

Senstar Symphony Benutzerhandbuch

Version 8.12

Inhaltsverzeichnis

Erste Schritte	7
Operatoren	7
Administratoren	9
Server	12
Anmelden	13
Geräte	14
Kameras	14
Browser	68
Vorlagen	69
Hardware	71
Integrationen	72
Zugangskontrollgerät	81
Gerätebaum	82
Sequenzen	84
Sicherheit	86
Benutzer	86
Gruppen	90
Sicherheitsprofile	91
Benutzeranmeldungen	102
Security Settings	103
Active-Directory-Integration	103
Sicherheitsauthentifizierung	104
Wasserzeichen	105
Regeln	105
Metadaten	106
Regel erstellen	107
Regel bearbeiten	108
Regel löschen	108
Ereignisse	108
Aktionssätze	120
Zeitpläne	122
Lizenzen	123
Einstellungen	124
Server	124
Allgemeine Einstellungen	130
Cloud-Dienste	138
Summen	139
Wartung	142

Backup & Wiederherstellen	143
Lageplan	146
Geschützte Aufnahmen	147
Serververwaltung	149
CPU-Auslastung prüfen	151
Dienste verwalten	151
Windows Client	153
Kennwort ändern	153
Benutzeroberfläche	153
Gerätebaum	154
Serverliste	161
Ansichts-Panels	162
Lagepläne	173
Senstar Symphony Messenger	180
Sequenzen	181
Zeitleiste	182
Anpassungen der Oberfläche	184
Mehrere Monitore	184
Video verwalten	185
Videoexport	185
Sperrzeiten	188
Lesezeichen	189
Visuelle Verfolgung	189
Aufnahmen schützen	190
Aufgezeichnetes Video löschen	191
Alarme verwalten	192
Alarmkonsole	194
Client-Optionen	197
Einstellungen	198
Kameraaktivität anzeigen	198
Symbolleiste anpassen	198
Zeitleisten-Farben ändern	198
Starteinstellungen	199
Anzeigeeinstellungen	199
Alarmeinstellungen	201
Videoeinstellungen	202
Anpassungseinstellungen	204
Toneinstellungen	206
Regionale Einstellungen	207

Globale Einstellungen	208
Sperrereinstellungen	208
Update-Einstellungen	209
Erweiterte Einstellungen	210
Videowand	211
Client registrieren	211
Videowand erstellen	212
Serverkonfiguration	212
Mit einem Server verbinden	212
Verbindung zu einem Server trennen	213
Informationen über den Server abrufen	213
Manueller Konfigurationseditor	213
Windows-Authentifizierung	216
Berichte und Protokolle	216
Ereignisse anzeigen	217
Alarmbericht	217
Alarmstatistikbericht	219
Gesichtserkennungsbericht	220
Heat-Map-Bildbericht	222
Bericht für automatische Kennzeichenerkennung	224
Objektzählungsbericht	225
Bericht für Objektzählung über eine Linie	226
Bericht für Personenzählung mit Überkopf-Kameras	228
Objektstatistikbericht	229
Anhang	230
Open-Befehl	231
Protokolldateien anzeigen	231
Single Sign-On deaktivieren	231
Timeout für SSL-Zertifikat konfigurieren	232
Web Client	233
Am Web Client anmelden	233
Überwachung	233
Eine Kamera anzeigen	234
Berichte	234
Bericht erstellen	235
Player	237
Player installieren	237
Wasserzeichenprüfung aktivieren	237
Eine Videodatei abspielen	237
Anhang	239
Versionshinweise	239

Glossar 243

Netzwerk-Ports 246

Rechtliche Informationen 247

 Senstar Symphony Drittanbieter-Hinweise 247

Die Senstar Symphony Common Operating Plattform ist eine intelligente, modulare Plattform für Videoüberwachung, Sicherheitsmanagement und Zutrittskontrolle.



Dieses Dokument wurde maschinell übersetzt. Bei Unklarheiten oder Abweichungen zwischen dieser übersetzten Version und der englischen Version ist die englische Version maßgeblich.

Erste Schritte

Die Online-Hilfe enthält Einstiegsseiten für Benutzer, die sich an deren typischer Rolle orientieren.

