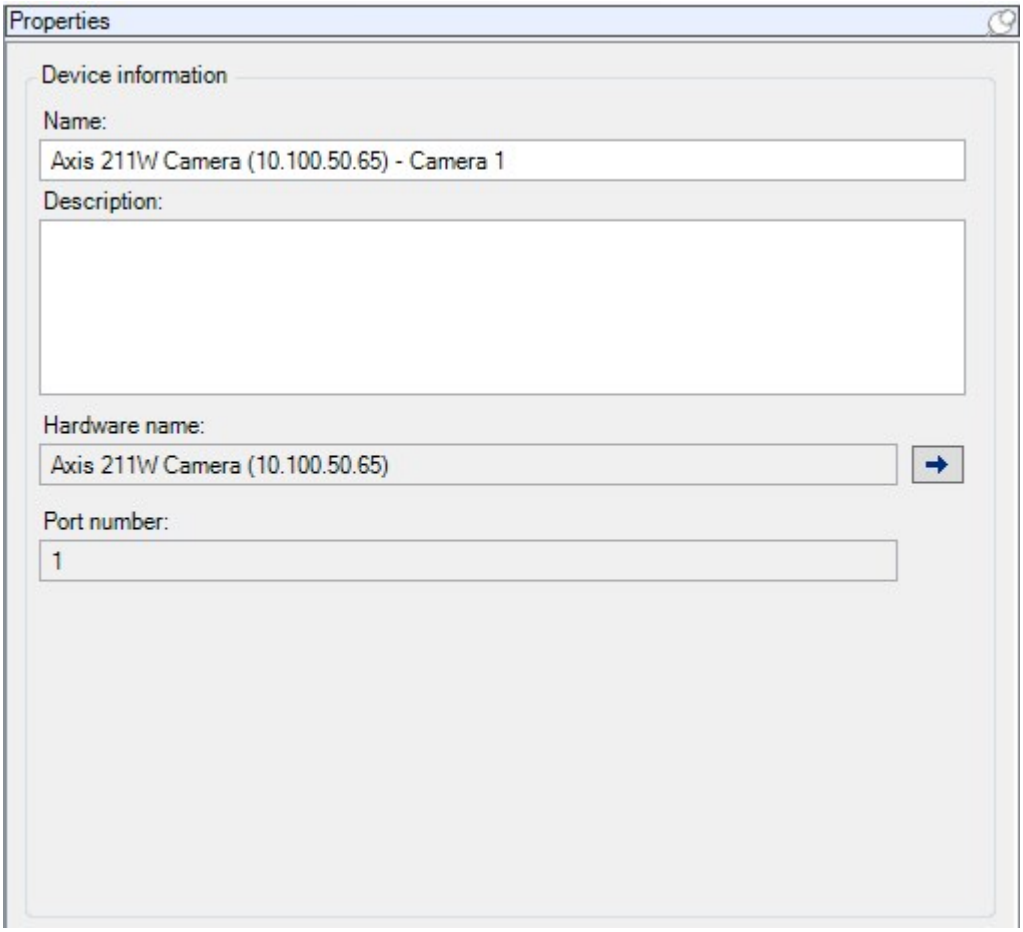
3. Klicken Sie in der Symbolleiste auf **Speichern**. Die Einstellungen werden auf den einzelnen Geräten und nicht in den Gerätegruppen gespeichert.

Site-Navigation: Registerkarten für Geräte

Registerkarte „Info (Geräte)“

Registerkarte Info (Erklärung)

Auf der Registerkarte **Info** können Sie grundlegende Geräteinformationen in einer Anzahl Felder anzeigen und bearbeiten.
Alle Geräte verfügen über eine **Info**-Registerkarte.



Registerkarte „Info“ (Eigenschaften)

Name	Beschreibung
Name	Der Name wird verwendet, wenn das Gerät im System und den Clients aufgelistet ist. Wenn Sie ein Gerät neu benennen, wird der Name im Management Client global geändert.
Beschreibung	Geben Sie eine Beschreibung des Geräts ein (optional). Die Beschreibung taucht in einer Anzahl Listen im System auf. Zum Beispiel, wenn Sie den Mauszeiger über den Namen im Bereich **Übersicht** halten.

Name	Beschreibung
Hardware-Name	Zeigt den Namen der Hardware an, mit der das Gerät verbunden ist. Das Feld kann von hier aus nicht bearbeitet werden, Sie können es jedoch verändern, indem Sie daneben auf **Gehe zu** klicken. So gelangen Sie zu den Hardware-Informationen, wo Sie den Namen ändern können.
Portnummer	Zeigt den Port an, über den das Gerät an der Hardware angebracht ist. Die Portnummer für Einzelgeräte-Hardware ist normalerweise **1**. Die Portnummer für Mehrfachgeräte-Hardware, wie etwa Video-Server mit mehreren Kanälen, zeigt normalerweise den Kanal an, über den das Gerät angebracht ist, zum Beispiel **3**.
Kurzbezeichnung	Geben Sie hier eine Kurzbezeichnung für die Kamera ein. Die maximale Zeichenanzahl beträgt 128. Wenn Sie Smart Map verwenden, wird die Kurzbezeichnung automatisch mit der Kamera auf der Smart Map angezeigt. Anderenfalls wird der vollständige Name angezeigt.
Geokoordinaten	Geben Sie den geografischen Standort der Kamera im Format **Breitengrad, Längengrad** ein. Der eingegebene Wert bestimmt die Position des Kamerasymbols auf der Smart Map im XProtect Smart Client.  Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen.
Richtung	Geben Sie die Blickrichtung der Kamera in Bezug auf eine genau nach Norden zeigende vertikale Achse an. Der eingegebene Wert bestimmt die Richtung des Kamerasymbols auf der Smart Map im XProtect Smart Client. Der Standardwert ist 0,0.  Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen.
Sichtfeld	Geben Sie das Sichtfeld in Grad ein. Der eingegebene Wert bestimmt das Sichtfeld des Kamerasymbols auf der Smart Map im XProtect Smart Client. Der Standardwert ist 0,0.

Name	Beschreibung
	Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen.
Tiefe	Geben Sie die Tiefe der Kamera in Metern oder Fuß ein. Der eingegebene Wert bestimmt die Tiefe des Kamerasymbols auf der Smart Map im XProtect Smart Client. Der Standardwert ist 0,0. Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen.
Positionsvorschau im Browser	Klicken Sie auf die Schaltfläche, um zu überprüfen, ob Sie die richtigen geographischen Koordinaten eingegeben haben. Google Maps öffnet sich an der von Ihnen angegebenen Position in Ihrem Standard-Webbrowser. Das Feld dient hauptsächlich für Smart Map und Drittanbieterintegrationen.

Registerkarte „Einstellungen“ (Geräte)

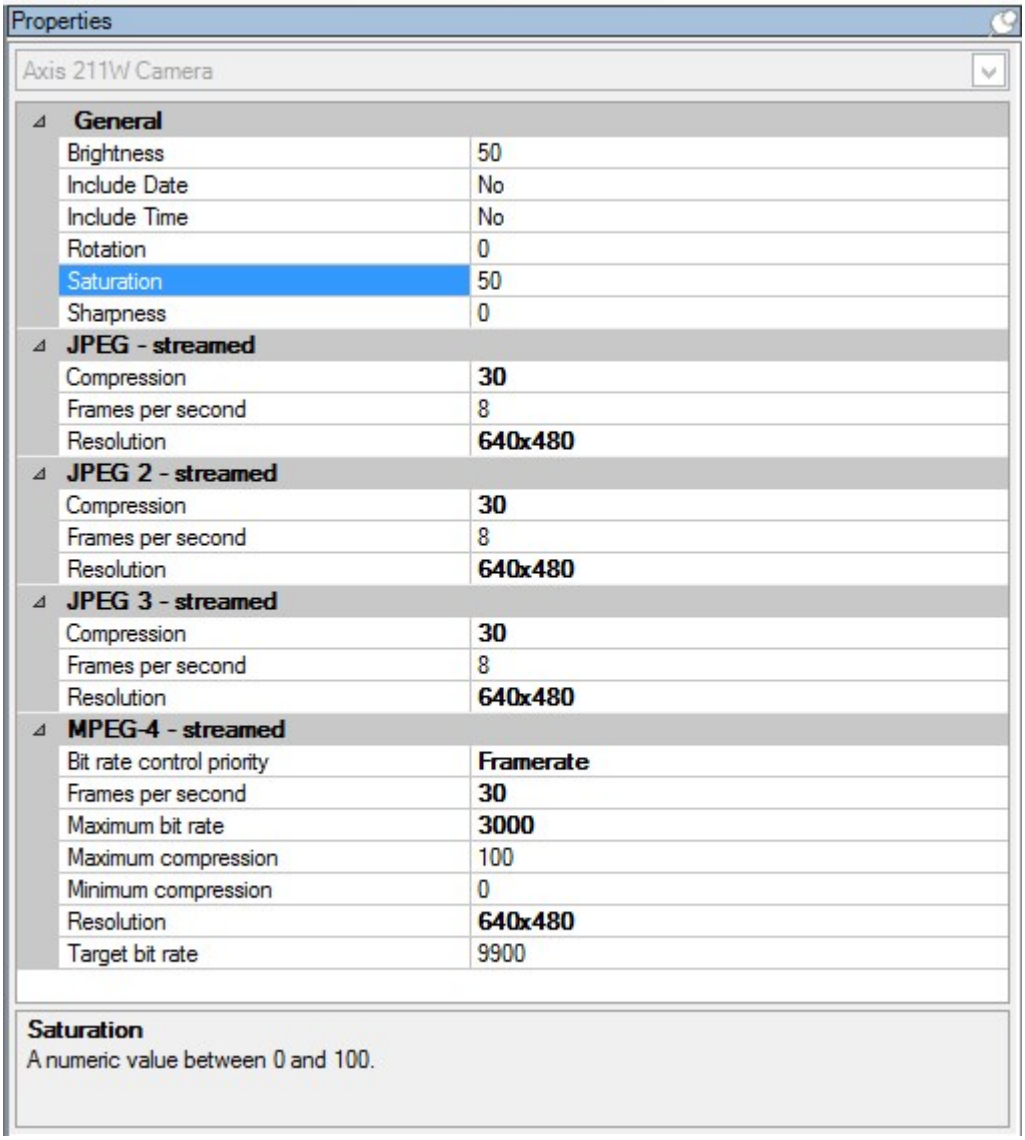
Registerkarte Einstellungen (Erklärung)

Auf der Registerkarte **Einstellungen** können Sie Geräteeinstellungen in einer Anzahl Felder anzeigen und bearbeiten.
Alle Geräte verfügen über eine **Einstellungen**-Registerkarte.

Die Werte erscheinen veränderlich oder schreibgeschützt in einer Tabelle. Wenn Sie eine Einstellung auf einen Nichtstandardwert setzen, erscheint der Wert in Fettdruck.

Der Inhalt der Tabelle hängt vom Gerätetreiber ab.

Erlaubte Bereiche tauchen im Informationsfenster unter der Einstellungstabelle auf:



Kamera-Einstellungen (Erklärung)

Sie können Einstellungen anzeigen oder bearbeiten, wie etwa:

- Standardbildrate
- Auflösung
- Komprimierung
- Die maximale Anzahl an Bildern zwischen Keyframes
- Bildschirmanzeige Datum/Uhrzeit/Text für eine ausgewählte Kamera oder für alle Kameras in einer Gerätegruppe

Die Kameratreiber bestimmen den Inhalt der Registerkarte **Einstellungen**. Die Treiber variieren je nach Kameratyp.

Für Kameras, die mehr als ein Streamformat unterstützen, zum Beispiel MJPEG und MPEG-4/H.264/H.265, können Sie Multi-Streaming nutzen, siehe Multistreaming (Erklärung) auf Seite 233.

Wenn Sie eine Einstellung verändern müssen, können Sie die Auswirkungen schnell überprüfen, wenn Sie den Bereich **Vorschau** aktiviert haben. Sie können über den Bereich **Vorschau** keine Veränderungen der Bildrate erkennen, da die Miniaturansicht im Bereich **Vorschau** eine andere Bildrate nutzt, die im Dialogfeld **Optionen** festgelegt ist.

Wenn Sie die Einstellungen für die **Max. Bilder zwischen Keyframes** und **Max. Bilder zwischen Keyframes-Modus** ändern, kann die Leistung einiger Funktionen im XProtect Smart Client verringert werden. Der XProtect Smart Client benötigt beispielsweise einen Keyframe, um Video anzeigen zu können, also verzögert ein längerer Zeitraum zwischen den Keyframes das Starten von XProtect Smart Client.

Registerkarte „Streams“ (Geräte)

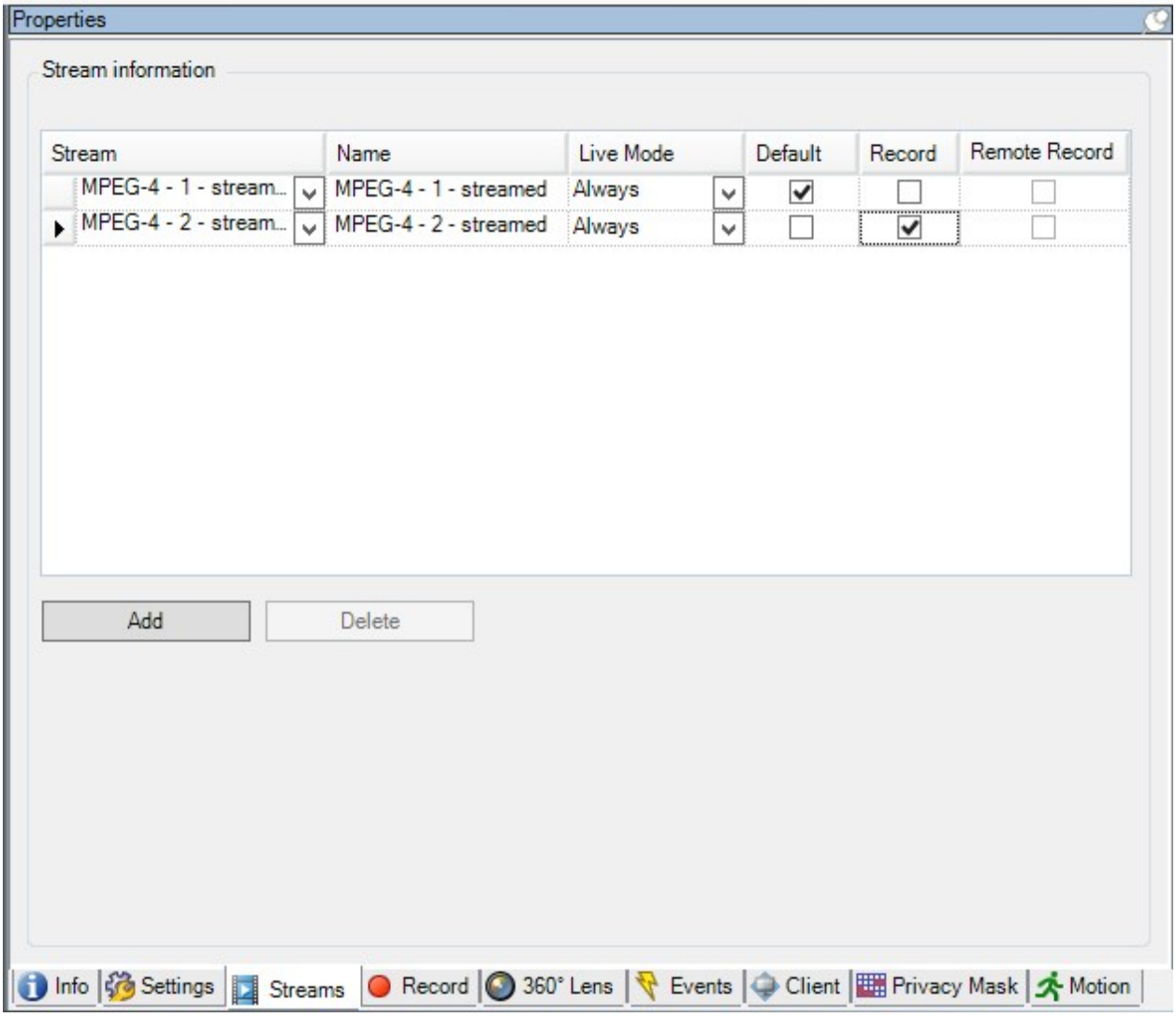
Registerkarte Streams (Erklärung)

Folgende Geräte verfügen über eine **Streams**-Registerkarte:

- Kameras

Die Registerkarte **Streams** enthält standardmäßig einen einzigen Stream. Es ist der Standard-Stream der ausgewählten Kamera, der für Live- und Videoaufzeichnungen verwendet wird.

Sie können so viele Live-Streams einrichten und verwenden, wie es die Kamera unterstützt, doch Sie können jeweils nur einen Stream gleichzeitig zum Aufzeichnen verwenden. Um den Stream für die Aufzeichnung zu wechseln, wählen Sie das Kontrollkästchen **Aufzeichnen** für den Stream aus, der aufgezeichnet werden soll.



Multistreaming (Erklärung)

Zum Betrachten von Live-Videoaufnahmen und zum Abspielen von aufgezeichneten Videos ist nicht unbedingt die gleiche Videoqualität und Bildfrequenz erforderlich. Sie können **entweder** einen Stream zur Live-Anzeige und einen weiteren zur Wiedergabe **oder** für mehrere getrennte Live-Streams mit verschiedenen Einstellungen für Auflösung, Kodierung und Bildrate haben.

Zur Handhabung des Streamings und zur Begrenzung unnötiger Datenübertragungen beginnt das Streaming nicht, wenn die folgenden Bedingungen erfüllt sind:

- Auf der Registerkarte **Streams** ist **Livemodus** auf Bei Bedarf eingestellt
- Auf der Registerkarte **Aufzeichnung** ist die **Aufzeichnung** deaktiviert
- Auf der Registerkarte **Bewegung** ist die **Bewegungserkennung** deaktiviert

Wenn diese Bedingungen erfüllt sind, werden Videosequenzen nur ausgeführt, wenn diese von einem Client angesehen werden.

Beispiel 1, Live-Videos und Videoaufzeichnungen:

- Für die Anzeige von **Live**-Video bevorzugt Ihre Organisation möglicherweise H.264 bei hoher Bildrate
- Für die Wiedergabe von **Videoaufzeichnungen** bevorzugt Ihre Organisation zur Einsparung von Festplattenspeicher evtl. MJPEG mit einer niedrigeren Bildrate

Beispiel 2, lokal und fernaufgezeichnete Live-Videos:

- Für die Anzeige von **Live-Video von einem lokalen Betriebspunkt** bevorzugt Ihre Organisation evtl. H.264 mit hoher Bildrate, um die bestmögliche Videoqualität zu erhalten
- Für die Anzeige von **Live-Video von einem über Fernzugriff verbundenen Betriebspunkt** bevorzugt Ihre Organisation evt. MJPEG mit niedrigerer Bildrate und Qualität, um Netzwerk-Bandbreite einzusparen

Beispiel 3, adaptives Streaming:

- Zur Anzeige von **Live-Video und zur Senkung der Arbeitsbelastung der CPU und GPU des XProtect Smart Client Computers** bevorzugt Ihre Organisation evtl. H.264/H.265 mit mehreren hohen Bildraten in unterschiedlicher Auflösung, die bei Verwendung von adaptivem Streaming der von XProtect Smart Client geforderten Auflösung entspricht. Weitere Informationen finden Sie unter Smart Client-Profileigenschaften auf Seite 298.

Wenn Sie **Live-Multicast** auf der Kamera-Registerkarte **Client** aktivieren, funktioniert dies nur auf dem Standard-Video-Stream.

Selbst wenn Kameras Multi-Streaming unterstützen, können die Multi-Streaming-Kapazitäten zwischen den einzelnen Kameras variieren. Weitere Informationen finden Sie in der Kameradokumentation.

Siehe die Registerkarte **Einstellungen**, um zu erfahren, ob eine Kamera verschiedene Streamformate anbietet.

Stream hinzufügen

1. Klicken Sie auf die Registerkarte **Streams** auf **Hinzufügen**. Ein zweiter Stream wird zur Liste hinzugefügt.
2. Bearbeiten Sie in der Spalte **Name** den Namen des Streams. Der Name erscheint in XProtect Smart Client.
3. Wählen Sie in der Spalte **Live-Modus** aus, wann Live-Streaming erforderlich ist:
   - **Immer**: Der Stream läuft, auch wenn keine XProtect Smart Client-Benutzer den Stream anfordern.
   - **Niemals**: Der Stream ist ausgeschaltet. Verwenden Sie diese Option nur für Aufzeichnungsstreams, z. B., wenn Sie Aufzeichnungen in hoher Qualität und die Bandbreite benötigen
   - **Bei Bedarf**: Der Stream startet, wenn ein Benutzer von XProtect Smart Client ihn anfordert.
4. Wählen Sie in der Spalte **Standard** aus, welcher Stream standardmäßig verwendet werden soll.

5. Aktivieren Sie in der Spalte **Aufzeichnung** das Kontrollkästchen, wenn Sie diesen Stream aufzeichnen möchten, oder deaktivieren Sie es, wenn Sie ihn nur für Live-Video verwenden möchten.
6. Klicken Sie auf **Speichern**.

Wenn Sie einen Stream auf **Standard** oder **Aufzeichnung** einstellen, läuft der Stream immer, unabhängig von der **Live-Modus**-Einstellung. Das Auswählen von **Bei Bedarf** und **Immer** hat die gleichen Auswirkungen im System; bei Auswahl von **Niemals** läuft der Stream, kann jedoch nicht live angezeigt werden.

Wenn Sie möchten, dass die Streams überhaupt nicht ausgeführt werden, es sei denn, jemand sieht sich Live-Bilder an, können Sie die **Standardregel – Start des Feeds** anpassen, damit mit dem vordefinierten Ereignis **Live-Client-Feed angefordert** bei Bedarf gestartet wird.

Registerkarte „Aufzeichnen“ (Geräte)

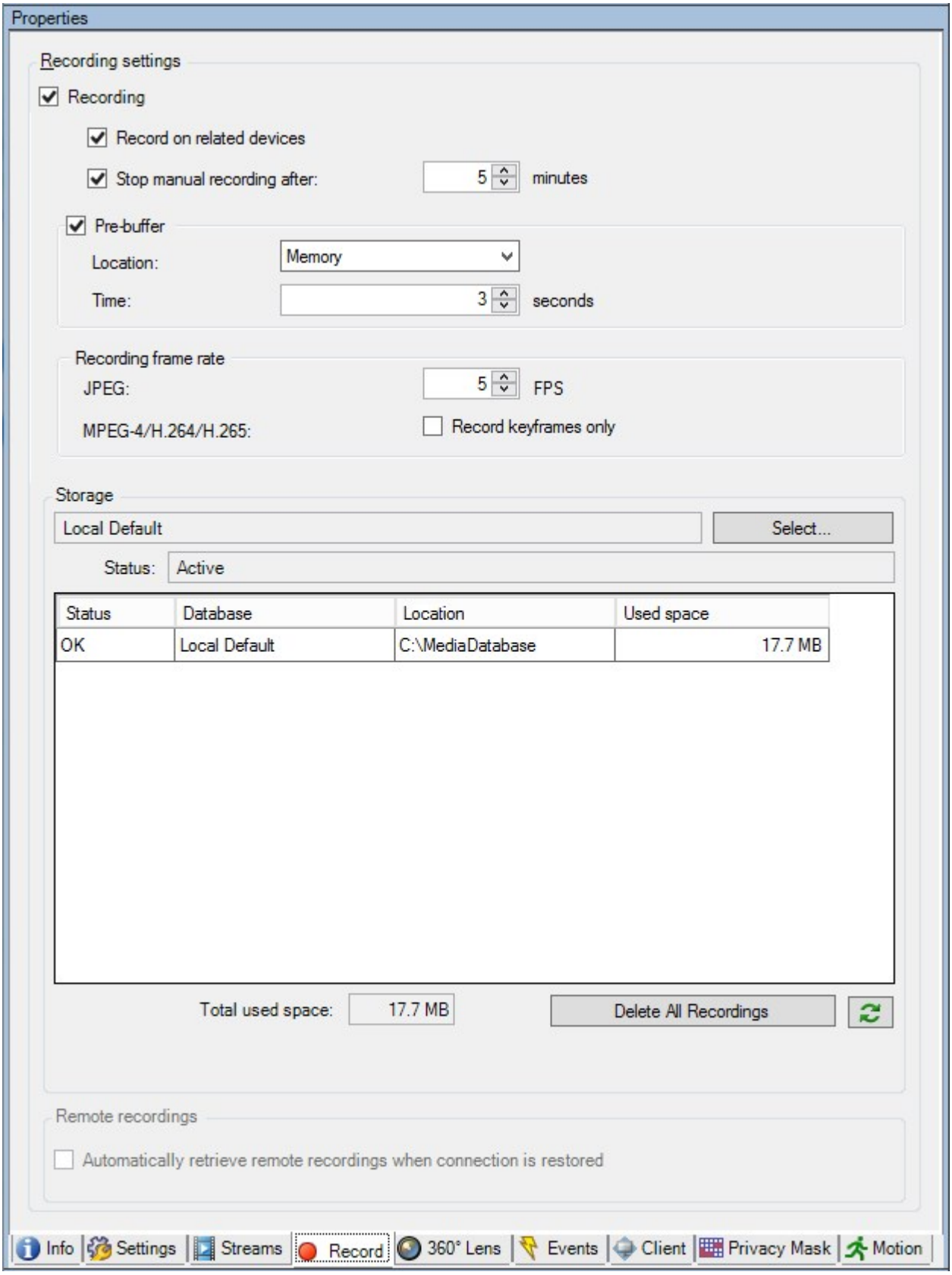
Registerkarte Aufzeichnung (erklärt)

Die folgenden Geräte besitzen eine **Aufzeichnen** Registerkarte:

- Kameras
- Mikrofone
- Lautsprecher
- Metadaten

Aufzeichnungen eines Geräts werden nur in einer Datenbank gespeichert, wenn Sie die Aufzeichnung aktiviert haben und die Aufzeichnungskriterien erfüllt werden.

Parameter, die für ein Gerät nicht konfiguriert werden können, sind ausgegraut.


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

Aufzeichnung aktivieren oder deaktivieren

Aufzeichnung ist standardmäßig aktiviert. Aufzeichnung aktivieren oder deaktivieren:

1. Wählen Sie im Bereich **Standort-Navigation Aufzeichnungsserver** aus.
2. Wählen Sie passende Gerät in der **Übersicht** aus.
3. In der **Aufzeichnen**-Registerkarte, wählen Sie das **Aufzeichnung**-Kontrollkästchen an oder ab.

> Sie müssen die Aufzeichnung für das Gerät aktivieren, bevor Sie Daten mit der Kamera aufzeichnen können. Eine Regel zum Bestimmen der Umstände eines Geräts, bei denen es aufzeichnet, funktioniert nicht, wenn Sie die Aufzeichnung für das Gerät deaktiviert haben.

Aktivieren der Aufzeichnung auf zugehörigen Geräten

Bei Kameras können Sie die Aufzeichnung zugehöriger Geräte aktivieren, wie zum Beispiel von Mikrofonen, die mit dem selben Aufzeichnungsserver verbunden sind. Dies bedeutet, dass zugehörige Geräte aufzeichnen, wenn die Kamera aufzeichnet.

Die Aufzeichnung auf zugehörigen Geräten ist bei neuen Kameras standardmäßig aktiviert, kann jedoch nach Bedarf an- und ausgeschaltet werden. Bei bestehenden Kameras im System ist das Kontrollkästchen standardmäßig nicht angewählt.

1. Wählen Sie im Bereich **Standort-Navigation Aufzeichnungsserver** aus.
2. Wählen Sie die zugehörige Kamera im Bereich **Übersicht** aus.
3. In der **Aufzeichnung**-Registerkarte, wählen Sie das Kontrollkästchen **Auf zugehörigem Gerät aufzeichnen** an oder ab.
4. In der **Client**-Registerkarte, bestimmen Sie die Geräte, die zu dieser Kamera gehören.

Wenn Sie die Aufzeichnung auf zugehörigen Geräten, die mit einem anderen Aufzeichnungsserver verbunden sind, aktivieren möchten, müssen Sie eine Regel erstellen.

Voralarm-Puffer (Erklärung)

Voralarm-Puffern ist die Möglichkeit, Audio und Video aufzuzeichnen bevor das eigentliche auslösende Ereignis auftritt. Dies ist besonders nützlich, wenn Sie Audio oder Video aufnehmen möchten, das zu einem Ereignis führt, welches die Aufzeichnung auslöst (z. B. das Öffnen einer Tür).

Voralarm-Puffern ist möglich, da das System kontinuierlich Audio- und Video-Streams von den verbundenen Geräten empfängt und diese temporär über den festgelegten Voralarm-Zeitraum speichert.

- Bei Auslösung einer Aufzeichnungsregel werden temporäre Aufzeichnungen zu permanenten während der eingestellten Voralarmaufzeichnungszeit
- Wenn keine Aufzeichnungsregel ausgelöst wird, werden die temporären Aufzeichnungen im Voralarm-Puffer automatisch nach der eingestellten Voralarm-Pufferzeit gelöscht

Für die Verwendung der Voralarm-Puffer-Funktion müssen die Geräte aktiviert sein und einen Stream an das System senden.

Geräte, die Voralarm-Puffern unterstützen

Kameras, Mikrofone und Lautsprecher unterstützen Voralarm-Puffern. Bei Lautsprechern werden die Streams nur gesendet, wenn der XProtect Smart Client-Benutzer die Funktion **Ausgabe Lautsprecher** verwendet. Dies hat zur Folge, dass je nachdem wie Ihre Lautsprecher-Streams ausgelöst werden, keine oder nur geringes Voralarm-Puffern zur Verfügung steht.

In den meisten Fällen werden Lautsprecher darauf eingestellt, die Aufzeichnung zu beginnen, wenn der XProtect Smart Client-Benutzer die Funktion **Ausgabe Lautsprecher** verwendet. In solchen Fällen steht der Voralarm-Puffer für Lautsprecher nicht zur Verfügung.

Speicherort der temporären Voralarm-Puffer-Aufzeichnungen

Sie können den Speicherort der temporären Voralarm-Puffer-Aufzeichnungen auswählen:

- Im Speicher ist der Voralarm-Zeitraum auf 15 Sekunden begrenzt.
- Auf der Festplatte (in der Mediendatenbank) können Sie alle Werte auswählen.

Der Speicher anstatt der Festplatte als direkter Speicherort verbessert die Systemleistung, ist jedoch nur für kürzere Voralarm-Zeiträume möglich.

Sollten Aufzeichnungen im Speicher aufbewahrt werden, müssen Sie einige der temporären Aufzeichnungen zu permanenten machen, wodurch die übrigen temporären Aufzeichnungen unwiederbringlich gelöscht werden. Wenn Sie die übrigen Aufzeichnungen behalten möchten, speichern Sie diese auf der Festplatte.

Verwalten von Voralarm-Puffern

Aktivieren und Deaktivieren der Vorpufferung

Das Voralarm-Puffern wird standardmäßig mit einem Voralarm-Puffer von drei Sekunden aktiviert und dem Speicherort im Speicher.

1. Wählen Sie den **Voralarm-Puffer** an/ab, um Voralarm-Puffern zu aktivieren/deaktivieren.

Angabe des Speicherortes und des Vorpufferzeitraums

Temporäre Voralarm-Puffer-Aufzeichnungen werden entweder im Speicher oder auf der Festplatte gespeichert:

1. Um auf **Standort** zuzugreifen, wählen Sie **Speicher** oder **Festplatte** und legen Sie die Sekundenzahl fest.

   Die Anzahl der festgelegten Sekunden muss groß genug sein, um den in den verschiedenen Aufzeichnungsregeln gesetzten Anforderungen zu entsprechen.

   Wenn Sie einen Voralarm-Puffer-Zeitraum benötigen, der 15 Sekunden überschreitet, wählen Sie **Festplatte**.

2. Wenn Sie den Standort zu **Speicher** ändern, senkt das System den Zeitraum automatisch auf 15 Sekunden.

Verwendung von Vorpufferung in Regeln

Bei der Erstellung von Regeln, welche eine Aufzeichnung auslösen, können Sie die Option wählen, dass Aufzeichnungen einige Zeit vor dem eigentlichen Ereignis starten (Voralarm-Puffer).

Beispiel: Die nachfolgende Regel legt fest, dass eine Aufzeichnung der Kamera beginnen soll, wenn 5 Sekunden vorher Bewegung von der Kamera erkannt wird.

Sie müssen auf dem aufzeichnenden Gerät das Voralarm-Puffern aktivieren und die Länge des Voralarm-Puffers mindestens mit der in der Regel festgelegten Länge abgleichen, um die Voralarm-Puffer-Aufzeichnungsfunktion in der Regel zu verwenden.

Manuelle Aufzeichnung verwalten

Manuelle Aufzeichnung danach anhalten ist standardmäßig mit einer Aufzeichnungszeit von fünf Minuten aktiviert. Dadurch ist gewährleistet, dass das System alle Aufzeichnungen anhält, die von den XProtect Smart Client-Benutzern gestartet wurden.

1. Wählen Sie das Kontrollkästchen für **Manuelle Aufzeichnung danach anhalten** an/ab, um die Funktion des Systems zum automatischen Stopp der manuellen Aufzeichnungen zu aktivieren/deaktivieren.
2. Bestimmen Sie eine Aufzeichnungszeit bei Aktivierung. Die Anzahl der festgelegten Minuten muss von ausreichender Größe sein, um den Anforderungen der verschiedenen manuellen Aufzeichnungen zu entsprechen, ohne dabei das System zu überladen.

Zu Rollen hinzufügen:

Sie müssen in **Rollen** auf der **Geräte**-Registerkarte den Client-Benutzern jeder Kamera die Rechte zum Starten und Anhalten manueller Aufzeichnungen gewähren.

Bei Regeln verwenden:

Die verfügbaren Ereignisse bei der Erstellung von Regeln im Bezug auf manuelle Aufzeichnungen sind:

- Manuelle Aufzeichnung gestartet
- Manuelle Aufzeichnung angehalten

Bildrate der Aufzeichnung festlegen

Sie können die Bildrate der Aufzeichnung von JPEG festlegen.

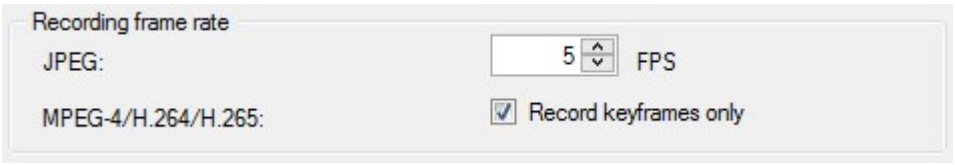
- Wählen Sie die Bildrate aus oder geben Sie die gewünschte Bildrate (in FPS, Frames per Second) für die Aufzeichnung in das Feld **Aufzeichnungsbildrate ein: (JPEG)**.

Keyframe-Aufzeichnung aktivieren

Sie können die Keyframe-Aufzeichnung für MPEG-4/H.264/H.265-Streams aktivieren. Dies hat zur Folge, dass das System je nach Regeleinstellungen zwischen alleinigen Keyframe-Aufzeichnungen und Aufzeichnungen aller Bilder wechselt.

Sie können beispielsweise zum Sparen von Speicherplatz das System Keyframes aufzeichnen lassen, wenn keine Bewegung in Sicht ist und zu allen Bildern wechseln, wenn Bewegung erkannt wird.

1. Wählen Sie die Option **Nur Keyframes aufzeichnen** aus.

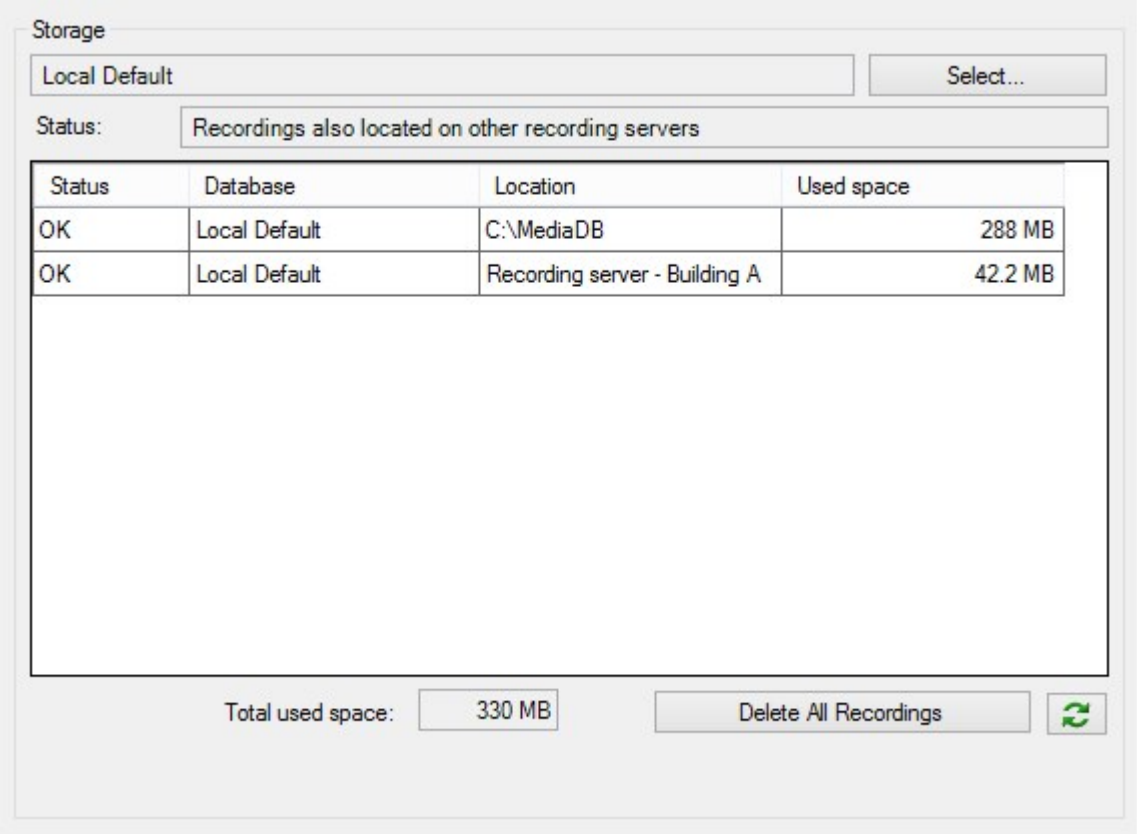


2. Erstellen Sie eine Regel, die diese Funktion aktiviert. Siehe Aktionen und Stopp-Aktionen (Erklärung) auf Seite 312.

Speicherort (Erklärung)

Unter **Speicherort** können sie Datenbanken für ein Gerät oder eine Gerätegruppe, die zum gleichen Aufzeichnungsserver gehören, überwachen und verwalten.

Über der Tabelle wird die ausgewählte Datenbank und ihr Status angezeigt. In diesem Beispiel ist die ausgewählte Datenbank der **Lokale Standard** und der Status sind **Aufzeichnungen, die sich auch auf anderen Aufzeichnungsservern befinden**. Der andere Server ist der Aufzeichnungsserver in Gebäude A.



Mögliche Status für die ausgewählte Datenbank

Name	Beschreibung
Aufzeichnungen befanden sich auch auf anderen Aufzeichnungsservern	Die Datenbank ist aktiv und wird ausgeführt und besitzt auch Aufzeichnungen an Speicherorten auf anderen Aufzeichnungsservern.
Archive befinden sich auch am alten Speicherort	Die Datenbank ist aktiv und wird ausgeführt und besitzt auch Archive an anderen Speicherorten.
Aktiv	Die Datenbank ist aktiv und wird ausgeführt.
Die Daten für einige der ausgewählten Geräte werden zurzeit an einen anderen Speicherort verschoben	Die Datenbank ist aktiv und wird ausgeführt und das System bewegt Daten für ein oder mehrere ausgewählte Geräte in einer Gruppe von einem Standort zum anderen.
Die Daten für das Gerät werden gerade	Die Datenbank ist aktiv und wird ausgeführt und das System

Name	Beschreibung
an einen anderen Speicherort verschoben	bewegt Daten für ein oder mehrere ausgewählte Geräte in einer Gruppe von einem Standort zum anderen.
Informationen nicht verfügbar im Failover-Modus	Das System kann keine Statusinformationen über die Datenbank sammeln, wenn sich die Datenbank im Failover-Modus befindet.

Weiter unten im Fenster können Sie den Status jeder Datenbank sehen (**OK**, **Offline** oder **Alter Speicherort**), den Standort jeder Datenbank und wie viel Speicherplatz diese verwenden.

Sie können im Feld **Gesamter genutzter Speicherplatz** den gesamten genutzten Speicherplatz am Speicherort sehen, wenn alle Server online sind.

Mittels der Schaltfläche **Alle Aufzeichnungen löschen** können Sie alle Aufzeichnungen für das Gerät oder die Gerätegruppe löschen, in der die Geräte des gleichen Servers zusammengefasst sind. Geschützte Daten werden nicht gelöscht.

Für Informationen über die Konfiguration des Speicherorts siehe Registerkarte „Speicher“ (Aufzeichnungsserver) auf Seite 157.

Umzug mit Geräten von einem Speicher zu einem anderen

Sie können viele Geräte einen neuen Speicherort auswählen, indem Sie **Auswählen...** unter **Speicher** auswählen.

So können Sie einen anderen Speicher für die Aufzeichnungen Ihrer Geräte auswählen, und diese werden dann entsprechend der Konfiguration für diesen Speicher archiviert.

Wenn Sie einen neuen Speicherort für Aufzeichnungen auswählen, werden vorhandene Aufzeichnungen nicht mit umgezogen. Diese verbleiben am aktuellen Speicherort zu den Bedingungen, die durch die Konfiguration des Speichers vorgegeben werden, zu dem sie gehören.

Fernaufzeichnung (Erklärung)

Die Option der Fernaufzeichnung steht nur zur Verfügung, wenn die ausgewählte Kamera lokalen Speicher unterstützt oder eine Kamera mit einer Milestone Interconnect-Einstellung ist.

Wählen Sie die Option **Automatisches Abrufen von Fernaufzeichnungen wenn Verbindungen wiederhergestellt sind**, um sicherzustellen, dass alle Aufzeichnungen bei Netzwerkproblemen gespeichert werden. Dies aktiviert den automatischen Abruf von Aufzeichnungen, sobald die Verbindung wiederhergestellt wurde.

Die Art der ausgewählten Hardware bestimmt woher Aufzeichnungen bezogen werden:

- Bei einer Kamera mit lokalem Aufzeichnungsspeicherort werden die Aufzeichnungen von diesem lokalen Aufzeichnungsspeicherort abgerufen
- Bei einem Milestone Interconnect-Remote-Systeminstallation werden Aufzeichnungen von den Aufzeichnungsservern dieses Systems abgerufen

Sie können die folgende Funktion unabhängig vom automatischen Abruf verwenden:

- Manuelle Aufzeichnung
- Die **Abrufen und Speichern der Fernaufzeichnungen von <Geräte>** Regel
- Die Regel **Abrufen und Speichern der Fernaufzeichnungen zwischen <Start- und Endzeit> von <Geräte>**

Registerkarte „Bewegung“ (Geräte)

Registerkarte Bewegung (Erklärung)

Die folgenden Geräte besitzen eine Registerkarte **Bewegung**:

- Kameras

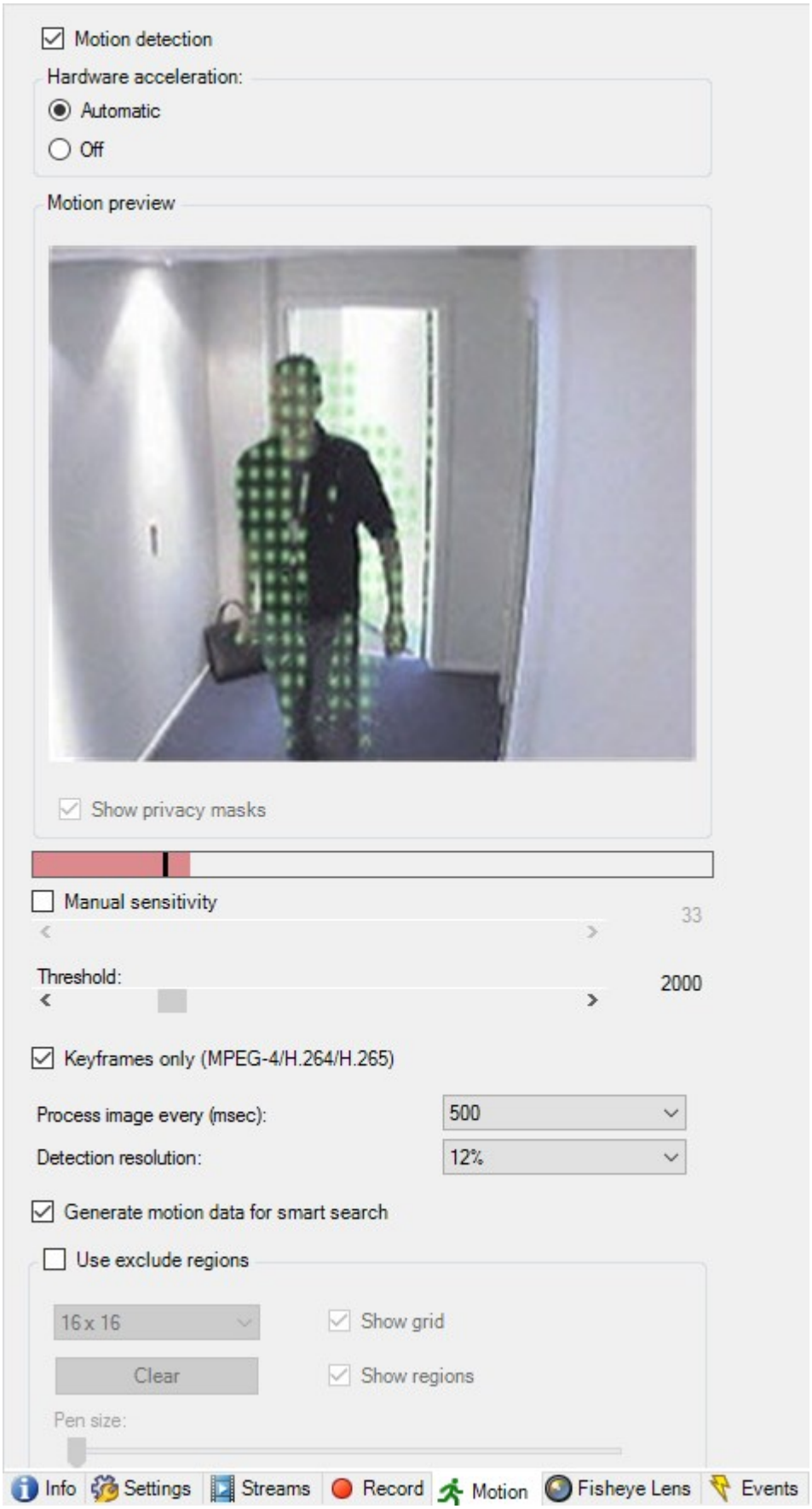
In der Registerkarte **Bewegung** können Sie die Bewegungserkennung für die ausgewählte Kamera aktivieren und konfigurieren. Die Konfiguration der Bewegungserkennung ist ein Schlüsselelement in Ihrem System: Die Konfiguration der Bewegungserkennung bestimmt, wann das System Bewegungsereignisse erstellt und wann Video aufgezeichnet wird.

Beispielsweise hilft die optimale Konfiguration der Bewegungserkennung jeder Kamera später dabei, unnötige Aufzeichnungen zu vermeiden. Je nach physischem Standort der Kamera könnte es von Vorteil sein, die Einstellungen der Bewegungserkennung unter verschiedenen Voraussetzungen, wie z. B. Tages-/Nachtzeit und windiges/ruhiges Wetter, zu testen.

Bevor Sie die Bewegungserkennung für eine Kamera konfigurieren, empfiehlt Milestone, dass Sie mit der Einstellung der Bildqualität der Kamera (Auflösung, Video-Codec und Stream-Einstellungen) in der Registerkarte **Einstellungen** beginnen. Wenn Sie später die Einstellungen der Bildqualität ändern, sollten Sie die Konfiguration der Bewegungserkennung danach unbedingt testen.

Wenn Sie Bereiche mit permanenten Privatzonenmaskenmasken auf der Registerkarte **Privatsphärenausblendung** (siehe Registerkarte Einrichtung von Privatsphärenausblendung (Geräte) auf Seite 273) festgelegt haben, können Sie durch Auswählen des Kontrollkästchens **Privatsphärenausblendung zeigen** auswählen, dass die Privatsphärenausblendung auf der Registerkarte **Bewegung** angezeigt werden sollen.

Es gibt keine Bewegungserkennung innerhalb von Bereichen, die von permanenten Privatzonenmasken gedeckt sind.


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

Sie können alle Einstellungen für eine komplette Gruppe Kameras einstellen, jedoch bietet es sich an, die Ausnahmebereiche pro Kamera festzulegen.

Aktivieren und Deaktivieren von Bewegungserkennung

Sie können die Standardeinstellungen für die Bewegungserkennung der Kameras in der Registerkarte **Tools** > **Optionen** > **Allgemein** festlegen.

Wie Sie die Bewegungserkennung für eine Kamera nachfolgend aktivieren oder deaktivieren:

- Wählen Sie das Kontrollkästchen **Bewegungserkennung** in der Registerkarte **Bewegung** an oder ab

> Bei Deaktivierung der Bewegungserkennung für eine Kamera, funktionieren Regeln bezüglich der Bewegungserkennung für diese Kamera nicht.

Festlegen der Einstellungen für die Bewegungserkennung

Sie können Einstellungen vornehmen, die im Bezug zur Anzahl der benötigten Änderungen in der Sicht einer Kamera stehen, um die Änderung als Bewegung erkennen zu lassen. Sie können beispielsweise Zeitspannen bestimmen zwischen Bewegungserkennungsanalysen und Sichtfeldern in denen Bewegungen ignoriert werden können. Sie können auch die Genauigkeit der Bewegungserkennung anpassen und dadurch die Last auf die Systemressourcen.

Hardwarebeschleunigung (Erklärung)

Wählen Sie **Automatisch**, um hardwarebeschleunigte Video-Bewegungserkennung zu ermöglichen. Dies ist die Standardeinstellung, wenn Sie eine Kamera hinzufügen. Falls verfügbar, verwendet der Aufzeichnungsserver nun GPU-Ressourcen. Dies reduziert die CPU-Last während der Videobewegungsanalyse und verbessert die allgemeine Leistung des Aufzeichnungsservers.

Hardwarebeschleunigte Videobewegungserkennung benutzt GPU-Ressourcen für:

- Intel-CPUs, die Intel Quick Sync unterstützen
- NVIDIA® an Ihren Aufzeichnungsserver angeschlossene Grafikkarten

Der Lastenausgleich zwischen den verschiedenen Ressourcen erfolgt automatisch. In dem **Systemmonitor** Knoten können Sie überprüfen, ob die aktuelle Bewegungsanalysen-Last der NVIDIA GPU-Ressourcen innerhalb der angegebenen Grenzen von dem **Systemmonitor Schwellenwerten** Knoten liegt. Die NVIDIA GPU-Lastenanzeigen sind:

- NVIDIA-Dekodierung
- NVIDIA-Speicher
- NVIDIA-Rendering

Wenn die Last zu hoch ist, können Sie GPU-Ressourcen zu Ihrem Recording-Server hinzufügen, indem Sie mehrfache NVIDIA Displayadapter installieren. Milestone empfiehlt nicht die Verwendung der Scalable Link-Interface (SLI)-Konfiguration Ihrer NVIDIA-Grafikkarten.

NVIDIA-Produkte haben unterschiedliche Rechenleistungen. Um zu überprüfen, ob Ihr NVIDIA-Produkt Hardwarebeschleunigung für die in Ihrem System Milestone XProtect verwendeten Codecs unterstützt, suchen Sie die unterstützten Codecs für die Rechenleistungsversion in nachstehender Tabelle.

Um die Rechenleistungsversion für Ihr NVIDIA-Produkt festzustellen, besuchen Sie die NVIDIA-Website (https://developer.nvidia.com/cuda-gpus/).

Rechenleistung	Architektur	H.264	H.265
3.x	Kepler	✓	-
5.x	Maxwell	✓	-
6.x	Pascal	✓	✓
7.x	Volta	✓	✓

Um zu sehen, ob die Videobewegungserkennung für eine bestimmte Kamera hardwarebeschleunigt ist, aktivieren Sie die Protokollierung in der Protokolldatei des Aufzeichnungsservers. Stellen Sie die Ebene auf **Debug** ein. Diagnosen werden in DeviceHandling.log protokolliert. Das Protokoll folgt dem Muster:
[zeit] [274] DEBUG – [guid] [Name] Konfigurierte Decodierung: Automatisch: Tatsächliche Decodierung: Intel/NVIDIA

Die BS-Version des Aufzeichnungsservers und die CPU-Generation können die Leistung hardwarebeschleunigter Videobewegungserkennung beeinflussen. Bei älteren Versionen ist die GPU-Speicherzuweisung oft das Nadelöhr (der typische Grenzwert liegt zwischen 0,5 GB und 1,7 GB).

Auf Windows 10/Server 2016 basierende Systeme und CPUs der sechsten Generation (Skylake) oder höher können 50 % des Systemspeichers der GPU zuweisen und dadurch dieses Nadelöhr eliminieren oder reduzieren.

Intel-CPUs der sechsten Generation bieten hardwarebeschleunigte Dekodierung von H.265. Dadurch ist die Leistung für diese CPU-Versionen mit H.264 vergleichbar.

Manuelle Empfindlichkeit aktivieren

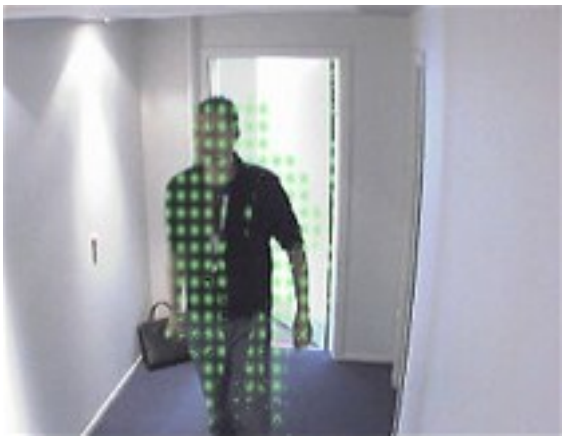
Die Empfindlichkeitseinstellung legt fest, **wie sehr sich ein Pixel** in den Bildern der Kamera verändern muss, bevor dies als Bewegung registriert wird.

1. Wählen Sie das Kontrollkästchen **Manuelle Empfindlichkeit** in der Registerkarte **Bewegung** aus.
2. Ziehen Sie den Schieberegler nach links für eine höhere Empfindlichkeit und nach rechts für eine niedrigere Empfindlichkeit.

   Je **höher** die Empfindlichkeit, desto weniger Veränderungen sind in jedem Pixel erlaubt, bevor es als Bewegung registriert wird.

   Je **niedriger** die Empfindlichkeit, desto mehr Veränderungen sind in jedem Pixel erlaubt, bevor es als Bewegung registriert wird.

   Pixel in denen Bewegung erkannt wird, werden im Vorschaubild Grün hervorgehoben.
3. Wählen Sie eine Position für den Schieberegler aus, bei der nur Erkennungen hervorgehoben werden, die Sie als Bewegungen erachten.



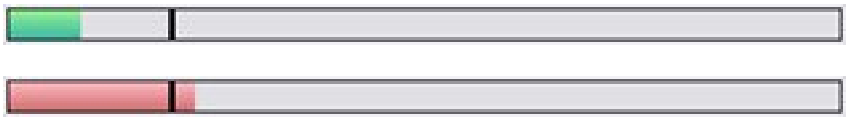
Anhand der Zahl an der rechten Seite des Schiebereglers, können Sie die genaue Empfindlichkeit zwischen Kameras vergleichen und einstellen.

Schwellenwert festlegen

Die Bewegungserkennung bestimmt, **wie viele Pixel** sich im Bild verändern müssen, bevor dies als Bewegung registriert wird.

1. Ziehen Sie den Schieberegler nach links für eine höhere Bewegungsrate und nach rechts für eine niedrigere Bewegungsrate.
2. Wählen Sie eine Position für den Schieberegler aus, bei der nur Erkennungen registriert werden, die Sie als Bewegungen erachten.

Die schwarze vertikale Linie in der Bewegungsanzeigeleiste zeigt den Schwellenwert der Bewegungserkennung: Wenn die erkannte Bewegung über dem ausgewählten Schwellenwert liegt, verändert sich die Farbe des Balkens von Grün zu Rot und zeigt so eine positive Erkennung an.



Bewegungsanzeigeleiste: wechselt die Farbe von Grün auf Rot, wenn Schwellenwert überschritten wird und zeigt so eine positive Bewegungserkennung an.

Keyframe-Einstellungen auswählen

Legt fest, ob Bewegungserkennung nur bei Keyframes anstatt im gesamten Videostream erfolgt. Gilt nur für MPEG-4/H.264/H.265.

Die Bewegungserkennung in Keyframes reduziert die verwendete Prozessorleistung für die Ausführung der Analyse.

Wählen Sie das Fenster **Nur Keyframes (MPEG-4/H.264/H.265)** aus, um Bewegungserkennung in Keyframes vorzunehmen.

Bildverarbeitungsintervall auswählen

Sie können auswählen, wie oft das System die Bewegungserkennungsanalyse durchführt.

Aus der Liste **Bild jede (ms) verarbeiten**:

- Wählen Sie das Intervall. Zum Beispiel, alle 1.000 Millisekunden bedeutet einmal jede Sekunde. Der Standardwert ist auf alle 500 Millisekunden festgelegt.

  Der Intervall wird angewendet, wenn die tatsächliche Bildrate höher als das hier eingestellte Intervall ist.

Erkennungsauflösung festlegen

Ermöglicht Ihnen eine Optimierung der Leistung der Bewegungserkennung durch eine Analyse von nur einem ausgewählten Prozentanteil des Bildes (z. B. 25 %). Durch die Analyse von 25 % wird nur jedes vierte anstatt alle Pixel untersucht.

Mittels optimierter Erkennung wird die benötigte Prozessorleistung für die Analyse verringert, führt jedoch zu einer weniger genauen Bewegungserkennung.

- Wählen Sie die gewünschte Bewegungsauflösung in der Liste für **Bewegungsauflösung**.

Erzeugung von Bewegungsdaten für Smart Search

Das System generiert mit aktivierter Option **Bewegungsdaten für Smart Search generieren**, Bewegungsdaten für die Bilder, die für die Bewegungserkennung verwendet werden. Wenn Sie beispielsweise Bewegungserkennung nur in Keyframes auswählen, werden diese Bewegungsdaten auch nur für Keyframes erstellt.

Durch die zusätzlichen Bewegungsdaten können die Client-Benutzer mittels der Smart Search Funktion schnell und einfach auf Grundlage der Bewegung in einem ausgewählten Bereich des Bildes nach relevanten Aufzeichnungen suchen. Das System erzeugt keine Bewegungsdaten in Bereichen mit permanenten Privatzonenmasken, nur in Bereichen mit aufhebbaren Privatzonenmasken (siehe Registerkarte Einrichtung von Privatsphärenausblendung (Geräte) auf Seite 273).

Der Schwellenwert für die Bewegungserkennung und Auschlussbereiche beeinflussen die generierten Bewegungsdaten nicht.

Sie können die Standardeinstellungen für die Generierung von Smart Search Daten für Kameras über die Registerkarte **Werkzeuge** > **Optionen** > **Allgemein** festlegen.

Ausschlussbereiche bestimmen

Sie können die Bewegungserkennung in bestimmten Bereichen des Sichtfelds einer Kamera deaktivieren.

> Bereiche mit permanenten Privatzonenmasken sind auch von der Bewegungserkennung ausgeschlossen. Wählen Sie das Kontrollkästchen **Privatzonenmasken zeigen**, um sie anzuzeigen.

Die Deaktivierung der Bewegungserkennung in bestimmten Bereichen hilft Ihnen die Erkennung irrelevanter Bewegungen zu vermeiden, z. B. wenn die Kamera einen Bereich abdeckt, in dem sich ein Baum im Wind bewegt oder Autos regelmäßig im Hintergrund vorbeifahren.

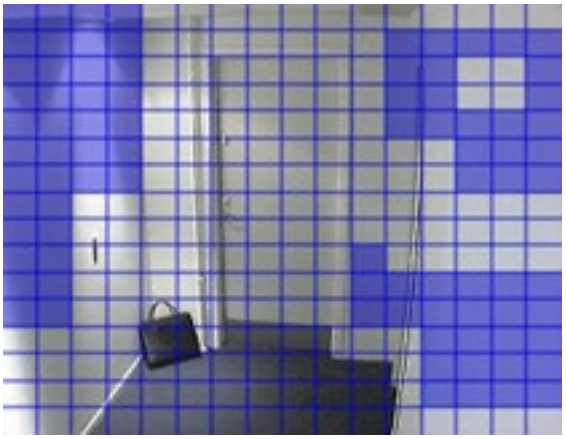
Bei der Verwendung von Ausschlussbereichen mit PTZ-Kameras und der Anwendung von Pan/Tilt/Zoom auf die Kamera, wird der Ausschlussbereich **nicht** entsprechend bewegt, da der Bereich im Bild der Kamera festgestellt wird und nicht am Objekt.

1. Für die Verwendung von Ausschlussbereichen, wählen Sie das Kontrollkästchen **Ausschlussbereiche verwenden** an.

   Ein Raster teilt das Vorschaubild in auswählbare Abschnitte.

2. Ziehen Sie den Mauszeiger mit gedrückter linker Maustaste über die erforderlichen Bereiche im Vorschaubild, um Ausschlussbereiche festzulegen. Die rechte Maustaste leert einen Rasterabschnitt.

Sie können so viele Ausschlussbereiche festlegen, wie Sie benötigen. Ausschlussbereiche werden in blau angezeigt:



Die blauen Ausschlussbereiche werden nur im Vorschaubild in der Registerkarte **Bewegung** angezeigt und nicht in einem anderen Vorschaubild oder im Management Client oder Access Client.

Registerkarte „Voreinstellungen" (Geräte)

Registerkarte Voreinstellungen (Erklärung)

Die folgenden Geräte besitzen eine Registerkarte **Voreinstellungen**:

- PTZ-Kameras, die Preset Positionen unterstützen

Auf der Registerkarte **Voreinstellungen** können Sie Preset Positionen erstellen oder importieren, zum Beispiel:

- Bei Regeln, welche die Bewegung einer PTZ (Pan/Tilt/Zoom)-Kamera zu einer bestimmten Preset Position festlegen, wenn ein Ereignis eintritt
- Bei Wachrundgängen, für die automatische Bewegung einer PTZ-Kamera zwischen mehreren Preset Positionen.
- Für manuelle Aktivierung durch die XProtect Smart Client-Benutzer.

Sie können eine Preset Position sperren, wenn Sie Benutzer im XProtect Smart Client oder Benutzer mit beschränkten Sicherheitsberechtigungen daran hindern möchten, diese Voreinstellung zu aktualisieren.

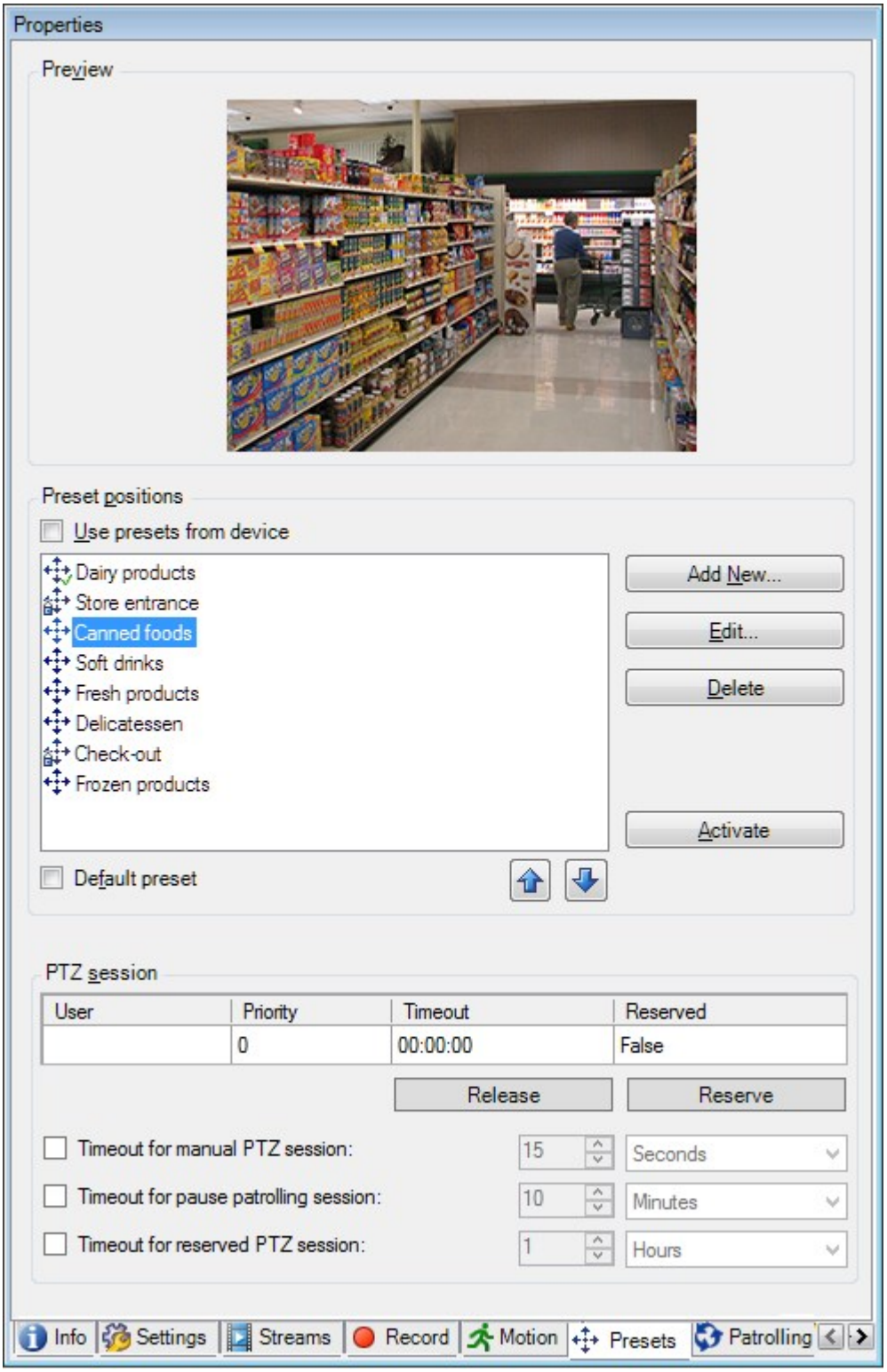
Gesperrte Voreinstellungen werden durch das Symbol angezeigt.

Administratoren mit Sicherheitsberechtigungen zum Ausführen einer reservierten PTZ-Sitzung (siehe Reservierte PTZ-Sitzungen (Erklärung) auf Seite 258) können die PTZ-Kamera in diesem Modus betreiben. So wird verhindert, dass andere Benutzer die Kontrolle über die Kamera übernehmen. Mit entsprechender Berechtigung können Sie die reservierten PTZ-Sitzungen anderer Benutzer freigeben (siehe PTZ-Sitzung freigeben auf Seite 258).

Auf der Registerkarte Gesamtsicherheit weisen Sie die PTZ-Genehmigung den entsprechenden Rollen zu (siehe die Registerkarte Registerkarte „Gesamtsicherheit" (Rollen) auf Seite 381) oder auf der Registerkarte PTZ (siehe die Registerkarte PTZ-Registerkarte (Rollen) auf Seite 417).

Sie können im Bereich **PTZ-Sitzung** überwachen, ob das System derzeit einen Wachrundgang durchführt oder ein Benutzer die Kontrolle übernommen hat. (siehe PTZ-Sitzungs-Eigenschaften auf Seite 259)

Sie können außerdem die Zeitüberschreitungen bei PTZ-Sitzungen für die Kamera ändern.



Hinzufügen einer Preset-Position (Typ 1) auf Seite 253

Verwendung der Preset Positionen der Kamera (Typ 2) auf Seite 255

Zuweisen einer standardmäßigen Preset Position auf Seite 255

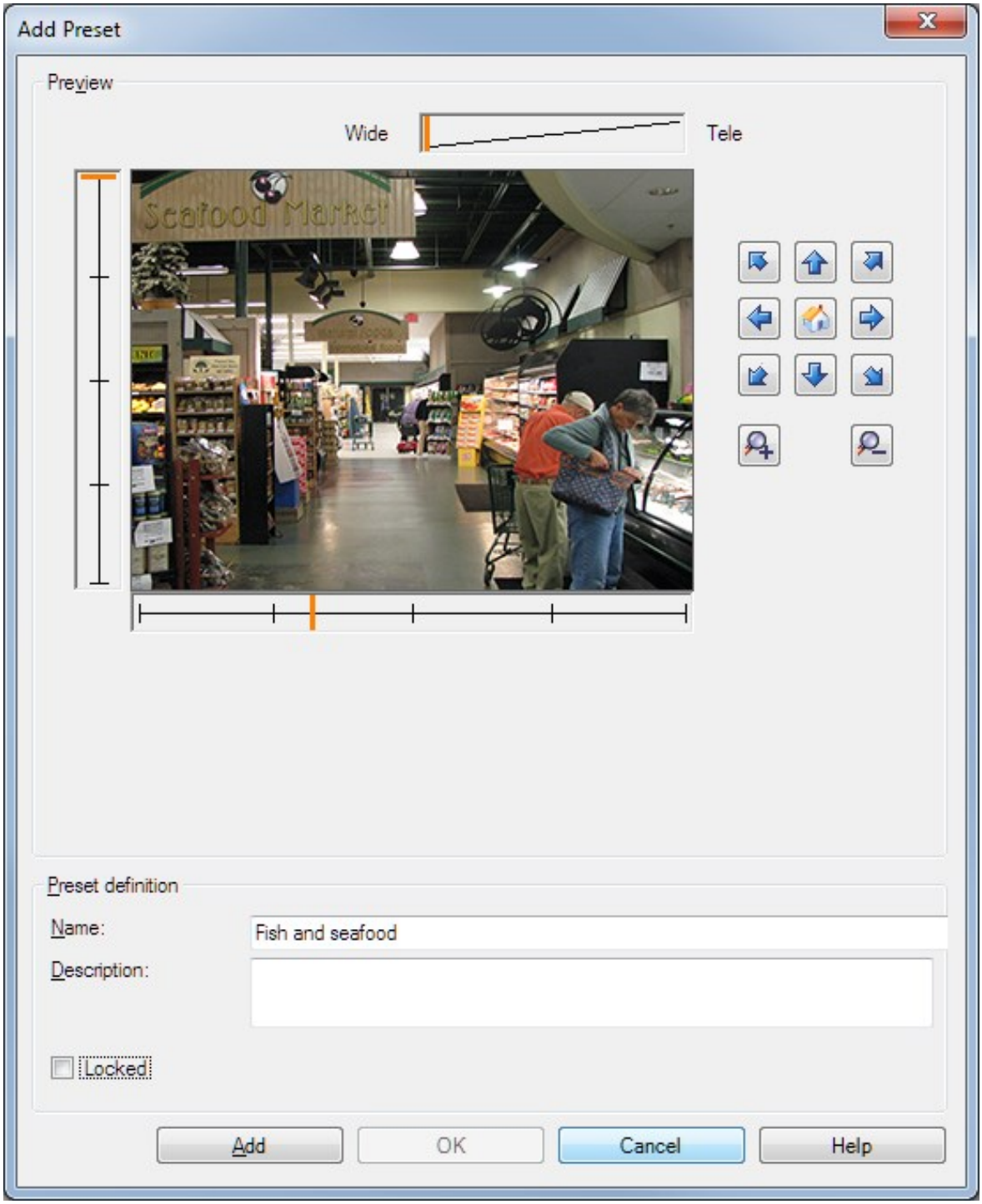
Bearbeiten einer Preset-Position (nur Typ 1) auf Seite 255

Testen einer Preset-Position (nur Typ 1) auf Seite 258

Hinzufügen einer Preset-Position (Typ 1)

Um eine Preset Position für die Kamera hinzuzufügen:

1. Klicken Sie auf **Neu hinzufügen**. Das Fenster **Voreinstellung hinzufügen** erscheint:



2. Das Fenster **Voreinstellung hinzufügen** zeigt ein Live-Vorschaubild der Kamera an. Navigieren Sie die Kamera mit den Navigationsschaltflächen und/oder den Schiebereglern zur erforderlichen Position.
3. Bestimmen Sie im Feld **Name** einen Namen für die Preset Position.

4. Sie können optional eine Beschreibung der Preset-Position in das Feld **Beschreibung** eingeben.
5. Wählen Sie **Gesperrt**, wenn Sie die Preset Position sperren möchten. Nur Benutzer mit der entsprechenden Berechtigung können die Position wieder entsperren.
6. Klicken Sie auf **Hinzufügen**, um Voreinstellungen zu bestimmen. Fügen Sie so lange Voreinstellungen hinzu, bis Sie mit diesen zufrieden sind.
7. Klicken Sie auf **OK**. Das Fenster **Voreinstellung hinzufügen** schließt sich und fügt die Position in die Liste der verfügbaren Preset Positionen für die Kamera auf der Registerkarte **Voreinstellungen** ein.

Verwendung der Preset Positionen der Kamera (Typ 2)

Alternativ zur Festlegung von Preset Positionen im System können Sie bei einigen PTZ-Kameras Preset Positionen auf der Kamera selbst festlegen. Dies können Sie normalerweise über eine produktspezifische Konfigurationswebseite durchführen.

1. Importieren Sie die Voreinstellungen in das System, indem Sie **Voreinstellungen des Geräts verwenden** wählen.

   Alle Voreinstellungen, die Sie zuvor für die Kamera festgelegt haben, werden gelöscht. Alle definierten Regeln und Zeitpläne für Wachrundgänge sind hierdurch betroffen und die für die XProtect Smart Client-Benutzer verfügbaren Voreinstellungen werden entfernt.
2. Klicken Sie auf **Löschen**, um überflüssige Voreinstellungen zu löschen.
3. Klicken Sie auf **Bearbeiten**, wenn Sie den Anzeigenamen der Voreinstellung ändern möchten (siehe Umbenennen einer Preset Position (nur Typ 2) auf Seite 257).
4. Wenn Sie solche gerätedefinierten Voreinstellungen später bearbeiten möchten, können Sie dies an der Kamera machen und importieren sie dann erneut.

Zuweisen einer standardmäßigen Preset Position

Bei Bedarf können Sie eine Preset Position einer PTZ-Kamera als die Standard-Preset Position der Kamera festlegen.

Eine Standard-Preset Position kann hilfreich sein, da sie Ihnen gestattet, Regeln zu definieren, die bestimmen, dass PTZ-Kameras unter bestimmten Umständen in die Standard-Preset Position gehen. Zum Beispiel nachdem Sie die PTZ-Kamera manuell bedient haben.

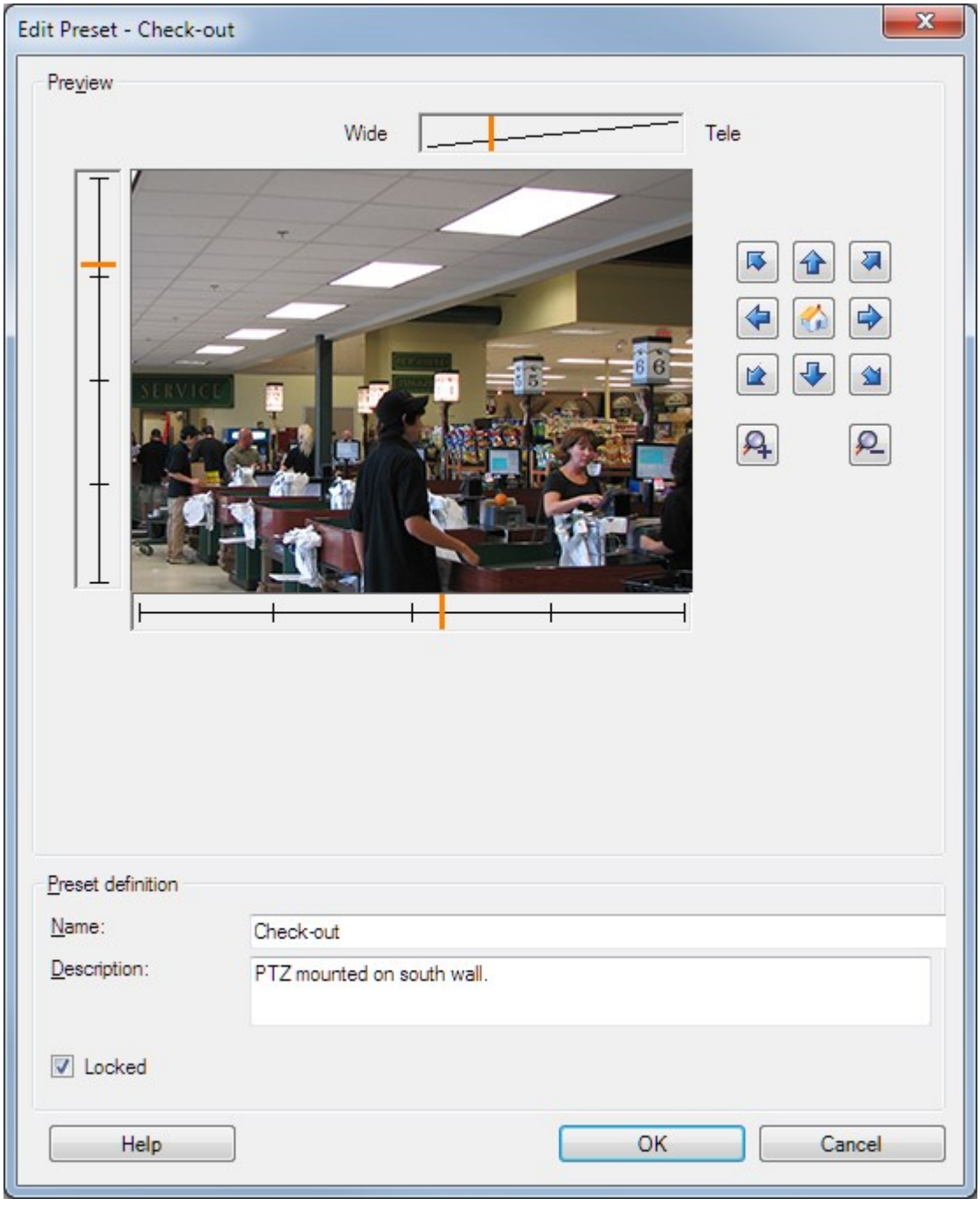
1. Wählen Sie eine Voreinstellung in Ihrer Liste der definierten Preset Positionen aus, um sie als Standard festzulegen.
2. Aktivieren Sie unter der Liste das Kontrollkästchen **Standard-Voreinstellung**.

Sie können nur eine Preset Position als Standard-Preset Position definieren.

Bearbeiten einer Preset-Position (nur Typ 1)

So bearbeiten Sie eine vorhandene, im System definierte Preset Position:

1. Wählen Sie die Preset Position in der Liste verfügbarer Preset Positionen für die Kamera in der Registerkarte **Voreinstellungen** aus.
2. Klicken Sie auf **Bearbeiten**. Das Fenster **Voreinstellung bearbeiten** wird geöffnet:



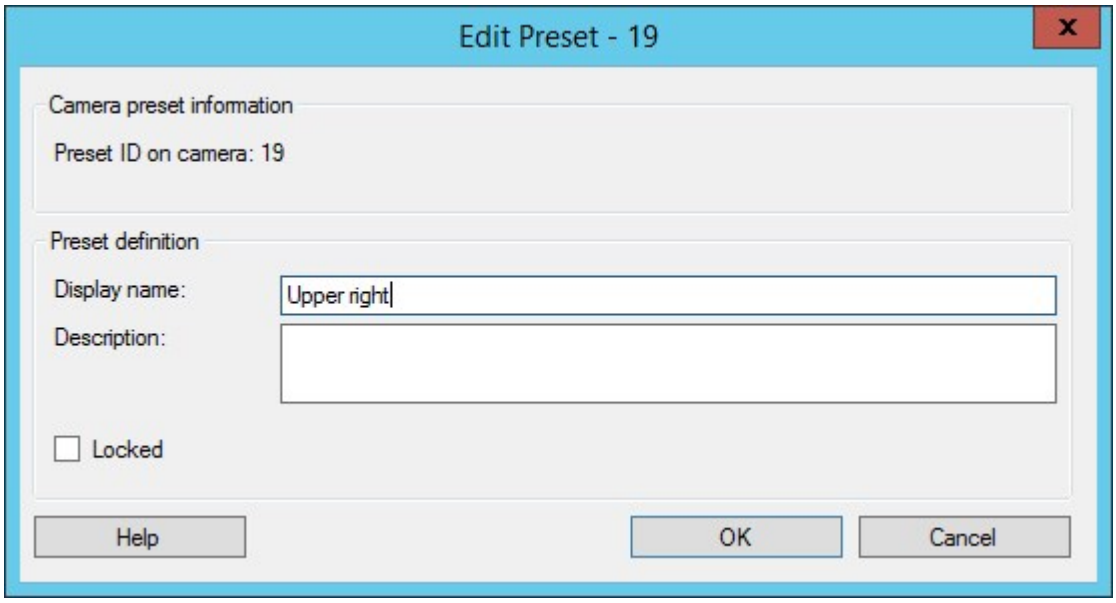
3. Das Fenster **Voreinstellung bearbeiten** zeigt ein Live-Video der Preset Position an. Ändern Sie die Preset Position mit den Navigationsschaltflächen und/oder den Schiebereglern nach Bedarf.
4. Ändern Sie den Namen/die Nummer und die Beschreibung der Preset Position bei Bedarf.

5. Wählen Sie **Gesperrt**, wenn Sie die Preset Position sperren möchten. Nur Benutzer mit der entsprechenden Berechtigung können die Position wieder entsperren.
6. Klicken Sie auf **OK**.

Umbenennen einer Preset Position (nur Typ 2)

So bearbeiten Sie den Namen einer in der Kamera definierten Preset Position:

1. Wählen Sie die Preset Position in der Liste verfügbarer Voreinstellungen für die Kamera in der Registerkarte **Voreinstellungen** aus.
2. Klicken Sie auf **Bearbeiten**. Das Fenster **Voreinstellung bearbeiten** wird geöffnet:



3. Ändern Sie den Namen und fügen Sie bei Bedarf eine Beschreibung der Preset Position hinzu.
4. Wählen Sie **Gesperrt**, wenn Sie den Namen der Voreinstellung sperren möchten. Sie können den Namen einer Preset Position sperren, wenn Sie Benutzer in XProtect Smart Client oder Benutzer mit beschränkten Sicherheitsberechtigungen daran hindern möchten, diese Namen zu aktualisieren oder die Voreinstellung zu löschen. Gesperrte Voreinstellungen werden durch das Symbol angezeigt. Nur Benutzer mit der entsprechenden Berechtigung können den Namen der Voreinstellung wieder entsperren.
5. Klicken Sie auf **OK**.

Sperren einer Preset Position

Sie können eine Preset Position sperren, wenn Sie Benutzer im XProtect Smart Client oder Benutzer mit beschränkten Sicherheitsberechtigungen daran hindern möchten, eine Voreinstellung zu aktualisieren oder zu löschen. Gesperrte Voreinstellungen werden durch das Symbol angezeigt.

Voreinstellungen sperren Sie im Rahmen der Hinzufügung (siehe Hinzufügen einer Preset-Position (Typ 1) auf Seite 253) und der Bearbeitung (siehe Bearbeiten einer Preset-Position (nur Typ 1) auf Seite 255).

Testen einer Preset-Position (nur Typ 1)

1. Wählen Sie die Preset Position in der Liste verfügbarer Preset Positionen für die Kamera in der Registerkarte **Voreinstellungen** aus.
2. Klicken Sie auf **Aktivieren**.
3. Die Kamera wird zur ausgewählten Preset Position bewegt.

Reservierte PTZ-Sitzungen (Erklärung)

Abhängig vom Überwachungssystem können Sie PTZ-Sitzungen reservieren.

Administratoren mit Sicherheitsberechtigungen zum Ausführen einer reservierten PTZ-Sitzung können die PTZ-Kamera in diesem Modus ausführen. So wird verhindert, dass andere Benutzer die Kontrolle über die Kamera übernehmen. Bei einer reservierten PTZ-Sitzung wird das standardmäßige PTZ-Prioritätssystem ignoriert, um zu verhindern, dass Benutzer mit einer höheren PTZ-Priorität die Sitzung unterbrechen.

Sie können die Kamera in einer reservierten PTZ-Sitzung sowohl von XProtect Smart Client als auch von Management Client aus bedienen.

Das Reservieren einer PTZ-Sitzung kann hilfreich sein, wenn Sie dringende Aktualisierungen oder Wartungsarbeiten an einer PTZ-Kamera oder deren Voreinstellungen vornehmen müssen, ohne dabei von anderen Benutzern gestört zu werden.

> Sie können eine PTZ-Sitzung nicht reservieren, wenn ein Benutzer mit einer höheren Priorität als die Ihre die Kamera steuert oder ein anderer Benutzer die Kamera bereits reserviert hat.

PTZ-Sitzung freigeben

Die Schaltfläche **Freigeben** ermöglicht es Ihnen, Ihre aktuelle PTZ-Sitzung freizugeben, sodass ein anderer Benutzer die Kamera steuern kann. Wenn Sie auf **Freigeben** klicken, wird die PTZ-Sitzung sofort beendet und ist für den nächsten Benutzer verfügbar, der die Kamera bedient.

Administratoren, denen die Sicherheitsberechtigung **PTZ-Sitzung freigeben** zugewiesen wurde, können die reservierten PTZ-Sitzungen anderer Benutzer jederzeit freigeben. Dies kann beispielsweise nützlich sein, wenn die PTZ-Kamera oder ihre Voreinstellungen beibehalten werden müssen oder andere Benutzer in Ausnahmesituationen die Kamera aus Versehen gesperrt haben.

Festlegen von PTZ-Sitzungs-Zeitüberschreitungen

Management Client- und XProtect Smart Client-Benutzer mit den notwendigen Benutzerrechten können Wachrundgänge von PTZ-Kameras manuell unterbrechen.

Sie können festlegen, wie viel Zeit vergehen soll, bevor alle PTZ-Kameras in Ihrem System reguläre Wachrundgänge wieder aufnehmen:

1. Wählen Sie **Tools** > **Optionen**.
2. Wählen Sie auf der Registerkarte **Allgemein** im Fenster **Optionen** den Zeitraum in der:
   - Liste **Zeitüberschreitung für manuelle PTZ-Sitzungen** (standardmäßig 15 Sekunden).
   - Liste **Zeitüberschreitung für Anhalten von Wachrundgängen** (standardmäßig 10 Minuten).
   - Liste **Zeitüberschreitung für reservierte PTZ-Sitzungen** (standardmäßig 1 Stunde).

   Diese Einstellungen betreffen alle PTZ-Kameras in Ihrem System.

Sie können die Zeitüberschreitungen individuell für jede Kamera ändern.

1. Klicken Sie im Bereich **Standort-Navigation** auf **Kamera**.
2. Wählen Sie im Bereich „Übersicht“ die Kamera aus.
3. Wählen Sie auf der Registerkarte **Voreinstellungen** den Zeitraum in der:
   - Liste **Zeitüberschreitung für manuelle PTZ-Sitzung** (standardmäßig 15 Sekunden).
   - Liste **Zeitüberschreitung für Anhalten von Wachrundgang** (standardmäßig 10 Minuten).
   - Liste **Zeitüberschreitung für reservierte PTZ-Sitzung** (standardmäßig 1 Stunde).

   Diese Einstellungen betreffen nur diese Kamera.

PTZ-Sitzungs-Eigenschaften

Die Tabelle **PTZ-Sitzung** zeigt den aktuellen Status der PTZ-Kamera an.

Name	Beschreibung
Benutzer	Zeigt den Benutzer an, der die Schaltfläche **Reserviert** gedrückt hat und im Augenblick die PTZ-Kamera steuert. Wenn ein Wachrundgang vom System aktiviert wird, wird **Wachrundgang** angezeigt.
Priorität	Zeigt die PTZ-Priorität des Benutzers an. Sie können PTZ-Sitzungen nur von Benutzern mit einer niedrigeren Priorität übernehmen.
Zeitüberschreitung	Zeigt die verbleibende Zeit der aktuellen PTZ-Sitzung an.
Reserviert	Zeigt an, ob die aktuelle Sitzung eine reservierte PTZ-Sitzung ist oder nicht: • **Wahr**: Reserviert • **Falsch**: Nicht reserviert

Sie können die folgenden Zeitüberschreitungen für jede PTZ-Kamera ändern.

Name	Beschreibung
Zeitüberschreitung für manuelle PTZ-Sitzung	Legen Sie die Zeitüberschreitung für manuelle PTZ-Sitzungen auf dieser Kamera fest, wenn die gewünschte Zeitüberschreitung vom Standard abweichen soll. Sie können den Standardzeitraum im Menü **Tools** unter **Optionen** festlegen.
Zeitüberschreitung für Wachrundgang-Pausierung von PTZ-Sitzung	Legen Sie die Zeitüberschreitung für die Pausierung von PTZ-Sitzungen auf dieser Kamera fest, wenn die gewünschte Zeitüberschreitung vom Standard abweichen soll. Sie können den Standardzeitraum im Menü **Tools** unter **Optionen** festlegen.
Zeitüberschreitung für reservierte PTZ-Sitzung	Legen Sie die Zeitüberschreitung für reservierte PTZ-Sitzungen auf dieser Kamera fest, wenn die gewünschte Zeitüberschreitung vom Standard abweichen soll. Sie können den Standardzeitraum im Menü **Tools** unter **Optionen** festlegen.

Registerkarte „Wachrundgang“ (Geräte)

Registerkarte Wachrundgang (Erklärung)

Die folgenden Geräte besitzen eine Registerkarte **Wachrundgang**:

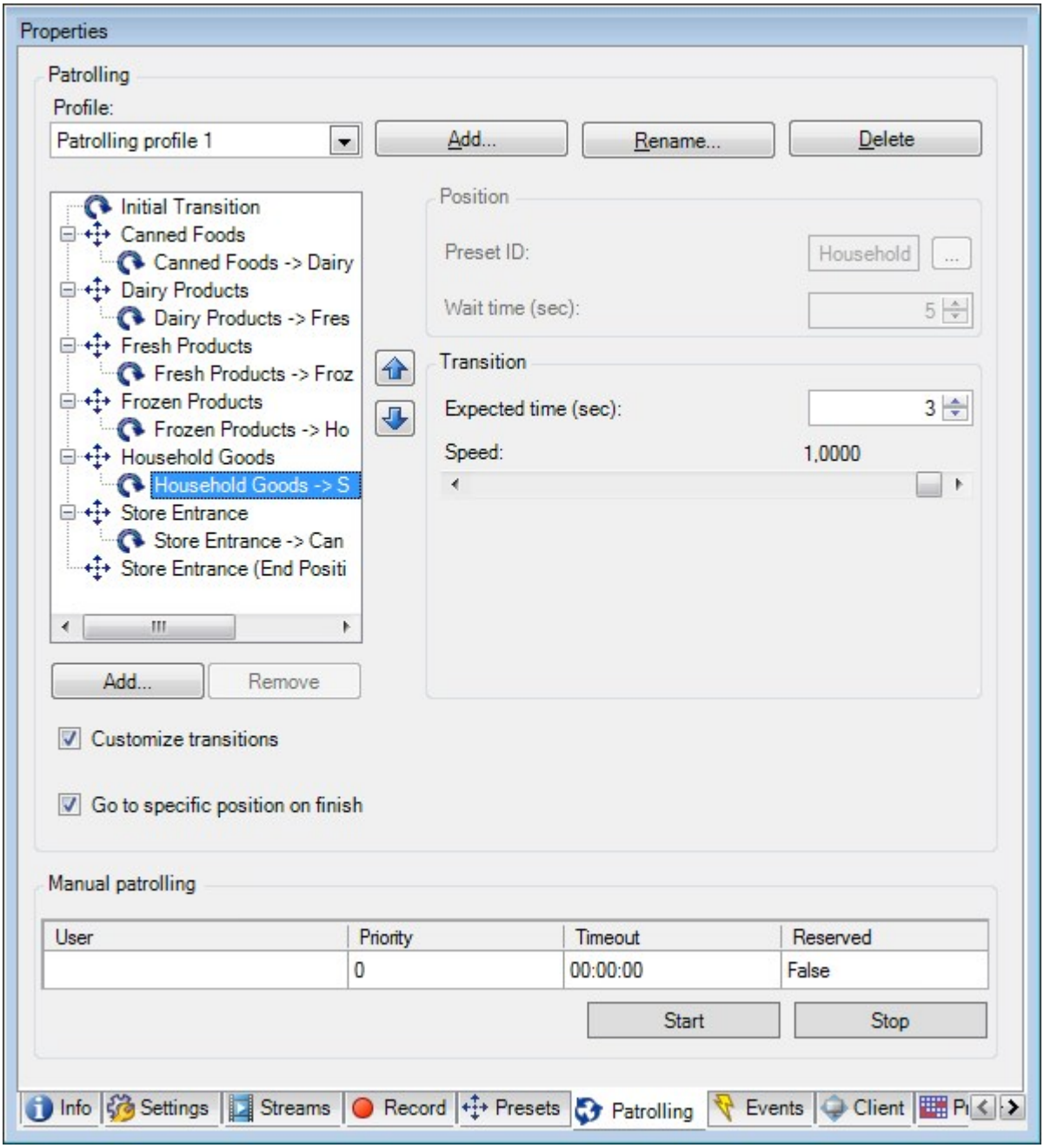
- PTZ-Kameras

Auf der Registerkarte **Wachrundgang** können Sie Wachrundgangprofile erstellen – die automatische Bewegung einer PTZ (Pan/Tilt/Zoom)-Kamera zwischen einer Reihe von voreingestellten Positionen.
Bevor Sie mit der Funktion Wachrundgang arbeiten können, müssen Sie auf der Registerkarte **Voreinstellungen** mindestens zwei voreingestellte Positionen für die Kamera festlegen.

Wachrundgangprofile legen fest, wie Wachrundgänge ablaufen sollen. Dazu gehören die Reihenfolge, in der sich die Kamera zwischen Preset-Positionen bewegen soll, und wie lange sie in jeder Position bleiben soll. Sie können eine unbegrenzte Zahl von Wachrundgangprofilen erstellen und sie in Ihren Regeln verwenden. Beispielsweise können Sie eine Regel erstellen, die festlegt, dass während der Öffnungszeiten tagsüber ein Wachrundgangprofil und nachts ein anderes Profil verwendet werden sollen.

Bevor Sie ein Wachrundgangprofil z. B. in einer Regel anwenden, können Sie es mit einem manuellen Wachrundgang testen. Sie können einen manuellen Wachrundgang auch verwenden, um einen Wachrundgang von einem anderen Benutzer oder von einem Wachrundgang mit aktivierter Regel zu übernehmen, sofern Sie eine höhere PTZ-Priorität haben.

Sie können im Bereich **Manueller Wachrundgang** überwachen, ob das System derzeit einen Wachrundgang durchführt oder ein Benutzer die Kontrolle übernommen hat.



Registerkarte **Wachrundgang**, die ein Wachrundgangprofil mit angepassten Übergängen zeigt.

Hinzufügen eines Wachrundgangprofils auf Seite 262

Festlegen von Preset-Positionen in einem Wachrundgangprofil auf Seite 262

Festlegen der Zeit in jeder Preset Position auf Seite 263

Übergänge anpassen (PTZ) auf Seite 263

Festlegen einer Endposition auf Seite 264

Festlegen einer manuellen PTZ-Sitzungs-Zeitüberschreitung (siehe Registerkarte Registerkarte „Voreinstellungen“ (Geräte) auf Seite 251)

Hinzufügen eines Wachrundgangprofils

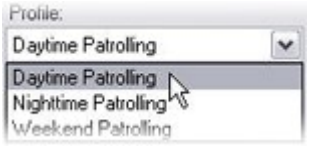
Hinzufügen eines Profils, das Sie in einer Regel verwenden möchten:

1. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Profil hinzufügen** wird angezeigt.
2. Geben Sie im Dialogfeld **Profil hinzufügen** einen Namen für das Wachrundgangprofil an.
3. Klicken Sie auf **OK**. Wenn der Name nicht einzigartig ist, ist die Schaltfläche deaktiviert.

   Das neue Wachrundgangprofil wird zur Liste **Profil** hinzugefügt. Sie können nun die Preset Position und andere Einstellungen für das Wachrundgangprofil festlegen.

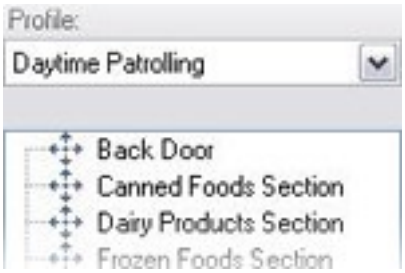
Festlegen von Preset-Positionen in einem Wachrundgangprofil

1. Wählen Sie das Wachrundgangprofil aus der Liste **Profil** aus.



2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie im Dialogfenster **Voreinstellung auswählen** die Preset Position für Ihr Wachrundgangprofil aus:

4. Klicken Sie auf **OK**. Die ausgewählten Voreinstellungsoptionen werden der Liste für Preset Positionen für das Wachrundgangprofil hinzugefügt:



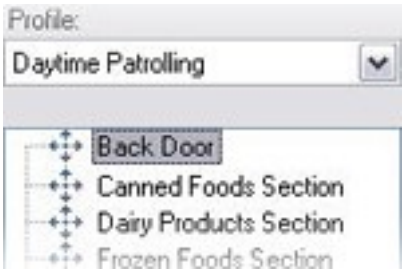
5. Die Kamera nutzt die Preset Position oben in der Liste als ersten Stopp, wenn sie einen Wachrundgang entsprechend dem Wachrundgangprofil ausführt. Die zweite Preset Position von oben ist der zweite Stopp usw.

Festlegen der Zeit in jeder Preset Position

Während des Wachrundgangs verbleibt die PTZ-Kamera standardmäßig 5 Sekunden an jeder Preset Position, die im Wachrundgang festgelegt ist.

So ändern Sie die Anzahl an Sekunden:

1. Wählen Sie das Wachrundgangprofil aus der Liste **Profil** aus.
2. Wählen Sie die Preset Position, deren Zeit Sie ändern wollen, aus:



3. Legen Sie die Zeit im Feld **Zeit an Position (s)** fest:
4. Wiederholen Sie diese Schritte ggf. für andere Preset Positionen.

Übergänge anpassen (PTZ)

Standardmäßig wird der Zeitraum, den die Kamera zur Bewegung von einer Preset Position zur nächsten benötigt, der sogenannte **Übergang**, auf drei Sekunden geschätzt. In diesem Zeitraum ist die Bewegungserkennung auf der Kamera standardmäßig deaktiviert, da sonst wahrscheinlich irrelevante Bewegung erkannt wird, während sich die Kamera zwischen den Preset Positionen bewegt.

Sie können Übergangsgeschwindigkeiten nur anpassen, wenn Ihre Kamera PTZ-Scanning unterstützt und Preset Positionen auf Ihrem System-Server konfiguriert und gespeichert werden (PTZ-Kamera Typ 1). Andernfalls ist der Schieberegler **Geschwindigkeit** ausgegraut.

Sie können Folgendes anpassen:

- Die geschätzte Übergangszeit
- Die Geschwindigkeit, mit der sich die Kamera während eines Übergangs bewegt

So passen Sie Übergänge zwischen den unterschiedlichen Preset Positionen an:

1. Wählen Sie das Wachrundgangprofil aus der Liste **Profil** aus.
2. Aktivieren Sie das Kontrollkästchen **Übergänge anpassen**.

   Übergangsanzeigen werden zur Liste der Preset Positionen hinzugefügt.
3. Wählen Sie auf der Liste den Übergang aus.

4. Legen Sie die geschätzte Übergangszeit (in Sekunden) im Feld **Geschätzte Zeit (Sek.)** fest.

5. Verwenden Sie den Schieberegler **Geschwindigkeit**, um die Übergangszeit festzulegen. Wenn sich der Schieberegler ganz rechts befindet, bewegt sich die Kamera in ihrer standardmäßigen Geschwindigkeit. Je weiter Sie den Schieberegler nach links bewegen, desto langsamer bewegt sich die Kamera während des ausgewählten Übergangs.
6. Wiederholen Sie dies bei Bedarf für weitere Übergänge.

Festlegen einer Endposition

Sie können angeben, dass sich die Kamera am Ende des im ausgewählten Wachrundgangprofil voreingestellten Wachrundgangs an eine bestimmte Preset Position bewegen soll.

1. Wählen Sie das Wachrundgangprofil aus der Liste **Profil** aus.
2. Aktivieren Sie das Kontrollkästchen **Am Ende des Wachgangs zu bestimmter Position gehen**. Das Dialogfeld **Voreinstellung auswählen** wird geöffnet.
3. Wählen Sie die Endposition aus und klicken sie auf **OK**.

> Sie können jede Preset Position der Kamera als Endposition auswählen. Sie sind nicht auf die im Wachrundgangprofil verwendeten Preset Positionen beschränkt.

4. Die ausgewählte Position wird der Liste „Profil“ hinzugefügt.

   Am Ende des im ausgewählten Wachrundgangprofil festgelegten Wachrundgang bewegt sich die Kamera zur festgelegten Endposition.

Manueller Wachrundgang (Erklärung)

Wenn Sie ein Wachrundgangprofil erstellt haben, können Sie es durch einen manuellen Wachrundgang testen, bevor Sie es im System anwenden. Verwenden Sie die Schaltflächen **Start** und **Stopp**, um manuelle Wachrundgänge zu initiieren und anzuhalten.

Wenn sich die Kamera bereits auf einem Wachrundgang befindet oder durch einen anderen Benutzer gesteuert wird, können Sie manuelle Wachrundgänge nur starten, wenn Sie eine höhere Priorität haben.

Wenn Sie einen manuellen Wachrundgang starten, während die Kamera einen Wachrundgang mit aktiver Regel durchführt, nimmt das System diesen Wachrundgang wieder auf, sobald Sie Ihren manuellen Wachrundgang beenden. Wenn ein anderer Benutzer einen manuellen Wachrundgang durchführt, Sie aber höhere Priorität besitzen und Ihren manuellen Wachrundgang starten, wird der manuelle Wachrundgang des anderen Benutzers nicht wieder aufgenommen.

Wenn Sie Ihren manuellen Wachrundgang nicht selbst beenden, wird er fortgesetzt bis ein Wachrundgang mit aktiver Regel oder ein Benutzer mit höherer Priorität übernimmt. Wenn der System-Wachrundgang mit aktiver Regel endet, nimmt das System Ihren manuellen Wachrundgang wieder auf. Wenn ein anderer Benutzer einen manuellen Wachrundgang startet, endet Ihr manueller Wachrundgang und wird nicht wieder aufgenommen.

Wenn Sie Ihren manuellen Wachrundgang beenden und eine Endposition für Ihr Wachrundgangprofil über **Am Ende des Wachgangs zu bestimmter Position gehen** festgelegt haben, kehrt die Kamera auf diese Position zurück.

Eigenschaften manueller Wachrundgänge

Die Tabelle **Manueller Wachrundgang** zeigt den aktuellen Status der PTZ-Kamera an.

Name	Beschreibung
Benutzer	Zeigt den Benutzer an, der entweder die PTZ-Sitzung reserviert oder einen manuellen Wachrundgang gestartet hat und im Augenblick die Kamera steuert. Wenn ein Wachrundgang vom System aktiviert wird, wird **Wachrundgang** angezeigt.

Name	Beschreibung
Priorität	Zeigt die PTZ-Priorität des Benutzers an. Sie können PTZ-Sitzungen nur von Benutzern oder Wachrundgangprofilen mit einer niedrigeren Priorität übernehmen.
Zeitüberschreitung	Zeigt die verbleibende Zeit der aktuellen reservierten oder manuellen PTZ-Sitzungen an.
Reserviert	Zeigt an, ob die aktuelle Sitzung eine reservierte PTZ-Sitzung ist oder nicht. • **Wahr**: Reserviert • **Falsch**: Nicht reserviert

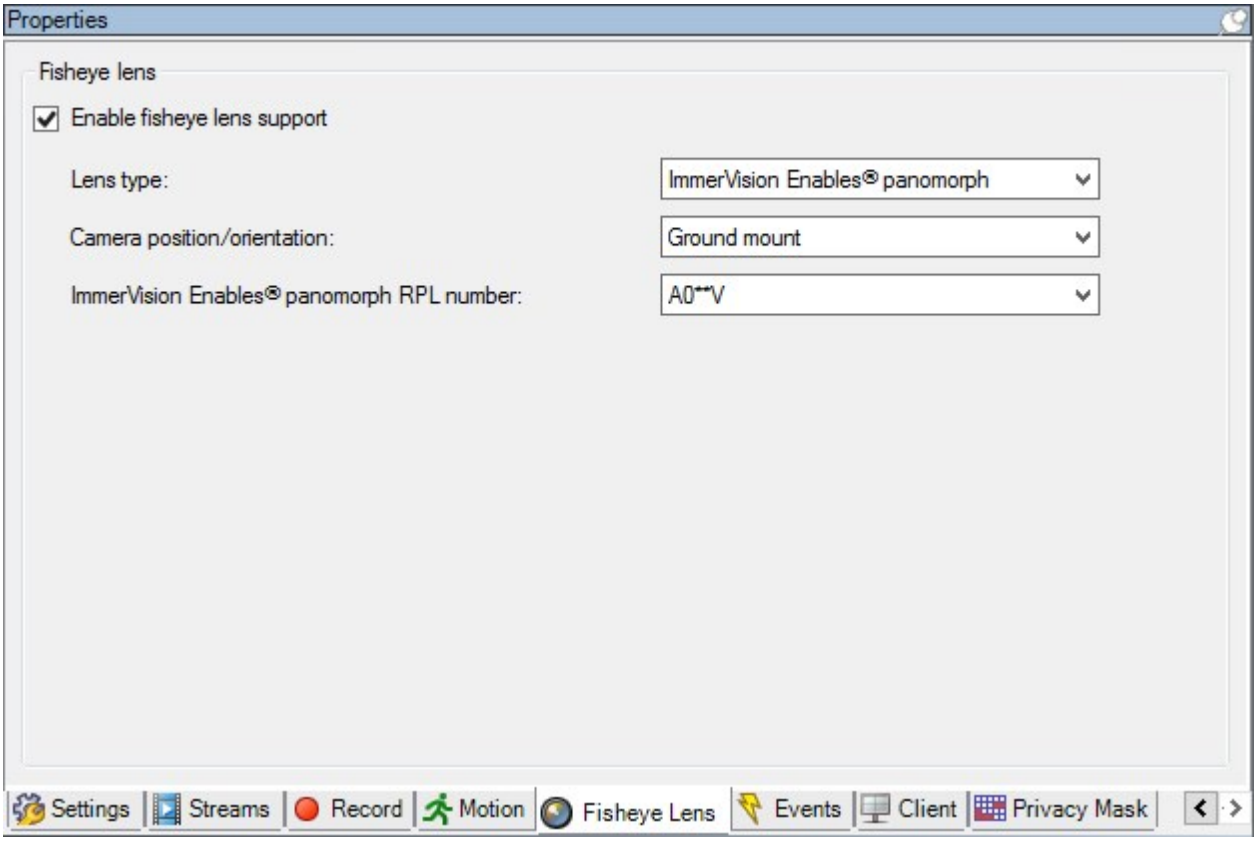
Registerkarte „Fischaugen-Linse“ (Geräte)

Registerkarte Fischaugen-Linse (Erklärung)

Die folgenden Geräte besitzen eine Registerkarte **Fischaugen-Linse**:

- Fixierte Kameras mit einer Fischaugen-Linse

In der Registerkarte **Fischaugen-Linse** können Sie die Unterstützung für Fischaugen-Linsen für die ausgewählte Kamera aktivieren und konfigurieren.



Unterstützung für Fischaugen-Linse aktivieren und deaktivieren

Die Unterstützung für Fischaugen-Linsen ist standardmäßig deaktiviert.

Wählen Sie im Kontrollkästchen **Unterstützung für Fischaugen-Linse** in der Registerkarte **Fischaugen-Linse** an oder ab, um es zu aktivieren bzw. deaktivieren.

Einstellungen für Fischaugen-Linse bestimmen

Wenn sie Unterstützung für Fischaugen-Linsen aktivieren:

1. Wählen Sie den Linsentyp aus.
2. Die physische Position/Ausrichtung der Kamera können Sie in der Liste **Kameraposition/Kameraausrichtung** bestimmen.
3. Wählen Sie eine Registered Panomorph Lens (RPL)-Nummer aus der Liste der **ImmerVision Enables® Panomorph-RPL-Nummern**.

   Dies gewährleistet eine ordnungsgemäße Identifikation und Konfiguration der Linse, die mit der Kamera verwendet wird. Sie finden normalerweise die RPL-Nummer auf der Linse selbst oder auf der Box mit der sie geliefert wurde. Für weitere Informationen über ImmerVision, Panomorph-Linsen und RPL, siehe Immervision Webseite (https://www.immervisionenables.com/).

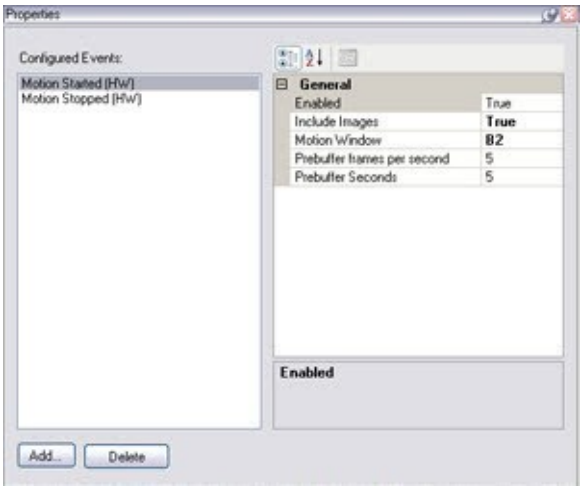
Registerkarte „Ereignisse“ (Geräte)

Registerkarte Ereignisse (Erklärung)

Die folgenden Geräte besitzen eine Registerkarte **Ereignisse**:

- Kameras
- Mikrofone
- Eingänge

Zusätzlich zum Ereignis des Systems, können einige Geräte so eingestellt werden, dass sie Ereignisse auslösen. Sie können diese Ereignisse verwenden, wenn Sie auf Ereignissen basierende Regeln im System erstellen. Eigentlich passieren sie sogar direkt an der Hardware/Gerät als im Überwachungssystem.



Registerkarte **Ereignis**, Beispiel von **Kamera**.

Wenn Sie ein Ereignis löschen, betrifft dies alle Regeln, die dieses Ereignis verwenden.

- Ein Ereignis hinzufügen auf Seite 268
- Ereigniseigenschaften festlegen auf Seite 269
- Verwenden von mehreren Instanzen eines Ereignisses auf Seite 269

Ein Ereignis hinzufügen

1. Wählen Sie im Fenster **Übersicht** ein Gerät aus.
2. Wählen Sie die Registerkarte **Ereignisse** und klicken Sie auf **Hinzufügen**. Dies öffnet das Fenster **Treiberereignis auswählen**.
3. Wählen sie ein Ereignis aus. Sie können nur ein Ereignis zur selben Zeit auswählen.

4. Wenn Sie eine Gesamtliste aller Ereignisse anschauen möchten, aus der Sie Ereignisse hinzufügen können, die bereits hinzugefügt wurden, wählen Sie **Bereits hinzugefügte Ereignisse anzeigen**.
5. Klicken Sie auf **OK**.
6. Klicken Sie in der Symbolleiste auf **Speichern**.

Ereigniseigenschaften festlegen

Sie können die Eigenschaften für jedes hinzugefügte Ereignis festlegen. Die Anzahl der Eigenschaften hängt vom Gerät und Ereignis ab. Damit das Ereignis wie gewollt funktioniert, müssen Sie einige oder alle Eigenschaften identisch sowohl auf dem Gerät als auch in dieser Registerkarte festlegen.

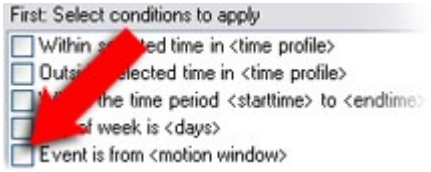
Verwenden von mehreren Instanzen eines Ereignisses

Sie können ein Ereignis mehr als einmal hinzufügen, um verschiedene Eigenschaften für verschiedene Instanzen eines Ereignisses zu bestimmen.

Das folgende Beispiel bezieht sich speziell auf Kameras.

Beispiel: Sie haben die Kamera mit zwei Bewegungsfenstern eingestellt, nämlich A1 und A2. Sie haben zwei Instanzen für das Ereignis Bewegung gestartet (HW) hinzugefügt. In den Eigenschaften einer Instanz haben Sie die Verwendung des Bewegungsfenster A1 festgelegt. In den Eigenschaften der anderen Instanz haben Sie die Verwendung des Bewegungsfenster A2 festgelegt.

Wenn Sie ein Ereignis in einer Regel verwenden, können Sie festlegen, dass das Ereignis auf erkannte Bewegung in einem bestimmten Bewegungsfenster reagieren sollte, damit die Regel ausgelöst wird:



Registerkarte „Ereignis“ (Eigenschaften)

Name	Beschreibung
Konfigurierte Ereignisse	Welches Ereignis Sie auswählen und in der Liste für **Konfigurierte Ereignisse** hinzufügen können, hängt ganz vom Gerät und seinen Einstellungen ab. Für einige Gerätetypen ist die Liste leer.

Name	Beschreibung
Allgemein	Die Liste der Eigenschaften hängt vom Gerät und dem Ereignis ab. Damit das Ereignis wie gewollt funktioniert, müssen Sie einige oder alle Eigenschaften identisch sowohl auf dem Gerät als auch in dieser Registerkarte festlegen.

Registerkarte „Client“ (Geräte)

Registerkarte Client (Erklärung)

Die folgenden Geräte besitzen eine Registerkarte **Client**:

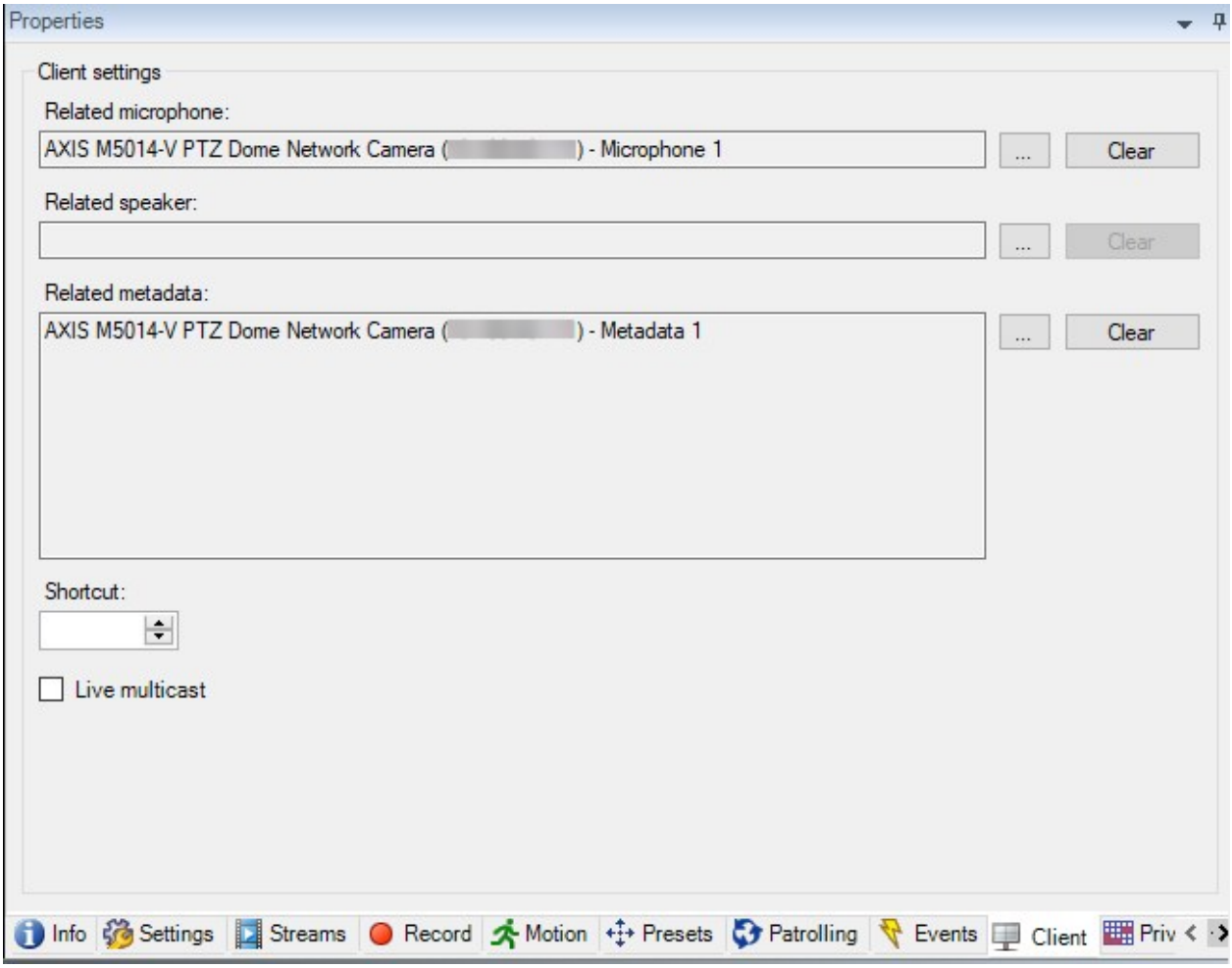
- Kameras

Auf der Registerkarte **Client** können Sie bestimmen, welche anderen Geräte angezeigt und gehört werden, wenn Sie eine Kamera im XProtect Smart Client verwenden.

Die dazugehörigen Geräte zeichnen auch dann auf, wenn die Kamera aufzeichnet, siehe Aktivieren der Aufzeichnung auf zugehörigen Geräten auf Seite 237.

Sie können außerdem **Live-Multicast** auf der Kamera aktivieren. Es bedeutet, dass die Kamera Live-Streams über den Aufzeichnungsserver an die Clients multicastet.

Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet.



Siehe auch:

- Aktivieren Sie Multicasting für den Recording-Server auf Seite 181
- Multicasting (Erklärung) auf Seite 180

Eigenschaften der Registerkarte „Client“

Name	Beschreibung
Zugehöriges Mikrofon	Legen Sie fest, von welchem Mikrofon an der Kamera XProtect Smart Client-Benutzer standardmäßig Audio empfangen. Der XProtect Smart Client-Benutzer kann ggf. manuell wählen,

Name	Beschreibung
	über ein anderes Mikrofon zuzuhören. Geben Sie das Mikrofon an, das zur Push-Videokamera gehört, mit der Video mit Ton gestreamt werden soll. Die zugehörigen Mikrofone zeichnen auf, wenn die Kamera aufzeichnet.
Zugehöriger Lautsprecher	Legen Sie fest, über welche Lautsprecher an der Kamera XProtect Smart Client-Benutzer standardmäßig sprechen. Der XProtect Smart Client-Benutzer kann bei Bedarf manuell einen anderen Lautsprecher auswählen. Die zugehörigen Lautsprecher zeichnen auf, wenn die Kamera aufzeichnet.
Zugehörige Metadaten	Legen Sie ein oder mehrere Metadatengeräte an der Kamera fest, von welchem XProtect Smart Client-Benutzer Metadaten empfangen werden können. Zugehörige Metadatengeräte zeichnen auf, wenn die Kamera aufzeichnet.
Verknüpfung	Definieren Sie Tastenkombinationen zu den Kameras, um die Kameraauswahl für die XProtect Smart Client-Benutzer zu erleichtern. • Erstellen Sie jede Tastenkombination so, dass sie die Kamera eindeutig identifiziert. • Die Kamera Kurzwahlnummer darf nicht länger als vier Ziffern sein.
Live Multicast	Ihr System unterstützt Multicast von Live-Streams vom Aufzeichnungsserver zum XProtect Smart Client. Zum Aktivieren von Multicast für Live-Streams von der Kamera, wählen Sie bitte das Kontrollkästchen aus.

Name	Beschreibung
	Live-Multicasting funktioniert nur in dem Stream, den Sie auf der Registerkarte **Streams** als Standardstream für die Kamera angegeben haben. Außerdem müssen Sie Multicasting für den Aufzeichnungsserver konfigurieren. Siehe Registerkarte „Multicast“ (Aufzeichnungsserver) auf Seite 178. Multicast-Streams werden nicht verschlüsselt, selbst wenn der Aufzeichnungsserver eine Verschlüsselung verwendet.

Registerkarte Einrichtung von Privatsphärenausblendung (Geräte)

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

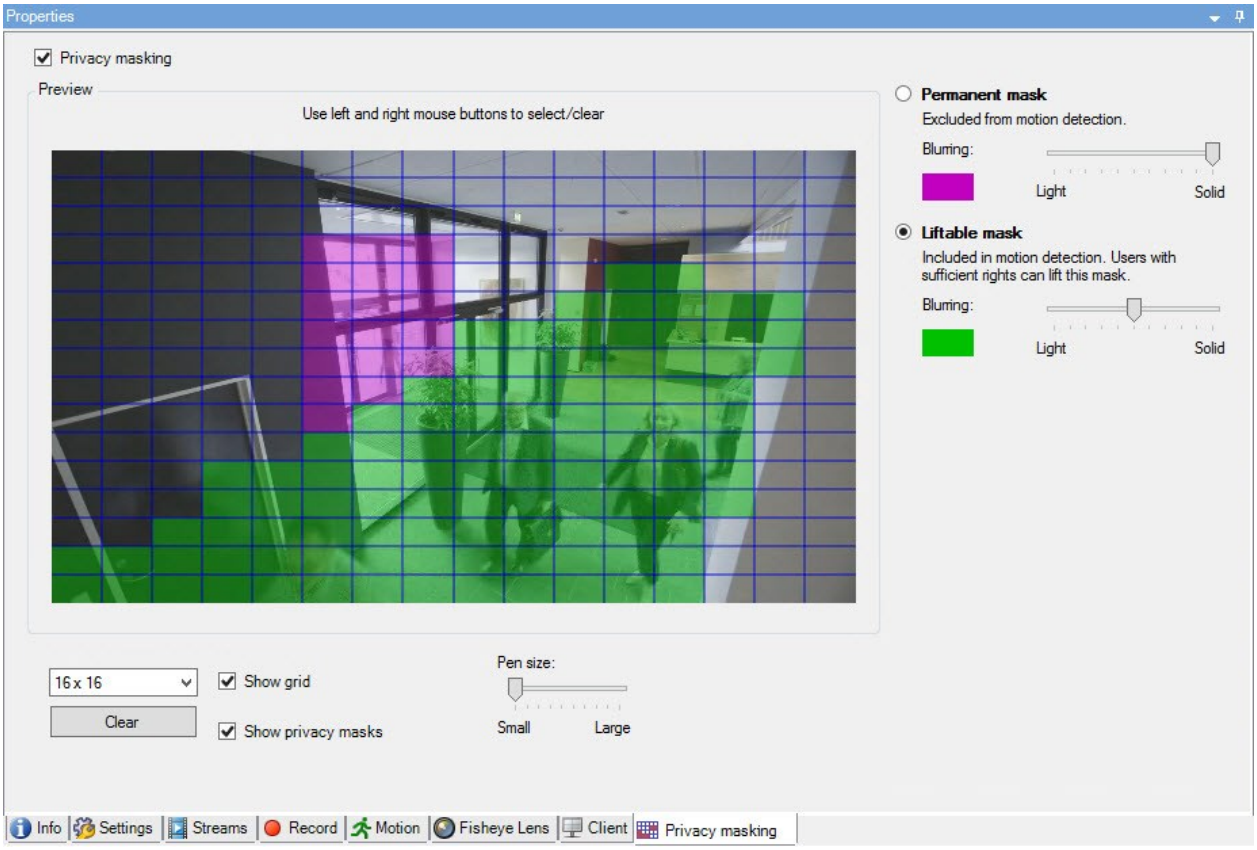
XProtect Essential+ 2018 R1 und neuere Versionen unterstützen die Einrichtung von Privatsphärenausblendung nicht. Wenn Sie also ein Upgrade auf einem System vornehmen, in dem Privatzonenmasken eingerichtet sind, werden diese entfernt.

Registerkarte Privatsphärenausblendung (Erklärung)

Folgende Geräte besitzen eine Registerkarte **Privatsphärenausblendung**:

- Kameras

Auf der Registerkarte **Privatsphärenausblendung** können Sie Privatzonenmaske für die ausgewählte Kamera aktivieren und konfigurieren.



Privatzonenmasken werden angewendet und auf einem Bereich des Kamerabilds verriegelt, sodass der gedeckte Bereich nicht den Schwenk-Neige-Zoom-Bewegungen folgt, sondern konstant den gleichen Bereich des Kamerabilds deckt. Auf manchen PTZ-Kameras können Sie an der Kamera selbst positionsbasierte Privatsphärenausblendung aktivieren.

In einer Milestone Interconnect-Einstellung ignoriert ein zentraler Standort die Privatzonenmasken in einem Remote-System. Wenn Sie die gleichen Privatzonenmasken anwenden möchten, müssen Sie diese am zentralen Standort neu festlegen.

- Privatsphärenausblendung (Erklärung) auf Seite 275
- Aktivieren/Deaktivieren von Privatsphärenausblendung auf Seite 277
- Privatzonenmasken festlegen auf Seite 277
- Ändern des Timeout für aufgehobene Privatzonenmasken auf Seite 279
- Benutzerberechtigung zum Aufheben von Privatzonenmasken erteilen auf Seite 278
- Erstellen Sie einen Bericht von der Konfiguration Ihrer Privatsphärenausblendung auf Seite 280

Privatsphärenausblendung (Erklärung)

Mit Privatsphärenausblendung können Sie festlegen, welche Bereiche des Videos von einer Kamera Sie mit Privatzonenmasken zu decken wünschen, wenn sie im Client gezeigt werden. Wenn eine Überwachungskamera beispielsweise eine Straße abdeckt, können Sie mit Privatzonenmasken bestimmte Bereiche eines Gebäudes (wie Fenster und Türen) verdecken, um die Privatsphäre der Bewohner zu schützen. In manchen Ländern ist dies eine gesetzliche Anforderung.

Sie können Privatzonenmasken als massiv oder unscharf bestimmen. Die Zonen decken Live-Videos, aufgezeichnete und exportierte Videos.

Es gibt zwei Typen von Privatzonenmasken:

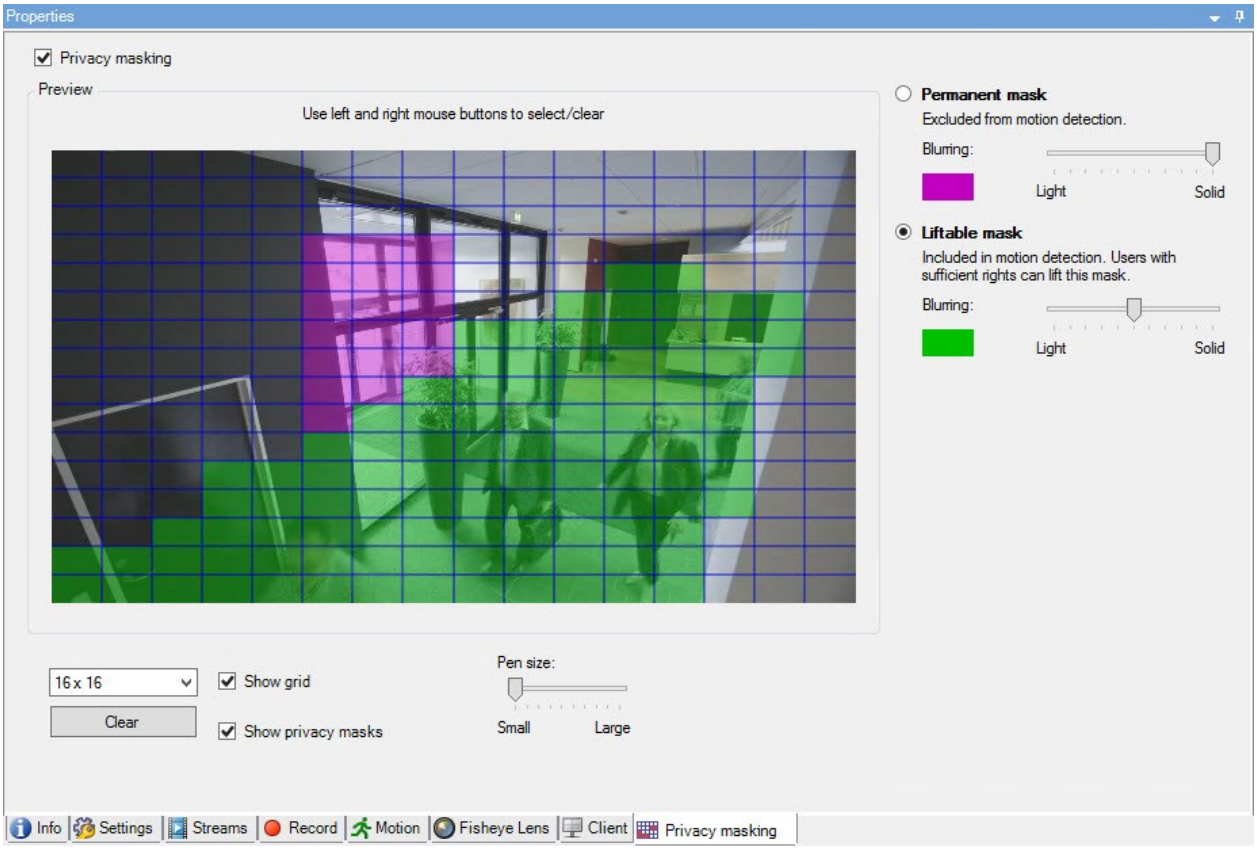
- **Permanente Privatzonenmaske**: Bereiche mit diesem Privatzonenmaskentyp sind in den Clients immer gedeckt. Sie können benutzt werden, um Bereiche des Videos abzudecken, die niemals Überwachung erfordern, wie öffentliche Bereiche oder Bereiche, in denen Überwachung nicht genehmigt ist. Bewegungserkennung ist ausgeschlossen von Bereichen mit permanenten Privatzonenmasken
- **Aufhebbare Privatzonenmaske**: Bereiche mit diesem Maskentyp können in XProtect Smart Client zeitweise aufgedeckt werden, von Benutzern mit der Ermächtigung zum Aufheben von Privatzonenmasken. Wenn der in XProtect Smart Client eingeloggte Benutzer kein Recht zum Aufheben der Privatzonenmasken hat, verlangt das System, dass ein befugter Benutzer die Aufhebung genehmigt. Privatzonenmasken werden aufgehoben, bis sie abgelaufen sind oder der Benutzer sie erneut anwendet. Seien Sie sich bewusst, dass Privatzonenmasken auf Video von allen Kameras aufgehoben werden, auf die der Benutzer Zugriff hat

> Wenn Sie ein Upgrade von einem 2017 R3-System oder älter vornehmen, in dem Privatzonenmasken angewendet sind, werden diese in aufhebbare Privatzonenmasken umgewandelt.

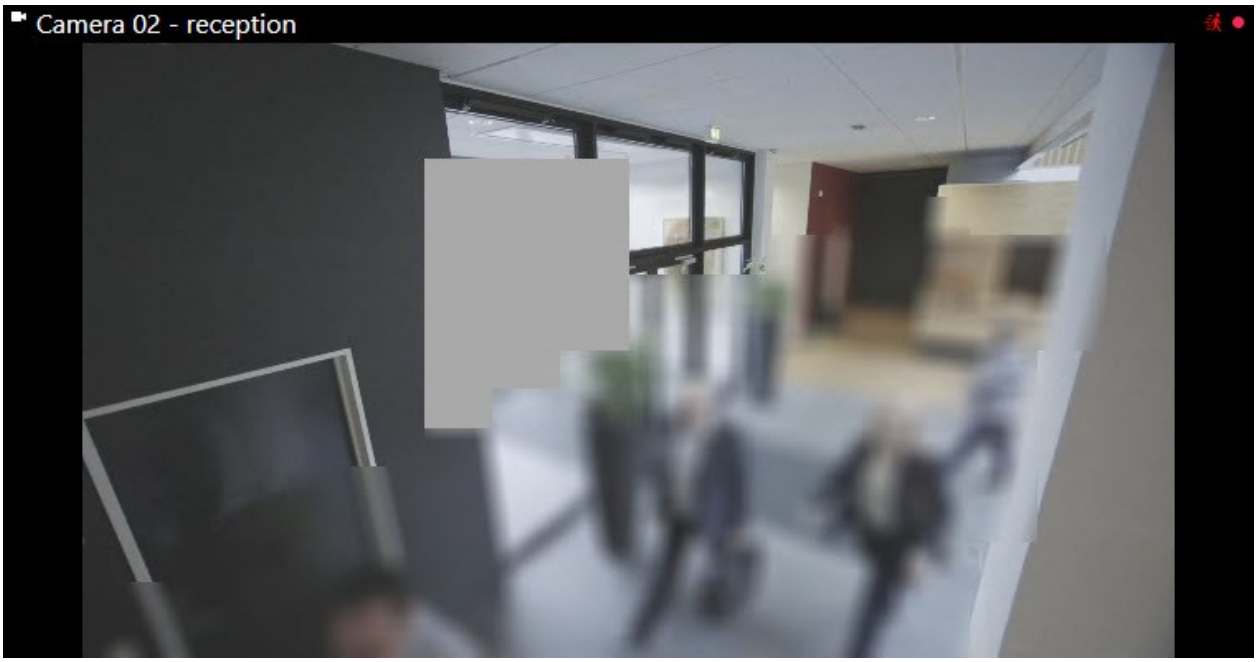
Wenn ein Benutzer Videoaufnahmen von einem Client exportiert oder abspielt, enthält das Video die zum Zeitpunkt der Aufnahme konfigurierten Privatzonenmasken, auch wenn Sie diese später geändert oder entfernt haben. Wenn der Datenschutz beim Exportieren aufgehoben wird, enthält das exportierte Video **nicht** die aufhebbaren Privatzonenmasken.

> Wenn Sie die Einstellungen der Privatsphärenausblendung oft ändern, beispielsweise einmal pro Woche, kann Ihr System potenziell überlastet werden.

Beispiel der Registerkarte **Privatsphärenausblendung** mit konfigurierten Privatzonenmasken:



Und so erscheinen sie in den Clients:



Sie können den Client über die Einstellungen der permanenten und aufhebbaren Privatzonenmasken informieren.

Aktivieren/Deaktivieren von Privatsphärenausblendung

Die Funktion für „Privatsphärenausblendung“ ist standardmäßig nicht aktiviert.

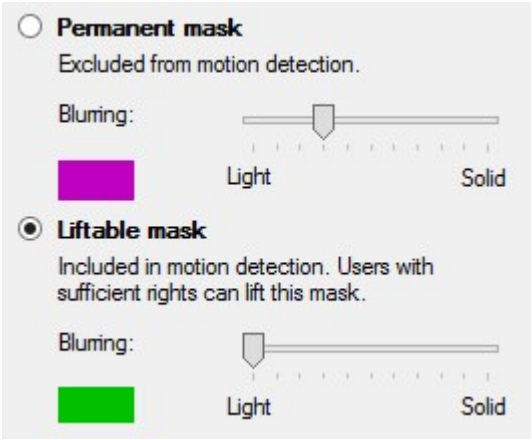
So aktivieren/deaktivieren Sie die Funktion „Privatsphärenausblendung“ für eine Kamera:

- Aktivieren oder deaktivieren Sie auf der Registerkarte **Privatsphärenausblendung** das Kontrollkästchen **Privatsphärenausblendung**

Privatzonenmasken festlegen

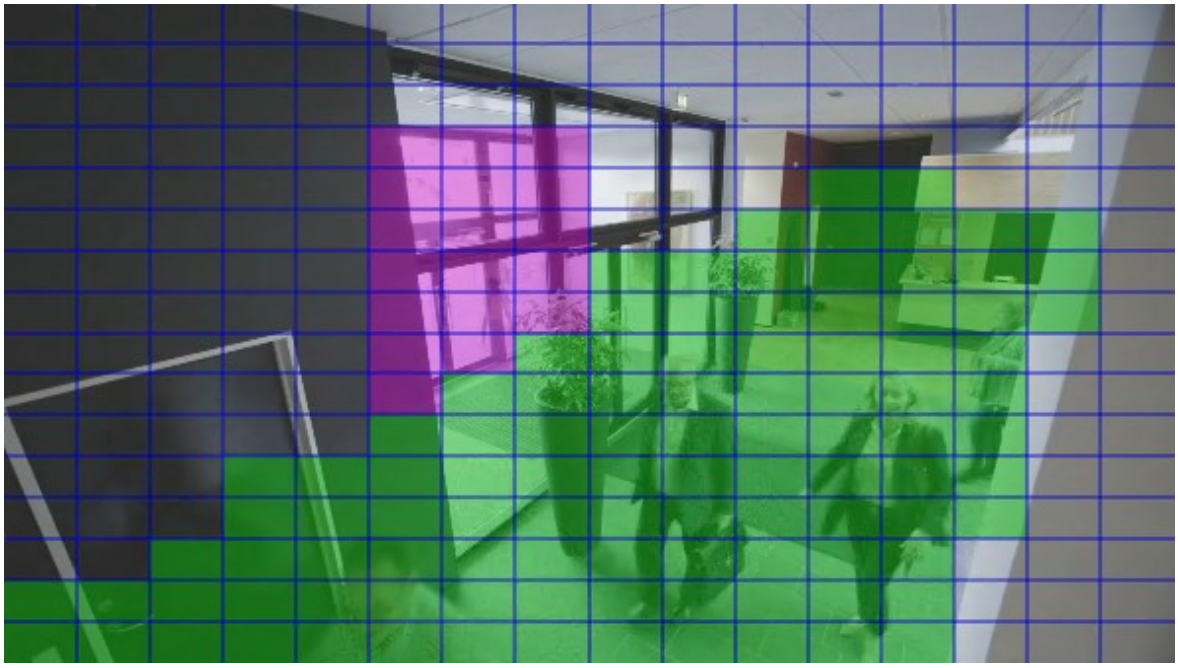
Wenn Sie die Privatsphärenausblendung-Funktion auf der Registerkarte **Privatzonenmaske** aktivieren, kommt ein Raster zur Anwendung auf die Kameravorschau.

1. Zum Abdecken eines Bereichs mit einer Privatzone wählen Sie zuerst eine permanente oder aufhebbare Privatzone.



2. Ziehen Sie den Mauszeiger über die Vorschau. Drücken Sie die linke Maustaste, um einen Rasterabschnitt auszuwählen. Drücken Sie die rechte Maustaste, um den Rasterabschnitt abzuwählen.

3. Sie können so viele Privatzonenmasken festlegen, wie Sie benötigen. Bereiche mit permanenten Privatzonenmasken erscheinen in Violett und Bereiche mit aufhebbaren Privatzonenmasken in Grün.



4. Bestimmen Sie, wie die Abdeckung der Bereiche im Video erscheinen soll, wenn dieses im Client gezeigt wird. Benutzen Sie die Schieber, um von einer leichten Unschärfe auf eine voll intransparente Maske zu wechseln.

> Permanente Privatzonenmasken werden auch auf der Registerkarte **Motion** eingeblendet.

5. Prüfen Sie in XProtect Smart Client, ob die Privatzonenmasken so eingeblendet werden, wie von Ihnen festgelegt.

Benutzerberechtigung zum Aufheben von Privatzonenmasken erteilen

Als Standard hat kein Benutzer die Berechtigung, Privatzonenmasken in XProtect Smart Client aufzuheben.

Aktivieren/deaktivieren der Berechtigung:

1. Wählen Sie unter **Rollen** die Rolle, der Sie die Berechtigung zur Aufhebung von Privatzonenmasken zu erteilen wünschen.
2. Auf der Registerkarte **Allgemeine Sicherheit** wählen Sie **Kameras**.
3. Wählen Sie das Kontrollkästchen **Genehmigen** für die Berechtigung zum **Aufheben von Privatzonenmasken**.

Benutzer, denen Sie diese Rolle zugewiesen haben, können Privatzonenmasken, die als aufhebbare Privatzonenmasken konfiguriert sind, selbst aufheben und das Aufheben auch für andere Benutzer XProtect Smart Client genehmigen.

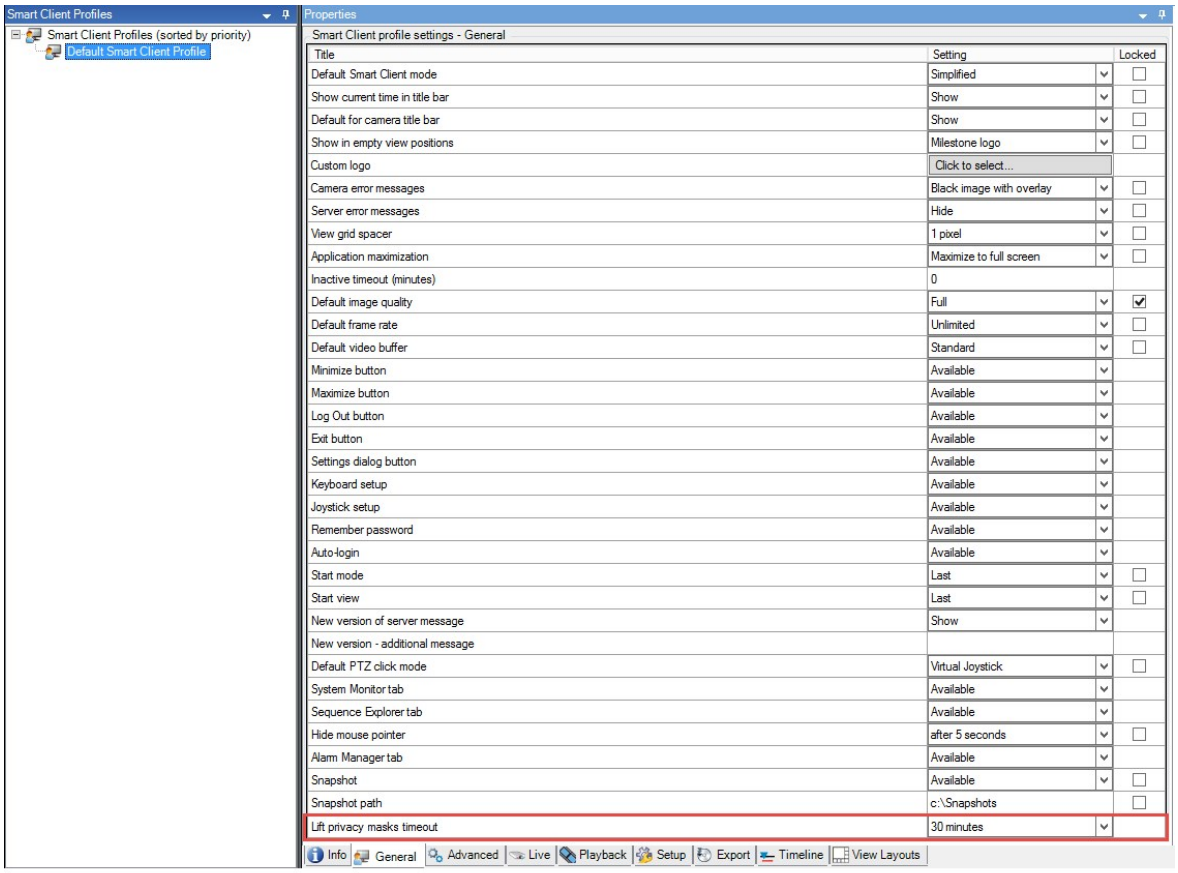
Ändern des Timeout für aufgehobene Privatzonenmasken

Als Standard werden Privatzonenmasken in XProtect Smart Client für 30 Minuten aufgehoben und anschließend automatisch wieder eingesetzt, aber das können Sie ändern.

> Wenn Sie das Timeout ändern, erinnern Sie sich daran, dies für das Smart Client-Profil zu tun, in Verbindung mit der Rolle welche die Genehmigung hat, Privatzonenmasken aufzuheben.

Änderung des Timeout:

1. Wählen Sie unter **Smart Client Profile** das entsprechende Smart Client-Profil aus.
2. Auf der Registerkarte **Allgemein** finden Sie **Timeout Aufheben von Privatzonenmasken**.



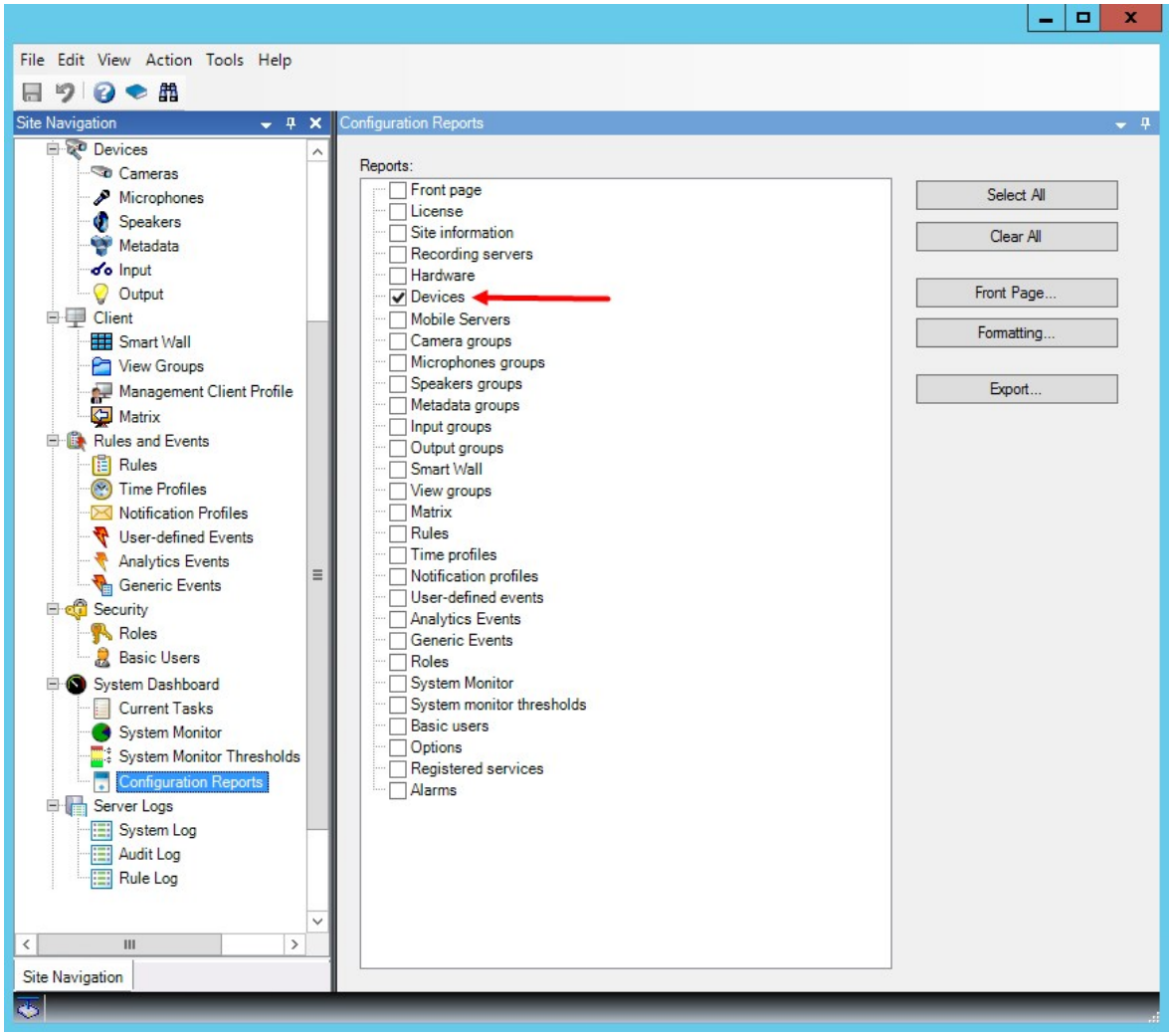
3. Wählen Sie zwischen den Werten:
    - **2 Minuten**
    - **10 Minuten**
    - **30 Minuten**
    - **1 Stunde**
    - **2 Stunden**
    - **Bis abgemeldet**
4. Klicken Sie auf **Speichern**.

Erstellen Sie einen Bericht von der Konfiguration Ihrer Privatsphärenausblendung

Der Gerätebericht enthält Informationen über die aktuellen Einstellungen der Privatsphärenausblendung Ihrer Kameras.

Zum Konfigurieren eines Berichts:

1. Wählen Sie unter **Konfigurationsberichte** den Bericht **Geräte**.



2. Wenn Sie den Bericht ändern wollen, können Sie die Titelseite und die Formatierung wechseln.
3. Klicken Sie auf **Export** und das System erstellt den Bericht als PDF-Datei.

Weitere Informationen über Berichte siehe Konfigurationsberichte (Erklärung) auf Seite 436.

Registerkarte Privatsphärenausblendung (Eigenschaften)

Name	Beschreibung
Rastergröße	Der Wert, den Sie in der Liste Rastergröße ausgewählt haben, bestimmt die Dichte

Name	Beschreibung
	des Rasters, egal ob es gezeigt wird, oder nicht. Wählen Sie zwischen den Werten 8×8, 16×16, 32×32 oder 64×64.
Löschen	Löscht **alle** Privatzonenmasken, die Sie festgelegt haben.
Gitter zeigen	Aktivieren Sie das Kontrollkästchen **Gitter anzeigen**, um das Raster sichtbar zu machen.
Privatzonenmasken anzeigen	Wenn Sie das Kontrollkästchen **Privatzonenmasken anzeigen** (Standard), werden die permanenten Privatzonenmasken in der Vorschau in Violett und die aufhebbaren Privatzonenmasken in Grün dargestellt. Milestone empfiehlt, dass Sie das Kästchen **Privatzonenmasken anzeigen** ausgewählt lassen, damit Sie und Ihre Kollegen die aktuelle Datenschutz-Konfiguration sehen können.
Stiftgröße	Verwenden Sie den Schieberegler **Stiftgröße**, um die Größen der Auswahl anzuzeigen, die Sie machen möchten, wenn Sie ins Raster klicken und ziehen, um Bereiche auszuwählen. Der Standard ist klein, was einem Quadrat im Raster entspricht.
Permanente Maske	Wird in der Vorschau auf dieser Registerkarte und auf der Registerkarte **Motion** in Violett dargestellt. Permanente Privatzonenmasken sind immer sichtbar in XProtect Smart Client und können nicht aufgehoben werden. Diese können benutzt werden, um Bereiche des Videos abzudecken, die niemals Überwachung erfordern, wie öffentliche Bereiche, in denen keine Überwachung genehmigt wird. Bewegungserkennung ist von permanenten Privatzonenmasken ausgeschlossen. Sie können die Abdeckung von Privatzonenmasken entweder als intransparent oder unscharf angeben. Die Deckungseinstellungen gelten sowohl für Live-Videos als auch für Aufzeichnungen.
Aufhebbare Maske	Wird in der Vorschau auf dieser Registerkarte in Grün dargestellt. Aufhebbare Privatzonenmasken können in XProtect Smart Client von Benutzern aufgehoben werden, die über ausreichende Benutzerrechte verfügen. Als Standard werden die Privatzonenmasken für 30 Minuten aufgehoben, oder bis der Benutzer sie wieder anwendet. Seien Sie sich darüber im Klaren, dass Privatzonenmasken auf

Name	Beschreibung
	Video von allen Kameras aufgehoben werden, auf die der Benutzer Zugriff hat. Wenn der XProtect Smart Client kein Recht zum Aufheben der Privatzonenmasken hat, verlangt das System einen Benutzer mit der Erlaubnis zur Genehmigung des Aufhebens. Sie geben die Abdeckung von Privatzonenmasken entweder als intransparent oder als unscharf an. Die Deckungseinstellungen gelten sowohl für Live-Videos als auch für Aufzeichnungen.
Unschärfe	Benutzen Sie den Schieber, um das Unschärfeniveau der Privatzonenmasken auszuwählen oder die Deckung auf voll intransparent zu stellen. Als Standard ist die Deckung von Bereichen mit permanenten Privatzonenmasken durchgehend (intransparent). Als Standard sind aufhebbare Privatzonenmasken halbscharf gedeckt. Sie können die Client-Benutzer über das Erscheinen von permanenten und aufhebbaren Privatzonenmasken informieren, damit sie in der Lage sind, diese zu unterscheiden.

Site-Navigation: Clients

Dieser Abschnitt beschreibt, wie die Benutzeroberfläche in XProtect Smart Client für Betreiber und in Management Client für Systemadministratoren benutzerdefiniert angepasst wird.

Clients (Erklärung)

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

Der Client Abschnitt von Management Client besteht aus:

Name	Beschreibung
XProtect Smart Wall	XProtect Smart Wall ein ist Add-on, das es Ihnen erlaubt, Ansichtsmaterial von XProtect Smart Client zu einer zugehörigen Videowand zu senden.

Name	Beschreibung
	Weitere detaillierte Informationen zu XProtect Smart Wall finden Sie unter XProtect Smart Wall (erklärt) auf Seite 31.
Ansichtsgruppen	Die Art und Weise, in der Videoaufnahmen von Kameras angezeigt wird, wird als Ansicht bezeichnet. Sie können steuern, welche Benutzer auf welche Inhalte im XProtect Smart Client zugreifen können, indem Sie Ansichtsgruppen erstellen, um Ansichten in logische Einheiten zu gruppieren. Der Zugriff auf diese Ansichtsgruppen kann Rollen zugeordnet werden, um auf diese Weise den Zugriff auf einzelne Ansichten auf bestimmte Rollen zu beschränken. Wählen Sie **Ansichtsgruppen**, um Ansichtsgruppen zu erstellen und mit ihnen zu arbeiten, damit sie an Ihre Überwachungsanforderungen angepasst sind.
Smart Client-Profile	Zur Unterscheidung der XProtect Smart Client-Benutzer können Sie Smart Client Profile erstellen, ihnen Prioritäten zuweisen und die Profile nach Bedarf an die jeweiligen Aufgaben anpassen.
Management Client Profile	Zur Unterscheidung der Management Client Benutzer mit Administrator-Rechten können Sie Management Client Profile erstellen, ihnen Prioritäten zuweisen und die Profile nach Bedarf an die jeweiligen Aufgaben anpassen.
Matrix	Matrix ist eine Funktion zur Remote-Verteilung von Videoaufzeichnungen. Wenn Sie Matrix verwenden, können sie Videoaufnahmen von einer Kamera in Ihrem Systemverbund zu jedem angeschlossenen XProtect Smart Client verschieben.

Site-Navigation: Clients: Konfigurieren von Smart Wall

Dieser Abschnitt beschreibt, wie XProtect Smart Wall konfiguriert wird.

XProtect Smart Wall Lizenzierung

XProtect Smart Wall benötigt die folgenden Lizenzen für Videowände:

- Eine **Basislizenz** für XProtect Smart Wall, die eine unbegrenzte Anzahl von Bildschirmen zum Anzeigen des Videos auf der Videowand zulässt.

Eine Basislizenz für XProtect Smart Wall ist in der Basislizenz für XProtect Corporate eingeschlossen. Wenn Sie XProtect Expert besitzen, können Sie eine Basislizenz für XProtect Smart Wall separat hinzukaufen.

Smart Walls konfigurieren

Eine Smart Wall-Konfiguration besteht aus der Einstellung des Smart Wall, dem Hinzufügen von Bildschirmen und die Bestimmung des Bildschirmlayouts sowie optional eine Einstellung von Smart Wall-Voreinstellungen, des Layouts und des Inhalts der verschiedenen Bildschirme.

Sie müssen die Smart Wall-Voreinstellungen nicht näher definieren, wenn Sie nur Kameras und XProtect Smart Client-Ansichten anzeigen lassen wollen, die Ihre XProtect Smart Client-Benutzer manuell an die Videowand schieben können.

Sie sollten die Smart Wall-Voreinstellungen dann näher definieren, wenn Sie Regeln zum automatischen Anzeigewechsel an der Videowand verwenden wollen oder wenn Sie bestimmte Überwachungsszenarien berücksichtigen möchten, bei denen die Anzeige des gleichen Inhalts wichtig ist, sobald dieses Szenario eintrifft.

Die Konfiguration der Smart Wall ist sehr flexibel. Sie können alle Bildschirme der Videowand in ein Smart Wall einbeziehen oder die Bildschirme und ein Smart Wall für jede Gruppe konfigurieren. Smart Wall-Voreinstellungen können das Layout und den Inhalt aller oder nur einiger Bildschirme in einem Smart Wall ändern. Bildschirme können Teil mehrerer Smart Wall und Smart Wall-Voreinstellungen sein. Erstellen Sie so viele Smart Wall und Smart Wall-Voreinstellungen wie Sie benötigen, um die optimale Abdeckung für Ihre Überwachungsszenarien zu erhalten.

a. Smart Wall definieren:

1. Erweitern Sie **Client** und wählen Sie **Smart Wall** aus.
2. Im Bereich **Übersicht** klicken Sie mit der rechten Maustaste auf **Smart Wall** und wählen Sie dann **Hinzufügen Smart Wall** aus.
3. Bestimmung der Einstellungen für das Smart Wall.
4. In den Einstellungen **Allgemeine Ansichtselementeigenschaften**, können Sie bei Bedarf die Systemstatusinformationen und Titelleisten einstellen, sodass diese über den Layout-Elementen der Kameras erscheinen.
5. Klicken Sie auf **OK**.

b. Hinzufügen von Bildschirmen und Bestimmen des Bildschirmlayouts:

1. Klicken Sie mit der rechten Maustaste auf Smart Wall und wählen Sie **Bildschirm hinzufügen** aus.
2. Konfigurieren Sie die Abmessungen des Bildschirms, damit es einem der physischen Bildschirme an der Videowand entspricht.

3. Verwenden Sie die Einstellungen für das voreingestellte Verhalten **Leere Voreinstellung** und **Leeres Voreinstellungselement**, um zu bestimmen was auf einem Bildschirm angezeigt werden soll mit einem leeren Voreinstellungslayout oder in einem leeren Voreinstellungselement, wenn eine neue Smart Wall Voreinstellung automatisch ausgelöst oder manuell in XProtect Smart Client ausgewählt wird. Sie können leere Voreinstellungen und leere Voreinstellungselemente für Inhalte verwenden, die nicht von der Smart Wall-Voreinstellung gesteuert werden.
4. Benutzen Sie die Einstellung für voreingestelltes Verhalten **Elementeinfügung**, um zu bestimmen, was passiert, wenn ein Benutzer von XProtect Smart Client eine Kamera auf ein Layout-Element in der Smart Wall-Voreinstellung zieht. Wählen Sie **Unabhängig**, um die Kamera, die bereits im Voreinstellungselement enthalten ist, mit der neuen Kamera auszutauschen. Sie können auch auf **Verlinkt** klicken, um den Inhalt des Layoutelements von links nach rechts relativ zur Position der Einfügung der neuen Kamera zu schieben.
5. Fügen Sie so viele Bildschirme wie auf der physischen Videowand vorhanden, hinzu.
6. Wählen Sie die Smart Wall und klicken Sie dann in der Registerkarte **Layout** auf **Bearbeiten**, um die verschiedenen Bildschirme so zu positionieren, dass es den physischen Bildschirmen an der Videowand ähnelt.
7. Klicken Sie auf **OK**. Das gleiche Layout wird in XProtect Smart Client verwendet.

c. Smart Wall-Voreinstellungen hinzufügen (optional):

1. Wählen Sie die Smart Wall und in der Registerkarte **Voreinstellungen**, klicken Sie auf **Neu Hinzufügen**.
2. Geben Sie einen Namen und Beschreibung ein und klicken Sie auf **OK**.
3. Klicken Sie auf **Aktivieren**, um die Smart Wall-Voreinstellungen auf der Videowand anzuzeigen.
4. Erstellen Sie so viele Smart Wall Voreinstellungen wie nötig.

d. Hinzufügen von Layout und Kameras zu den Bildschirmen (erfordert eine Smart Wall-Voreinstellung):

1. Wählen Sie einen der Bildschirme, die Sie erstellt haben und in der Registerkarte **Voreinstellungen**, wählen Sie dann eine Voreinstellung aus der Liste, um die Anzeige des Bildschirms mit der ausgewählten Smart Wall-Voreinstellung zu konfigurieren.
2. Klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf die Schaltfläche „Layout", um das Layout für Ihren Bildschirm auszuwählen, und klicken Sie dann auf **OK**.
   

4. Ziehen Sie Kameras aus den **Gerätegruppen**, **Aufzeichnungsserver** oder der Registerkarte **Hierachie der förderalen Standorte**. Die Kameras in der Registerkarte **Hierachie der förderalen Standorte** sind verfügbar über eine Milestone Federated Architecture-Einrichtung. Sie können Layout-Elemente leer lassen, damit diese für andere Inhalte zur Verfügung stehen, die nicht von der Smart Wall-Voreinstellung gesteuert werden.
5. Wenn der Bildschirm bereits ein Layout für die ausgewählte Voreinstellung besitzt, können Sie auf **Löschen** klicken, um ein neues Layout festzulegen, oder um den Bildschirm aus der Smart Wall-Voreinstellung auszuschließen, damit der Bildschirm für andere Inhalte, die nicht von dieser Smart Wall-Voreinstellung gesteuert werden, zur Verfügung steht.
6. Klicken Sie auf **OK**.
7. Wiederholen Sie die Schritte bis Sie ein Layout und Kameras an die Bildschirme hinzugefügt haben, die Sie in der Smart Wall-Voreinstellung einschließen möchten.

Benutzerrechte einrichten für XProtect Smart Wall

Sie können die Aufgaben steuern, damit XProtect Smart Client-Benutzer in XProtect Smart Wall arbeiten können, indem Sie Benutzerrechte für Rollen festlegen. Die Benutzerrechte gelten für alle Benutzer, die dieser Rolle zugewiesen sind. Weitere Informationen zu Rollen mit Smart Wall Rechten finden Sie unter Rolleneinstellungen auf Seite 379.

Die Auswahl für die Benutzerrechte zum **Lesen**, **Bearbeiten** und **Löschen** werden immer angewendet. Die Benutzerrechte **Ausführen** und **Wiedergabe** können Sie auch in ausgewählten Zeiträumen an ausgewählte Profile gewähren. Zum Beispiel ist dies vorteilhaft, wenn Sie einem Benutzer erlauben möchten, den Inhalt zu ändern, der auf einem angezeigt Smart Wall wird. Dies gilt nur während der normalen Arbeitszeit.

Zum Festlegen von Benutzerrechten für eine Rolle, folgen Sie diesen Schritten:

1. Erweitern Sie im Bereich Standort-Navigation das Feld **Sicherheit** und wählen Sie **Rollen** aus.
2. Im Bereich **Rollen**, wählen Sie die Rolle aus, oder erstellen Sie eine neue Rolle per Rechtsklick mit der Maustaste in den Bereich und der Auswahl **Rolle hinzufügen**.
3. Im oberen Teil des Bereichs für die **Rolleneinstellungen**, wählen Sie Smart Wall aus.

4. Im unteren Teil des Bereichs für die Rolleneinstellungen, klicken Sie auf die Registerkarte **Smart Wall**, und wählen dann die Benutzerrechte aus, die zugewiesen werden sollen.
   - **Lesen** – Anzeigen von Smart Walls in Client-Anwendungen
   - **Bearbeiten** – Modifizieren von Smart Walls in Client-Anwendungen
   - **Löschen** – Löschen von Smart Walls in Client-Anwendungen
   - **Ausführen** – Layouts auf ausgewählte Bildschirme in Client-Anwendungen anwenden, und Voreinstellungen aktivieren
   - **Wiedergabe** – Überprüfen und Verwalten von aufgezeichnetem und Live-Video

   Wenn Sie nicht die Genehmigung für **Wiedergabe** auswählen, können Benutzer zwar den Inhalt an der Videowand sehen, aber nicht verändern. Wenn ein Benutzer eine Änderung vornimmt, trennt das System sich automatisch vom geteilten Status und der Inhalt an der Videowand wird nicht beeinträchtigt. Wenn Sie sich wieder mit der allgemeinen Ansicht verbinden wollen, klicken Sie auf die Option **Smart Wall-Monitor wieder verbinden**.

5. Optional: Zum Gewähren der Benutzerrechte für **Ausführen** oder **Wiedergabe** in einem bestimmten Zeitraum, wählen Sie das Kontrollkästchen an und dann das Zeitprofil.

Verwendung von Regeln mit Smart Wall-Voreinstellungen (Erklärung).

Durch die Kombination von Regeln und Smart Wall-Voreinstellungen können Sie bestimmen was auf Ihrer Videowand angezeigt wird, in einer ähnlichen Art und Weise wie das System auch Regeln verwendet, um das Verhalten von Kameras usw. zu steuern. Beispielsweise kann eine Regel auslösen, die Ihre Videowand zum Anzeigen einer bestimmten Smart Wall-Voreinstellung zu einer bestimmten Tageszeit veranlasst. Sie können Regeln auch verwenden, um zu steuern, was einzelne Bildschirme in einer Videowand anzeigen. Weitere Information zur Erstellung von Regeln, finden Sie unter Regeln auf Seite 340.

Beispiel einer Regel, die eine Smart Wall-Voreinstellung auslöst:

Smart Wall Eigenschaften

Registerkarte „Info“ (Smart Wall-Eigenschaften)

Auf der Registerkarte **Info** für ein Smart Wall, können Sie Smart Wall hinzufügen und bearbeiten.

Name	Beschreibung
Name	Der Name des Smart Wall. Angezeigt in XProtect Smart Client als der Smart Wall Ansichtsgruppenname.
Beschreibung	Eine Beschreibung von Smart Wall. Die Beschreibung wird nur intern im Management Client verwendet.
Statustext	Bei Auswahl werden Informationen zum Systemstatus und Kameras über Layout-Elemente der Kameras in der Videowand angezeigt.
Keine Titelleiste	Bei Auswahl haben alle Smart Wall Layout-Elemente keine Titelleisten auf der Videowand.
Titelleiste	Bei Auswahl haben alle Smart Wall Layout-Elemente Titelleisten auf der Videowand.
Titelleiste mit Live-Anzeige	Bei Auswahl zeigen alle Smart Wall Titelleisten der Layout-Elemente, Live- und Bewegungsindikatoren auf der Videowand an.

Registerkarte „Voreinstellungen“ (Smart Wall-Eigenschaften)

In der Registerkarte **Voreinstellungen** für ein Smart Wall, können Sie Smart Wall-Voreinstellungen hinzufügen und bearbeiten.

Name	Beschreibung
Hinzufügen	Klicken, um eine Voreinstellung zu Ihrer XProtect Smart Wall-Installation hinzuzufügen. Bestimmen Sie einen Namen und eine Beschreibung für die neue Smart Wall-Voreinstellung.
Bearbeiten	Den Namen und/oder Beschreibung einer Smart Wall-Vorstellung bearbeiten.
Löschen	Eine Smart Wall-Voreinstellung löschen.
Aktivieren	Klicken Sie, um Smart Wall-Voreinstellung auf der Videowand anzuzeigen. Sie müssen Regeln mit der Smart Wall-Voreinstellung erstellen, bevor das System automatisch die Anzeige der Smart Wall-Voreinstellung auslösen kann. Siehe auch Verwendung von Regeln mit Smart Wall-Voreinstellungen (Erklärung). auf Seite 288.

Registerkarte „Layout“ (Smart Wall-Eigenschaften)

In der Registerkarte **Layout** für ein Smart Wall, positionieren Sie die Bildschirme für Ihr Smart Wall, damit dessen Positionen dem Aufbau der physischen Bildschirme in der Videowand ähneln. Das Layout wird auch im XProtect Smart Client verwendet.

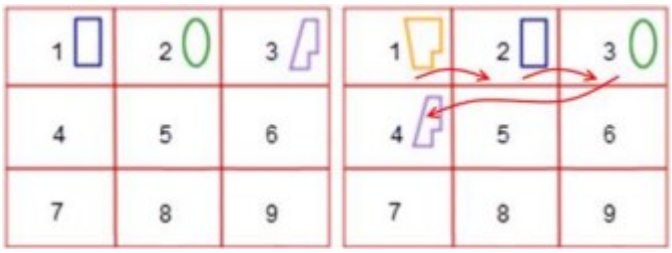
Name	Beschreibung
Bearbeiten	Klicken Sie zur Anpassung der Bildschirmpositionen.
Bewegung	Zur Verschiebung eines Bildschirms an eine neue Position, wählen Sie einfach den relevanten Bildschirm aus und ziehen Sie ihn an die gewünschte Position. Alternativ können Sie den Bildschirm auch mit den Pfeiltasten in die ausgewählte Richtung bewegen.
Zoomschaltfläche	Klicken Sie die Schaltflächen zum Heran- und Herauszoomen aus der Smart Wall-Layout Vorschau, um eine ordnungsgemäße Position der Bildschirme sicherzustellen.
Name	Der Name des Bildschirms. Der Name wird in XProtect Smart Client angezeigt.
Größe	Die Größe des physischen Bildschirms an der Videowand.
Seitenverhältnis	Das Höhe-/Breitenverhältnis des physischen Bildschirms an der Videowand.

Bildschirmeigenschaften

Registerkarte „Info“ (Bildschirmeigenschaften)

In der Registerkarte **Info** für einen Bildschirm in einer Smart Wall-Voreinstellung, können Sie Bildschirme hinzufügen und dessen Einstellungen bearbeiten.

Name	Beschreibung
Name	Der Name des Bildschirms. Der Name wird in XProtect Smart Client angezeigt.
Beschreibung	Eine Beschreibung des Bildschirms. Die Beschreibung wird nur intern im

Name	Beschreibung
	Management Client verwendet.
Größe	Die Größe des physischen Bildschirms an der Videowand.
Seitenverhältnis	Das Höhe-/Breitenverhältnis des physischen Bildschirms an der Videowand.
Leere Voreinstellung	Definiert, was auf einen Bildschirm mit einem leeren voreingestellten Layout-Element angezeigt werden soll, wenn eine neue Smart Wall-Voreinstellung ausgelöst oder in XProtect Smart Client ausgewählt wird. Wählen Sie **Beibehalten**, um den derzeitigen Inhalt auf dem Bildschirm beizubehalten. Wählen Sie **Löschen**, um den Inhalt zu löschen, damit nichts auf dem Bildschirm angezeigt wird.
Leeres Voreinstellungselement	Definiert, was in einem leeren voreingestellten Layout-Element angezeigt werden sollte, wenn eine neue Smart Wall-Voreinstellung ausgelöst oder in XProtect Smart Client ausgewählt wird. Wählen Sie **Beibehalten**, um den derzeitigen Inhalt im Layout-Element beizubehalten. Wählen Sie **Löschen**, um den Inhalt zu löschen, damit nichts im Layout-Element angezeigt wird.
Elementeinfügung	Bestimmt wie Kameras im Bildschirmlayout eingefügt werden, wenn sie in XProtect Smart Client angezeigt werden. Bei Auswahl von **Unabhängig**, verändert sich nur der Inhalt des betroffenen Layout-Elements, der Rest der Inhalte im Layout bleiben unverändert. Bei Auswahl von **Verlinkt**, wird der Inhalt der Layout-Elemente von links nach rechts verschoben. Wenn, beispielsweise, eine Kamera in Position 1 eingefügt wird, verschiebt sich die Kamera, die vorher auf Position 1 platziert war, auf Position 2, die Kamera auf Position 2 wiederum verschiebt sich auf Position 3, usw. 

Registerkarte „Voreinstellungen“ (Bildschirmeigenschaften)

In der Registerkarte **Voreinstellungen** für einen Bildschirm in einer Smart Wall-Voreinstellung, können Sie das Layout und Inhalt des Bildschirms hinzufügen sowie in der ausgewählten Smart Wall-Voreinstellung bearbeiten.

Name	Beschreibung
Voreinstellung	Eine Liste von Smart Wall-Voreinstellungen für die ausgewählten Smart Wall.
Bearbeiten	Klicken Sie auf **Bearbeiten**, um das Layout und den Inhalt des ausgewählten Bildschirms zu bearbeiten. Machen Sie einen Doppelklick auf eine Kamera, um eine einzelne Kamera zu entfernen. Klicken Sie auf **Löschen**, um ein neues Layout festzulegen, oder um den Bildschirm in der Smart Wall-Voreinstellung auszuschließen, damit der Bildschirm für andere Inhalte, die nicht von dieser Smart Wall-Voreinstellung gesteuert werden, zur Verfügung steht. Klicken Sie auf  , um das Layout zu wählen, das Sie mit Ihrem Bildschirm in der ausgewählten Voreinstellung verwenden möchten, und klicken Sie dann auf **OK**. Ziehen Sie Kameras aus den **Gerätegruppen**, **Aufzeichnungsserver** oder der Registerkarte **Förderale Standorte**. Sie können Layout-Elemente leer lassen, damit diese für andere Inhalte zur Verfügung stehen, die nicht von der Smart Wall-Voreinstellung gesteuert werden.