Meine Rolle	Typische Aufgaben
Bediener	Live-Video anzeigen, auf Alarme reagieren, in aufgezeichnetem Material suchen, Berichte erstellen
Administrator	Server einrichten, Kameras und Geräte hinzufügen, Regeln konfigurieren, Benutzer verwalten, Backups planen

Inhalt

Abschnitt	Beschreibung
Erste Schritte	Produktüberblick und das Zusammenspiel der Komponenten.
Server	Eine Senstar Symphony-Bereitstellung konfigurieren: Geräte, Sicherheit, Regeln, Standorte und Einstellungen.
Windows Client	Mit dem Windows Client Kameras überwachen, Videos verwalten, Berichte erstellen und auf Alarme reagieren.
Web Client	Funktionalität ähnlich dem Windows Client, jedoch im Browser.
Player	Offline-Anwendung zum Anzeigen exportierter Videodateien.
Anhang	Versionshinweise, Verwendung der Netzwerk-Ports, Glossar und rechtliche Hinweise.

Erste Schritte

Senstar Symphony bietet eine Common Operating Plattform für intelligente Videoüberwachung, Videoanalyse und Sicherheitsmanagement.

Senstar Symphony läuft auf gängiger IT-Hardware, unterstützt IP-Kameras von Hunderten von Herstellern, bietet eine funktionsreiche, leicht bedienbare Oberfläche und enthält IT-freundliche Funktionen, die die Administration vereinfachen. Senstar Symphony kann auf einem einzelnen Computer oder in einer Serverfarm aus mehreren Computern betrieben werden.

Senstar Symphony besteht aus folgenden Komponenten:

- **Server** — Über die Konfigurationsoberfläche des Server konfigurieren Sie Senstar Symphony. Der Server zeichnet Video auf, betreibt die Regel-Engine und speichert die Alarm- und Ereignishistorie.
- **Windows Client** — Eine Windows-Desktop-Anwendung zur Bedienung der mit dem Server verbundenen Kameras. Damit sehen Sie Live-Video an, spielen Aufzeichnungen ab, reagieren auf Alarme und führen Berichte aus.
- **Web Client** — Bietet Funktionen ähnlich dem Windows Client, läuft jedoch im Webbrowser und benötigt keine Software-Installation.
- **Player** — Spielt Videodateien ab, die Sie aus dem Windows Client exportiert haben.

Gängige Rollen

Meine Rolle	Häufige Aufgaben
Operator	Live-Video ansehen, auf Alarme reagieren, in Aufzeichnungen suchen, Berichte ausführen
Administrator	Server einrichten, Kameras und Geräte hinzufügen, Regeln konfigurieren, Benutzer verwalten, Backups planen

Operatoren

Bediener verwenden den Windows Client (und optional den Web Client), um Live- und aufgezeichnete Videos zu betrachten, auf Alarme zu reagieren, Vorfälle zu untersuchen und Berichte zu erstellen. Auf dieser Seite finden Sie schnell die passende Vorgehensweise; verwenden Sie [Benutzeroberfläche](#), wenn Sie sich über bestimmte Steuerelemente oder Funktionen informieren möchten.



Einige Vorgänge erfordern Berechtigungen, die Ihr Standortadministrator über [Sicherheitsprofile](#) vergibt. Wenn ein Menü oder eine Schaltfläche nicht sichtbar ist, verfügt Ihr Konto möglicherweise nicht über die entsprechende Berechtigung — wenden Sie sich an Ihren Administrator.

Grundlagen

- [Mit einem Server verbinden](#) — Beim Windows Client anmelden.
- [Benutzeroberfläche](#) — Funktionen der einzelnen Bildschirmbereiche kennenlernen.
- [Kameraansicht laden](#) — Ein gespeichertes Kamera-Layout wiederherstellen.
- [Alarmkonsole](#) — Die Konsole für die Alarmbehandlung der aktuellen Schicht öffnen.
- [Kennwort ändern](#) — Falls die Standortrichtlinie eine regelmäßige Änderung verlangt.

- Von einem Server trennen — Von der Anwendung abmelden.