Site-Navigation: Clients: Ansichtsgruppen

Die Art und Weise wie das System Video von einer oder mehreren Kameras in Clients anzeigt, wird Ansicht genannt. Eine Ansichtsgruppe ist ein Behälter für eine oder mehrere logische Gruppen solcher Ansichten. In Clients wird eine Ansichtsgruppe als ausklappbarer Ordner dargestellt, von dem Benutzer Gruppen und die gewünschte Ansicht auswählen können:

Beispiel von XProtect Smart Client: Ein Pfeil zeigt eine Ansichtsgruppe an, die eine logische Gruppe beinhaltet (Annehmlichkeiten genannt), die wiederum 3 Ansichten enthält.

Ansichtsgruppen und Rollen anzeigen (Erklärung)

Standardmäßig wird jede Rolle, die Sie in der Management Client festlegen, auch als Ansichtsgruppe erstellt. Wenn Sie eine Rolle in der Management Client hinzufügen, erscheint diese Rolle standardmäßig als Ansichtsgruppe zur Verwendung in Clients.

- Sie können eine Ansichtsgruppe auf Grundlage einer Rolle zu Benutzern/Gruppen mit relevanter Rolle zuteilen. Sie können die Rechte dieser Ansichtsgruppen durch die spätere Einstellung dieser Rolle ändern
- Eine rollenbasierte Ansichtsgruppe hat den Namen der Rolle inne.

  Beispiel: Wenn Sie eine Rolle mit dem Namen **Aufbauen eines Sicherheitspersonals** erstellen, erscheint es in XProtect Smart Client als Ansichtsgruppe namens **Aufbauen eines Sicherheitspersonals**.

  Zusätzlich zu den Ansichtsgruppen beim Hinzufügen von Rollen, können Sie beliebig viele Ansichtsgruppen erstellen. Sie können auch Ansichtsgruppen entfernen, einschließlich derer, die automatisch beim Hinzufügen von Rollen erstellt werden
- Selbst wenn jedes Mal eine Ansichtsgruppe beim Hinzufügen einer Rolle erstellt wird, müssen Ansichtsgruppen nicht Rollen entsprechen. Sie können nach Bedarf jede Ihrer Ansichtsgruppen hinzufügen, umbenennen oder entfernen

Wenn Sie eine Ansichtsgruppe umbenennen, müssen sich bereits verbundene Client-Benutzer ausloggen und wieder einloggen, bevor die Namensänderung sichtbar wird.

Ansichtsgruppe hinzufügen

1. Rechtsklick auf **Ansichtsgruppen** und dann **Ansichtsgruppe hinzufügen** auswählen. Dies öffnet das Dialogfenster **Ansichtsgruppe hinzufügen**.
2. Geben Sie den Namen und optional eine Beschreibung der neuen Ansichtsgruppe ein und klicken Sie dann auf **OK**.

Rollen haben keine Rechte zur Verwendung der neu hinzugefügten Ansichtsgruppe bis Sie solche Rechte festgelegt haben. Sollten Sie die Rollen festgelegt haben, die eine neu hinzugefügte Ansichtsgruppe verwenden darf, müssen bereits verbundene Client-Benutzer mit den betroffenen Rollen aus- und wieder einloggen, bevor sie die Ansichtsgruppe sehen können.

Site-Navigation: Clients: Smart Client Profile

Verfügbare Funktionalität hängt vom verwendeten System ab. Weitere Informationen

finden Sie unter https://www.milestonesys.com/solutions/platform/product-index/.

Mit Smart Client-Profilen können Systemadministratoren das Aussehen und Verhalten von XProtect Smart Client steuern und auf welche Funktionen und Bereiche XProtect Smart Client-Benutzer Zugriff haben. Sie können für folgende Dinge Benutzerrechte einrichten: Bereiche und Optionen, Minimierungs- / Maximierungsoptionen, Inaktivitäts-Zeitsteuerung, Passwort-Erinnerungsfunktion, Ansicht nach der Anmeldung, Layout von Druckberichten, Exportpfad und mehr.

Erweitern Sie zur Verwaltung von Smart Client-Profilen im System **Client** und wählen Sie **Smart Client-Profile aus**. Außerdem können Sie sich über die Beziehung zwischen Smart Client-Profilen, Rollen und Zeitprofilen informieren und wie Sie diese zusammen nutzen können (siehe Erstellen und Einrichten von Smart Client-Profilen, Rollen und Zeitprofilen auf Seite 295).

Hinzufügen und Konfigurieren eines Smart Client-Profils

Sie müssen ein Smart Client-Profil erstellen, bevor Sie es konfigurieren können.

1. Klicken Sie mit der rechten Maustaste auf **Smart Client-Profile**.
2. Wählen Sie **Smart Client-Profil hinzufügen** aus.
3. Geben Sie im Dialogfenster **Smart Client-Profil hinzufügen** einen Namen und eine Beschreibung des neuen Profils ein und klicken Sie dann auf **OK**.
4. Klicken Sie im Bereich **Überblick** auf das erstellte Profil, um es zu konfigurieren.
5. Passen Sie die Einstellungen auf einer, mehreren oder allen verfügbaren Registerkarten an und klicken Sie auf **OK**.

Kopieren eines Smart Client-Profils

Wenn Sie ein Smart Client-Profil mit komplexen Einstellungen oder Rechten haben und ein ähnliches Profil benötigen, kann es einfacher sein, ein bereits bestehendes Profil zu kopieren und geringe Anpassungen an der Kopie vorzunehmen, als ein Profil von Grund auf neu zu erstellen.

1. Klicken Sie auf **Smart Client-Profile**, klicken Sie mit der rechten Maustaste auf das Profil im Bereich **Übersicht**, wählen Sie **Smart Client-Profil kopieren** aus.
2. Es erscheint ein Dialogfenster; geben Sie dem kopierten Profil einen neuen einmaligen Namen und eine Beschreibung. Klicken Sie auf **OK**.
3. Klicken Sie im Bereich **Überblick** auf das gerade erstellte Profil, um es zu konfigurieren. Hierzu müssen die Einstellungen auf einer, mehreren oder allen verfügbaren Registerkarten angepasst werden. Klicken Sie auf **OK**.

Erstellen und Einrichten von Smart Client-Profilen, Rollen und Zeitprofilen

Wenn Sie mit Smart Client-Profilen arbeiten, ist ein Verständnis der Interaktionen zwischen Smart Client-Profilen, Rollen und Zeitprofilen von höchster Bedeutung:

- Smart Client Profile beziehen sich auf Benutzerrechtseinstellungen in XProtect Smart Client
- Rollen beziehen sich auf Sicherheitseinstellungen in Clients, MIP SDK und mehr
- Zeitprofile beziehen sich auf zeitliche Aspekte der beiden Profiltypen

Kombiniert bieten diese drei Funktionen einzigartige Steuerungs- und Anpassungsmöglichkeiten in Bezug auf die XProtect Smart Client-Benutzerrechte.

Beispiel: Sie benötigen einen Benutzer in Ihrer XProtect Smart Client-Einrichtung, der nur Live-Video (keine Wiedergaben) von ausgewählten Kameras sehen darf, und das nur während der normalen Arbeitszeit (8:00–16:00 Uhr). Eine Einrichtung könnte folgendermaßen vonstattengehen:

1. Erstellen Sie ein Smart Client-Profil und nennen Sie es beispielsweise **Nur Live**.
2. Legen Sie die benötigten Live-/Wiedergabeeinstellungen für **Nur Live** fest.
3. Erstellen Sie ein Zeitprofil und nennen Sie es beispielsweise **Nur Tag**.
4. Legen Sie die benötigte Zeitspanne für **Nur Tag** fest.
5. Erstellen Sie eine neue Rolle und nennen Sie sie beispielsweise **Bewachen (ausgewählte Kameras)**.
6. Legen Sie fest, welche Kameras **Bewachen (ausgewählte Kameras)** verwenden kann.
7. Weisen Sie das Smart Client-Profil **Nur Live** und das Zeitprofil **Nur Tag** der Rolle **Bewachen (ausgewählte Kameras)** zu, um die drei Elemente zu verbinden.

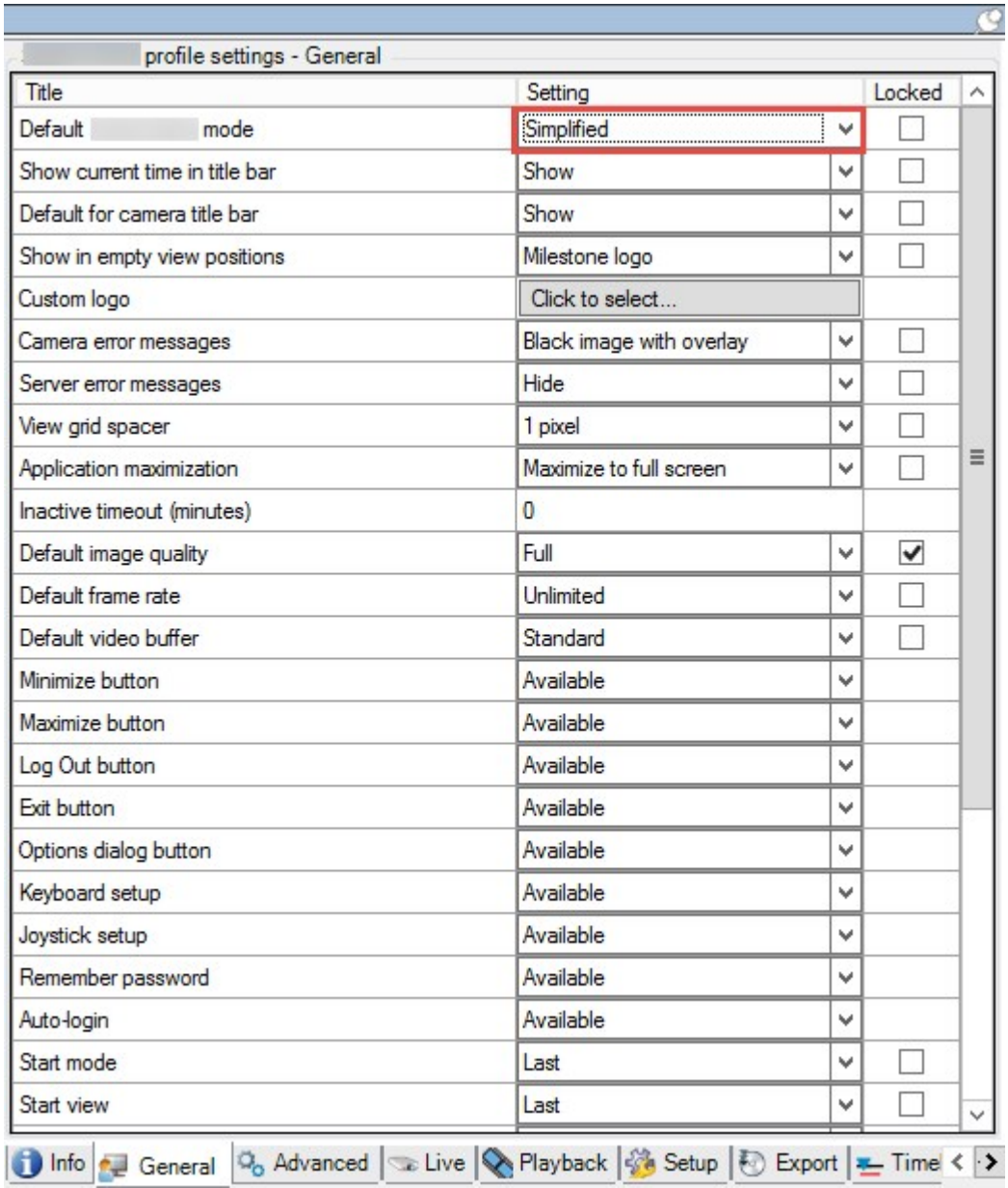
Sie haben jetzt durch die Vermischung dieser drei Funktionen das gewünschte Ergebnis und können sie problemlos weiter verfeinern und anpassen. Sie können die Einrichtung auch in einer anderen Reihenfolge vornehmen. Beispielsweise können Sie die Rolle zuerst erstellen und dann das Smart Client-Profil sowie das Zeitprofil, oder in jeder beliebigen Reihenfolge.

Einrichtung des vereinfachten Modus als Standardmodus

Über die Smart Client-Profile können Sie Ihr System darauf konfigurieren, XProtect Smart Client automatisch im vereinfachten Modus mit einer begrenzten Auswahl an Funktionen und Registerkarten zu öffnen. Standardmäßig wird XProtect Smart Client im erweiterten Modus geöffnet und verfügt über alle Funktionen und Registerkarten.

Wenn der XProtect Smart Client-Anwender zu irgendeinem Zeitpunkt beschließt, aus dem Standardmodus in einen anderen Modus zu wechseln, speichert XProtect Smart Client diese Einstellung, wenn der Anwender das Programm das nächste Mal öffnet.

1. Erweitern Sie im Management Client den Knoten **Client**.
2. Wählen Sie das gewünschte Smart Client-Profil aus.
3. Klicken Sie auf die Registerkarte **Allgemein**.

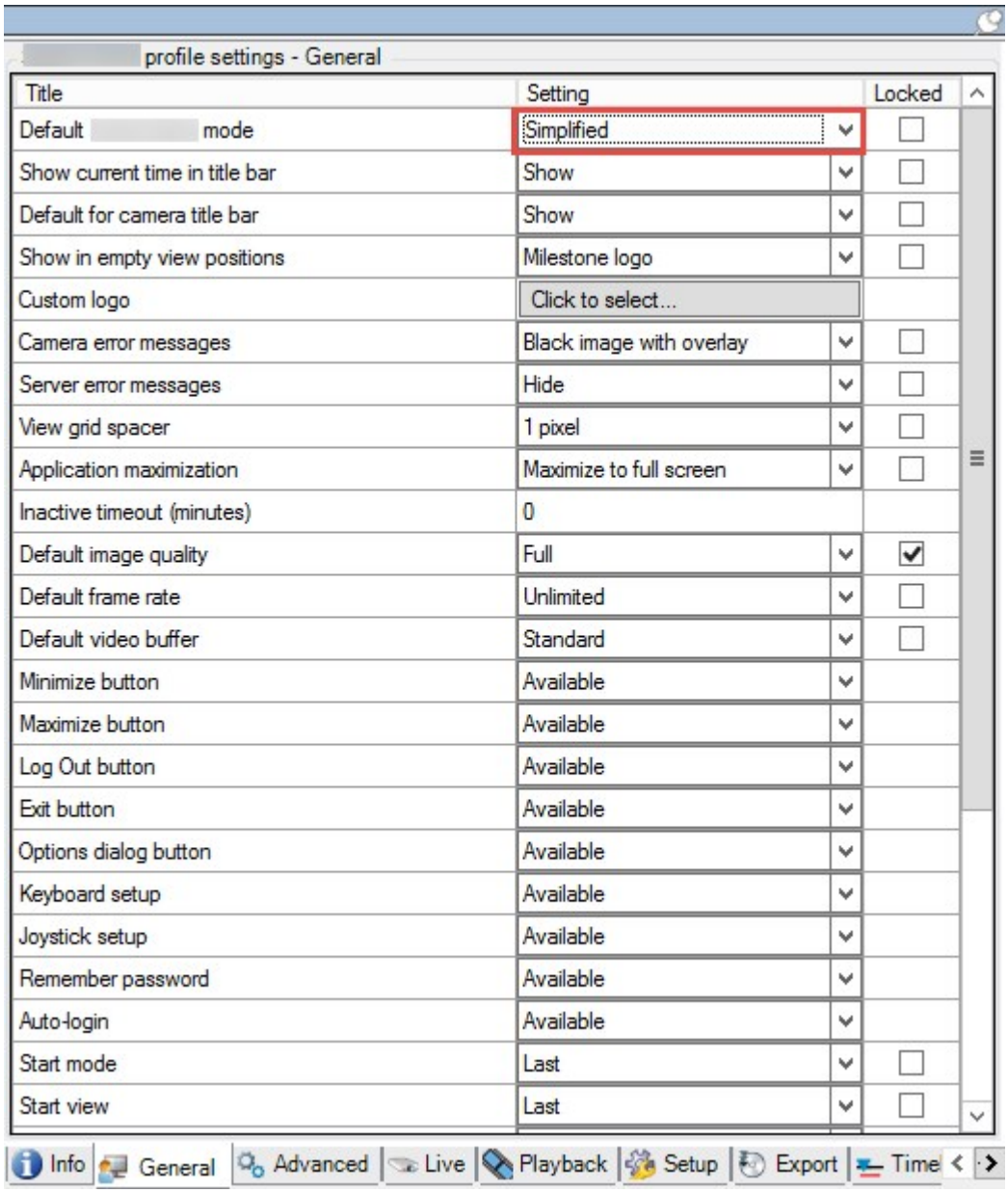


4. Wählen Sie in der **Standard-Smart Client Modus**-Liste **Vereinfacht** aus. XProtect Smart Client wird nun für die mit dem aktuellen Smart Client-Profil verbundenen Benutzer im vereinfachten Modus geöffnet.

Verhinderung des Umschaltens zwischen dem einfachen und dem erweiterten Modus durch Anwender

Im XProtect Smart Client können Anwender zwischen dem einfachen und dem erweiterten Modus umschalten. Sie können die XProtect Smart Client-Anwender jedoch daran hindern. Technisch gesehen müssen Sie die Einstellung sperren, die bestimmt, ob XProtect Smart Client im einfachen oder erweiterten Modus geöffnet wird.

1. Erweitern Sie im Management Client den Knoten **Client**.
2. Wählen Sie das gewünschte Smart Client-Profil aus.
3. Klicken Sie auf die Registerkarte **Allgemein**.



4. Stellen Sie sicher, dass die Liste **Standard-Smart Client-Modus** den richtigen Wert enthält. Wenn es **Aktiviert** ist, wird der XProtect Smart Client im vereinfachten Modus geöffnet.
5. Aktivieren Sie das Kontrollkästchen **Gesperrt**. Die Schaltfläche zum Umschalten zwischen den Modi wird im XProtect Smart Client verborgen.

Siehe auch Einrichtung des vereinfachten Modus als Standardmodus auf Seite 295.

Smart Client-Profileigenschaften

Auf den folgenden Registerkarten können Sie die Eigenschaften jedes Smart Client-Profils festlegen. Sie können die Einstellungen bei Bedarf im Management Client sperren, damit XProtect Smart Client-Benutzer sie nicht ändern können.

Registerkarte „Info“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Info	Name und Beschreibung, Priorität vorhandener Profile und ein Überblick über die Rollen, die das Profil verwenden. Wenn ein Benutzer mehr als eine Rolle hat und diese Rollen jeweils ein eigenes Smart Client-Profil haben, erhält der Benutzer das Smart Client-Profil mit der höchsten Priorität.

Registerkarte Allgemein (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Allgemein	Einstellungen wie Anzeigen/Verbergen und Minimieren und Maximieren der Menüeinstellungen, An-/Abmeldung, Systemstart, Zeitüberschreitung, Info- und Benachrichtigungsoptionen sowie aktivieren oder deaktivieren bestimmter Registerkarten in XProtect Smart Client.

Registerkarte	Beschreibung
	Wenn Sie die Fehlermeldungen von der Kamera **Verbergen**, besteht das Risiko, dass das Bedienpersonal übersieht, dass die Verbindung zu einer Kamera unterbrochen wurde. Die Einstellung Online-Hilfe gibt Ihnen die Möglichkeit, das Hilfesystem in XProtect Smart Client zu deaktivieren. Die Einstellung **Video-Anleitungen** gibt Ihnen die Möglichkeit, die Schaltfläche **Video-Anleitungen** in XProtect Smart Client zu deaktivieren. Die Schaltfläche leitet den Benutzer auf die Seite mit den Video-Anleitungen um: https://www.milestonesys.com/support/help-yourself/video-tutorials/

Registerkarte Erweitert (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Erweitert	Erweiterte Einstellungen wie etwa die maximale Anzahl an Dekodierungsthreads, Deinterlacing und Zeitzoneneinstellungen. Die **maximale Anzahl an Dekodierungsthreads** steuert, wie viele Dekodierungsthreads zur Dekodierung von Video-Streams verwendet werden. Diese Option trägt zur Verbesserung der Leistung auf Multicore-Computern im Live- und im Wiedergabemodus bei. Die genaue Leistungsverbesserung ist abhängig vom Video-Stream. Diese Einstellung ist hauptsächlich relevant, wenn in hohem Maße codierte hochauflösende Videostreams wie H.264/H.265 verwendet werden, bei denen das Leistungssteigerungspotenzial signifikant sein kann. Sie ist weniger relevant, wenn beispielsweise JPEG oder MPEG-4 verwendet wird. Bei **Deinterlacing** wandeln Sie das Video in ein Format ohne Interlacing um. Beim Interlacing wird definiert, wie ein Bild auf einem Bildschirm aktualisiert wird. Das Bild wird aktualisiert, indem zunächst die ungeraden Zeilen und dann die geraden Zeilen des Bildes abgetastet werden. Dies ermöglicht eine höhere Bildwiederholrate, weil während jedes

Registerkarte	Beschreibung
	Lesevorgangs weniger Informationen verarbeitet werden müssen. Das Interlacing kann jedoch ein Flackern bewirken bzw. die Änderungen an der Hälfte der Bildzeilen können wahrnehmbar sein. **Adaptives Streaming** ermöglicht XProtect Smart Client das automatische Auswählen der Live-Videostreams, deren Auflösung am besten zu den Streams passt, die von dem zu betrachteten Gegenstand gefordert wird. Auf diese Weise wird die Belastung der CPU und der GPU gesenkt und damit Dekodierfähigkeit und -leistung des Computers verbessert. Hierzu ist es erforderlich, dass Multi-Streaming von Live-Videostreams mit unterschiedlicher Auflösungen konfiguriert wird, siehe Registerkarte „Streams“ (Geräte) auf Seite 232.

Registerkarte „Live“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Live	Verfügbarkeit von Live-Registerkarten/-Bereichen, Kamerawiedergabe und Overlay-Schaltflächen, Begrenzungsrahmen und Live-MIP-Plug-ins.

Registerkarte „Wiedergabe“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Wiedergabe	Verfügbarkeit von Wiedergabe-Registerkarten/-Bereichen, Layout von Druckberichten, unabhängige Wiedergabe, Lesezeichen, Begrenzungsrahmen und wiedergabebezogene MIP Plug-ins.

Registerkarte Einrichtung (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Konfiguration	Verfügbarkeit allgemeiner Einrichtung/Bereiche/Schaltflächen, einrichtungsbezogene MIP Plug-ins und Berechtigungen zur Bearbeitung von Karten und zur Bearbeitung von Live-Video-Pufferung.

Registerkarte „Export“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Exporte	Pfade, Privatzonenmasken, Video- und Standbildformate und Anweisungen zum Export selbiger, zum Export von Formaten für XProtect Smart Client – Player und vieles mehr.

Registerkarte „Zeitachse“ (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Zeitlinie	Ob Audio aufgenommen werden soll oder nicht, Zeit- und Bewegungsanzeige und der Umgang mit Wiedergabelücken. Außerdem können Sie auswählen, ob weitere Daten oder weitere Markierungen aus anderen Quellen angezeigt werden sollen.

Registerkarte Zutrittskontrolle (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Zutrittskontrolle	Wählen Sie aus, ob Zutrittsanforderungs-Benachrichtigungen auf dem XProtect Smart Client-Bildschirm angezeigt werden sollen, wenn sie von Ereignissen ausgelöst werden.

Registerkarte Alarm-Manager (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Alarm-Manager	Geben Sie an, ob auf den Computern, auf denen XProtect Smart Client installiert ist, Desktop-Benachrichtigungen für Alarme angezeigt werden sollen. Die Benachrichtigungen erscheinen nur, wenn XProtect Smart Client läuft - selbst wenn dieser minimiert ist. Desktop-Benachrichtigung für Alarme erscheinen nur, wenn die Alarme bestimmte Prioritäten haben, z.B. **Mittel** oder **Hoch**. Um zu konfigurieren, welche Alarmprioritäten Benachrichtigungen auslösen, gehen Sie auf **Alarme** > **Alarmdateneinstellungen** > **Alarmdatenniveaus**. Aktivieren Sie für jede erforderliche Alarmpriorität das Kontrollkästchen **Desktop-Benachrichtigungen aktivieren**. Siehe Alarmdateneinstellungen auf Seite 450.

Registerkarte „Smart Map" (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Registerkarte	Beschreibung
Smart Map	Angabe der Einstellungen für die Smart-Map-Funktion. Sie können angeben, ob OpenStreetMaps zur Verwendung als geographischer Hintergrund

Registerkarte	Beschreibung
	zur Verfügung steht und ob XProtect Smart Client automatisch Orte erstellt, wenn ein Benutzer ein benutzerdefiniertes Overlay für die Smart Map erstellt. Sie können außerdem angeben, wie oft das System Daten in Verbindung mit Smart Maps von Ihrem Computer löschen soll. Damit XProtect Smart Client Smart Map schneller anzeigen kann, speichert der Client die Kartendaten im Cache auf Ihrem Computer. Im Laufe der Zeit kann dies Ihren Computer verlangsamen. Caching kommt nicht zur Anwendung für Google Maps. Wenn Sie Bing Maps oder Google Maps als geographische Hintergründe verwenden möchten, geben Sie einen Bing Maps API-Schlüssel, oder einen Maps Static API-Schlüssel von Google ein.

Registerkarte „Layout-Ansicht" (Smart Client-Profile)

Diese Registerkarte ermöglicht Ihnen, die folgenden Eigenschaften zu bestimmen:

Site-Navigation: Clients: Management Client Profile

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

Management Client Profile ermöglichen es Systemadministratoren, die Management Client-Benutzeroberfläche für andere Benutzer zu ändern. Ordnen Sie Management Client-Profile Rollen zu, damit die Benutzeroberfläche nur die Funktionen der jeweiligen Administratorrolle anzeigt.

Wie Sie eine Rolle einem Management Client-Profil zuordnen, erfahren Sie auf der Registerkarte **Info** in den **Einstellungen für Rollen**. Siehe auch der Registerkarte Registerkarte „Info" (Rollen) auf Seite 379. Management Client-Profile regeln nur die visuelle Aufstellung von Systemfunktionen, nicht den tatsächlichen Zugriff dazu. Wie Sie den allgemeinen Zugriff auf Systemfunktionen für eine Rolle beschränken, erfahren Sie auf der Registerkarte **Allgemeine Sicherheit**. Siehe auch die Registerkarte Registerkarte „Gesamtsicherheit" (Rollen) auf Seite 381.

Damit alle Rollen Zugriff auf Managementserver haben, muss die Sicherheitsberechtigung **Verbinden**, die sich in den **Einstellungen für Rollen** > **Managementserver** > auf der Registerkarte Rolleneinstellungen auf Seite 379 befindet, aktiviert sein.

Sie können die Einstellungen für die Sichtbarkeit aller Management Client-Elemente ändern. Standardmäßig können über das Management Client-Profil alle Funktionen im Management Client angezeigt werden.

- Deaktivieren Sie die Kontrollkästchen für die relevanten Funktionen, um die Funktion für alle Benutzer visuell aus dem Management Client zu entfernen, und zwar für alle Management Client-Benutzer, die eine mit diesem Management Client-Profil zugeordnete Rolle haben

> Neben der integrierten Administratorrolle können nur Benutzer, die einer Rolle zugeordnet wurden, der das Recht zur **Verwaltung von Sicherheitsberechtigungen** auf dem Management-Server in der Registerkarte **Gesamtsicherheit** gewährt wurde, Management Client-Profile hinzufügen, bearbeiten und löschen.

Hinzufügen und Konfigurieren eines Management Client-Profils

Wenn Sie das Standardprofil nicht verwenden möchten, können Sie ein Management Client-Profil erstellen, um dieses zu konfigurieren.

1. Klicken Sie mit der rechten Maustaste auf **Management Client-Profile**.
2. Wählen Sie **Management Client-Profil hinzufügen** aus.
3. Geben Sie im Dialogfenster **Management Client-Profil hinzufügen** einen Namen und eine Beschreibung des neuen Profils ein und klicken Sie dann auf **OK**.
4. Klicken Sie im Bereich **Überblick** auf das erstellte Profil, um es zu konfigurieren.
5. Aktivieren oder deaktivieren Sie auf der Registerkarte **Profil** Funktionen des Management Client-Profils.

Kopieren eines Management Client-Profils

Wenn Sie ein Management Client-Profil mit Einstellungen haben, die Sie gerne wiederverwenden möchten, können Sie ein bereits vorhandenes Profil kopieren und kleine Änderungen an der Kopie vornehmen, anstatt ein Profil von Grund auf neu zu erstellen.

1. Klicken Sie auf **Management Client-Profil**, klicken Sie mit der rechten Maustaste auf das Profil im Bereich **Übersicht**, wählen Sie **Management Client-Profil kopieren** aus.
2. Es erscheint ein Dialogfenster; geben Sie dem kopierten Profil einen neuen einmaligen Namen und eine Beschreibung. Klicken Sie auf **OK**.
3. Klicken Sie im Bereich **Übersicht** auf das Profil und gehen Sie zur Registerkarte **Info** oder **Profil**, um das Profil zu konfigurieren.

Management Client-Profileigenschaften

Registerkarte „Info“ (Management Client-Profile)

Auf der Registerkarte **Info** können Sie Folgendes für Management Client-Profile festlegen:

Komponente	Voraussetzung
Name	Geben Sie einen Namen für das Management Client-Profil ein.
Priorität	Verwenden Sie die Pfeile nach oben und unten, um eine Priorität für das Management Client-Profil festzulegen.
Beschreibung	Geben Sie eine Beschreibung für das Profil ein. Dies ist optional.
Rollen, die das Management Client-Profil verwenden:	Dieses Feld zeigt die Rollen an, die Sie dem Management Client-Profil zugeordnet haben. Sie können dieses Feld nicht bearbeiten.

Registerkarte „Profil“ (Management Client-Profile)

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

Auf der Registerkarte **Profil** können Sie die Sichtbarkeit der folgenden Elemente von der Oberfläche des Management Client-Benutzers aktivieren oder deaktivieren:

Navigation

In diesem Abschnitt können Sie entscheiden, ob ein dem Management Client-Profil zugeordneter Administrator die unterschiedlichen Funktionen im Bereich **Navigation** sehen kann.

Navigationselement	Beschreibung
Grundlagen	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Lizenzinformationen** und **Standortinformationen** anzuzeigen.
Fernzugriffsdienste	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, die **Axis One-click-Kameraverbindung** anzuzeigen.

Navigationselement	Beschreibung
Server	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Aufzeichnungsserver** und **Failover-Server** anzuzeigen.
Geräte	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Kameras**, **Mikrofone**, **Lautsprecher**, **Metadaten**, **Eingang** und **Ausgang** anzuzeigen.
Client	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Smart Wall**, **Ansichtsgruppen**, **Smart Client-Profile**, **Management Client-Profile** und **Matrix** anzuzeigen.
Regeln und Ereignisse	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Regeln**, **Zeitprofile**, **Benachrichtigungsprofile**, **benutzerdefinierte Ereignisse**, **Analyseereignisse** und **generische Ereignisse** anzuzeigen.
Sicherheit	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Rollen** und **Basisnutzer** anzuzeigen.
System-Dashboard	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, den **Systemmonitor**, **Systemmonitor-Schwellenwerte**, **Beweissicherung**, **aktuelle Aufgaben** und **Konfigurationsberichte** anzuzeigen.
Server-Protokolle	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, Systemprotokolle, Auditprotokolle und durch Regeln ausgelöste Protokolle anzuzeigen.
Zutrittskontrolle	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Zutrittskontrollfunktionen** anzuzeigen, wenn Sie Ihrem System Zutrittskontroll-Systemintegrationen oder Plug-ins hinzugefügt haben.

Details

In diesem Abschnitt können Sie entscheiden, ob ein dem Management Client-Profil zugeordneter Administrator die unterschiedlichen Registerkarten für einen spezifischen Gerätekanal anzeigen darf, wie etwa die Registerkarte **Einstellungen** oder die Registerkarte **Aufzeichnung** für Kameras.

Gerätekanal	Beschreibung
Kameras	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle kamerabezogenen Einstellungen und Registerkarten anzuzeigen.
Mikrofone	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle mikrofonbezogenen Einstellungen und Registerkarten anzuzeigen.
Lautsprecher	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle lautsprecherbezogenen Einstellungen und Registerkarten anzuzeigen.
Metadaten	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle metadatenbezogenen Einstellungen und Registerkarten anzuzeigen.
Eingang	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle eingangsbezogenen Einstellungen und Registerkarten anzusehen.
Ausgang	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, einige oder alle ausgangsbezogenen Einstellungen und Registerkarten anzusehen.

Menü „Extras“

In diesem Abschnitt können Sie entscheiden, ob ein dem Management Client-Profil zugeordneter Administrator die Elemente des Menüs **Werkzeuge** ansehen kann.

Werkzeugmenüoption	Beschreibung
Registrierte Services	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Registrierte Dienste** anzusehen.
Effektive Rollen	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Effektive Rollen** anzusehen.
Optionen	Ermöglicht es dem Administrator, der dem Management Client-Profil zugeordnet wurde, **Optionen** anzusehen.

Föderale Sites

In diesem Abschnitt können Sie entscheiden, ob ein dem Management Client-Profil zugeordneter Administrator den Bereich **Hierarchie der föderalen Standorte** ansehen kann.

Site-Navigation: Clients: Konfigurieren von Matrix

Mit Matrix können Sie Video von jeder Kamera eines Netzwerks in Ihrem System zu Matrix-Empfänger senden. Ein Matrix-Empfänger ist ein Computer, der von Matrix ausgelöstes Video anzeigt. Es gibt zwei Arten von Matrix-Empfänger:

- Computer, auf denen eine zugehörige Matrix Anwendung ausgeführt wird
- Computer, die XProtect Smart Client ausführen

Um eine Liste von Matrix-Empfängern zu sehen, die in der Management Client konfiguriert wurden, erweitern Sie **Client** im Bereich **Standort-Navigation** und wählen Sie **Matrix**. Eine Liste von Matrix-Konfigurationen wird im Bereich **Eigenschaften** angezeigt.

> Jeder Matrix-Empfänger, ob Computer mit dem Matrix Monitor oder dem XProtect Smart Client, muss zum Empfang von durch Matrix ausgelösten Video konfiguriert werden. Weitere Informationen finden Sie unter XProtect Smart Wall (erklärt) auf Seite 31 und XProtect Smart Client (erklärt) auf Seite 26.

Matrix Empfänger hinzufügen

Um über das Management Client einen bereits bestehenden Matrix-Empfänger hinzuzufügen, zum Beispiel eine bestehende Matrix Monitor- oder XProtect Smart Client-Installation:

1. Klappen Sie **Clients** aus und wählen Sie **Matrix**.
2. Klicken Sie mit der rechten Maustaste auf **Matrix Konfigurationen** und wählen Sie **Hinzufügen Matrix** aus.
3. Füllen Sie die Felder im Dialogfenster **Hinzufügen Matrix** aus.
    1. Im Feld **Adresse** geben Sie die IP-Adresse oder den Hostname des Matrix-Empfängers ein.
    2. Geben Sie im Feld **Port** die Portnummer des Systems, die von der Installation des Matrix-Empfängers verwendet wird. Sie können die Portnummer und das Passwort auf diese Weise finden: Für eine Matrix Monitor Anwendung, gehen Sie zum Dialogfenster Matrix Monitor **Konfiguration**. Für XProtect Smart Client, das Benutzerhandbuch für XProtect Smart Client..
4. Klicken Sie auf **OK**.

Sie können nun die Matrix-Empfänger in Regeln verwenden.

Ihr System bestätigt nicht, ob die Portnummer oder Passwort korrekt ist oder ob Portnummer, Passwort oder Typ dem tatsächlichen Matrix-Empfänger entspricht. Stellen Sie also sicher, dass Sie die richtigen Informationen eingeben.

Regeln dafür festlegen, wie Videoaufzeichnungen an Matrix-Empfänger gesendet werden

Damit Video an Matrix-Empfänger gesendet wird, müssen Sie die Matrix-Empfänger in einer Regel einschließen, welche die Übertragung des Videos an den zugehörigen Matrix-Empfänger auslöst. Dafür müssen Sie folgendes tun:

1. Erweitern Sie im Bereich **Standort-Navigation Regeln und Ereignisse** > **Rules**. Klicken Sie mit der rechten Maustaste auf **Regeln**, um den Assistenten für **Regel verwalten** zu öffnen. Beim ersten Schritt wählen Sie einen Regeltypen aus und im Zweiten eine Bedingung.
2. In Schritt 3 von **Regel verwalten** (**Schritt 3: Aktionen**) wählen Sie die Aktion **Auf Matrix Ansicht stellen <Geräte>** aus.
3. Klicken Sie auf den Matrix-Link in der Beschreibung der ersten Regel.
4. Im Dialogfenster **Matrix-Konfiguration auswählen**, wählen Sie den relevanten Matrix-Empfänger und klicken Sie auf **OK**.
5. Klicken Sie auf den Link **Geräte** in der Beschreibung der ersten Regel und wählen Sie von welcher Kamera Sie das Video an den Matrix-Empfänger senden möchten. Klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.
6. Klicken Sie auf **Fertig**, wenn die Regel abgeschlossen ist oder legen Sie nach Bedarf weitere Aktionen und/oder eine Anhalte-Aktion fest.

Wenn Sie einen Matrix-Empfänger entfernen, funktioniert keine der Regeln mehr, die diesen Matrix-Empfänger beinhalten.

Dasselbe Video an mehrere XProtect Smart Client Ansichten senden

Wenn der Matrix-Empfänger XProtect Smart Client ist, können Sie das gleiche Video an Matrix Positionen in mehreren von XProtect Smart Client Ansichten senden, wenn die Matrix Positionen der Ansichten dieselben Portnummern und Passwörter vorweisen:

1. Erstellen Sie in XProtect Smart Client die zugehörigen Ansichten und Matrix Positionen, welche die gleiche Portnummer und Passwörter teilen.
2. In Management Client, fügen Sie die relevanten XProtect Smart Client als Matrix-Empfänger hinzu.
3. Sie können die Matrix-Empfänger in einer Regel einschließen.

Site-Navigation: Regeln und Ereignisse

Dieser Abschnitt beschreibt, wie Ereignisse und Regeln konfiguriert werden, damit Sie Maßnahmen und Alarme im System auslösen können. Er erklärt außerdem, wie Benachrichtigungen per E-Mail und Zeitlimits zu Regeln eingerichtet werden.

Regeln und Ereignisse (Erklärung)

Regeln sind ein zentrales Element Ihres Systems. Regeln bestimmen äußerst wichtige Einstellungen, beispielsweise wann Kameras aufzeichnen sollten, wann PTZ-Kameras Wachrundgänge ausführen sollten, wann Benachrichtigungen verschickt werden sollten, etc.

Beispiel - Eine Regel, die festlegt, dass eine bestimmte Kamera die Aufzeichnung starten sollte, sobald sie eine Bewegung registriert:

Ereignisse sind zentrale Elemente bei der Anwendung des Assistenten **Regel verwalten**. In diesem Assistenten werden Ereignisse primär zur Auslösung von Aktionen verwendet. Sie können beispielsweise eine Regel erstellen, die festlegt, dass beim **Ereignis** Bewegungsregistrierung das Überwachungssystem die **Aktion** ausführen sollte, von einer bestimmten Kamera aus mit der Videoaufzeichnung zu beginnen.

Die folgenden Arten von Bedingungen können Regeln auslösen:

Name	Beschreibung
Ereignisse	Wenn im Überwachungssystem Ereignisse auftreten, beispielsweise sobald Bewegungen registriert werden, oder das System Informationen von externen Sensoren empfängt.
Zeitintervall	Wenn Sie bestimmte Zeiträume eingeben, zum Beispiel: `Donnerstag, der 16. August 2007, 7:00 bis 7:59 Uhr` oder `jeden Samstag und Sonntag`
Wiederholte Zeit	Wenn Sie eine Aktion einrichten, die nach einem detaillierten, sich wiederholenden Zeitplan ausgeführt werden soll.

Name	Beschreibung
	Beispielsweise: • Jede Woche Dienstags, alle 1 Stunde(n) zwischen 15:00 und 15:30 • Am 15. alle 3 Monat(e) um 11:45 Uhr • Jeden Tag alle 1 Stunde(n) zwischen 15:00 und 19:00 Uhr  Die Zeit basiert auf den örtlichen Zeiteinstellungen des Servers, auf dem Management Client installiert ist. Weitere Informationen finden Sie unter Wiederholte Zeit auf Seite 349.

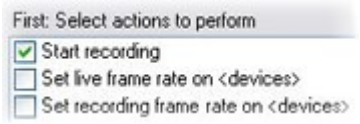
Sie können mit folgenden Punkten unter **Regeln und Ereignisse** arbeiten:

- **Regeln**: Regeln sind ein zentrales Element des Systems. Das Verhalten Ihres Überwachungssystems wird maßgeblich durch Regeln bestimmt. Wenn Sie eine Regel erstellen, können Sie mit allen möglichen Ereignistypen arbeiten
- **Zeitprofile**: Zeitprofile sind im Management Client definierte Zeiträume. Sie verwenden sie beim Erstellen von Regeln im Management Client, z. B. um eine Regel zu erstellen, die festlegt, dass in einem bestimmten Zeitprofil eine bestimmte Aktion ausgeführt werden soll
- **Benachrichtigungsprofile**: Sie können Benachrichtigungsprofile zum Einstellen gebrauchsfertiger E-Mail-Benachrichtigungen verwenden, die automatisch von Regeln ausgelöst werden können, z. B. beim Eintreten eines bestimmten Ereignisses
- **Benutzerdefinierte Ereignisse**: Benutzerdefinierte Ereignisse sind maßgeschneiderte Ereignisse, die es Benutzern ermöglichen, Ereignisse im System manuell auszulösen oder auf Eingänge des Systems zu reagieren
- **Analyseereignisse**: Analyseereignisse werden zum Empfang von Daten von Video-Content-Analyse-Lösungen (VCA) von anderen Herstellern benutzt. Sie können Analyseereignisse als Basis für Alarme verwenden
- **Generische Ereignisse**: Generische Ereignisse ermöglichen es Ihnen, Aktionen im XProtect Event-Server auszulösen, indem einfache Zeichenketten über das IP-Netzwerk an Ihr System gesendet werden

Siehe Ereignisübersicht auf Seite 328 für eine Liste von Ereignissen.

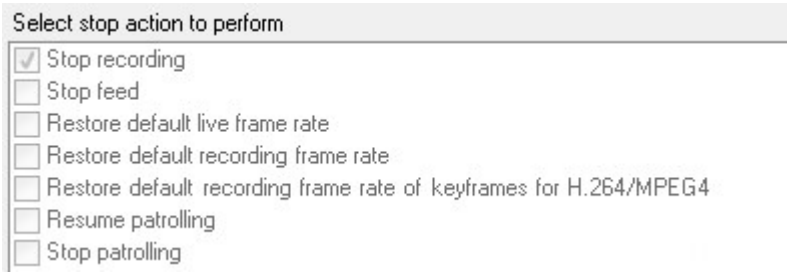
Aktionen und Stopp-Aktionen (Erklärung)

Beim Hinzufügen von Regeln (siehe Hinzufügen einer Regel auf Seite 347) im Assistenten **Regel verwalten** können Sie zwischen verschiedenen Aktionen wählen:



Einige der Aktionen erfordern eine Stopp-Aktion. **Beispiel**: Wenn Sie die Aktion **Aufzeichnung starten** auswählen, beginnt die Aufzeichnung und läuft potenziell für unbegrenzte Zeit weiter. Aus diesem Grund hat die Aktion **Aufzeichnung starten** eine obligatorische Stopp-Aktion namens **Aufzeichnung stoppen**.

Der Assistent **Regel verwalten** stellt sicher, dass Sie Stopp-Aktionen festlegen, wenn dies erforderlich ist:



Auswählen von Stopp-Aktionen. Beachten Sie in dem Beispiel die obligatorische Stopp-Aktion (ausgewählt, ausgegraut), die irrelevanten Stopp-Aktionen (ausgegraut) und die optionalen Stopp-Aktionen (auswählbar).

Alle Aktionstypen über das XProtect-System sind beschrieben. Ihnen können mehr Aktionen zur Verfügung stehen, wenn Ihre Systeminstallation Zusatzprodukte oder anbieterspezifische Plug-ins nutzt. Für jeden Aktionstyp sind Informationen zur Stopp-Aktion angeführt, falls relevant:

Aktion	Beschreibung
Aufzeichnung auf <Geräten> starten	Starten der Aufzeichnung und Speichern der Daten von den ausgewählten Geräten in der Datenbank. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, Folgendes festzulegen: Wann die Aufnahme beginnen soll. Das passiert entweder sofort oder ein paar Sekunden vor dem auslösenden Ereignis/Beginn des auslösenden Zeitintervalls; auf welchen Geräten die Aktion durchgeführt werden soll.

Aktion	Beschreibung
	Für diesen Aktionstyp muss die Aufzeichnung auf den Geräten aktiviert sein, mit denen die Aktion verknüpft ist. Sie können Daten vor einem Ereignis oder Zeitintervall nur dann speichern, wenn Sie Voralarm-Puffer für die entsprechenden Geräte aktiviert haben. Die Aktivierung der Aufzeichnung und die Einstellungen für Voralarm-Puffer für ein Gerät erfolgen auf der Registerkarte **Aufzeichnung**. **Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Aufzeichnung stoppen**. Ohne diese Stopp-Aktion würde die Aufzeichnung potenziell für unbegrenzte Zeit weiterlaufen. Sie können auch weitere Stopp-Aktionen festlegen.
Feed auf <Geräten> starten	Starten des Datenfeeds von Geräten zum System. Wenn der Feed von einem Gerät gestartet wird, werden Daten vom Gerät zum System übertragen, sodass Sie diese je nach Datentyp anzeigen oder aufzeichnen können. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, festzulegen, auf welchen Geräten die Feeds gestartet werden sollen. Das System beinhaltet eine Standardregel, die sicherstellt, dass Feeds immer auf allen Kameras gestartet werden. **Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Feed stoppen**. Sie können auch weitere Stopp-Aktionen festlegen. Durch die Verwendung der obligatorischen Stopp-Aktion **Feed stoppen** zum Stoppen des Feeds von einem Gerät werden keine Daten mehr vom Gerät zum System übertragen. Damit sind dann beispielsweise Live-Ansicht und Aufzeichnung von Videos nicht mehr möglich. Ein Gerät, für das Sie den Feed gestoppt haben, kann jedoch weiter mit dem Aufzeichnungsserver kommunizieren und Sie können den

Aktion	Beschreibung
	Feed über eine Regel wieder automatisch starten – anders, als wenn Sie das Gerät manuell deaktiviert haben. Dieser Aktionstyp ermöglicht zwar Zugriff auf die Datenfeeds der ausgewählten Geräte, garantiert jedoch nicht, dass Daten aufgezeichnet werden, da Sie die Aufzeichnungseinstellungen separat festlegen müssen.
Einstellen von <Smart Wall> auf <Voreinstellung>	Stellt XProtect Smart Wall auf eine ausgewählte Voreinstellung ein. Legen Sie die Voreinstellung auf der Registerkarte **Smart Wall Voreinstellungen** fest. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
<Smart Wall>-<Bildschirm> auf Anzeigen von <Kameras> setzen	Stellt einen bestimmten XProtect Smart Wall-Monitor auf die Anzeige von Live-Video von den ausgewählten Kameras an diesem Standort oder an einem untergeordneten Standort ein, der in Milestone Federated Architecture konfiguriert wurde. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
<Smart Wall>-<Bildschirm> auf Anzeigen von Text-<Nachrichte> setzen	Stellt einen bestimmten XProtect Smart Wall-Monitor auf die Anzeige einer benutzerdefinierten Textnachricht mit bis zu 200 Zeichen ein. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.

Aktion	Beschreibung
<Kameras> vom <Smart Wall>-Monitor <Bildschirm> entfernen	Stoppen der Videoanzeige von einer bestimmten Kamera. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Live-Bildrate auf <Geräten> festlegen	Legt die Bildrate für die Anzeige von Live-Video durch das System von den ausgewählten Kameras fest; sie ersetzt die Standardbildrate der Kameras. Die Einstellung erfolgt auf der Registerkarte **Einstellungen**. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, die Bildrate und die Geräte dafür festzulegen. Überprüfen Sie stets, ob die angegebene Bildrate an den entsprechenden Kameras verfügbar ist. **Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Standard-Live-Bildrate wiederherstellen**. Ohne diese Stopp-Aktion würde die Standardbildrate potenziell nie wiederhergestellt werden. Sie können auch weitere Stopp-Aktionen festlegen.
Aufzeichnungsbildrate auf <Geräten> festlegen	Legt die Bildrate für das Speichern aufgezeichneter Videos von den ausgewählten Kameras in der Datenbank fest; sie ersetzt die Standardbildrate der Kameras. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, die Aufzeichnungsbildrate und die Kameras dafür festzulegen. Sie können nur eine Aufzeichnungsbildrate für JPEG festlegen, einen Video-Codec, bei dem jedes Bild separat in ein JPEG-Bild komprimiert wird. Für diesen Aktionstyp muss auch die Aufzeichnung an den Kameras aktiviert sein, mit denen die Aktion verknüpft ist. Die Aktivierung der Aufzeichnung für eine Kamera erfolgt auf der Registerkarte **Aufzeichnung**. Die

Aktion	Beschreibung
	maximale Bildrate, die festgelegt werden kann, hängt von den entsprechenden Kameratypen und ihrer ausgewählten Bildauflösung ab. **Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Standard-Aufzeichnungsbildrate wiederherstellen**. Ohne diese Stopp-Aktion würde die Standard-Aufzeichnungsbildrate potenziell nie wiederhergestellt werden. Sie können auch weitere Stopp-Aktionen festlegen.
Aufzeichnungsbildrate für alle Bilder bei MPEG-4/H.264/H.265 auf <Geräte> setzen	Legt die Bildrate für das Speichern aufgezeichneter Videos von den ausgewählten Kameras in der Datenbank für die Aufzeichnung aller Bilder, nicht bloß von Keyframes, fest. Aktivieren Sie die Funktion zur Aufzeichnung nur der Keyframes auf der Registerkarte **Aufzeichnung**. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, auszuwählen, für welche Geräte die Aktion gelten soll. Sie können für MPEG-4/H.264/H.265 nur die Keyframe-Aufzeichnung aktivieren. Für diesen Aktionstyp muss auch die Aufzeichnung an den Kameras aktiviert sein, mit denen die Aktion verknüpft ist. Die Aktivierung der Aufzeichnung für eine Kamera erfolgt auf der Registerkarte **Aufzeichnung**. **Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Standard-Aufzeichnungsbildrate von Keyframes für MPEG-4/H.264/H.265 wiederherstellen** Ohne diese Stopp-Aktion würde die Standardeinstellung potenziell nie wiederhergestellt werden. Sie können auch weitere Stopp-Aktionen festlegen.
Wachrundgang auf <Gerät> unter	Startet PTZ-Wachrundgang für eine bestimmte PTZ-Kamera

Aktion	Beschreibung
Verwendung von <Profil> mit Priorität auf PTZ <Priorität> starten	mit einer bestimmten Priorität gemäß einem bestimmten Wachrundgangprofil. Dies ist eine genaue Definition der Art und Weise, wie der Wachrundgang ausgeführt werden soll, einschließlich der Sequenz von Preset Positionen, Zeitsteuerungseinstellungen usw. Wenn Sie Ihr System von einer älteren Systemversion aktualisiert haben, wurden die alten Werte (**Sehr niedrig**, **Niedrig**, **Mittel**, **Hoch** und **Sehr hoch**) folgendermaßen übersetzt: • Sehr niedrig = 1.000 • Niedrig = 2.000 • Mittel = 3.000 • Hoch = 4.000 • Sehr hoch = 5.000 Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, ein Wachrundgangprofil auszuwählen. Sie können für ein Gerät jeweils nur ein Wachrundgangprofil auswählen. Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, PTZ-Geräte sein. Sie müssen mindestens ein Wachrundgangprofil für das/die Gerät (e) definieren. Auf der Registerkarte **Wachrundgang** können Sie Wachrundgangprofile für eine PTZ-Kamera definieren. **Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die

Aktion	Beschreibung
	Stopp-Aktion festzulegen: **Wachrundgang stoppen** Ohne diese Stopp-Aktion würde der Wachrundgang potenziell nie aufhören. Sie können auch weitere Stopp-Aktionen festlegen.
Wachrundgang für <Geräte> anhalten	Hält den Wachrundgang an. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, die Geräte festzulegen, für die der Wachrundgang angehalten werden soll. Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, PTZ-Geräte sein. Sie müssen mindestens ein Wachrundgangprofil für das/die Gerät (e) definieren. Auf der Registerkarte **Wachrundgang** können Sie Wachrundgangprofile für eine PTZ-Kamera definieren. **Stopp-Aktion benötigt**: Dieser Aktionstyp benötigt eine oder mehrere Stopp-Aktionen. Während einem der folgenden Schritte fordert Sie der Assistent automatisch dazu auf, die Stopp-Aktion festzulegen: **Wachrundgang fortsetzen** Ohne diese Stopp-Aktion würde der Wachrundgang potenziell für unbegrenzte Zeit angehalten bleiben. Sie können auch weitere Stopp-Aktionen festlegen.
<Gerät> auf Position <Voreinstellung> mit Priorität auf PTZ <Priorität> verschieben	Bewegt eine bestimmte Kamera in eine bestimmte Preset Position – jedoch immer gemäß Priorität. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, eine Preset-Position auszuwählen. Nur eine Preset-Position an einer Kamera kann ausgewählt

Aktion	Beschreibung
	werden. Es können nicht mehrere Preset-Positionen ausgewählt werden. Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, PTZ-Geräte sein. Für diese Aktion müssen Sie mindestens eine Preset Position für diese Geräte definiert haben. Auf der Registerkarte **Voreinstellungen** können Sie Preset Positionen für eine PTZ-Kamera definieren. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Auf <Geräte> mit Priorität auf PTZ <Priorität> auf Standardvoreinstellung verschieben	Verschiebt eine oder mehr Kameras in ihre jeweiligen Standard-Voreinstellungspositionen – jedoch immer gemäß Priorität. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, auszuwählen, für welche Geräte die Aktion gelten soll. Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, PTZ-Geräte sein. Für diese Aktion müssen Sie mindestens eine Preset Position für diese Geräte definiert haben. Auf der Registerkarte **Voreinstellungen** können Sie Preset Positionen für eine PTZ-Kamera definieren.

Aktion	Beschreibung
	Stopp-Aktion nicht obligatorisch: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Geräteausgang auf <Status> setzen	Legt einen Ausgang auf einem Gerät auf einen bestimmten Status fest (aktiviert oder deaktiviert). Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, den Status und die Geräte dafür festzulegen. Für diesen Aktionstyp müssen die Geräte, mit denen die Aktion verknüpft ist, jeweils mindestens einen externen Ausgang besitzen, der mit einem Ausgangsport verbunden ist. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Lesezeichen auf <Gerät> erstellen	Erstellt ein Lesezeichen bei Live-Streaming oder Aufzeichnungen von einem bestimmten Gerät. Über Lesezeichen lassen sich bestimmte Ereignisse oder Zeitabschnitte einfach zurückverfolgen. Lesezeicheneinstellungen werden im Dialogfeld **Optionen** festgelegt. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, Lesezeichendetails festzulegen und Geräte auszuwählen. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Audio <Nachricht> auf <Gerät> mit <Priorität> Wiedergabe	Gibt bei Auslösung durch ein Ereignis eine Audionachricht auf ausgewählten Geräten wieder. Bei den Geräten handelt es sich meistens um Lautsprecher oder Kameras. Dieser Aktionstyp erfordert, dass Sie die Nachricht bei **Tools** > **Optionen** > Registerkarte **Audionachrichten** ins System hochgeladen haben.

Aktion	Beschreibung
	Sie können mehrere Regeln für ein Ereignis erstellen und verschiedene Nachrichten an die Geräte senden, jedoch immer gemäß Priorität. Die Prioritäten, die die Sequenz festlegen, sind diejenigen, die auf der Registerkarte **Sprache** für die Regel und das Gerät für eine Rolle festgelegt sind: • Wenn eine Nachricht wiedergegeben wird und eine andere Nachricht mit derselben Priorität an denselben Lautsprecher gesendet wird, wird die erste Nachricht abgeschlossen, dann wird die zweite Nachricht wiedergegeben • Wenn eine Nachricht wiedergegeben wird und eine andere Nachricht mit höherer Priorität an denselben Lautsprecher gesendet wird, wird die erste Nachricht unterbrochen und die zweite Nachricht sofort wiedergegeben
Benachrichtigung senden an <Profil>	Sendet eine Benachrichtigung mit einem bestimmten Benachrichtigungsprofil. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, ein Benachrichtigungsprofil sowie die Geräte auszuwählen, von denen Voralarm-Bilder enthalten sein sollen. Sie können nur ein einziges Benachrichtigungsprofil auswählen. Für ein einzelnes Benachrichtigungsprofil können jedoch mehrere Empfänger vorhanden sein. Sie können auch mehrere Regeln für dasselbe Ereignis erstellen und für jedes der Benachrichtigungsprofile unterschiedliche Benachrichtigungen versenden. Um die Inhalte von Regeln zu kopieren und wiederzuverwenden, klicken Sie in der Liste **Regeln** mit der rechten Maustaste auf eine Regel. Für diesen Aktionstyp müssen Sie mindestens ein Benachrichtigungsprofil definiert haben. Voralarm-Bilder sind nur enthalten, wenn Sie die Option **Bilder einschließen** für das entsprechende Benachrichtigungsprofil aktiviert haben. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen

Aktion	Beschreibung
	festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Neuen <Protokolleintrag> vornehmen	Generiert einen Eintrag im Regelprotokoll. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, einen Text für den Protokolleintrag festzulegen. Beim Angeben des Protokolltexts können Sie in die Protokollnachricht Variablen einfügen, wie z. B. **$DeviceName$** oder **$EventName$**. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Plug-In auf <Geräten> starten	Startet ein oder mehrere Plug-ins. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, erforderliche Plug-ins und die Geräte, auf denen die Plug-ins gestartet werden sollen, festzulegen. Für diesen Aktionstyp müssen ein oder mehrere Plug-ins auf Ihrem System installiert sein. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Plug-In auf <Geräten> stoppen	Stoppt ein oder mehrere Plug-ins. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, erforderliche Plug-ins und die Geräte, auf denen die Plug-ins gestoppt werden sollen, festzulegen. Für diesen Aktionstyp müssen ein oder mehrere Plug-ins auf Ihrem System installiert sein. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.

Aktion	Beschreibung
Neue Einstellungen auf <Geräte> anwenden	Ändert die Geräteeinstellungen auf einem oder mehreren Geräten. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, die relevanten Geräte festzulegen, und Sie können die relevanten Einstellungen an diesen Geräten festlegen. Wenn Sie Einstellungen für mehrere Geräte festlegen, können Sie nur solche Einstellungen ändern, die für alle angegebenen Geräte verfügbar sind. **Beispiel**: Sie legen fest, dass die Aktion mit Gerät 1 und Gerät 2 verknüpft sein soll. Gerät 1 hat die Einstellungen A, B und C, Gerät 2 die Einstellungen B, C und D. In diesem Fall können Sie nur die Einstellungen ändern, die für beide Geräte verfügbar sind, nämlich B und C. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Matrix auf Ansicht von <Geräte> setzen	Sorgt dafür, dass Videos von den ausgewählten Kameras auf einem Rechner angezeigt werden, der Matrix-ausgelöste Videos anzeigen kann – z. B. einem Rechner, auf dem Sie entweder XProtect Smart Client oder die Matrix Monitor-Anwendung installiert haben. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, einen Matrix-Empfänger und ein oder mehrere Geräte festzulegen, deren Videobilder auf dem ausgewählten Matrix-Empfänger angezeigt werden sollen. Mit diesem Aktionstyp können Sie jeweils immer nur einen Matrix-Empfänger auswählen. Wenn Sie wollen, dass Videobilder von den ausgewählten Geräten bei mehreren Matrix-Empfängern angezeigt werden, sollten Sie eine Regel

Aktion	Beschreibung
	für jeden benötigten Matrix-Empfänger erstellen oder die XProtect Smart Wall-Funktion verwenden. Um die Inhalte von Regeln zu kopieren und wiederzuverwenden, klicken Sie in der Liste **Regeln** mit der rechten Maustaste auf eine Regel. So müssen Sie nicht mehrere, beinahe identische Regeln von Grund auf neu erstellen. Im Rahmen der Konfiguration der Matrix-Empfänger selbst müssen Benutzer die Portnummer und das Passwort festlegen, die für die Matrix-Kommunikation benötigt werden. Vergewissern Sie sich, dass die Benutzer Zugriff auf diese Informationen haben. Die Benutzer müssen im Allgemeinen auch die IP-Adressen von zulässigen Hosts festlegen, von denen Befehle in Bezug auf die Anzeige Matrix-ausgelöster Videobilder akzeptiert werden. In diesem Fall müssen die Benutzer auch die IP-Adresse des Management-Servers sowie etwaige verwendete Router oder Firewalls kennen.
SNMP-Trap senden	Generiert eine kurze Nachricht, die Ereignisse bei ausgewählten Geräten protokolliert. Der Text von SNMP-Traps wird automatisch generiert und ist nicht anpassbar. Er kann den Quelltyp und den Namen des Geräts enthalten, bei dem das Ereignis aufgetreten ist. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Fernaufzeichnungen von <Geräten> abrufen und speichern	Ruft Fernaufzeichnungen für einen angegebenen Zeitraum vor und nach dem auslösenden Ereignis von ausgewählten

Aktion	Beschreibung
	Geräten ab und speichert sie (die Geräte müssen lokale Aufzeichnung unterstützen). Diese Regel ist unabhängig von der Einstellung der **Option zum automatischen Abruf von Fernaufzeichnungen, wenn Verbindung wiederhergestellt wurde**. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Fernaufzeichnungen zwischen <Start- und Endzeit> von <Geräten> abrufen und speichern	Ruft Fernaufzeichnungen in einem angegebenen Zeitraum von ausgewählten Geräten ab und speichert sie (die Geräte müssen lokale Aufzeichnung unterstützen). Diese Regel ist unabhängig von der Einstellung der **Option zum automatischen Abruf von Fernaufzeichnungen, wenn Verbindung wiederhergestellt wurde**. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Angehängte Bilder speichern	Sorgt dafür, dass ein Bild, das vom Ereignis „Bilder empfangen“ empfangen wird (per SMTP-E-Mail von einer Kamera gesendet) zur zukünftigen Verwendung gespeichert wird. In Zukunft können andere Ereignisse diese Aktion potenziell auch auslösen. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Archivierung auf <Archive> aktivieren	Startet die Archivierung bei einem oder mehreren Archiven. Wenn Sie diesen Aktionstyp auswählen, fordert Sie der Assistent **Regel verwalten** dazu auf, relevante Archive auszuwählen. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt

Aktion	Beschreibung
	keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Auf <Site> <benutzerdefiniertes Ereignis> auslösen	Diese Aktion ist vorwiegend in der Milestone Federated Architecture relevant, Sie können sie jedoch auch in einer Konfiguration mit einem einzigen Standort verwenden. Mit dieser Regel lösen Sie ein benutzerdefiniertes Ereignis an einem Standort aus, üblicherweise einem Remote-System in einer föderalen Hierarchie. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
<Zutrittsanforderungsbenachrichtigung> anzeigen	Hierüber können Sie auf Anforderungsnachrichten-Pop-ups auf dem XProtect Smart Client-Bildschirm zugreifen, wenn die Kriterien für die auslösenden Ereignisse erfüllt sind.Milestone empfiehlt, dass Sie Zutrittskontrollereignisse als auslösende Ereignisse für diese Aktion anwenden, weil Zutrittsanforderungsnachrichten typischerweise zum Betrieb an entsprechenden Zutrittskontroll-Befehlen und Kameras konfiguriert sind. Für diesen Aktionstyp müssen ein oder mehrere Zutrittskontroll-Plug-ins auf Ihrem System installiert sein. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
<Kamera> auf <regelbasiertem DLNA Kanal> einstellen	Kameras werden auf der Grundlage von Ereignissen an dem regelbasierten DLNA Kanal hinzugefügt. Für diese Art von Aktion müssen Sie einen DLNA-Server auf Ihrem System installiert haben. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem

Aktion	Beschreibung
	bestimmten Zeitraum ausgeführt werden.
Entfernen Sie die <Kamera> vom <regelbasierten DLNA Kanal>	Kameras werden auf der Grundlage von Ereignissen von dem regelbasierten DLNA Kanal entfernt. Für diese Art von Aktion müssen Sie einen DLNA-Server auf Ihrem System installiert haben. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Aktuelle Kamera vom <regelbasierten DLNA Kanal> entfernen	Die Kamera mit dem aktiven Stream wird basierend auf Ereignissen aus dem regelbasierten DLNA-Kanal entfernt. Für diese Art von Aktion müssen Sie einen DLNA-Server auf Ihrem System installiert haben. **Stopp-Aktion nicht obligatorisch**: Dieser Aktionstyp benötigt keine Stopp-Aktion.Sie können optionale Stopp-Aktionen festlegen, die entweder bei einem Ereignis oder nach einem bestimmten Zeitraum ausgeführt werden.
Das Passwort auf Hardwaregeräten ändern	Ändert das Passwort ausgewählter Hardwaregeräte in ein zufällig erzeugtes Passwort auf der Grundlage der Passwortanforderungen für das jeweilige Hardwaregerät. Eine Liste der unterstützten Hardwaregeräte finden Sie unter https://www.milestonesys.com/community/business-partner-tools/supported-devices/. Diese Aktion steht nur zur Verfügung, wenn Sie mithilfe des Regeltyps **Eine Aktion ausführen an einem <recurring time>** eine Regel dafür aufstellen. Für diese Maßnahme stehen die folgenden Ereignisse zur Verfügung: • Planmäßige Passwortänderung gestartet auf Seite 340

Aktion	Beschreibung
	• Planmäßige Passwortänderung erfolgreich abgeschlossen auf Seite 340 • Planmäßige Passwortänderung abgeschlossen, jedoch mit Fehlern auf Seite 340 Für Aktionen dieses Typs gibt es keine Stopp-Aktion. Sie können den Fortgang dieser Aktion in dem Knoten **Aktuelle Aufgaben** ansehen. Weitere Informationen finden Sie unter Derzeitige Aufgaben (Erklärung) auf Seite 435. Um die Ergebnisse der Aktion anzusehen - gehen Sie zu dem Knoten **Serverprotokolle** auf der Registerkarte **Systemprotokolle** . Weitere Informationen finden Sie auf der Registerkarte Registerkarte „Serverprotokolle“ (Optionen) auf Seite 124. Weitere Informationen finden Sie unter Systemprotokolle (Eigenschaften) auf Seite 440.

Ereignisübersicht

Wenn Sie eine ereignisbasierte Regel im **Regel verwalten**-Assistenten hinzufügen, können Sie unter einer Anzahl unterschiedlicher Ereignistypen wählen. Damit Sie einen guten Überblick erhalten, sind auswählbare Ereignisse nach folgenden Kriterien in Gruppen aufgelistet:

Hardware:

Einige Hardware kann Ereignisse selbst erstellen, um beispielsweise Bewegung zu registrieren. Sie können diese Ereignisse verwenden, müssen sie jedoch erst auf der Hardware konfigurieren, bevor Sie diese im System nutzen können. Sie können die aufgelisteten Ereignisse möglicherweise nicht auf jeder Hardware nutzen, da nicht alle Kameratypen Manipulationen oder Temperaturveränderungen erkennen können.

Hardware – Konfigurierbare Ereignisse:

Konfigurierbare Ereignisse von Hardware werden durch Gerätetreiber automatisch importiert. Dies bedeutet, dass sie von Hardware zu Hardware variieren und deswegen hier nicht dokumentiert sind. Konfigurierbare Ereignisse werden nicht ausgelöst, bis Sie diese dem System hinzugefügt und sie auf der Registerkarte **Ereignis** auf der Hardware konfiguriert haben. Für einige konfigurierbare Ereignisse müssen Sie sogar die Kamera (Hardware) an sich konfigurieren.

Hardware – Voreingestellte Ereignisse:

Ereignis	Beschreibung
Kommunikationsfehler (Hardware)	Tritt auf, wenn die Verbindung zur Hardware unterbrochen wird.
Kommunikation gestartet (Hardware)	Tritt auf, wenn die Verbindung zur Hardware hergestellt wurde.
Kommunikation gestoppt (Hardware)	Tritt auf, wenn die Verbindung zur Hardware beendet wurde.

Geräte – Konfigurierbare Ereignisse:

Konfigurierbare Ereignisse von Geräten werden durch Gerätetreiber automatisch importiert. Dies bedeutet, dass sie von Gerät zu Gerät variieren und deswegen hier nicht dokumentiert sind. Konfigurierbare Ereignisse werden nicht ausgelöst, bis Sie diese dem System hinzugefügt und sie auf der Registerkarte **Ereignis** auf einem Gerät konfiguriert haben.

Geräte – Vordefinierte Ereignisse:

Ereignis	Beschreibung
Lesezeichenreferenz angefordert	Tritt auf, wenn ein Lesezeichen im Live- oder Wiedergabemodus in den Clients erstellt wird. Außerdem eine Voraussetzung zum Anwenden der standardmäßigen Regel zur Aufzeichnung von Lesezeichen.
Kommunikationsfehler (Gerät)	Tritt auf, wenn die Verbindung zu einem Gerät unterbrochen wurde oder wenn ein Versuch unternommen wird, mit einem Gerät zu kommunizieren und dieser Versuch fehlschlägt.
Kommunikation gestartet (Gerät)	Tritt auf, wenn die Verbindung zu einem Gerät hergestellt wurde.
Kommunikation gestoppt (Gerät)	Tritt auf, wenn die Verbindung zu einem Gerät beendet wurde.

Ereignis	Beschreibung
Beweissicherung geändert	Tritt auf, wenn eine Beweissicherung für Geräte von einem Client-Benutzer oder über das MIP SDK geändert wurde.
Beweissicherung	Tritt auf, wenn eine Beweissicherung für Geräte von einem Client-Benutzer oder über das MIP SDK erstellt wurde.
Beweissicherung aufgehoben	Tritt auf, wenn eine Beweissicherung für Geräte von einem Client-Benutzer oder über das MIP SDK aufgehoben wurde.
Feed-Überlauf gestartet	Feed-Überlauf (Medienüberlauf) tritt auf, wenn ein Aufzeichnungsserver empfangene Daten nicht so schnell verarbeiten kann, wie in der Konfiguration festgelegt wurde, und deswegen einige Aufzeichnungen verwerfen muss. Wenn der Server einwandfrei funktioniert, wird der Feed-Überlauf üblicherweise durch langsame Speicherungen verursacht. Sie können dieses Problem lösen, indem Sie entweder die Menge der zu speichernden Daten verringern oder die Leistung des Speichersystems verbessern. Verringern Sie die Menge der zu speichernden Daten, indem Sie Bildraten, Auflösung oder Bildqualität Ihrer Kameras senken. Dies kann allerdings die Aufzeichnungsqualität senken. Stattdessen können Sie aber auch die Leistung Ihres Speichersystems verbessern, indem Sie zusätzliche Festplatten installieren, um die Belastung zu verringern, oder indem Sie schnellere Festplatten oder Steuerungen installieren. Sie können dieses Ereignis nutzen, um Aktionen auszulösen, durch die Sie das Problem umgehen, um beispielsweise die Aufzeichnungsbildrate zu senken.
Feed-Überlauf gestoppt	Hinzukommt es, wenn ein Feed-Überlauf (siehe Feed-Überlauf gestartet auf Seite 330) endet.
Live-Client-Feed angefordert	Tritt auf, wenn Client-Benutzer einen Live-Stream von einem Gerät anfordern. Das Ereignis tritt bei Anforderung auf, auch wenn die Anforderung des Client-Benutzers später fehlschlägt, weil der Client-Benutzer beispielsweise nicht die erforderliche Berechtigung hat, um den angeforderten Live-Feed anzusehen oder weil der Feed aus irgendeinem Grund beendet wird.
Live Client-Feed beendet	Tritt auf, wenn Client-Benutzer einen Live-Stream von einem Gerät nicht länger anfordern.
Manuelle	Tritt auf, wenn ein Client-Benutzer eine Aufzeichnung für eine Kamera startet.

Ereignis	Beschreibung
Aufzeichnung gestartet	Das Ereignis wird auch dann ausgelöst, wenn das Gerät bereits über Regelaktionen aufnimmt.
Manuelle Aufzeichnung angehalten	Tritt auf, wenn ein Client-Benutzer eine Aufzeichnung für eine Kamera anhält. Wenn das Regelsystem ebenfalls eine Aufzeichnung gestartet hat, nimmt es weiterhin auf, sogar nachdem die manuelle Aufzeichnung angehalten wurde.
Referenz für markierte Daten angefordert	Tritt auf, wenn eine Beweissicherung im Wiedergabemodus über die Clients oder das MIP SDK erstellt wird. Es wird ein Ereignis erstellt, das Sie in Ihren Regeln verwenden können.
Bewegung gestartet	Tritt auf, wenn das System Bewegungen auf Video erkennt, das es von einer Kamera erhält. Für diesen Ereignistyp wird eine aktivierte Bewegungserkennung der Kamera im System benötigt, mit der das Ereignis verknüpft ist. Neben der Bewegungserkennung durch das System können einige Kameras Bewegung selbstständig erkennen und das Ereignis **Bewegung gestartet (HW)** auslösen, doch dies hängt von der Konfiguration der Hardware der Kamera und vom System ab. Siehe auch Hardware – Konfigurierbare Ereignisse: auf Seite 328.
Bewegung gestoppt	Tritt auf, wenn Bewegung im empfangenen Video nicht mehr registriert werden kann. Siehe auch Bewegung gestartet auf Seite 331. Für diesen Ereignistyp wird eine aktivierte Bewegungserkennung der Kamera im System benötigt, mit der das Ereignis verknüpft ist. Neben der Bewegungserkennung durch das System können einige Kameras Bewegung selbstständig erkennen und das Ereignis „Bewegung gestoppt“ (HW) auslösen, doch dies hängt von der Konfiguration der Hardware der Kamera und vom System ab. Siehe auch Hardware – Konfigurierbare Ereignisse: auf Seite 328.
Ausgang aktiviert	Tritt auf, wenn ein externer Ausgangsport eines Geräts aktiviert wird. Für diesen Ereignistyp muss mindestens ein Gerät in Ihrem System Ausgangsports unterstützen.
Ausgang geändert	Tritt auf, wenn der Status eines externen Ausgangsports eines Geräts verändert wird.

Ereignis	Beschreibung
	Für diesen Ereignistyp muss mindestens ein Gerät in Ihrem System Ausgangsports unterstützen.
Ausgang deaktiviert	Tritt auf, wenn ein externer Ausgangsport eines Geräts deaktiviert wird. Für diesen Ereignistyp muss mindestens ein Gerät in Ihrem System Ausgangsports unterstützen.
Manuelle PTZ-Sitzung gestartet	Tritt auf, wenn eine manuell bediente PTZ-Sitzung auf einer Kamera gestartet wird (anders als eine PTZ-Sitzung, die auf planmäßigen Wachrundgängen basiert oder die automatisch durch ein Ereignis ausgelöst wird). Für diesen Ereignistyp müssen die dem Ereignis zugeordneten Kameras PTZ-Kameras sein.
Manuelle PTZ-Sitzung gestoppt	Tritt auf, wenn eine manuell bediente PTZ-Sitzung auf einer Kamera gestoppt wird (anders als eine PTZ-Sitzung, die auf planmäßigen Wachrundgängen basiert oder die automatisch durch ein Ereignis ausgelöst wird). Für diesen Ereignistyp müssen die dem Ereignis zugeordneten Kameras PTZ-Kameras sein.
Aufzeichnung gestartet	Tritt auf, wenn eine Aufzeichnung gestartet wird. Für das manuelle Starten von Aufzeichnungen gibt es ein separates Ereignis.
Aufzeichnung angehalten	Tritt auf, wenn eine Aufzeichnung angehalten wird. Für das manuelle Anhalten von Aufzeichnungen gibt es ein separates Ereignis.
Einstellungen geändert	Tritt auf, wenn die Einstellungen auf einem Gerät geändert wurden.
Fehler beim Ändern der Einstellungen	Tritt auf, wenn ein Versuch unternommen wird, die Einstellungen auf einem Gerät zu ändern und dieser Versuch fehlschlägt.

Externe Ereignisse – Voreingestellte Ereignisse:

Ereignis	Beschreibung
Wiedergabe der Audionachricht anfordern	Aktiviert, wenn das Abspielen von Audio-Nachrichten über das MIP SDK angefordert wird. Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins (z. B. für die Integration mit externen Zutrittskontrollsystemen) für Ihr System entwickeln.
Aufzeichnungsbeginn anfordern	Wird aktiviert, wenn ein Aufzeichnungsstart über das MIP SDK angefordert wird. Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins (z. B. für die Integration mit externen Zutrittskontrollsystemen) für Ihr System entwickeln.
Aufzeichnungsstopp anfordern	Wird aktiviert, wenn ein Aufzeichnungsstopp über das MIP SDK angefordert wird. Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins (z. B. für die Integration mit externen Zutrittskontrollsystemen) für Ihr System entwickeln.

Externe Ereignisse – Generische Ereignisse:

Generische Ereignisse ermöglichen es Ihnen, Aktionen im System auszulösen, indem einfache Zeichenketten über das IP-Netzwerk an das Videoverwaltungssystem gesendet werden. Der Zweck generischer Ereignisse besteht darin, so vielen externen Quellen wie möglich zu ermöglichen, mit dem System zu interagieren.

Externe Ereignisse – Benutzerdefinierte Ereignisse:

Auch eine Anzahl an Ereignissen, die genau auf Ihr System zugeschnitten sind, könnte zur Auswahl stehen. Sie können benutzerdefinierte Ereignisse für Folgendes verwenden:

- Sie können Client-Benutzern ermöglichen, manuell Ereignisse auszulösen, während sie Live-Video in den Clients ansehen
- Zahllose andere Anwendungsmöglichkeiten. Sie können beispielsweise benutzerdefinierte Ereignisse erstellen, die auftreten, wenn ein bestimmter Datentyp von einem Gerät empfangen wird

  Siehe auch Benutzerdefinierte Ereignisse (Erklärung) auf Seite 360

Aufzeichnungsserver:

Ereignis	Beschreibung
Archiv verfügbar	Hierzu kommt es, wenn ein Archiv für einen Aufzeichnungsserver wieder zur Verfügung steht, nachdem es zuvor nicht zur Verfügung stand. Siehe auch Archiv ist nicht verfügbar auf Seite 334.
Archiv ist nicht verfügbar	Tritt auf, wenn ein Archiv für einen Aufzeichnungsserver nicht mehr verfügbar ist, beispielsweise durch die Unterbrechung der Verbindung zu einem Archiv im Netzlaufwerk. In solchen Fällen können Sie keine Aufzeichnungen archivieren. Sie können das Ereignis verwenden, um beispielsweise einen Alarm oder ein Benachrichtigungsprofil auszulösen, damit eine E-Mailbenachrichtigung automatisch an das zuständige Personal in Ihrem Unternehmen gesendet wird.
Archivierung nicht abgeschlossen	Tritt ein, wenn ein Archiv für einen Aufzeichnungsserver den letzten Archivierungsgang noch nicht abgeschlossen hat, wenn der Start des nächsten Vorgangs geplant ist.
Datenbank - Löschen von Aufzeichnungen vor Erreichen der festgelegten Speichergröße	Tritt ein, wenn das Speicherzeitlimit vor dem Datenbankgrößenlimit erreicht ist.
Datenbank - Löschen von Aufzeichnungen vor Erreichen der festgelegten Speicherzeit	Tritt ein, wenn das Datenbankgrößenlimit vor dem Speicherzeitlimit erreicht ist.
Datenbankfestplatte ist voll – automatische Archivierung	Tritt ein, wenn eine Datenbankfestplatte voll ist. Eine Datenbankfestplatte wird als voll vermerkt, wenn nur noch weniger als 5 GB Speicherplatz auf der Festplatte vorhanden sind: Wenn weniger als 5 GB Speicherplatz frei sind, werden immer die ältesten Daten in einer Datenbank automatisch archiviert (oder gelöscht, wenn kein nächstes Archiv festgelegt ist).

Ereignis	Beschreibung
Datenbankfestplatte ist voll - Löschen	Tritt ein, wenn eine Datenbankfestplatte voll ist und weniger als 1 GB Speicherplatz frei ist. Daten werden gelöscht, auch wenn ein nächstes Archiv definiert ist. Eine Datenbank erfordert 250 MB an freiem Speicherplatz. Ist dieser Grenzwert erreicht (wenn Daten nicht schnell genug gelöscht werden), werden erst dann wieder Daten in die Datenbank geschrieben, wenn genügend Speicherplatz freigegeben wurde. Die tatsächliche Maximalgröße Ihrer Datenbank entspricht der Anzahl der angegebenen Gigabyte minus 5 GB.
Datenbank ist voll - automatische Archivierung	Tritt ein, wenn ein Archiv für einen Aufzeichnungsserver voll ist und automatisch in ein Archiv im Speicher archivieren muss.
Datenbankreparatur	Tritt ein, wenn eine Datenbank beschädigt ist. In diesem Fall versucht das System automatisch, zwei Reparaturmethoden für die Datenbank durchzuführen: eine schnelle Reparatur und eine umfassende Reparatur.
Datenbankspeicher verfügbar	Hierzu kommt es, wenn ein Speichergerät für einen Aufzeichnungsserver wieder zur Verfügung steht, nachdem es zuvor nicht zur Verfügung stand. Siehe auch Datenbankspeicher nicht verfügbar auf Seite 335. Sie können das Ereignis z. B. verwenden, um die Aufzeichnung zu starten, wenn sie durch das Ereignis **Datenbankspeicher nicht verfügbar** angehalten wurde.
Datenbankspeicher nicht verfügbar	Tritt ein, wenn ein Speicher für einen Aufzeichnungsserver nicht mehr verfügbar ist, z. B. durch die Unterbrechung der Verbindung zu einem Speicher im Netzwerklaufwerk. In solchen Fällen können Sie keine Aufzeichnungen archivieren. Sie können das Ereignis z. B. verwenden, um die Aufzeichnung anzuhalten sowie einen Alarm oder ein Benachrichtigungsprofil auszulösen, damit eine E-Mailbenachrichtigung automatisch an das zuständige Personal in Ihrem Unternehmen gesendet wird.
Fehler bei der verschlüsselten Failover-Kommunikation	Hierzu kommt es bei einem SSL-Kommunikationsfehler zwischen dem Failover-Server und überwachten Aufzeichnungsservern.
Failover gestartet	Tritt ein, wenn ein Failover-Aufzeichnungsserver die Aufgabe eines Aufzeichnungsservers übernimmt. Siehe auch Failover-Aufzeichnungsserver

Ereignis	Beschreibung
	(Erklärung) auf Seite 184.
Failover angehalten	Tritt ein, wenn ein Aufzeichnungsserver wieder verfügbar ist und wieder die Aufgabe eines Failover-Aufzeichnungsservers übernehmen kann.

Systemmonitor-Ereignisse

Systemmonitorereignisse werden ausgelöst, wenn Schwellenwerte überschritten werden, die in dem Knoten **Systemmonitorschwellenwerte** konfiguriert wurden. Siehe auch Schwellenwerte des Systemmonitors (Erklärung) auf Seite 429.

Diese Funktion erfordert, dass der Data Collector-Dienst ausgeführt wird.

Systemmonitor - Server:

Ereignis	Beschreibung
CPU-Auslastung - kritisch	Tritt in, wenn die CPU-Auslastung den kritischen CPU-Schwellenwert überschreitet.
CPU-Auslastung - normal	Tritt in, wenn die CPU-Auslastung den Schwellenwert der Warn-CPU unterschreitet.
CPU-Auslastung - Warnung	Tritt ein, wenn die CPU-Auslastung den Schwellenwert der Warn-CPU überschreitet oder unter den kritischen CPU-Schwellenwert fällt.
Rechenkapazitätauslastung - kritisch	Tritt ein, wenn die Rechenkapazitätauslastung den kritischen Speicherschwellenwert überschreitet.
Rechenkapazitätauslastung - normal	Tritt ein, wenn die Rechenkapazitätauslastung unter den Schwellenwert für den Warnspeicher zurückfällt.
Rechenkapazitätauslastung	Tritt ein, wenn die Rechenkapazitätauslastung den Schwellenwert

Ereignis	Beschreibung
- Warnung	für Warnspeicher überschreitet oder unter den Schwellenwert für die kritische Rechenkapazitätauslastung zurückfällt.
NVIDIA Dekodierung kritisch	Tritt ein, wenn die NVIDIA Dekodierung die kritische NVIDIA-Decodierungsschwelle überschreitet.
NVIDIA Dekodierung normal	Tritt ein, wenn die NVIDIA-Dekodierungsauslastung unter den Warn-NVIDIA-Dekodierungsschwellenwert fällt.
NVIDIA Dekodierung Warnung	Tritt ein, wenn die NVIDIA-Decodierungsverwendung den Warn-NVIDIA-Decodierschwellenwert überschreitet oder unter den kritischen NVIDIA-Decodierschwellenwert fällt.
NVIDIA Speicherplatz kritisch	Tritt ein, wenn die NVIDIA-Speicherbelegung den kritischen NVIDIA-Speichergrenzwert überschreitet.
NVIDIA Speicherplatz normal	Tritt auf, wenn die NVIDIA-Speicherbelegung unter den NVIDIA-Warnschwellenwert für Warnungen zurückfällt.
NVIDIA Speicherplatz Warnung	Tritt auf, wenn die NVIDIA-Speicherauslastung den Warngrenzwert für NVIDIA-Speicher überschreitet oder unter den kritischen NVIDIA-Speicherschwellenwert fällt.
NVIDIA Übertragung kritisch	Tritt ein, wenn die NVIDIA-Übertragungsnutzung den kritischen NVIDIA-Übertragungs-Schwellenwert überschreitet.
NVIDIA Übertragung normal	Tritt ein, wenn die NVIDIA-Übertragungsnutzung unter den Warn-NVIDIA-Übertragungs-Schwellenwert fällt.
NVIDIA Übertragung Warnung	Tritt ein, wenn die NVIDIA-Übertragungsnutzung den Warn-NVIDIA-Übertragungs-Schwellenwert überschreitet oder unter den kritischen NVIDIA-Übertragungs-Schwellenwert fällt.
Dienstverfügbarkeit - kritisch	Tritt ein, wenn ein Serverdienst nicht mehr ausgeführt wird. Für dieses Ereignis gibt es keine Schwellenwerte.
Dienstverfügbarkeit - normal	Tritt ein, wenn sich der Status eines Serverdiensts in ausführen ändert. Für dieses Ereignis gibt es keine Schwellenwerte.