Kameras und Sensoren überwachen

- Kamera anzeigen — Einen Live-Videostream in einem Anzeigebereich öffnen.
- Lageplan anzeigen — Einen Standortplan mit Geräte- und Alarmindikatoren anzeigen.
- Sequenzen — Eine Reihe von Kameras automatisch durchschalten.
- PTZ-Steuerung — PTZ-Kameras schwenken, neigen und zoomen.
- Kamera-Zeitleiste anzeigen — Sehen, wann aufgezeichnete Aktivitäten und Ereignisse stattgefunden haben.

Auf Alarme reagieren

Den vollständigen Ablauf finden Sie unter [Alarme verwalten](#).

- Alarme anzeigen — Auf Bearbeitung wartende Alarme anzeigen.
- Alarm bestätigen — Verantwortung für einen Alarm übernehmen und ihn klassifizieren (echt, echt mit Handlungsbedarf, falsch).
- Alarm teilen — Alarm eskalieren, indem Sie ihn an einen anderen Bediener weiterleiten.
- Alarme abrufen — Ältere Alarme zur Überprüfung erneut sichten.

Einen Vorfall untersuchen

- Video nach Datum anzeigen — Zu aufgezeichnetem Material zu einem bestimmten Zeitpunkt springen.
- Suchen — Clips nach Objektklasse (Person, Fahrzeug) und Verhalten (Bewegung, Herumlungern) finden.
- Sofortwiedergabe — Kürzlich erfasstes Live-Video zurückspulen, ohne den Anzeigebereich zu verlassen.
- Lesezeichen — Stellen in aufgezeichnetem Video markieren, damit Sie oder andere sie später wiederfinden.
- Aufnahmen schützen — Verhindern, dass ein Abschnitt von aufgezeichnetem Video durch die Aufbewahrungseinstellungen gelöscht wird.
- Visuelle Verfolgung — Eine Zielperson anhand vorkonfigurierter Verknüpfungen über mehrere Kameras hinweg verfolgen.
- Video exportieren — Ein Video als Datei zur Weitergabe speichern.

Berichte erstellen

Eine vollständige Übersicht der Berichte finden Sie unter [Berichte und Protokolle](#).

- Alarmbericht
- Alarmstatistikbericht
- Gesichtserkennungsbericht
- Heatmap-Bildbericht
- Objektzählungsbericht

- Ereignisse anzeigen (Roh-Ereignisprotokoll).

Den Windows Client anpassen

- Kameraansicht speichern — Das aktuelle Layout sichern.
- Einstellungen anpassen — Festlegen, was in der Symbolleiste und den Statusbereichen erscheint.
- Anzeigeeinstellungen — Die Videodarstellung anpassen.
- Toneinstellungen — Alarmtöne und Benachrichtigungssignale steuern.
- Regionaleinstellungen — Datums-, Uhrzeit- und Spracheinstellungen festlegen.

Administratoren

Administratoren konfigurieren den Server: Sie fügen Geräte hinzu, legen fest, wer was sehen und tun darf, erstellen die Regeln, die Ereignisse in Alarme und Aktionen umwandeln, und sorgen dafür, dass das System dauerhaft fehlerfrei läuft. Die folgenden Seiten sind nach dem typischen Ablauf für einen neuen Administrator gegliedert — Bereitstellung planen, einrichten und anschließend betreiben — und nicht nach dem Aufbau der Konfigurationsoberfläche. Eine seitenweise Darstellung der Konfigurationsoberfläche finden Sie unter [Server](#).

Bereitstellung planen

Bevor Sie etwas zum System hinzufügen, treffen Sie folgende Entscheidungen:

- **Standortaufbau** — wie viele Kameras, wo sie installiert werden, was sie erfassen müssen und welche Ereignisse relevant sind. Dies bestimmt später die Regel- und Analyseentscheidungen.
- **Speicher** — die Aufbewahrungsrichtlinie für Videoaufzeichnungen (Anzahl Tage, die das Material vorgehalten wird) bestimmt die Festplattengröße. Siehe [Videospeicher für eine Serverfarm](#).
- **Benutzerrollen** — welche Personen das System bedienen und welche es administrieren, und ob Sie Rollen wie Nur-Anzeige, Vollbediener, Ermittler oder Standortadministrator benötigen. Siehe [Sicherheitsprofile](#).
- **Netzwerk** — die [Netzwerk-Ports](#), die zwischen Server, Clients und Kameras geöffnet sein müssen.
- **Backups** — wo Backups gespeichert werden und wie sie in Ihren Notfallwiederherstellungsplan passen. Siehe [Backups konfigurieren](#).

Erstmalige Einrichtung

Der Ablauf für die erstmalige Einrichtung eines neuen Server:

Schritt	Seite
Bei der Konfigurationsoberfläche anmelden	Anmeldung
Lizenz anwenden	Lizenzen
Erste Kamera hinzufügen und Video überprüfen	Kamera hinzufügen
Aufbewahrungsrichtlinie für den Standort festlegen	Videospeicher für eine Serverfarm
Benutzer und Gruppen hinzufügen	Benutzer hinzufügen · Gruppe hinzufügen

Schritt	Seite
Sicherheitsprofile für jede Rolle erstellen	Sicherheitsprofil hinzufügen
Erste Regel erstellen (Ereignis + Aktionssatz + Zeitplan)	Regeln · Regel erstellen
Backups konfigurieren	Backups konfigurieren

Geräteverwaltung

- **Übersicht der Geräte** — was die Konfigurationsoberfläche als „Geräte“ bezeichnet und wie die Untertypen zusammenhängen.
- **Kameras** — Kameras hinzufügen, importieren, exportieren und bearbeiten.
- **Videoanalyse** — kameraspezifische Analysefunktionen wie Bewegungserkennung, Personenverfolgung und Gesichtserkennung aktivieren.
- **Hardware · Integrationen · Zugangskontrollgeräte** — Hardware außer Kameras.
- **Vorlagen** — eine gespeicherte Konfiguration auf viele Kameras gleichzeitig anwenden.
- **Gerätebaum** — wie Geräte im Windows Client angezeigt werden organisieren.

Sicherheit und Zugriffskontrolle

- **Benutzer** — Benutzer hinzufügen, kopieren, gruppieren und deaktivieren.
- **Gruppen** — Container für Benutzer; Berechtigungen werden Gruppen, nicht einzelnen Benutzern zugewiesen.
- **Sicherheitsprofile** — wiederverwendbare Berechtigungspakete (siehe Rollenvorlagen unter **Benutzerberechtigungen**).
- **Active Directory** — Integration mit einem vorhandenen Verzeichnisdienst, statt separate Konten zu pflegen.
- **Sicherheitsauthentifizierung** — wie Anmeldedaten gespeichert und überprüft werden.
- **Benutzeranmeldungen** — aktive und vergangene Sitzungen einsehen.

Regel-Engine

Regeln wandeln Ereignisse in Aktionen um. Eine Regel besteht aus drei Teilen: einem **Ereignis** (dem Auslöser), einem **Aktionssatz** (was passiert) und einem **Zeitplan** (wann die Regel aktiv ist). Siehe **Regeln** für das Modell und **Regel erstellen** für die Vorgehensweise.

Berichte, Überwachung und Wartung

- **CPU-Auslastung prüfen** — überlastete Server erkennen.
- **Dienste verwalten** — die Hintergrunddienste steuern.
- **Cloud-Dienste** — Zustandsüberwachung, Fernverwaltung und Cloud-Backup.
- **Wartung** — automatische Updates, Server-Update-Prüfungen und Client-Update-Richtlinie.
- **Geschützte Aufnahmen** — das Video überprüfen, das Benutzer vor dem Löschen geschützt haben, und den **Schutz aufheben** für nicht mehr benötigtes Video.
- **Backup & Wiederherstellen** — geplante Backups und Wiederherstellungswege.