Systemmonitor - Kamera:

Ereignis	Beschreibung
Live-FPS- kritisch	Tritt ein, wenn die Live-FPS-Rate unter den kritischen Live-FPS-Schwellenwert fällt.
Live-FPS- normal	Tritt ein, wenn die Live-FPS-Rate den Warngrenzwert für Live-FPS überschreitet.
Live-FPS - Warnung	Tritt ein, wenn die Live-FPS-Rate unter den Warnungs-FPS-Schwellenwert fällt oder den kritischen Live-FPS-Schwellenwert überschreitet.
Aufzeichnender FPS - kritisch	Tritt ein, wenn die Aufzeichnungs-FPS-Rate unter den kritischen FPS-Schwellenwert für die Aufzeichnung fällt.
Aufzeichnender FPS - normal	Tritt ein, wenn die Aufzeichnungs-FPS-Rate den Schwellenwert für die Warnaufzeichnung überschreitet.
Aufzeichnender FPS - Warnung	Tritt ein, wenn die Aufzeichnungs-FPS-Rate unter den FPS-Schwellenwert für die Warnaufnahme fällt oder den Schwellenwert für die kritische Aufnahme-FPS überschreitet.
Verwendeter Speicherplatz - kritisch	Tritt ein, wenn der Speicherplatz für Aufnahmen einer bestimmten Kamera den kritischen Schwellenwert für den verwendeten Speicherplatz überschreitet.
Verwendeter Speicherplatz - normal	Tritt ein, wenn der Speicherplatz für Aufnahmen einer bestimmten Kamera unter den Schwellenwert für den Schwellenwert für Warnmeldungen zurückfällt.
Verwendeter Speicherplatz - Warnung	Tritt ein, wenn der für Aufnahmen einer bestimmten Kamera verwendete Speicher den Schwellenwert für den Schwellenwert für Warnmeldungen überschreitet oder unter den kritischen Schwellenwert für den verwendeten Speicherplatz zurückfällt.

Systemmonitor - Festplatte:

Ereignis	Beschreibung
Freier Speicherplatz - kritisch	Tritt ein, wenn die Speicherplatzbelegung den kritischen Schwellenwert für den freien Speicherplatz überschreitet.
Freier Speicherplatz - normal	Tritt ein, wenn die Speicherplatzbelegung unter den Schwellenwert für die Warnung über freien Speicherplatz fällt.
Freier Speicherplatz - Warnung	Tritt ein, wenn die Speicherplatzbelegung den Schwellenwert für den Schwellenwert für Warnspeicher überschreitet oder unter den Schwellenwert für kritischen freien Speicherplatz zurückfällt.

Systemmonitor - Speicher:

Ereignis	Beschreibung
Speicherzeit - kritisch	Tritt ein, wenn das System vorhersagt, dass der Speicher schneller gefüllt wird als der Schwellenwert für die kritische Speicherzeit. Wenn beispielsweise Daten aus Videostreams den Speicher schneller füllen als erwartet.
Speicherzeit - normal	Tritt ein, wenn das System vorhersagt, dass der Speicher langsamer gefüllt wird als der Schwellenwert für die Warnungs-Speicherzeit. Zum Beispiel, wenn Daten aus Videostreams den Speicher mit der erwarteten Rate füllen.
Speicherzeit - Warnung	Tritt ein, wenn das System vorhersagt, dass der Speicher schneller gefüllt wird als der Schwellenwert für die Warnungs-Speicherzeit oder langsamer als der Schwellenwert für die kritische Speicherzeit. Wenn zum Beispiel Daten von Videostreams den Speicher schneller füllen als erwartet, weil mehr Bewegung von den Kameras erfasst wird, die für die Aufzeichnung von Bewegungen konfiguriert sind.

Andere:

Ereignis	Beschreibung
Automatische Lizenzaktivierung ist fehlgeschlagen	Tritt ein, wenn automatische Lizenzaktivierung fehlschlägt. Es gibt keine Schwellenwerte für dieses Ereignis.
Planmäßige Passwortänderung gestartet	Hierzu kommt es, wenn eine planmäßige Passwortänderung gestartet wird.
Planmäßige Passwortänderung erfolgreich abgeschlossen	Hierzu kommt es, wenn eine planmäßige Passwortänderung ohne Fehler abgeschlossen wird.
Planmäßige Passwortänderung abgeschlossen, jedoch mit Fehlern	Hierzu kommt es, wenn eine planmäßige Passwortänderung mit Fehlern abgeschlossen wird.

Ereignisse von Zusatzprodukten und -integrationen:

Ereignisse von Zusatzprodukten und -integrationen können im Regelsystem verwendet werden, zum Beispiel:

- Analyseereignisse können auch im Regelsystem verwendet werden

Regeln

Regeln (Erklärung)

Regeln bestimmen Aktionen, die unter bestimmten Bedingungen ausgeführt werden. Beispiel: Wenn eine Bewegung erkannt wird (Bedingung), startet eine Kamera die Aufzeichnung (Aktion).

Nachfolgend sind **Beispiele** für Anwendungen der Regeln aufgelistet:

- Starten und Anhalten der Aufzeichnung
- Nicht-standardmäßige Livebildrate einstellen
- Nicht-standardmäßige Aufzeichnungsbildrate einstellen
- Starten und Beenden des PTZ-Wachrundgangs
- Pausieren und Wiederaufnahme des PTZ-Wachrundgangs
- Bewegung der PTZ-Kameras zu bestimmten Positionen
- Status des Ausgangs als aktiviert/deaktiviert einstellen
- Senden von Benachrichtigungen per E-Mail

- Erstellen von Protokolleinträgen
- Ereignisse erstellen
- Übernehmen von neuen Geräteeinstellungen, beispielsweise eine andere Auflösung einer Kamera
- Videos in Matrix-Empfängern erscheinen lassen
- Starten und Anhalten von Plug-ins
- Starten und Beenden von Geräte-Feeds

Das Anhalten eines Geräts bedeutet, dass das Videosignal nicht mehr vom Gerät auf das System übertragen wird, wodurch Sie keine Videos live sehen und aufnehmen können. Im Gegensatz dazu kann ein Gerät, für das Sie den Feed angehalten haben, jedoch weiterhin mit dem Aufzeichnungsserver kommunizieren und Sie können den Feed vom Gerät über eine Regel automatisch starten – anders als wenn das Gerät manuell im Management Client deaktiviert wurde.

Für einige Regeln kann es erforderlich sein, dass bestimmte Funktionen für die entsprechenden Geräte aktiviert sind. Beispiel: Eine Regel, die bestimmt, dass eine Kamera aufzeichnet, funktioniert nicht wie beabsichtigt, wenn die Aufzeichnung für die entsprechende Kamera nicht aktiviert ist. Vor dem Erstellen einer Regel empfiehlt Milestone, dass Sie überprüfen, ob die entsprechenden Geräte die beabsichtigte Aktion durchführen können.

Standardregeln (Erklärung)

Ihr System umfasst eine Reihe von Standardregeln, die Sie für Grundfunktionen verwenden können, ohne selbst etwas einrichten zu müssen. Sie können die Standardregeln nach Bedarf deaktivieren oder bearbeiten. Wenn Sie die Standardregeln bearbeiten oder deaktivieren, funktioniert das System möglicherweise nicht wie gewünscht und es ist nicht sichergestellt, dass Video- oder Audiofeeds automatisch ins System übertragen werden.

Standardregel	Beschreibung
Zu Voreinstellung gehen, wenn PTZ ausgeführt wurde	Stellt sicher, dass PTZ-Kameras in ihre jeweiligen standardmäßigen Preset Positionen gehen, nachdem Sie diese manuell betätigt haben. Diese Regel ist standardmäßig nicht aktiviert. Auch, wenn Sie die Regel aktiviert haben, müssen Sie standardmäßigen Preset-Positionen für die relevanten PTZ-Kameras definiert haben, damit die Regel funktioniert. Gehen Sie

Standardregel	Beschreibung
	dazu zur Registerkarte **Voreinstellungen**.
Audio auf Anfrage abspielen	Stellt sicher, dass Videos automatisch aufgezeichnet werden, wenn eine externe Anforderung eingeht. Die Anforderung wird immer von einem System ausgelöst, das extern mit Ihrem System integriert wird, und die Regel wird in erster Linie von Integratoren externer Systeme oder Plug-ins verwendet.
Aufzeichnung für Lesezeichen	Sorgt dafür, dass automatisch ein Video aufgezeichnet wird, wenn ein Anwender ein Lesezeichen im XProtect Smart Client festlegt. Voraussetzung ist, dass die Aufzeichnung für die entsprechenden Kameras aktiviert wurde. Aufzeichnung ist standardmäßig aktiviert. Die Standardaufzeichnungszeit für diese Regel ist: drei Sekunden, bevor das Lesezeichen gesetzt ist, und 30 Sekunden, nachdem das Lesezeichen gesetzt ist. Sie können die Standardaufzeichnungszeiten in der Regel bearbeiten. Der Voralarm-Puffer, den Sie auf der Registerkarte „Aufzeichnung“ festlegen, muss gleich lang wie oder länger als die Voralarmaufzeichnungszeit sein.
Bei Bewegung aufzeichnen	Stellt sicher, dass das Video aufgezeichnet wird, solange im Videobild von Kameras Bewegung erkannt wird (vorausgesetzt, Aufzeichnung ist für die relevanten Kameras aktiviert). Aufzeichnung ist standardmäßig aktiviert. Die Standardregel legt zwar Aufzeichnungen basierend auf erkannter Bewegung fest, stellt aber nicht sicher, dass das System tatsächlich Video aufzeichnet, da Sie Aufzeichnung bei einer oder mehreren Kameras deaktiviert haben könnten. Auch bei aktivierter Aufzeichnung kann die Qualität der Aufzeichnungen durch die jeweiligen Aufzeichnungseinstellungen der einzelnen Kameras beeinflusst werden.
Aufzeichnung nach Bedarf	Stellt sicher, dass Videos automatisch aufgezeichnet werden, wenn eine externe Anforderung eingeht (vorausgesetzt,

Standardregel	Beschreibung
	Aufzeichnung ist für die relevanten Kameras aktiviert). Aufzeichnung ist standardmäßig aktiviert. Die Anforderung wird immer von einem System ausgelöst, das extern mit Ihrem System integriert wird, und die Regel wird in erster Linie von Integratoren externer Systeme oder Plug-ins verwendet.
Start des Audiofeeds	Sorgt dafür, dass Audiofeeds aller angeschlossenen Mikrofone und Lautsprecher automatisch an das System übertragen werden. Die Standardregel ermöglicht zwar sofort nach der Systeminstallation Zugriff auf die Audiofeeds angeschlossener Mikrofone und Lautsprecher, stellt aber nicht sicher, dass Audio tatsächlich aufgezeichnet wird, da Sie die Aufzeichnungseinstellungen separat festlegen müssen.
Start des Feeds	Bewirkt, dass Videofeeds aller angeschlossenen Kameras automatisch an das System übertragen werden. Die Standardregel ermöglicht zwar sofort nach der Systeminstallation Zugriff auf die Videofeeds angeschlossener Kameras, stellt aber nicht sicher, dass Video tatsächlich aufgezeichnet wird, da Sie die Aufzeichnungseinstellungen der Kameras separat festlegen müssen.
Start des Metadatenfeeds	Bewirkt, dass Datenfeeds aller angeschlossenen Kameras automatisch an das System übertragen werden. Die Standardregel ermöglicht zwar sofort nach der Systeminstallation Zugriff auf die Datenfeeds angeschlossener Kameras, stellt aber nicht sicher, dass Daten tatsächlich aufgezeichnet werden, da Sie die Aufzeichnungseinstellungen der Kameras separat festlegen müssen.
Anzeigen der Zutrittsanforderungsbenachrichtigung	Bewirkt, dass alle Zutrittskontrollereignisse, die als „Zutrittsanforderung“ kategorisiert sind, die Anzeige eine Zutrittsanforderungsbenachrichtigung in XProtect Smart Client auslösen (sofern die Benachrichtigungsfunktion nicht im Smart Client-Profil deaktiviert ist).

Wiederherstellung von Standardregeln

Wenn Sie versehentlich eine der Standardregeln löschen, können Sie sie durch Eingabe folgender Daten wiederherstellen:

Standardregel	Einzugebender Text
Zu Voreinstellung gehen, wenn PTZ ausgeführt wurde	Aktion für „Manuelle PTZ-Sitzung gestoppt“ von „Alle Kameras“ durchführen Sofort zur Standardvoreinstellung auf dem Gerät wechseln, auf dem das Ereignis aufgetreten ist
Audio auf Anfrage abspielen	Aktion für „Wiedergabe der Audionachricht von extern anfordern“ durchführen Audionachricht von Metadaten auf den Geräten für Metadaten mit Priorität 1 wiedergeben
Aufzeichnung für Lesezeichen	Aktion für „Lesezeichenreferenz von allen Kameras, allen Mikrofonen, allen Lautsprechern angefordert“ durchführen, Aufzeichnung drei Sekunden vorher auf dem Gerät starten, auf dem das Ereignis aufgetreten ist Aktion 30 Sekunden nachher durchführen, Aufzeichnung sofort anhalten
Bei Bewegung aufzeichnen	Aktion für „Bewegung von allen Kameras gestartet“ durchführen, Aufzeichnung drei Sekunden vorher auf dem Gerät starten, auf dem das Ereignis aufgetreten ist Anhalteaktion für „Bewegung gestoppt von allen Kameras“ durchführen, Aufzeichnung drei Sekunden danach anhalten
Aufzeichnung nach Bedarf	Aktion für „Starten der Aufzeichnung von extern anfordern“ durchführen, Aufzeichnung auf den Geräten von Metadaten sofort starten Stopp-Aktion für „Stoppen der Aufzeichnung von extern anfordern“ durchführen, Aufzeichnung sofort anhalten
Start des Audiofeeds	Aktion in einem Zeitintervall durchführen, Feed immer bei allen Mikrofonen, allen Lautsprechern starten

Standardregel	Einzugebender Text
	Aktion durchführen, wenn Zeitintervall endet, Feed sofort stoppen
Start des Feeds	Aktion in einem Zeitintervall durchführen, Feed immer bei allen Kameras starten Aktion durchführen, wenn Zeitintervall endet, Feed sofort stoppen
Start des Metadatenfeeds	Aktion in einem Zeitintervall durchführen, Feed immer bei allen Metadaten starten Aktion durchführen, wenn Zeitintervall endet, Feed sofort stoppen
Anzeigen der Zutrittsanforderungsbenachrichtigung	Aktion für Zutrittsanforderung (Zutrittskontroll-Kategorien) von Systemen [+ Geräten] durchführen Integrierte Zugriffsanforderungsbenachrichtigung anzeigen

Regelkomplexität (Erklärung)

Die genaue Anzahl der Optionen hängt vom Typ der Regel ab, die Sie erstellen möchten, und von der Anzahl der Geräte, die auf Ihrem System verfügbar sind. Regeln ermöglichen ein hohes Maß an Flexibilität: Sie können Ereignis- und Zeitbedingungen kombinieren, mehrere Aktionen in einer einzigen Regel bestimmen und häufig Regeln erstellen, die mehrere oder alle Geräte auf Ihrem System abdecken.

Sie können Ihre Regeln so einfach oder komplex wie erforderlich gestalten. Sie können zum Beispiel sehr einfache zeitbasierte Regeln erstellen:

Beispiel	Erläuterung
Sehr einfache zeitbasierte Regel	Montags zwischen 08:30 Uhr und 11:30 Uhr (Zeitbedingung) beginnen Kamera 1 und Kamera 2 die Aufzeichnung (Aktion), wenn der Zeitraum beginnt und beenden die Aufzeichnung (Aktion anhalten), wenn der Zeitraum endet.

Beispiel	Erläuterung
Sehr einfache ereignisbasierte Regel	Wenn Bewegung auf Kamera 1 erkannt wird (Ereignisbedingung), beginnt Kamera 1 sofort die Aufzeichnung (Aktion) und beendet die Aufzeichnung dann nach 10 Sekunden (Aktion beenden). Auch wenn eine ereignisbasierte Regel durch ein Ereignis auf einem Gerät aktiviert wird, können Sie bestimmen, dass Aktionen auf einem oder mehreren anderen Geräten erfolgen sollen.
Regel mit mehreren Geräten	Wenn Bewegung auf Kamera 1 erkannt wird (Ereignisbedingung), beginnt Kamera 2 sofort die Aufzeichnung (Aktion) und die Sirene, die mit Ausgang 3 verbunden ist, wird sofort aktiviert (Aktion). Nach 60 Sekunden soll Kamera 2 dann die Aufnahme anhalten (Aktion beenden) und die Sirene, die mit Ausgang 3 verbunden ist, wird deaktiviert (Aktion beenden).
Regel, die Zeit, Ereignisse und Geräte kombiniert	Wenn Bewegung auf Kamera 1 erkannt wird (Ereignisbedingung) und der Wochentag ein Samstag oder Sonntag ist (Zeitbedingung), beginnen Kamera 1 und Kamera 2 sofort die Aufzeichnung (Aktion) und es wird eine Benachrichtigung an die Sicherheitsleitung gesendet (Aktion). 5 Sekunden später, wenn keine Bewegung mehr auf Kamera 1 oder Kamera 2 erkannt wird, halten die beiden Kameras die Aufzeichnung an (Aktion beenden).

Den Anforderungen und Bedürfnissen Ihres Unternehmens entsprechend, ist es in vielen Fällen besser viele einfache Regeln zu erstellen als einige wenige komplexe Regeln. Auch wenn dies bedeutet, dass Sie mehr Regeln in Ihrem System haben, können Sie dadurch auf einfache Weise einen Überblick über die Auswirkungen Ihrer Regeln behalten. Wenn Sie Ihre Regeln einfach halten, haben Sie auch eine größere Flexibilität beim Deaktivieren/Aktivieren von einzelnen Regelbestandteilen. Mit einfachen Regeln können Sie bei Bedarf gesamte Regeln deaktivieren/aktivieren.

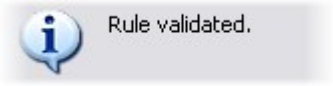
Validierung von Regeln (Erklärung)

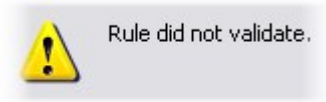
Sie können den Inhalt einer einzelnen Regel oder aller Regeln auf einmal validieren. Bei der Erstellung einer Regel stellt der **Regel verwalten**-Assistent sicher, dass alle Bestandteile der Regel Sinn ergeben. Wenn eine Regel einige Zeit lang bestanden hat, können ein oder mehrere Bestandteile der Regel durch eine andere Konfiguration beeinträchtigt worden sein, wodurch die Regel nicht mehr funktionieren könnte. Wenn beispielsweise eine Regel durch ein bestimmtes Zeitprofil ausgelöst wird, funktioniert die Regel nicht, wenn Sie das Zeitprofil gelöscht haben oder, wenn Sie keine Rechte mehr darauf haben. Es kann schwierig sein, den Überblick über solche unbeabsichtigten Konfigurationsauswirkungen zu behalten.

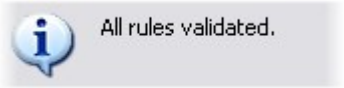
Die Regelvalidierung hilft Ihnen dabei, nachzuvollziehen, welche Regeln beeinträchtigt wurden. Die Validierung erfolgt pro Regel und jede Regel wird für sich genommen validiert. Sie können Regeln nicht untereinander validieren, zum Beispiel um herauszufinden, ob eine Regel im Konflikt zu einer anderen Regel steht, auch nicht mit der Funktion **Alle Regeln validieren**.

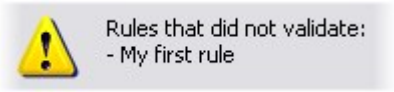
> Sie können nicht validieren, ob die Konfiguration von Anforderungen außerhalb der Regel verhindert, dass die Regel funktioniert. Beispiel: Eine Regel, die bestimmt, dass die Aufzeichnung starten soll, wenn eine Bewegung von einer bestimmten Kamera erkannt wird, wird validiert, wenn die Bestandteile in der Regel selbst korrekt sind, auch wenn die Bewegungserkennung, die auf der Kameraebene aktiviert wird, nicht für die entsprechende Kamera aktiviert wurde.

Sie validieren eine einzelne Regel oder alle Regeln auf einmal mit einem Rechtsklick auf die Regel, die Sie validieren möchten und durch Auswahl von **Regel validieren** oder **Alle Regeln validieren**. Ein Dialogfeld informiert Sie darüber, ob die Regel(n) erfolgreich validiert wurde(n) oder nicht. Wenn Sie sich dafür entschieden haben, mehr als eine Regel zu validieren, und eine oder mehrere Regeln nicht erfolgreich waren, so werden in der Dialogbox die Namen der betreffenden Regeln aufgeführt.







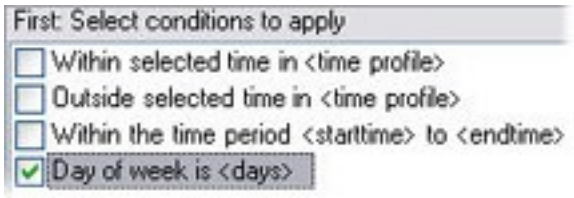


Hinzufügen einer Regel

Beim Erstellen von Regeln werden Sie vom Assistenten **Regel verwalten** begleitet, der nur relevante Optionen auflistet.

Er stellt sicher, dass einer Regel keine Bestandteile fehlen. Je nach Regelinhalt empfiehlt er automatisch passende Stopp-Aktionen, d. h. was geschehen soll, wenn die Regel nicht mehr gilt. Dadurch wird sichergestellt, dass Sie nicht unbeabsichtigt eine endlose Regel erstellen.

1. Klicken Sie mit der rechten Maustaste auf das Objekt in **Regeln** > **Regel** hinzufügen. Dadurch öffnet sich der Assistent **Regel verwalten**. Der Assistent begleitet Sie beim Bestimmen des Inhalts Ihrer Regel.
2. Bestimmen Sie einen Namen und eine Beschreibung für die neue Regel in den Feldern **Name** und **Beschreibung**.
3. Wählen Sie den passenden Bedingungstyp für die Regel: entweder eine Regel, die eine oder mehrere Aktionen durchführt, wenn ein bestimmtes Ereignis eintritt, oder eine Regel, die eine oder mehrere Aktionen durchführt, wenn Sie einen bestimmten Zeitraum eingeben.
4. Klicken Sie auf **Weiter**, um mit dem zweiten Schritt des Assistenten fortzufahren. Definieren Sie im zweiten Schritt des Assistenten weitere Bedingungen für die Regel.
5. Wählen Sie eine oder mehrere Bedingungen aus, zum Beispiel **Der Wochentag ist <Tag>**:

   Bearbeiten Sie die Beschreibung der Regel entsprechend Ihrer Auswahl im unteren Teil des Assistenten-Fensters:

   Klicken Sie auf die unterstrichenen Elemente in **fetter Kursivschrift**, um ihren genauen Inhalt zu bestimmen. Wenn Sie zum Beispiel auf den Link **Tage** in unserem Beispiel klicken, können Sie einen oder mehrere Wochentage auswählen, an denen die Regel gelten soll.
6. Wenn Sie Ihre Bedingungen festgelegt haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt des Assistenten fortzufahren und auszuwählen, welche Aktionen die Regel abdecken soll. Dem Inhalt und der Komplexität Ihrer Regel entsprechend müssen Sie unter Umständen weitere Schritte festlegen, wie beispielsweise Stopp-Ereignisse und Stopp-Aktionen. Wenn eine Regel zum Beispiel vorsieht, dass ein Gerät eine bestimmte Aktion während eines bestimmten Zeitintervalls (zum Beispiel Donnerstag zwischen 08:00 und 10:30 Uhr) durchführt, könnte Sie der Assistent darum bitten, festzulegen, was nach Ablauf dieses Zeitintervalls geschehen soll.
7. Ihre Regel ist standardmäßig nach der Erstellung aktiv, wenn ihre Bedingungen erfüllt sind. Wenn Sie nicht wollen, dass die Regel sofort aktiv ist, entfernen Sie das Häkchen bei **Aktiv**.
8. Klicken Sie auf **Fertigstellen**.

Bearbeiten, Kopieren und Umbenennen einer Regel

1. Klicken Sie im Bereich **Übersicht** mit der rechten Maustaste auf die entsprechende Regel.
2. Wählen Sie entweder:

   Regel bearbeiten oder **Regel kopieren** oder **Regel umbenennen**. Der Assistent **Regel verwalten** wird geöffnet.
3. Im Assistenten die Regel umbenennen und/oder ändern. Wenn Sie **Regel kopieren** ausgewählt haben, wird der Assistent geöffnet und zeigt eine Kopie der ausgewählten Regel an.
4. Klicken Sie auf **Fertigstellen**.

Deaktivieren und Aktivieren einer Regel

Ihr System wendet eine Regel an, sobald die Bedingungen der Regel erfüllt sind. Die Regel ist somit aktiv. Wenn Sie nicht möchten, dass eine Regel aktiv ist, können Sie die Regel deaktivieren. Wenn Sie die Regel deaktivieren, wendet das System die Regel nicht an; nicht einmal, wenn die Bedingungen der Regel erfüllt sind. Sie können eine deaktivierte Regel später einfach wieder aktivieren.

Deaktivieren einer Regel

1. Wählen Sie im Bereich **Übersicht** die Regel aus.
2. Entfernen Sie im Bereich **Eigenschaften** das Häkchen bei **Aktiv**.
3. Klicken Sie in der Symbolleiste auf **Speichern**.
4. Ein Symbol mit einem roten „x“ bedeutet, dass die Regel in der Liste **Regeln** deaktiviert ist:

Aktivieren einer Regel

Wenn Sie die Regel wieder aktivieren wollen, wählen Sie die Regel aus, setzen Sie ein Häkchen bei **Aktivieren** und speichern Sie die Einstellung.

Wiederholte Zeit

Wenn Sie eine Aktion einrichten, die nach einem detaillierten, sich wiederholenden Zeitplan ausgeführt werden soll.

Beispielsweise:

- Jede Woche Dienstags, alle 1 Stunde(n) zwischen 15:00 und 15:30
- Am 15. alle 3 Monat(e) um 11:45 Uhr
- Jeden Tag alle 1 Stunde(n) zwischen 15:00 und 19:00 Uhr

Die Zeit basiert auf den örtlichen Zeiteinstellungen des Servers, auf dem Management Client installiert ist.

Sie können optional ein Zeitprofil auswählen, um sicherzustellen, dass die Regel nur innerhalb bzw. außerhalb des Intervalls dieses Zeitprofils ausgeführt wird.

Allgemeine Anweisungen dazu, wie eine neue Regel eingerichtet wird, finden Sie unter Hinzufügen einer Regel auf Seite 347.

Informationen zu Zeitprofilen finden Sie unter Zeitprofile auf Seite 350.

Zeitprofile

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

Zeitprofile sind vom Administrator definierte Zeiträume. Sie können Zeitprofile beim Erstellen von Regeln verwenden, z. B. eine Regel, die festlegt, dass in einem bestimmten Zeitraum eine bestimmte Aktion ausgeführt werden soll.

Zeitprofile sind zusammen mit Smart Client-Profilen auch Rollen zugeteilt. Standardmäßig sind alle Rollen dem Standardzeitprofil **Immer** zugeteilt. Das bedeutet, dass Mitglieder von Rollen mit diesem Standardzeitprofil keine zeitbasierten Einschränkungen ihrer Benutzerrechte im System haben. Sie können einer Rolle auch ein alternatives Zeitprofil zuteilen.

Zeitprofile sind äußerst flexibel: Sie können sie auf Basis eines oder mehrerer einzelner Zeiträume oder eines oder mehrerer wiederkehrender Zeiträume oder einer Kombination einzelner und wiederkehrender Zeiträume festlegen. Viele Benutzer sind evtl. mit den Konzepten einzelner und wiederkehrender Zeiträume aus Kalenderanwendungen vertraut, wie z.B. der in Microsoft® Outlook.

Zeitprofile gelten immer für die Ortszeit. Das bedeutet, dass wenn sich Ihre Aufzeichnungsserver in verschiedenen Zeitzonen befinden, alle Aktionen (zum Beispiel Kameraaufzeichnungen) hinsichtlich der Zeitprofile zur Ortszeit des jeweiligen Aufzeichnungsservers ausgeführt werden. Beispiel: Wenn Sie ein Zeitprofil haben, das den Zeitraum zwischen 08:30 und 09:30 Uhr abdeckt, werden alle damit verbundenen Aktionen auf einem Aufzeichnungsserver in New York zur Ortszeit zwischen 08:30 bis 09:30 Uhr ausgeführt. Die gleichen Aktionen werden auf einem Aufzeichnungsserver in Los Angeles erst einige Stunden später ausgeführt, nämlich zur dortigen Ortszeit zwischen 08:30 bis 09:30 Uhr.

Sie können Zeitprofile durch Erweitern von **Regeln und Ereignisse** > **Zeitprofile** erstellen und verwalten. Die Liste **Zeitprofile** wird geöffnet. Nur ein Beispiel:

Eine Alternative zu den Zeitprofilen finden Sie unter Zeitprofil für Tageslänge (Erklärung) auf Seite 353.

Bestimmen eines Zeitprofils

1. Klicken Sie in der Liste **Zeitprofile** mit der rechten Maustaste auf **Zeitprofile** > **Zeitprofil hinzufügen**. Das Fenster **Zeitprofile** wird geöffnet.
2. Geben Sie im Fenster **Zeitprofil** einen Namen für das neue Zeitprofil in das Feld **Name** ein. Optional können Sie eine Beschreibung für das neue Zeitprofil im Feld **Beschreibung** eingeben.
3. Wählen Sie im Kalender des Fensters **Zeitprofil** entweder die **Tagesansicht**, **Wochenansicht** oder **Monatsansicht** aus, klicken mit der rechten Maustaste und wählen Sie dann entweder **Einzelne Zeit hinzufügen** oder **Serienzeit hinzufügen** aus.
4. Wenn Sie die Zeiträume für das Zeitprofil bestimmt haben, klicken Sie im Fenster **Zeitprofil** auf **OK**. Das System fügt Ihr neues Zeitprofil zu der Liste **Zeitprofile** hinzu. Wenn Sie das Zeitprofil später bearbeiten oder löschen möchten, können Sie dies ebenfalls über die Liste **Zeitprofile** tun.

Hinzufügen einer einzelnen Zeit

Wenn Sie **Einzelne Zeit hinzufügen** auswählen, erscheint das Fenster **Zeit auswählen**:

Auf Ihrem Computer wird möglicherweise ein anderes Uhrzeit- und Datumsformat verwendet.

1. Bestimmen Sie im Fenster **Zeit auswählen** eine **Startzeit** und eine **Endzeit**. Wenn die Zeit ganze Tage abdecken soll, setzen Sie ein Häkchen bei **Ganztägiges Ereignis**.
2. Klicken Sie auf **OK**.

Bestimmen einer Zeitserie

Wenn Sie **Serienzeit hinzufügen** auswählen, erscheint das Fenster **Serienzeit auswählen**:

1. Bestimmen Sie im Fenster **Zeit auswählen** den Zeitraum, das Serienmuster und die Seriendauer.
2. Klicken Sie auf **OK**.

Ein Zeitprofil kann mehrere Zeiträume beinhalten. Wenn Sie möchten, dass Ihr Zeitprofil weitere Zeiträume beinhaltet, fügen Sie weitere einzelne Zeiten oder Serienzeiten hinzu.

Bearbeiten eines Zeitprofils

1. Klicken Sie in der Liste **Zeitprofile** im Bereich **Übersicht** mit der rechten Maustaste auf das gewünschte Zeitprofil und wählen Sie **Zeitprofil bearbeiten** aus. Das Fenster **Zeitprofile** wird geöffnet.
2. Bearbeiten Sie das Zeitprofil nach Bedarf. Wenn Sie Änderungen am Zeitprofil vorgenommen haben, klicken Sie im Fenster **Zeitprofil** auf **OK**. Sie kehren zur Liste **Zeitprofile** zurück.

Im Fenster **Zeitprofilinformation** können Sie das Zeitprofil nach Bedarf bearbeiten. Beachten Sie, dass ein Zeitprofil mehrere Zeiträume beinhalten kann und dass Zeiträume

wiederkehren können. Die kleine Monatsübersicht in der Ecke rechts oben kann Ihnen dabei helfen, schnell einen Überblick über die Zeiträume zu erhalten, die von einem Zeitprofil abgedeckt werden, da Daten mit festgelegten Zeiten fett hervorgehoben werden.

In diesem Beispiel zeigen die Daten in Fettdruck, dass Sie Zeiträume für mehrere Tage bestimmt haben und dass Sie für eine Serienzeit für Montage bestimmt haben.

Zeitprofil für Tageslänge (Erklärung)

Wenn Sie Kameras im Freien aufstellen, müssen Sie oftmals die Kameraauflösung verringern, schwarz/weiß aktivieren oder andere Einstellungen ändern, wenn es dunkel oder hell wird. Je weiter die Kameras nördlich oder südlich vom Äquator entfernt sind, desto stärker variieren die Sonnenaufgangs- und -untergangszeiten im Jahresverlauf. Deshalb ist es unmöglich, feste Standardzeitprofile für die Anpassung der Kameraeinstellungen entsprechend den Lichtverhältnissen zu verwenden.

In solchen Situationen können Sie stattdessen Tageslängen-Zeitprofile erstellen, um den Sonnenaufgang und -untergang für ein bestimmtes geografisches Gebiet zu definieren. Über die geographischen Koordinaten berechnet das System die Zeit des Sonnenauf- und Untergangs und bezieht sogar täglich die Sommerzeit mit ein. Dadurch folgt das Zeitprofil automatisch den jährlichen Veränderungen des Sonnenaufgangs und -untergangs im ausgewählten Gebiet, sodass das Profil nur dann aktiv ist, wenn es gebraucht wird. Alle Zeiten und Daten richten sich nach den Zeit- und Datumseinstellungen des Management-Servers. Sie können auch einen positiven oder negativen Offsetwert (in Minuten) für die Startzeit (Sonnenaufgang) und Endzeit (Sonnenuntergang) einstellen. Der Offsetwert für die Start- und Endzeit kann identisch oder unterschiedlich sein.

Sie können Tageslängenprofile beim Erstellen von Regeln und Rollen verwenden.

Hinzufügen eines Tageslängen-Zeitprofils

1. Erweitern Sie den Ordner **Regeln und Ereignisse** > **Zeitprofile**.
2. Klicken Sie auf der Liste **Zeitprofile** mit der rechten Maustaste auf **Zeitprofile** und wählen Sie **Hinzufügen eines Tageslängen-Zeitprofils** aus.
3. Geben Sie die erforderlichen Informationen in das Fenster **Tageslängen-Zeitprofil** ein. Für die Regelung der Übergangszeiten zwischen Tag und Nacht können Sie die Aktivierung und Deaktivierung des Profils verschieben. Zeit und Monatsnamen werden entsprechend den Sprach- und Regionseinstellungen Ihres Computers angezeigt.
4. Um den Ort der eingegebenen geographischen Koordinaten auf einer Karte zu sehen, klicken Sie auf **Position in Browser anzeigen**. Dadurch wird ein Browser mit einer Karte geöffnet, auf der Sie den Standort sehen können.
5. Klicken Sie auf **OK**.

Eigenschaften der Tageslängen-Zeitprofile

Stellen Sie die folgenden Eigenschaften für Tageslängen-Zeitprofile ein:

Name	Beschreibung
Name	Der Name des Profils.
Beschreibung	Eine Beschreibung des Profils (optional).
Geokoordinaten	Die geographischen Koordinaten, die den physischen Standort der Kamera(s) anzeigen, die dem Profil zugeordnet sind.
Offset Sonnenaufgang	Anzahl der Minuten (+/-), um die die Aktivierung des Profils durch den Sonnenaufgang verschoben wird.
Offset Sonnenuntergang	Anzahl der Minuten (+/-), um die die Deaktivierung des Profils durch den Sonnenuntergang verschoben wird.
Zeitzone	Zeitzone, die den physischen Standort der Kamera(s) anzeigt.

Benachrichtigungsprofile

Benachrichtigungsprofile (Erklärung)

Mit Benachrichtigungsprofilen können Sie vorgefertigte E-Mail-Benachrichtigungen einstellen. Benachrichtigungen können automatisch von Regeln ausgelöst werden können, z. B. wenn ein bestimmtes Ereignis eintritt.

Wenn Sie das Benachrichtigungsprofil erstellen, geben Sie einen Benachrichtigungstext ein und entscheiden, ob Sie Standbilder und AVI-Videoclips in die E-Mail-Benachrichtigungen aufnehmen wollen.

> ⚠ Außerdem kann es erforderlich sein, mögliche E-Mailscanner zu deaktivieren, welche die Anwendung vom Versenden der E-Mailbenachrichtigungen abhalten.

Anforderungen an die Erstellung von Benachrichtigungsprofilen

Bevor Sie ein Benachrichtigungsprofil erstellen können, müssen Sie die Einstellungen für den ausgehenden Mailserver für die E-Mailbenachrichtigungen festlegen.

Sie können die Kommunikation zum Mailserver sichern, wenn Sie die nötigen Sicherheitszertifikate auf dem Mailserver installieren.

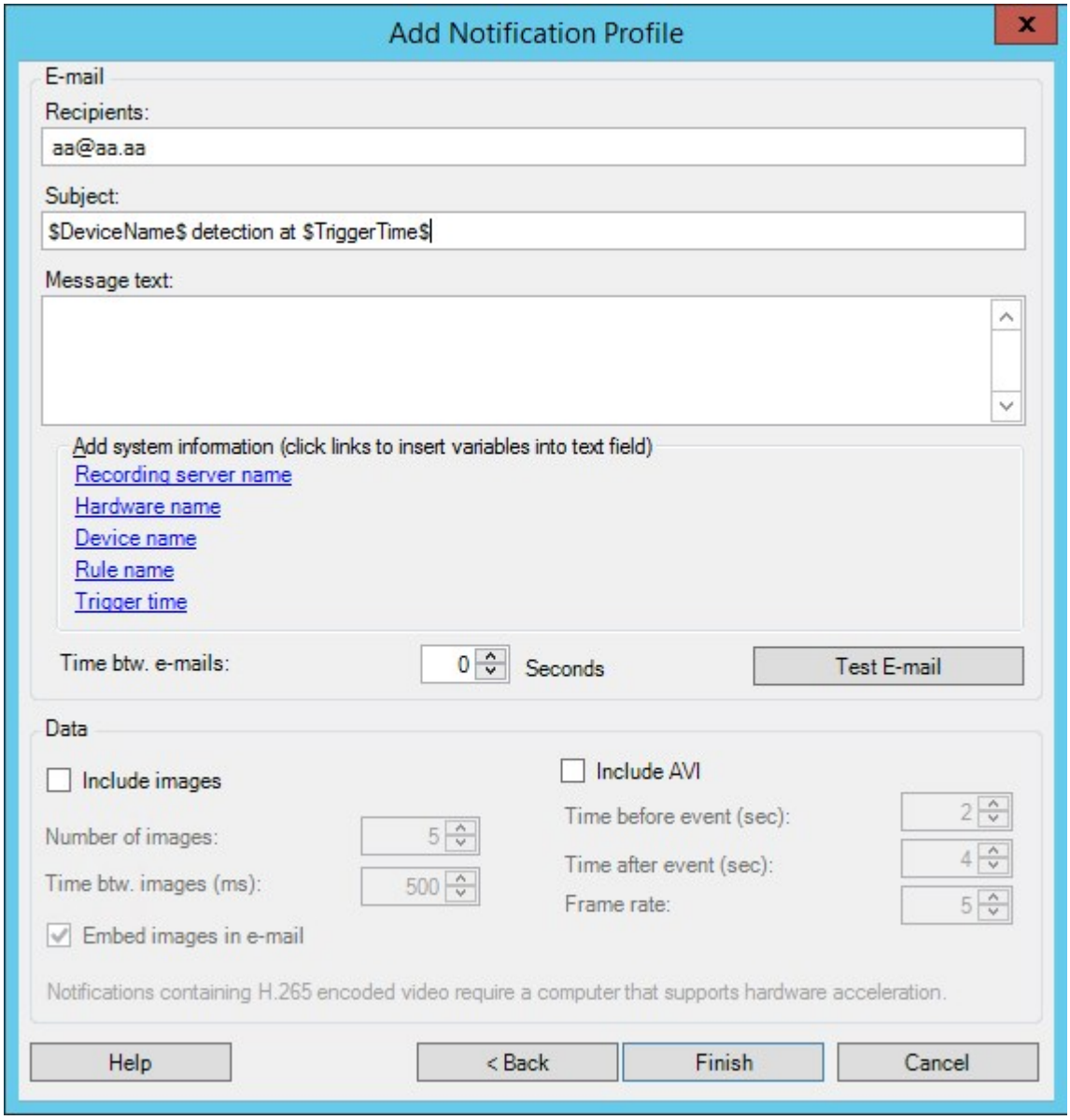
Wenn Sie AVI-Videoclips in die E-Mailbenachrichtigungen einbinden können möchten, müssen Sie auch die Komprimierungseinstellungen dafür festlegen:

1. Gehen Sie zu **Werkzeuge** > **Optionen**. Dadurch öffnet sich das Fenster **Optionen**.
2. Konfigurieren Sie den Mailserver auf der Registerkarte **Mail Server** (Registerkarte Registerkarte „Mailserver“ (Optionen) auf Seite 125) und die Kompressionseinstellungen auf der Registerkarte **AVI-Generation** Registerkarte „AVI-Generierung“ (Optionen) auf Seite 126.

Hinzufügen von Benachrichtigungsprofilen

1. Erweitern Sie **Regeln und Ereignisse** und klicken Sie mit der rechten Maustaste auf **Benachrichtigungsprofile** > **Benachrichtigungsprofil hinzufügen**. Der Assistent **Benachrichtigungsprofil hinzufügen** wird geöffnet.
2. Geben Sie Namen und Beschreibung ein. Klicken Sie auf **Weiter**.

3. Geben Sie Empfänger, Betreff, Nachrichtentext und Zeit zwischen E-Mails ein:



4. Um an die angegebenen Empfänger eine Test-E-Mailbenachrichtigung zu senden, klicken Sie auf **Test-E-Mail**.

5. Um Voralarm-Standbilder einzubinden, wählen Sie **Bilder einschließen** und geben Folgendes ein: die Anzahl der Bilder, die Zeit zwischen den Bildern und, ob die Bilder in die E-Mails eingebettet werden sollen oder nicht.

6. Um AVI-Videoclips einzubinden, wählen Sie **AVI beifügen** und bestimmen Sie die Zeit vor und nach dem Ereignis sowie die Bildrate.

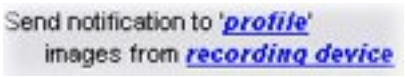
> Benachrichtigungen mit H.265-verschlüsselten Videodaten erfordern einen Computer, der die Hardwarebeschleunigung unterstützt.

7. Klicken Sie auf **Fertigstellen**.

Auslösen von E-Mailbenachrichtigungen durch Regeln

Sie verwenden **Regel verwalten** zum Erstellen von Regeln. Der Assistent führt Sie durch alle relevanten Schritte. Den Verwendungszweck eines Benachrichtigungsprofils können Sie während des Schritts festlegen, bei dem Sie die Regelaktionen bestimmen.

Wenn Sie die Aktion **Benachrichtigung senden an <Profil>** auswählen, können Sie das gewünschte Benachrichtigungsprofil auswählen und festlegen, welche Aufzeichnungen von welchen Kameras in die E-Mailbenachrichtigungen des Benachrichtigungsprofils eingebunden werden sollen:



Klicken Sie bei **Regel verwalten** auf die Links, um Ihre Auswahl zu treffen.

Bedenken Sie, dass Sie nur dann Aufzeichnungen in die E-Mailbenachrichtigungen des Benachrichtigungsprofils einbinden können, wenn tatsächlich etwas aufgezeichnet wird. Wenn Sie Standbilder oder AVI-Videoclips in den E-Mailbenachrichtigungen einschließen möchten, überprüfen Sie, ob die Regel bestimmt, dass eine Aufzeichnung erfolgen soll. Das folgende Beispiel basiert auf einer Regel, die sowohl die Aktion **Aufzeichnung starten** als auch **Benachrichtigung senden an** enthält:

Benachrichtigungsprofil (Eigenschaften)

Legen Sie die folgenden Eigenschaften für Benachrichtigungsprofile fest:

Komponente	Voraussetzung
Name	Geben Sie dem Benachrichtigungsprofil einen beschreibenden Namen. Der Name erscheint später immer, wenn Sie eine Regel erstellen und das Benachrichtigungsprofil auswählen.
Beschreibung (optional)	Geben Sie eine Beschreibung für das Benachrichtigungsprofil ein. Die Beschreibung wird angezeigt, wenn Sie den Mauszeiger über dem Benachrichtigungsprofil auf der Liste **Benachrichtigungsprofile** im Bereich „Übersicht" ruhen lassen.
Empfänger	Geben Sie die E-Mailadressen ein, an die die E-Mailbenachrichtigungen des Benachrichtigungsprofils gesendet werden sollen. Wenn Sie mehrere E-Mailadressen eingeben möchten, trennen Sie diese mit einem Strichpunkt ab. Beispiel: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
Betreff	Geben Sie hier den Text ein, der als Betreff der E-Mailbenachrichtigung angezeigt werden soll. Sie können Systemvariablen, wie z. B. **Gerätename**, in die Betreffzeile oder das Nachrichtentextfeld eingeben. Um Variablen einzufügen, klicken Sie auf die gewünschten Variablenlinks im Kasten unterhalb des Felds.
Nachrichtentext	Geben Sie hier den Text ein, der im Textteil der E-Mailbenachrichtigungen angezeigt werden soll. Zusätzlich zum Nachrichtentext enthält der Textteil jeder E-Mailbenachrichtigung automatisch diese Informationen: • Auslöser der E-Mailbenachrichtigung • Quelle aller angehängten Standbilder oder AVI-Videoclips
Zeit zwischen E-Mails	Bestimmen der Mindestdauer (in Sekunden) zwischen dem Versenden jeder einzelnen E-Mailbenachrichtigung. Beispiele: • Wenn Sie einen Wert von **120** festlegen, vergehen mindestens 2 Minuten zwischen dem Versenden jeder einzelnen E-Mailbenachrichtigung, auch wenn das Benachrichtigungsprofil wieder von einer Regel ausgelöst wird, bevor die 2 Minuten vergangen sind

Komponente	Voraussetzung
	• Wenn Sie einen Wert von **0** festlegen, wird jedes Mal eine E-Mailbenachrichtigung versendet, wenn das Benachrichtigungsprofil von einer Regel ausgelöst wird. Das kann unter Umständen dazu führen, dass sehr viele E-Mailbenachrichtigungen versendet werden. Wenn Sie also den Wert **0** verwenden, sollten Sie sich genau überlegen, ob Sie das Benachrichtigungsprofil bei Regeln verwenden möchten, die wahrscheinlich häufig ausgelöst werden
Anzahl der Bilder	Legen Sie die Höchstzahl der Standbilder fest, die Sie pro E-Mailbenachrichtigung des Benachrichtigungsprofils einbinden möchten. Standardmäßig sind es fünf Bilder.
Zeit zwischen Bildern (ms)	Legen Sie eine Zeit in Millisekunden fest, die zwischen den Aufnahmen der eingebundenen Bilder bestehen soll. Beispiel: Beim Standardwert von 500 Millisekunden werden die eingebundenen Bilder als Aufzeichnungen mit einem Bildabstand von einer halben Sekunde angezeigt.
Zeit vor Ereignis (Sek.)	Mit dieser Einstellung wird der Anfang der AVI-Datei festgelegt. Standardmäßig beginnt die Aufzeichnung auf der AVI-Datei 2 Sekunden vor Auslösen des Benachrichtigungsprofils. Sie können diesen Wert auf einen gewünschten Wert in Sekunden ändern.
Zeit nach Ereignis (Sek.)	Mit dieser Einstellung wird das Ende der AVI-Datei festgelegt. Standardmäßig endet die AVI-Datei 4 Sekunden nach Auslösen des Benachrichtigungsprofils. Sie können diesen Wert auf einen gewünschten Wert in Sekunden ändern.
Bildrate	Legen Sie die gewünschte Anzahl an Bildern pro Sekunde für die AVI-Datei fest. Der Standardwert beträgt fünf Bilder pro Sekunde. Je größer die Bildrate, desto höher die Bildqualität und desto größer die AVI-Datei.
Bilder in E-Mail einbetten	Wenn ausgewählt (Standardeinstellung), werden Bilder in den Textteil der E-Mailbenachrichtigungen eingefügt. Wenn nicht ausgewählt, werden die Bilder den E-Mailbenachrichtigungen als angehängte Dateien beigefügt.

Benutzerdefinierte Ereignisse

Benutzerdefinierte Ereignisse (Erklärung)

Wenn das von Ihnen benötigte Ereignis nicht in der Liste **Ereignisübersicht** auftaucht, können Sie Ihre eigenen benutzerdefinierten Ereignisse erstellen. Benutzen Sie solche benutzerdefinierte Ereignisse, um andere Systeme in Ihr Überwachungssystem zu integrieren.

Durch benutzerdefinierte Ereignisse, ist es Ihnen möglich Daten eines Zutrittskontrollsystems von Dritten als Ereignisse in das System einzuspeisen. Die Ereignisse können später Aktionen auslösen. Auf diese Weise können Sie beispielsweise Video von relevanten Kameras aufzeichnen lassen, sobald jemand das Gebäude betritt.

Sie können also benutzerdefinierte Ereignisse für manuell ausgelöste Ereignisse verwenden, während Sie Live-Video in XProtect Smart Client ansehen oder sogar automatisch, wenn Sie diese in Regeln benutzen. Zum Beispiel: wenn benutzerdefiniertes Ereignis 37 geschieht, sollte PTZ-Kamera 224 aufhören zu überwachen und zur Preset Position 18 gehen.

Über Rollen definieren Sie, welche Benutzer die benutzerdefinierten Ereignisse auslösen können. Sie können bei Bedarf benutzerdefinierte Ereignisse auf zwei Arten und zur selben Zeit verwenden:

Ereignisse	Beschreibung
Für die Bereitstellung der Fähigkeit, manuell Ereignisse in XProtect Smart Client auszulösen	In diesem Falle ermöglichen es benutzerdefinierte Ereignisse den Endbenutzern manuell Ereignisse auszulösen, während sie Live-Video in XProtect Smart Client ansehen. Wenn ein benutzerdefiniertes Ereignis auftritt, weil ein Benutzer von XProtect Smart Client es manuell auslöst, kann eine Regel dafür sorgen, dass eine oder mehr Aktionen im System stattfinden sollen.
Für die Bereitstellung der Fähigkeit Ereignisse über API auszulösen	In diesem Fall können Sie benutzerdefinierte Ereignisse außerhalb des Überwachungssystem auslösen. Das Verwenden von benutzerdefinierten Ereignissen auf diese Weise erfordert, dass ein eigenes API (Application Program Interface, Eine Reihe von Bausteinen für die Erstellung oder Anpassung von Softwareanwendungen) verwendet wird, wenn das benutzerdefinierte Ereignis ausgelöst wird. Eine Authentifizierung durch das Active Directory ist erforderlich, um ein benutzerdefiniertes Ereignis auf diese Art zu verwenden. Dies gewährleistet, dass auch wenn benutzerdefinierte Ereignisse außerhalb des Überwachungssystems ausgelöst werden können, dies nur durch autorisierte Benutzer geschehen kann. Des weiteren können benutzerdefinierte Ereignisse über API mit Metadaten verbunden werden, die gewisse Geräte oder Gerätegruppen definieren. Dies ist

Ereignisse	Beschreibung
	besonders nützlich, wenn benutzerdefinierte Ereignisse genutzt werden, um Regeln auszulösen, denn Sie vermeiden es eine Regel für jedes Gerät zu haben, die im Grunde das gleiche ausführen. Beispiel: Ein Unternehmen verwendet eine Zutrittskontrolle bei 35 Eingängen, jedes mit einem Zutrittskontrollgerät. Wenn ein Zutrittskontrollgerät aktiviert wird, löst ein benutzerdefiniertes Ereignis im System aus. Dieses benutzerdefinierte Ereignis startet mittels einer Regel die Aufzeichnung einer Kamera, die mit diesem aktiviertem Zutrittskontrollgerät verbunden ist. In den Metadaten wird festgelegt, welche Kamera welcher Regel folgt. Auf diese Art und Weise muss das Unternehmen nicht 35 verschiedene benutzerdefinierte Ereignisse einrichten und mittels zugehöriger 35 Regeln auslösen. Ein einzelnes benutzerdefiniertes Ereignis und eine einzelne Regel sind ausreichend. Wenn Sie benutzerdefinierte Ereignisse auf diese Art verwenden, stehen diese gegebenenfalls nicht immer für eine manuelle Auslösung in XProtect Smart Client zur Verfügung. Sie können Rollen nutzen, um die Sichtbarkeit von benutzerdefinierten Ereignissen in XProtect Smart Client festzulegen.

Ungeachtet dessen, wie Sie benutzerdefinierte Ereignisse verwenden möchten, müssen Sie jedes benutzerdefinierte Ereignis über Management Client hinzufügen.

Wenn Sie ein benutzerdefiniertes Ereignis umbenennen, müssen bereits verbundene XProtect Smart Client-Benutzer ausloggen und wieder einloggen, bevor die Namensänderung sichtbar wird.

Bei Löschung eines benutzerdefinierten Ereignisses ist jede Regel, die von ihr verwendet wurde, betroffen. Ein entferntes benutzerdefiniertes Ereignis verschwindet auch nur von XProtect Smart Client, wenn die XProtect Smart Client-Benutzer sich abmelden.

Benutzerdefiniertes Ereignis hinzufügen

1. **Regeln und Ereignisse** ausklappen > **Benutzerdefinierte Ereignisse**.
2. Im Bereich **Übersicht**, klicken Sie mit der rechten Maustaste auf **Ereignisse** > **Benutzerdefiniertes Ereignis** hinzufügen.

3. Geben Sie einen Namen für das neue benutzerdefinierte Ereignis ein und klicken Sie dann auf **OK**. Das neu hinzugefügte benutzerdefinierte Ereignis wird nun in der Liste im Bereich **Übersicht** angezeigt.

Der Benutzer kann jetzt das benutzerdefinierte Ereignis in XProtect Smart Client manuell auslösen, wenn die nötigen Nutzerrechte vorhanden sind.

Ein benutzerdefiniertes Ereignis umbenennen

1. **Regeln und Ereignisse** ausklappen > **Benutzerdefinierte Ereignisse**.
2. Wählen Sie das benutzerdefinierte Ereignis im Bereich **Übersicht** aus.
3. Überschreiben Sie den bestehenden Namen im Bereich **Eigenschaften**.
4. Klicken Sie in der Symbolleiste auf **Speichern**.

Analyseereignisse

Analyseereignisse (Erklärung)

Analyseereignisse werden typischerweise zum Empfang von Daten von Video-Content-Analyse-Lösungen (CVA) von anderen Herstellern benutzt.

Die Verwendung von Analyseereignissen als Grundlage für Alarme ist ein Prozess mit drei Schritten:

- Erster Schritt: Aktivierung der Funktion der Analyseereignisse und Durchführung der zugehörigen Sicherheitseintellungen. Durch die Verwendung einer Liste zugelassener Adressen kann gesteuert werden, wer Ereignisdaten an das System senden kann und auf welchen Port der Server reagiert
- Zweiter Schritt: Erstellung des Analyseereignisses, wenn möglich mit einer Beschreibung und Test des Ereignisses
- Dritter Schritt: Verwendung des Analyseereignisses als Quelle für die Definition eines Alarms

Sie können Analyseereignisse in der Liste **Regeln und Ereignisse** im Bereich **Standort-Navigation** einstellen.

Zur Verwendung von auf VCA basierenden Ereignissen, ist ein VCA-Tool Dritter nötig, um das System mit Daten zu versorgen. Welches VCA-Tool Sie benutzen möchten liegt dabei ganz bei Ihnen, so lange die Daten aus dem Tool dem richtigen Format entsprechen. Dieses Format wird in der MIP SDK Dokumentation zu Analyseereignissen erläutert.

Detaillierte Informationen erhalten Sie von Ihrem Systemanbieter. VCA-Tools von Drittanbietern werden von unabhängigen Partnern entwickelt, die Lösungen auf Grundlage einer Open-Platform von Milestone anbieten. Diese Lösungen können Einfluss auf die Leistung des Systems haben.

Ein Analyseereignis hinzufügen und bearbeiten

Ein Analyseereignis hinzufügen

1. Erweitern Sie **Regeln und Ereignisse**, klicken Sie mit der rechten Maustaste auf **Analyseereignisse** und wählen Sie **Neu hinzufügen** aus.
2. Geben Sie im Fenster **Eigenschaften** einen Namen für das Ereignis in das Feld **Name** ein.
3. Falls nötig, geben Sie im Feld **Beschreibung** einen Beschreibungstext ein.
4. Klicken Sie in der Symbolleiste auf **Speichern**. Sie können die Gültigkeit eines Ereignisses testen, durch Anklicken von **Ereignis testen**. Sie können jederzeit Fehler, die im Test angezeigt werden korrigieren und den Test so oft wie Sie möchten und zu jeder Zeit neu ausführen.

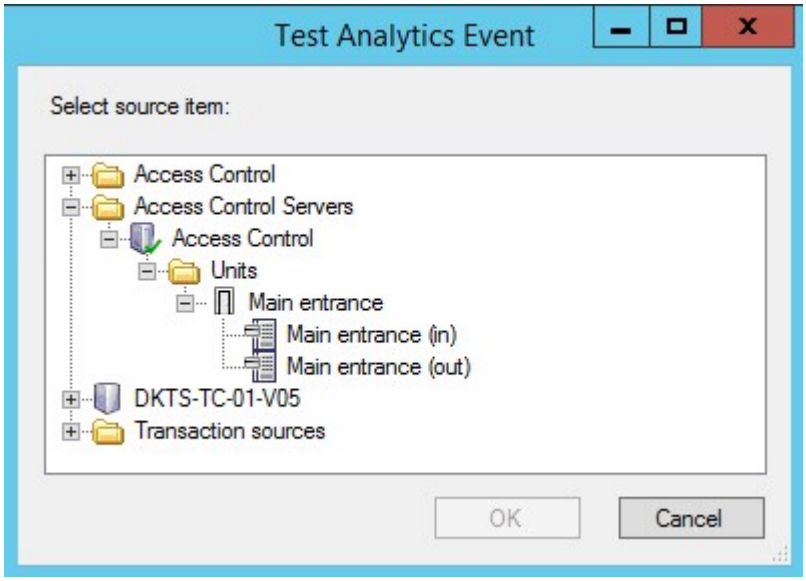
Ein Analyseereignis bearbeiten

1. Klicken Sie auf ein bestehendes Analyseereignis, um das Fenster **Eigenschaften** anzeigen zu lassen, in dem Sie relevante Felder bearbeiten können.
2. Sie können die Gültigkeit eines Ereignisses testen, durch Anklicken von **Ereignis testen**. Sie können jederzeit Fehler, die im Test angezeigt werden korrigieren und den Test so oft wie Sie möchten und zu jeder Zeit neu ausführen.

Ein Analyseereignis testen

Nachdem Sie ein Analyseereignis erstellt haben, können Sie die Anforderungen testen (siehe Analyseereignisse testen (Eigenschaften) auf Seite 364), z. B. ob die Funktion Analyseereignis in Management Client aktiviert wurde.

1. Wählen Sie ein bestehendes Analyseereignis aus.
2. Klicken Sie in den Eigenschaften auf die Schaltfläche **Ereignis testen**. Ein Fenster mit allen möglichen Quellen des Ereignisses erscheint.



3. Wählen Sie die Quelle für Ihr Testereignis, zum Beispiel eine Kamera. Das Fenster wird geschlossen und ein neues Fenster erscheint, welches vier Bedingungen fordert, damit das Analyseereignis funktioniert.

Sie können als zusätzlichen Test in XProtect Smart Client bestätigen, dass das Analyseereignis an den Event Server gesendet wurde. Dafür öffnen Sie einfach XProtect Smart Client und sehen dann das Ereignis auf der Registerkarte **Alarm-Manager**.

Siehe auch

Analyseereignisse (Erklärung) auf Seite 362

Analyseereignisse testen (Eigenschaften)

Beim Test der Anforderungen eines Analyseereignisses erscheint ein Fenster, welches vier Bedingungen untersucht und mögliche Beschreibungen und Lösungen von Fehlern anbietet.

Bedingung	Beschreibung	Fehlermeldungen und Lösungen
Änderungen gespeichert	Wenn das Ereignis neu ist, wird es gespeichert? Oder	**Speichern Sie die Änderungen vor dem Testen des Analyseereignisses**. Lösung/Erklärung: Speichern

Bedingung	Beschreibung	Fehlermeldungen und Lösungen
	werden Änderungen am Ereignisnamen gespeichert?	Sie die Änderungen.
Analyseereignisse aktiviert	Wurde die Funktion Analyseereignis aktiviert?	**Analyseereignisse wurde nicht aktiviert**. Lösung/Erklärung: Aktivieren Sie die Funktion Analyseereignis. Um dies zu tun, klicken Sie auf **Tools** > **Optionen** > **Analyseereignisse** und wählen Sie das Kontrollkästchen **Aktiviert** aus.
Adresse zugelassen	Ist die IP-Adresse/der Hostname des Geräts, welche die Ereignisse sendet, dazu berechtigt (auf der Adressenliste für Analyseereignisse aufgeführt)?	**Der lokale Hostname muss in die Liste der zugelassenen Adressen für den Analyseereignis-Dienst hinzugefügt werden**. Lösung/Erklärung: Fügen Sie Ihr Gerät zur Liste der zugelassenen IP-Adressen oder Hostnamen für Analyseereignisse hinzu. **Fehler beim Auflösen des lokalen Hostnamens**. Lösung/Erklärung: Die IP-Adresse oder Hostname des Geräts kann nicht gefunden werden oder ist ungültig.
Analyseereignis senden	War das Senden des Testereignisses an den Event Server erfolgreich?	Siehe Tabelle unten.

Jeder Schritt ist entweder als fehlgeschlagen: ✗ oder erfolgreich markiert: ✓.

Fehlermeldungen und Lösungen für die Bedingung **Analyseereignis senden**:

Fehlermeldung	Lösung
Event Server nicht gefunden	Nicht möglich den Event Server auf der Liste registrierter Dienste zu finden.
Fehler beim Verbinden mit Event Server	Nicht möglich mit dem Event Server über den angegeben Port zu verbinden. Der Fehler entsteht wahrscheinlich aufgrund von Netzwerkproblemen oder der

Fehlermeldung	Lösung
	Ereignisserver-Dienst wurde gestoppt.
Fehler beim Senden von Analyseereignis	Die Verbindung zum Event Server wurde aufgebaut, aber das Ereignis kann nicht gesendet werden. Der Fehler entsteht wahrscheinlich aufgrund von Netzwerkproblemen (z. B. ein Timeout).
Fehler beim Empfangen der Antwort vom Event Server	Das Ereignis wurde zum Event Server gesendet, aber es gab keine Antwort. Der Fehler entsteht wahrscheinlich aufgrund von Netzwerkproblemen oder einem belegtem Port. Sehen Sie sich das Event Server-Protokoll an, das normalerweise unter *ProgramData\Milestone\XProtect Event Server\Logs\ zu finden ist.*
Analyseereignis beim Event Server unbekannt	Der Ereignisserver-Dienst erkennt das Ereignis nicht. Der Fehler entsteht aufgrund des Ereignisses oder Änderungen am Ereignis wurden nicht gespeichert.
Ungültiges Analyseereignis vom Event Server empfangen	Das Format des Ereignisses ist nicht korrekt.
Absender nicht vom Event Server autorisiert	Höchstwahrscheinlich steht Ihre Anlage nicht auf der Liste der erlaubten IP-Adressen oder Hostnamen.
Interner Fehler auf Event Server	Fehler auf Event Server. Sehen Sie sich das Event Server-Protokoll an, das normalerweise unter *ProgramData\Milestone\XProtect Event Server\Logs\ zu finden ist.*
Ungültige Antwort vom Event Server empfangen	Die Antwort ist ungültig. Möglicherweise ist der Port belegt oder das Netzwerk hat Probleme. Sehen Sie sich das Event Server-Protokoll an, das normalerweise unter *ProgramData\Milestone\XProtect Event Server\Logs* zu finden ist.
Unbekannte Antwort vom Event Server	Die Antwort ist gültig, kann aber nicht verarbeitet werden. Der Fehler entsteht möglicherweise aufgrund von Netzwerkproblemen oder einem belegten Port. Sehen Sie sich das Event Server-Protokoll an, das normalerweise unter

Fehlermeldung	Lösung
	ProgramData\Milestone\XProtect Event Server\Logs zu finden ist.
Unerwarteter Fehler	Bitte kontaktieren Sie für weitere Hilfe den Milestone-Support.

Einstellungen für Analyseereignisse bearbeiten

Gehen Sie in der Symbolleiste auf **Tools** > **Optionen** > Registerkarte **Analyseereignisse**, um relevante Einstellungen zu bearbeiten.

Generische Ereignisse

Generische Ereignisse (Erklärung)

Diese Funktion ist nur verfügbar, wenn der XProtect Event Server installiert ist.

Generische Ereignisse ermöglichen es Ihnen, Aktionen im XProtect Event-Server auszulösen, indem einfache Zeichenketten über das IP-Netzwerk an Ihr System gesendet werden.

Sie können jede Hardware oder Software verwenden, die Strings über TCP oder UDP versenden kann, um generische Ereignisse auszulösen. Ihr System kann erhaltene TCP- oder UDP-Datenpakete analysieren und automatisch generische Ereignisse auslösen, wenn bestimmte Bedingungen erfüllt sind. Auf diese Weise können Sie in Ihr System externe Quellen, z. B. Zutrittskontrollsysteme und Alarmsysteme integrieren. Das Ziel besteht darin, so vielen externen Quellen wie möglich zu erlauben, mit dem System zu interagieren.

Mit dem Konzept der Datenquellen vermeiden Sie Drittanbieter-Tools verwenden zu müssen, um den Standards Ihres Systems gerecht werden zu können. Mithilfe der Datenquellen können Sie mit einem bestimmten Teil Ihrer Hardware oder Software über einen bestimmten IP-Port kommunizieren und die Interpretation der Bytes, die an diesem Port ankommen, optimieren. Jeder generische Ereignistyp hängt mit einer Datenquelle zusammen und stellt eine Sprache dar, die für die Kommunikation mit einem bestimmten Teil der Hardware oder Software verwendet wird.

Die Arbeit mit Datenquellen erfordert allgemeine Kenntnisse über IP-Netzwerke und Fachkenntnisse über die jeweilige Hardware oder Software, die Sie als Interface verwenden möchten. Es gibt viele Parameter, die Sie verwenden können und keinen vorgefertigten Lösungsweg, nach dem Sie vorgehen müssen. Grundsätzlich gilt, dass Ihr System die Tools, aber nicht die Lösung liefert. Im Gegensatz zu benutzerdefinierten Ereignissen gibt es bei generischen Ereignissen keine Authentifizierung. Dadurch sind sie einfacher auszulösen, aber damit die Sicherheit nicht gefährdet wird, werden nur Ereignisse von lokalen Hosts akzeptiert. Sie können andere Client-IP-Adressen von der Registerkarte **generische Ereignisse** des Menüs **Optionen** zulassen.

Hinzufügen eines generischen Ereignisses

Sie können generische Ereignisse definieren und damit der VMS dabei helfen, bestimmte Zeichenketten in TCP- und UDP-Paketen von einem externen System zu erkennen. Dem generischen Ereignis entsprechend können Sie den Management Client dazu konfigurieren, Aktionen auszulösen, z. B. mit der Aufzeichnung oder Alarme zu starten.

Voraussetzungen
Sie haben generische Ereignisse aktiviert sowie die zugelassenen Quellen und Ziele bestimmt. Weitere Informationen finden Sie auf der Registerkarte Registerkarte „Generische Ereignisse“ (Optionen) auf Seite 134.

Ein Generisches Ereignis hinzufügen:

1. Erweitern Sie **Regeln und Ereignisse**.
2. Klicken Sie mit der rechten Maustaste auf **Generisches Ereignis** und wählen Sie die Option **Neu hinzufügen** aus.
3. Geben Sie die erforderlichen Informationen und Eigenschaften ein. Weitere Informationen finden Sie unter Generisches Ereignis (Eigenschaften) auf Seite 368.
4. (Optional) Um zu validieren, ob ein Suchausdruck gültig ist, geben Sie den Suchstring in das Feld **Prüfen Sie, ob der Ausdruck mit dem Ereignis-String übereinstimmt** ein, das dem erwarteten Paket entspricht:
   - **Übereinstimmung** - der String kann mit dem Suchausdruck validiert werden
   - **Keine Übereinstimmung** - der Suchausdruck ist ungültig. Ändern Sie ihn und versuchen Sie es erneut

Im XProtect Smart Client können Sie überprüfen, ob Ihre generischen Ereignisse vom Event Server empfangen wurden. Das können Sie in der **Alarmliste** auf der Registerkarte **Alarm-Manager** machen, indem Sie **Ereignisse** auswählen.

Generisches Ereignis (Eigenschaften)

Komponente	Voraussetzung
Name	Einmaliger Name für das generische Ereignis. Der Name muss einmalig unter allen Ereignistypen sein, wie z. B. benutzerdefinierte Ereignisse, Analyseereignisse und so weiter.
Aktiviert	Generische Ereignisse sind standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen,

Komponente	Voraussetzung
	um das Ereignis zu deaktivieren.
Ausdruck	Ausdruck, nach dem das System bei der Analyse von Datenpaketen suchen soll. Sie können die folgenden Operatoren verwenden: • **( )**: Wird verwendet, um sicherzustellen, dass verwandte Begriffe zusammen als logische Einheit verarbeitet werden. Sie können verwendet werden, um eine bestimmte Verarbeitungsreihenfolge in der Analyse zu erzwingen **Beispiel**: Bei den Suchkriterien "(**Benutzer001** ODER **Tür053**) UND **Sonntag**" werden zuerst die beiden Begriffe zwischen den Klammern verarbeitet, dann wird das Ergebnis mit dem letzten Teil des Strings kombiniert. Also sucht das System zuerst nach Paketen, die einen der beiden Begriffe **Benutzer001** oder **Tür053** beinhalten; dann wird überprüft, welche der Ergebnispakete zusätzlich den Begriff **Sonntag** enthalten. • **UND**: Mit dem UND-Operator bestimmen Sie, dass die Begriffe auf beiden Seiten des UND-Operators vorhanden sein müssen **Beispiel**: Die Suchkriterien "**Benutzer001** UND **Tür053** UND **Sonntag**" liefern nur dann ein Ergebnis, wenn die Begriffe **Benutzer001**, **Tür053** und **Sonntag** alle in Ihrem Ausdruck vorkommen. Es reicht nicht aus, wenn nur einer oder zwei der Begriffe darin vorkommen. Je mehr Begriffe Sie mit UND verbinden, desto weniger Ergebnisse erhalten Sie. • **ODER**: Mit dem ODER-Operator bestimmen Sie, dass entweder der eine oder der andere Begriff vorhanden sein muss **Beispiel**: Die Suchkriterien "**Benutzer001** ODER **Tür053** ODER **Sonntag**" liefern alle Ergebnisse, die entweder **Benutzer001**, **Tür053** oder **Sonntag** beinhalten. Je mehr Begriffe Sie mit ODER verbinden, desto mehr Ergebnisse erhalten Sie.
Ausdruckstyp	Legt fest, wie genau das System beim Analysieren von erhaltenen Datenpaketen vorgehen soll. Es gibt die folgenden Optionen: • **Suche**: Damit das Ereignis eintritt, muss das erhaltene Datenpaket den Text enthalten, der im Feld **Ausdruck** angegeben wurde, aber es darf auch noch weitere Inhalte haben. **Beispiel**: Wenn Sie bestimmt haben, dass das erhaltene Paket die Begriffe **Benutzer001** und **Tür053** enthalten soll, wird das Ereignis ausgelöst, wenn das empfangene Paket die Begriffe **Benutzer001** und **Tür053** und **Sonntag** enthält, da Ihre beiden gewünschten Begriffe im erhaltenen Paket enthalten sind

Komponente	Voraussetzung
	• **Übereinstimmung**: Damit das Ereignis eintritt, muss das erhaltene Datenpaket genau den Text enthalten, der im Feld **Ausdruck** angegeben wurde, und nichts anderes • **Regulärer Ausdruck**: Damit das Ereignis eintritt, muss der Text, der im Feld **Ausdruck** angegeben wurde, bestimmte Muster in den erhaltenen Datenpaketen angeben Wenn Sie von **Suche** oder **Übereinstimmung** auf **Regulärer Ausdruck** wechseln, wird der Text im Feld **Ausdruck** automatisch in einen regulären Ausdruck übersetzt.
Priorität	Die Priorität muss als Zahl zwischen 0 (niedrigste Priorität) und 999999 (höchste Priorität) festgelegt werden. Dasselbe Datenpaket kann auf unterschiedliche Ereignisse analysiert werden. Mit der Funktion des Zuweisens einer Priorität zu jedem Ereignis können Sie einstellen, welches Ereignis ausgelöst werden soll, wenn ein erhaltenes Paket mit den Kriterien von mehreren Ereignissen übereinstimmt. Wenn das System ein TCP- und/oder UDP-Paket erhält, beginnt die Analyse des Pakets auf das Ereignis, das die höchste Priorität hat. Auf diese Weise wird nur das Ereignis mit der höchsten Priorität ausgelöst, wenn ein Paket mit den Kriterien von mehreren Ereignissen übereinstimmt. Wenn ein Paket mit den Kriterien von mehreren Ereignissen mit identischer Priorität übereinstimmt, z. B. zwei Ereignisse mit Priorität 999, werden alle Ereignisse dieser Priorität ausgelöst.
Prüfen Sie, ob der Ausdruck mit dem Ereignis-String übereinstimmt	Ein Ereignis-String, der mit dem Ausdruck abgeglichen werden soll, der im Feld **Ausdruck** eingegeben wurde.

Generisches Ereignis: Datenquelle (Eigenschaften)

Komponente	Voraussetzung
Datenquelle	Sie können zwischen zwei standardmäßigen Datenquellen wählen und eine benutzerdefinierte Datenquelle einstellen. Die Wahl hängt von Ihrem Drittanbieterprogramm und/oder der Hardware oder Software ab, die Sie als Interface verwenden möchten: **Kompatibel**: Werkseinstellungen sind aktiviert, Echo bei allen Bytes, TCP und UDP, nur IPv4, Port 1234, kein Trennzeichen, nur lokaler Host, aktuelle Codepage-Verschlüsselung (ANSI). **International**: Werkseinstellungen sind aktiviert, Echo nur bei Statistiken, nur TCP, IPv4+6, Port 1235, <CR><LF> als Trennzeichen, nur lokaler Host, UTF-8-Kodierung. (<CR><LF> = 13,10). [Datenquelle A] [Datenquelle B] und so weiter.
Neu	Anklicken, um eine neue Datenquelle zu erstellen.
Name	Name der Datenquelle.
Aktiviert	Datenquellen sind standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Datenquelle zu deaktivieren.
Zurücksetzen	Anklicken, um alle Einstellungen der ausgewählten Datenquelle zurückzusetzen. Der Name, der im Feld **Name** eingegeben wurde, bleibt.
Port	Die Portnummer der Datenquelle.
Protokolltypauswahl	Protokolle, die vom System beachtet und analysiert werden sollen, um generische Ereignisse zu erkennen: **Beliebig**: Sowohl TCP als auch UDP. **TCP**: Nur TCP. **UDP**: Nur UDP. TCP- und UDP-Pakete, die für generische Ereignisse verwendet werden,

Komponente	Voraussetzung
	dürfen Sonderzeichen enthalten, wie z. B. @, #, +, ~ und andere.
IP-Typauswahl	Auswählbare IP-Adressentypen: IPv4, IPv6 oder beide.
Separator-Bytes	Wählen Sie die Separator-Bytes aus, um einzelne generische Ereignisaufzeichnungen zu trennen. Der Standardwert für den Datenquelltyp **International** (siehe Datenquelle auf Seite 371) ist **13.10**.13.10 = <CR><IF>).
Echotypauswahl	Verfügbare Formate für die Echorückstrahlung: • **Echo-Statistiken**: Echo für das folgende Format: **[X],[Y],[Z],[Name generisches Ereignis]** **[X]** = Anforderungsnummer. **[Y]** = Zeichenzahl. **[Z]** = Anzahl der Übereinstimmungen mit einem generischen Ereignis. **[Name des generischen Ereignisses]** = Name, der im Feld **Name** eingegeben wurde. • **Echo bei allen Bytes**: Echo bei allen Bytes • **Kein Echo**: Unterdrückt alle Echos
Kodierungstypauswahl	Standardmäßig zeigt die Liste nur die wichtigsten Optionen. Aktivieren Sie das Kontrollkästchen **Alle anzeigen**, um alle verfügbaren Kodierungsoptionen anzuzeigen.
Alle anzeigen	Siehe vorheriger Eintrag.
Zulässige externe IPv4-Adressen	Bestimmen Sie die IP-Adressen, mit denen Management-Server kommunizieren können muss, um externe Ereignisse zu verwalten. Sie können damit auch IP-Adressen ausschließen, von denen Sie keine Daten möchten.
Zulässige externe IPv6-Adressen	Bestimmen Sie die IP-Adressen, mit denen Management-Server kommunizieren können muss, um externe Ereignisse zu verwalten. Sie können damit auch IP-Adressen ausschließen, von denen Sie keine Daten möchten.

Bereiche können in jeder der vier Positionen bestimmt werden, wie **100,105,110-120**. Zum Beispiel können alle Adressen auf dem 10.10-Netzwerk zugelassen werden von **10.10.[0-254].[0-254]** oder von **10.10.255.255**.

Site-Navigation: Sicherheit

Dieser Abschnitt beschreibt, wie Basisbenutzer erstellt und wie Rollen aufgestellt, Benutzerrechte für eine Rolle festgelegt und Benutzer zugewiesen werden.

Regeln (Erklärung)

Rollen bestimmen auf welche Geräte Nutzer zugreifen können. Rollen bestimmen auch Rechte und regeln die Sicherheit innerhalb des Videoverwaltungssystems. Zuerst fügen Sie Rollen hinzu, dann Benutzer und Gruppen und zuletzt ein Smart Client- und ein Management Client-Profil sowie weitere Standardprofile, die jeder Rolle angehören. Rollen, die Sie im System erstellen können, haben ihre eigenen Ansichtsgruppen im XProtect Smart Client, in denen ihre Ansichten erstellt und gespeichert werden.

Damit alle Rollen Zugriff auf Managementserver haben, muss die Sicherheitsberechtigung **Verbinden**, die sich in den **Einstellungen für Rollen** > **Managementserver** > auf der Registerkarte Registerkarte „Gesamtsicherheit“ (Rollen) auf Seite 381 befindet, aktiviert sein.

Sie fügen Benutzer und Gruppen der Rolle des **Administrators** genauso zu wie jeder anderen Rolle. Siehe Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen auf Seite 377).

Zusätzlich zur Rolle des **Administrators** können Sie so viele Rollen hinzufügen, wie erforderlich. Sie können z. B. verschiedene Rollen für die Benutzer von XProtect Smart Client festlegen, je nachdem auf welche Kameras Sie Zugriff erhalten sollen oder Einschränkungen ähnlicher Art. Um Rollen in Ihrem System zu erstellen, erweitern Sie **Sicherheit** > **Rollen**.

Rechte einer Rolle (Erklärung)

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

Wenn Sie in Ihrem System eine Rolle erstellen, können Sie der Rolle verschiedene Rechte für die Systemkomponenten oder -funktionen geben; die jeweilige Rolle kann auf diese dann zugreifen und sie verwenden. Sie könnten z. B. Rollen erstellen, die nur Rechte für Funktionen in XProtect Smart Client oder anderen Milestone-Anzeige-Clients haben, und somit nur die Rechte besitzen, bestimmte Kameras anzeigen zu lassen. Wenn Sie solche Rollen erstellen, sollten diese keine Rechte zum Zugriff auf oder die Verwendung von Management Client haben, aber Zugriff auf einen Teil oder alle Funktionen in XProtect Smart Client oder anderen

Clients. Um dies zu erreichen, erstellen Sie eine Rolle, die einige oder die meisten typischen Administratorenrechte hat, z. B. die Rechte, Kameras und Server hinzuzufügen oder zu entfernen und ähnliche Funktionen.

Sie können Rollen erstellen, die einige oder die meisten Rechte eines Systemadministrators haben. Das kann z. B. relevant sein, wenn Ihr Unternehmen zwischen Leuten unterscheiden will, die ein Subnetz des Systems verwalten dürfen und Leuten, die das gesamte System verwalten dürfen. Diese Funktion ermöglicht es Ihnen, differenzierte Administratorenrechte für den Zugriff, das Bearbeiten oder Ändern von zahlreichen Systemfunktionen zu erteilen, z. B. das Recht, die Server- oder Kameraeinstellungen in Ihrem System zu bearbeiten. Sie bestimmen diese Berechtigungen auf der Registerkarte Gesamtsicherheit (siehe Registerkarte „Gesamtsicherheit“ (Rollen) auf Seite 381). Damit der differenzierte Systemadministrator zumindest Management Client starten kann, müssen Sie der entsprechenden Rolle auf dem Management-Server eine Leseberechtigung erteilen.

Damit alle Rollen Zugriff auf Managementserver haben, muss die Sicherheitsberechtigung **Verbinden**, die sich in den **Einstellungen für Rollen** > **Managementserver** > auf der Registerkarte Registerkarte „Gesamtsicherheit“ (Rollen) auf Seite 381 befindet, aktiviert sein.

Sie können auch die gleichen Einschränkungen in der Benutzeroberfläche des Management Client s für jede Rolle vornehmen, indem Sie die Rolle mit einem Management Client-Profil verknüpfen, das die entsprechenden eingeschränkten Systemfunktionen von der Benutzeroberfläche hat. Siehe Site-Navigation: Clients: Management Client Profile auf Seite 303 für weitere Informationen.

Um einer Rolle solche differenzierten Administratorenrechte zu geben, muss die Person mit der standardmäßigen Rolle des Gesamtadministrators die Rolle unter **Sicherheit** > **Rollen > Registerkarte Info > Neu hinzufügen** erstellen. Wenn Sie die neue Rolle erstellen, können Sie die Rolle mit Ihren eigenen Profilen verknüpfen, genauso wie beim Erstellen einer anderen Rolle im System oder bei der Verwendung der Standardprofile des Systems. Für weitere Informationen, siehe Hinzufügen und Verwalten einer Rolle auf Seite 376.

Sobald Sie festgelegt haben, mit welchen Profilen Sie die Rolle verknüpfen möchten, gehen Sie auf die Registerkarte **Gesamtsicherheit**, um die Rechte der Rolle zu bestimmen.

Die Rechte, die Sie für eine Rolle einstellen können, sind zwischen Ihren Produkten unterschiedlich. Sie können nur einer Rolle in XProtect Corporate alle verfügbaren Rechte geben.

Benutzer (Erklärung)

Der Begriff **Benutzer** bezeichnet primär Benutzer, die sich über die Clients mit dem Überwachungssystem verbinden. Sie können solche Benutzer auf zwei verschiedene Weisen konfigurieren:

- Als **Basisnutzer**, Authentifizierung durch Benutzername und Passwort
- Als **Windows-Benutzer**, Authentifizierung auf Basis ihrer Windows-Anmeldung

Windows-Benutzer

Sie können Windows-Benutzer mithilfe von Active Directory hinzufügen. Active Directory (AD) ist ein Verzeichnisdienst, der von Microsoft für Windows-Domänennetzwerke implementiert wird. Dieser Dienst ist in den meisten Windows Server-Betriebssystemen enthalten. Er identifiziert die Ressourcen in einem Netzwerk, sodass Benutzer oder Anwendungen darauf zugreifen können. Active Directory verwendet die Konzepte von Benutzern und Gruppen.

Benutzer sind Active Directory-Objekte, Einzelpersonen werden durch ein Benutzerkonto dargestellt. Beispiel:

Gruppen sind Active Directory-Objekte mit mehreren Benutzern. In diesem Beispiel hat die Management-Gruppe drei Benutzer:

Gruppen können eine beliebige Anzahl an Benutzern beinhalten. Wenn Sie dem System eine Gruppe hinzufügen, fügen Sie alle Gruppenmitglieder auf einmal hinzu. Sobald Sie die Gruppe dem System hinzugefügt haben, werden alle Änderungen, die an der Gruppe in Active Directory vorgenommen wurden (z. B. neue Mitglieder, die Sie hinzufügen oder alte Mitglieder, die Sie später entfernen) sofort auf das System übertragen. Ein Benutzer kann Mitglied mehrerer Gruppen zugleich sein.

Wenn Sie Active Directory verwenden, um bestehende Benutzer- und Gruppeninformationen dem System hinzuzufügen, hat dies einige Vorteile:

- Benutzer und Gruppen werden zentral in Active Directory angelegt, deshalb müssen Sie Benutzerkonten nicht von Grund auf neu erstellen
- Sie brauchen die Benutzerauthentifizierung nicht auf dem System zu konfigurieren, da Active Directory die Authentifizierung regelt

Bevor Sie Benutzer und Gruppen über den Active Directory-Dienst hinzufügen können, muss in Ihrem Netzwerk ein Server vorhanden sein, auf dem Active Directory installiert ist.

Basisnutzer

Wenn Ihr System keinen Zugriff zu Active Directory hat, erstellen Sie einen Basisnutzer (siehe Benutzer (Erklärung) auf Seite 374). Informationen dazu, wie Basisnutzer erstellt werden, siehe Basisnutzer erstellen (siehe Erstellen von Basisnutzer auf Seite 424).

Hinzufügen und Verwalten einer Rolle

1. Erweitern Sie **Sicherheit** und klicken Sie mit der rechten Maustaste auf **Rollen**.
2. Wählen Sie **Rolle hinzufügen**. Das Dialogfeld **Rolle hinzufügen** öffnet sich.
3. Geben Sie einen Namen und eine Beschreibung für die neue Rolle ein und klicken Sie auf **OK**.
4. Die neue Rolle wird der Liste **Rollen** hinzugefügt. Standardmäßig ist eine neue Rolle nicht mit Benutzern oder Gruppen verknüpft, aber mit einigen Standardprofilen.
5. Um verschiedene Smart Client- und Management Client-Profile, Beweissicherungsprofile oder Zeitprofile auszuwählen, klicken Sie auf die Dropdown-Listen.
6. Sie können jetzt Benutzer/Gruppen der Rolle zuweisen und festlegen, auf welche Systemfunktionen sie Zugriff haben.