Konzepte

Grundlagenthemen, die jeder Administrator einmal lesen sollte:

- Regeln, Ereignisse, Aktionssätze und Zeitpläne
- Berechtigungsmodell: Benutzer → Gruppen → Profile
- Pipeline der Videoanalyse
- Backup & Wiederherstellen

Server

Der Server ist der Kern einer Senstar Symphony-Bereitstellung. Er zeichnet Videos der angeschlossenen Kameras auf, betreibt die Regel-Engine, die Ereignisse in Alarme und Aktionen umwandelt, speichert die Alarm- und Ereignishistorie und setzt das Berechtigungsmodell durch, das festlegt, wer was sehen und tun darf.

Administratoren konfigurieren den Server über die Konfigurationsoberfläche des Server und den Senstar Symphony-Einrichtungsassistenten. Sie können die Konfigurationsoberfläche direkt im Browser oder aus dem Windows Client heraus öffnen. Der Einrichtungsassistent wird über das Startmenü auf dem Computer ausgeführt, der den Server hostet.

Eine aufgabenorientierte Übersicht zur Administration des Server finden Sie unter [Administratoren](#).

Erste Schritte

Wenn Sie einen neuen Server einrichten, arbeiten Sie diese Seiten in der angegebenen Reihenfolge durch:

Schritt	Thema
Bei der Konfigurationsoberfläche anmelden	Anmeldung
Lizenz anwenden	Lizenzen
Erste Kamera hinzufügen	Kamera hinzufügen
Videospeicher und Aufbewahrung für den Standort festlegen	Videospeicher für eine Serverfarm
Benutzer und Gruppen hinzufügen	Benutzer hinzufügen
Sicherheitsprofile für jede Rolle festlegen	Sicherheitsprofile
Erste Regel erstellen	Regel erstellen
Backups konfigurieren	Backups konfigurieren

Häufige Aufgaben

Aktion	Thema
Kamera hinzufügen	Kamera hinzufügen
Videoanalyse für eine Kamera aktivieren	Videoanalyse
Sensor zur Perimeter-Einbruchserkennung hinzufügen	Senstar Network Manager
Integration hinzufügen (Zutrittskontrolle, Drittanbieter-Sensoren)	Integrationshardware hinzufügen
Regel erstellen (Ereignis + Aktionssatz + Zeitplan)	Regel erstellen
Benutzer hinzufügen und Sicherheitsprofil zuweisen	Benutzer hinzufügen
Konfigurations-Backups planen	Backups konfigurieren

Aktion	Thema
Serverzustand prüfen	CPU-Auslastung prüfen

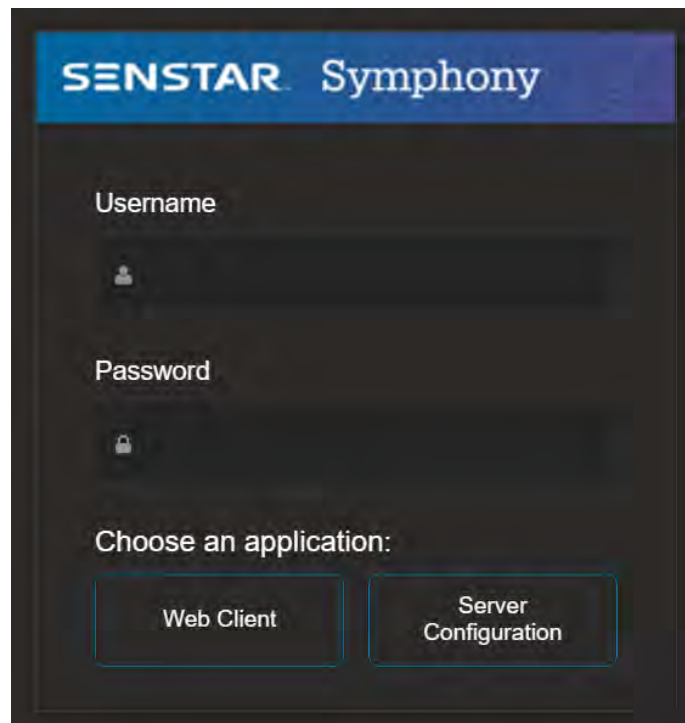
Referenzabschnitte

- [Geräte](#) — Kameras, Hardware, Integrationen, Zugangskontrollgeräte, Vorlagen.
- [Sicherheit](#) — Benutzer, Gruppen, Sicherheitsprofile, Benutzeranmeldungen, Authentifizierung.
- [Regeln](#) — Ereignisse, Aktionssätze, Zeitpläne.
- [Lizenzen](#)
- [Einstellungen](#) — Server, Allgemein, Cloud-Dienste, Summen, Wartung, Backup & Wiederherstellen, Lagepläne.
- [Serververwaltung](#) — CPU-Auslastung, Dienste.