Für weitere Informationen siehe Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen auf Seite 377 und Rolleneinstellungen auf Seite 379.

Kopieren, Umbenennen oder Löschen einer Rolle

Kopieren einer Rolle

Wenn Sie eine Rolle mit komplexen Einstellungen und/oder Rechten haben und eine gleiche oder ähnliche Rolle benötigen, kann es einfacher sein, die bereits bestehende Rolle zu kopieren und geringe Anpassungen an der Kopie vorzunehmen, als eine neue Rolle von Grund auf neu zu erstellen.

1. Erweitern Sie **Sicherheit**, klicken Sie auf **Rollen**, klicken Sie mit der rechten Maustaste auf die gewünschte Rolle und wählen Sie **Rolle kopieren**.
2. Es erscheint ein Dialogfenster; geben Sie der kopierten Rolle einen neuen einmaligen Namen und eine Beschreibung.
3. Klicken Sie auf **OK**.

Umbenennen einer Rolle

Wenn Sie eine Rolle umbenennen, ändert sich damit nicht der Name der Ansichtsgruppe, die auf der Rolle basiert.

1. Erweitern Sie **Sicherheit** und klicken Sie mit der rechten Maustaste auf **Rollen**.
2. Klicken Sie mit der rechten Maustaste auf die gewünschte Rolle und wählen Sie **Rolle umbenennen**.
3. Es erscheint ein Dialogfenster; ändern Sie den Namen der Rolle.
4. Klicken Sie auf **OK**.

Löschen einer Rolle

1. Erweitern Sie **Sicherheit** und klicken Sie auf **Rollen**.
2. Klicken Sie mit der rechten Maustaste auf die zu löschende Rolle und wählen Sie **Rolle löschen**.
3. Klicken Sie auf **Ja**.

> Wenn Sie eine Rolle löschen, entfernen Sie damit nicht die Ansichtsgruppe, die auf der Rolle basiert.

Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen

Um Windows-Benutzer oder -Gruppen oder Basisnutzer Rollen zuzuweisen oder aus Rollen zu entfernen:

1. Erweitern Sie **Sicherheit** und wählen Sie **Rollen**. Wählen Sie dann die gewünschte Rolle im Bereich **Übersicht**:
2. Wählen Sie unten im Bereich **Eigenschaften** die Registerkarte **Benutzer und Gruppen**.
3. Klicken Sie auf **Hinzufügen** und wählen Sie zwischen **Windows-Benutzer** und **Basisnutzer**.

Zuweisen von Windows-Benutzern und -Gruppen zu einer Rolle

1. Wählen Sie **Windows-Benutzer**. Dadurch öffnen sich die Dialogfelder **Benutzer auswählen** und **Computer und Gruppen**:
2. Verifizieren Sie, dass der erforderliche Objekttyp festgelegt wurde. Wenn Sie z. B. einen Computer hinzufügen möchten, klicken Sie auf **Objekttypen** und markieren Sie **Computer**. Verifizieren Sie, dass die gewünschte Domäne im Feld **Von diesem Speicherort** festgelegt ist. Wenn nicht, klicken Sie auf **Standorte**, um zur gewünschten Domäne zu navigieren.
3. In das Feld **Auszuwählende Objektnamen eingeben** geben Sie die gewünschten Benutzernamen, Initialen oder andere Identifikationsarten ein, die Active Directory erkennen kann. Verwenden Sie die Funktion **Namen überprüfen**, um zu verifizieren, dass Active Directory die Namen oder Initialen erkennt, die Sie eingegeben haben. Alternativ können Sie die Funktion **"Erweitert..."** verwenden, um nach Benutzern oder Gruppen zu suchen.

4. Klicken Sie auf **OK**. Die ausgewählten Benutzer/Gruppen werden jetzt der Benutzerliste der Registerkarte **Benutzer und Gruppen** hinzugefügt, denen Sie die ausgewählte Rolle zugeteilt haben. Sie können weitere Benutzer und Gruppen hinzufügen, indem sie mehrere Namen eingeben, die mittels eines Strichpunkts (;) voneinander abgetrennt sind.

Zuweisen von Basisnutzer zu einer Rolle

1. Wählen Sie **Basisnutzer**. Das Dialogfeld **Basisnutzer zum Hinzufügen zur Rolle auswählen** öffnet sich:
2. Wählen die Basisnutzer aus, die Sie dieser Rolle zuweisen möchten.
3. Optional: Klicken Sie auf **Neu**, um einen neuen Basisnutzer zu erstellen.
4. Klicken Sie auf **OK**. Die ausgewählten Basisnutzer werden jetzt der Basisnutzerliste der Registerkarte **Benutzer und Gruppen** hinzugefügt, denen Sie die ausgewählte Rolle zugeteilt haben.

Entfernen von Benutzern und Gruppen aus einer Rolle

1. Wählen Sie auf der Registerkarte **Benutzer und Gruppen** den Benutzer oder die Gruppe aus, die Sie entfernen möchten, und klicken Sie auf **Entfernen** im unteren Teil der Registerkarte. Sie können mehrere Benutzer oder Gruppen oder bei Bedarf eine Kombination von Gruppen und einzelnen Benutzern auswählen.
2. Bestätigen Sie, dass Sie die ausgewählten Benutzer und/oder Gruppen entfernen möchten. Klicken Sie auf **Ja**.

> Ein Benutzer kann auch Rollen durch Gruppenmitgliedschaften haben. Wenn das der Fall ist, können Sie den einzelnen Benutzer nicht aus der Rolle entfernen. Gruppenmitglieder können auch als Personen Rollen haben. Um herauszufinden, welche Rollen Benutzer, Gruppen oder einzelne Gruppenmitglieder haben, verwenden Sie die Funktion **Effektive Rollen anzeigen**.

Effektive Rollen anzeigen

Mit der Funktion „Effektive Rollen" können Sie alle Rollen eines ausgewählten Benutzers oder einer ausgewählten Gruppe ansehen. Das ist praktisch bei der Verwendung von Gruppen und es ist die einzige Methode zum Überprüfen, welche Rollen ein bestimmter Benutzer hat.

1. Öffnen Sie das Fenster **Effektive Rollen**, indem Sie **Sicherheit** erweitern, mit der rechten Maustaste auf **Rollen** klicken und dann **Effektive Rollen** auswählen.
2. Wenn Sie Informationen über einen Basisnutzer erhalten möchten, geben Sie den Namen in das Feld **Benutzername** ein. Klicken Sie auf **Aktualisieren**, um die Rollen des Benutzers anzuzeigen.
3. Wenn Sie Windows-Benutzer oder -Gruppen in Active Directory verwenden, klicken Sie auf die **...**-Schaltfläche zum Durchsuchen. Wählen Sie den Objekttyp, geben Sie den Namen ein und klicken Sie dann auf **OK**. Die Rollen des Benutzers werden automatisch angezeigt.

Rolleneinstellungen

Registerkarte „Info“ (Rollen)

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

Auf der Registerkarte **Info** einer Rolle können Sie folgende Einstellungen vornehmen:

Name	Beschreibung
Name	Geben Sie einen Namen für die Rolle ein.
Beschreibung	Geben Sie eine Beschreibung für die Rolle ein.
Management Client-Profil	Wählen Sie ein Management Client-Profil zum Verknüpfen mit der Rolle aus. Dies können Sie nicht auf die standardmäßige Rolle des **Administrators** anwenden. Erfordert Berechtigungen zur Verwaltung der Sicherheit auf dem Management-Server.
Smart Client-Profil	Wählen Sie ein Smart Client-Profil zum Verknüpfen mit der Rolle aus. Erfordert Berechtigungen zur Verwaltung der Sicherheit auf dem Management-Server.
Standardzeitprofil	Wählen Sie ein Standardzeitprofil zum Verknüpfen mit der Rolle aus. Dies können Sie nicht auf die standardmäßige Rolle des **Administrators** anwenden.
Beweissicherungsprofil	Wählen Sie ein Beweissicherungsprofil zum Verknüpfen mit der Rolle aus.
Smart Client Anmeldung innerhalb des Zeitprofils	Wählen Sie ein Zeitprofil aus, über das sich der XProtect Smart Client-Benutzer anmelden darf, der mit dieser Rolle verknüpft ist. Sollte der XProtect Smart Client-Benutzer angemeldet sein, wenn die Zeit abläuft,

Name	Beschreibung
	wird diese Person automatisch abgemeldet. Dies können Sie nicht auf die standardmäßige Rolle des **Administrators** anwenden.
Smart Client-Anmeldung erlauben	Aktivieren Sie das Kontrollkästchen, um mit dieser Rolle verknüpften Benutzern zu erlauben, sich auf XProtect Smart Client anzumelden. Der Zugriff auf Smart Client ist standardmäßig zugelassen. Deaktivieren Sie das Kontrollkästchen, um den Zugriff auf XProtect Smart Client zu verweigern.
XProtect Mobile-Client-Anmeldung erlauben	Aktivieren Sie das Kontrollkästchen, um mit dieser Rolle verknüpften Benutzern zu erlauben, sich auf dem XProtect Mobile-Client anzumelden. Der Zugriff auf den XProtect Mobile-Client ist standardmäßig zugelassen. Deaktivieren Sie das Kontrollkästchen, um den Zugriff auf den XProtect Mobile-Client zu verweigern.
XProtect Web Client-Anmeldung erlauben	Aktivieren Sie das Kontrollkästchen, um mit dieser Rolle verknüpften Benutzern zu erlauben, sich auf XProtect Web Client anzumelden. Der Zugriff auf XProtect Web Client ist standardmäßig zugelassen. Deaktivieren Sie das Kontrollkästchen, um den Zugriff auf XProtect Web Client zu verweigern.
Anmelde-Autorisierung erforderlich	Aktivieren Sie das Kontrollkästchen, um die Anmelde-Autorisierung mit der Rolle zu verknüpfen. Das bedeutet, dass XProtect Smart Client oder der Management Client nach einer zweiten Autorisierung fragt, meist durch einen Superuser oder Manager, wenn sich der Benutzer anmeldet. Um es Administratoren zu ermöglichen, Benutzer zu autorisieren, konfigurieren Sie die Option **Benutzer autorisieren** auf der Registerkarte **Gesamtsicherheit** des Management-Servers. Dies können Sie nicht auf die standardmäßige Rolle des **Administrators** anwenden.
Benutzer während PTZ-Sitzungen anonymisieren	Aktivieren Sie das Kontrollkästchen, um die Namen der Benutzer auszublenden, die mit dieser Rolle verknüpft sind, wenn sie PTZ-Sitzungen regeln.

Benutzer und Gruppen-Registerkarte (Rollen)

Auf der Registerkarte **Benutzer und Gruppen** weisen Sie Benutzer und Gruppen Rollen zu (siehe Zuweisen/Entfernen von Benutzern und Gruppen zu/aus Rollen auf Seite 377). Sie können Windows-Benutzer und -Gruppen oder Basisbenutzer zuweisen (siehe Benutzer (Erklärung) auf Seite 374).

Name	Beschreibung
Name	Zeigt den Namen des Benutzers oder der Gruppe an, die mit dieser Regel verknüpft ist.
Beschreibung	Zeigt die Beschreibung an, die Sie beim Erstellen des Basisnutzers eingegeben haben.

Registerkarte „Gesamtsicherheit“ (Rollen)

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

Auf der Registerkarte **Gesamtsicherheit** legen Sie die Gesamtrechte für Rollen fest. Definieren Sie für jede in Ihrem System verfügbare Komponente Zugriffsrechte für die Rollen, indem Sie **Zulassen** oder **Verweigern** auswählen. Wenn einer Rolle der Zugriff auf eine Komponente verwehrt wird, so ist die betreffende Komponente auf der Registerkarte **Gesamtsicherheit** für einen Benutzer in dieser Rolle nicht sichtbar.

Die Reigisterkarte **Globale Sicherheit** ist in der Gratis-XProtect Essential+ nicht verfügbar.

Sie können für XProtect Corporate mehr Zugriffsberechtigungen festlegen als für XProtect Expert, XProtect Professional+, und XProtect Express+. Das ist so, weil Sie in XProtect Corporate nur differenzierte Administrator-Rechte einsetzen können, während Sie Gesamtrechte für eine Rolle einsetzen können, die einen XProtect Smart Client-, XProtect Web Client- oder XProtect Mobile-Client in allen Produkten benutzt.

Die Gesamtsicherheitseinstellungen gelten nur für den aktuellen Standort.

Wenn Sie einem Nutzer mehr als eine Rolle zuweisen und **Verweigern** als Sicherheitseinstellung für eine Rolle auswählen und für eine andere **Zulassen**, überschreibt die Einstellung **Verweigern** die Einstellung **Zulassen**.

Die folgenden Beschreibungen zeigen, was bei jeder einzelnen Berechtigung für die verschiedenen Systemkomponenten passiert, wenn Sie für die betreffende Rolle **Zulassen** auswählen. Bei Verwendung von XProtect Corporate sehen Sie unter jeder Systemkomponente, welche Einstellungen **nur** für Ihr System verfügbar sind.

Für jede Systemkomponente oder -funktion kann der Gesamtsystemadministrator die Kontrollkästchen **Zulassen** oder **Verweigern** verwenden, um Sicherheitsberechtigungen für die Rolle einzurichten. Sicherheitsberechtigungen, die Sie hier einrichten, werden für die gesamte Systemkomponente oder -funktion eingerichtet. Wenn Sie z.B. das Kontrollkästchen **Verweigern** bei **Kameras** auswählen, sind für die Rolle keine der zum System hinzugefügten Kameras verfügbar. Wenn Sie dagegen das Kontrollkästchen **Zulassen** aktivieren, sind für die Rolle alle zum System hinzugefügten Kameras sichtbar. Die Auswahl von **Zulassen** oder **Verweigern** für Ihre Kameras bewirkt, dass die Kameraeinstellungen auf der Registerkarte **Gerät** Ihre Auswahl auf der Registerkarte **Gesamtsicherheit** übernehmen, sodass für die jeweilige Rolle entweder alle Kameras verfügbar oder nicht verfügbar sind.

Wenn Sie Sicherheitsberechtigungen für **einzelne** Kameras oder Ähnliches festlegen möchten, können Sie diese individuellen Berechtigungen nur dann auf der Registerkarte der betreffenden Systemkomponente oder -funktion einstellen, wenn Sie **keine Gesamtberechtigungen** für die Systemkomponente oder -funktion auf der Registerkarte **Gesamtsicherheit** festgelegt haben.

Die folgenden Beschreibungen gelten auch für die Rechte, die Sie über die MIP SDKs konfigurieren können.

> ⚠ Wenn Sie Ihre Basislizenz von XProtect Corporate auf eines der anderen Produkte, wechseln möchten, stellen Sie sicher, dass Sie alle Sicherheitsrechte entfernen, die nur für XProtect Corporate verfügbar sind. Wenn Sie diese Rechte nicht entfernen, können Sie nicht wechseln.

Management Server

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	
Verbinden	Dies ermöglicht es den Benutzern, sich mit Managementserver zu verbinden. Die Erlaubnis ist standardmäßig aktiviert. Sie können die Erlaubnis für die Verbindung für Rollen für Wartungszwecke vorübergehend verweigern und dann den Zugriff auf das System erneut beantragen. ⚠ Diese Erlaubnis muss ausgewählt werden, um den Zugriff zum System zuzulassen.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
Lesen	Das Recht zur Nutzung einer großen Auswahl von Funktionen, darunter: • Anmelden mit dem Management Client • Liste aktueller Aufgaben • Server-Protokolle Darüber hinaus ermöglicht es den Zugriff auf: • Fernzugriffsdienste • Smart Client Profile • Management Client Profile • Matrix • Zeitprofile • Registrierte Server und Service Registration API	Nur verfügbar
Bearbeiten	Das Recht, Daten bei zahlreichen Funktionen zu bearbeiten, darunter: • Optionen • Lizenzverwaltung Benutzer können außerdem das Folgende erstellen, löschen und bearbeiten: • Fernzugriffsdienste • Gerätegruppen • Matrix • Zeitprofile • Benachrichtigungsprofile • Registrierte Server	Nur verfügbar

Sicherheitsrecht	Beschreibung	XProtect Corporate
	Das Recht, beim Konfigurieren des Netzwerks auf dem Aufzeichnungsserver lokale IP-Bereiche zu konfigurieren.	
Systemmonitor	Das Recht, die Daten des Systemmonitors anzuzeigen.	Nur verfügbar
Status-API	Das Recht, Abfragen für die Status-API auf dem Aufzeichnungsserver durchzuführen. Das heißt, die Rolle mit diesem Recht hat eine Leseberechtigung für den Status der Elemente auf dem Aufzeichnungsserver.	
Hierarchie der föderalen Standorte verwalten	Das Recht, den aktuellen Standort zu anderen Standorten in einer Hierarchie der föderalen Standorte hinzuzufügen bzw. davon zu lösen. Wenn Sie diese Berechtigung nur für den untergeordneten Standort zulassen, kann der Benutzer dennoch den Standort vom übergeordneten Standort lösen.	Nur verfügbar
Sicherung von Konfiguration	Aktiviert das Recht, mithilfe der Sicherungs-/Wiederherstellungsfunktion des Systems Sicherungen der Systemkonfiguration vorzunehmen und Funktionalität wieder herzustellen.	Nur verfügbar
Benutzer autorisieren	Das Recht, Benutzer zu autorisieren, wenn sie um eine zweite Anmeldung beim XProtect Smart Client oder Management Client gebeten werden. Auf der Registerkarte **Info** legen Sie fest, ob eine Rolle eine Anmeldungsautorisierung erfordert.	
Sicherheit verwalten	Das Recht, Berechtigungen für den Management-Server zu verwalten. Benutzer können außerdem folgende Funktionsbereiche erstellen, löschen und bearbeiten:	Nur verfügbar

Sicherheitsrecht	Beschreibung	XProtect Corporate
	• Rollen • Basisnutzer • Smart Client Profile • Management Client Profile	

Aufzeichnungsserver

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Bearbeiten	Aktiviert das Recht, Eigenschaften auf den Aufzeichnungsservern zu bearbeiten, ausgenommen Netzwerkkonfigurationseinstellungen, die das Recht zum Bearbeiten direkt auf dem Management-Server erfordern.
Löschen	Das Recht, Aufzeichnungsserver zu löschen. Hierfür müssen Sie dem Benutzer auch Löschberechtigungen für Folgendes geben: • Hardwaresicherheitsgruppe, wenn Sie Hardware zum Aufzeichnungsserver hinzugefügt haben Wenn eines der Geräte auf dem Aufzeichnungsserver Beweissicherungen enthält, können Sie den Aufzeichnungsserver nur löschen, wenn er offline ist.
Hardware verwalten	Das Recht, Hardware zu Aufzeichnungsservern hinzuzufügen.
Speicher verwalten	Das Recht, Speichercontainer auf dem Aufzeichnungsserver zu verwalten, d. h. Speichercontainer zu erstellen, zu löschen, zu verschieben und zu leeren.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Aufzeichnungsserver zu verwalten.

Failover-Server

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Das Recht, Failover-Server im Management Client anzuzeigen und aufzurufen.
Bearbeiten	Aktiviert das Recht, Failover-Server im Management Client zu erstellen, zu aktualisieren, zu löschen, zu verschieben und zu aktivieren/deaktivieren.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für die Failover-Server zu verwalten.

Mobile Server

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Das Recht, Mobile Server im Management Client anzuzeigen und aufzurufen.
Bearbeiten	Das Recht, Mobile Server im Management Client zu bearbeiten und zu löschen.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für die Mobile Server zu verwalten.
Erstellen	Das Recht, Mobile Server zum System hinzuzufügen.

Hardware

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Bearbeiten	Das Recht, Eigenschaften von Hardware zu bearbeiten.
Löschen	Das Recht, Hardware zu löschen. Wenn eines der Hardwaregeräte Beweissicherungen enthält, können Sie die Hardware nur löschen, wenn der Aufzeichnungsserver offline ist.
Treiberbefehle	Das Recht besondere Befehle an die Treiber zu senden und dadurch Funktionen und Konfiguration auf dem Gerät selbst zu steuern. Das **Treiberbefehle**-Recht gilt nur für speziell entwickelte MIP Plug-ins in den Clients. Es steuert keine Aufgaben, die Standardkonfiguration betreffend.
Passwörter anzeigen	Erteilt die Berechtigung, Passwörter für Hardwaregeräte in der Dialogbox **Hardware bearbeiten** zu sehen.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für die Hardware zu verwalten.

Kameras

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	
Lesen	Das Recht, Kameraeräte in den Clients und im Management Client anzuzeigen.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
Bearbeiten	Das Recht, Kameraeigenschaften im Management Client zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Kameras.	Nur verfügbar
Live ansehen	Das Recht, Live-Video von Kameras in den Clients und im Management Client anzuzeigen.	
Wiedergabe	Das Recht, aufgezeichnete Videos von Kameras in allen Clients wiederzugeben.	
Fernaufzeichnungen abrufen	Das Recht, Aufzeichnungen in den Clients von Kameras an Remote-Systemen oder von lokalen Speichern in Kameras abzurufen.	
Sequenzen lesen	Aktiviert die Berechtigung zum Lesen der Sequenzinformationen, z. B. in Bezug auf das Abspielen von Videoaufzeichnungen in den Clients.	
intelligente Suche	Das Recht zur Verwendung der Smart Search-Funktion in den Clients.	
Exportieren	Das Recht zum Exportieren von Aufzeichnungen von den Clients.	
Lesezeichen erstellen	Das Recht zum Erstellen von Lesezeichen in aufgezeichneten und Live-Videos in den Clients.	
Lesezeichen lesen	Das Recht zum Suchen nach und Lesen von Lesezeichendetails in den Clients.	
Lesezeichen bearbeiten	Das Recht zum Bearbeiten von Lesezeichen in den Clients.	
Lesezeichen löschen	Das Recht zum Löschen von Lesezeichen in den Clients.	
Beweissicherungen erstellen und	Das Recht zum Erstellen und Erweitern von Beweissicherungen in den Clients.	Nur verfügbar

Sicherheitsrecht	Beschreibung	XProtect Corporate
erweitern		
Beweissicherungen lesen	Das Recht zum Durchsuchen und Lesen von Beweissicherungen in den Clients.	Nur verfügbar
Beweissicherungen löschen und reduzieren	Das Recht zum Löschen und Reduzieren von Beweissicherungen in den Clients.	Nur verfügbar
Manuelle Aufzeichnung starten	Das Recht zum Starten manueller Videoaufzeichnungen in den Clients.	
Manuelle Aufzeichnung stoppen	Das Recht zum Stoppen manueller Videoaufzeichnungen in den Clients.	
AUX-Befehle	Das Recht zum Verwenden von Hilfsbefehlen (AUX) für die Kamera von den Clients. **AUX-Befehle** bieten Benutzern z. B. die Möglichkeit, Wischer an Kameras zu steuern, die über einen Videoencoder verbunden sind. Mit Kameras verknüpfte Geräte, die über Hilfsanschlüsse verbunden sind, werden vom Client gesteuert.	
Manuelles PTZ	Das Recht zum Verwenden von PTZ-Funktionen für PTZ-Kameras in den Clients und im Management Client.	
PTZ-Preset-Positionen oder Wachrundgangprofil aktivieren	Das Recht, PTZ-Kameras in Preset Positionen zu bewegen, Wachrundgangprofile zu starten/stoppen und einen Wachrundgang in den Clients und im Management Client anzuhalten. Wenn Sie möchten, dass diese Rolle weitere PTZ-Funktionen für die Kamera verwenden kann, müssen Sie das Recht **Manuelles PTZ** aktivieren.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
PTZ-Voreinstellungen oder Wachrundgangprofile verwalten	Das Recht zum Hinzufügen, Bearbeiten und Löschen von PTZ-Preset-Positionen und Wachrundgangprofilen für PTZ-Kameras in den Clients und im Management Client. Wenn Sie möchten, dass diese Rolle weitere PTZ-Funktionen für die Kamera verwenden kann, müssen Sie das Recht **Manuelles PTZ** aktivieren.	
PTZ-Voreinstellungen sperren/entsperren	Das Recht zum Sperren und Entsperren von PTZ-Preset-Positionen im Management Client. Ermöglicht oder verhindert, dass andere Benutzer Preset-Positionen in den Clients und im Management Client ändern können.	Nur verfügbar
PTZ-Sitzungen reservieren	Das Recht, PTZ-Kameras in den Clients und im Management Client in den Modus „reservierte PTZ-Sitzung“ zu schalten. In einer reservierten PTZ-Sitzung können andere Benutzer mit einer höheren PTZ-Priorität nicht die Kontrolle übernehmen. Wenn Sie möchten, dass diese Rolle weitere PTZ-Funktionen für die Kamera verwenden kann, müssen Sie das Recht **Manuelles PTZ** aktivieren.	Nur verfügbar
PTZ-Sitzungen freigeben	Das Recht, PTZ-Sitzungen anderer Benutzer über den Management Client freizugeben. Sie können Ihre eigenen PTZ-Sitzungen jederzeit ohne diese Berechtigung freigeben.	Nur verfügbar
Aufzeichnungen löschen	Das Recht, gespeicherte Videoaufzeichnungen über den Management Client aus dem System zu löschen.	Nur verfügbar
Privatzonenmasken aufheben	Aktiviert das Recht, Privatzonenmasken in XProtect Smart Client zeitweise aufzuheben. Es aktiviert ebenso das Recht, anderen XProtect Smart Client-Nutzern die Aufhebung von Privatzonenmasken zu genehmigen.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
	Die Aufhebung von Privatzonenmasken gilt nur für Privatzonenmasken, die im Management Client als aufhebbar konfiguriert sind.	
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen im Management Client für die Kamera zu verwalten.	Nur verfügbar

Mikrofone

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	
Lesen	Das Recht, Mikrofongeräte in den Clients und im Management Client anzuzeigen.	
Bearbeiten	Das Recht, Mikrofoneigenschaften im Management Client zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Mikrofonen.	Nur verfügbar
Abhören	Das Recht, Live-Audio von Mikrofonen in den Clients und im Management Client abzuhören.	
Wiedergabe	Das Recht, Audioaufzeichnungen von Mikrofonen in den Clients wiederzugeben.	
Fernaufzeichnungen abrufen	Das Recht, Aufzeichnungen in den Clients von Mikrofonen an Remote-Systemen oder von lokalen Speichern in Kameras abzurufen.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
Sequenzen lesen	Aktiviert die Berechtigung zum Lesen der Sequenzinformationen, z. B. in Bezug auf die Registerkarte **Abspielen** in den Clients.	
Exportieren	Das Recht zum Exportieren von Aufzeichnungen von den Clients.	
Lesezeichen erstellen	Das Recht zum Erstellen von Lesezeichen in den Clients.	
Lesezeichen lesen	Das Recht zum Suchen nach und Lesen von Lesezeichendetails in den Clients.	
Lesezeichen bearbeiten	Das Recht zum Bearbeiten von Lesezeichen in den Clients.	
Lesezeichen löschen	Das Recht zum Löschen von Lesezeichen in den Clients.	
Beweissicherungen erstellen und erweitern	Das Recht zum Erstellen oder Erweitern von Beweissicherungen in den Clients.	Nur verfügbar
Beweissicherungen lesen	Das Recht zum Durchsuchen und Lesen von Beweissicherungsdetails in den Clients.	Nur verfügbar
Beweissicherungen löschen und reduzieren	Das Recht zum Löschen und Reduzieren von Beweissicherungen in den Clients.	Nur verfügbar
Manuelle Aufzeichnung starten	Das Recht zum Starten manueller Audioaufzeichnungen in den Clients.	
Manuelle Aufzeichnung stoppen	Das Recht zum Stoppen manueller Audioaufzeichnungen in den Clients.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
Aufzeichnungen löschen	Das Recht, gespeicherte Aufzeichnungen aus dem System zu löschen.	Nur verfügbar
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Mikrofone im Management Client zu verwalten.	Nur verfügbar

Lautsprecher

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	
Lesen	Das Recht, Lautsprechergeräte in den Clients und im Management Client anzuzeigen.	
Bearbeiten	Das Recht, Lautsprechereigenschaften im Management Client zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Lautsprechern.	Nur verfügbar
Abhören	Das Recht, Live-Audio über Lautsprecher in den Clients und im Management Client abzuhören.	
Sprechen	Das Recht, über die Lautsprecher in den Clients zu sprechen.	
Wiedergabe	Das Recht, Audioaufzeichnungen über Lautsprecher in den Clients wiederzugeben.	
Fernaufzeichnungen abrufen	Das Recht, Aufzeichnungen in den Clients von Lautsprechern an Remote-Systemen oder von lokalen Speichern in Kameras abzurufen.	
Sequenzen lesen	Das Recht zur Nutzung der Sequenzfunktion beim	

Sicherheitsrecht	Beschreibung	XProtect Corporate
	Durchsuchen von Audioaufzeichnungen von Lautsprechern in den Clients.	
Exportieren	Das Recht, Audioaufzeichnungen von Lautsprechern in den Clients zu exportieren.	
Lesezeichen erstellen	Das Recht zum Erstellen von Lesezeichen in den Clients.	
Lesezeichen lesen	Das Recht zum Suchen nach und Lesen von Lesezeichendetails in den Clients.	
Lesezeichen bearbeiten	Das Recht zum Bearbeiten von Lesezeichen in den Clients.	
Lesezeichen löschen	Das Recht zum Löschen von Lesezeichen in den Clients.	
Beweissicherungen erstellen und erweitern	Aktiviert das Recht zum Erstellen oder Erweitern von Beweissicherungen zum Schutz von Audioaufzeichnungen in den Clients.	Nur verfügbar
Beweissicherungen lesen	Aktiviert das Recht, Audioaufzeichnungen anzuzeigen, die in den Clients durch Beweissicherungen geschützt sind.	Nur verfügbar
Beweissicherungen löschen und reduzieren	Aktiviert das Recht zum Löschen oder Reduzieren von Beweissicherungen für geschützte Audioaufzeichnungen in den Clients.	Nur verfügbar
Manuelle Aufzeichnung starten	Das Recht zum Starten manueller Audioaufzeichnungen in den Clients.	
Manuelle Aufzeichnung stoppen	Das Recht zum Stoppen manueller Audioaufzeichnungen in den Clients.	
Aufzeichnungen	Das Recht, gespeicherte Aufzeichnungen aus dem System	Nur verfügbar

Sicherheitsrecht	Beschreibung	XProtect Corporate
löschen	zu löschen.	
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Lautsprecher im Management Client zu verwalten.	Nur verfügbar

Metadaten

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	
Lesen	Das Recht zum Empfangen von Metadaten in den Clients.	
Bearbeiten	Das Recht, Metadateneigenschaften im Management Client zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Metadatengeräten.	Nur verfügbar
Live	Das Recht zum Empfangen von Live-Metadaten von Kameras in den Clients.	
Wiedergabe	Aktiviert das Recht, aufgezeichnete Daten von Metadatengeräten in den Clients wiederzugeben.	
Fernaufzeichnungen abrufen	Das Recht, Aufzeichnungen in den Clients von Metadatengeräten an Remote-Systemen oder von lokalen Speichern in Kameras abzurufen.	
Sequenzen lesen	Aktiviert die Berechtigung zum Lesen der Sequenzinformationen, z. B. in Bezug auf die Registerkarte **Abspielen** in den Clients.	
Exportieren	Das Recht zum Exportieren von Aufzeichnungen in den Clients.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
Beweissicherungen erstellen und erweitern	Das Recht zum Erstellen von Beweissicherungen in den Clients.	Nur verfügbar
Beweissicherungen lesen	Das Recht, Beweissicherungen in den Clients anzuzeigen.	Nur verfügbar
Beweissicherungen löschen und reduzieren	Das Recht zum Löschen und Reduzieren von Beweissicherungen in den Clients.	Nur verfügbar
Manuelle Aufzeichnung starten	Aktiviert das Recht manuelle Metadatenaufzeichnungen in den Clients zu starten.	
Manuelle Aufzeichnung stoppen	Aktiviert das Recht manuelle Metadatenaufzeichnungen in den Clients zu stoppen.	
Aufzeichnungen löschen	Das Recht, gespeicherte Aufzeichnungen aus dem System zu löschen.	Nur verfügbar
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Metadaten im Management Client zu verwalten.	Nur verfügbar

Eingang

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	Nur verfügbar
Lesen	Das Recht, Eingabegeräte in den Clients und im Management Client anzuzeigen.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
Bearbeiten	Das Recht, Eigenschaften von Eingabegeräten im Management Client zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Eingabegeräten.	Nur verfügbar
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Eingabegeräte im Management Client zu verwalten.	Nur verfügbar

Ausgang

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	
Lesen	Das Recht, Ausgabegeräte in den Clients anzuzeigen.	
Bearbeiten	Das Recht, Eigenschaften von Ausgabegeräten im Management Client zu bearbeiten. Ermöglicht Benutzern außerdem das Aktivieren oder Deaktivieren von Ausgabegeräten.	Nur verfügbar
Aktivieren	Das Recht zum Aktivieren von Ausgängen in den Clients.	
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Ausgabegeräte im Management Client zu verwalten.	Nur verfügbar

Smart Wall

Folgende Einstellungen sind nur in XProtect Expert und XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	
Lesen	Das Recht, Smart Walls in den Clients anzuzeigen.	
Bearbeiten	Das Recht, Eigenschaften für Smart Wall im Management Client zu bearbeiten.	Nur verfügbar
Löschen	Das Recht, vorhandene Smart Walls im Management Client zu löschen.	Nur verfügbar
Bedienen	Das Recht zum Aktivieren und Bearbeiten von Smart Walls, z. B. um Voreinstellungen zu ändern und zu aktivieren oder um Kameras in Ansichten in den Clients und in den Management Client zu übernehmen.	
Smart Wall Erstellen	Das Recht, neue Smart Walls im Management Client zu erstellen.	Nur verfügbar
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen in Management Client für Smart Wall zu verwalten.	Nur verfügbar
Wiedergabe	Das Recht, aufgezeichnete Daten aus Smart Walls in den Clients wiederzugeben.	

Ansichtsgruppen

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	
Lesen	Das Recht, Ansichtsgruppen in den Clients und im Management Client anzuzeigen. Ansichtsgruppen werden im Management Client erstellt.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
Bearbeiten	Das Recht, Eigenschaften für die Ansichtsgruppen im Management Client zu bearbeiten.	Nur verfügbar
Löschen	Das Recht, Ansichtsgruppen im Management Client zu löschen.	
Bedienen	Aktiviert das Recht, Ansichtsgruppen im XProtect Smart Client zum Erstellen und Löschen von Untergruppen sowie Ansichten zu verwenden.	
Ansichtsgruppe erstellen	Das Recht, Ansichtsgruppen im Management Client zu erstellen.	Nur verfügbar
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Ansichtsgruppen im Management Client zu verwalten.	Nur verfügbar

Benutzerdefinierte Ereignisse

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	
Lesen	Das Recht, benutzerdefinierte Ereignisse in den Clients anzuzeigen.	
Bearbeiten	Das Recht, Eigenschaften für benutzerdefinierte Ereignisse im Management Client zu bearbeiten.	Nur verfügbar
Löschen	Das Recht, benutzerdefinierte Ereignisse im Management Client zu löschen.	Nur verfügbar
Auslöser	Das Recht, benutzerdefinierte Ereignisse in den Clients auszulösen.	

Sicherheitsrecht	Beschreibung	XProtect Corporate
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für benutzerdefinierte Ereignisse im Management Client zu verwalten.	Nur verfügbar
Benutzerdefiniertes Ereignis erstellen	Das Recht, neue benutzerdefinierte Ereignisse im Management Client zu erstellen.	Nur verfügbar

Analyseereignisse

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Das Recht, Analyseereignisse im Management Client anzuzeigen.
Bearbeiten	Das Recht, Eigenschaften für Analyseereignisse im Management Client zu bearbeiten.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Analyseereignisse im Management Client zu verwalten.

Generische Ereignisse

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Das Recht, generische Ereignisse in den Clients und im Management Client anzuzeigen.
Bearbeiten	Das Recht, Eigenschaften für generische Ereignisse im Management Client zu

Sicherheitsrecht	Beschreibung
	bearbeiten.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für generische Ereignisse im Management Client zu verwalten.

Matrix

Sicherheitsrecht	Beschreibung	XProtect Corporate
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.	Nur verfügbar
Lesen	Das Recht, von den Clients Video auszuwählen und an den Matrix-Empfänger zu senden.	
Bearbeiten	Aktiviert das Recht, Eigenschaften für Matrix im Management Client zu bearbeiten.	Nur verfügbar
Löschen	Aktiviert das Recht zum Löschen von Matrix im Management Client.	Nur verfügbar
Matrix Erstellen	Aktiviert das Recht, neue Matrix s im Management Client zu erstellen.	Nur verfügbar
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen in Management Client für alle Matrizen zu verwalten Matrix.	Nur verfügbar

Regeln

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Das Recht, vorhandene Regeln im Management Client anzuzeigen.
Bearbeiten	Das Recht, Eigenschaften von Regeln zu bearbeiten und das Regelverhalten im Management Client festzulegen. Erfordert außerdem, dass der Benutzer auf alle von der Regel betroffenen Geräte Schreibzugriff hat.
Löschen	Das Recht zum Löschen von Regeln im Management Client. Erfordert außerdem, dass der Benutzer auf alle von der Regel betroffenen Geräte Schreibzugriff hat.
Regel erstellen	Das Recht, neue Regeln im Management Client zu erstellen. Erfordert außerdem, dass der Benutzer auf alle von der Regel betroffenen Geräte Schreibzugriff hat.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für alle Regeln im Management Client zu verwalten.

Sites

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Das Recht, andere Standorte im Management Client anzuzeigen. Verbundene Standorte sind über die Milestone Federated Architecture verbunden. Zur Bearbeitung von Eigenschaften benötigen Sie auf dem Management-Server Bearbeitungsberechtigungen für jeden Standort.
Sicherheit verwalten	Aktiviert das Recht, Sicherheitsberechtigungen für alle Standorte zu verwalten.

Systemmonitor

Folgende Einstellungen sind nur in XProtect Expert und XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Aktiviert das Recht, Systemmonitore in XProtect Smart Client anzuzeigen.
Bearbeiten	Aktiviert das Recht, Eigenschaften für Systemmonitore im Management Client zu bearbeiten.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für alle Systemmonitore im Management Client zu verwalten.

Metadatensuche

Folgende Einstellungen sind nur in XProtect Expert und XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Aktiviert die Berechtigung, die Funktion **Verwendung von Metadaten** in Management Client und die damit zusammenhängenden Einstellungen einzusehen, aktiviert jedoch nicht die Berechtigung, die Einstellungen zu ändern.
Konfiguration der Metadatensuche bearbeiten	Aktiviert die Berechtigung, Metadatensuchkategorien im Management Client.zu aktivieren oder zu deaktivieren, z.B. Metadaten für Personen oder Fahrzeuge.
Sicherheit verwalten	Aktiviert die Berechtigung, Sicherheitsberechtigungen für Metadatensuchen zu verwalten.

Suchen

Folgende Einstellungen sind nur in XProtect Expert und XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Öffentliche Suchen lesen	Gibt die Berechtigung, gespeicherte öffentliche Suchen in XProtect Smart Client einzusehen und zu öffnen.
Öffentliche Suchen erstellen	Gibt die Berechtigung, neu konfigurierte Suchen als öffentliche Suchen in XProtect Smart Client abzuspeichern.
Öffentliche Suchen bearbeiten	Gibt die Berechtigung, die Einzelheiten oder die Konfiguration abgespeicherter öffentlicher Suchen in XProtect Smart Client zu bearbeiten, z.B. den Namen, die Beschreibung, Kameras und Suchkategorien.
Öffentliche Suchen löschen	Gibt die Berechtigung, gespeicherte öffentliche Suchen zu löschen.
Sicherheit verwalten	Gibt die Berechtigung, im Management Client Sicherheitsberechtigungen für die Suche zu verwalten.

Alarme

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Management	Aktiviert das Recht, Alarme im Management Client zu verwalten. Zum Beispiel die Prioritäten der Alarme zu ändern und Alarme auf andere Benutzer zu delegieren, Alarme zu bestätigen und den Status von mehreren Alarmen gleichzeitig zu ändern, z. B. von Neu auf Zugewiesen, Alarmdefinitionen, Alarmtöne und Alarmdateneinstellungen anzuzeigen.

Sicherheitsrecht	Beschreibung
	Die Registerkarte **Alarme und Ereignisse** im Dialogfeld **Optionen** wird nur angezeigt, wenn Sie diese Berechtigung erteilen.
Bearbeiten	Aktiviert das Recht, Alarme anzusehen und Alarmberichte auszudrucken.
Alarme deaktivieren	Aktiviert das Recht, Alarme zu deaktivieren.
Benachrichtigungen empfangen	Aktiviert das Recht, Benachrichtigungen über Alarme in XProtect Mobile-Clients und XProtect Web Client zu empfangen.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Alarme zu verwalten.
Erstellen	Das Recht, neue Alarmdefinitionen im Management Client zu erstellen.

Server-Protokolle

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Systemprotokolleinträge lesen	Aktiviert die Berechtigung dazu, Systemprotokolleinträge einzusehen.
Auditprotokolleinträge lesen	Aktiviert die Berechtigung dazu, Auditprotokolleinträge einzusehen.

Sicherheitsrecht	Beschreibung
Von Regeln ausgelöste Protokolleinträge lesen	Aktiviert die Berechtigung dazu, von Regeln ausgelöste Protokolleinträge einzusehen.
Protokollkonfiguration lesen	Aktiviert die Berechtigung dazu, Protokolleinstellungen in **Extras > Optionen > Serverprotokolle** zu lesen.
Aktualisierung der Protokollkonfiguration	Aktiviert die Berechtigung dazu, Protokolleinstellungen in **Extras > Optionen > Serverprotokolle** zu ändern.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für Alarme zu verwalten.

Zutrittskontrolle

Folgende Einstellungen sind nur in XProtect Corporate verfügbar.

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Bearbeiten	Das Recht, die Eigenschaften von Zutrittskontrollsystemen im Management Client zu bearbeiten.
Zutrittskontrolle verwenden	Ermöglicht dem Benutzer, alle auf die Zutrittskontrolle bezogenen Funktionen in den Clients zu verwenden.
Karteninhaberliste anzeigen	Ermöglicht dem Benutzer, die Karteninhaberliste auf der Registerkarte **Zutrittskontrolle** in den Clients zu sehen.
Benachrichtigungen	Erlaubt es dem Benutzer Benachrichtigungen über Zutrittsanforderungen in den

Sicherheitsrecht	Beschreibung
empfangen	Clients zu erhalten.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für alle Zutrittskontrollsysteme zu verwalten.

LPR

Wenn Ihr System mit XProtect LPR läuft, legen Sie die folgenden Rechte für die Benutzer fest:

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
LPR verwenden	Aktiviert das Recht, alle LPR-bezogenen Funktionen in den Clients zu verwenden
Nummernschild-Übereinstimmungslisten verwalten	Aktiviert das Recht, Nummernschild-Übereinstimmungsliste in den Management Client hinzuzufügen, zu importieren, zu bearbeiten, zu exportieren und zu löschen.
Nummernschild-Übereinstimmungslisten lesen	Aktiviert das Recht, Nummernschild-Übereinstimmungslisten anzusehen.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für alle Transaktionsdefinitionen im Management Client zu verwalten.

Transaktionsquellen

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Das Recht, die Eigenschaften von Transaktionsquellen im Management Client

Sicherheitsrecht	Beschreibung
	anzuzeigen.
Bearbeiten	Das Recht, die Eigenschaften von Transaktionsquellen im Management Client zu bearbeiten.
Löschen	Das Recht, Transaktionsquellen im Management Client zu löschen.
Erstellen	Das Recht, neue Transaktionsquellen im Management Client zu erstellen.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für alle Transaktionsquellen im Management Client zu verwalten.

Transaktionsdefinition

Sicherheitsrecht	Beschreibung
Vollständige Kontrolle	Das Recht, alle Sicherheitseinträge in diesem Teil des Systems zu verwalten.
Lesen	Das Recht, die Eigenschaften von Transaktionsdefinitionen im Management Client anzuzeigen.
Bearbeiten	Das Recht, die Eigenschaften von Transaktionsdefinitionen im Management Client zu bearbeiten.
Löschen	Das Recht, Transaktionsdefinitionen im Management Client zu löschen.
Erstellen	Das Recht, neue Transaktionsdefinitionen im Management Client zu erstellen.
Sicherheit verwalten	Das Recht, Sicherheitsberechtigungen für alle Transaktionsdefinitionen im Management Client zu verwalten.

MIP-Plug-ins

Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins für Ihr System entwickeln, z. B. für die Integration in externe Zutrittskontrollsysteme oder ähnliche Funktionen.

Registerkarte „Geräte“ (Rollen)

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

Auf der Registerkarte **Geräte** können Sie bestimmen, welche Funktionen die Benutzer/Gruppen mit der ausgewählten Rolle für jedes Gerät (z. B. eine Kamera) oder jede Gerätegruppe im XProtect Smart Client verwenden können.

Denken Sie daran, die Einstellungen bei jedem Gerät zu wiederholen. Sie können auch eine Gerätegruppe auswählen und die Rollenrechte für alle Geräte in der Gruppe auf einmal bestimmen.

Sie können auch die Kontrollkästchen mit den Quadraten aktivieren oder deaktivieren, aber bedenken Sie, dass dann Ihre Auswahl auf **alle** Geräte in der Gerätegruppe angewendet wird. Alternativ können Sie auch die einzelnen Geräte in der Gerätegruppe auswählen, um genau festzulegen, auf welche Geräte das jeweilige Recht angewendet wird.

Kamerabezogene Rechte

Bestimmen Sie die folgenden Rechte für Kameras:

Name	Beschreibung
Lesen	Die ausgewählten Kameras sind in den Clients sichtbar.
Live ansehen	Ermöglicht es, Live-Videos von den ausgewählten Kameras in den Clients zu sehen. Bei XProtect Smart Client ist es erforderlich, dass die Rolle das Recht zur Ansicht der Registerkarte **Live** des Clients erhalten hat. Dieses Recht wird als Teil der Anwendungsrechte verliehen. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei.
Wiedergabe > Innerhalb des Zeitprofils	Ermöglicht es, aufgezeichnete Videos von den ausgewählten Kameras in den Clients wiederzugeben. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei.
Wiedergabe > Wiedergabe beschränken auf	Ermöglicht es, aufgezeichnete Videos von den ausgewählten Kameras in den Clients wiederzugeben. Bestimmen Sie eine Wiedergabebeschränkung oder wenden Sie keine Beschränkungen an.
Sequenzen lesen	Ermöglicht es, die Sequenzinformationen, z. B. bezüglich des Sequenz Explorers, in den Clients zu lesen.

Name	Beschreibung
intelligente Suche	Ermöglicht es dem Benutzer, die Smart Search-Funktion in den Clients zu verwenden.
Exportieren	Ermöglicht es dem Benutzer, Aufzeichnungen von den Clients zu exportieren.
Manuelle Aufzeichnung starten	Ermöglicht es, eine manuelle Aufzeichnung der Videos von den ausgewählten Kameras in den Clients zu starten.
Manuelle Aufzeichnung stoppen	Ermöglicht es, eine manuelle Aufzeichnung der Videos von den ausgewählten Kameras in den Clients zu stoppen.
Lesezeichen lesen	Ermöglicht es, Lesezeichendetails in den Clients zu suchen und zu lesen.
Lesezeichen bearbeiten	Ermöglicht es, Lesezeichen in den Clients zu bearbeiten.
Lesezeichen erstellen	Ermöglicht es, Lesezeichen in den Clients hinzuzufügen.
Lesezeichen löschen	Ermöglicht es, Lesezeichen in den Clients zu löschen.
AUX-Befehle	Ermöglicht es Hilfsbefehle von den Clients zu verwenden.
Beweissicherungen erstellen und erweitern	Gibt dem Client-Benutzer folgende Möglichkeiten: • Hinzufügen der Kameras zu neuen oder bestehenden Beweissicherungen • Erweitern der Ablaufzeit für bestehende Beweissicherungen • Erweitern des geschützten Intervalls für bestehende Beweissicherungen Erfordert Benutzerrechte für alle Geräte, die zur Beweissicherung verwendet werden.

Name	Beschreibung
Beweissicherungen löschen und reduzieren	Gibt dem Client-Benutzer folgende Möglichkeiten: • Entfernen der Kamera aus bestehenden Beweissicherungen • Löschen von bestehenden Beweissicherungen • Verkürzen der Ablaufzeit für bestehende Beweissicherungen • Verkürzen des geschützten Intervalls für bestehende Beweissicherungen  Erfordert Benutzerrechte für alle Geräte, die zur Beweissicherung verwendet werden.
Beweissicherungen lesen	Ermöglicht es dem Client-Benutzer, nach Beweissicherungsdetails zu suchen und sie zu lesen.

Mikrofonbezogene Rechte

Bestimmen Sie die folgenden Rechte für Mikrofone:

Name	Beschreibung
Lesen	Die ausgewählten Mikrofone sind in den Clients sichtbar.
Live > Abhören	Ermöglicht es, Live-Audio von den ausgewählten Mikrofonen in den Clients zu hören. Bei XProtect Smart Client ist es erforderlich, dass die Rolle das Recht zur Ansicht der Registerkarte **Live** des Clients erhalten hat. Dieses Recht wird als Teil der Anwendungsrechte verliehen. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei.
Wiedergabe > Innerhalb des Zeitprofils	Ermöglicht es, aufgezeichnetes Audio von den ausgewählten Mikrofonen in den Clients wiederzugeben. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei.
Wiedergabe >	Ermöglicht es, aufgezeichnetes Audio von den ausgewählten Mikrofonen

Name	Beschreibung
Wiedergabe beschränken auf	in den Clients wiederzugeben. Bestimmen Sie eine Wiedergabebeschränkung oder wenden Sie keine Beschränkungen an.
Sequenzen lesen	Ermöglicht es, die Sequenzinformationen, z. B. bezüglich des Sequenz Explorers, in den Clients zu lesen.
Exportieren	Ermöglicht es dem Benutzer, Aufzeichnungen von den Clients zu exportieren.
Manuelle Aufzeichnung starten	Ermöglicht es, eine manuelle Aufzeichnung vom Audio der ausgewählten Mikrofone in den Clients zu starten.
Manuelle Aufzeichnung stoppen	Ermöglicht es, eine manuelle Aufzeichnung vom Audio der ausgewählten Mikrofone in den Clients zu stoppen.
Lesezeichen lesen	Ermöglicht es, Lesezeichendetails in den Clients zu suchen und zu lesen.
Lesezeichen bearbeiten	Ermöglicht es, Lesezeichen in den Clients zu bearbeiten.
Lesezeichen erstellen	Ermöglicht es, Lesezeichen in den Clients hinzuzufügen.
Lesezeichen löschen	Ermöglicht es, Lesezeichen in den Clients zu löschen.
Beweissicherungen erstellen und erweitern	Gibt dem Client-Benutzer folgende Möglichkeiten: • Hinzufügen des Mikrofons zu neuen oder bestehenden Beweissicherungen • Erweitern der Ablaufzeit für bestehende Beweissicherungen • Erweitern des geschützten Intervalls für bestehende Beweissicherungen

Name	Beschreibung
	Erfordert Benutzerrechte für alle Geräte, die zur Beweissicherung verwendet werden.
Beweissicherungen löschen und reduzieren	Gibt dem Client-Benutzer folgende Möglichkeiten: • Entfernen des Mikrofons aus bestehenden Beweissicherungen • Löschen von bestehenden Beweissicherungen • Verkürzen der Ablaufzeit für bestehende Beweissicherungen • Verkürzen des geschützten Intervalls für bestehende Beweissicherungen Erfordert Benutzerrechte für alle Geräte, die zur Beweissicherung verwendet werden.
Beweissicherungen lesen	Ermöglicht es dem Client-Benutzer, nach Beweissicherungsdetails zu suchen und sie zu lesen.

Lautsprecherbezogene Rechte

Bestimmen Sie die folgenden Rechte für Lautsprecher:

Name	Beschreibung
Lesen	Die ausgewählten Lautsprecher sind in den Clients sichtbar.
Live > Abhören	Ermöglicht es, Live-Audio von den ausgewählten Lautsprechern in den Clients zu hören. Bei XProtect Smart Client ist es erforderlich, dass die Rolle das Recht zur Ansicht der Registerkarte **Live** des Clients erhalten hat. Dieses Recht wird als Teil der Anwendungsrechte verliehen. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei.

Name	Beschreibung
Wiedergabe > Innerhalb des Zeitprofils	Ermöglicht es, aufgezeichnetes Audio von den ausgewählten Lautsprechern in den Clients wiederzugeben. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei.
Wiedergabe > Wiedergabe beschränken auf	Ermöglicht es, aufgezeichnetes Audio von den ausgewählten Lautsprechern in den Clients wiederzugeben. Bestimmen Sie eine Wiedergabebeschränkung oder wenden Sie keine Beschränkungen an.
Sequenzen lesen	Ermöglicht es, die Sequenzinformationen, z. B. bezüglich des Sequenz Explorers, in den Clients zu lesen.
Exportieren	Ermöglicht es dem Benutzer, Aufzeichnungen von den Clients zu exportieren.
Manuelle Aufzeichnung starten	Ermöglicht es, eine manuelle Aufzeichnung vom Audio der ausgewählten Lautsprecher in den Clients zu starten.
Manuelle Aufzeichnung stoppen	Ermöglicht es, eine manuelle Aufzeichnung vom Audio der ausgewählten Lautsprecher in den Clients zu stoppen.
Lesezeichen lesen	Ermöglicht es, Lesezeichendetails in den Clients zu suchen und zu lesen.
Lesezeichen bearbeiten	Ermöglicht es, Lesezeichen in den Clients zu bearbeiten.
Lesezeichen erstellen	Ermöglicht es, Lesezeichen in den Clients hinzuzufügen.
Lesezeichen löschen	Ermöglicht es, Lesezeichen in den Clients zu löschen.
Beweissicherungen erstellen und erweitern	Gibt dem Client-Benutzer folgende Möglichkeiten: • Hinzufügen der Lautsprecher zu neuen oder bestehenden Beweissicherungen • Erweitern der Ablaufzeit für bestehende Beweissicherungen

Name	Beschreibung
	• Erweitern des geschützten Intervalls für bestehende Beweissicherungen Erfordert Benutzerrechte für alle Geräte, die zur Beweissicherung verwendet werden.
Beweissicherungen löschen und reduzieren	Gibt dem Client-Benutzer folgende Möglichkeiten: • Entfernen der Lautsprecher aus bestehenden Beweissicherungen • Löschen von bestehenden Beweissicherungen • Verkürzen der Ablaufzeit für bestehende Beweissicherungen • Verkürzen des geschützten Intervalls für bestehende Beweissicherungen Erfordert Benutzerrechte für alle Geräte, die zur Beweissicherung verwendet werden.
Beweissicherungen lesen	Ermöglicht es dem Client-Benutzer, nach Beweissicherungsdetails zu suchen und sie zu lesen.

Metadatenbezogene Rechte

Bestimmen Sie die folgenden Rechte für Metadatengeräte:

Name	Beschreibung
Lesen	Aktiviert das Recht, Metadatengeräte zu sehen und von ihnen Daten in den Clients abzurufen.
Bearbeiten	Aktiviert das Recht, die Einstellungen der Metadaten zu bearbeiten. Ermöglicht Nutzern außerdem, Metadatengeräte in Management Client und über das MIP SDK zu aktivieren oder zu deaktivieren.

Name	Beschreibung
Live ansehen	Aktiviert das Recht Kamerametadaten in den Clients anzuzeigen. Bei XProtect Smart Client ist es erforderlich, dass die Rolle das Recht zur Ansicht der Registerkarte **Live** des Clients erhalten hat. Dieses Recht wird als Teil der Anwendungsrechte verliehen.
Wiedergabe	Aktiviert das Recht, aufgezeichnete Daten von Metadatengeräten in den Clients wiederzugeben.
Sequenzen lesen	Aktiviert das Recht, die Sequenzfunktion beim Durchsuchen von Aufzeichnungen der Metadatengeräte in den Clients zu verwenden.
Exportieren	Aktiviert das Recht, aufgezeichnete Audiodateien von Metadatengeräten in den Clients zu exportieren.
Beweissicherungen erstellen und erweitern	Aktiviert das Recht, Beweissicherungen auf Metadaten in den Clients zu erstellen und zu erweitern.
Beweissicherungen lesen	Aktiviert das Recht, Beweissicherungen auf Metadaten in den Clients anzuzeigen.
Beweissicherungen löschen und reduzieren	Aktiviert das Recht zum Löschen oder Reduzieren von Beweissicherungen in den Clients.
Manuelle Aufzeichnung starten	Aktiviert das Recht manuelle Metadatenaufzeichnungen in den Clients zu starten.
Manuelle Aufzeichnung stoppen	Aktiviert das Recht manuelle Metadatenaufzeichnungen in den Clients zu stoppen.

Eingangsbezogene Rechte

Bestimmen Sie die folgenden Rechte für Eingabegeräte:

Name	Beschreibung
Lesen	Der/die ausgewählte/n Eingang/Eingänge ist/sind in den Clients sichtbar.

Ausgangsbezogene Rechte

Bestimmen Sie die folgenden Rechte für Ausgabegeräte:

Name	Beschreibung
Lesen	Die ausgewählten Ausgänge sind in den Clients sichtbar. Wenn sichtbar, ist der Ausgang auf einer Liste in den Clients auswählbar.
Aktivieren	Die ausgewählten Ausgänge können vom Management Client und den Clients aktiviert werden. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei.

PTZ-Registerkarte (Rollen)

Sie legen Rechte für PTZ-Kameras (Pan/Tilt/Zoom) auf der Registerkarte **PTZ** fest. Sie bestimmen die Funktionen, die Benutzer/Gruppen in den Clients verwenden können. Auswählen können Sie einzelne PTZ-Kameras oder Gerätegruppen, die PTZ-Kameras enthalten.

Bestimmen Sie die folgenden Rechte für PTZ:

Name	Beschreibung
Manuelles PTZ	Bestimmt, ob die ausgewählte Rolle PTZ-Funktionen verwenden und einen Wachrundgang an der ausgewählten Kamera anhalten kann. Bestimmen Sie ein Zeitprofil, wählen Sie **Immer** oder behalten Sie den Standardwert bei, der dem Standardzeitprofil folgt, das auf der Registerkarte **Info** für diese Rolle definiert ist.

Name	Beschreibung
PTZ-Voreinstellungen oder Wachrundgangprofile aktivieren	Legt fest, ob die ausgewählte Rolle die ausgewählte Kamera zu Preset-Positionen bewegen, Wachrundgangprofile starten und stoppen sowie einen Wachrundgang anhalten kann. Bestimmen Sie ein Zeitprofil, wählen Sie **Immer** oder behalten Sie den Standardwert bei, der dem Standardzeitprofil folgt, das auf der Registerkarte **Info** für diese Rolle definiert ist. Wenn Sie möchten, dass diese Rolle weitere PTZ-Funktionen für die Kamera verwenden kann, müssen Sie das Recht **Manuelles PTZ** aktivieren.
PTZ-Priorität	Legt die Priorität der PTZ-Kameras fest. Wenn mehrere Benutzer an einem Überwachungssystem dieselbe PTZ-Kamera zur selben Zeit steuern möchten, können Konflikte auftreten. Sie können solche Situationen vermeiden, indem Sie eine Priorität für die Verwendung der ausgewählten PTZ-Kameras nach Benutzern/Gruppen mit der ausgewählten Rolle bestimmen. Bestimmen Sie eine Priorität zwischen 1 und 32.000, wobei 1 die niedrigste Priorität bedeutet. Die Standardpriorität liegt bei 3.000. Die Rolle mit dem höchsten Prioritätswert kann die PTZ-Kameras steuern.
PTZ-Voreinstellungen oder Wachrundgangprofile verwalten	Bestimmt das Recht, PTZ-Preset-Positionen und Wachrundgangprofile auf der ausgewählten Kamera im Management Client und XProtect Smart Client hinzuzufügen, zu bearbeiten und zu löschen. Wenn Sie möchten, dass diese Rolle weitere PTZ-Funktionen für die Kamera verwenden kann, müssen Sie das Recht **Manuelles PTZ** aktivieren.
PTZ-Voreinstellungen sperren/entsperren	Bestimmt, ob die Rolle Preset-Positionen für die ausgewählte Kamera sperren und entsperren kann.
PTZ-Sitzungen reservieren	Bestimmt das Recht, die ausgewählte Kamera in den Modus „reservierte PTZ-Sitzung“ zu versetzen. In einer reservierten PTZ-Sitzung können andere Benutzer oder Wachrundgangsitzungen mit einer höheren PTZ-Priorität nicht die Kontrolle übernehmen. Wenn Sie möchten, dass diese Rolle weitere PTZ-Funktionen für die

Name	Beschreibung
	Kamera verwenden kann, müssen Sie das Recht **Manuelles PTZ** aktivieren.
PTZ-Sitzungen freigeben	Bestimmt, ob die ausgewählte Rolle die PTZ-Sitzungen von anderen Benutzern freigeben kann mit Management Client. Sie können Ihre eigenen PTZ-Sitzungen jederzeit ohne diese Berechtigung freigeben.

Registerkarte „Sprache" (Rollen)

Nur relevant, wenn Sie Lautsprecher auf Ihrem System verwenden. Bestimmen Sie die folgenden Rechte für Lautsprecher:

Name	Beschreibung
Sprechen	Bestimmen Sie, ob Benutzer über die ausgewählten Lautsprecher sprechen dürfen. Bestimmen Sie das Zeitprofil oder behalten Sie den Standardwert bei.
Sprechpriorität	Wenn mehrere Client-Benutzer über dieselben Lautsprecher zur selben Zeit sprechen möchten, können Konflikte auftreten. Lösen Sie das Problem, indem Sie eine Priorität für die Nutzung der ausgewählten Lautsprecher durch Benutzer/Gruppen mit der ausgewählten Rolle festlegen. Bestimmen Sie eine Priorität von **Sehr niedrig** bis **Sehr hoch**. Die Rolle mit der höchsten Priorität darf den Lautsprecher vor den anderen Rollen verwenden. Wenn zwei Benutzer mit der gleichen Rolle zur selben Zeit sprechen möchten, gilt das Windhundprinzip.

Registerkarte „Fernaufzeichnungen" (Rollen)

Bestimmen Sie die folgenden Rechte für Fernaufzeichnungen:

Name	Beschreibung
Fernaufzeichnungen abrufen	Aktiviert das Recht, Aufzeichnungen in den Clients von Kameras, Mikrofonen, Lautsprechern und Metadatengeräten an Remote-Systeminstallationen oder von lokalen Speichern in Kameras abzurufen.

Smart Wall Registerkarte (Rollen)

Mithilfe von Rollen können Sie Ihren Client-Benutzern Smart Wall-bezogene Benutzerrechte für die Funktion Smart Wall geben:

Name	Beschreibung
Lesen	Ermöglicht es Benutzern, in den Clients die ausgewählte Smart Wall zu sehen.
Bearbeiten	Ermöglicht es Benutzern, die ausgewählte Smart Wall im Management Client zu bearbeiten.
Löschen	Ermöglicht es Benutzern, die ausgewählte Smart Wall im Management Client zu löschen.
Bedienen	Ermöglicht es Benutzern, auf die ausgewählte Smart Wall im Client Layouts anzuwenden und die ausgewählte Voreinstellung zu aktivieren.
Wiedergabe	Ermöglicht es den Benutzern, aufgezeichnete Daten von der ausgewählten Smart Wall in den Clients wiederzugeben.

Registerkarte „Externes Ereignis“ (Rollen)

Bestimmen Sie die folgenden Rechte zu externen Ereignissen:

Name	Beschreibung
Lesen	Ermöglicht es Benutzern nach dem ausgewählten externen Systemereignis in den Clients und im Management Client zu suchen und dieses anzusehen.

Name	Beschreibung
Bearbeiten	Ermöglicht es Nutzern, das ausgewählte externe Systemereignis im Management Client zu bearbeiten.
Löschen	Ermöglicht es Nutzern, das ausgewählte externe Systemereignis im Management Client zu löschen.
Auslöser	Ermöglicht es Nutzern, das ausgewählte externe Systemereignis in den Clients auszulösen.

Registerkarte „Ansichtsgruppe“ (Rollen)

Auf der Registerkarte **Ansichtsgruppe** bestimmen Sie, welche Ansichtsgruppen die Benutzer und Benutzergruppen mit der ausgewählten Rolle in den Clients verwenden können.

Bestimmen Sie die folgenden Rechte für Ansichtsgruppen:

Name	Beschreibung
Lesen	Aktiviert das Recht, die Ansichtsgruppen in den Clients und im Management Client anzusehen. Ansichtsgruppen werden im Management Client erstellt.
Bearbeiten	Aktiviert das Recht, Eigenschaften für Ansichtsgruppen in Management Client zu bearbeiten.
Löschen	Das Recht, Ansichtsgruppen im Management Client zu löschen.
Bedienen	Aktiviert das Recht, Ansichtsgruppen im XProtect Smart Client zum Erstellen und Löschen von Untergruppen sowie Ansichten zu verwenden.

Registerkarte „Server“ (Rollen)

Das Bestimmen von Rollenrechten auf der Registerkarte **Server** ist nur dann relevant, wenn Ihr System in einer Milestone Federated Architecture Konfiguration läuft.

Name	Beschreibung
Sites	Aktiviert das Recht, den ausgewählten Standort im Management Client anzusehen. Verbundene Standorte sind über die Milestone Federated Architecture verbunden. Zur Bearbeitung von Eigenschaften benötigen Sie auf dem Management-Server Bearbeitungsberechtigungen für jeden Standort.

Weitere Informationen finden Sie unter Konfigurieren von Milestone Federated Architecture auf Seite 461.

Matrix Registerkarte (Rollen)

Wenn Sie Matrix-Empfänger auf Ihrem System konfiguriert haben, können Sie Matrix-Rollenrechte konfigurieren. Von einem Client können Sie Videos an ausgewählte Matrix-Empfänger senden. Wählen Sie die Benutzer, die diese empfangen können, auf der Registerkarte Matrix.

Die folgenden Rechte sind verfügbar:

Name	Beschreibung
Lesen	Bestimmen Sie, ob Benutzer und Gruppen mit der ausgewählten Rolle Videos auswählen und an die Matrix-Empfänger der Clients senden können.

Registerkarte „Alarme“ (Rollen)

Wenn Sie in Ihrer Systemkonfiguration Alarme verwenden, um eine allgemeine Übersicht und Kontrolle über Ihre Installation zu erhalten (einschließlich weiterer XProtect-Server), können Sie die Registerkarte **Alarme** dazu verwenden, um festzulegen, welche Alarmrechte Benutzer/Gruppen mit der ausgewählten Rolle haben sollen. Zum Beispiel wie Alarme in den Clients zu verwalten sind.

Bestimmen Sie die folgenden Rechte für Alarme:

Name	Beschreibung
Management	Aktiviert das Recht, Alarme zu verwalten und so z. B. die Prioritäten der Alarme zu ändern und Alarme auf andere Benutzer zu delegieren, Alarme zu bestätigen und den Status von mehreren Alarmen gleichzeitig zu ändern, z. B. von **Neu** auf **Zugewiesen**.
Ansicht	Aktiviert das Recht, Alarme anzusehen und Alarmberichte auszudrucken.
Alarme deaktivieren	Aktiviert das Recht, Alarme zu deaktivieren.
Benachrichtigungen empfangen	Aktiviert das Recht, Benachrichtigungen über Alarme in XProtect Mobile-Clients und XProtect Web Client zu empfangen.

Registerkarte „Zutrittskontrolle“ (Rollen)

Wenn Sie Basisnutzer, Windows-Benutzer oder -Gruppen hinzufügen oder bearbeiten, können Sie Zutrittskontrolleinstellungen bestimmen:

Name	Beschreibung
Zutrittskontrolle verwenden	Ermöglicht dem Benutzer, alle auf die Zutrittskontrolle bezogenen Funktionen in den Clients zu verwenden.
Karteninhaberliste anzeigen	Ermöglicht dem Benutzer, die Karteninhaberliste auf der Registerkarte **Zutrittskontrolle** in den Clients zu sehen.
Benachrichtigungen empfangen	Erlaubt es dem Benutzer Benachrichtigungen über Zutrittsanforderungen in den Clients zu erhalten.

Registerkarte „LPR“ (Rollen)

Wenn Ihr System mit XProtect LPR läuft, können Sie die folgenden Rechte für die Benutzer festlegen:

Name	Beschreibung
LPR verwenden	Aktiviert das Recht, alle LPR-bezogenen Funktionen in den Clients zu verwenden.
Nummernschild-Übereinstimmungslisten verwalten	Aktiviert das Recht, Nummernschild-Übereinstimmungsliste in den Management Client hinzuzufügen, zu importieren, zu bearbeiten, zu exportieren und zu löschen.
Nummernschild-Übereinstimmungslisten lesen	Aktiviert das Recht, Nummernschild-Übereinstimmungslisten anzusehen.

MIP Registerkarte (Rollen)

Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins für Ihr System entwickeln, z. B. für die Integration in externe Zutrittskontrollsysteme oder ähnliche Funktionen.

Die Einstellungen, die Sie ändern, hängen vom tatsächlichen Plug-in ab. Finden Sie die benutzerdefinierten Einstellungen für die Plug-ins auf der Registerkarte **MIP**.

Basisnutzer (Erklärung)

Wenn Sie einen Basisnutzer zu Ihrem System hinzufügen, erstellen Sie ein zugehöriges Benutzerkonto für das Überwachungssystem mit Basisnutzername und Passwortauthentifizierung für den einzelnen Benutzer. Das wird im Gegensatz zu Windows-Benutzern über Active Directory hinzugefügt.

Wenn Sie mit Basisnutzer arbeiten, ist es wichtig, den Unterschied zwischen Basisnutzern und Windows-Benutzern zu verstehen.

- Basisnutzer authentifizieren sich durch einen Benutzernamen und ein Passwort und bestehen speziell für ein System. Selbst wenn Basisnutzer denselben Namen und dasselbe Passwort haben, hat ein Basisnutzer, der an einem föderalen Standort erstellt wurde, keinen Zugriff auf einen anderen föderalen Standort
- Windows-Benutzer authentifizieren sich auf Basis ihrer Windows-Anmeldung und sind auf einen bestimmten Computer beschränkt

Erstellen von Basisnutzer

So erstellen Sie einen Basisnutzer auf Ihrem System:

1. Erweitern Sie **Sicherheit** > **Basisnutzer**.
2. Klicken Sie mit der rechten Maustaste auf das Feld **Basisnutzer**, und wählen Sie die Option **Basisnutzer erstellen** aus.
3. Legen Sie einen Benutzernamen und ein Passwort fest und wiederholen Sie es, um zu bestätigen, dass Sie es richtig eingegeben haben.

   Das Passwort muss die Anforderungen an die Komplexität für das Windows-Betriebssystem auf dem Computer erfüllen, auf dem der Managementserver-Dienst installiert ist.

4. Klicken Sie auf **OK**, um den Basisnutzer zu erstellen.

Site-Navigation: System-Dashboard

Dieser Abschnitt beschreibt, wie Sie Ihr System überwachen und wie Sie Berichte erstellen und Daten schützen können.

System-Dashboard (Erklärung)

Das System-Dashboard bietet Ihnen die Funktion Ihr System und seine Komponenten zu überwachen.

Greifen Sie auf die folgende Funktionalität zu:

Name	Beschreibung
Systemmonitor	Überwachen Sie den Status Ihrer Server und Kameras mittels der von Ihnen festgelegten Parameter.
Schwellenwerte des Systemmonitors	Stellen Sie Schwellenwerte für überwachte Parameter auf dem Server ein und überwachen Sie Kacheln, die im Systemmonitor verwendet werden.
Beweissicherung	Erhalten Sie eine Übersicht über alle geschützten Daten im System.
Aktuelle Aufgabe	Erhalten Sie eine Übersicht über alle laufenden Aufgaben auf einem ausgewählten Aufzeichnungsserver.
Konfigurationsberichte	Entscheiden Sie über den Inhalt Ihrer Systemkonfigurationsberichte, bevor Sie drucken.

Systemmonitor (Erklärung)

Der Systemmonitor liefert Ihnen dank farbiger Kacheln, die die Systemhardware widerspiegeln, einen schnellen, visuellen Überblick über den aktuellen Status der Server und Kameras Ihres Systems. Standardmäßig zeigt das System Kacheln an, die alle **Aufzeichnungsserver**, **alle Server** und **alle Kameras** widerspiegeln.

Die Farbe der Kacheln:

Kachelfarbe	Beschreibung
Grün	**Normaler** Status. Alles läuft normal.
Gelb	**Warnstatus**. Mindestens ein überwachter Parameter liegt über dem Schwellenwert (siehe Schwellenwerte des Systemmonitors (Erklärung) auf Seite 429) für den **normalen** Status.
Rot	**Kritischer** Status. Mindestens ein überwachter Parameter liegt über dem Schwellenwert für den **normalen** Status und dem **Warnstatus**.

Sie können den Server und die Kamerakacheln anpassen, wenn Sie mehr oder weniger Kacheln auf dem Dashboard anzeigen lassen möchten. Zum Beispiel können Sie Kacheln einrichten, die einen einzelnen Server, eine einzelne Kamera oder eine Gruppe von Kameras oder Server widerspiegelt. Sie können eine Kachel auch entfernen, wenn Sie diese nicht verwenden oder dessen Überwachungsparameter bearbeiten möchten. Überwachungsparameter sind beispielsweise die CPU-Auslastung oder verfügbarer Speicher eines Servers. Wenn Sie diese Parameter von der Server-Kachel entfernen, kann die Kachel diese Parameter auf der zugehörigen Kachel nicht überwachen. Klicken Sie auf **Anpassen** in der oberen rechten Ecke der Registerkarte, um das Fenster zum Anpassen des Dashboards zu öffnen. Weitere Informationen finden Sie unter Dashboard anpassen.

Die Kacheln ändern ihren Status und dementsprechend ihre Farbe basierend auf Schwellenwerten, die unter den Systemmonitor-Schwellenwerten festgelegt sind. Das System legt einige standardmäßige Schwellenwerte fest, aber Sie können selbst entscheiden, welche Schwellenwerte für jedes der drei Status gelten sollen. Um Schwellenwerte einzustellen oder zu ändern, können Sie die Option **Systemmonitor-Schwellenwerte** verwenden. Weitere Informationen finden Sie unter Schwellenwerte des Systemmonitors (Erklärung) auf Seite 429.

Falls eine Kachel ihre Farbe ändert und Sie wissen möchten, welcher Server/Parameter für die Farbänderung der Kachel verantwortlich ist, klicken Sie auf die Kachel. Dadurch öffnet sich eine Übersicht am unteren Rand des Bildschirms, in der jeder überwachte Parameter, den Sie für Ihre Kachel aktiviert haben, in Rot, Gelb oder Grün angezeigt wird. Klicken Sie auf die Schaltfläche **Details**, um weitere umfassende Informationen für den Grund der Statusänderung anzuzeigen.

Wenn Sie ein Warnzeichen sehen und Ihre Maus darüber platzieren, zeigt das System eine

Fehlermeldung an.

Die Systemmonitor-Funktion erfordert, dass der Data Collector-Dienst ausgeführt wird.

Dashboard anpassen

Eine neue Kamera- oder Server-Kachel hinzufügen:

1. Klicken Sie im Systemmonitor-Fenster auf **Anpassen**.
2. In dem geöffneten Fenster **Dashboard anpassen**, klicken Sie auf **Neu** unter **Server-Kacheln** oder **Kamerakacheln**.
3. Im Fenster **Neue Server-Kachel/Neue Kamerakachel**, wählen Sie die Kameras oder Server, die Sie überwachen möchten.
4. Unter **Überwachungsparameter** wählen Sie die Kontrollkästchen für die Parameter, die Sie zur zugehörigen Kacheln hinzufügen oder entfernen möchten entweder an oder ab.
5. Klicken Sie auf **OK**. Der neue Server- oder Kamerakachel wurde nun zu den angezeigten Kacheln in Ihrem Dashboard hinzugefügt.

Überwachungsparameter bearbeiten:

1. Klicken Sie im Fenster Systemmonitor-Dashboard auf **Anpassen**.
2. In dem geöffneten Fenster **Dashboard anpassen**, klicken Sie auf **Bearbeiten** unter **Server-Kacheln** oder **Kamerakacheln**.
3. Wählen Sie die Serverkomponente oder Kameras, die Sie bearbeiten möchten im Fenster **Server-Kachel bearbeiten** oder **Kamerakachel bearbeiten** aus.
4. Wählen Sie im Feld **Überwachungsparameter** die Kontrollkästchen für die Überwachungsparameter an oder ab, die Sie der ausgewählten Kachel hinzufügen oder von ihr entfernen möchten.
5. Klicken Sie auf **OK**. Die veränderten Überwachungsparameter sind nun Teil von oder entfernt von der relevanten Kachel.

Sie können, falls gewünscht, historische Daten auf dem System aktivieren oder deaktivieren. Bei Deaktivierung dieser Daten, ist es nicht mehr möglich die Graphen von früherem Systemverhalten anzusehen. Wenn Sie die Belastung auf dem SQL Server und auf der Datenbank oder Ihrer Bandbreite verringern möchten, können Sie das Abtastintervall für historische Daten reduzieren. Durch die Reduzierung des Abtastintervalls der historischen Daten, stehen in den Graphen weniger Details zur Verfügung.

Systemmonitor-Details (Erklärung)

Wenn Sie auf einen Server oder Kamerakachel klicken, können Sie den Status jedes ausgewählten Überwachungsparameters unterhalb des Dashboards sehen.

Beispiel: Die Überwachungsparameter für LIVE-FPS einer Kamera hat den Warnstatus erreicht.

Das **Status**-Feld zeigt den Status der Kamera an. Es wird beispielsweise eine Warnung in Rot angezeigt, wenn die Verbindung zum Gerät unterbrochen ist. Dieses Symbol beinhaltet ein Tool-Tip mit einer kurzen Beschreibung des Problems, welches die Warnung verursacht.

Das Feld **Verwendeter Speicherplatz** zeigt Daten anderer Aufzeichnungsserver, auf denen dieses Gerät Aufzeichnungen besitzt. Zum Beispiel wenn sich das Gerät vorher auf anderen Aufzeichnungsservern befunden hat.

Wenn Sie die Schaltfläche **Details** für den betroffenen Server bzw. die Kamera anklicken, können Sie Systeminformationen sehen und Berichte über folgendes erstellen:

Komponente	Beschreibung
Managementserver	Zeigt die Daten vom ausgewählten Management-Server an
Aufzeichnungsserver	Zeigt die Daten vom ausgewählten Aufzeichnungsserver an. Sie können diese über Folgendes ansehen: • Datenträger • Speicher • Netzwerk • Kamera

Komponente	Beschreibung
Failover-Aufzeichnungsserver	Zeigt die Daten vom ausgewählten Failover-Aufzeichnungsserver an.
Zusätzliche Server	Zeigt Daten auf dem Log-Server, Event Server und mehr.
Kameras	Zeigt Daten auf einer beliebigen Kamera in einer beliebigen Kameragruppe in Ihrer Konfiguration an.

Jedes dieser Elemente ist ein Bereich, den Sie anklicken und erweitern können. Wenn Sie diesen Bereich anklicken, liefert es Ihnen relevante dynamische Daten über diesen Server oder Kamera.

Die Leiste **Kameras** enthält eine Liste der Kameragruppen, die zur Auswahl stehen. Nachdem Sie eine Gruppe ausgewählt haben, können Sie eine bestimmte Kamera auswählen und sich für diese die dynamischen Daten ansehen. Alle Server zeigen die Daten zur CPU-Auslastung und zum freien Arbeitsspeicher an. Darüber hinaus zeigen Aufzeichnungsserver die Daten zum Verbindungsstatus an. In jeder Ansicht finden Sie einen Link **Verlauf**. Klicken Sie darauf, um sich die Verlaufsdaten und -berichte anzusehen (um sich die Berichte einer Kamera anzusehen, klicken Sie auf den Namen der jeweiligen Kamera). Für jeden Verlaufsbericht können Sie die Daten der letzten 24 Stunden, 7 Tage oder 30 Tage einsehen. Um Berichte zu speichern und/oder zu drucken, klicken Sie auf das Symbol **An PDF senden**. Verwenden Sie < und die Symbole auf der Startseite, um im Systemmonitor zu navigieren.

Sie können nur historische Berichte von Daten des Aufzeichnungsservers erstellen, bei dem sich das Gerät derzeit befindet.

Wenn Sie auf die Details des Systemmonitors von einem Server-Betriebssystem aus zugreifen, könnten Sie eine Meldung bezüglich **Internet Explorer erweiterte Sicherheitskonfiguration** bekommen. Folgen Sie den Anweisungen in der Meldung, um die **Systemmonitor**-Seite zu den **Vertrauenswürdigen Seiten** hinzuzufügen, bevor Sie fortfahren.

Schwellenwerte des Systemmonitors (Erklärung)

Mit den Schwellenwerten für den Systemmonitor können Sie die Schwellenwerte dafür einrichten und anpassen, wann die Kacheln auf dem Systemmonitor visuell anzeigen sollen, dass Ihre Systemhardware ihren Betriebszustand ändert, z.B. wenn die CPU-Nutzung eines Servers von Normal (grün) auf Warnung (gelb) wechselt.

Im System sind Standardschwellenwerte eingerichtet, so dass Sie von dem Moment an, an dem Ihr System fertig eingerichtet ist, damit beginnen können, Ihre Systemhardware zu überwachen. Zum Ändern von Schwellenwerten siehe Schwellenwerte des Systemmonitors einstellen auf Seite 432.

Das System ist standardmäßig so eingerichtet, dass es Schwellenwerte für alle Instanzen einer bestimmten Hardware anzeigt, z.B. alle Kameras oder alle Server. Sie können Schwellenwerte auch für einzelne Server oder Kameras, oder für eine Untergruppe davon, einrichten. Schwellenwerte für einzelne Server oder Kameras einzurichten kann hilfreich sein, z.B. wenn es für bestimmte Kameras erlaubt sein soll, eine höhere **Live-FPS** oder **Aufzeichnungs-FPS** zu verwenden als für andere Kameras.

Sie können die Schwellenwerte für Server, Kameras, Festplatten und Speicher einstellen. Wenn Sie die Schwellenwerte ändern wollen, können Sie dazu den Schieberegler für die Schwellenwerte verwenden. Mit dem Schieberegler für die Schwellenwerte können Sie die Schwellenwerte erhöhen bzw. senken, indem Sie die Griffe, durch die die Zustände getrennt sind, nach oben oder unten ziehen. Der Schieberegler für den Schwellenwert ist in ähnlichen Farben unterteilt wie die auf den Server- oder Kamerakacheln im Systemmonitor (siehe Schwellenwerte des Systemmonitors (Erklärung) auf Seite 429).

Um sicherzustellen, dass Sie keinen **Kritischen** oder **Alarm**-Zustand sehen, falls die Nutzung oder Belastung Ihrer Systemhardware lediglich für einen Moment eine obere Schwelle erreicht, verwenden Sie das **Berechnungsintervall**. Das Berechnungsintervall mittelt die Auswirkungen kurzfristiger oder häufiger Änderungen eines Systemhardwarezustands heraus. In der Praxis bedeutet dies, dass die Funktion zur Berechnung des Intervalls die Auswirkungen von Hardwareänderungen im zeitlichen Verlauf ausgleicht, so dass Sie nicht jedes Mal alarmiert werden, wenn eine Schwelle überschritten wird.

Zum Beispiel können Sie das **Berechnungsintervall** auf eine (1) Minute setzen, womit gewährleistet ist, dass Sie nur dann alarmiert werden, wenn der Durchschnittswert für die ganze Minute den Schwellenwert überschreitet. Der Vorteil hiervon ist, dass Sie Alarme zu häufigen und evtl. irrelevanten Änderungen im Hardwarezustand vermeiden und nur solche Alarme erhalten, die z.B. dauerhafte Probleme mit der CPU-Nutzung oder der Speichernutzung anzeigen. Zum Ändern der Werte für die Berechnungsintervalle siehe Schwellenwerte des Systemmonitors einstellen auf Seite 432.

Serverschwellenwerte

Schwellenwert	Beschreibung	Einheit
CPU-Auslastung	Schwellenwerte für die CPU-Nutzung auf den von Ihnen überwachten Servern.	%
Verfügbare Rechenkapazität	Schwellenwerte für den auf den von Ihnen überwachten Servern genutzten RAM-Speicher.	MB

Schwellenwert	Beschreibung	Einheit
NVIDIA-Dekodierung	Schwellenwerte für die Nutzung der NVIDIA-Dekodierung auf den von Ihnen überwachten Servern.	%
NVIDIA-Speicher	Schwellenwerte für den auf den von Ihnen überwachten Servern genutzten NVIDIA-RAM-Speicher.	%
NVIDIA-Rendering	Schwellenwerte für die Nutzung des NVIDIA-Renderings auf den von Ihnen überwachten Servern.	%

Kameraschwellenwerte

Schwellenwert	Beschreibung	Einheit
Live-FPS	Schwellenwerte für die FPS der bei der Anzeige von Live-Video auf den von Ihnen überwachten Kameras verwendeten Kameras.	%
Aufzeichnungs-FPS	Schwellenwerte für die FPS der verwendeten Kameras, wenn das System auf den von Ihnen überwachten Kameras Videoaufzeichnungen erstellt.	%
Verwendeter Speicherplatz	Schwellenwerte für den von den von Ihnen überwachten Kameras verwendeten Speicherplatz.	GB

Schwellenwerte für Festplatten

Schwellenwert	Beschreibung	Einheit
Freier Speicherplatz	Schwellenwerte für den verfügbaren Speicherplatz auf den von Ihnen überwachten Festplatten.	GB

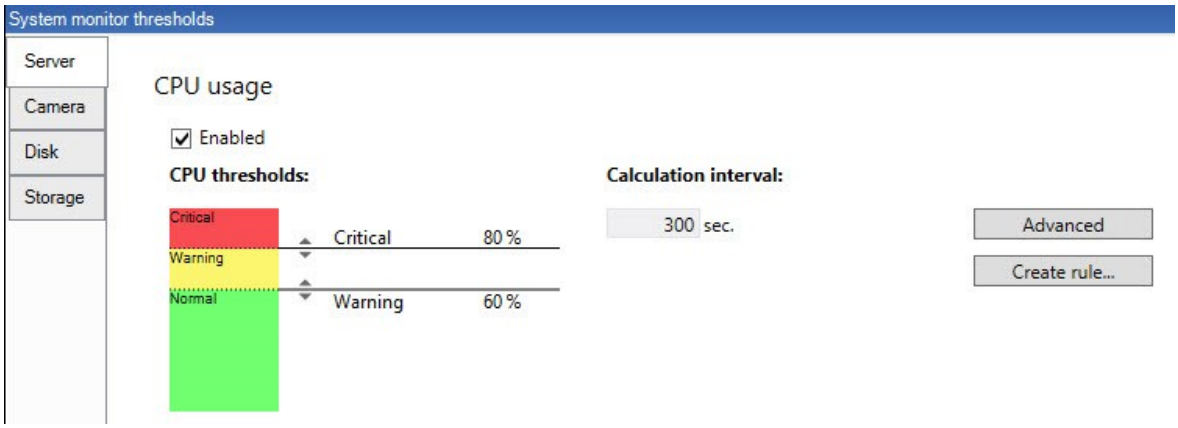
Schwellenwerte für Speicher

Schwellenwert	Beschreibung	Einheit
Speicherzeit	Schwellenwert, der eine Prognose dafür anzeigt, wann in Ihrem Speicher kein Platz mehr vorhanden sein wird. Der angezeigte Betriebszustand basiert auf Ihrer Systemeinrichtung und wird zweimal täglich aktualisiert.	Tage

Sie können auch Regeln aufstellen (siehe Regeln auf Seite 340), um bestimmte Maßnahmen durchzuführen oder um Alarme zu aktivieren (siehe System-Dashboard (Erklärung) auf Seite 425), wenn ein Schwellenwert von einem Zustand in einen anderen wechselt.

Schwellenwerte des Systemmonitors einstellen

1. Klicken Sie im Bereich **Standort-Navigation** auf **Systemmonitor-Schwellenwerte**.
2. Zum Aktivieren relevanter Hardware wählen Sie das Kontrollkästchen **Aktivieren** aus, falls Sie es noch nicht aktiviert haben. Die Abbildung unten zeigt ein Beispiel.

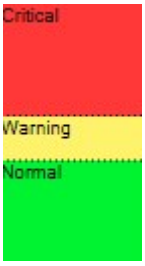


3. Ziehen Sie den Schieberegler für Schwellenwerte hoch oder runter, um den Schwellenwert zu erhöhen bzw. zu reduzieren. Es stehen zwei Schieberegler für jedes Teil der Hardware, das in der Schwellenwertsteuerung angezeigt wird, zur Verfügung; es wird zwischen den Ebenen **Normal**, **Warnung** und **Kritisch** aufgeteilt.
4. Geben Sie einen Wert für das Berechnungsintervall an oder behalten Sie den Standardwert bei.
5. Wenn Sie Werte für individuelle Hardwareteile festlegen möchten, klicken Sie auf **Advanced**.
6. Wenn Sie Regeln für bestimmte Ereignisse oder in bestimmten Zeitintervallen festlegen möchten, klicken

Sie auf **Regel erstellen**.

7. Sobald Sie die Schwellenwertebenen und Berechnungsintervalle eingestellt haben, wählen Sie im Menü **Datei** > **Speichern**.

Beispiel für die Einstellung eines Schwellenwerts:



- Rot zeigt an, dass Sie einen kritischen Zustand erreicht haben
- Gelb ist ein Warnstatus, der anzeigt, dass Sie sich dem kritischen Zustand nähern
- Grün zeigt an, dass sich die Dinge in einem Normalzustand und innerhalb der ausgewählten Schwellenwerte befinden

Beweissicherung (Erklärung)

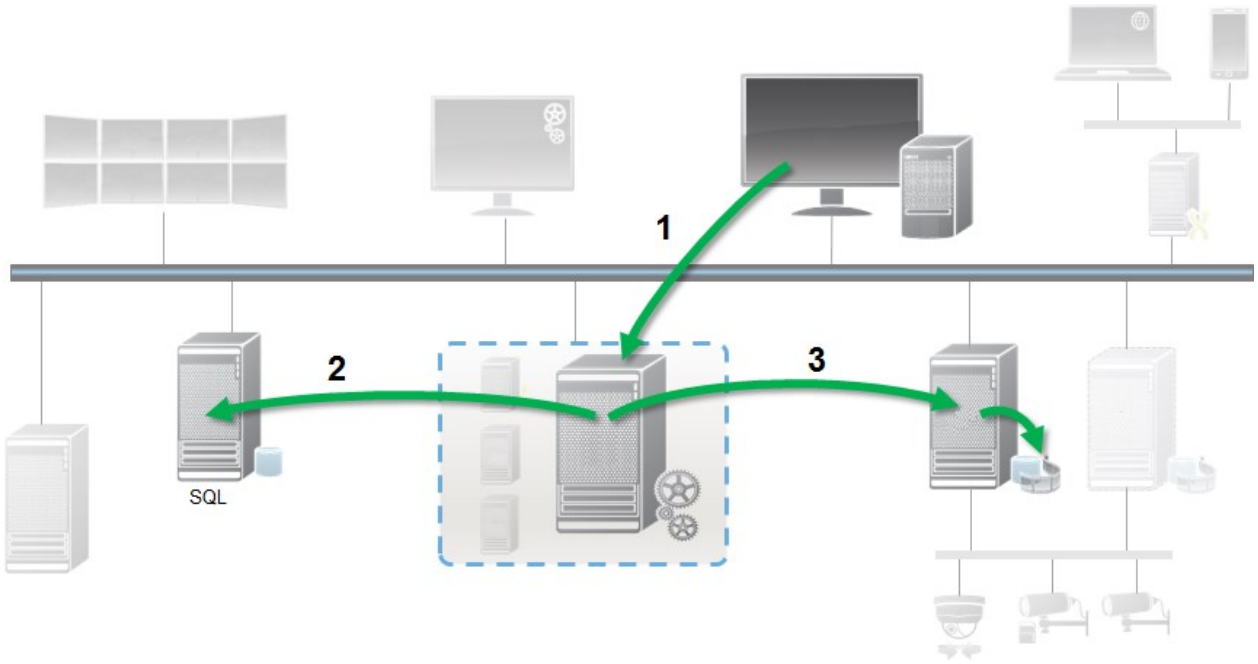
Verfügbare Funktionalität hängt vom verwendeten System ab. Weitere Informationen finden Sie unter https://www.milestonesys.com/solutions/platform/product-index/.

Ab XProtect VMS Version 2020 R2, ist es bei einem Upgrade des Management Servers von einer früheren Version erst wieder möglich, Beweissicherungen auf Aufzeichnungsservern zu erstellen oder zu ändern, die zur Version 2020 R1 oder früher gehören, wenn diese Aufzeichnungsserver aktualisiert wurden.
Das bedeutet auch, dass wenn Hardware von einem Aufzeichnungsserver (ab 2020 R1 oder früher) auf einen anderen umgezogen ist, und dieser weiterhin Aufzeichnungen enthält, Beweissicherungen weder erstellt noch geändert werden können.

Mit der Funktionalität Beweissicherung können Client-Anwender VideoSequenzen, einschließlich Audio und andere Daten vor dem Löschen schützen, falls erforderlich, z. B. bei einer laufenden Untersuchung oder einem laufenden Gerichtsverfahren. Weitere Informationen über Beweissicherungen finden Sie in der XProtect Smart Client-Dokumentation.

Sofern geschützt, können Daten nicht gelöscht werden, weder automatisch vom System nach der standardmäßigen Speicherzeit oder in anderen Situationen, noch manuell vom Client-Benutzer. Das System oder Benutzer kann die Daten nicht löschen bis ein Benutzer mit den notwendigen Rechte das Beweismaterial entsperrt.

Flussdiagramm für Beweissicherung:



1. Benutzer erstellt eine Beweissicherung in XProtect Smart Client. Information wird an den Management-Server gesendet.
2. Der Management Server speichert die Informationen zur Beweissicherung in der SQL-Datenbank.
3. Der Management-Server informiert den Aufzeichnungsserver darüber, die geschützten Aufzeichnungen in der Datenbank zu speichern und sicherzustellen.

Wenn der Anwender eine Beweissicherung erstellt, bleiben die geschützten Daten am Speicherort der Aufzeichnungen und werden dann an archivierende Festplatten zusammen mit den ungeschützten Daten verschoben. Allerdings gilt für die geschützten Daten:

- Folgen der Speicherzeit, die für die Beweissicherung festgelegt wurde. Potentiell unendlich
- Behält die ursprüngliche Qualität der Aufzeichnungen bei, auch wenn die Ausdünnung für ungeschützte Daten eingestellt wurde

Wenn ein Anwender Sicherungen erstellt, beträgt die minimale Größe einer Sequenz den Zeitraum, in dem die Datenbank die aufgezeichneten Dateien aufteilt; Standard-Einstellung sind einstündige Sequenzen. Sie können dies ändern, allerdings erfordert das eine Anpassung der Datei RecorderConfig.xml auf dem Aufzeichnungsserver. Wenn sich eine kleine Sequenz über zwei einstündige Zeiträume hinauszieht, sichert das System die Aufzeichnungen jeweils in beiden Zeiträumen.

Im Auditprotokoll im Management Client, können Sie sehen, wenn ein Benutzer Beweissicherungen erstellt, bearbeitet oder entfernt.

Sollte eine Festplatte nicht mehr genügend Speicherplatz haben, sind geschützte Daten nicht betroffen. Stattdessen werden die ältesten ungeschützten Daten gelöscht. Wenn dem System keine ungeschützten Daten zum Löschen mehr zur Verfügung stehen, wird die Aufzeichnung angehalten. Sie können Regeln und Alarme erstellen, die bei Ereignissen mit vollem Speicherplatz auslösen und Sie so automatisch benachrichtigen.

Die Funktion der Beweissicherung beeinflusst nicht die Systemleistung, außer dass mehr Daten für einen längeren Zeitraum gespeichert werden und daher die Speicherkapazität beeinträchtigen könnte.

Wenn Sie Hardware zu einem anderen Aufzeichnungsserver verschieben (siehe Hardware verschieben auf Seite 506):

- Aufzeichnungen, die von der Beweissicherung geschützt werden, bleiben auf dem alten Aufzeichnungsserver bestehen, gemäß der eingestellten Speicherzeit bei Erstellung der Beweissicherung
- Der XProtect Smart Client-Benutzer kann immer noch Daten mit einer Beweissicherung in den Aufzeichnungen schützen, die auf einer Kamera gemacht wurden, bevor diese zu einem anderen Aufzeichnungsserver verschoben wurden. Selbst wenn Sie die Kamera mehrmals verschieben und die Aufzeichnungen auf mehreren Aufzeichnungsservern gespeichert werden

Standardmäßig wird allen Anwendern ein Standard-Beweissicherungsprofil zugewiesen, das allerdings keine Benutzerzugriffsrechte zu dieser Funktion bietet. Zur Angabe der Zugriffsrechte einer Rolle für die Beweissicherung siehe die Registerkarte Registerkarte „Geräte“ (Rollen) auf Seite 409 zu den Einstellungen einer Rolle. Zur Angabe der Zugriffsrechte einer Rolle für die Beweissicherung siehe die Registerkarte Registerkarte „Info“ (Rollen) auf Seite 379 zu den Einstellungen einer Rolle.

Im Management Client, können Sie die Eigenschaften des Standard-Beweissicherungsprofil bearbeiten und zusätzliche Profile dieser Art erstellen und stattdessen den Rollen zuweisen.

Die Option **Beweissicherung** unter **System-Dashboard** zeigt eine Übersicht aller geschützten Daten auf dem derzeitigen Überwachungssystem:

- Beginn und Enddatum der geschützten Daten
- Der Benutzer, der die Beweise gesichert hat
- Wenn Beweise nicht länger gesichert sind
- Wo die Daten gespeichert sind
- Die Größer jeder Beweissicherung

Alle Informationen in **Beweissicherung** sind Momentaufnahmen. Drücken Sie F5, um zu aktualisieren.

Derzeitige Aufgaben (Erklärung)

Der Knoten **Aktuelle Aufgaben** zeigt eine Übersicht von Aufgaben unter einem ausgewählten Aufzeichnungsserver, dessen Anfangszeit, geschätzte Endzeit und den Fortschritt. Alle Informationen in **Aktuelle Aufgaben** sind Momentaufnahmen. Sie können diese durch Klicken auf die Schaltfläche **Aktualisieren** in der

unteren rechten Ecke des **Eigenschaften** Bereichs aktualisieren.

Konfigurationsberichte (Erklärung)

Wenn Sie PDF-Konfigurationsberichte erstellen, können Sie jegliche gewünschte Elemente Ihres System in diesem Bericht einschließen. Sie können beispielsweise Lizenzen, Gerätekonfigurationen, Alarmkonfigurationen und vieles mehr hinzufügen. Sie können auch Ihre Schriftart und den Seitenaufbau anpassen sowie eine benutzerdefinierte Front Page einschließen.

Einen Konfigurationsbericht hinzufügen

1. Erweitern Sie **System-Dashboard** und klicken Sie auf **Konfigurationsberichte**. Dies zeigt die Seite für die Berichtekonfiguration an.
2. Wählen Sie die Elemente aus, die Sie Ihrem Bericht hinzufügen möchten.
3. **Optional**: Klicken Sie auf **Front Page** zum Anpassen der Front Page. Geben Sie die nötigen Informationen in das Fenster ein. Wählen Sie **Front Page** als einzuschließendes Element in Ihrem Bericht, ansonsten wird die von Ihnen angepasste Front Page nicht im Bericht eingeschlossen.
4. Klicken Sie auf **Formatierung**, um die Schriftart, Seitengröße und -grenzen anzupassen. Wählen Sie im neuen Fenster die gewünschten Einstellungen.
5. Wenn Sie bereit zum Exportieren sind, klicken Sie auf **Exportieren** und wählen Sie einen Namen sowie einen Speicherort für Ihren Bericht.

Berichtdetails konfigurieren

Folgendes steht zur Verfügung, wenn Berichte eingerichtet werden:

Name	Beschreibung
Alle auswählen	Wählt alle Elemente in der Liste aus.
Alle abwählen	Löscht alle Elemente aus der Liste.
Front Page	Passen Sie die Front Page des Berichts an.
Formatierung	Formatieren Sie den Bericht.
Exportieren	Wählen Sie einen Speicherort für den Bericht und erstellen Sie eine PDF.

Site-Navigation: Server-Protokolle

Dieser Abschnitt beschreibt, wie Protokolleinstellungen und Filterprotokolle geändert und Exporte erstellt werden.

Protokolle (erklärt)

Protokolle sind detaillierte Aufzeichnungen von Benutzeraktivitäten, Ereignissen, Aktionen und Fehler im System.

Um Protokolle zu sehen, wählen Sie aus dem Bereich **Standortnavigation** die **Serverprotokolle**.

Protokolltyp	Was wird protokolliert?
Systemprotokolle	Systembezogene Informationen
Auditprotokolle	Benutzeraktivitäten
Von Regel ausgelöste Protokolle	Regeln, in denen Benutzer die Aktion **Neuen <Protokolleintrag> erstellen** bestimmt haben Für weitere Informationen über die Aktion <Protokolleintrag> siehe Aktionen und Stopp-Aktionen (Erklärung) auf Seite 312.

Zum Anzeigen von Protokollen in einer anderen Sprache, siehe Registerkarte „Allgemein“ (Optionen) auf Seite 122 unter **Optionen**.

Um Protokolle als Dateien aus kommagetrennten Werten (.csv) zu exportieren, siehe Protokolle exportieren auf Seite 438.

Siehe Registerkarte „Serverprotokolle“ (Optionen) auf Seite 124, um die Protokolleinstellungen zu ändern.

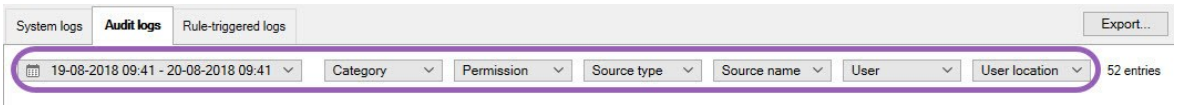
Filterprotokolle

In jedem Protokollfenster, können Sie Filter anwenden, um Log-Einträge betreffend, zum Beispiel, eine bestimmte Zeitspanne, ein Gerät oder einen Benutzer anzuzeigen.

1. Wählen Sie aus dem Bereich **Standortnavigation** die **Serverprotokolle**. Standardmäßig erscheint die Registerkarte **Systemprotokolle**.

   Um zwischen Protokolltypen zu navigieren, wählen Sie eine andere Registerkarte aus.

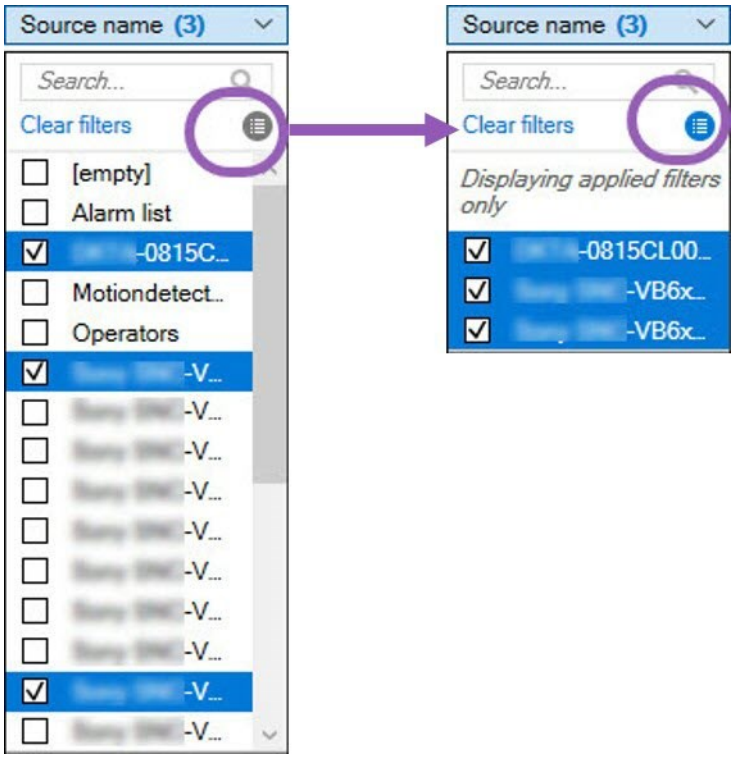
2. Unter den Registerkarten, wählen Sie eine Filtergruppe, zum Beispiel, **Kategorie**, **Quelltyp**, oder **Benutzer** aus.



   Es wird eine Liste von Filtern erscheinen.

3. Wählen Sie einen Filter, um ihn anzuwenden. Wählen Sie den Filter erneut, um ihn zu entfernen.

   Optional: In einer Liste von Filtern, wählen Sie **Nur angewandte Filter anzeigen**, um nur die angewendeten Filter anzuzeigen.



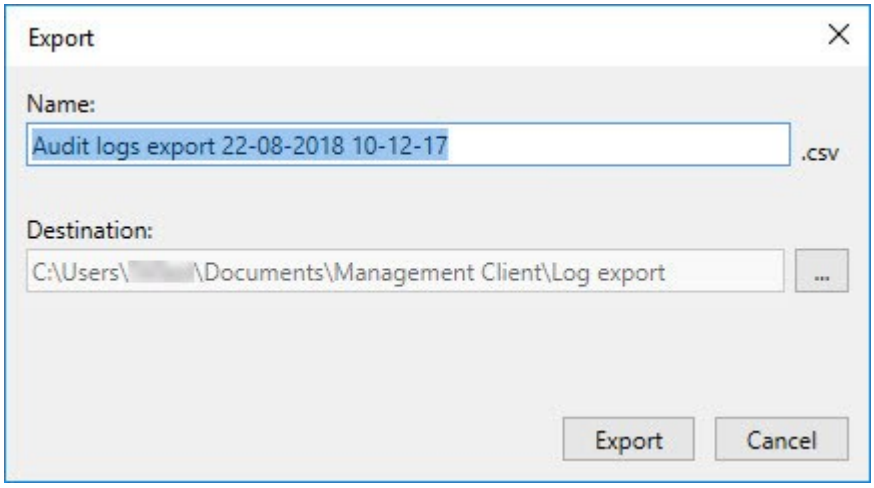
> Der Inhalt von Ihr Export ändert sich, je nachdem welche Filter Sie anwenden. Für Informationen über Ihren Export, siehe Protokolle exportieren auf Seite 438.

Protokolle exportieren

Das Exportieren von Protokollen hilft Ihnen, zum Beispiel, Protokolleinträge über den Aufbewahrungszeitraum für Protokolle hinaus zu speichern. Sie können Protokolle als Dateien aus kommagetrennten Werten (.csv) exportieren.

Wie man ein Protokoll exportiert:

1. Wählen Sie **Export** in der oberen rechten Ecke. Das Fenster **Exportieren** wird geöffnet.



2. Im Fenster **Export** des Felds **Name** können Sie einen Namen für die Protokolldatei bestimmen.
3. Standardmäßig werden Protokolldateien im Ordner **Protokollexport** gespeichert. Um einen anderen Standort zu bestimmen, wählen Sie ... rechts vom Feld **Ziel** aus.
4. Wählen Sie **Export** zum Exportieren des Protokolls.

Der Inhalt von Ihr Export ändert sich, je nachdem welche Filter Sie anwenden. Für Informationen über Ihren Export, siehe Filterprotokolle auf Seite 437.

2018 R2 und früheren Komponenten erlauben, Protokolle aufzuzeichnen

Die 2018 R3 Version des Log-Servers führt eine Authentifizierung für zusätzliche Sicherheit ein. Dies verhindert, dass 2018 R2 und frühere Komponenten auf dem neuen Log-Server Protokolle anlegen können.

Betroffene Komponenten:

- XProtect Smart Client
- XProtect LPR Plug-In
- LPR Server
- Zutrittskontroll-Plug-in
- Event Server
- Alarm Plug-in

Wenn Sie 2018 R2 oder eine frühere Version einer der oben aufgeführten Komponenten einsetzen, müssen Sie entscheiden, ob die Komponente Protokolle auf dem neuen Log-Server anlegen darf:

1. Wählen Sie **Tools** > **Optionen**.
2. Im Dialogfeld **Optionen** am unteren Rand der Registerkarte **Serverprotokoll**, suchen Sie das Kontrollkästchen **2018 R2 und früheren Komponenten erlauben, Protokolle zu schreiben**.
   - Wählen Sie das Kontrollkästchen, das es 2018 R2 und früheren Komponenten erlaubt, Protokolle aufzuzeichnen
   - Leeren Sie das Kontrollkästchen, um es 2018 R2 und früheren Komponenten zu verbieten, Protokolle aufzuzeichnen

Systemprotokolle (Eigenschaften)

Jede Zeile in einem Protokoll stellt einen Protokolleintrag dar. Jeder Protokolleintrag enthält einige Informationsfelder:

Name	Beschreibung
Protokollstufe	Info, Warnung oder Fehler.
Lokalzeit	Zeitstempel in der Ortszeit des Servers Ihres Systems.
Nachrichtentext	Die Identifikationsnummer für den protokollierten Vorfall.
Kategorie	Der Typ des protokollierten Vorfalls.
Quelltyp	Der Gerätetyp, auf dem sich der protokollierte Vorfall ereignet hat, beispielsweise ein Server oder Gerät.
Quellname	Name des Ausrüstungsgegenstands, auf dem sich der protokollierte Vorfall ereignet hat.
Ereignistyp	Der Ereignistyp, den der protokollierte Vorfall repräsentiert.

Auditprotokoll (Eigenschaften)

Jede Zeile in einem Protokoll stellt einen Protokolleintrag dar. Jeder Protokolleintrag enthält einige Informationsfelder:

Name	Beschreibung
Lokalzeit	Zeitstempel in der Ortszeit des Servers Ihres Systems.
Nachrichtentext	Zeigt eine Beschreibung des protokollierten Vorfalls an.
Berechtigung	Die Informationen darüber, ob die Remote Nutzeraktion erlaubt (genehmigt) war oder nicht.
Kategorie	Der Typ des protokollierten Vorfalls.
Quelltyp	Der Gerätetyp, auf dem sich der protokollierte Vorfall ereignet hat, beispielsweise ein Server oder Gerät.
Quellname	Name des Ausrüstungsgegenstands, auf dem sich der protokollierte Vorfall ereignet hat.
Benutzer	Der Benutzername des Remote Nutzers, der den protokollierten Vorfall verursacht hat.
Benutzerstandort	Die IP-Adresse oder der Hostname des Computers, mit dem der Remote Nutzer den protokollierten Vorfall verursacht hat.

Regelausgelöste Protokolle (Eigenschaften)

Jede Zeile in einem Protokoll stellt einen Protokolleintrag dar. Jeder Protokolleintrag enthält einige Informationsfelder:

Name	Beschreibung
Lokalzeit	Zeitstempel in der Ortszeit des Servers Ihres Systems.
Nachrichtentext	Zeigt eine Beschreibung des protokollierten Vorfalls an.
Kategorie	Der Typ des protokollierten Vorfalls.
Quelltyp	Der Gerätetyp, auf dem sich der protokollierte Vorfall ereignet hat, beispielsweise ein

Name	Beschreibung
	Server oder Gerät.
Quellname	Name des Ausrüstungsgegenstands, auf dem sich der protokollierte Vorfall ereignet hat.
Ereignistyp	Der Ereignistyp, den der protokollierte Vorfall repräsentiert.
Regelname	Name der Regel, die den Protokolleintrag ausgelöst hat.
Dienstname	Name des Dienstes, auf dem sich der protokollierte Vorfall ereignet hat.

Seitennavigation: Verwendung von Metadaten

In diesem Artikel lernen Sie zu konfigurieren, wie Ihr Videoüberwachungssystem mit Metadaten umgeht.

Zur Verwaltung und Konfiguration von Metadatengeräten siehe Metadaten-Geräte (Erklärung) auf Seite 218.

Was sind Metadaten?

Metadaten sind Daten zu Daten, z. B. Daten, die das Videobild, den Inhalt, Objekte im Bild oder den Ort beschreiben, an dem das Bild aufgezeichnet wurde.

Metadaten können erzeugt werden von:

- Das Gerät, das selbst die Daten liefert, z. B. eine Kamera, die Videoaufzeichnungen liefert
- Einem Drittsystem oder Integration über einen generischen Metadatentreiber

Metadatensuche (Erklärung)

Eine Metadatensuche ist jede Suche nach Videoaufzeichnungen in XProtect Smart Client, bei der Suchkategorien und Suchfilter verwendet werden, die sich auf Metadaten beziehen.

Die Standardsuchkategorien für Milestone Metadaten sind:

- Ort
- Personen
- Fahrzeuge

Suchanforderungen für Metadaten

Um Suchergebnisse zu erhalten, müssen Sie einen der folgenden Schritte ausführen:

- Mindestens ein Gerät in Ihrem Videoüberwachungssystem, das Videoaufzeichnungen analysieren kann und das korrekt konfiguriert ist
- Ein Videoverarbeitungsdienst in Ihrem Videoüberwachungssystem, der Metadaten erzeugt

In beiden Fällen müssen die Metadaten das erforderliche Metadatenformat haben.

Weitere Informationen finden Sie in der Dokumentation für Integration der Metadatensuche.

Lassen Sie sich die Suchkategorien und Suchfilter für Metadaten anzeigen, in XProtect Smart Client

Benutzer von XProtect Management Client mit Administratorrechten können die Standardsuchkategorien Milestone für Metadaten und Suchfilter in XProtect Smart Client anzeigen und verbergen lassen. Diese Suchkategorien und Suchfilter werden standardmäßig verborgen. Sich diese anzeigen zu lassen, ist nützlich, wenn Ihr Videoüberwachungssystem die Suchanforderungen für Metadaten erfüllt.

Diese Einstellung betrifft alle XProtect Smart Client Benutzer.

Die Einstellung hat keine Auswirkungen auf die Sichtbarkeit von:

- Sonstige Milestone Suchkategorien und Suchfilter die keine Metadaten betreffen, z. B. **Bewegung**, **Lesezeichen**, **Alarme** und **Ereignisse**
- Suchkategorien und Suchfilter von Drittanbietern

1. In XProtect Management Client, im Bereich **Seitennavigation**, wählen Sie **Nutzung von Metadaten** > **Metadatensuche**.
2. Wählen Sie im Bereich **Metadatensuche** die Suchkategorie aus, für die Sie die Anzeigeeinstellungen ändern möchten.
3. Um die Sichtbarkeit einer Suchkategorie oder eines Suchfilters zu aktivieren, aktivieren Sie das entsprechende Kontrollkästchen. Um die Sichtbarkeit einer Suchkategorie oder eines Suchfilters zu deaktivieren, deaktivieren Sie das entsprechende Kontrollkästchen.

Site-Navigation: Alarme

Dieser Abschnitt beschreibt, wie Sie Alarme einstellen können, die, durch Ereignisse ausgelöst, im System erscheinen sollen.

Alarme (Erklärung)

Diese Funktion ist nur verfügbar, wenn XProtect Event Server installiert ist.

Auf Basis der Funktionalität im Event-Server bietet die Alarmfunktion einen allgemeinen Überblick sowie Kontrolle und Skalierbarkeit für Alarme in einer beliebigen Anzahl von Installationen (einschließlich weiterer XProtect-Systeme) innerhalb Ihres Unternehmens. Sie können die Funktion so konfigurieren, dass Alarme auf Folgendem basieren können:

- **Interne systembezogene Ereignisse**

  Zum Beispiel Bewegung, Server antwortet/antwortet nicht, Archivierungsprobleme, zu wenig Speicherplatz usw.

- **Externe integrierte Ereignisse**

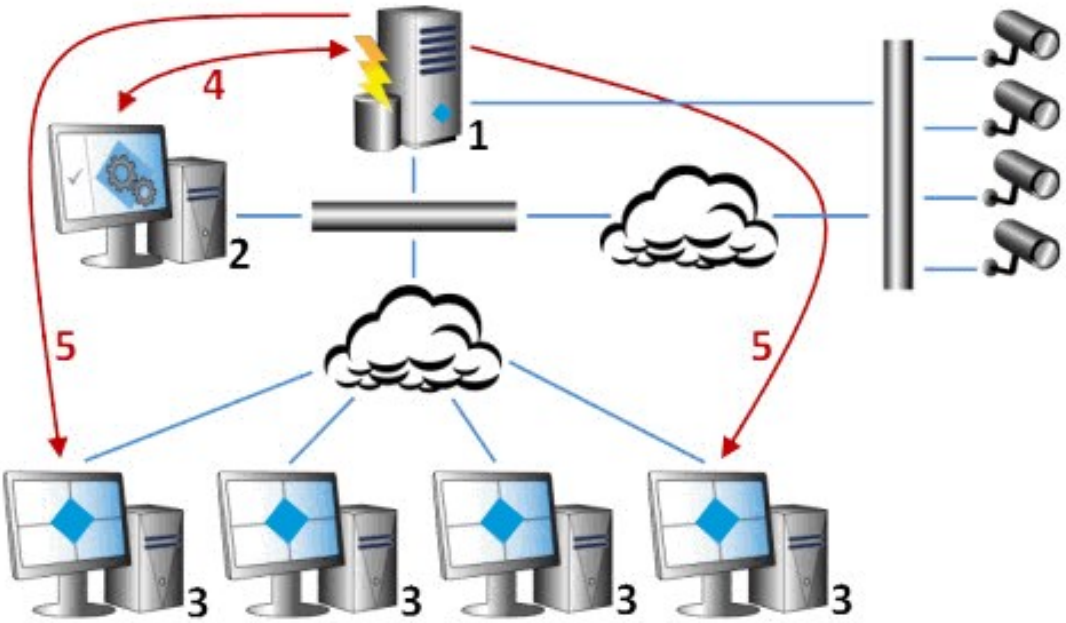
  Diese Gruppe kann aus verschiedenen externen Ereignissen bestehen:

  - **Analyseereignisse**

    Dies betrifft in der Regel Daten, die von Video-Content-Analyse-Lösungen (CVA) anderer Hersteller bezogen wurden.

  - **MIP Plug-in-Ereignisse**

    Mit dem MIP SDK kann ein Drittanbieter individuelle Plug-ins (z. B. für die Integration mit externen Zutrittskontrollsystemen) zu Ihrem System entwickeln.



Legende:

1. Überwachungssystem
2. Management Client
3. XProtect Smart Client
4. Alarmkonfiguration
5. Alarmdatenfluss

Sie bearbeiten und delegieren Alarme in der Alarmliste in XProtect Smart Client. Sie können Alarme auch in die Smart-Map- und Karten-Funktion des XProtect Smart Client integrieren.

Alarmkonfiguration (Erklärung)

Die Alarmkonfiguration umfasst:

- Dynamische rollenbasierte Einrichtung der Alarmbearbeitung
- Zentraler technischer Überblick über alle Komponenten: Server, Kameras und externe Einheiten
- Konfiguration der zentralen Protokollierung aller eingehenden Alarme und Systeminformationen
- Handhabung von Plug-ins zur Unterstützung der benutzerdefinierten Integration anderer Systeme, z. B. externer Zutrittskontroll- oder VCA-basierter Systeme

In der Regel werden Alarme durch die Sichtbarkeit des Objekts kontrolliert, das den Alarm verursacht. Deshalb gibt es vier verschiedene Aspekte, die eine wichtige Rolle in Bezug auf Alarme spielen und bestimmen, wer sie in welchem Umfang kontrollieren/verwalten kann:

Name	Beschreibung
Sichtbarkeit Quelle/Gerät	Wenn das Gerät, das einen Alarm verursacht, in einer Benutzerrolle nicht als sichtbar eingerichtet ist, kann der Benutzer den Alarm nicht in der Alarmliste in XProtect Smart Client sehen.
Das Recht, benutzerdefinierte Ereignisse auszulösen	Dieses Recht legt fest, ob die Rolle des Benutzers die ausgewählten benutzerdefinierten Ereignisse in XProtect Smart Client auslösen kann.
Externe Plug-ins	Wenn in Ihrem System externe Plug-ins eingerichtet wurden, steuern diese möglicherweise die Benutzerrechte zur Bearbeitung von Alarmen.
Allgemeine Rollenrechte	Legen fest, ob der Benutzer Alarme nur ansehen oder auch verwalten darf. Was ein Benutzer von **Alarme** mit Alarmen tun kann, hängt von der Rolle des Benutzers und von den für diese Rolle konfigurierten Einstellungen ab.

Auf der Registerkarte **Alarme und Ereignisse** in **Optionen** können Sie Einstellungen für Alarme, Ereignisse und Protokolle festlegen.

Alarmdefinitionen

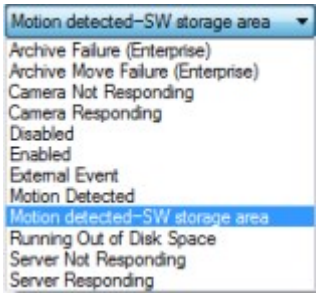
Wenn Ihr System auf Ihrem System ein Ereignis registriert, können Sie das System so konfigurieren, dass es einen Alarm im XProtect Smart Client erstellt. Sie müssen Alarme definieren, bevor Sie diese verwenden können und Alarme werden auf Basis der Ereignisse definiert, die auf Ihren Systemservern registriert werden. Sie können auch benutzerdefinierte Ereignisse verwenden, um Alarme auszulösen und dasselbe Ereignis verwenden, um mehrere verschiedene Alarme auszulösen.

Hinzufügen eines Alarms

Um einen Alarm zu definieren, müssen Sie eine Alarmdefinition erstellen, auf der Sie beispielsweise festlegen, was den Alarm auslöst, wie der Anwender reagieren soll und wodurch oder wann der Alarm angehalten wird. Weitere Einzelheiten zu den Einstellungen s. Alarmdefinitionen (Eigenschaften).

1. Im Bereich **Standort-Navigation** erweitern Sie **Alarme** und klicken mit der rechten Maustaste auf **Alarmdefinitionen**.
2. Wählen Sie **Neu hinzufügen** aus.

3. Tragen Sie diese Eigenschaften ein:
   - **Name**: Geben Sie einen Namen für die Alarmdefinition ein. Der Name der Alarmdefinition erscheint immer, wenn die Alarmdefinition aufgelistet wird.
   - **Anweisungen**: Hier können Sie Anweisungen für den Anwender eingeben, der den Alarm erhält.
   - **Auslösendes Ereignis**: Verwenden Sie die Dropdown-Menüs, um einen Ereignistyp und eine Ereignisnachricht auszuwählen, die verwendet werden, wenn der Alarm ausgelöst wird.

     Eine Liste auswählbarer auslösender Ereignisse. Das hervorgehobene wird mithilfe von Analyseereignissen erstellt und angepasst.
   - **Quellen**: Wählen Sie die Kameras oder anderen Geräte aus, von denen das alarmauslösende Ereignis stammen soll. Ihre Optionen hängen vom Ereignistyp ab, den Sie ausgewählt haben.
   - **Zeitprofil**: Wenn Sie möchten, dass der Alarm während eines bestimmten Zeitintervalls aktiviert wird, wählen Sie die Optionsschaltfläche und dann ein Zeitprofil im Dropdown-Menü aus.
   - **Ereignisgesteuert**: Wenn Sie möchten, dass der Alarm durch ein Ereignis ausgelöst wird, wählen Sie die Optionsschaltfläche aus und bestimmen Sie, welches Ereignis den Alarm starten soll. Sie müssen auch das Ereignis bestimmen, das den Alarm anhalten soll.
4. Bestimmen Sie im Dropdown-Menü **Zeitgrenze** eine Zeitgrenze, an welcher eine Aktion des Anwenders erforderlich ist.
5. Bestimmen Sie im Dropdown-Menü **Ausgelöste Ereignisse**, welches Ereignis ausgelöst werden soll, wenn die Zeitgrenze überschritten wurde.
6. Legen Sie weitere Einstellungen fest, z. B. zugehörige Kameras und anfänglicher Eigentümer des Alarms.

Alarmdefinitionen (Eigenschaften)

Alarmdefinitionseinstellungen:

Name	Beschreibung
Aktivieren	Standardmäßig ist die Alarmdefinition aktiviert. Wählen Sie das Kontrollkästchen ab, um dies zu deaktivieren.
Name	Alarmnamen müssen nicht einmalig sein, aber die Verwendung von einmaligen und selbsterklärenden Alarmnamen bietet in vielen Situationen Vorteile.
Anweisungen	Geben Sie einen beschreibenden Text zu dem Alarm ein und wie das Problem, das den Alarm verursacht hat, zu lösen ist. Der Text erscheint im XProtect Smart Client, wenn der Benutzer den Alarm behandelt.
Auslösendes Ereignis	Wählen Sie die Ereignisnachricht, die angezeigt werden soll, wenn der Alarm ausgelöst wird. Wählen Sie zwischen zwei Dropdown-Menüoptionen: • Die erste Menüoption: Wählen Sie den Ereignistyp, z. B. Analyseereignis und Systemereignisse • Die zweite Menüoption: Wählen Sie die speziell zu verwendende Ereignisnachricht aus. Die verfügbaren Nachrichten werden durch den Ereignistyp bestimmt, den Sie im ersten Dropdown-Menü ausgewählt haben
Quellen	Wählen Sie die Quellen, aus denen die Ereignisse stammen. Abgesehen von Kameras oder anderen Geräten, kann es sich bei den Quellen auch um Plug-in-definierte Quellen handeln, z. B. VCA und MIP. Die Optionen hängen vom Ereignistyp ab, den Sie ausgewählt haben.

Alarmauslöser:

Name	Beschreibung
Zeitprofil	Wählen Sie die Optionsschaltfläche **Zeitprofil** aus, um das Zeitintervall zu bestimmen,

Name	Beschreibung
	während dem die Alarmdefinition aktiv ist. Es wird nur das Zeitprofil auf der Liste angezeigt, das Sie unter dem Knoten **Regeln und Ereignisse** definiert haben. Wenn keines definiert wurde, ist nur die Option **Immer** verfügbar.
Ereignisgesteuert	Wenn Sie möchten, dass der Alarm auf einem Ereignis basiert, wählen Sie diese Optionsschaltfläche. Legen Sie nach dem Auswählen das Start- und Stoppereignis fest. Sie können für Kameras, Videoserver und -eingänge festgelegte Hardware-Ereignisse auswählen. Siehe auch Ereignisübersicht auf Seite 328. Auch globale/manuelle Ereignisdefinitionen können verwendet werden. Siehe auch Benutzerdefinierte Ereignisse auf Seite 360.

Anwenderaktion erforderlich:

Name	Beschreibung
Zeitgrenze	Wählen Sie eine Zeitgrenze, vor der eine Aktion des Anwenders erforderlich ist. Der Standardwert ist 1 Minute. Die Zeitgrenze ist erst aktiv, wenn Sie im Dropdown-Menü **Ausgelöste Ereignisse** ein Ereignis angehängt haben.
Ausgelöste Ereignisse	Wählen Sie aus, welche Ereignisse ausgelöst werden sollen, wenn die Zeitgrenze überschritten wurde.

Karten:

Name	Beschreibung
Alarm-Manager-Ansicht	Weisen Sie dem Alarm entweder eine Smart Map oder eine Karte zu, wenn der Alarm in XProtect Smart Client > **Alarm Manager** aufgeführt ist.  Smart Map zeigt Alarme an, wenn diese von einer Kamera ausgelöst werden und wenn diese Kamera zu der Smart Map hinzugefügt wird. Weitere Informationen dazu, wie Kameras zur Smart Map hinzugefügt werden, finden Sie unter Hinzufügen, Löschen oder Bearbeiten von Kameras auf einer Smart Map.

Andere:

Name	Beschreibung
Zugehörige Kameras	Wählen Sie bis zu 15 Kameras aus, die in die Alarmdefinition eingeschlossen werden, auch wenn diese Kameras den Alarm nicht selbst auslösen. Das kann relevant sein, wenn Sie z. B. eine externe Ereignisnachricht (wie z. B. eine Tür, die geöffnet wird) als Quelle Ihres Alarms ausgewählt haben. Wenn Sie eine oder mehrere Kameras in der Nähe der Tür definieren, können Sie die Kameraaufzeichnungen des Vorfalls an den Alarm anhängen.
Anfänglicher Eigentümer des Alarms	Auswahl eines standardmäßig verantwortlichen Benutzers für den Alarm.
Anfängliche Alarmpriorität	Wählen Sie eine Priorität für den Alarm aus. Verwenden Sie diese Prioritäten in XProtect Smart Client, um die Wichtigkeit eines Alarms zu festzulegen.
Alarmkategorie	Wählen Sie für den Alarm eine Alarmkategorie aus, z. B. **Fehlalarm** oder **Untersuchung erforderlich**.
Durch Alarm ausgelöste Ereignisse	Definieren Sie ein Ereignis, das der Alarm in XProtect Smart Client auslösen kann.
Alarm automatisch schließen	Aktivieren Sie dieses Kontrollkästchen, wenn ein bestimmtes Ereignis den Alarm automatisch anhalten soll. Nicht alle Ereignisse können Alarme auslösen. Deaktivieren Sie das Kontrollkästchen, um den neuen Alarm am Anfang zu deaktivieren.
Administratoren zuzuordnende Alarme	Wählen Sie das Kontrollkästchen aus, um Benutzern mit Administratorrolle in die Liste **Zugewiesen zu** aufzunehmen. Die**, die der** Liste zugeordnet ist, befindet sich in den Alarmdetails auf der Registerkarte **Alarm Manager** in XProtect Smart Client. Deaktivieren Sie das Kontrollkästchen, um Benutzer mit Administratorrolle aus der Liste **Zugewiesen zu** herauszufiltern, um die Liste zu kürzen.

Alarmdateneinstellungen

Legen Sie beim Konfigurieren der Alarmdateneinstellungen Folgendes fest:

Registerkarte „Alarm-Datenstufen“
Prioritäten

Name	Beschreibung
Stufe	Fügen Sie neue Prioritäten mit frei wählbaren Stufenzahlen hinzu oder verwenden/bearbeiten Sie die standardmäßigen Prioritätsstufen (Zahl 1, 2 oder 3). Diese Prioritätsstufen werden zur Konfiguration der Einstellung **Anfängliche Alarmpriorität** verwendet.
Name	Geben Sie einen Namen für die Entität ein. Sie können beliebig viele erstellen.
Ton	Wählen Sie den Ton, der mit dem Alarm verknüpft werden soll. Verwenden Sie einen der Standardtöne oder fügen Sie weitere unter **Toneinstellungen** hinzu.
Ton wiederholen	Entscheiden Sie, ob der Ton nur einmal oder wiederholt abgespielt werden soll, bis der Benutzer in XProtect Smart Client in der Alarmliste auf den Alarm klickt.
Aktivieren Sie die Desktop-Benachrichtigungen	Für jede Alarmpriorität können Sie die Desktop-Benachrichtigungen aktivieren oder deaktivieren. Wenn Sie ein XProtect VMS verwenden, das Smart Client-Profile unterstützt, müssen Sie auf den erforderlichen Smart Client Profilen auch die Benachrichtigungen aktivieren. Siehe die Registerkarte Registerkarte Alarm-Manager (Smart Client-Profile) auf Seite 302.

Zustände

Name	Beschreibung
Stufe	Zusätzlich zu den standardmäßigen Zustandsstufen (Zahlen **1**, **4**, **9** und **11**, die nicht bearbeitet oder wiederverwendet werden können) können Sie neue Zustände mit frei wählbaren Stufenzahlen hinzufügen. Diese Zustandsstufen sind nur auf der *Alarmliste* von XProtect Smart Client sichtbar.

Kategorien

Name	Beschreibung
Stufe	Fügen Sie neue Kategorien mit frei wählbaren Stufenzahlen hinzu. Diese Kategoriestufen werden zur Konfiguration der Einstellung **Anfängliche Alarmkategorie** verwendet.
Name	Geben Sie einen Namen für die Entität ein. Sie können beliebig viele erstellen.

Konfiguration der Alarmliste-Registerkarte

Name	Beschreibung
Verfügbare Spalten	Verwenden Sie >, um auszuwählen, welche Spalten in der *Alarmliste* von XProtect Smart Client verfügbar sein sollen. Verwenden Sie < zum Aufheben der Auswahl. Danach sollte **Ausgewählte Spalten** die einzuschließenden Elemente enthalten.

Registerkarte „Gründe für das Schließen“

Name	Beschreibung
Aktivieren	Auswählen, um zu aktivieren, dass allen Alarmen ein Schließungsgrund zugewiesen werden muss, bevor sie geschlossen werden können.
Grund	Fügen Sie Schließungsgründe hinzu, zwischen denen der Benutzer beim Schließen von Alarmen wählen kann. Diese könnten z. B. sein: *Unbefugter Zutritt aufgeklärt* oder *Fehlalarm*. Sie können beliebig viele erstellen.

Toneinstellungen

Legen Sie beim Konfigurieren der Toneinstellungen Folgendes fest:

Name	Beschreibung
Töne	Wählen Sie den Ton, der mit dem Alarm verknüpft werden soll. Die Tonliste enthält einige standardmäßige Windows-Sounds. Sie können auch neue Töne hinzufügen (.wav oder .mp3).
Hinzufügen	Töne hinzufügen. Suchen Sie in den Audiodateien und laden Sie eine oder mehrere .wav- oder .mp3-Dateien hoch.
Entfernen	Entfernen Sie einen ausgewählten Ton von der Liste der manuell hinzugefügten Töne. Standardtöne können nicht entfernt werden.
Test	Testen Sie den Ton. Wählen Sie den Ton auf der Liste. Der Ton wird einmal abgespielt.

Verschlüsselung aktivieren

Wenn Sie die Verschlüsselung für eine Gruppe von Servern konfigurieren, muss diese entweder mit einem Zertifikat aktiviert werden, das zum gleichen CA-Zertifikat gehört, oder, wenn sie deaktiviert ist, muss sie auf allen Computern in dieser Gruppe von Servern deaktiviert werden.

Die Verschlüsselung zum und vom Managementserver aktivieren

Sie können die wechselseitige Verbindung zwischen dem Management Server und dem Aufzeichnungsserver oder sonstigen Remote Servern mit dem Datensammler (Ereignisserver, Protokollserver, LPR Server und Mobile Server) verschlüsseln.

Wenn Ihr System mehrere Aufzeichnungsserver oder Remote Server hat, müssen Sie die Verschlüsselung für alle diese Server aktivieren. Weitere Informationen finden Sie unter Verschlüsselung des Managementservers (Erläuterung): auf Seite 70.

Voraussetzungen:

- Einem Server-Authentifizierungszertifikat wird auf dem Computer vertraut, auf dem der Managementserver gehostet wird

Aktivieren Sie zunächst die Verschlüsselung auf dem Managementserver.

Schritte:

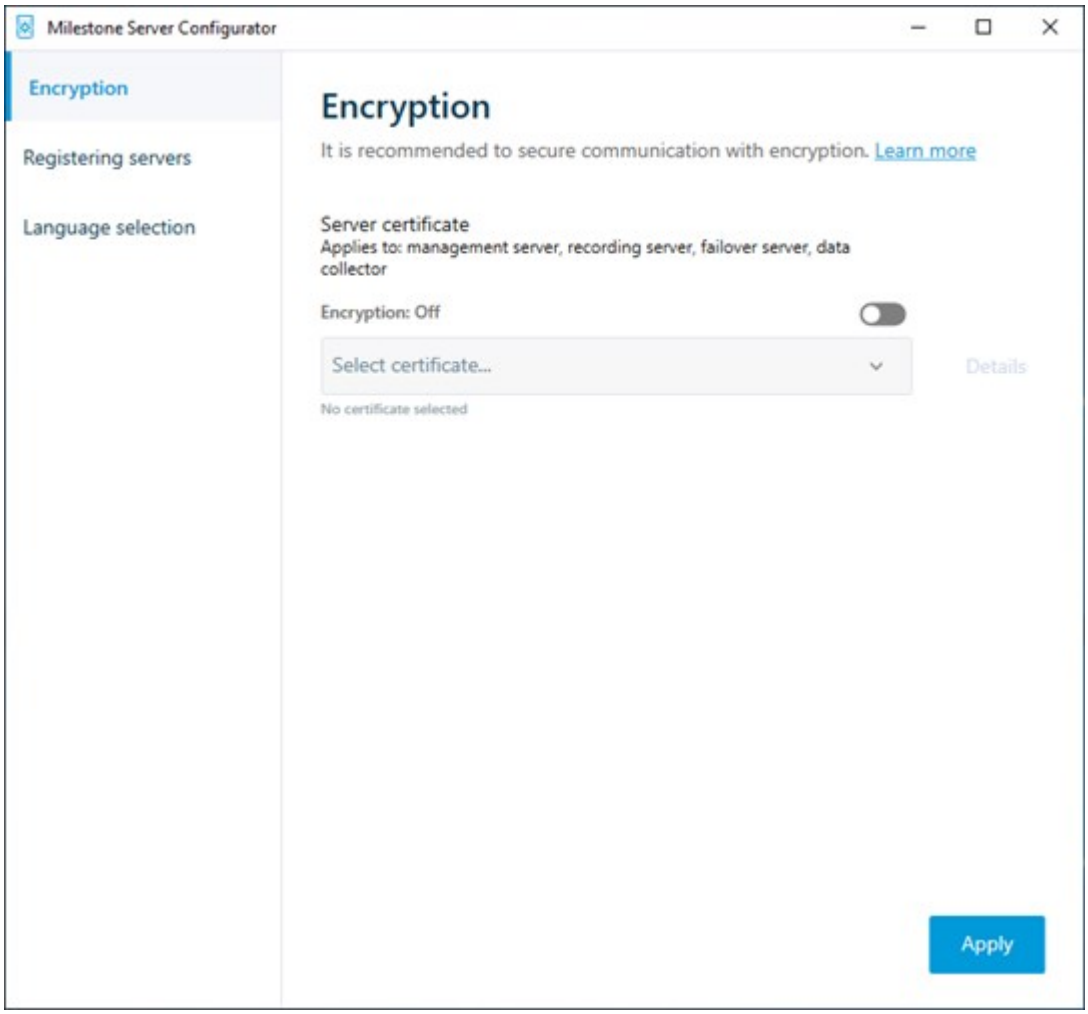
1. Öffnen Sie auf einem Computer mit installiertem Management Server die **Server Configurator** von:
   - Das Windows-Startmenü

   oder

- Das Management Server Manager durch Klicken mit der rechten Maustaste auf das Symbol Management Server Manager auf der Taskleiste des Computers

2. Aktivieren Sie in der **Server Configurator**, unter **Serverzertifikat** die **Verschlüsselung**.
3. Klicken Sie auf **Zertifikat auswählen**, um eine Liste der eindeutigen Themennamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und die auf dem lokalen Computer im Windows Certificate Store installiert sind.
4. Wählen Sie ein Zertifikat aus, das zur Verschlüsselung der Kommunikation zwischen dem Aufzeichnungsserver, dem Management Server, dem Failover-Server und dem Datensammlerserver verwendet werden soll.

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



5. Klicken Sie auf **Anwenden**.

Um die Aktivierung der Verschlüsselung abzuschließen, ist der nächste Schritt die Aktualisierung der Verschlüsselungseinstellungen auf jedem Aufzeichnungsserver und auf jedem Server mit einem Datensammler (Ereignisserver, Protokollserver, LPR Server und Mobile Server).

Weitere Informationen finden Sie unter Verschlüsselung für Aufzeichnungsserver oder Remote Server aktivieren auf Seite 455.

Verschlüsselung für Aufzeichnungsserver oder Remote Server aktivieren

Sie können die wechselseitige Verbindung zwischen dem Management Server und dem Aufzeichnungsserver oder sonstigen Remote Servern mit dem Datensammler (Ereignisserver, Protokollserver, LPR Server und Mobile Server) verschlüsseln.

Wenn Ihr System mehrere Aufzeichnungsserver oder Remote Server hat, müssen Sie die Verschlüsselung für alle diese Server aktivieren. Weitere Informationen finden Sie unter Verschlüsselung vom Management-Server zum Aufzeichnungsserver (Erläuterung) auf Seite 72 und Verschlüsselung zwischen dem Management Server und den Data Collector Server (Erläuterung) auf Seite 73.

Voraussetzungen:

- Sie haben die Verschlüsselung auf dem Managementserver aktiviert, s. Verschlüsselung aktivieren auf Seite 453

Schritte:

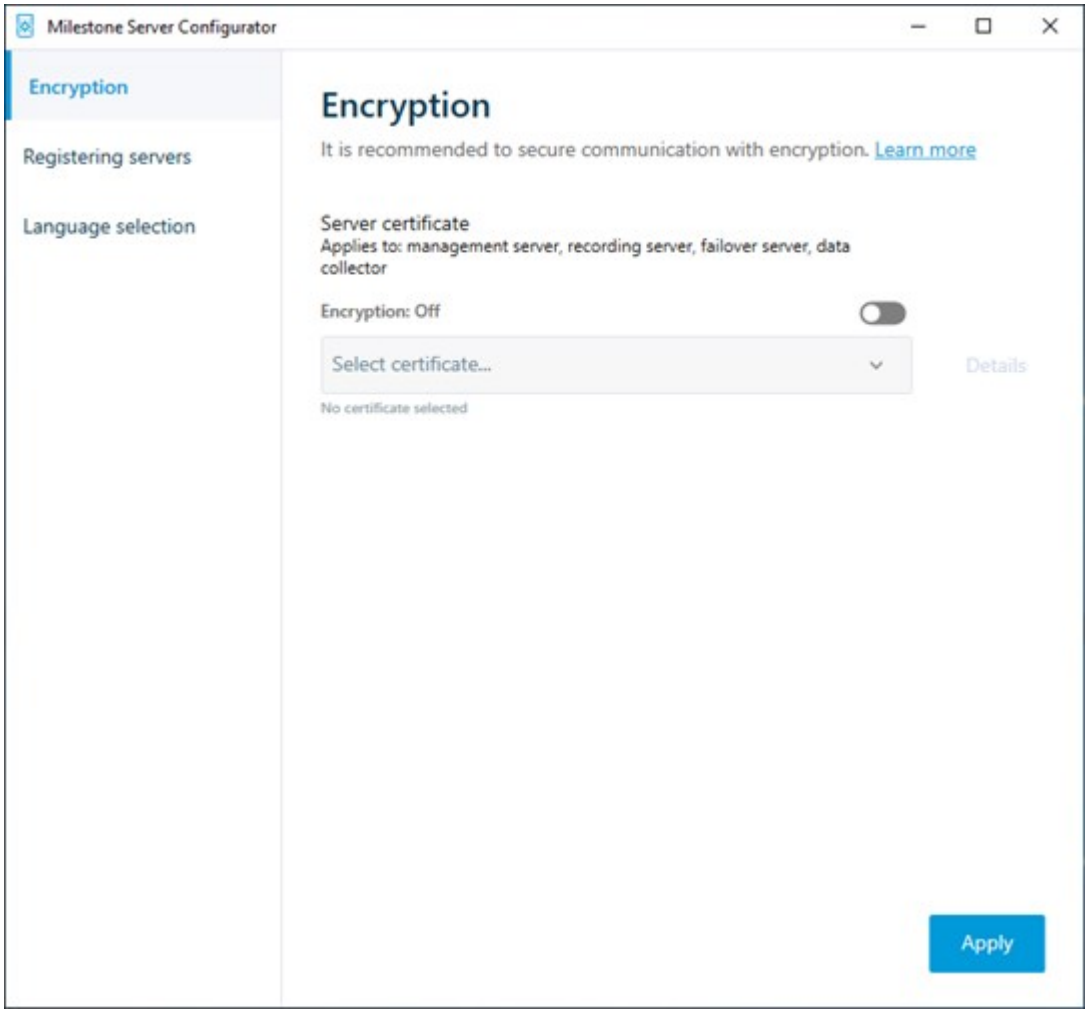
1. Öffnen Sie auf einem Computer mit installiertem Aufzeichnungsserver die **Server Configurator** von:
   - Das Windows-Startmenü

   oder

   - Das Recording Server Manager durch Klicken mit der rechten Maustaste auf das Symbol Recording Server Manager auf der Taskleiste des Computers
2. Aktivieren Sie in der **Server Configurator**, unter **Serverzertificat** die **Verschlüsselung**.
3. Klicken Sie auf **Zertifikat auswählen**, um eine Liste der eindeutigen Themennamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und die auf dem lokalen Computer im Windows Certificate Store installiert sind.
4. Wählen Sie ein Zertifikat aus, das zur Verschlüsselung der Kommunikation zwischen dem Aufzeichnungsserver, dem Management Server, dem Failover-Server und dem Datensammlerserver verwendet werden soll.

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

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



2. Klicken Sie auf **Anwenden**.

> Wenn Sie Zertifikate anwenden, wird der Aufzeichnungsserver angehalten und neu gestartet. Das Anhalten des Dienstes Aufzeichnungsserver bedeutet, dass Sie keine Live-Videoaufnahmen machen und anschauen können, während Sie die Basiskonfiguration des Aufzeichnungsservers überprüfen oder ändern.

Verschlüsselung zu Clients und Servern aktivieren

Sie können Verbindungen vom Aufzeichnungsserver an Clients und Dienste verschlüsseln, die Daten vom Aufzeichnungsserver streamen. Weitere Informationen finden Sie unter Verschlüsselung an alle Clients und Dienste, die Daten vom Aufzeichnungsserver abrufen (Erläuterung) auf Seite 74.

Voraussetzungen:

- Dem zu verwendenden Serverauthenfizierungszertifikat wird von allen Computern vertraut, die Dienste

ausführen, die Datenstreams vom Aufzeichnungsserver abrufen

- XProtect Smart Client und alle Dienste, die Datenströme vom Aufzeichnungsserver abrufen, müssen die Version 2019 R1 oder später haben
- Manche der Lösungen von Drittanbietern, die mit Hilfe von Versionen von MIP SDK erstellt wurden, die vor der Version 2019 R1 lagen, müssen ggf. aktualisiert werden

Schritte:

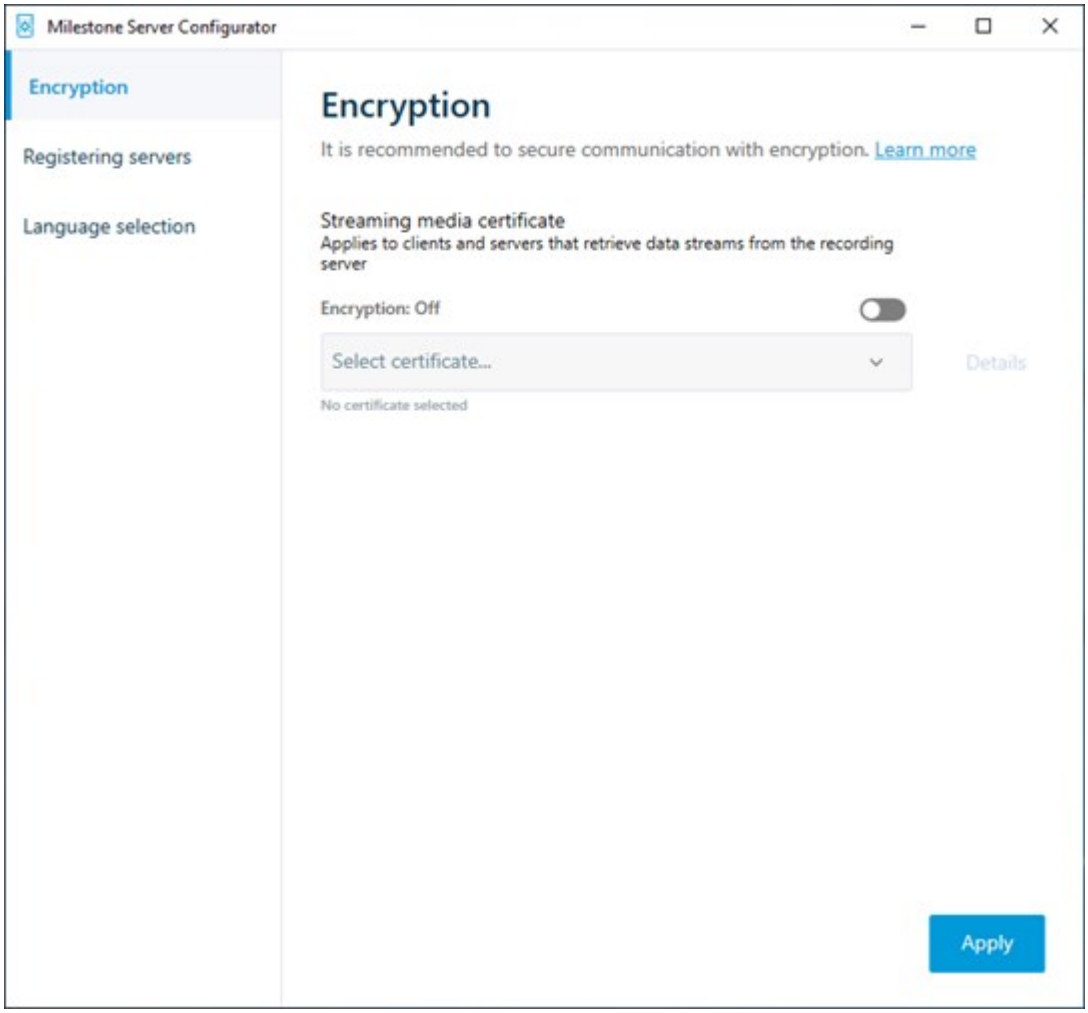
1. Öffnen Sie auf einem Computer mit installiertem Aufzeichnungsserver die **Server Configurator** von:
   - Das Windows-Startmenü

   oder

   - Das Recording Server Manager durch Klicken mit der rechten Maustaste auf das Symbol Recording Server Manager auf der Taskleiste des Computers
2. Aktivieren Sie in der **Server Configurator**, unter **Zertifikat für Streaming-Medien** die **Verschlüsselung**.
3. Klicken Sie auf **Zertifikat auswählen**, um eine Liste der eindeutigen Themennamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und die auf dem lokalen Computer im Windows Certificate Store installiert sind.
4. Wählen Sie ein Zertifikat aus, das für die Verschlüsselung der Kommunikation zwischen den Clients und Servern verwendet werden soll, die Datenstreams vom Aufzeichnungsserver abrufen.

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

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



2. Klicken Sie auf **Anwenden**.

> Wenn Sie Zertifikate anwenden, wird der Aufzeichnungsserver angehalten und neu gestartet. Das Anhalten des Dienstes Aufzeichnungsserver bedeutet, dass Sie keine Live-Videoaufnahmen machen und anschauen können, während Sie die Basiskonfiguration des Aufzeichnungsservers überprüfen oder ändern.

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

Aktivieren Sie die Verschlüsselung auf dem mobilen Server.

Wenn Sie für die Verbindung zwischen einem mobilen Server und den Clients und Diensten ein sicheres HTTPS-Protokoll verwenden möchten, müssen Sie auf dem Server ein gültiges Zertifikat installieren. Das Zertifikat

bestätigt, dass der Zertifikatsinhaber berechtigt ist, sichere Verbindungen herzustellen. Weitere Informationen finden Sie unter Datenverschlüsselung des mobilen Servers (Erläuterung) auf Seite 76 und Anforderungen zur Verschlüsselung mobiler Server für Clients auf Seite 77.

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

Schritte:

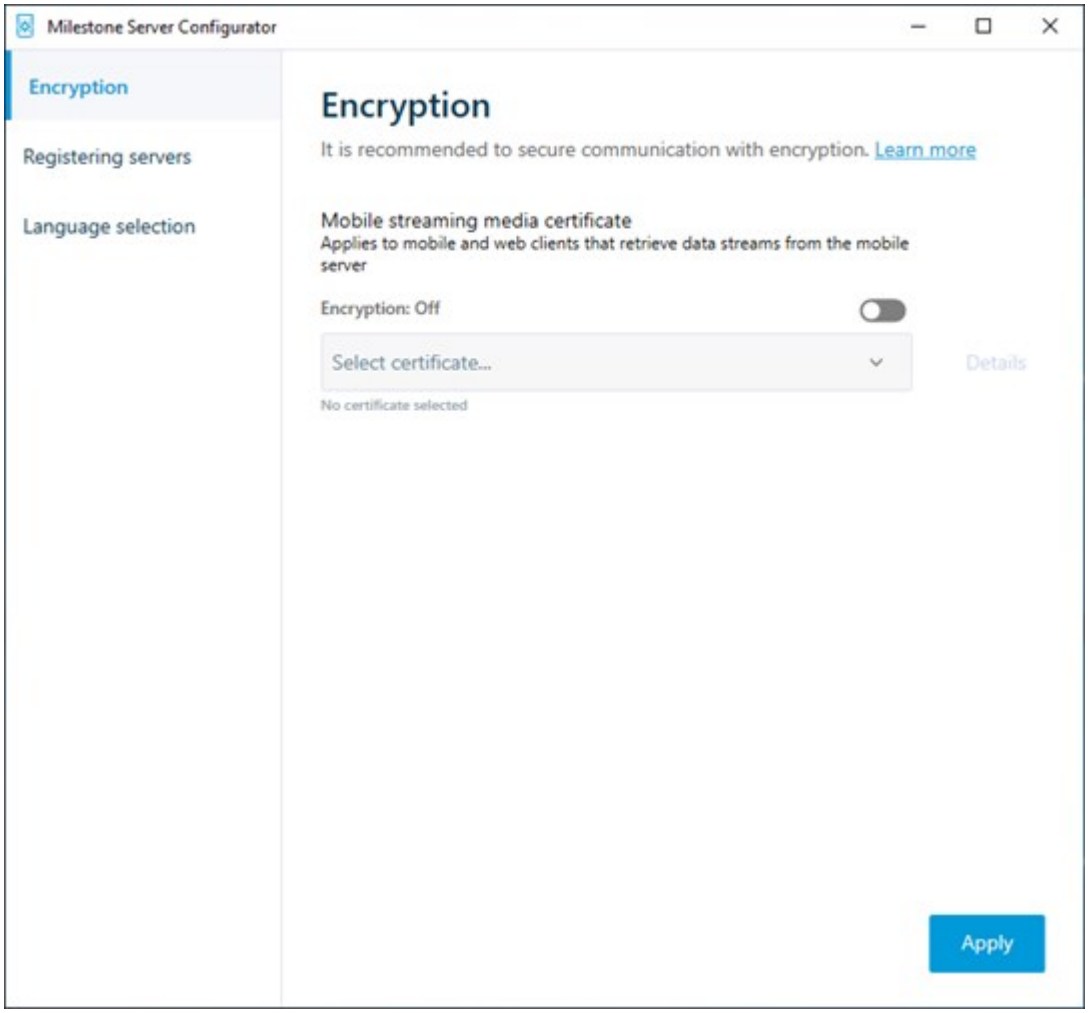
1. Öffnen Sie auf einem Computer mit installiertem Management Server die **Server Configurator** von:
   - Das Windows-Startmenü

   oder

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

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

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



2. Klicken Sie auf **Anwenden**.

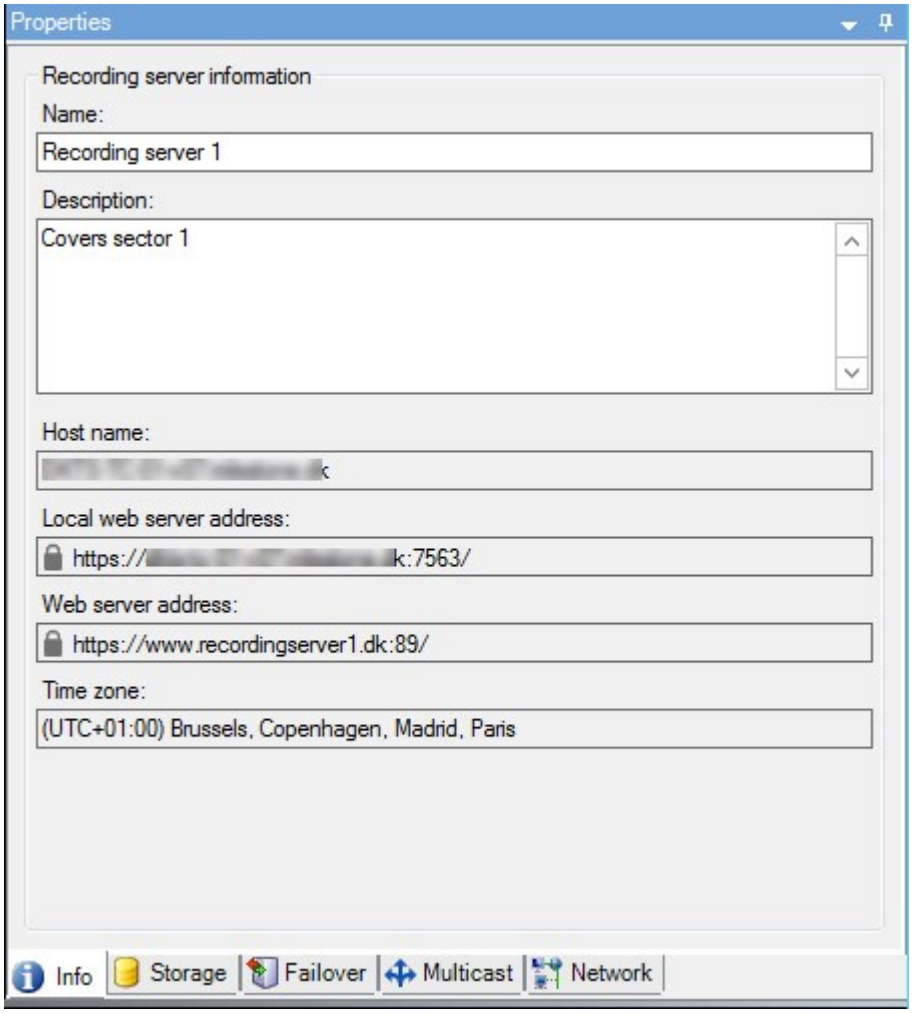
Wenn Sie Zertifikate anwenden, wird der Mobile Server-Dienst neu gestartet.

Verschlüsselungsstatus an Clients anzeigen

Um zu überprüfen, ob Ihr Aufzeichnungsserver eine Verschlüsselung verwendet:

1. Öffnen Sie den Management Client.
2. Wählen Sie im Bereich **Standort-Navigation** die Optionen **Server** > **Aufzeichnungsserver**. Daraufhin wird eine Liste mit Aufzeichnungsservern geöffnet.

3. Wählen Sie in dem Fenster **Übersicht** den jeweiligen Aufzeichnungsserver aus und gehen Sie auf die Registerkarte **Info**.
   Wenn die Verschlüsselung zu Clients und Servern, die Datenstreams vom Aufzeichnungsserver abrufen, aktiviert ist, erscheint ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der des optionalen Webservers.



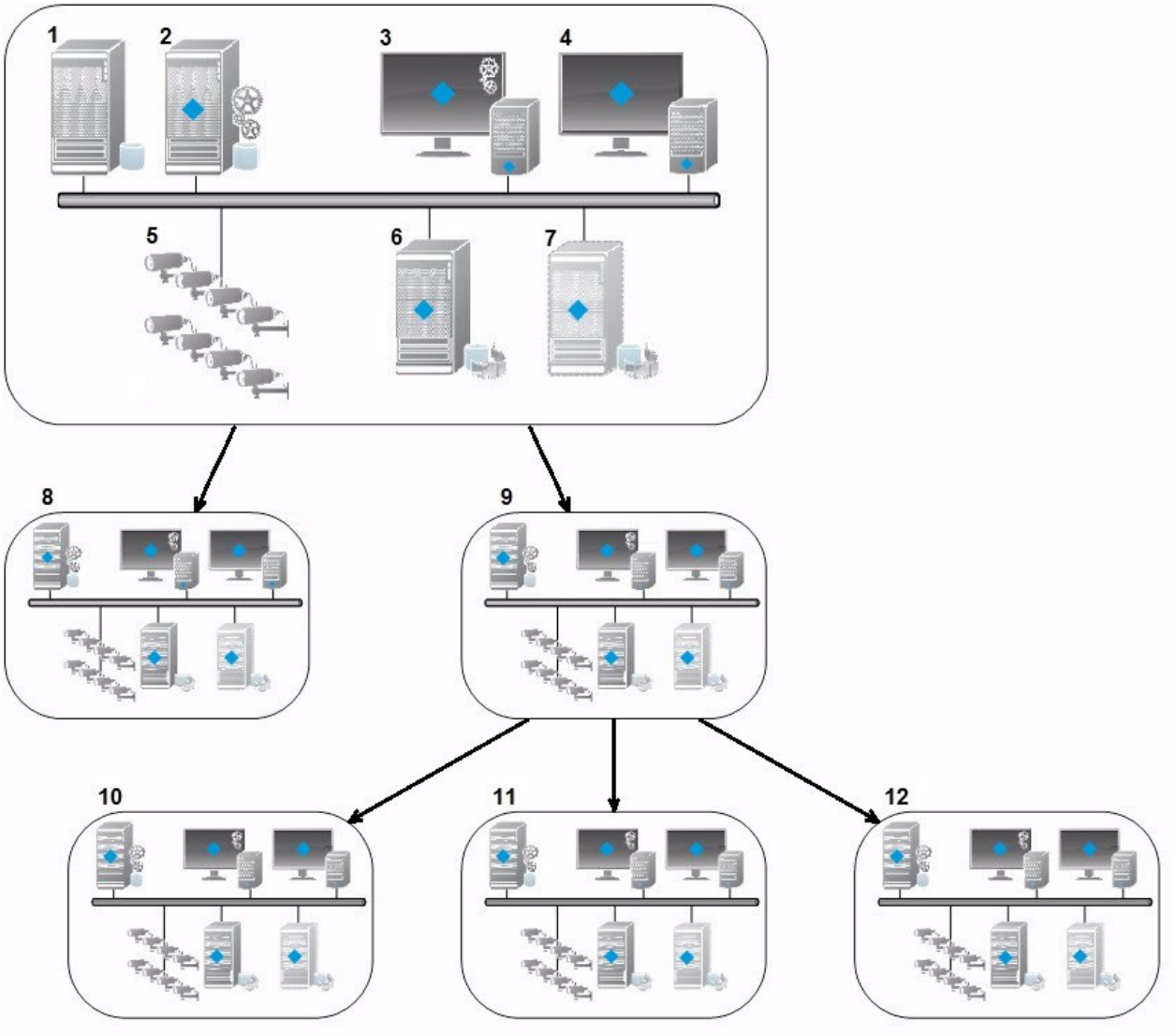
Konfigurieren von Milestone Federated Architecture

XProtect Expert können nur als untergeordnete Standorte eingebunden werden.

Milestone Federated Architecture verbindet mehrere einzelne Standardsysteme zu einer Hierarchie von über- und untergeordneten föderalen Standorten. Client-Benutzer mit ausreichenden Rechten haben nahtlosen Zugriff auf Video, Audio und andere Ressourcen an den individuellen Standorten. Administratoren können ab 2018 R1 und neueren Versionen innerhalb der föderalen Hierarchie aufgrund ihrer Administratorrechte für die einzelnen Standorte alle diese Standorte zentral verwalten.

Benutzer mit Basisrechten werden in Milestone Federated Architecture-Systemen nicht unterstützt, daher müssen Sie über den Dienst Active Directory neue Benutzer als Windows-Benutzer hinzufügen.

Milestone Federated Architecture besteht aus einem zentralen Standort (übergeordneter Standort) und einer unbegrenzten Anzahl an föderalen Standorten (siehe Einrichten Ihres Systems für föderale Standorte auf Seite 465). Wenn Sie sich an einem Standort anmelden, haben Sie Zugriff auf die Informationen aller untergeordneten Standorte und auch auf die Standorte, die wiederum diesen untergeordnet sind. Die Verknüpfung zwischen zwei Standorten wird aufgebaut, wenn Sie die Verbindung vom übergeordneten Standort anfordern (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 467). Ein untergeordneter Standort kann nur mit einem einzigen übergeordneten Standort verbunden werden. Sollten Sie nicht der Administrator des untergeordneten Standorts sein, wenn Sie ihn zur Hierarchie der föderalen Standorte hinzufügen, muss die Anfrage vom Administrator des untergeordneten Standorts angenommen werden.



Die Bestandteile einer Milestone Federated Architecture-Konfiguration:

1. Server mit SQL Server
2. Managementserver
3. Management Client
4. XProtect Smart Client
5. Kameras
6. Aufzeichnungsserver
7. Failover-Aufzeichnungsserver
8. bis 12. Föderale Standorte

Synchronisierung der Hierarchie

Ein übergeordneter Standort enthält eine sich aktualisierende Liste aller gegenwärtig untergeordneten Standorte, der Standorte die wiederum diesen untergeordnet sind und so weiter. Die Hierarchie der föderalen Standorte verfügt sowohl über eine planmäßige Synchronisierung zwischen den Standorten, als auch über eine Synchronisierung, die ausgelöst wird, wenn ein Standort durch einen System-Administrator hinzugefügt oder entfernt wird. Die Synchronisierung der Hierarchie durch das System läuft von Ebene zu Ebene ab, wobei jede Ebene die Kommunikation weiterleitet und zurücksendet, bis Sie den Server erreicht, der die Informationen anfordert. Das System versendet jedes Mal weniger als 1 MB. Je nach Anzahl der Ebenen kann es einige Zeit dauern, bis die Änderungen an einer Hierarchie in Management Client sichtbar werden. Sie können den Zeitplan für die Synchronisierungen nicht selbst festlegen.

Datenverkehr

Das System sendet Kommunikations- oder Konfigurationsdaten, wenn sich ein Benutzer oder Administrator ein Live-Video oder eine Videoaufzeichnung ansieht oder einen Standort konfiguriert. Die Datenmenge hängt davon ab, was und wie viel angesehen oder konfiguriert wird.

Milestone Federated Architecture mit anderen Produkten

- Wenn der zentrale Standort XProtect Smart Wall verwendet, können Sie auch die Funktionen von XProtect Smart Wall in der Hierarchie der föderalen Standorte verwenden. Siehe Smart Walls konfigurieren auf Seite 285 zur Einrichtung von XProtect Smart Wall
- Wenn der zentrale Standort XProtect Access verwendet und sich ein XProtect Smart Client-Benutzer an einem Standort der föderalen Standorthierarchie anmeldet, erscheinen Benachrichtigungen für Zutrittsanforderungen von den föderalen Standorten auch in XProtect Smart Client
- Sie können XProtect Expert 2013-Systeme oder neuere zur Hierarchie der föderalen Standorte als untergeordnete Standorte hinzufügen, nicht als übergeordnete Standorte.

- Die Milestone Federated Architecture benötigt keine zusätzlichen Lizenzen
- Weitere Informationen zu Anwendungsfällen und deren Vorteilen finden Sie im Whitepaper zu Milestone Federated Architecture.

Anlegen einer Hierarchie der föderalen Standorte

Milestone empfiehlt Ihnen, aufzuzeichnen, wie Sie Ihre Standorte miteinander verbinden wollen, bevor Sie in Management Client die Hierarchie aufbauen.

Sie installieren und konfigurieren jeden Standort in einer föderalen Hierarchie als ein normales Standalone-System mit standardmäßigen Systemkomponenten, Einstellungen, Regeln, Zeitplänen, Administratoren, Benutzern und Benutzerrechten. Wenn Sie die Standorte bereits installiert und konfiguriert haben und sie nur noch in eine Hierarchie der föderalen Standorte kombinieren müssen, sind Ihre Systeme zum Einrichten bereit.

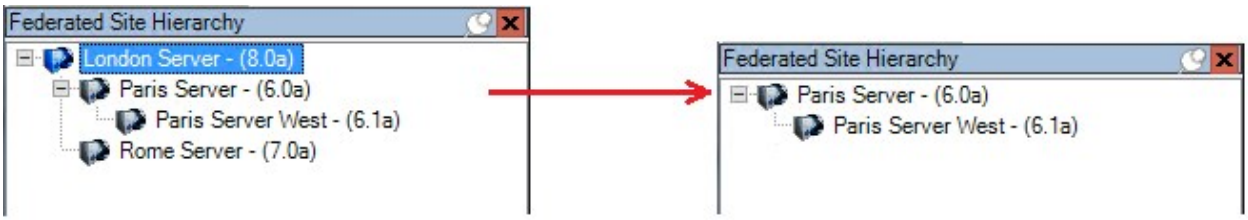
Sobald die einzelnen Standorte installiert sind, müssen Sie sie einrichten, damit sie als föderale Standorte funktionieren (siehe Einrichten Ihres Systems für föderale Standorte auf Seite 465).

Um mit dem Aufbau der Hierarchie zu beginnen, melden Sie sich an dem Standort an, der als zentraler Standort dienen soll, und fügen Sie den ersten Verbundstandort hinzu (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 467). Sobald die Verbindung besteht, erstellen die beiden Standorte automatisch eine Hierarchie der föderalen Standorte im Fenster **Hierarchie der föderalen Standorte** in Management Client. Hier können Sie weitere Standorte hinzufügen und damit die föderale Hierarchie ausbauen.

Sobald Sie eine Hierarchie der föderalen Standorte erstellt haben, können sich Benutzer und Administratoren an einem Standort anmelden und auf diesen sowie alle zugehörigen föderalen Standorte zugreifen. Der Zugriff auf föderale Standorte hängt von den Benutzerrechten ab.

Sie können der föderalen Hierarchie eine unbeschränkte Anzahl an Standorten hinzufügen. Außerdem kann ein Standort auf einer älteren Produktversion mit einer neueren Version verbunden sein und umgekehrt. Die Versionsnummern erscheinen automatisch und können nicht gelöscht werden. Der Standort, an dem Sie angemeldet sind, befindet sich immer ganz oben im Fenster **Hierarchie der föderalen Standorte** und wird als Heimstandort bezeichnet.

Weiter unten finden Sie ein Beispiel für einen föderalen Standort im Management Client. Auf der linken Seite hat sich der Benutzer auf dem obersten Standort angemeldet. Auf der rechten Seite hat sich der Benutzer bei einer der untergeordneten Standpunkte, dem Pariser Server, angemeldet, der dann der Home-Standort ist.



Statussymbole in der Milestone Federated Architecture

Die Symbole repräsentieren den Status eines Standorts:

Beschreibung	Symbol
Der oberste Standort in der ganzen Hierarchie ist betriebsbereit.	
Der oberste Standort in der ganzen Hierarchie ist betriebsbereit, aber es liegt mindestens ein Problem vor. Wird oben auf dem Symbol des obersten Standorts angezeigt.	
Der Standort ist betriebsbereit.	
Der Standort wartet darauf, in die Hierarchie aufgenommen zu werden.	
Der Standort wird gerade angegliedert, ist aber noch nicht betriebsbereit.	

Einrichten Ihres Systems für föderale Standorte

Um Ihr System auf die Milestone Federated Architecture vorzubereiten, müssen Sie bestimmte Entscheidungen beim Installieren des Management Servers treffen. Je nachdem wie Ihre IT-Infrastruktur aufgebaut ist, können Sie zwischen drei verschiedenen Möglichkeiten wählen.

Möglichkeit 1: Verbinden von Standorten aus derselben Domäne (mit einem gemeinsamen Domänen-Benutzer)

Vor der Installation des Managementservers müssen Sie einen Common Domain User erstellen und diesen auf allen Servern, die zur Hierarchie der Federated Site gehören, als Administrator konfigurieren. Wie Sie die Seiten verbinden, hängt von dem erstellten Benutzerkonto ab.

Mit einem Windows-Benutzerkonto

1. Beginnen Sie die Installation des Produkts auf dem Server, der als Management-Server dienen soll, und wählen Sie **Benutzerdefiniert**.
2. Wählen Sie die Installation des Managementserver-Dienstes über ein Benutzerkonto. Das ausgewählte Benutzerkonto muss das Administratorkonto sein, das auf allen Management-Servern verwendet wird. Sie müssen dasselbe Benutzerkonto verwenden, wenn Sie die anderen Management-Server in der Hierarchie der föderalen Standorte installieren.
3. Beenden Sie die Installation. Wiederholen Sie die Schritte 1-3 zum Installieren aller weiteren Systeme, die Sie zur Hierarchie der föderalen Standorte hinzufügen wollen.
4. Fügen Sie einen Standort zur Hierarchie hinzu (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 467).

Mit einem eingebauten Windows-Benutzerkonto (Netzwerkdienst)

1. Beginnen Sie die Installation des Produkts auf dem ersten Server, der als Management-Server dienen soll, und wählen Sie **Einzelcomputer** oder **Benutzerdefiniert** aus. Dadurch wird der Management-Server über ein Netzwerkdienstkonto installiert. Wiederholen Sie diesen Schritt für alle Standorte in Ihrer Hierarchie der föderalen Standorte.
2. Melden Sie sich bei dem Standort an, der in der Hierarchie der föderalen Standorte als zentraler Standort dienen soll.
3. Im Management Client erweitern Sie **Sicherheit** > **Rollen** > **Administratoren**.
4. Auf der Registerkarte **Benutzer und Gruppen**: auf **Hinzufügen** klicken und **Windows-Benutzer** auswählen.
5. Im Dialogfeld **Computer** als Objekttyp auswählen, den Servernamen des föderalen Standorts eingeben und auf **OK** klicken, um den Server zur **Administrator**-Rolle des zentralen Standorts hinzuzufügen. Wiederholen Sie diesen Schritt, bis Sie alle föderalen Standorte auf diese Weise hinzugefügt haben, und schließen Sie die Anwendung.
6. Melden Sie sich bei jedem föderalen Standort an und fügen Sie die folgenden Server auf die oben beschriebene Weise zur **Administrator**-Rolle hinzu:
   - Der Server des übergeordneten Standorts.
   - Die Server der untergeordneten Standorte, die Sie direkt mit diesem föderalen Standort verbinden möchten.
7. Fügen Sie einen Standort zur Hierarchie hinzu (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 467).

Möglichkeit 2: Verbinden von Standorten aus unterschiedlichen Domänen

Stellen Sie zum Verbinden von Standorten unterschiedlicher Domänen sicher, dass eine Vertrauensstellung zwischen den Domänen besteht. Sie können eine Vertrauensstellung zwischen unterschiedlichen Domänen in der Domänenkonfiguration von Microsoft Windows einrichten. Sobald Sie eine Vertrauensstellung zwischen den unterschiedlichen Domänen an jedem Standort in der Hierarchie der föderalen Standorte geschaffen haben, folgen Sie einfach der Beschreibung bei Möglichkeit 1. Weitere Informationen über die Einrichtung einer Vertrauensstellung zwischen Domänen finden Sie auf der Microsoft Website (https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/).

Milestone empfiehlt Milestone Interconnect für die Erstellung von vernetzten Systemen mit mehreren Standorten und Domänen.

Möglichkeit 3: Verbinden von Standorten in Arbeitsgruppen

Wenn Sie Standorte innerhalb von Arbeitsgruppen verbinden wollen, muss dasselbe Administratorkonto auf allen Servern vorhanden sein, die Sie in der Hierarchie der föderalen Standorte verbinden wollen. Sie müssen vor der Installation des Systems das Administratorkonto festlegen.

1. Melden Sie sich mit einem allgemeinen Administratorkonto bei **Windows** an.
2. Beginnen Sie die Installation des Produkts und klicken Sie auf **Benutzerdefiniert**.
3. Installieren Sie den Managementserver-Dienst unter Verwendung des allgemeinen Administratorkontos.

4. Beenden Sie die Installation. Wiederholen Sie die Schritte 1-4, um weitere, zu verbindende Systeme zu installieren. Sie müssen all diese Systeme mit dem allgemeinen Administratorkonto installieren.
5. Fügen Sie einen Standort zur Hierarchie hinzu (siehe Hinzufügen eines Standorts zur Hierarchie auf Seite 467).

Milestone empfiehlt Milestone Interconnect zur Erstellung von vernetzten Systemen mit mehreren Standorten, wenn die Standorte nicht zu einer Domäne gehören.

Sie können Domänen und Arbeitsgruppen nicht mischen. Das bedeutet, dass Sie nicht Standorte von einer Domäne mit Standorten von einer Arbeitsgruppe verbinden können und umgekehrt.

Hinzufügen eines Standorts zur Hierarchie

Bei der Erweiterung Ihres Systems können Sie Standorte zu Ihrem obersten Standort und zu dessen untergeordneten Standorten hinzufügen, solange das System korrekt konfiguriert ist.

1. Wählen Sie den Bereich **Hierarchie der föderalen Standorte** aus.
2. Wählen Sie den Standort aus, dem Sie einen untergeordneten Standort hinzufügen möchten, klicken Sie mit der rechten Maustaste, und klicken Sie dann auf **Standort der Hierarchie hinzufügen**.
3. Geben Sie die URL des angeforderten Standorts in das Fenster **Standort der Hierarchie hinzufügen** ein und klicken Sie auf **OK**.
4. Der übergeordnete Standort sendet eine Verknüpfungsanfrage an den untergeordneten Standort und nach einer Weile wird dem Bereich **Hierarchie der föderalen Standorte** eine Verknüpfung zwischen den beiden Standorten hinzugefügt.
5. Können Sie die Verknüpfung zum untergeordneten Standort ohne Genehmigungsanfrage an den Administrator des untergeordneten Standorts einrichten, gehen Sie zu Schritt 7.

   Ist dies **nicht** der Fall, wird für den untergeordneten Standort das Symbol für eine ausstehende Genehmigung angezeigt, bis der Administrator des untergeordneten Standortes die Anfrage genehmigt hat.
6. Stellen Sie sicher, dass der Administrator des untergeordneten Standorts die Verknüpfungsanfrage vom übergeordneten Standort aus genehmigt (Siehe Zustimmen der Aufnahme in die Hierarchie auf Seite 468).
7. Die neue Verknüpfung zwischen übergeordnetem und untergeordnetem Standort wird eingerichtet und der Bereich **Hierarchie der föderalen Standorte** wird mit dem Symbol für den neuen untergeordneten Standort aktualisiert.

Zustimmen der Aufnahme in die Hierarchie

Hat ein untergeordneter Standort eine Verknüpfungsanfrage von einem potenziellen übergeordneten Standort erhalten und der Administrator hatte keine Administratorenrechte für den untergeordneten Standort, wird das Symbol für eine ausstehende Genehmigung  angezeigt.

Gehen Sie zum Akzeptieren einer Verknüpfungsanfrage wie folgt vor:

1. Melden Sie sich am Standort an.
2. Klicken Sie im Bereich **Hierarchie der föderalen Standorte** mit der rechten Maustaste auf den Standort und klicken Sie auf **Aufnahme in Hierarchie zustimmen**.

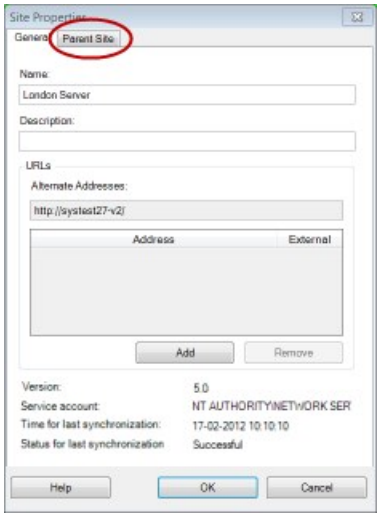
   Führt der Standort die XProtect Expert-Version aus, klicken Sie mit der rechten Maustaste auf das **Site-Navigationsfenster**.
3. Klicken Sie auf **Ja**.
4. Die neue Verknüpfung zwischen übergeordnetem und untergeordnetem Standort wird eingerichtet und der Bereich **Hierarchie der föderalen Standorte** wird mit dem normalen  Standortsymbol für den ausgewählten Standort aktualisiert.

> Es kann einige Zeit dauern, bis Änderungen für untergeordnete Standorte, die vom übergeordneten Standort weit entfernt sind, im Bereich **Hierarchie der föderalen Standorte** angezeigt werden.

Festlegen von Standorteigenschaften

Sie können Eigenschaften auf Ihrem Heimatstandort und dessen untergeordneten Standorten anzeigen und möglicherweise auch bearbeiten.

1. Wählen Sie im Management Client im Bereich **Hierarchie der föderalen Standorte** den entsprechenden Standort aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Eigenschaften** aus.



2. Ändern Sie ggf. Folgendes:

   Registerkarte **Allgemein** (siehe Allgemein auf Seite 470)

   Registerkarte **Übergeordneter Standort** (siehe Registerkarte Registerkarte „Übergeordneter Standort“ auf Seite 471) **(nur an untergeordneten Standorten verfügbar)**

> Aufgrund von Synchronisierungsproblemen kann es einige Zeit dauern, bis Änderungen an entfernten untergeordneten Standorten im Bereich **Standort-Navigation** angezeigt werden.

Standorthierarchie aktualisieren

Das System synchronisiert die Hierarchie regelmäßig automatisch in allen Ebenen Ihrer Einrichtung mit übergeordneten und untergeordneten Standorten. Sie können auch manuell eine Aktualisierung durchführen, wenn die Änderungen sofort in der Hierarchie angezeigt werden sollen und Sie nicht bis zur nächsten automatischen Synchronisierung warten möchten.

Sie müssen für eine manuelle Aktualisierung an einem Standort angemeldet sein. Durch eine Aktualisierung werden nur für diesen Standort seit der letzten Synchronisierung gespeicherte Änderungen angezeigt. Es kann also sein, dass Änderungen weiter unten in der Hierarchie durch diese manuelle Aktualisierung nicht angezeigt werden, wenn die Änderungen den Standort noch nicht erreicht haben.

1. Melden Sie sich am entsprechenden Standort an.
2. Klicken Sie im Bereich **Hierarchie der föderalen Standorte** mit der rechten Maustaste auf den obersten Standort und klicken Sie auf **Standorthierarchie aktualisieren**.

   Das dauert ein paar Sekunden.

Anmelden an anderen Standorten in der Hierarchie

Sie können sich an anderen Standorten anmelden und diese verwalten. Der Standort, an dem Sie angemeldet sind, ist Ihr Heimatstandort.

1. Klicken Sie im Bereich **Hierarchie der föderalen Standorte** mit der rechten Maustaste auf den Standort, an dem Sie sich anmelden möchten.
2. Klicken Sie auf **An Standort anmelden**.

   Das Management Client für diesen Standort wird geöffnet.
3. Geben Sie die Anmeldeinformationen ein und klicken Sie auf **OK**.
4. Nach der Anmeldung können Sie sich um Ihre Verwaltungsaufgaben für diesen Standort kümmern.

Trennen eines Standorts von der Hierarchie

Wenn Sie einen Standort von seinem übergeordneten Standort trennen, wird die Verknüpfung zwischen den Standorten unterbrochen. Sie können Standorte vom zentralen Standort, vom Standort selbst oder vom übergeordneten Standort trennen.

1. Klicken Sie im Bereich **Hierarchie der föderalen Standorte** mit der rechten Maustaste auf den Standort und klicken Sie auf **Standort von Hierarchie trennen**.
2. Klicken Sie auf **Ja**, um den Bereich **Hierarchie der föderalen Standorte** zu aktualisieren.

   Verfügt der getrennte Standort über untergeordnete Standorte, wird er zum neuen obersten Standort dieses Zweigs der Hierarchie und das normale Standortsymbol  ändert sich zu einem Symbol für den obersten Standort  .
3. Klicken Sie auf **OK**.

Die Änderungen an der Hierarchie werden nach einer manuellen Aktualisierung oder einer automatischen Synchronisierung angezeigt.

Eigenschaften für einen föderalen Standort

Dieser Abschnitt beschreibt die Registerkarte **Allgemein** und die Registerkarte **Mutterseite**.

Allgemein

Sie können einige der Informationen zum Standort, an dem Sie gerade angemeldet sind, ändern.

Name	Beschreibung
Name	Geben Sie den Namen des Standorts ein.
Beschreibung	Geben Sie eine Standortbeschreibung ein.
URLs	Verwenden Sie die Liste, um URL(s) für diesen Standort hinzuzufügen und zu entfernen und um anzugeben, ob diese extern sind oder nicht. Externe Adressen können außerhalb des lokalen Netzwerks aufgerufen werden.
Version	Die Versionsnummer des Management-Servers des Standorts.
Dienstkonto	Das Dienstkonto, unter dem der Management-Server ausgeführt wird.
Zeitpunkt der letzten Synchronisierung	Zeit und Datum der letzten Synchronisierung der Hierarchie.
Status der letzten Synchronisierung	Der Status der letzten Synchronisierung der Hierarchie. Der Status kann entweder **Erfolgreich** oder **Fehlgeschlagen** sein.

Registerkarte „Übergeordneter Standort“

In dieser Registerkarte werden Informationen zum übergeordneten Standort des Standorts angezeigt, an dem Sie gerade angemeldet sind. Diese Registerkarte ist nicht sichtbar, wenn Ihr Standort über keinen übergeordneten Standort verfügt.

Name	Beschreibung
Name	Zeigt den Namen des übergeordneten Standorts an.
Beschreibung	Zeigt eine Beschreibung des übergeordneten Standorts an (optional).
URLs	Listet URL(s) für diesen übergeordneten Standort auf und gibt an, ob sie extern oder intern sind. Externe Adressen können außerhalb des lokalen Netzwerks aufgerufen werden.

Name	Beschreibung
Version	Die Versionsnummer des Management-Servers des Standorts.
Dienstkonto	Das Dienstkonto, unter dem der Management-Server ausgeführt wird.
Zeitpunkt der letzten Synchronisierung	Zeit und Datum der letzten Synchronisierung der Hierarchie.
Status der letzten Synchronisierung	Der Status der letzten Synchronisierung der Hierarchie. Der Status kann entweder **Erfolgreich** oder **Fehlgeschlagen** sein.

Konfigurieren von Milestone Interconnect

Dieser Abschnitt beschreibt Milestone Interconnect und wie die Funktion konfiguriert wird.

Auswahl von Milestone Interconnect oder Milestone Federated Architecture (Erklärung)

In einem physisch verteiltem System, in dem Benutzer am zentralen Standort Zugriff auf Video am Remote-System benötigen, können Sie zwischen Milestone Interconnect™ oder Milestone Federated Architecture™ wählen.

Milestone empfiehlt Milestone Federated Architecture, wenn:

- Die Netzwerkverbindung zwischen dem zentralen Standort und dem föderalen Standort instabil ist
- Das Netzwerk die selbe Domäne verwendet
- Es weniger größere Standorte gibt
- Die Bandbreite für die gewünschte Nutzung ausreicht

Milestone empfiehlt Milestone Interconnect, wenn:

- Die Netzwerkverbindung zwischen dem zentralen Standort und dem Remote-System instabil ist
- Sie oder Ihr Unternehmen ein anderes Produkt von XProtect am Remote-System verwenden möchten
- Das Netzwerk verschiedene Domains oder Arbeitsgruppen benutzt
- Es kleinere Standorte gibt

Milestone Interconnect und Lizenzierung

Für die Ausführung von Milestone Interconnect benötigen Sie Milestone Interconnect Kameralizenzen an Ihrem zentralen Standort, um Video von Geräten an Remote-Systemen anzusehen. Beachten Sie, dass ausschließlich XProtect Corporate als zentraler Standort agieren kann.

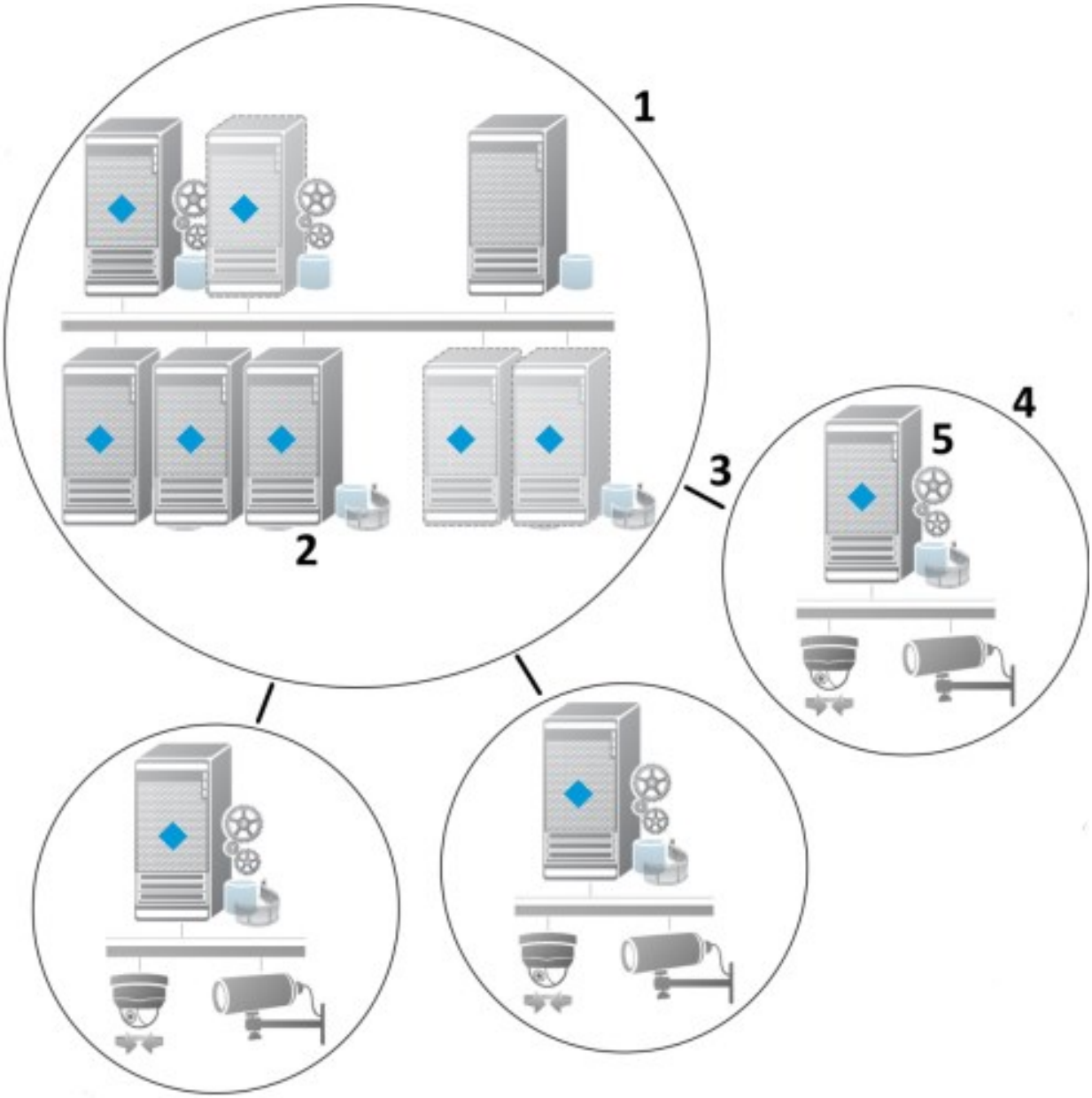
Den Status Ihrer Milestone Interconnect Kameralizenzen finden Sie auf der Seite **Lizenzinformationen** am zentralen Standort.

Milestone Interconnect (erklärt)

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

Milestone Interconnect™ erlaubt Ihnen die Integration einer Anzahl kleiner, physisch fragmentierter und entfernter XProtect Installationen mit einer XProtect Corporate zentralen Seite. Sie können diese kleineren Standorte (Remote-Systeme) mobil mitführen, z. B. auf Booten, Bussen oder Zügen. Das bedeutet, dass solche Standorte nicht permanent mit einem Netzwerk verbunden sein müssen.

Die folgende Abbildung zeigt die Einrichtung von Milestone Interconnect in Ihrem System:



1. Milestone Interconnect Zentraler XProtect Corporate-Standort
2. Milestone Interconnect Treiber (verwalten die Verbindung zwischen den Aufzeichnungsservern des zentralen und des Remote-Systems; muss aus einer Liste von Treibern ausgewählt werden, wenn Remote-Systeme per **Hardware hinzufügen**-Assistenten hinzugefügt werden)
3. Milestone Interconnect Verbindung
4. Milestone Interconnect Remote-System (der gesamte Remote-System mit Systeminstallation, Benutzer, Kameras usw.)
5. Milestone Interconnect Remote-System (die tatsächliche technische Installation am Remote-Systeminstallation)

Sie fügen Remote-Systeme zu Ihrem zentralen Standort mittels des Assistenten zum **Hinzufügen von Hardware** vom zentralen Standort aus hinzu (siehe Einen Remote-Standort zum zentralen Milestone Interconnect-Standort hinzufügen auf Seite 476 hinzufügen).

Jeder Remote-System läuft unabhängig und kann jegliche normalen Überwachungsaufgaben übernehmen. Je nach Netzwerkverbindung und dazugehörigen Benutzerrechten (siehe Benutzerrechte zuweisen auf Seite 478) bietet Milestone Interconnect Ihnen direkte Live-Ansicht von Kameras an Remote-Systemen und Wiedergabe von Aufzeichnungen dieser Remote-Systeminstallation am zentralen Standort.

Der zentrale Standort kann nur solche Geräte sehen und auf diese zugreifen, auf die das bestimmte Benutzerkonto (beim Hinzufügen des Remote-Systems) Zugriff hat. Dies ermöglicht es lokalen Systemadministratoren zu steuern, welche Geräte dem zentralen Standort und dessen Benutzern zur Verfügung gestellt werden soll.

Am zentralen Standort können Sie den eigenen Status des Systems für die verbundenen Kameras sehen, allerdings nicht den direkten Status des Remote-Systems. Stattdessen können Sie zur Überwachung des Remote-Systems die Funktion zum Auslösen von Alarmen und anderen Meldungen am zentralen Standort durch Ereignisse am Remote-System verwenden (siehe Konfigurieren Sie Ihren zentralen Standort, so dass er auf Ereignisse von Remote-Systemen reagiert auf Seite 480).

Dies bietet Ihnen auch die Möglichkeit, Aufzeichnungen des Remote-Systems an den zentralen Standort zu senden, basierend entweder auf Ereignissen, Regeln/Planung, oder manuellen Anfragen von XProtect Smart Client-Benutzern.

Nur XProtect Corporate-Systeme können als zentrale Standorte fungieren. Alle anderen Produkte können Remote-Systeme sein, einschließlich XProtect Corporate. Welche Versionen und wie viele Kameras sowie die Art und Weise (oder überhaupt) des Umgangs mit Geräten und Ereignissen des Remote-Systems am zentralen Standort, unterscheidet sich von Einstellung zu Einstellung. Weitere Details dazu, wie bestimmte XProtect-Produkte in einer Milestone Interconnect-Konfiguration interagieren, finden Sie auf der Webseite Milestone Interconnect (https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/).

Milestone Interconnect-Einrichtungen (Erklärung)

Es gibt drei Wege Milestone Interconnect auszuführen. Wie Sie Ihre Einstellung ausführen hängt von Ihrer Netzwerkverbindung, Ihrer Wiedergabeart und ob Sie Fernaufzeichnungen abrufen und in welcher Weise ab.

Folgend sind die drei wahrscheinlichsten Einstellungen beschrieben:

Direkte Wiedergabe von Remote-Systemen (gute Netzwerkverbindungen)

Die direkteste Einstellung. Der zentrale Standort ist durchgehend mit seinen Remote-Systemen verbunden und Benutzer am zentralen Standort können Fernaufzeichnungen direkt von den Remote-Systemen Wiedergabe. Dies erfordert die Verwendung der Option **Aufzeichnungen vom Remote-System Wiedergabe** (siehe Aktivieren der direkten Wiedergabe von der Kamera am Remote-System auf Seite 479).

Regel- oder XProtect Smart Client-basierender Abruf ausgewählter FernaufzeichnungsSequenzen von Remote-Systemen (zeitweilig begrenzte Netzwerkverbindungen)

Wird verwendet, wenn ausgewählte AufzeichnungsSequenzen (vom Remote-System) zentral gespeichert werden sollten, um die Unabhängigkeit der Remote-Systeme zu garantieren. Unabhängigkeit ist äußerst wichtig im Falle von Netzwerkfehlern oder -einschränkungen. Sie können die Abrufeinstellungen der Fernaufzeichnungen in der Registerkarte **Fernabruf** konfigurieren (siehe Registerkarte „Fernabfrage“ auf Seite 213).

Der Abruf von Fernaufzeichnungen kann bei Bedarf vom XProtect Smart Client gestartet werden oder durch eine Regel gesteuert werden. In einigen Szenarien sind Remote-Systeme die meiste Zeit online und in anderen offline. Dies hängt oft von der Branche ab. In einigen Branchen ist es üblich, dass der zentrale Standort permanent mit seinen Remote-Systemen in Kontakt steht (zum Beispiel die Hauptverwaltung eines Einzelhandels (zentraler Standort) und eine Anzahl von Läden (Remote-Systeme)). Bei anderen Branchen, wie in der Logistik und Transport, sind Remote-Systeme mobil (bspw. Busse, Züge, Schiffe usw.) und können nur sporadisch eine Netzwerkverbindung aufbauen. Sollte die Netzwerkverbindung während des Abrufs von Fernaufzeichnungen ausfallen, kann sie bei nächster Gelegenheit fortgesetzt werden.

Wenn das System den automatischen Abruf, oder eine Anforderung dessen von dem XProtect Smart Client außerhalb des in der Registerkarte **Fernabfrage** festgelegten Zeitintervalls erhält, wird es zwar angenommen, aber nicht gestartet, bis diese Zeit erreicht ist. Neue Abrufanfragen für Fernaufzeichnungen werden eingereiht und gestartet, sobald das eingestellte Zeitintervall erreicht ist. Sie können anstehende Abrufanfragen für Fernaufzeichnungen ansehen, unter **System-Dashboard** -> **Aktuelle Aufgaben**.

Nach einem Verbindungsfehler werden fehlende Fernaufzeichnungen automatisch vom Remote-System abgefragt

Verwendet Remote-Systeme, wie ein Aufzeichnungsserver den lokalen Speicher einer Kamera. Normalerweise sind Remote-Systeme mit ihrem zentralen Standort verbunden und beliefern ihn mit einem Live-Stream, den der zentrale Standort dann aufzeichnet. Sollte aus einem Grund das Netzwerk ausfallen, gehen dem zentralen Standort diese AufzeichnungsSequenzen verloren. Sobald das Netzwerk wieder hergestellt wurde, fragt der zentrale Standort automatisch die Fernaufzeichnungen des verpassten Zeitraums ab. Hierfür ist es erforderlich, die Option **Fernaufzeichnungen automatisch abrufen, wenn die Verbindung wiederhergestellt wird** zu verwenden (siehe Abruf von Fernaufzeichnungen von Kamera an Remote-System auf Seite 479) auf der Registerkarte **Aufzeichnung** für die jeweilige Kamera.

Sie können jeder der oben genannten Lösungen den individuellen Bedürfnissen Ihrer Organisation anpassen.

Einen Remote-Standort zum zentralen Milestone Interconnect-Standort hinzufügen

Sie können Remote-Systeme zum zentralen Standort hinzufügen, mittels des Assistenten für **Hardware hinzufügen**.
Voraussetzungen

- Ausreichende Anzahl von Milestone Interconnect-Kameralizenzen (siehe Milestone Interconnect und Lizenzierung auf Seite 473)
- Ein weiteres konfiguriertes und funktionstüchtiges XProtect System mit einem Benutzerkonto (Basisbenutzer, lokaler Windows-Benutzer oder Windows Active Directory-Benutzer) mit Berechtigungen für die Geräte, auf die das zentrale XProtect Corporate-System Zugriff haben sollte
- Die Netzwerkverbindung zwischen dem zentralen XProtect Corporate-Standort und den Remote-Systemenen mit Zugriff oder Port-Forwarding zu den verwendeten Ports der Remote-Systemen.

Zum Hinzufügen eines Remote-Systems:

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Erweitern Sie im Übersicht-Bereich den relevanten Aufzeichnungsserver und klicken Sie mit der rechten Maustaste.
3. Wählen Sie **Hardware hinzufügen** aus, um den Assistenten zu starten.
4. Wählen Sie auf der ersten Seite **-Adressbereich scannen** oder **Manuell** aus und klicken Sie auf **Weiter**.
5. Benutzernamen und Passwörter festlegen. Das Benutzerkonto muss auf dem Remote-Systeminstallation voreingestellt werden. Sie können Benutzernamen und Passwörter nach Bedarf hinzufügen, indem Sie auf **Hinzufügen** klicken. Wenn Sie bereit sind, klicken Sie auf **Weiter**.
6. Wählen Sie die zu verwendenden Treiber für einen Scan. In diesem Fall, wählen Sie die Milestone-Treiber aus. Klicken Sie auf **Weiter**.
7. Bestimmen Sie die IP-Adressen und Portnummern, die Sie scannen möchten. Die Standardeinstellung ist Port 80. Klicken Sie auf **Weiter**.

   Warten Sie, bis Ihr System die Remote-Standorte erkannt hat. Eine Statusanzeige zeigt den Erkennungsfortschritt. Im Falle einer erfolgreichen Erkennung erscheint eine **Erfolgsmeldung** in der **Status**-Spalte. Sollte ein Hinzufügen fehlschlagen, können Sie über die **Fehlgeschlagen**-Meldung den Grund erfahren.
8. Aktivieren oder deaktivieren Sie erfolgreich erkannte Systeme. Klicken Sie auf **Weiter**.
9. Warten Sie, während Ihr System die Hardware erkennt und gerätespezifische Informationen sammelt. Klicken Sie auf **Weiter**.
10. Aktivieren oder Deaktivieren Sie erfolgreich erkannte Hardware und Geräte. Klicken Sie auf **Weiter**.
11. Wählen Sie eine Standard-Gruppe. Klicken Sie auf **Fertigstellen**.
12. Nach der Installation können Sie das System und dessen Geräte im Bereich **Übersicht** sehen.

    Abhängig von den Benutzerrechten für den ausgewählten Benutzer am Remote-System, erhält der zentrale Standort Zugriff auf alle oder einen Teil der Kameras und Funktionen.

Benutzerrechte zuweisen

Benutzerrechte für eine verbundene Kamera konfigurieren Sie so wie andere Kameras, indem Sie eine Rolle erstellen und den Zugriff auf Funktionen zuweisen.

1. Erweitern Sie auf der zentralen Seite, in dem Fenster **Standort-Navigation** das Feld **Sicherheit** und wählen Sie **Rollen** aus.
2. Klicken Sie in dem Übersichtsfenster mit der rechten Maustaste auf die eingebaute Administratorrolle und wählen Sie **Rolle hinzufügen** aus (siehe Hinzufügen und Verwalten einer Rolle auf Seite 376).
3. Benennen Sie die Rolle und konfigurieren Sie die Einstellungen auf der Registerkarte **Gerät** (siehe die Registerkarte Rolleneinstellungen auf Seite 379) und die Registerkarte **Fernaufzeichnungen** (siehe die Registerkarte Rolleneinstellungen auf Seite 379).

Hardware des Remote-Systems aktualisieren

Wenn die Konfiguration am Remote-System beispielsweise durch das Hinzufügen und Entfernen von Kameras und Ereignissen verändert wurde, müssen Sie die Konfiguration am zentralen Standort aktualisieren, damit die neue am Remote-System wiedergespiegelt wird.

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Im Bereich der Übersicht, erweitern Sie den benötigten Aufzeichnungsserver und wählen das relevante Remote-Systeminstallation. Machen Sie einen Rechtsklick darauf.
3. Wählen Sie **Hardware aktualisieren**. Dies öffnet das Dialogfenster **Hardware aktualisieren**.
4. Das Dialogfenster zeigt alle Änderungen (Geräte, die entfernt, aktualisiert oder hinzugefügt wurden) im Remote-Systeminstallation, ab dem Zeitpunkt der Einrichtung oder letzten Aktualisierung Ihrer Milestone Interconnect-Einstellung. Klicken Sie auf **Bestätigen**, um Ihren zentralen Standort mit diesen Änderungen zu aktualisieren.

Die Remote-Desktop-Verbindung zum Remote-Systeminstallation aufbauen

Sie können sich per Fernzugriff mit System in Ihrer Milestone Interconnect-Einrichtung verbinden.

Voraussetzungen
Die Remote-Desktop-Verbindung zum gewünschten Computer, muss ausgeführt werden.

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Im Bereich der Übersicht, erweitern Sie den benötigten Aufzeichnungsserver und wählen das relevante Remote-Systeminstallation.
3. Im Bereich der Eigenschaften, wählen Sie die Registerkarte **Info**.
4. Geben Sie im Bereich **Fernverwaltung** den entsprechenden Windows-Benutzernamen und das Passwort ein.
5. Sobald Name und Passwort gespeichert sind, klicken Sie auf **Verbinden**, um eine Remote-Desktop-

Verbindung herzustellen.

6. Klicken Sie in der Symbolleiste auf **Speichern**.

Aktivieren der direkten Wiedergabe von der Kamera am Remote-System

Wenn Ihr zentraler Standort permanent mit den Remote-Systemen verbunden ist, können Sie Ihr System so konfigurieren, dass die Benutzer die Aufzeichnungen direkt von den Remote-Systemen abspielen können. Weitere Informationen finden Sie unter Milestone Interconnect-Einrichtungen (Erklärung) auf Seite 475.

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Im Bereich der Übersicht, erweitern Sie den benötigten Aufzeichnungsserver und wählen das relevante Remote-Systeminstallation. Wählen Sie die relevante verbundene Kamera.
3. Wählen Sie im Eigenschaften Bereich, die Registerkarte **Aufzeichnen**, und wählen Sie dann die Option **Wiedergabe der Aufzeichnungen von Remote-Systeminstallation**.
4. Klicken Sie in der Symbolleiste auf **Speichern**.

In einer Milestone Interconnect-Einstellung ignoriert ein zentraler Standort die Privatzonenmasken in einem Remote-System. Wenn Sie die gleichen Privatzonenmasken anwenden möchten, müssen Sie diese am zentralen Standort neu festlegen.

Abruf von Fernaufzeichnungen von Kamera an Remote-System

Sollte Ihr zentraler Standort **nicht** permanent mit den Remote-Systemen verbunden sein, können Sie Ihr System so konfigurieren, dass es Fernaufzeichnungen zentral speichert und den Abruf von Fernaufzeichnungen durchführt, wenn die Netzwerkverbindung optimal dafür ist. Weitere Informationen finden Sie unter Milestone Interconnect-Einrichtungen (Erklärung) auf Seite 475.

Damit Benutzer tatsächlich Aufzeichnungen abrufen können, muss diese Genehmigung für die zugehörige Rolle aktiviert werden (siehe Rolleneinstellungen auf Seite 379).

Zur Konfigurierung Ihres Systems:

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Im Bereich der Übersicht, erweitern Sie den benötigten Aufzeichnungsserver und wählen das relevante Remote-Systeminstallation. Wählen Sie den relevanten Remote-Server aus.
3. Wählen Sie im Fenster Eigenschaften die Registerkarte **Fernabfrage** aus und aktualisieren Sie die Einstellungen (siehe die Registerkarte Registerkarte „Fernabfrage“ auf Seite 213).

Wenn aus irgendeinem Grund das Netzwerk ausfällt, verliert der zentrale Standort AufzeichnungsSequenzen. Sie können daher Ihr System darauf konfigurieren, dass der zentrale Standort automatisch Fernaufzeichnungen abruft, um solche Zeiträume zu überbrücken, sobald das Netzwerk wiederhergestellt wurde.

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Im Bereich der Übersicht, erweitern Sie den benötigten Aufzeichnungsserver und wählen das relevante Remote-Systeminstallation. Wählen Sie die gewünschte Kamera.
3. Wählen Sie im Eigenschaftsfenster die Registerkarte **Aufzeichnen**, und wählen Sie dann die **-Option zum automatischen Abruf von Fernaufzeichnungen**, wenn die Verbindung wiederhergestellt wurde (siehe Geräte, die Voralarm-Puffern unterstützen auf Seite 238).
4. Klicken Sie in der Symbolleiste auf **Speichern**.

Als Alternative können Sie Regeln verwenden oder bei Bedarf den Abruf von Fernaufzeichnungen von XProtect Smart Client starten.

In einer Milestone Interconnect-Einstellung ignoriert ein zentraler Standort die Privatzonenmasken in einem Remote-System. Wenn Sie die gleichen Privatzonenmasken anwenden möchten, müssen Sie diese am zentralen Standort neu festlegen.

Konfigurieren Sie Ihren zentralen Standort, so dass er auf Ereignisse von Remote-Systemen reagiert

Sie können Ereignisse am Remote-System so einstellen, dass Regeln und Alarme am zentralen Standort ausgelöst werden und dadurch sofortige Reaktion auf Ereignisse am Remote-System folgen kann. Dies erfordert, dass die Remote-Systeme verbunden und online sind. Die Anzahl und Typ der Ereignisse ist abhängig von den Konfigurationen und Voreinstellungen an den Remote-Systemen.

Die Liste der unterstützten Ereignisse finden Sie auf der Milestone Webseite (https://www.milestonesys.com/).

Sie können voreingestellte Ereignisse nicht löschen.

Anforderungen:

- Wenn Sie benutzerdefinierte/manuelle Ereignisse vom Remote-System als auslösende Ereignisse verwenden möchten, müssen Sie diese zuerst am Remote-System erstellen
- Stellen Sie sicher, dass Sie eine aktualisierte Liste der Ereignisse am Remote-System haben (siehe Hardware des Remote-Systems aktualisieren auf Seite 478).

Hinzufügen eines benutzerdefinierten/manuellen Ereignisses von einem Remote-System:

1. Erweitern Sie am zentralen Standort **Server** und wählen Sie **Aufzeichnungsserver** aus.
2. Unter Übersicht wählen Sie den passenden Remote-Server und dann die Registerkarte **Ereignisse**.
3. Diese Liste enthält voreingestellte Ereignisse. Klicken Sie auf **Hinzufügen**, um benutzerdefinierte oder manuelle Ereignisse vom Remote-System aus der Liste einzuschließen.

Verwenden eines Ereignisses an einem Remote-System, um einen Alarm am zentralen Standort auszulösen:

1. Am zentralen Standort, erweitern Sie **Alarme** und wählen dann **Alarmdefinitionen** aus.
2. Im Bereich Übersicht, klicken Sie mit der rechten Maustaste auf **Alarmdefinitionen** und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie Werte nach Bedarf ein.
4. Im Feld **Ereignis auslösen**, können Sie zwischen den unterstützten voreingestellten und benutzerdefinierten Ereignissen auswählen.
5. Im Feld **Quellen**, können Sie den Remote-Server auswählen, von dessen assoziierten Remote-Server Sie Alarme erhalten möchten.
6. Speichern Sie die Konfiguration, wenn Sie fertig sind.

Verwenden eines Ereignisses an einem Remote-System zum Auslösen einer regelbasierten Aktion am zentralen Standort:

1. Erweitern Sie am zentralen Standort **Regeln und Ereignisse** und wählen dann **Regeln**.
2. Im Übersichtsbereich, klicken Sie mit der rechten Maustaste auf **Regeln** und dann auf **Regeln hinzufügen**.
3. Im erscheinenden Assistenten wählen Sie **Eine Aktion durchführen bei <Ereignis>**.
4. Im Bereich **Regelbeschreibung bearbeiten**, klicken Sie auf **Ereignis** und wählen zwischen den voreingestellten und benutzerdefinierten Ereignissen aus. Klicken Sie auf **OK**.
5. Klicken Sie auf **Geräte/Aufzeichnungsserver/Management-Server** und wählen Sie den Remote-Server des Remote-Systems für den der zentrale Standort eine Aktion starten soll. Klicken Sie auf **OK**.
6. Klicken Sie auf **Weiter**, um zur nächsten Seite des Assistenten zu gelangen.
7. Wählen Sie die Bedingungen aus, die auf diese Regel zutreffen sollen. Wenn Sie keine Bedingungen auswählen, gilt die Regel immer. Klicken Sie auf **Weiter**.
8. Wählen Sie eine Aktion aus und bestimmen Sie die Einzelheiten im Bereich **Regelbeschreibung bearbeiten**. Klicken Sie auf **Weiter**.
9. Wählen Sie bei Bedarf ein Kriterium zum Stoppen. Klicken Sie auf **Weiter**.
10. Wählen Sie bei Bedarf eine Aktion zum Stoppen. Klicken Sie auf **Fertigstellen**.

Konfigurieren von Fernzugriffsdiensten

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

Die Funktion Fernzugriffsdienste enthält die von Axis Communications entwickelte Kameraverbindungstechnik Axis One-click. Damit kann das System Video- (und Audio-)Aufnahmen von externen Kameras abrufen, wo Firewalls und/oder die Routernetzwerkkonfiguration normalerweise verhindern, dass Verbindungen zu solchen Kameras hergestellt werden. Die eigentliche Kommunikation findet dann über sichere Tunnelserver (ST-Server) statt. ST-Server verwenden VPN. Innerhalb eines VPN können nur solche Geräte betrieben werden, die über einen gültigen Schlüssel verfügen. Dies ermöglicht einen sicheren Tunnel, wo öffentliche Netzwerke auf sichere Weise Daten austauschen können.

Mit den Fernzugriffsdiensten können Sie

- Innerhalb des Axis Dispatch Service Anmeldedaten bearbeiten
- ST-Server hinzufügen, bearbeiten und entfernen
- Axis One-click-Kameras anmelden/abmelden und bearbeiten
- Gehen Sie zu der Hardware, die zu der Axis One-Click-Kamera gehört

Bevor Sie die Verbindung zur Axis One-click-Kamera benutzen können, müssen Sie zunächst eine geeignete ST-Server Umgebung installieren. Für die Arbeit mit sicheren Tunnelserver (ST-Server) Umgebungen und Axis One-click-Kameras müssen Sie sich zunächst an Ihren Systemanbieter wenden, damit er Ihnen den erforderlichen Benutzernamen und das dazugehörige Passwort für Axis Dispatch Services zur Verfügung stellt.

Installieren Sie die STS-Umgebung für die One-Click-Kameraverbindung

Voraussetzungen

- Wenden Sie sich an Ihren Systemanbieter, um den erforderlichen Benutzernamen und das dazugehörige Passwort für die Axis-Dispatch-Dienste zu erhalten
- Achten Sie darauf, dass Ihre Kameras das Axis Video Hosting System unterstützen. Gehen Sie auf die Internetseite von Axis, um zu sehen, welche Geräte unterstützt werden (https://www.axis.com/products/axis-guardian)
- Aktualisieren Sie ggf. die Firmware Ihrer Axis-Kameras. Gehen Sie auf die Internetseite von Axis, um die Firmware herunterzuladen (https://www.axis.com/techsup/firmware.php/)

1. Gehen Sie auf der Startseite jeder Kamera auf **Basiseinrichtung**, **TCP/IP**, und wählen Sie **AVHS aktivieren** und **Immer** aus.
2. Gehen Sie von Ihrem Management-Server aus auf die Downloadseite Milestone (https://www.milestonesys.com/downloads/) und laden Sie die Software **AXIS One-Click** herunter. Führen Sie das Programm zum Einrichten eines geeigneten Axis Secure Tunnel Framework aus.

STS hinzufügen/bearbeiten

1. Gehen Sie wie folgt vor:
   - Um einen ST-Server hinzuzufügen, klicken Sie mit der rechten Maustaste auf den obersten Knoten **Axis Secure Tunnel Server** und wählen Sie dann **Axis Secure Tunnel Server hinzufügen** aus
   - Zum Bearbeiten eines ST-Servers klicken Sie mit der rechten Maustaste darauf und wählen Sie **Axis Secure Tunnel Server bearbeiten** aus
2. Geben Sie in das Fenster, das sich dann öffnet, die entsprechenden Informationen ein.
3. Wenn Sie sich dafür entscheiden, bei der Installation der **Axis One-Click Connection Komponente** die Anmeldeinformationen zu verwenden, wählen Sie das Kontrollkästchen **Anmeldeinformationen verwenden** aus und geben Sie denselben Benutzernamen und dasselbe Passwort ein, das Sie auch für die Komponente **Axis One-Click Connection** verwendet haben.
4. Klicken Sie auf **OK**.

Registrieren Sie eine neue Axis One-Click-Kamera

1. Klicken Sie zum Registrieren einer Kamera unter einem ST-Server mit der rechten Maustaste darauf, und wählen Sie **Axis One-Click-Kamera registrieren** aus.
2. Geben Sie in das Fenster, das sich dann öffnet, die entsprechenden Informationen ein.
3. Klicken Sie auf **OK**.
4. Die Kamera erscheint nun unter dem jeweiligen ST-Server.

Die Kamera kann in den folgenden Farben codiert sein:

Farbe	Beschreibung
Rot	Eingangsstatus. Registriert, jedoch nicht mit dem ST-Server verbunden.
Gelb	Registriert. Mit dem ST-Server verbunden, jedoch nicht als Hardware hinzugefügt.
Grün	Als Hardware hinzugefügt. Ist mit dem ST-Server verbunden, oder auch nicht.

Wenn Sie eine neue Kamera hinzufügen, ist deren Status stets grün. Der Verbindungsstatus wird von den **Geräten** an **Aufzeichnungsservern** in dem Fenster **Übersicht** angezeigt. Im Bereich **Übersicht** können Sie Ihre Kameras gruppieren, um einen besseren Überblick zu haben. Wenn Sie sich dafür entscheiden, Ihre Kamera zu diesem Zeitpunkt **nicht** beim Axis Dispatch Service anzumelden, können Sie dies später nachholen, indem Sie mit der rechten Maustaste das Kontextmenü aufrufen (und **Axis One-Click-Kamera bearbeiten** auswählen).

Verbindungseigenschaften der Axis One-Click-Kamera

Name	Beschreibung
Kamerapasswort	Eingabe/bearbeiten. Beim Kauf im Lieferumfang Ihrer Kamera enthalten. Weitere Einzelheiten finden Sie im Handbuch für Ihre Kamera, oder gehen Sie auf die Internetseite von Axis (https://www.axis.com/).
Kamerabenutzer	Siehe die Einzelheiten für das **Kamerapasswort**.
Beschreibung	Eingabe/Bearbeitung einer Beschreibung für die Kamera.
Externe Adresse	Eingabe/Bearbeitung der Internetadresse des ST-Servers, mit dem sich die Kamera(s) verbindet (verbinden).
Interne Adresse	Eingabe/Bearbeitung der Internetadresse des ST-Servers, mit dem sich der Aufzeichnungsserver verbindet.
Name	Bearbeiten Sie ggf. den Namen des Inhalts.
Authentifizierungsschlüssel des Eigentümers	Siiehe **Kamerapasswort**.
Passwörter (für Dispatch Server)	Passwort eingeben. Dies muss demjenigen entsprechen, das Sie von Ihrem Systemanbieter erhalten haben.
Passwörter (für ST-Server)	Passwort eingeben. Dieses muss demjenigen entsprechen, das Sie eingegeben haben **, als die Axis One-Click-Connection-Komponente** installiert wurde.
An-/abmelden beim Axis Dispatch Service	Geben Sie an, ob sie ihre Axis-Kamera bei Axis Dispatch Service registrieren möchten. Dies kann zum Zeitpunkt der Einrichtung oder später erfolgen.
Seriennummer	Seriennummer der Hardware, wie vom Hersteller angegeben. Die Seriennummer ist oft, aber nicht immer, mit der MAC-Adresse identisch.
Anmeldedaten verwenden	Wählen Sie das Kontrollkästchen aus, wenn Sie sich dafür entschieden haben, während der Installation des ST-Servers die Anmeldedaten zu verwenden.

Name	Beschreibung
Benutzername (für den Dispatch Server)	Geben Sie einen Benutzernamen ein. Der Name des Benutzers muss demjenigen entsprechen, den Sie von Ihrem Systemanbieter erhalten haben.
Benutzername (für den ST-Server)	Geben Sie den Benutzernamen ein. Dieses muss demjenigen entsprechen, das Sie eingegeben haben, als die **Axis One-Click-Connection-Komponente** installiert wurde.

Konfigurieren einer Smart Map

In diesem Abschnitt wird beschrieben, wie Sie:

- Die geografischen Hintergründe konfigurieren, die Sie aus Ihrer Smart Map auswählen können
- Aktivieren der Bearbeitung von Smart Maps, einschließlich Kameras, in XProtect Smart Client
- Stellen Sie Ihre Smart Map ein, mit Milestone Federated Architecture

Geographische Hintergründe (Erklärung)

Bevor Sie einen geographischen Hintergrund in XProtect Smart Client auswählen können, müssen Sie zunächst die geographischen Hintergründe in XProtect Management Client konfigurieren.

- **Einfache Weltkarte** – Verwenden des standardmäßigen geografischen Hintergrunds, der in XProtect Smart Client zur Verfügung steht. Hierfür ist keine Konfiguration erforderlich. Diese Karte ist für den Einsatz als allgemeine Referenz gedacht und umfasst keine Funktionen wie Ländergrenzen, Städte oder andere Details. Aber wie die anderen geografischen Hintergründe auch, enthält sie georeferenzierte Daten
- **Bing Maps** – Verbinden mit Bing Maps
- **Google Maps** – Verbinden mit Google Maps
- **OpenStreetMap** gibt Ihnen drei Optionen:
    - Stellen Sie eine Verbindung zu einem kommerziellen Tile Server Ihrer Wahl her
    - Stellen Sie eine Verbindung zu Ihrem eigenen, lokalen Tile Server her

Die Bing Maps- und Google Maps-Optionen benötigen Zugriff zum Internet, und Sie müssen einen Schlüssel von Microsoft oder Google kaufen.

Falls Sie nicht Ihren eigenen, lokalen Tile Server verwenden, ist für OpenStreetMap außerdem ein Internetzugriff erforderlich.

Standardmäßig stellen Bing Maps und Google Maps Satellitenbilder (Satellit) dar. Sie können die Bilder in XProtect Smart Client ändern, z.B. in „Luft“ oder „Boden“, um verschiedene Einzelheiten zu sehen.

Erwerben Sie einen API-Schlüssel für Google Maps oder Bing Maps

Google Maps

Zum einbetten von Google Maps in Ihre Smart Map benötigen Sie einen Maps-Static-API-Schlüssel von Google. Um den API-Schlüssel zu erhalten, müssen Sie zunächst ein Google-Cloud-Rechnungskonto erstellen. Die Berechnung erfolgt je nach dem Volumen der geladenen Karten pro Monat.

Sobald Sie den API-Schlüssel haben, müssen Sie ihn in XProtect Management Client eingeben. Siehe Aktivieren Sie Bing Maps oder Google Maps in Management Client auf Seite 486.

Für weitere Informationen, siehe:

- Google Maps-Platform - der Einstieg: https://cloud.google.com/maps-platform/
- Anleitung zur Rechnungsstellung auf der Google Maps-Plattform: https://developers.google.com/maps/billing/gmp-billing
- Anleitung für Entwickler für Maps Static API: https://developers.google.com/maps/documentation/maps-static/dev-guide

Bing Maps

Zum einbetten von Bing Maps in Ihre Smart Map benötigen Sie einen Basis- oder Enterprise-Schlüssel. Der Unterschied besteht darin, dass Basis-Schlüssel kostenlos sind, jedoch nur eine begrenzte Anzahl von Transaktionen erlauben, bevor die Transaktionen berechnet werden können oder der Zugriff auf den Kartendienst verweigert wird. Der Enterprise-Schlüssel ist kostenpflichtig, erlaubt aber unbegrenzte Transaktionen.

Weitere Informationen zu Bing Maps finden Sie unter (https://www.microsoft.com/en-us/maps/licensing/).

Sobald Sie den API-Schlüssel haben, müssen Sie ihn in XProtect Management Client eingeben. Siehe Aktivieren Sie Bing Maps oder Google Maps in Management Client auf Seite 486.

Aktivieren Sie Bing Maps oder Google Maps in Management Client

Sie können einen Schlüssel mehreren Benutzern durch deren Eingabe für ein Smart Client-Profil im Management Client zur Verfügung stellen. Alle Nutzer, die diesem Profil zugewiesen sind, können den Schlüssel verwenden.

Schritte:

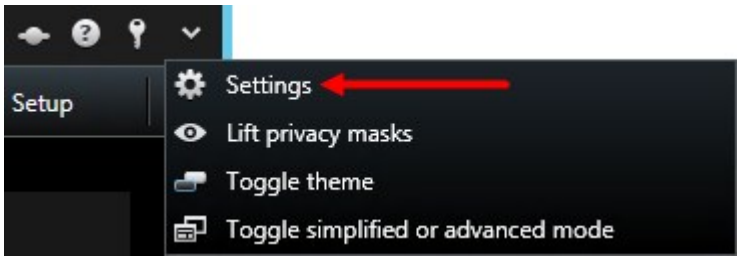
1. Klicken Sie in Management Client im Bereich **Standort-Navigation** auf **Smart Client Profile**.
2. Wählen Sie in dem Fenster **Smart Client**-Profile das entsprechende Smart Client-Profil aus.
3. Klicken Sie im Bereich **Eigenschaften** auf die Registerkarte **Smart Map**:
   - Für Bing Maps geben Sie Ihren Basis- oder Enterprise-Schlüssel im Feld **Bing Maps-Schlüssel** ein
   - Für Google Maps geben Sie Ihren Maps Static API Schlüssel in dem Feld **Privater Schlüssel für Google Maps** ein
4. Um zu verhindern, dass XProtect Smart Client der Betreiber einen anderen Schlüssel verwendet, aktivieren Sie das Kontrollkästchen **Gesperrt**.

Aktivieren Sie Bing Maps oder Google Maps in XProtect Smart Client

Um zuzulassen, dass XProtect Smart Client Betreiber einen anderen Schlüssel verwenden als den vom Smart Client-Profil, müssen Sie den Schlüssel in den Einstellungen in XProtect Smart Client eingeben.

Schritte:

1. Öffnen in XProtect Smart Client Sie das Fenster **Einstellungen**.



2. Klicken Sie auf **Smart Map**.
3. Unternehmen Sie folgende Schritte, abhängig vom gewünschten Kartendienst:
   - Für Bing Maps geben Sie den Schlüssel im Feld **Bing Maps Schlüssel** ein
   - Für Google Maps geben Sie den Schlüssel im Feld **Schlüssel für Google Maps** ein

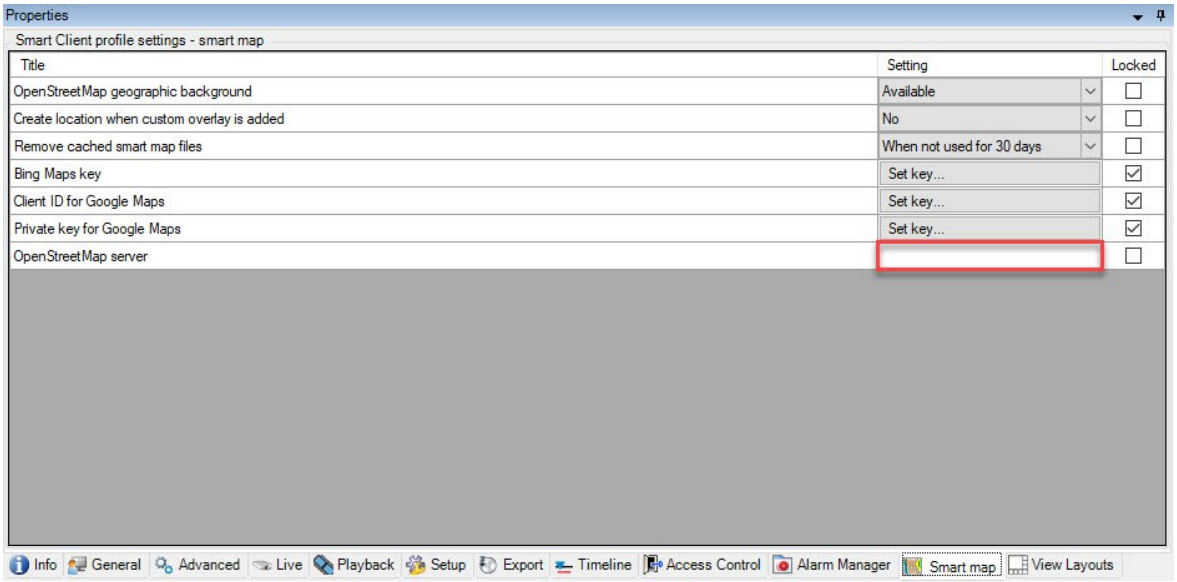
Geben Sie den OpenStreetMap Tile Server an

Falls Sie die Option **OpenStreetMap** als geographischen Hintergrund für Ihre Smart Map verwenden, müssen Sie angeben, von wo die gekachelten Bilder abgerufen werden. Dies können Sie tun, indem Sie die Adresse entweder eines kommerziellen oder lokalen Kachelservers angeben, z. B. wenn Ihre Organisation über eigene Karten für Bereiche wie Flughäfen oder Häfen verfügt.

> Sie können die Adresse des Tile Servers auch in dem Fenster **Einstellungen** in XProtect Smart Client angeben.

Schritte:

1. Erweitern Sie im Fenster **Standort-Navigation** den Knoten **Client** und klicken Sie auf **Smart Client Profile**.
2. Wählen Sie das passende Smart Client-Profil in der Übersicht aus.
3. Klicken Sie im Bereich **Eigenschaften** auf die Registerkarte **Smart Map**.



4. Geben Sie in dem Feld **OpenStreetMap-Server** die Adresse des Tile Servers ein.
5. Um diese Einstellung in XProtect Smart Client zu erzwingen, wählen Sie das Kontrollkästchen **Gesperrt** aus. Dann kann das XProtect Smart Client Betriebspersonal die Adresse nicht ändern.
6. Speichern Sie die Änderungen.

Zwischengespeicherte Smart Map Dateien (Erklärung)

Wenn Sie Google Maps als geographischen Hintergrund verwenden, werden die Dateien nicht im Cache gespeichert.

Die Dateien, die Sie für Ihren geografischen Hintergrund verwenden, werden von einem Kachelserver abgerufen. Die Speicherdauer für Dateien im Cache-Ordner ist abhängig von dem auf der Liste **Entfernte gecachte Smart-Map-Dateien** in dem Dialog **Einstellungen** in XProtect Smart Client ausgewählten Wert. Die Speichermöglichkeiten für die Dateien sind die folgenden:

- Unbegrenzt (**Nie**)
- 30 Tage lang, wenn die Datei nicht verwendet wird (**Wenn sie 30 Tage lang nicht verwendet wird**)
- Wenn der Anwender den XProtect Smart Client beendet (**Bei Beendigung**).

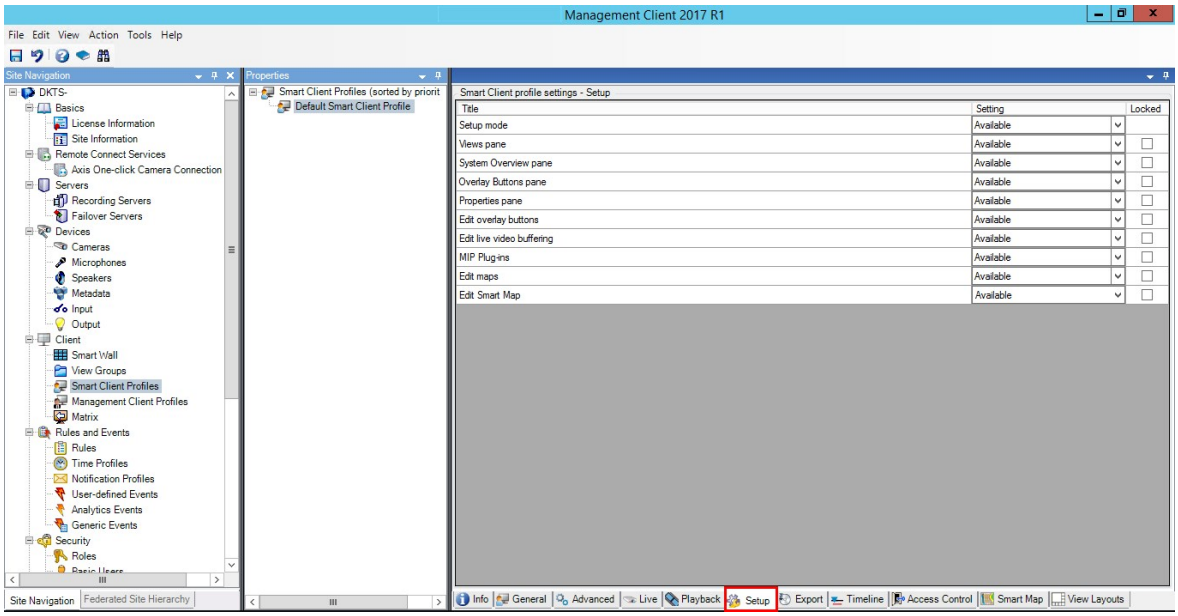
Beim Ändern der Adresse des Kachelservers wird automatisch ein neuer zwischengespeicherter Ordner erstellt. Die vorherigen Map-Dateien bleiben im jeweiligen zwischengespeicherten Ordner auf Ihrem lokalen Computer gespeichert.

Aktivieren der Smart Map-Bearbeitung

Anwender können die Smart Maps im Setup-Modus im XProtect Smart Client nur dann bearbeiten, wenn die Bearbeitung im Management Client aktiviert ist. Wenn diese Funktion nicht aktiviert ist, müssen Sie die Bearbeitung für jedes relevante Smart Client-Profil aktivieren.

Schritte:

1. Erweitern Sie im Fenster **Standort-Navigation** den Knoten **Client**.
2. Klicken Sie auf **Smart Client-Profile**.



3. Wählen Sie das passende Smart Client-Profil in der Übersicht aus.
4. Klicken Sie im Bereich **Eigenschaften** auf die Registerkarte **Einrichten**.
5. Wählen Sie aus der Liste **Smart Map bearbeiten** den Punkt **Verfügbar** aus.
6. Wiederholen Sie diese Schritte für jedes relevante Smart Client-Profil.
7. Speichern Sie Ihre Änderungen. Wenn sich Benutzer, die dem von Ihnen ausgewählten Smart Client-Profil zugewiesen sind, das nächste Mal beim XProtect Smart Client anmelden, werden sie Smart Maps bearbeiten können.

Wählen Sie in der Liste **Smart Map bearbeiten Nicht verfügbar** aus, um die Bearbeitungsfunktion zu deaktivieren.

Aktivieren der Kamerabearbeitung in Smart Map

Um es Anwendern zu ermöglichen, eine Kamera auf der Smart Map zu positionieren und das Sichtfeld und die Ausrichtung anzupassen, müssen Sie die Kamerabearbeitung für jede Rolle aktivieren.

Voraussetzungen
Vergewissern Sie sich, dass die Bearbeitung von Smart Maps aktiviert ist, bevor Sie anfangen (siehe Aktivieren der Smart Map-Bearbeitung auf Seite 489). Überprüfen Sie dafür das Smart Client-Profil, mit dem die Rolle des Anwenders verbunden ist.

Schritte:

1. Erweitern Sie den Knoten **Sicherheit** > **Rollen**.
2. Wählen Sie im Fenster **Rollen** die Rolle aus, mit der Ihr Anwender verbunden ist.
3. So geben Sie der Rolle Bearbeitungsrechte:
   - Klicken Sie auf die Registerkarte **Gesamtsicherheit** und wählen Sie **Kameras** im Bereich **Rolleneinstellungen** aus
   - Wählen Sie in der Spalte **Zulassen** das Kontrollkästchen **Vollständige Kontrolle** oder **Bearbeiten** aus
4. Speichern Sie die Änderungen.

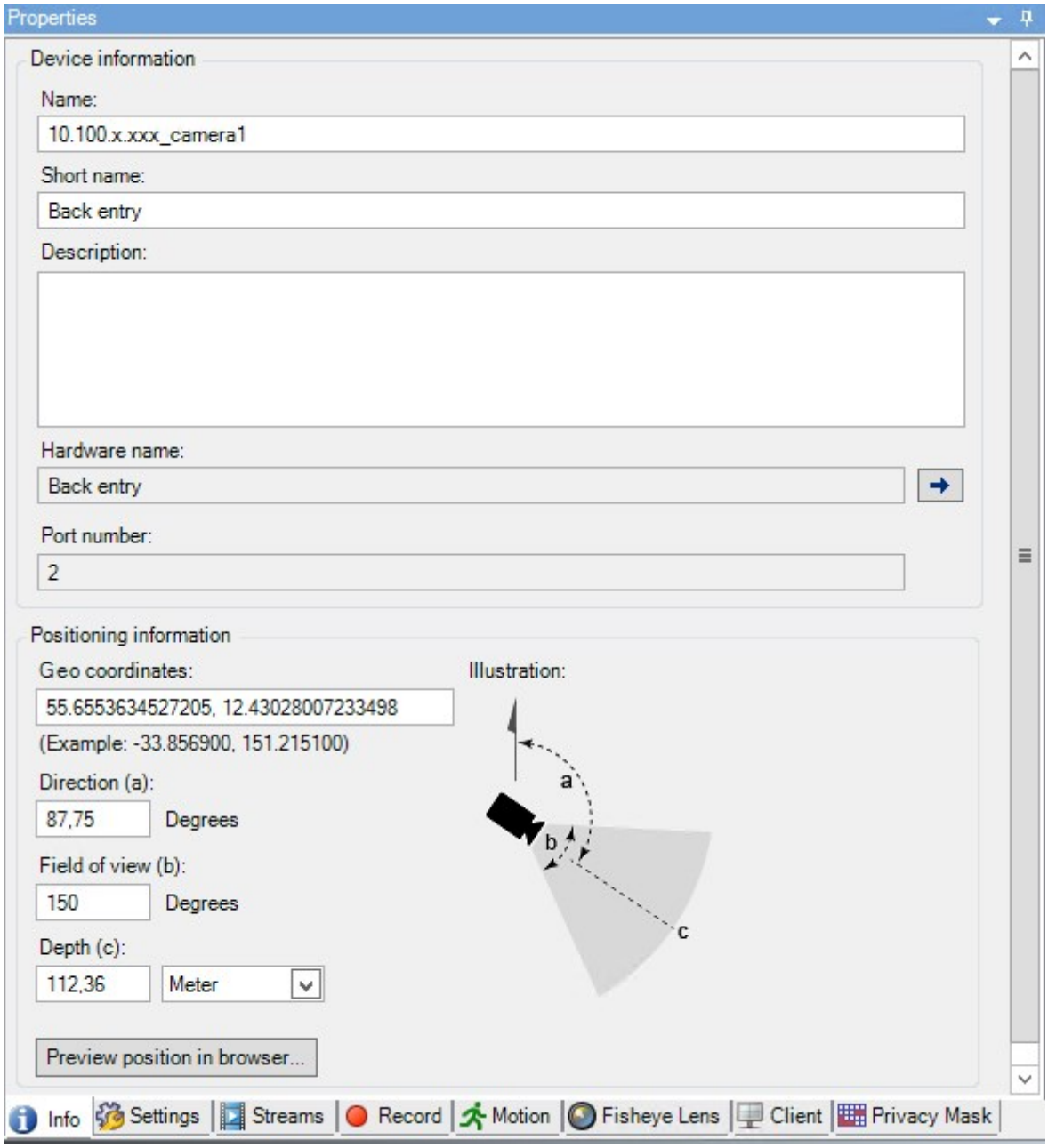
Die oben aufgeführten Schritte geben der Rolle das Recht zur Bearbeitung aller Kameras. Zur Aktivierung der Bearbeitung von einzelnen Kameras gehen Sie auf die Registerkarte **Gerät** und wählen Sie die entsprechende Kamera aus.

Festlegen von Position, Ausrichtung, Sichtfeld und Tiefe einer Kamera (Smart Map)

Um sicherzustellen, dass eine Kamera auf der Smart Map korrekt positioniert ist, können Sie die geographischen Koordinaten, die Ausrichtung der Kamera, das Blickfeld und die Anzeigetiefe einstellen. Damit wird die Kamera automatisch zur Smart Map hinzugefügt, wenn ein Anwender sie das nächste Mal in XProtect Smart Client lädt.

Schritte:

1. Erweitern Sie in Management Client den Knoten **Gerät** und wählen Sie **Kameras** aus.
2. Wählen Sie im Bereich **Gerät** die entsprechende Kameragruppe und die Kamera aus.
3. Scrollen Sie auf der Registerkarte **Info** herunter zu **Positionierungsinformationen**.



4. Geben Sie in das Feld **Geokoordinaten** dem Breitengrad und den Längengrad in dieser Reihenfolge ein. Verwenden Sie einen Punkt als Dezimaltrennzeichen und ein Komma zur Abtrennung der beiden Werte.
5. Geben Sie in das Feld **Richtung** einen Wert zwischen 0 und 360 Grad ein.
6. Geben Sie in das Feld **Sichtfeld** einen Wert zwischen 0 und 360 Grad ein.

7. Geben Sie in das Feld **Tiefe** die Sichttiefe ein, entweder in Metern oder in Fuß.
8. Speichern Sie die Änderungen.

Sie können die Eigenschaften auch auf den Aufzeichnungsservern festlegen.

Smart Map einrichten mit Milestone Federated Architecture

Wenn Sie Smart Map in einem Milestone Federated Architecture benutzen, erscheinen alle Kameras von den verbundenen Standorten auf der Smart Map. Die allgemeinen Schritte in diesem Thema beschreiben, wie Smart Map in einer föderalen Architektur eingerichtet wird.

Weitere allgemeine Informationen über Milestone Federated Architecture finden Sie unter Konfigurieren von Milestone Federated Architecture auf Seite 461.

1. Bevor Sie den obersten Standort mit untergeordneten Standorten verbinden, achten Sie darauf, dass die geographischen Koordinaten für alle Kameras an allen Standorten angegeben wurden. Die geographischen Koordinaten werden automatisch hinzugefügt, wenn eine Kamera durch XProtect Smart Client auf der Smart Map positioniert wird; Sie können sie in Management Client jedoch auch manuell in den Kameraeigenschaften hinzufügen. Weitere Informationen finden Sie unter Festlegen von Position, Ausrichtung, Sichtfeld und Tiefe einer Kamera (Smart Map) auf Seite 490.
2. Sie müssen die Smart Client-Anwender als Windows-Benutzer am übergeordneten Standort und an allen föderalen Standorten festlegen. Zumindest am übergeordneten Standort müssen die Windows-Benutzer über Bearbeitungsrechte für Smart Map verfügen. Dies ermöglicht ihnen, die Smart Map für den übergeordneten Standort und alle untergeordneten Standorte zu bearbeiten. Als nächstes müssen Sie bestimmen, ob die Windows-Benutzer an den Unterstandorten Smart Map-Editorenrechte benötigen. In Management Client erstellen Sie zuerst die Windows-Benutzer unter **Rollen**, und dann aktivieren Sie Smart Map-Bearbeitung. Weitere Informationen finden Sie unter Aktivieren der Smart Map-Bearbeitung auf Seite 489.
3. Am übergeordneten Standort müssen Sie die Unterstandorte als Windows-Benutzer einer Rolle mit Administratorrechten hinzufügen. Wenn Sie den Objekttyp angeben, aktivieren Sie das Kontrollkästchen **Computer**.
4. An jedem der Unterstandorte müssen Sie den Hauptstandort als Windows-Benutzer derselben Administratorrolle hinzufügen, die am Hauptstandort verwendet wird. Wenn Sie den Objekttyp angeben, aktivieren Sie das Kontrollkästchen **Computer**.
5. Stellen Sie sicher, dass Sie am Hauptstandort das Fenster der **Hierarchie der föderalen Standorte** sehen können. Gehen Sie in Management Client auf **Ansicht** und wählen Sie **Hierarchie der föderalen Standorte** aus. Fügen Sie jeden der untergeordneten Standorte zum übergeordneten Standort hinzu. Weitere Informationen finden Sie unter Hinzufügen eines Standorts zur Hierarchie auf Seite 467.

6. Jetzt können Sie testen, ob es in XProtect Smart Client funktioniert. Melden Sie sich als Administrator oder als Operator an dem Hauptstandort an und öffnen Sie eine Ansicht, die die Smart Map enthält. Wenn sie korrekt eingerichtet wurde, erscheinen alle Kameras sowohl von dem Hauptstandort als auch von allen Unterstandorten auf der Smart Map. Wenn Sie sich bei einem der Unterstandorte anmelden, werden nur die Kameras von diesem Standort und dessen Unterstandorten angezeigt.

Um Kameras auf einer Smart Map zu bearbeiten, z. B. die Kameraposition und den Kamerawinkel, benötigen Benutzer Kamera-Editoren-Rechte.

Wartung

Sicherung und Wiederherstellung einer Systemkonfiguration

Milestone empfiehlt regelmäßige Datensicherungen Ihrer Serverkonfiguration durchzuführen, um die Daten nach Notfällen wiederherstellen zu können. Auch wenn es selten vorkommt, dass Ihre Konfiguration verloren geht, kann es dennoch unter unglücklichen Umständen passieren. Es ist wichtig, dass Sie Ihre gesicherten Daten schützen, entweder durch technische oder durch organisatorische Maßnahmen.

Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung)

Das System enthält eine integrierte Sicherungsfunktion, welche die gesamte Systemkonfiguration sichert und die Sie im Management Client definieren können. Die Log-Server-Datenbank und die Protokolldateien (einschließlich Auditprotokolldateien) sind nicht in dieser Sicherung eingeschlossen.

Sollte Ihr System besonders groß sein, empfiehlt Milestone, dass Sie planmäßige Sicherungen einrichten. Dies geschieht über das Tool eines Drittanbieters: Microsoft® SQL Server Management Studio. Diese Sicherung schließt die gleichen Daten als manuelle Sicherung ein.

Während einer Sicherung bleibt Ihr System online.

Die Sicherung Ihrer System-Konfiguration kann einige Zeit in Anspruch nehmen. Die Sicherungsdauer hängt ab von:

- Ihre Systemkonfiguration
- Ihre Hardware
- Ob Sie den SQL Server, die Ereignisserver-Komponente und die Managementserver-Komponente auf einem einzigen Server oder auf mehreren Servern installiert haben

Jedes Mal, wenn Sie eine manuelle und planmäßige Datensicherung durchführen, wird die Transaktionsprotokolldatei der SQL-Datenbank geleert. Weitere Informationen dazu, wie die Transaktionsprotokolldatei geleert wird, siehe SQL-Datenbanktransaktionsprotokoll (Erläuterung) auf Seite 59.

> ⚠ Stellen Sie bei der Erstellung der Sicherung sicher, dass Sie die Passworteinstellungen in Ihrer Systemkonfiguration kennen.

Für Systeme, die FIPS 140-2 erfüllen, mit Exports und archivierten Mediendatenbanken aus XProtect VMS-Versionen vor 2017 R3, die mithilfe von nicht FIPS-konformen Chiffren verschlüsselt sind, müssen die Daten an einem Ort archiviert werden, wo sie nach Aktivierung von FIPS weiterhin zugänglich sind.
Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

Gemeinsamen Sicherungsordner auswählen

Vor der Sicherung und Wiederherstellung einer Systemkonfiguration müssen Sie einen Sicherungsordner für diesen Zweck bestimmen.

1. Klicken Sie mit der rechten Maustaste auf das Symbol für den Managementserver-Dienst im Benachrichtigungsbereich und wählen Sie **Gemeinsamen Sicherungsordner auswählen** aus.
2. Finden Sie im erscheinendem Fenster den gewünschten Dateipfad.
3. Klicken Sie zweimal auf **OK**.
4. Bei der Frage, ob Sie die derzeitigen Dateien im Sicherungsordner löschen möchten, klicken Sie je nach Bedarf auf **Ja** oder **Nein**

Manuelle Sicherung der Systemkonfiguration

1. Wählen Sie aus der Menüleiste **Datei** > **Konfiguration sichern**.
2. Lesen Sie den Hinweis im Dialogfenster und klicken Sie auf **Sicherung**.
3. Geben Sie einen Dateinamen für die .cnf-Datei ein.
4. Geben Sie einen Zielordner an und klicken Sie auf **Speichern**.
5. Warten Sie bis die Sicherung fertiggestellt wurde und klicken Sie dann auf **Schließen**.

Alle relevanten Systemkonfigurationsdateien sind in einer einzigen .cnf-Datei zusammengefasst, die an einem festgelegtem Ort gespeichert wird. Während der Sicherung werden zuerst alle Sicherungsdateien in einen temporären Backup-Systemordner auf dem Management-Server exportiert. Sie können einen anderen temporären Ordner auswählen, in dem Sie mit der rechten Maustaste auf das Managementserver-Dienst-Symbol des Benachrichtigungsbereichs klicken und „Gemeinsamen Sicherungsordner auswählen“ auswählen.

Wiederherstellen einer Systemkonfiguration aus einer manuellen Sicherung

Wichtige Information

- Sowohl der installierende Benutzer als auch der wiederherstellende Benutzer müssen lokale Administratoren der Systemkonfiguration der SQL-Datenbank auf dem Management-Server sein, **und** auch auf dem SQL Server
- Bis auf Ihre Aufzeichnungsserver, muss Ihr System für die Dauer der Wiederherstellung vollständig heruntergefahren werden. Dies könnte einige Zeit in Anspruch nehmen
- Eine Sicherung kann nur auf dem System wiederhergestellt werden, in dem sie erstellt wurde. Stellen Sie sicher, dass die Einrichtung der zu dem Zeitpunkt möglichst ähnlich ist, als die Sicherung durchgeführt wurde. Ansonsten könnte die Wiederherstellung fehlschlagen
- Wenn Sie bei der Wiederherstellung dazu aufgefordert werden, das Passwort für die Systemkonfiguration einzugeben, müssen Sie ein Passwort für die Systemkonfiguration eingeben, das zu dem Zeitpunkt gültig war, als das Backup erstellt wurde. Ohne dieses Passwort können Sie Ihre Konfiguration nicht aus dem Backup wiederherstellen.
- Wenn Sie eine Sicherung der SQL-Datenbank vornehmen, und sie anschließend auf einem frisch aufgesetzten SQL Server wiederherstellen, funktionieren die Fehlermeldungen aus der SQL-Datenbank nicht und Sie erhalten nur eine generische Fehlermeldung vom SQL Server. Um dies zu vermeiden, installieren Sie zunächst Ihr XProtect-System neu mithilfe eines frischen SQL Server und stellen Sie dann dessen Sicherungskopie wieder her
- Wenn die Wiederherstellung während der Validierungsphase fehlschlägt, können Sie die alte Konfiguration erneut starten, da keine Änderungen vorgenommen haben
  Wenn die Wiederherstellung an anderer Stelle im Prozess fehlschlägt, können Sie nicht zur alten Konfiguration zurückkehren
  Solange die Backup-Datei nicht beschädigt ist, können Sie eine weitere Wiederherstellung vornehmen
- Die Wiederherstellung ersetzt die aktuelle Konfiguration. Dies bedeutet, dass jegliche Änderungen an der Konfiguration seit der letzten Sicherung verloren gehen
- Es werden keine Protokolle (einschließlich Auditprotokolle) wiederhergestellt
- Sobald die Wiederherstellung gestartet wurde, kann diese nicht abgebrochen werden

Wiederherstellung

1. Klicken Sie mit der rechten Maustaste auf das Symbol für den Managementserver-Dienst im Benachrichtigungsbereich und wählen Sie **Konfiguration wiederherstellen** aus.
2. Lesen Sie den wichtigen Hinweis, und klicken Sie auf **Wiederherstellen**.
3. Suchen Sie im Dialogfenster 'Datei öffnen' das Verzeichnis mit der Sicherungsdatei der Systemkonfiguration, wählen Sie diese aus und klicken Sie dann auf **Öffnen**.

   Die Sicherungsdatei befindet sich auf dem Management Client-Computer. Sollte Management Client auf einem anderen Server installiert sein, kopieren Sie die

Sicherungsdatei zu diesen Server, bevor Sie ein Zielverzeichnis auswählen.

4. Das Fenster **Konfiguration wiederherstellen** öffnet. Warten Sie bis die Wiederherstellung beendet ist und klicken Sie dann auf **Schließen**.

Passwort für die Systemkonfiguration (Erklärung)

Sie können sich aussuchen, ob Sie die Gesamtsystemkonfiguration schützen wollen, indem Sie ein Passwort für die Systemkonfiguration festlegen. Sobald Sie ein Passwort für die Systemkonfiguration festgelegt haben, werden alle Backups mit diesem Passwort geschützt. Die Passworteinstellungen werden auf demjenigen Computer gespeichert, auf dem der Management Server in einem sicheren Ordner läuft. Dieses Passwort benötigen Sie für:

- Die Wiederherstellung der Konfiguration aus einem Backup, das mit anderen Passworteinstellungen erstellt wurde als den aktuellen
- Umzug oder Installation des Management Servers auf einem anderen Computer aufgrund eines Hardwarefehlers (Wiederherstellung)
- Die Konfiguration eines zusätzlichen Management Servers in einem System mit Clustering

Das Passwort für die Systemkonfiguration kann während oder nach der Installation festgelegt werden. Das Passwort muss den Anforderungen von Windows an die Komplexität entsprechen, die in der Windows-Passwortrichtlinie festgelegt sind.

Es ist wichtig, dass Systemadministratoren dieses Passwort sicher aufbewahren. Wenn Sie ein Passwort für die Systemkonfiguration festgelegt haben, und Sie wollen ein Backup wiederherstellen, werden Sie ggf. dazu aufgefordert, das Passwort für die Systemkonfiguration einzugeben. Ohne dieses Passwort können Sie Ihre Konfiguration nicht aus dem Backup wiederherstellen.

Passworteinstellungen für die Systemkonfiguration

Die Passworteinstellungen für die Systemkonfiguration können geändert werden. In den Passworteinstellungen für die Systemkonfiguration haben Sie die folgenden Optionen:

- Sie können sich aussuchen, ob Sie die Systemkonfiguration mit einem Passwort schützen wollen, indem Sie ein Passwort für die Systemkonfiguration festlegen
- Sie können das Passwort für die Systemkonfiguration ändern
- Sie können sich dafür entscheiden, die Systemkonfiguration nicht mit einem Passwort zu schützen, indem Sie ggf. vorhandene Passwörter für die Systemkonfiguration entfernen

Die Passworteinstellungen für die Systemkonfiguration ändern

Wenn Sie das Passwort ändern, ist es wichtig, dass die Systemadministratoren die mit den verschiedenen Backups verbundenen Passwörter sicher aufbewahren. Bei der Wiederherstellung eines Backup werden Sie ggf. dazu aufgefordert, das Passwort für die Systemkonfiguration einzugeben, das zu dem Zeitpunkt gültig war, als das Backup erstellt wurde. Ohne dieses Passwort können Sie Ihre Konfiguration nicht aus dem Backup wiederherstellen.

Um die Änderungen anzuwenden, müssen Sie die Management Server Dienste neu starten.

1. Suchen Sie das Taskleistensymbol für den Management Server und achten Sie darauf, dass der Dienst läuft.
2. Klicken Sie mit der rechten Maustaste auf das Symbol für den Managementserver-Dienst im Benachrichtigungsbereich und wählen Sie **Einstellungen für Systemkonfigurationspasswort ändern** aus.
3. Das Fenster zum Ändern der Einstellungen für das Passwort für die Systemkonfiguration wird angezeigt.

Vergeben Sie ein Passwort

1. Geben Sie das neue Passwort in das Feld **Neues Passwort** ein.
2. Geben Sie das neue Passwort in das Feld **Neues Passwort bestätigen** ein und drücken Sie **Eingabe**.
3. Lesen Sie die Benachrichtigung und klicken Sie dann auf **ja**, um die Änderung anzunehmen.
4. Warten Sie auf die Bestätigung der Änderung und wählen Sie dann **Schließen.**
5. Um die Änderungen anzuwenden, müssen Sie die Management Server Dienste neu starten.
6. Achten Sie nach dem Neustart darauf, dass der Management Server läuft.

Entfernen Sie den Passwortschutz

Falls Sie keinen Passwortschutz benötigen, können Sie sich dafür entscheiden, ihn wegzulassen:

1. Aktivieren Sie das Kontrollkästchen: **Ich möchte meine Systemkonfiguration nicht mit einem Passwort schützen, und mir ist klar, dass die Systemkonfiguration dann nicht verschlüsselt ist**.
2. Lesen Sie die Benachrichtigung und klicken Sie dann auf **ja**, um die Änderung anzunehmen.

3. Warten Sie auf die Bestätigung der Änderung und wählen Sie dann **Schließen**.
4. Um die Änderungen anzuwenden, müssen Sie die Management Server Dienste neu starten.
5. Achten Sie nach dem Neustart darauf, dass der Management Server läuft.

Geben Sie die Einstellungen für das Passwort für die Systemkonfiguration ein (Wiederherstellung)

Wenn die Datei mit den Passworteinstellungen aufgrund eines Hardwarefehlers oder aus anderen Gründen gelöscht wird, müssen Sie die Einstellungen für das Passwort für die Systemkonfiguration eingeben, um auf die Datenbank zugreifen zu können, die die Systemkonfiguration enthält. Während der Installation auf Ihrem neuen Computer werden Sie aufgefordert, die Passworteinstellungen für die Systemkonfiguration einzugeben.

Falls jedoch die Datei, die die Passworteinstellungen enthält, gelöscht oder beschädigt wird, und der Computer, auf dem der Managementserver läuft, keine sonstigen Probleme hat, haben Sie die Option, die Passworteinstellungen für die Systemkonfiguration einzugeben:

1. Suchen Sie das Taskleistensymbol für den Management Server.
2. Klicken Sie mit der rechten Maustaste auf das Symbol für den Managementserver-Dienst im Benachrichtigungsbereich und wählen Sie **Passwort für die Systemkonfiguration eingeben** aus.
3. Das Fenster "Ändern der Passworteinstellungen für die Systemkonfiguration" wird angezeigt.

Die Systemkonfiguration ist passwortgeschützt

1. Geben Sie das Passwort in das Feld **Passwort** ein und drücken Sie **Eingabe**.
2. Warten Sie, bis das Passwort übernommen wird. Wählen Sie **Schließen.**
3. Achten Sie darauf, dass der Management Server läuft.

Die Systemkonfiguration ist nicht passwortgeschützt

1. Aktivieren Sie das Kontrollkästchen: **Dieses System verwendet kein Passwort für die Systemkonfiguration** und wählen Sie **Eingabe**.
2. Warten Sie, bis die Einstellung übernommen wird. Wählen Sie **Schließen.**
3. Achten Sie darauf, dass der Management Server läuft.

Manuelle Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung)

Wenn Sie eine manuelle Sicherung der SQL-Datenbank des Management-Servers durchführen möchten, die Ihre Systemkonfiguration enthält, sollten Sie darauf achten, dass Ihr System online bleibt. Der standardmäßig vergebene Name für die SQL-Datenbank des Management-Servers ist **Überwachung**.

Hier einige Dinge, die Sie vor dem Beginn der Sicherung beachten sollten:

- Sie können eine Sicherung der SQL-Datenbank nicht zum Kopieren von Systemkonfigurationen auf andere Systeme verwenden
- Die Sicherung der SQL-Datenbank kann einige Zeit in Anspruch nehmen. Es hängt von Ihrer Systemkonfiguration, Ihrer Hardware und davon ab, ob Ihr SQL Server, Ihr Management-Server und Ihr Management Client auf demselben Computer installiert sind
- Protokolle, einschließlich Auditprotokolle, werden in der SQL-Datenbank des Protokollservers gespeichert und werden daher **nicht** bei der Sicherung der SQL-Datenbank des Management-Servers mit gesichert. Der standardmäßig vergebene Name für die SQL-Datenbank des Protokollservers ist **SurveillanceLogServerV2**. Beide SQL-Datenbanken werden auf die gleiche Art und Weise gesichert.

Sicherung und Wiederherstellung der Event-Server-Konfiguration (Erklärung)

Der Inhalt Ihrer Event-Server-Konfiguration ist bei der Sicherung und Wiederherstellung Ihrer Systemkonfiguration mit eingeschlossen.

Bei der ersten Ausführung des Event-Servers werden dessen Konfigurationsdateien alle automatisch in die SQL Datenbank verschoben. Sie können die wiederhergestellte Konfiguration auf den Event-Server anwenden, ohne ihn neustarten zu müssen und der Event-Server kann während des Ladens der Konfigurationswiederherstellung jegliche externe Kommunikation starten und stoppen.

Planmäßige Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung)

Der Management-Server speichert die Systemkonfiguration in einer SQL-Datenbank. Milestone empfiehlt regelmäßige Datensicherungen dieser SQL-Datenbank, um die Daten im Notfall wiederherstellen zu können. Auch wenn es selten vorkommt, dass die Systemkonfiguration verloren geht, kann es dennoch unter unglücklichen Umständen passieren. Zum Glück dauert dies lediglich 1 Minute, und die Datensicherung hat den weiteren Vorteil, dass dabei das Transaktionsprotokoll Ihrer SQL-Datenbank geleert wird.

Wenn Sie ein kleineres System besitzen und keine planmäßigen Sicherungen benötigen, können Sie Ihre Systemkonfiguration auch manuell sichern. Anweisungen hierzu finden Sie unter Manuelle Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung) auf Seite 499.

Achten Sie bei der Sicherung/Wiederherstellung Ihrer Management-Server darauf, dass die SQL-Datenbank mit der Systemkonfiguration der Sicherung/Wiederherstellung mit berücksichtigt wird.

Anforderungen an die Verwendung von planmäßiger Sicherung und Wiederherstellung

Microsoft® SQL Server Management Studio, ein Tool, das kostenlos von ihrer Internetseite (https://www.microsoft.com/downloads/) heruntergeladen werden kann.

Abgesehen von der Verwaltung von SQL Server und von deren Datenbanken enthält das Tool einfach anzuwendende Sicherungs- und Wiederherstellungsfunktionen. Laden Sie das Tool herunter und installieren Sie es auf Ihrem Management-Server.

Sicherung der Systemkonfiguration mit planmäßiger Sicherung

1. Öffnen Sie im Windows-Startmenü Microsoft® SQL Server Management Studio.
2. Geben Sie bei der Verbindung den Namen des erforderlichen SQL Server an. Benutzen Sie das Konto mit dem Sie die SQL-Datenbank erstellt haben.
    1. Suchen Sie die SQL-Datenbank, die Ihre gesamte Systemkonfiguration enthält, einschließlich des Event-Servers, der Aufzeichnungsserver, Kameras, Eingaben, Ausgaben, Benutzern, Regeln, Wachrundgangsprofilen usw. Der standardmäßig vergebene Name für diese SQL-Datenbank ist **Überwachung**.
    2. Führen Sie eine Sicherung der SQL-Datenbank durch und stellen achten Sie auf folgendes:
        - Überprüfen Sie, ob die ausgewählte SQL-Datenbank die richtige ist
        - Bestätigen Sie, dass der Sicherungstyp **Vollständig** ist
        - Legen Sie den Termin für die wiederkehrende Sicherung. Sie können mehr über planmäßige und automatische Sicherungen auf der Microsoft-Webseite (https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017) erfahren.
        - Bestätigen Sie, dass der vorgeschlagene Pfad zufriedenstellend ist oder wählen Sie einen alternativen Pfad aus
        - Wählen Sie **Bestätigung bei Sicherungsende** aus und **Checksum ausführen, bevor auf Medium geschrieben wird**
3. Folgen Sie den Anweisungen im Tool bis zum Ende.

Erwägen Sie auch eine Sicherung der SQL-Datenbank des Protokollservers mitsamt Ihren Protokollen nach der gleichen Methode. Der standardmäßig vergebene Name für die SQL-Datenbank des Protokollservers ist **SurveillanceLogServerV2**.

Wiederherstellen einer Systemkonfiguration aus einer planmäßigen Sicherung

Voraussetzungen
Damit während der Wiederherstellung der SQL-Datenbank der Systemkonfiguration keine Änderungen an der Systemkonfiguration vorgenommen werden, stoppen Sie den:

- Managementserver Dienst (siehe Serverdienste verwalten auf Seite 515)
- Ereignisserver Dienst (erfolgt über Windows-**Dienste** (suchen Sie auf Ihrem Computer nach **services.msc**. Suchen Sie innerhalb von **Dienste** nach **Milestone XProtect Event Server**))
- World Wide Web Publishing Service, auch als Internet Information Service (IIS) bekannt. Erfahren Sie, wie man den IIS stoppt (https://technet.microsoft.com/library/cc732317(WS.10).aspx/)

Öffnen Sie Microsoft® SQL Server Management Studio vom Windows-**Startmenü** aus.

Machen Sie im Tool Folgendes:

1. Geben Sie bei der Verbindung den Namen des erforderlichen SQL Server an. Verwenden Sie das Konto, unter dem die SQL-Datenbank erstellt wurde.
2. Suchen Sie die SQL-Datenbank (deren standardmäßig vergebene Name **Überwachung** ist), die Ihre vollständige Systemkonfiguration enthält, einschließlich des Event-Servers, der Aufzeichnungsserver, Kameras, Eingaben, Ausgaben, Benutzer, Regeln, Wachrundgangsprofilen usw.
3. Führen Sie eine Wiederherstellung der SQL-Datenbank durch und achten Sie darauf, :
   - Auswählen, um **vom** Gerät zu sichern
   - Auswählen von Sicherungsmedium **Datei**
   - Suchen Sie Ihre Sicherungsdatei (**.bak** aus und wählen Sie sie aus
   - Auswählen, um **bereits bestehende Datenbank zu überschreiben**
4. Folgen Sie den Anweisungen im Tool bis zum Ende.

Verwenden Sie die gleiche Methode zur Wiederherstellung der SQL-Datenbank des Protokollservers mit Ihren Protokollen. Der standardmäßig vergebene Name für die SQL-Datenbank des Protokollservers ist **SurveillanceLogServerV2**.

Das System funktioniert nicht, während der Managementserver-Dienst angehalten wird. Es ist wichtig daran zu denken, alle Dienste nach der Wiederherstellung der Datenbank wieder zu starten.

Sicherung der SQL-Datenbank des Protokollservers

Bearbeiten Sie die SQL-Datenbank des Protokollservers mit der gleichen Methode wie die oben beschriebene Bearbeitung der Systemkonfiguration. Die SQL-Datenbank des Protokollservers enthält alle Ihre Systemprotokolle, einschließlich der von Aufzeichnungsservern und Kameras gemeldeten Fehler. Der standardmäßig vergebene Name für die SQL-Datenbank des Protokollservers ist **SurveillanceLogServerV2**.

Die SQL-Datenbank befindet sich auf dem SQL Server des Protokollservers. Protokollserver und Management-Server haben typischerweise ihre SQL-Datenbanken auf demselben SQL Server. Die Sicherung der SQL-Datenbank des Protokollservers ist nicht von unbedingter Wichtigkeit, da sie keinerlei Systemkonfigurationen enthält, allerdings könnte Ihnen der Zugriff auf Systemprotokolle aus der Zeit vor der Sicherung/Wiederherstellung des Management-Servers von Nutzen sein.

Fehler bei der Sicherung und Wiederherstellung sowie weitere Problemfälle (Erklärung)

- Wenn Sie nach Ihrer letzten Sicherung der Systemkonfiguration den Event-Server oder andere registrierte Dienste, wie z. B. den Log-Server verschoben haben sollten, müssen Sie die Konfiguration der registrierten Dienste für Ihr neues System auswählen. Sie können die neue Konfiguration beibehalten, nachdem das System zur alten Version wiederhergestellt wurde. Sie können einfach entscheiden, indem Sie einen Blick auf die Hostnamen der Dienste werfen.

- Wenn die Wiederherstellung der Systemkonfiguration fehlschlägt, weil der Event-Server nicht am angegeben Ort aufzufinden ist (beispielsweise, wenn Sie eine ältere Einrichtung registrierter Dienste gewählt haben), sollten Sie eine erneute Wiederherstellung durchführen.
- Wenn Sie bei der Wiederherstellung der Konfiguration von einem Backup das Passwort für die Systemkonfiguration falsch eingeben, müssen Sie das Passwort für die Systemkonfiguration eingeben, das zu dem Zeitpunkt gültig war, als das Backup erstellt wurde.

Den Management-Server bewegen

Der Management-Server speichert die Systemkonfiguration in einer SQL-Datenbank. Sollten Sie den Management-Server von einem physischen Server zu einen anderen verschieben, ist es besonders wichtig, sicherzustellen, dass Ihr neuer Management-Server ebenfalls Zugriff zu dieser SQL-Datenbank bekommt. Die SQL-Datenbank für die Systemkonfiguration kann auf zweierlei Arten gespeichert werden:

- **Netzwerk SQL Server**: Wenn Sie Ihre Systemkonfiguration in einer SQL-Datenbank auf einem SQL Server in Ihrem Netzwerk speichern, können Sie auf den Speicherort der SQL-Datenbank auf diesem SQL Server verweisen, wenn Sie die Management-Server-Software auf Ihrem neuen Management-Server installieren. In diesem Fall gilt lediglich der folgende Absatz zum Hostnamen des Management-Servers und zur IP-Adresse, und Sie sollten den Rest dieses Themas ignorieren:

  Hostname und IP-Adresse des Management-Servers: Wenn Sie den Management-Server von einem physischen Server zum anderen verschieben, erweist es sich am Einfachsten dem neuen Server den gleichen Hostnamen und IP-Adresse wie dem Alten zu geben. Dies liegt daran, dass der Aufzeichnungsserver sich automatisch mit dem Hostnamen und der IP-Adresse des alten Management-Servers verbindet. Wenn Sie dem neuen Managementserver einen neuen Hostnamen bzw. eine neue IP-Adresse geben, kann der Aufzeichnungsserver den Managementserver nicht mehr finden. Sie müssen dann jeden Aufzeichnungsserver-Dienst in Ihrem System von Hand anhalten, die URL des dort angegebenen Managementservers ändern, den Aufzeichnungsserver erneut registrieren, und wenn dies erfolgt ist, den Dienst Aufzeichnungsserver starten.
- **Lokal SQL Server**: Wenn Sie Ihre Systemkonfiguration in einer SQL-Datenbank auf einem SQL Server auf dem Management-Server selbst speichern, ist es wichtig, dass Sie die Datenbank mit der SQL-Datenbank mit der Systemkonfiguration des bestehenden Management-Servers vor dem Verschieben sichern. Durch die Sicherung der SQL-Datenbank und anschließende Wiederherstellung auf einem SQL Server auf dem neuen Management-Server vermeiden Sie, nach dem Umzug Ihre Kameras, Regeln, Zeitprofile usw. neu konfigurieren zu müssen

Wenn Sie mit dem Management Server umziehen, brauchen Sie das aktuelle Passwort für die Systemkonfiguration, um das Backup wiederherzustellen, siehe Passwort für die Systemkonfiguration (Erklärung) auf Seite 497.

Voraussetzungen

- **Das Installationsdatei der Software für die Installation auf dem neuen Management-Server**
- **Die Software-Lizenzdatei (.lic)**, die Sie erhalten haben als Sie das System gekauft und zuerst installiert haben. Sie sollten nicht die aktivierte Software-Lizenzdatei verwenden, die Sie nach einer manuellen Offline-Aktivierung einer Lizenz erhalten haben. Eine aktivierte Software-Lizenzdatei enthält Informationen über den spezifischen Server, auf dem das System installiert ist. Daher kann eine aktivierte Software-Lizenzdatei beim Umzug auf einen neuen Server nicht wiederverwendet werden

Wenn Sie beim Umzug auch Ihre Systemsoftware upgraden, haben Sie eine neue Software-Lizenzdatei erhalten. Verwenden Sie diese einfach.

- **Nur lokale SQL Server Benutzer: Microsoft® SQL Server Management Studio**
- Was geschieht, während der Management-Server nicht mehr verfügbar ist? Nicht verfügbare Management-Server (Erklärung) auf Seite 504)
- Kopieren Sie die Protokollserver-Datenbank (siehe Sicherung der SQL-Datenbank des Protokollservers auf Seite 502)

Nicht verfügbare Management-Server (Erklärung)

- **-Aufzeichnungsserver können weiterhin aufzeichnen**: Jeder derzeitige laufende Aufzeichnungsserver erhielt eine Kopie Ihrer Konfiguration vom Management-Server, damit sie weiterhin arbeiten und Aufzeichnungen selbstständig speichern können, während der Management-Server heruntergefahren ist. Planmäßige und durch Bewegung ausgelöste Aufzeichnung funktioniert daher weiterhin, und durch Ereignisse ausgelöste Aufzeichnung ebenfalls, wenn die Ereignisse in Relation zum Management-Server oder einem anderen Aufzeichnungsserver besteht, da diese durch den Management-Server geleitet werden
- **Aufzeichnungsserver speichern Protokolldaten vorübergehend lokal**: Sie senden automatisch Protokolldaten zum Management-Server, wenn dieser wieder zur Verfügung steht:
  - **Clients können sich nicht anmelden**: Clientzugriff wird durch den Management-Server autorisiert. Ohne den Management-Server können sich Clients nicht anmelden
  - **Clients, die bereits angemeldet sind, bleiben bis zu eine Stunde eingeloggt**: Wenn sich Clients anmelden werden sie vom Management-Server autorisiert und können mit dem Aufzeichnungsserver bis zu eine Stunde lang kommunizieren. Ihre Benutzer sind nicht betroffen, sofern Sie einen neuen Management-Server innerhalb einer Stunde aufsetzen
  - **Keine Fähigkeit zur Konfiguration des Systems**: Ohne den Management-Server können Sie die Systemkonfiguration nicht ändern

Milestone empfiehlt, dass Sie Ihre Benutzer über die Möglichkeit von Verbindungsabbrüchen mit dem Überwachungssystem, während der Ausfallzeit des Management-Servers, informieren.

Verschieben der Systemkonfiguration

Das Bewegen Ihrer Systemkonfiguration ist ein Prozess mit drei Schritten:

1. Führen Sie eine Sicherung Ihrer Systemkonfiguration durch. Dies entspricht exakt der Erstellung einer geplanten Sicherungskopie. Siehe auch Sicherung der Systemkonfiguration mit planmäßiger Sicherung auf Seite 501.
2. Installieren Sie den neuen Management-Server auf dem neuen Server. Siehe „planmäßige Sicherung", Schritt 2.
3. Stellen Sie Ihre Systemkonfiguration im neuen System wieder her. Siehe auch Wiederherstellen einer Systemkonfiguration aus einer planmäßigen Sicherung auf Seite 501.

Ersetzen eines Aufzeichnungsservers

Wenn ein Aufzeichnungsserver ausfällt und Sie möchten ihn mit einem neuen Server ersetzen, der die Einstellungen des alten Aufzeichnungsservers übernimmt:

1. Rufen Sie die Aufzeichnungsserver-ID des alten Aufzeichnungsserver ab:
    1. Wählen Sie **Aufzeichnungsserver**, dann wählen Sie im Bereich **Übersicht** den alten Aufzeichnungsserver aus.
    2. Wählen Sie die Registerkarte **Speicher** aus.
    3. Drücken und halten Sie die STRG-Taste auf Ihrer Tastatur, während Sie die Registerkarte **Info** auswählen.
    4. Kopieren Sie die Aufzeichnungsserver-ID in den unteren Teil der Registerkarte **Info**. Kopieren Sie nicht den Begriff *ID*, sondern nur die Zahl selbst.

2. Ersetzen Sie die Aufzeichnungsserver-ID auf dem neuen Aufzeichnungsserver:
    1. Stoppen Sie den Aufzeichnungsserver-Dienst auf dem alten Aufzeichnungsserver und stellen Sie dann in den Windows-**Diensten** den **Starttyp** auf **Deaktiviert**.

> Es ist äußerst wichtig, dass Sie nicht zwei Aufzeichnungsserver mit identischer ID zur gleichen Zeit starten.

    2. Öffnen Sie auf dem neuen Aufzeichnungsserver ein Explorerfenster und gehen Sie zu *C:\ProgramData\Milestone\XProtect Recording Server* oder den Pfad, wo Ihr Aufzeichnungsserver untergebracht ist.
    3. Öffnen Sie die Datei *RecorderConfig.xml*.

4. Löschen Sie die ID, die zwischen den Tags *<id>* und *</id>* angegeben ist.

5. Fügen Sie die kopierte Aufzeichnungsserver-ID zwischen den Tags *<id>* und *</id>* ein. Speichern Sie die *RecorderConfig.xml*-Datei.
6. Gehen Sie in die Registry: *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation*.
7. Öffnen Sie **RecorderIDOnMachine** und ersetzen Sie die alte Aufzeichnungsserver-ID mit der neuen ID.

3. Registrieren Sie den neuen Aufzeichnungsserver auf dem Managementserver. Klicken Sie hierfür mit der rechten Maustaste auf das Taskleistensymbol Recording Server Manager und klicken Sie auf **Registrieren**. Weitere Informationen finden Sie unter Registrieren eines Aufzeichnungsservers auf Seite 149.
4. Starten Sie den Aufzeichnungsserver-Dienst neu. Sobald der neue Aufzeichnungsserver-Dienst gestartet wird, wurden alle Einstellungen des alten Aufzeichnungsservers übernommen.

Hardware verschieben

Sie können Hardware zwischen Aufzeichnungsservern verschieben, die zum selben Standort gehören. Nachdem sie verschoben worden sind, laufen die Hardware und Geräte auf dem neuen Aufzeichnungsserver und neue Aufzeichnungen werden auf diesem gespeichert. Das Verschieben von Hardware und Geräten ist für Clientbenutzer transparent.

Die Aufzeichnungen auf dem alten Aufzeichnungsserver bleiben dort, bis:

- Das System sie löscht, wenn die Speicherzeit abläuft. Aufzeichnungen, die mit einer Beweissicherung geschützt sind (siehe Beweissicherung (Erklärung) auf Seite 433), werden nicht gelöscht, bis die Beweissicherungsfrist abläuft. Bei der Erstellung von Beweissicherungen bestimmen Sie ihre Speicherzeit. Potenziell läuft die Speicherzeit nie ab
- Sie löschen sie vom neuen Aufzeichnungsserver jedes Geräts auf der Registerkarte **Aufzeichnen**

Sie erhalten eine Warnung, wenn Sie versuchen einen Aufzeichnungsserver zu entfernen, der noch Aufzeichnungen enthält.

Wenn Sie Hardware auf einen Aufzeichnungsserver verschieben, dem gerade keine Hardware hinzugefügt ist, müssen die Clientbenutzer sich ausloggen und wieder einloggen, um Daten von den Geräten zu empfangen.

Sie können die Funktion zum Verschieben von Hardware für Folgendes nutzen:

- **Lastausgleich**: Falls beispielsweise die Festplatte eines Aufzeichnungsservers überlastet ist, können Sie einen neuen Aufzeichnungsserver hinzufügen und einige Hardware-Einheiten verschieben
- **Upgrade**: Wenn Sie beispielsweise den Hostserver des Aufzeichnungsservers durch ein neueres Modell ersetzen müssen, können Sie einen neuen Aufzeichnungsserver installieren und die Hardware vom alten auf den neuen Server verschieben
- **Ersetzen eines defekten Aufzeichnungsservers**: Wenn der Server beispielsweise offline ist und nie wieder online gehen wird, können Sie die Hardware auf andere Aufzeichnungsserver verschieben und so das System aufrechterhalten. Sie haben keinen Zugriff auf die alten Aufzeichnungen. Weitere Informationen finden Sie unter Ersetzen eines Aufzeichnungsservers auf Seite 505.

Fernaufzeichnungen

Wenn Sie Hardware auf einen anderen Aufzeichnungsserver verschieben, bricht das System laufende oder planmäßige Abfragen von verbundenen Standorten oder lokalen Speichern in Kameras ab. Die Aufzeichnungen werden nicht gelöscht, aber die Daten werden von den Datenbanken nicht gespeichert und empfangen wie üblich. Ist dies der Fall, erhalten Sie eine Warnung. Die Abfrage des XProtect Smart Client-Benutzers, der eine Abfrage bei Verschiebung der Hardware gestartet hat, schlägt fehl. Der XProtect Smart Client-Benutzer wird benachrichtigt und kann es später erneut versuchen.

Falls Hardware auf einen Remote-System verschoben wurde, müssen Sie den zentralen Standort mit der Option **Hardware aktualisieren** manuell synchronisieren, um die neue Konfiguration des Remote-Systems widerzuspiegeln. Wenn Sie keine Synchronisierung durchführen, bleiben die verschobenen Kameras vom zentralen Standort abgeschnitten.

Hardware verschieben (Assistent)

Führen Sie den **Hardware verschieben**-Assistenten aus, um Hardware zwischen Aufzeichnungsservern zu verschieben. Der Assistent führt Sie durch die notwendigen Schritte, um ein oder mehrere Hardware-Geräte zu verschieben.

Voraussetzungen
Bevor Sie den Assistenten starten:

- Stellen Sie sicher, dass der neue Aufzeichnungsserver über das Netzwerk Zugriff auf die physische Kamera hat
- Installieren Sie einen Aufzeichnungsserver, auf den Sie Hardware verschieben möchten (siehe Installation neuer XProtect-Komponenten auf Seite 93 oder Installation neuer XProtect-Komponenten auf Seite 93)
- Installieren Sie auf dem neuen Aufzeichnungsserver, das auf dem vorhandenen Server läuft, dasselbe Treiberpaket (siehe Gerätetreiber (Erklärung) auf Seite 69).

So starten Sie den Assistenten:

1. Wählen Sie im Bereich **Standort-Navigation Aufzeichnungsserver** aus.
2. Klicken Sie im Bereich **Übersicht** mit der rechten Maustaste auf den Aufzeichnungsserver, von dem Sie Hardware verschieben möchten, oder auf ein bestimmtes Gerät.
3. Wählen Sie **Hardware verschieben**.

   Es erscheint eine Fehlermeldung, falls der Aufzeichnungsserver, von dem Sie Hardware verschieben, vom Netzwerk getrennt ist. Sie sollten Hardware nur von einem getrennten Aufzeichnungsserver verschieben, wenn Sie sicher sind, dass dieser nie wieder online geht. Falls Sie Hardware trotzdem verschieben und der Server wieder online geht, riskieren Sie ein unerwartetes Verhalten des Systems, da dieselbe Hardware für einige Zeit auf zwei Aufzeichnungsservern läuft. Mögliche Probleme sind beispielsweise Lizenzfehler oder Ereignisse, die nicht an den richtigen Aufzeichnungsserver gesendet werden.

4. Wenn Sie den Assistenten auf der Ebene des Aufzeichnungsservers gestartet haben, erscheint die Seite **Wählen Sie die Hardware, die Sie verschieben möchten**. Wählen Sie die Geräte aus, die Sie verschieben möchten.
5. Wählen Sie auf der Seite **Wählen Sie den Aufzeichnungsserver, auf den Sie die Hardware verschieben möchten** aus der Liste der an diesem Standort installierten Aufzeichnungsservern aus.
6. Auf der Seite **Wählen Sie den Speicher, auf dem Aufzeichnungen zukünftig gespeichert werden sollen** zeigt der Speicherauslastungsbalken die freie Kapazität in der Aufzeichnungsdatenbank nur für Live-Aufzeichnungen an, nicht für Archive. Die gesamte Speicherzeit ist die Speicherzeit für die Aufzeichnungsdatenbank und die Archive.
7. Das System verarbeitet Ihre Anforderung.
8. Klicken Sie auf **Schließen**, wenn die Hardware erfolgreich verschoben wurde. Wenn Sie den neuen Aufzeichnungsserver im Management Client auswählen, können Sie die verschobene Hardware sehen und Aufzeichnungen werden nun auf diesem Server gespeichert.

   Wenn der Vorgang fehlgeschlagen ist, können Sie das Problem unten beheben.

   In einem vernetzten System müssen Sie den zentralen Standort nach einer Verschiebung von Hardware auf einen Remote-System manuell synchronisieren, um die Änderungen, die Sie oder ein anderer Systemadministrator gemacht haben, widerzuspiegeln.

Fehlerbehandlung beim Verschieben von Hardware

Wenn Hardware nicht verschoben werden konnte, kann einer der folgenden Gründe dafür verantwortlich sein:

Fehlertyp	Fehlerbehandlung
Der Aufzeichnungsserver ist nicht verbunden oder befindet sich im Failover-Modus.	Stellen Sie sicher, dass der Aufzeichnungsserver online ist. Sie müssen ihn ggf. registrieren. Falls sich der Server im Failover-Modus befindet, warten Sie und versuchen Sie es dann erneut.
Bei dem Aufzeichnungsserver handelt es sich nicht um die aktuellste Version.	Aktualisieren Sie den Aufzeichnungsserver, damit er dieselbe Version wie der Management-Server hat.
Der Aufzeichnungsserver konnte in der Konfiguration nicht gefunden werden.	Stellen Sie sicher, dass der Aufzeichnungsserver nicht deinstalliert wurde.
Die Aktualisierung der Konfiguration oder die Kommunikation mit der Konfigurationsdatenbank ist fehlgeschlagen.	Achten Sie darauf, dass Ihr SQL Server und die dazugehörige Datenbank verbunden sind und laufen.
Das Beenden der Hardware auf dem aktuellen Aufzeichnungsserver ist fehlgeschlagen	Möglicherweise wurde der Aufzeichnungsserver durch einen anderen Prozess gesperrt, oder er befindet sich im Fehler-Modus. Stellen Sie sicher, dass der Aufzeichnungsserver läuft und versuchen Sie es erneut.
Die Hardware ist nicht vorhanden.	Stellen Sie sicher, dass die Hardware, die Sie verschieben möchten, nicht durch einen anderen Benutzer simultan vom System deinstalliert wurde. Dieses Szenario ist sehr unwahrscheinlich.
Der Aufzeichnungsserver, dessen Hardware verschoben wurde, ist wieder online, doch Sie haben ihn ignoriert, als er offline war.	Höchstwahrscheinlich waren Sie der Ansicht, dass der alte Aufzeichnungsserver nicht mehr online gehen wird, als Sie den Assistenten zum **Hardware verschieben** gestartet haben, doch der Server ist während des Vorgangs online gegangen. Starten Sie den Assistenten erneut und wählen Sie **Nein** aus, wenn Sie aufgefordert werden zu bestätigen, dass der Server wieder online geht.
Der Quellenaufzeichnungsspeicher ist nicht verfügbar.	Sie versuchen, Hardware mit Geräten zu verschieben, die mit einem Aufzeichnungsspeicher konfiguriert sind, der derzeit jedoch offline

Fehlertyp	Fehlerbehandlung
	ist. Ein Aufzeichnungsspeicher ist offline, wenn die Festplatte offline oder anderweitig nicht verfügbar ist. Stellen Sie sicher, dass der Aufzeichnungsserver online ist, und versuchen Sie es erneut.
Alle Aufzeichnungsspeicher müssen auf dem Ziel-Aufzeichnungsserver verfügbar sein.	Sie versuchen, Hardware auf einen Aufzeichnungsserver zu verschieben, auf dem derzeit ein oder mehrere Aufzeichnungsspeicher offline sind. Stellen Sie sicher, dass alle Aufzeichnungsspeicher auf dem Ziel-Aufzeichnungsserver online sind. Ein Aufzeichnungsspeicher ist offline, wenn die Festplatte offline oder anderweitig nicht verfügbar ist.

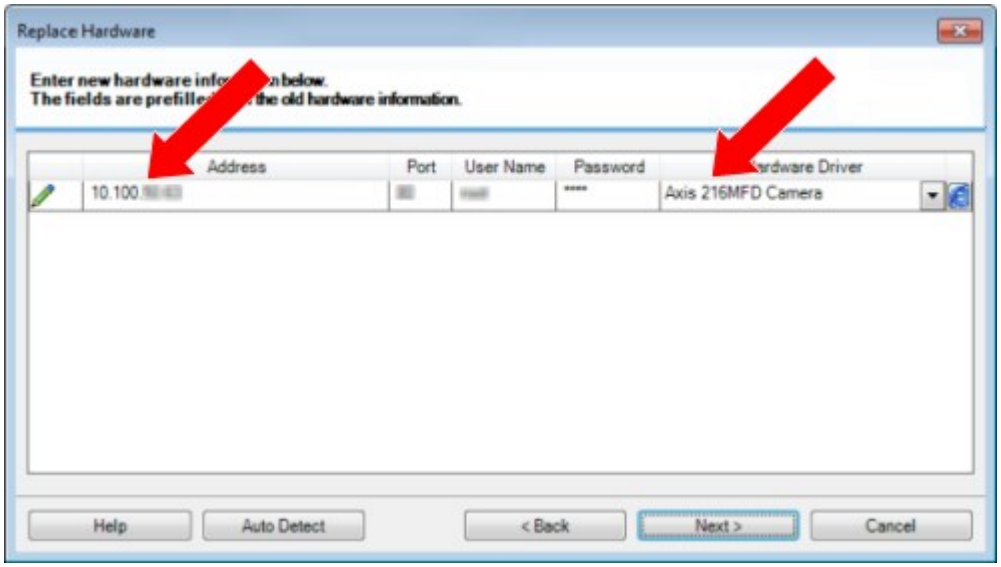
Hardware ersetzen

Wenn Sie ein Gerät in Ihrem Netzwerk mit einem anderen ersetzen, müssen Sie die IP-Adressen, den Port, Benutzernamen und das Passwort des neuen Geräts kennen.

Wenn Sie die Lizenzinformationen auf Seite 138 nicht aktiviert haben und alle Geräteänderungen ohne Aktivierung (siehe Lizenzinformationen auf Seite 138) aufgebraucht haben, müssen Sie Ihre Lizenzen manuell aktivieren, **nachdem** Sie die Geräte ausgetauscht haben. Sollte die neue Anzahl an Geräten Ihre Gesamtanzahl von Gerätelizenen überschreiten, müssen Sie neue Lizenzen kaufen.

1. Erweitern Sie den erforderlichen Aufzeichnungsserver, und klicken Sie mit der rechten Maustaste auf die Hardware, die Sie ersetzen möchten.
2. Wählen Sie **Hardware ersetzen** aus.
3. Der Assistent **Hardware ersetzen** erscheint. Klicken Sie auf **Weiter**.

4. Im Feld **Adresse** des Assistenten (durch roten Pfeil in der Abbildung markiert), geben Sie die IP-Adresse der neuen Hardware ein. Falls bekannt, wählen Sie die zugehörigen Treiber aus der Dropdown-Liste **Hardware-Treiber**. Andernfalls wählen Sie die **Automatische Erkennung** aus. Wenn Port, Benutzername oder Passwortdaten der neuen Hardware abweichen, korrigieren Sie dies **bevor der Prozess der automatischen Erkennung (falls benötigt) startet**.



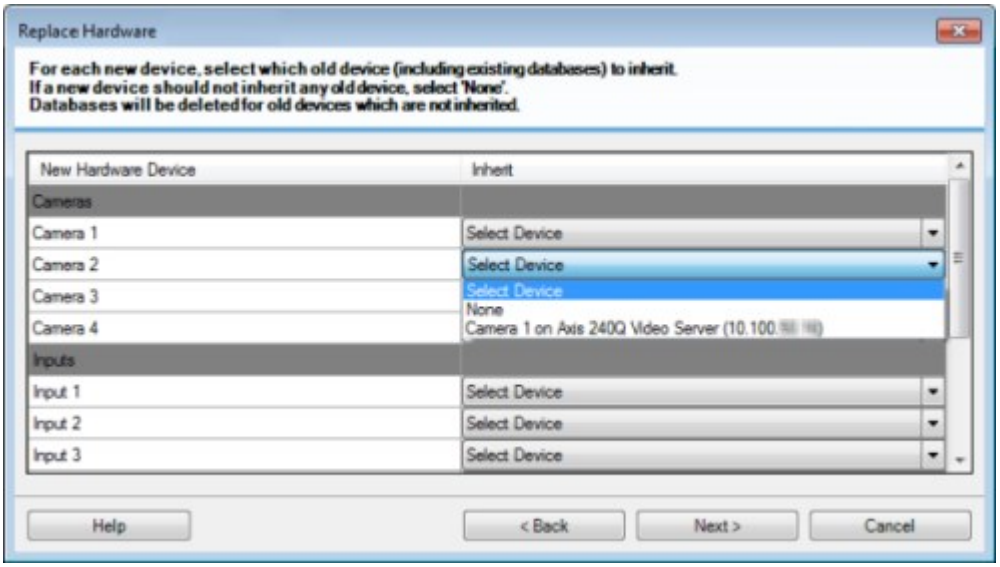
Der Assistent ist vorgefüllt mit Daten aus der bestehenden Hardware. Wenn Sie diese mit einem ähnlichen Gerät ersetzen, können Sie einige Daten gegebenenfalls wiederverwenden (z. B. Port- und Treiberinformationen).

5. Gehen Sie wie folgt vor:
   - Wenn Sie die erforderlichen Gerätetreiber direkt aus der Liste ausgewählt haben, klicken Sie auf **Weiter**
   - Wenn Sie **Automatische Erkennung** in der Liste ausgewählt haben, klicken Sie auf **Automatische Erkennung**, warten Sie auf den erfolgreichen Abschluss dessen (durch ein ✓ ganz links markiert) und klicken Sie dann auf **Weiter**

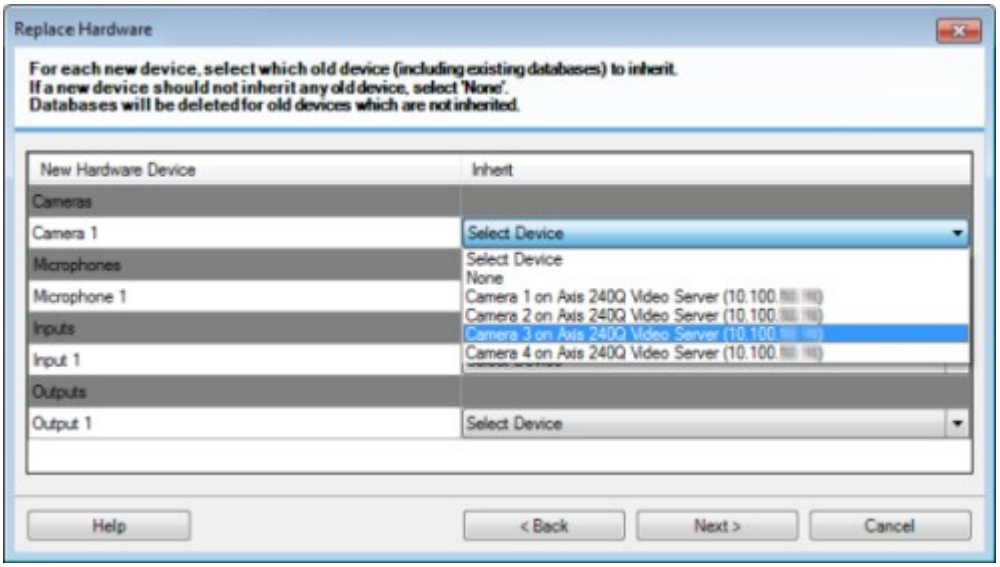
     Dieser Schritt hilft Ihnen dabei Geräte und ihre Datenbanken zusammenzuführen, abhängig von der Anzahl individueller Kameras, Mikrofone, Eingaben, Ausgaben usw., die an der alten bzw. neuen Hardware angebracht ist.

     Es ist wichtig darüber nachzudenken, **wie** man Datenbanken alter Geräte zu den Datenbanken neuer Geräte zusammenfügt. Sie führen die tatsächliche Zusammenführung individueller Geräte mittels der Auswahl einer korrespondierenden Kamera, Mikrofon, Eingabe, Ausgabe oder **Nichts** dergleichen in der Spalte auf der rechten Seite durch.

     > ⚠ Stellen Sie sicher, **alle** Kameras, Mikrofone, Eingaben, Ausgaben, usw. zuzuordnen. Inhalte, denen **Nichts** zugeordnet wird, gehen **verloren**.



Beispiel, in dem die alte Hardware über mehr individuelle Geräte verfügt als die neue:



Klicken Sie auf **Weiter**.

6. Ihnen wird eine Liste mit Hardware angeboten, die Sie hinzufügen, ersetzen oder entfernen können. Klicken Sie auf **Bestätigen**.
7. Der letzte Schritt ist eine Zusammenfassung hinzugefügter, ersetzter und übernommener Geräte und ihren Einstellungen. Klicken Sie auf **In die Zwischenablage kopieren**, um Inhalte in die Windows-Zwischenablage zu kopieren oder/und **Schließen**, um den Assistenten zu beenden.

Verwaltung des SQL Server und der Datenbanken

Ändern des SQL Server und der Datenbankadressen (Erläuterung)

Wenn Sie ein System in der Probeversion installieren oder eine große Installation neu strukturieren, müssen Sie ggf. eine andere SQL Server und Datenbank verwenden. Dies können Sie mit dem Tool zum **Aktualisieren SQL Server der Adresse** tun.

Mit diesem Tool können Sie die Adresse des SQL Server und der Datenbank ändern, die vom Management-Server und vom Event-Server verwendet wird, sowie die Adresse des vom Protokollserver verwendeten SQL Server und der Datenbank. Die einzige Beschränkung ist die, dass Sie die SQL-Adressen des Management-Servers und des Event-Servers nicht gleichzeitig mit den SQL-Adressen des Protokollservers ändern können. Sie können dies aber nacheinander machen.

Sie müssen die Adressen der SQL Server und der Datenbanken lokal auf den Computern ändern, auf denen Sie den Management-Server, den Event-Server und den Protokollserver installiert haben. Wenn Ihr Management-Server und Ihr Event-Server auf separaten Computern installiert sind, müssen Sie das Tool **Update SQL Server von Adressen** auf beiden Computern ausführen.

Die SQL-Datenbank muss kopiert werden, bevor Sie fortfahren.

Ändern der SQL Server und der Datenbank des Protokollservers

1. Gehen Sie zu dem Computer, auf dem Sie den Management-Server installiert haben, und kopieren Sie das Verzeichnis *%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress* (samt Inhalt) in ein temporäres Verzeichnis auf dem Event-Server.
2. Fügen Sie das Verzeichnis ein, das Sie an einen temporären Speicherort auf dem Computer kopiert haben, auf dem der Protokollserver installiert ist, und führen Sie die darin enthaltene Datei aus: *VideoOS.Server.ChangeSqlAddress.exe*. Das Dialogkästchen **Adresse SQL Server Aktualisieren** erscheint.
3. Wählen Sie den **Log Server** aus und klicken Sie dann auf **Weiter**.
4. Geben Sie einen neuen SQL Server ein oder wählen Sie ihn aus und klicken Sie dann auf **Weiter**.
5. Wählen Sie die neue SQL-Datenbank aus und klicken Sie auf **Auswahl**.
6. Warten Sie, während die Adressenänderung durchgeführt wird. Klicken Sie zur Bestätigung auf **OK**.

Ändern der SQL-Adressen des Management-Servers und des Event-Servers

Management-Server und Event-Server verwenden dieselbe SQL-Datenbank.

1. Wenn Ihr Management-Server und Event-Server lokalisiert sind:
    1. gemeinsam auf demselben Computer und Sie möchten beide SQL-Adressen aktualisieren, gehen Sie zu dem Computer, auf dem Ihr Management-Server installiert ist.
    2. auf verschiedenen Computer, und Sie möchten die SQL-Adresse des Management-Servers (und später die SQL-Adresse des Event Servers) aktualisieren. Verwenden Sie hierfür den Computer, auf dem Ihr Management-Server installiert ist.
    3. auf verschiedenen Computern, und Sie möchten die SQL-Adresse des Event-Servers aktualisieren (oder Sie haben sie bereits auf dem Management-Server aktualisiert); verwenden Sie hierfür den Computer, auf dem Ihr Management-Server installiert ist, und kopieren Sie das Verzeichnis *%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress* (samt Inhalt) in ein temporäres Verzeichnis auf dem Event-Server.
2. Wenn Sie:
    1. Schritte **1.1** und **1.2** auswählen, gehen Sie in den Benachrichtigungsbereich der Taskleiste. Klicken Sie dort mit der rechten Maustaste auf das Symbol **Management-Server**, und wählen Sie dann **SQL-Adresse aktualisieren** aus. Sie müssen den Prozess wiederholen, um die SQL-Adresse des Event-Servers zu aktualisieren.
    2. Schritt **1.3** – Fügen Sie das Verzeichnis ein, das Sie an einen vorläufigen Ort auf dem Computer kopiert haben, auf dem der Event-Server installiert ist, und führen Sie die enthaltene Datei aus:*VideoOS.Server.ChangeSqlAddress.exe*.

3. Das Dialogkästchen **Adresse SQL Server Aktualisieren** erscheint. Wählen Sie **Management-Serverdienste** aus und klicken Sie dann auf **Weiter**.
4. Geben Sie einen neuen SQL Server ein oder wählen Sie ihn aus und klicken Sie dann auf **Weiter**.
5. Wählen Sie die neue SQL-Datenbank aus und klicken Sie auf **Auswahl**.
6. Warten Sie, während die Adressenänderung durchgeführt wird. Wenn eine Bestätigungsmeldung gezeigt wird, klicken Sie auf **OK**.

Serverdienste verwalten

Auf dem Rechner, auf dem Serverdienste laufen, finden Sie Serververwaltungs-Taskleistensymbole im Benachrichtigungsbereich. Über diese Symbole können Sie Informationen über die Serverdienste erhalten und gewisse Aktionen durchführen. Dies schließt beispielsweise das Überprüfen des Status der Dienste ein, sowie eine Ansicht von Protokollen oder Statusmeldungen und das Starten/Stoppen der Dienste.

Taskleistensymbole für den Servermanager (Erläuterung)

Die Taskleistensymbol in der Tabelle zeigen die verschiedenen Zustände der Dienste, die auf dem Managementserver, dem Aufzeichnungsserver, dem ausfallsicheren Aufzeichnungsserver und auf dem Ereignisserver laufen. Diese werden im Benachrichtigungsbereich auf den Computern angezeigt, auf denen die Server installiert sind:

Management Server Manager Taskleistensymbol	Recording Server ManagerTaskleistensymbol	Event Server Manager Taskleistensymbol	Failover Recording Server Manager Taskleistensymbol	Beschreibung
				**Läuft** Erscheint, wenn ein Serverdienst aktiviert ist und gestartet wird.

Management Server Manager Taskleistensymbol	Recording Server ManagerTaskleistensymbol	Event Server Manager Taskleistensymbol	Failover Recording Server Manager Taskleistensymbol	Beschreibung
				Wenn der Failover Recording Server Dienst läuft, sodass

Management Server Manager Taskleistensymbol	Recording Server ManagerTaskleistensymbol	Event Server Manager Taskleistensymbol	Failover Recording Server Manager Taskleistensymbol	Beschreibung
				**Gestoppt** Erscheint, wenn ein Serverdienst angehalten wurde.

Management Server Manager Taskleistensymbol	Recording Server ManagerTaskleistensymbol	Event Server Manager Taskleistensymbol	Failover Recording Server Manager Taskleistensymbol	Beschreibung
				Wenn der Failover Recording Server-Dienst anhält, sodass kein

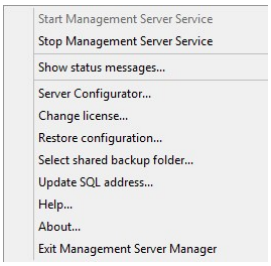
Management Server Manager Taskleistensymbol	Recording Server ManagerTaskleistensymbol	Event Server Manager Taskleistensymbol	Failover Recording Server Manager Taskleistensymbol	Beschreibung
				**Starte** Erscheint, wenn ein Serverdienst dabei ist, zu starten. Unter normalen Umständen wechselt das Taskleistensymbol nach kurzer Zeit in **Läuft**.
				**Halte an** Erscheint, wenn ein Serverdienst dabei ist, anzuhalten. Unter normalen Umständen wechselt das Taskleistensymbol nach kurzer Zeit in **Angehalten**.
				**In unbestimmtem Zustand** Erscheint, wenn der Serverdienst zunächst geladen wird, und bis die erste Information erhalten wird, worauf das Taskleistensymbol unter normalen Umständen in **Starte** wechselt, und danach in **Läuft**.

Management Server Manager Taskleistensymbol	Recording Server ManagerTaskleistensymbol	Event Server Manager Taskleistensymbol	Failover Recording Server Manager Taskleistensymbol	Beschreibung
				**Läuft offline** Erscheint typischerweise, wenn der Aufzeichnungsserver oder der ausfallsichere Aufzeichnungsserver läuft, der Managementserver Dienst jedoch nicht.

Starten oder Stoppen des Managementserver-Dienstes

Das Management Server Manager-Taskleistensymbol zeigt den Status des Managementserver-Dienstes an, beispielsweise **Läuft**. Durch dieses Symbol können Sie den Managementserver-Dienst starten oder stoppen. Wenn Sie den Managementserver-Dienst stoppen, können Sie den Management Client nicht nutzen.

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das Management Server Manager-Taskleistensymbol. Ein Kontextmenü erscheint.



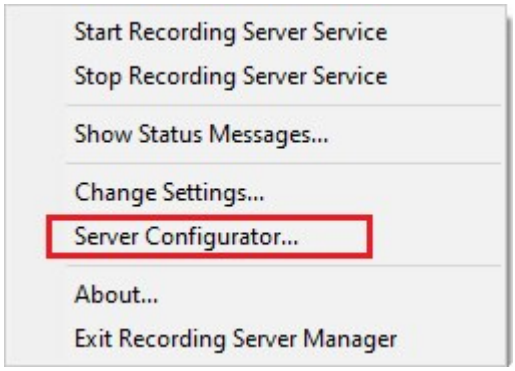
2. Wenn der Dienst angehalten wurde, klicken Sie auf **Managementserver-Dienst starten**, um ihn zu starten. Die Änderungen des Taskleistensymbols spiegeln den neuen Status wieder.
3. Um den Dienst anzuhalten, klicken Sie auf **Managementserver-Dienst stoppen**.

Für weitere Informationen über die Taskleistensymbole, siehe Taskleistensymbole für den Servermanager (Erläuterung) auf Seite 515.

Starten oder Stoppen des Aufzeichnungsserver-Dienstes

Das Recording Server Manager-Taskleistensymbol zeigt den Status des Aufzeichnungsserver-Dienstes an, beispielsweise **Läuft**. Durch dieses Symbol können Sie den Aufzeichnungsserver-Dienst starten oder stoppen. Wenn Sie den Aufzeichnungsserver-Dienst stoppen, kann Ihr System nicht mit den Geräten interagieren, die mit dem Server verbunden sind. Dies bedeutet, dass Sie kein aufgezeichnetes oder Live-Video ansehen können.

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das Recording Server Manager-Taskleistensymbol. Ein Kontextmenü erscheint.

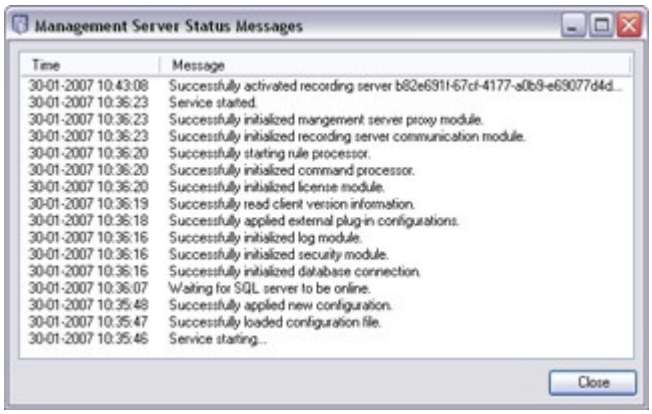


2. Wenn der Dienst angehalten wurde, klicken Sie auf **Aufzeichnungsserver-Dienst starten**, um ihn zu starten. Die Änderungen des Taskleistensymbols spiegeln den neuen Status wieder.
3. Um den Dienst anzuhalten, klicken Sie auf **Aufzeichnungsserver-Dienst stoppen**.

Für weitere Informationen über die Taskleistensymbole, siehe Taskleistensymbole für den Servermanager (Erläuterung) auf Seite 515.

Statusmeldungen für Management-Server oder Aufzeichnungsserver ansehen

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das relevante Taskleistensymbol. Ein Kontextmenü erscheint.
2. Wählen Sie **Statusmeldungen anzeigen**. Je nach Servertyp wird entweder das Fenster **Management-Server-Statusmeldungen** oder das Fenster **Aufzeichnungsserver-Statusmeldungen** mit Zeitstempel-Statusmeldungen eingeblendet:



Verschlüsselung verwalten mit dem Server Configurator

Verwenden Sie Server Configurator zum Auswählen von Zertifikaten auf den lokalen Servern für die verschlüsselte Kommunikation und registrieren Sie die Serverdienste, damit sie für die Kommunikation mit den Servern qualifiziert sind.

Öffnen Sie Server Configurator entweder vom Windows-Startmenü oder vom Taskleistensymbol für den Management Server aus.

Bevor Sie die Verschlüsselung aktivieren, müssen Sie auf dem Computer, auf dem der Management Server installiert ist, und auf allen Computern mit Aufzeichnungsservern, Sicherheitszertifikate installieren Weitere Informationen finden Sie im Zertifikate-Leitfaden dazu, wie Sie Ihre XProtect VMS Installationen sichern können..

Stellen Sie im Abschnitt **Verschlüsselung** des Server Configurator die folgenden Verschlüsselungstypen ein:

- **Serverzertifikate**

  Wählen Sie das Zertifikat aus, dass zur Verschlüsselung der wechselseitigen Verbindung zwischen dem Management Server, den Datensammlern und den Aufzeichnungsservern verwendet werden soll.

  > Die Verschlüsselung für den Mobile Server wird von Taskleistensymbol Mobile Server aus aktiviert.

- **Streamingmedienzertifikat**

  Wählen Sie das Zertifikat aus, das für die Verschlüsselung der Kommunikation zwischen den Aufzeichnungsservern und allen Clients, Servern und Integrationen verwendet werden soll, die Datenstreams von den Aufzeichnungsservern abrufen.

- **Zertifikat für mobile Streamingmedien**

  Wählen Sie ein Zertifikat aus, das für die Verschlüsselung der Kommunikation zwischen dem Mobile Server und den mobilen und Web Clients verwendet werden soll, die Datenstreams vom Moile Server abrufen.

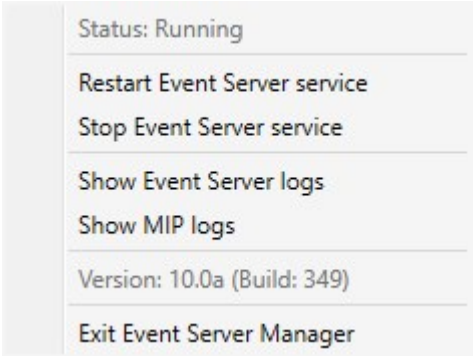
Registrieren Sie im Abschnitt **Server registrieren** des Server Configurator die Server, die auf dem Computer mit dem designierten Management Server laufen.

Zum Registrieren des Servers überprüfen Sie die Adresse des Management Servers und wählen Sie **Registrieren** aus.

Den Ereignisserver Dienst starten, anhalten oder neu starten

Das Event Server Manager-Taskleistensymbol zeigt den Status des Ereignisserver-Dienstes an, beispielsweise **Läuft**. Durch dieses Symbol können Sie den Ereignisserver-Dienst starten, stoppen oder neu starten. Wenn sie den Dienst anhalten funktionieren Teile des Systems nicht mehr, einschließlich Ereignisse und Alarme. Sie können allerdings immer noch Video ansehen und aufzeichnen. Weitere Informationen finden Sie unter Den Ereignisserver-Dienst stoppen auf Seite 524.

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das Event Server Manager-Taskleistensymbol. Ein Kontextmenü erscheint.



2. Wenn der Dienst angehalten wurde, klicken Sie auf **Ereignisserver-Dienst starten**, um ihn zu starten. Die Änderungen des Taskleistensymbols spiegeln den neuen Status wieder.
3. Um den Dienst neu zu starten oder anzuhalten, klicken Sie auf **Ereignisserver-Dienst neu starten** oder **Ereignisserver-Dienst stoppen**.

Für weitere Informationen über die Taskleistensymbole, siehe Taskleistensymbole für den Servermanager (Erläuterung) auf Seite 515.

Den Ereignisserver-Dienst stoppen

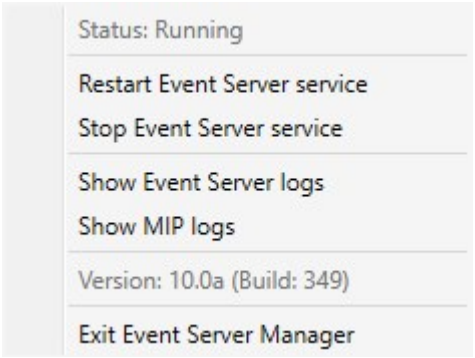
Bei Installation des MIP-Plug-ins auf dem Event-Server müssen Sie zuerst den Ereignisserver-Dienst stoppen und ihn danach neu starten. Allerdings funktionieren weite Teile des VMS-Systems nicht, während der Dienst gestoppt ist:

- Keinerlei Ereignisse oder Alarme werden auf dem Event-Server gespeichert. System- und Geräteereignisse lösen jedoch immer noch Aktionen, wie das Starten einer Aufzeichnung aus
- Zusatzprodukte funktionieren in XProtect Smart Client nicht und können vom Management Client nicht konfiguriert werden.
- Analyseereignisse funktionieren nicht
- Generische Ereignisse funktionieren nicht
- Keinerlei Alarme werden ausgelöst
- In XProtect Smart Client funktionieren Karten-Ansichtselemente, Alarmlisten-Ansichtselemente und der Alarm-Manager-Arbeitsplatz nicht
- MIP Plug-ins im Event-Server können nicht ausgeführt werden
- MIP Plug-ins in Management Client und XProtect Smart Client funktionieren nicht richtig

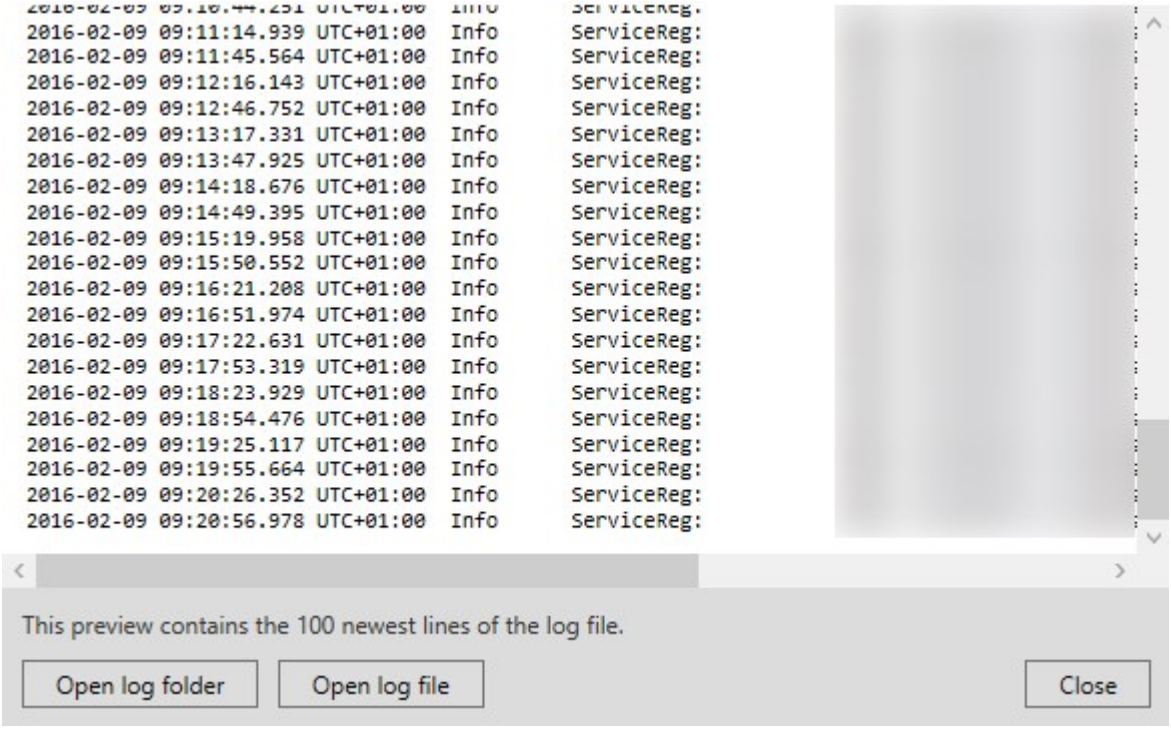
Event Server oder MIP-Protokolle anzeigen

Sie können Informationen mit Zeitstempel über Event-Server-Aktivitäten im Event-Server-Protokoll ansehen. Informationen über Integrationen von Dritten wird im MIP-Protokoll in einem Unterordner des **Event-Server**-Ordners gespeichert.

1. Klicken Sie im Benachrichtigungsbereich mit der rechten Maustaste auf das Event Server Manager-Taskleistensymbol. Ein Kontextmenü erscheint.



2. Zur Ansicht der 100 aktuellsten Zeilen im Event-Server-Protokoll, klicken Sie auf **Event-Server-Protokoll zeigen**. Ein Log-Viewer erscheint.



   1. Klicken Sie auf **Protokolldatei öffnen**, um die Protokolldatei anzusehen.
   2. Klicken Sie auf **Protokollordner öffnen**, um den Protokollordner zu öffnen.

3. Zur Ansicht der 100 aktuellsten Zeilen im MIP-Protokoll, gehen Sie zurück in das Kontextmenü und klicken Sie auf **MIP-Protokolle anzeigen**. Ein Log-Viewer wird angezeigt.

> Das Menü wird ausgegraut, wenn die Protokolldateien aus dem Protokollverzeichnis gelöscht werden. Sie müssen zunächst die Protokolldateien zurück in einen der folgenden Ordner kopieren, um den Log-Viewer zu öffnen: *C:\ProgramData\Milestone\XProtect Event Server\logs* oder *C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs*.

Verwaltung registrierter Dienste

Zeitweise gibt es Server und/oder Dienste, die mit dem System kommunizieren sollten, auch wenn sie nicht direkt Teil des System sind. Einige, aber nicht alle, Dienste können sich automatisch selbst im System registrieren. Dienste, die automatisch registriert werden können:

- Ereignisserver Dienst
- Protokollserver Dienst

Registrierte Dienste werden automatisch in der Liste registrierter Dienste angezeigt.

Sie können Server/Dienste als registrierte Dienste im Management Client manuell festlegen.

Registrierte Dienste hinzufügen und bearbeiten

1. Im Fenster **Registrierte Dienste hinzufügen/entfernen**, klicken Sie je nach Bedarf auf **Hinzufügen** oder **Bearbeiten**.
2. Im Fenster **Registrierten Dienst hinzufügen** oder **Registrierten Dienst bearbeiten** (je nach vorheriger Auswahl), können Sie Einstellungen festlegen oder bearbeiten.
3. Klicken Sie auf **OK**.

Netzwerkkonfiguration verwalten

In den Netzwerkkonfigurationseinstellungen können Sie die LAN- und WAN-Adressen des Management-Servers bestimmen und so eine Kommunikation zwischen Management-Server und vertrauten Servern ermöglichen.

1. Im Fenster **Registrierte Dienste hinzufügen/entfernen**, klicken Sie auf **Netzwerk**.
2. Geben Sie die LAN- und/oder WAN-IP-Adresse des Management-Servers an.

   Wenn alle beteiligten Server (Management-Server und vertraute Server) sich in Ihrem lokalen Netzwerk befinden, können Sie einfach die LAN-Adresse angeben. Wenn ein oder mehrere beteiligte Server über eine Internetverbindung auf das System zugreifen, müssen Sie außerdem die WAN-Adresse angeben.

3. Klicken Sie auf **OK**.

Eigenschaften registrierter Dienste

Im Fenster **Registrierten Dienst hinzufügen** oder **Registrierten Dienst bearbeiten**, legen Sie folgendes fest:

Komponente	Voraussetzung
Typ	Vorgefülltes Feld.
Name	Name des registrierten Dienstes. Der Name wird nur zu Anzeigezwecken im Management Client verwendet.
URLs	Klicken Sie auf **Hinzufügen**, um die IP-Adresse oder den Hostnamen des registrierten

Komponente	Voraussetzung
	Dienstes hinzuzufügen. Wenn ein Hostname als Teil einer URL angegeben wird, muss der Host vorhanden und auf dem Netzwerk verfügbar sein. URLs müssen mit *http://* oder *https://* anfangen und dürfen folgende Zeichen nicht enthalten: < > & ' " * ? | [ ] ". **Beispiel** für ein typisches URL-Format: *http://ipaddress:port/directory* (wobei Port und Verzeichnis optional sind). Sie können bei Bedarf mehr als eine URL hinzufügen.
Vertrauenswürdig	Wählen Sie diese Option aus, wenn der registrierte Dienst absolut vertrauenswürdig ist (dies ist oft der Fall, doch die Option bietet Ihnen die Flexibilität, den registrierten Dienst hinzuzufügen und ihn dann als vertrauenswürdig zu markieren, indem Sie ihn später bearbeiten). Durch das Ändern des Status der Vertrauenswürdigkeit wird auch der Status anderer registrierter Dienste geändert, die eine oder mehrere URLs mit dem relevanten registrierten Dienst gemeinsam haben.
Beschreibung	Beschreibung des registrierten Dienstes. Die Beschreibung wird nur zu Anzeigezwecken im Management Client verwendet.
Erweitert	Ein „erweiterter" Dienst verfügt er über besondere URI-Schemata (z. B. HTTP, HTTPS, TCP oder UDP), die für jede Host-Adresse, die Sie definieren, eingerichtet werden müssen. Daher hat eine Hostadresse mehrere Endpunkte, die jeweils über ein eigenes Schema, eine eigene Hostadresse und einen eigenen IP-Port für dieses Schema verfügen.

Entfernen von Gerätetreibern (Erklärung)

Wenn Sie die Gerätetreiber nicht länger auf Ihrem Computer benötigen, können Sie die Treiberpakete aus Ihrem System löschen. Dafür folgen Sie einfach der normalen Prozedur unter Windows zur Deinstallation von Programmen.

Sollten Sie mehrere Treiberpakete installiert haben und Probleme beim Löschen dieser Dateien haben, können Sie das Skript im Installationsordner des Treiberpakets verwenden, um diese vollständig zu löschen.

Bei Entfernen von Gerätetreibern ist die Kommunikation zwischen Aufzeichnungsserver und Kameras nicht länger möglich. Entfernen Sie deshalb Treiberpakete nicht wenn Sie aktualisieren, sondern installieren Sie die neue Version über die Alte. Nur wenn Sie das gesamte System deinstallieren, sollten Sie das Treiberpaket entfernen.

Deinstallieren eines Aufzeichnungsservers

Wenn Sie einen Aufzeichnungsserver deinstallieren, werden alle im Management Client festgelegten Konfigurationen für diesen Aufzeichnungsserver entfernt, inklusive der **gesamten** mit dem Aufzeichnungsserver assoziierten Hardware (Kameras, Eingabegeräte usw.).

1. Klicken Sie mit der rechten Maustaste im Bereich **Übersicht** auf den Aufzeichnungsserver, den Sie deinstallieren möchten.
2. Wählen Sie **Aufzeichnungsserver deinstallieren**.
3. Wenn Sie sich sicher sind, klicken Sie auf **Ja**.
4. Der Aufzeichnungsserver und die gesamte zugehörige Hardware werden deinstalliert.

Löschen sämtlicher Hardware auf einem Aufzeichnungsserver

Wenn Sie Hardware löschen, werden alle durch diese Hardware aufgezeichneten Daten dauerhaft gelöscht.

1. Klicken Sie mit der rechten Maustaste auf den Aufzeichnungsserver, von dem Sie sämtliche Hardware löschen möchten.
2. Wählen Sie **Sämtliche Hardware löschen**.
3. Bestätigen Sie die Löschung.

Fehlerbehandlung

Problem: Änderungen von SQL Server und Datenbankadressen verhindern den Zugriff auf die Datenbanken

Werden die Adressen zum SQL Server und zur Datenbank geändert, z.B. durch die Änderung des Host-Namen des Computers, auf dem der SQL Server läuft, so verliert der Aufzeichnungsserver den Zugriff auf die Datenbank. **Lösung: Verwenden Sie das Werkzeug zur Aktualisierung der SQL-Adresse, das im Recording Server Manager Taskleistensymbol** zu finden ist.

Problem: Aufzeichnungsserver läuft aufgrund eines Portkonflikts nicht an

Zu diesem Problem kann nur dann kommen, wenn der Dienst Simple Mail Transfer Protocol (SMTP) läuft, da dieser den Port 25 verwendet. Ist der Port 25 bereits in Gebrauch, so kann der Dienst Aufzeichnungsserver evtl. nicht gestartet werden. Es ist wichtig, dass Portnummer 25 für den SMTP-Dienst des Aufzeichnungsservers zur Verfügung steht.

SMTP-Dienst: Überprüfung und Lösungen

Zur Überprüfung, ob der SMTP-Dienst installiert wurde:

1. Wählen Sie aus dem Windows **Startmenü Systemsteuerung** aus.
2. Klicken Sie in der **Systemsteuerung** doppelt auf **Programme hinzufügen oder entfernen**.
3. Klicken Sie links in dem Fenster **Programme hinzufügen oder entfernen** auf **Windowskomponenten hinzufügen/entfernen**.
4. Wählen Sie in dem Assistenten **Windowskomponenten Internet Information Services (IIS)** aus und klicken Sie auf **Details**.
5. Überprüfen Sie in dem Fenster **Internet Information Services (IIS)** ob das Kontrollkästchen **SMTP-Dienst** ausgewählt ist. Wenn ja, so ist der SMTP-Dienst installiert.

Wenn der SMTP-Dienst installiert ist, wählen Sie eine der folgenden Lösungen:

Lösung 1: Deaktivieren Sie den SMTP-Dienst, oder setzen Sie ihn auf manuellen Start

Mit dieser Lösung können Sie den Aufzeichnungsserver starten, ohne jedes Mal den SMTP-Dienst anhalten zu müssen:

1. Wählen Sie aus dem Windows **Startmenü Systemsteuerung** aus.
2. Klicken Sie in der **Systemsteuerung** doppelt auf **Administrative Werkzeuge**.
3. Klicken Sie in **Administrative Werkzeuge** doppelt auf **Dienste**.

4. Klicken Sie in den **Diensten** doppelt auf **Simple Mail Transfer Protocol (SMTP)**.
5. Klicken Sie in dem Fenster **Eigenschaften von SMTP** auf **Anhalten**, und stellen Sie dann den **Starttyp** entweder auf **Manuell** oder auf **deaktiviert**.

   Wenn der SMTP-Dienst auf **Manuell** steht, kann er von dem Fenster **Dienste** aus manuell gesteuert werden, oder von einer Eingabeaufforderung aus mithilfe des Befehls *net start SMTPSVC*.
6. Klicken Sie auf **OK**.

Lösung 2: Entfernen des SMTP-Dienstes

Das Entfernen des SMTP-Dienstes kann Auswirkungen auf andere Anwendungen haben, die den SMTP-Dienst nutzen.

1. Wählen Sie aus dem Windows **Startmenü Systemsteuerung** aus.
2. Klicken Sie in der **Systemsteuerung** doppelt auf **Programme hinzufügen oder entfernen**.
3. Klicken Sie links in dem Fenster **Programme hinzufügen oder entfernen** auf **Windowskomponenten hinzufügen/entfernen**.
4. Wählen Sie in dem Assistenten **Windowskomponenten Internet Information Services (IIS)** aus und klicken Sie auf **Details**.
5. Deaktivieren Sie in dem Fenster **Internet Information Services (IIS)** das Kontrollkästchen **SMTP-Dienst**.
6. Klicken Sie auf **OK**, **Weiter**, und **Fertigstellen**.

Problem: Aufzeichnungsserver geht beim Umschalten auf Managementserver Clusterknoten offline

Wenn Sie einen Microsoft-Cluster für Managementserver-Redundanz einrichten, so können die Aufzeichnungsserver oder Aufzeichnungsservers beim Umschalten von Managementserver zwischen den Clusterknoten offline gehen.

Um dies zu korrigieren, ändern Sie die folgenden Konfigurationsseinstellungen:

An den Managementserver Knoten:

- In C:\ProgramData\Milestone\XProtectManagementserver**ServerConfig.xml**:

  ```
  <AuthorizationServerUri>http://ClusterRoleAddress/IDP</AuthorizationServerUri>
  ```
- In C:\Program Files\Milestone\XProtectManagementserver\IIS\IDP**appsettings.json**:

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

Überprüfen Sie an den Aufzeichnungsservers ob die Adresse des Autorisierungsservers auch auf der Adresse der Clusterrolle steht:

In C:\ProgramData\Milestone\XProtectAufzeichnungsserver**RecorderConfig.xml**:

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

Upgrade

Upgrade (Erklärung)

Wenn Sie ein Upgrade durchführen, werden alle gegenwärtig auf dem Computer installierten Komponenten mit aktualisiert. Während eines Upgrades ist es nicht möglich, installierte Komponenten zu entfernen. Wenn Sie installierte Komponenten entfernen möchten, verwenden Sie hierfür vor oder nach einem Upgrade die Windows-Funktion **Programme hinzufügen und entfernen**. Bei einem Upgrade werden alle Komponenten, mit Ausnahme der Management-Server-Datenbank, automatisch deinstalliert und ersetzt. Dies schließt die Treiber des Treiberpakets ein.

Die Management-Server-Datenbank enthält alle Systemkonfigurationen (Aufzeichnungsserver-Konfigurationen, Kamerakonfigurationen, Regeln usw.). So lange Sie die Management-Server-Datenbank nicht deinstallieren, müssen Sie Ihre Systemkonfiguration nicht neu konfigurieren, auch wenn Sie vermutlich einige der neuen Funktionen in der neuen Version konfigurieren wollen.

Die Abwärtskompatibilität mit Aufzeichnungsservern von Versionen von XProtect vor der derzeitgen Version ist begrenzt. Auf solchen älteren Aufzeichnungsservern können Sie trotzdem Aufnahmen abrufen, um jedoch ihre Konfiguration zu ändern, müssen sie von derselben Version sein, wie die aktuelle. Milestone empfiehlt ein Upgrade aller Aufzeichnungsserver in Ihrem System.

Wenn Sie ein Upgrade durchführen, das auch Ihre Aufzeichnungsserver umfasst, werden Sie gefragt, ob Sie die Video-Gerätetreiber aktualisieren oder beibehalten wollen. Wenn Sie eine Aktualisierung durchführen, kann es nach dem Neustart Ihres Systems einige Minuten dauern, bis Ihre Geräte den Kontakt zu den neuen Video-Gerätetreibern hergestellt haben. Der Grund dafür sind eine Vielzahl interner Kontrollen der neu installierten Treiber.

Wenn Sie die Version 2017 R3 oder früher zur Version 2018 R1 oder später aktualisieren, und wenn Ihr System ältere Kameras hat, müssen Sie das Gerätepaket mit Stammtreibern manuell von unserer Download-Website (https://www.milestonesys.com/downloads/) herunterladen. Für Angaben darüber, ob Ihre Kameras Treiber aus dem Stammgerätepaket nutzen, besuchen Sie diese Seite auf unserer Website (https://www.milestonesys.com/community/business-partner-tools/device-packs/).

Wenn Sie von Version 2018 R1 oder früher auf Version 2018 R2 oder höher aktualisieren, ist es wichtig, dass Sie vor dem Upgrade alle Aufzeichnungsserver in Ihrem System mit einem Sicherheitspatch aktualisieren. Eine Aktualisierung ohne den Sicherheitspatch führt dazu, dass die Aufzeichnungsserver versagen.

Die Anleitung zum Installieren des Sicherheitspatches auf Ihren Aufzeichnungsservern finden Sie auf unserer Website https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/.

Wenn alle Aufzeichnungsserver in Ihrem System auf die Version 2019 R2 oder später aktualisiert wurden,empfiehlt Milestone Ihnen, in der Konfigurationsdatei für den Managementserver UseRemoting auf 'False' zu setzen. Weitere Informationen dazu, wie Sie Ihre XProtect VMS Installationen gegen Cyber-Angriffe sichern finden Sie im Leitfaden zur Sicherheitsoptimierung.

Wenn Sie die Verbindung zwischen dem Management Server und den Aufzeichnungsserver verschlüsseln möchten, müssen alle Aufzeichnungsserver mindestens auf 2019 R2 erweitert werden.

Upgrade-Anforderungen

- Halten Sie Ihre Softwarelizenzdatei (.lic) bereit (siehe Lizenzen (Erklärung) auf Seite 50):
  - **Service-Pack Upgrade**: Der Assistent könnte Sie während der Installation des Management-Servers zur Spezifikation des Standortes Ihrer Software-Lizenzdatei auffordern. Sie können sowohl die Software-Lizenzdatei verwenden, die Sie nach dem Kauf Ihres Systems bekommen haben (oder neuestem Upgrade) als auch die aktivierte Software-Lizenzdatei, die Sie nach Ihrer letzten Lizenzaktivierung erhalten haben
  - **Versionsupgrade**: Nach dem Kauf der neuen Version, erhalten Sie eine neue Software-Lizenzdatei. Der Assistent fordert Sie während der Installation des Management-Servers zur Spezifikation des Standortes Ihrer neuen Software-Lizenzdatei auf

  Das System überprüft Ihre Software-Lizenzdatei, bevor Sie fortfahren können. Bereits hinzugefügte und andere Geräte, die eine Lizenz benötigen, beginnen dann eine Probeversion. Sollten Sie die Automatische Lizenzaktivierung (siehe Automatische Lizenzaktivierung aktivieren auf Seite 144) nicht eingeschaltet haben, denken Sie daran, Ihre Lizenzen manuell zu aktivieren, bevor die Karenzfrist abläuft. Sollten Sie keine Software-Lizenzdatei besitzen, kontaktieren Sie bitte Ihren XProtect-Reseller.
- Halten Sie Ihre **neue Produktversion** der Software bereit. Sie können sie von der Downloadseite auf der Website Milestone herunterladen.

- Achten Sie darauf, ein Backup der Systemkonfiguration durchzuführen (siehe Sicherung und Wiederherstellung einer Systemkonfiguration (Erklärung) auf Seite 494)

  Der Management-Server speichert die Systemkonfiguration in einer SQL-Datenbank. Die SQL-Datenbank kann sich in einer SQL Server auf dem Computer mit dem Management-Server selbst oder in einem SQL Server im Netzwerk befinden.

  Wenn Sie eine SQL-Datenbank in einem SQL Server in Ihrem Netzwerk verwenden, muss der Management-Server auf dem SQL Server über Administratorrechte verfügen, wann immer Sie die SQL-Datenbank erstellen, verschieben oder aktualisieren wollen. Für die regelmäßige Verwendung und für die Wartung der SQL-Datenbank muss der Management-Server lediglich der Besitzer der SQL-Datenbank sein.

- Falls Sie vorhaben, die Verschlüsselung während der Installation zu aktivieren, müssen Sie die entsprechenden Zertifikate auf allen entsprechenden Computern installieren, und diese müssen ihm vertrauen. Weitere Informationen finden Sie unter Sichere Kommunikation (Erläuterung). auf Seite 69

Wenn Sie bereit zum Start des Upgrades sind, folgen Sie den dargelegten Schritten in Optimale Vorgehensweise beim Upgrade auf Seite 535.

Aktualisieren Sie XProtect VMS. damit Ihr System im FIPS 140-2-konformen Modus läuft

Ab der Version 2020 R3 ist XProtect VMS so konfiguriert, dass er im Betrieb ausschließlich die FIPS 140-2-zertifizierten Algorithmusinstanzen verwendet.

Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

> Für Systeme, die FIPS 140-2 erfüllen, mit Exports und archivierten Mediendatenbanken aus XProtect VMS-Versionen vor 2017 R3, die mithilfe von nicht FIPS-konformen Chiffren verschlüsselt sind, müssen die Daten an einem Ort archiviert werden, wo sie nach Aktivierung von FIPS weiterhin zugänglich sind.

Das folgende Verfahren beschreibt, was zur Konfiguration von XProtect VMS erforderlich ist, damit es im FIPS 140-2-konformen Modus läuft:

1. Deaktivieren Sie die Windows-FIPS-Sicherheitsrichtlinie auf allen Computern, die zum VMS gehören, einschließlich des Computers, auf dem der SQL-Server gehosted wird.

   Während das Upgrades können Sie XProtect VMS nicht installieren, wenn FIPS auf dem Windows-Betriebssystem aktiviert ist.

2. Achten Sie darauf, dass eigenständige Dritt-Integrationen auf einem FIPS-fähigen Windows-Betriebssystem laufen können.

   Entspricht eine eigenständige Integration nicht FIPS 140-2, so kann sie nicht ausgeführt werden, wenn Sie das Windows-Betriebssystem so einrichten, dass es im FIPS-Modus läuft.

   Gehen Sie wie folgt vor, um dies zu vermeiden:

   - Führen Sie eine Bestandsaufnahme aller Ihrer eigenständigen Integrationen durch, um zu XProtect VMS
   - Wenden Sie sich an die Anbieter dieser Integrationen und fragen Sie sie, ob die Integrationen FIPS 140-2-konform sind
   - Setzen Sie die FIPS 140-2-konformen eigenständigen Integrationen ein

3. Vergewissern Sie sich, dass die Treiber, damit die Kommunikation mit den Geräten, FIPS 140-2-konform sind.

   XProtect VMS wird garantiert und kann die FIPS 140-2-konforme Betriebsart erzwingen, wenn die folgenden Kriterien erfüllt sind:

   - Die Geräte verwenden ausschließlich geprüfte Treiber für die Verbindung mit XProtect VMS

     Weitere Informationen zu Treibern, die Compliance gewährleisten und erzwingen können, finden Sie im Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

     > Die Treibermodule können die Einhaltung von FIPS 140-2 durch eine Verbindung über HTTP nicht garantieren. Die Verbindung mag konform sein, es gibt jedoch keine Garantie dafür, dass sie tatsächlich konform ist.

   - Die Geräte verwenden das Device Pack in der Version 11.1 oder höher

     Die Treiber aus den Legacy Driver Device Packs können keine FIPS 140-2-konforme Verbindung garantieren.

   - Die Geräte werden über HTTPS verbunden, und entweder über Secure Real-Time Transport Protocol (SRTP) oder Real Time Streaming Protocol (RTSP) über HTTPS für Video-Stream
   - Auf dem Computer, auf dem der Aufzeichnungsserver läuft, läuft das Betriebssystem Windows mit aktiviertem FIPS-Modus

4. Achten Sie darauf, dass die Daten in den Mediendatenbanken mithilfe von FIPS 140-2-konformen Chiffren verschlüsselt werden.

   Dies erfolgt durch Ausführen des Upgrade-Tools für Mediendatenbanken. Detaillierte Informationen dazu, wie Sie Ihren XProtect VMS so konfigurieren, dass er im FIPS 140-2-konformen Modus läuft, s. den Abschnitt FIPS 140-2-Compliance im Leitfaden zur Sicherheitsoptimierung.

5. Bevor Sie im Betriebssystem Windows FIPS aktivieren, und nachdem Sie Ihr XProtect VMS-System konfiguriert und sich vergewissert haben, dass alle Komponenten und Geräte in einer FIPS-fähigen Umgebung laufen können, aktualisieren Sie die Passwörter für Ihre vorhandene Hardware im XProtect Management Client.

   Klicken Sie dazu im Management Client, vom ausgewählten Aufzeichnungsserver in dem Knoten **Aufzeichnungsserver** aus mit der rechten Maustaste und wählen Sie **Hardware hinzufügen...**. Klicken Sie sich durch den Assistenten **Hardware hinzufügen**. Damit werden alle aktuellen Anmeldedaten aktualisiert und so verschlüsselt, dass sie FIPS erfüllen.

Sie können FIPS erst aktivieren, wenn Sie das gesamte VMS aktualisiert haben, einschließlich aller Clients.

Optimale Vorgehensweise beim Upgrade

Informieren Sie sich vor Beginn des eigentlichen Upgrades über die Anforderungen für ein Upgrade (siehe Upgrade-Anforderungen auf Seite 532), einschließlich eines Backups der SQL-Datenbank.

> Die Gerätetreiber sind jetzt auf zwei Gerätepakete aufgeteilt: das reguläre Gerätepaket mit neueren Treibern und ein Stammgerätepaket mit älteren Treibern. Das reguläre Gerätepaket wird bei einem Update oder Upgrade ständig automatisch installiert. Wenn Sie ältere Kameras haben, die Gerätetreiber aus dem Stammgerätepaket nutzen, und Sie haben noch kein Stammgerätepaket installiert, installiert das System nicht automatisch das Stammgerätepaket.

> Wenn Ihr System ältere Kameras hat, empfiehlt Milestone, auf dieser Seite (https://www.milestonesys.com/community/business-partner-tools/device-packs/) zu prüfen, ob Sie Kameratreiber aus dem Stammgerätepaket nutzen. Um Herauszufinden, ob Sie das Stammpaket bereits installiert haben, schauen Sie in die XProtect Systemordner. Wenn Sie das Stammgerätepaket herunterladen müssen, gehen Sie auf die Download-Seite (https://www.milestonesys.com/downloads/).

Wenn Sie ein **Einzelcomputer**-System verwenden, können Sie die neue Software über die bereits vorhandene Installation installieren.

In einem Milestone Interconnect oder Milestone Federated Architecture System müssen Sie zunächst die zentrale Seite aktualisieren und danach die entfernten Seiten.

Führen Sie in einem verteilten System die Aktualisierung in der folgenden Reihenfolge durch:

1. Führen Sie ein Upgrade des Management-Servers mit der Option **Benutzerdefiniert** im Installationsprogramm durch (siehe Systeminstallation - Benutzerdefiniert auf Seite 88).
    1. Auf der Seite des Assistenten, auf der Sie die Komponenten auswählen können, sind bereits alle Komponenten des Managementservers ausgewählt.
    2. Geben Sie die SQL Server und die Datenbank an. Entscheiden Sie, ob die SQL-Datenbank, die Sie bereits verwenden, beibehalten werden und ob die vorhandenen Daten in der Datenbank verbleiben sollen.

    > Wenn Sie die Installation starten, verlieren Sie Funktionen des ausfallsicheren Aufzeichnungsservers (siehe Failover-Aufzeichnungsserver (Erklärung) auf Seite 184).

    > Wenn Sie die Verschlüsselung auf dem Managementserver aktivieren, sind die Aufzeichnungsserver solange offline, bis ein Upgrade für diese durchgeführt wurde und Sie die Verschlüsselung zum Managementserver aktiviert haben (siehe Vor dem Start der Installation auf Seite 59).

2. Aktualisierung des Failover-Aufzeichnungsservers. Installieren Sie von der Downloadseite ihres Management-Server (die von der Download Manager kontrolliert wird), Aufzeichnungsserver.

    > Wenn Sie vorhaben, die Verschlüsselung auf den Failover-Aufzeichnungsservern zu aktivieren, und Sie die Failoverfunktion erhalten möchten, so aktualisieren Sie die Failover-Aufzeichnungsserver ohne Verschlüsselung und aktivieren Sie diese, nachdem Sie die Aufzeichnungsserver aktualisiert haben.

    Ab diesem Zeitpunkt besteht wieder volle Funktionalität des Failover-Servers.

3. Wenn Sie vorhaben, die Verschlüsselung auf den Aufzeichnungsservern oder den Failover-Aufzeichnungsservern zu den Clients zu aktivieren, und es wichtig ist, dass die Clients während der Aktualisierung Daten abrufen können, so aktualisieren Sie alle Clients und Dienste, die Datenstreams von den Aufzeichnungsservern abrufen, bevor Sie die Aufzeichnungsserver aktualisieren. Diese Clients und Dienste sind:
    - XProtect Smart Client
    - Management Client
    - Managementserver
    - XProtect Mobile-Server
    - XProtect Event Server

- DLNA Server Manager
- Milestone Open Network Bridge
- Seiten, die Datenstreams vom Aufzeichnungsserver abrufen durch Milestone Interconnect
- Manche der MIP-SDK-Integrationen von Drittanbietern

4. Aktualisieren Sie den Aufzeichnungsserver. Sie können Aufnahmeserver mit Hilfe des Installationsassistenten installieren (siehe Installation neuer XProtect-Komponenten auf Seite 93) oder still (siehe Installation neuer XProtect-Komponenten auf Seite 93). Der Vorteil einer automatischen Installation ist die Möglichkeit zur Ferninstallation.

   > ⚠ Wenn Sie die Verschlüsselung aktivieren, und dem ausgewählten Serverauthenfizierungszertifikat wird nicht auf allen Computern vertraut, so verlieren diese die Verbindung. Weitere Informationen finden Sie unter Vor dem Start der Installation auf Seite 59.

Folgen Sie diesen Schritten an den weiteren Standorten in Ihrem System.

Upgrade in einem Arbeitsgruppen-Setup

Wenn Sie kein Domänen-Setup, sondern ein Arbeitsgruppen-Setup verwenden, müssen Sie für ein Upgrade folgende Schritte ausführen:

1. Erstellen Sie auf dem Aufzeichnungsserver einen lokalen Windows-Benutzer.
2. Suchen Sie in der Windows-**Systemsteuerung** nach dem **Data Collector-Dienst**. Klicken Sie mit der rechten Maustaste darauf und wählen Sie **Eigenschaften** und dann die Registerkarte **Anmelden** aus. Richten Sie den Data Collector-Dienst so ein, dass er als lokaler Windows-Benutzer, den Sie gerade auf dem Aufzeichnungsserver erstellt haben, läuft.
3. Erstellen Sie auf dem Management-Server denselben lokalen Windows-Benutzer (mit demselben Benutzernamen und demselben Passwort).
4. Fügen Sie im Management Client diesen lokalen Windows-Benutzer zur Gruppe des **Administrators** hinzu.

Zur Installation mit Arbeitsgruppen, siehe Installation für Arbeitsgruppen auf Seite 103.

Upgrade in einem Cluster

Stellen Sie sicher, dass Sie ein Backup der Datenbank durchführen, bevor Sie den Cluster aktualisieren.

1. Deinstallieren Sie den Managementserver-Service auf allen Management-Servern im Cluster.
2. Deinstallieren Sie den Management-Server auf allen Servern im Cluster.
3. Verwenden Sie das Verfahren zur Installation mehrerer Managementserver in einem Cluster, wie unter "In einem Cluster installieren" beschrieben. Siehe Installation eines neuen XProtect-Systems auf Seite 78.

Achten Sie bei der Installation darauf, den vorhandenen SQL Server und die vorhandene SQL-Datenbank zu verwenden, in der die Systemkonfiguration aktuell gespeichert ist. Die Systemkonfiguration wird automatisch aktualisiert.

helpfeedback@milestone.dk

Über Milestone

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