Anmelden

Sie können die Konfigurationsoberfläche des Server auf verschiedene Weise öffnen:

- Webbrowser: Verwenden Sie die IP-Adresse des Servers.
- Windows Client: Klicken Sie in der Symbolleiste auf die Schaltfläche Server Configuration und wählen Sie Server Configuration.
- Web Client: Klicken Sie auf den Anmeldebildschirm auf die Schaltfläche Server Configuration oder in der Symbolleiste (nach der Anmeldung).



Anmeldung am Web Client

1. Navigieren Sie in einem Browser zur IP-Adresse des Web Client.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
3. Klicken Sie auf Server Configuration.

Server-Webanmeldung

1. Navigieren Sie in einem Browser zur IP-Adresse Ihres Server.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
3. Wählen Sie die Sprache der Benutzeroberfläche aus.
4. Klicken Sie auf Login.

Geräte

Senstar Symphony unterstützt Kameras, Einbruchmeldesensoren, digitale Eingangs-/Ausgangsgeräte und Zutrittskontrollgeräte. Konfigurieren Sie jeden Gerätetyp über die Konfigurationsoberfläche des Server; die meisten Administratoren beginnen mit Kameras und fügen anschließend die Sensoren, I/O- und Zutrittskontrollgeräte hinzu, die der Standort benötigt.

Abschnitt	Beschreibung
Kameras	Kameras der wichtigsten Hersteller importieren.
Browser	Konfigurieren Sie Webseiten, die in Anzeigepanels neben Videostreams und Lageplänen angezeigt werden.
Vorlagen	Wenden Sie eine gespeicherte Sammlung von Konfigurationseinstellungen auf Kameras an.
Hardware	Konfigurieren Sie Sensoren und I/O-Geräte, um Alarmer und andere Ereignisse auszulösen.
Integrationen	Verbinden Sie Sicherheitssysteme von Drittanbietern (Zutrittskontrolle, Perimetersensoren und dergleichen) mit dem Server.
Zugangskontrollgerät	Verwalten Sie Türsteuerungen und andere Zutrittskontrollgeräte.
Gerätebaum	Organisieren Sie, wie Kameras und Geräte im Windows Client angezeigt werden.
Sequenzen	Durchlaufen Sie mehrere Kamerastreams in einem Anzeigepanel und zeigen Sie Videos für eine festgelegte Zeit an.

Kameras

Der Server ist mit analogen und IP-Kameras einer Vielzahl von Herstellern kompatibel.

Der Server unterstützt die folgenden Standards:

- ONVIF Profile S
- ONVIF Profile G
- ONVIF Profile T

- Real Time Streaming Protocol (RTSP)

Der Server unterstützt die jeweils aktuellste offizielle Firmware für Kameras, wie sie von den Kameraherstellern bereitgestellt wird. Bei analogen Kameras verbinden Sie die Kamera über einen Videoencoder mit dem Server. Bei PTZ-Kameras müssen Sie den Steuerport für die Kamera konfigurieren und ihn in der Konfigurationsoberfläche des Server auswählen.

Auf der Seite Cameras in der Konfigurationsoberfläche des Server werden die mit dem Server verbundenen Kameras aufgelistet. Sie können die Liste filtern, indem Sie Werte in die Kopfzeile eingeben oder dort auswählen, und Sie können die Liste sortieren, indem Sie auf einen Spaltentitel klicken.

Kamera hinzufügen

Sie können eine Kamera manuell, automatisch oder als mobile Kamera zum Server hinzufügen.

Kamera manuell hinzufügen

Sie können Kameras in der Konfigurationsoberfläche des Server manuell zum Server hinzufügen.

Um eine Kamera über RTSP hinzuzufügen, geben Sie die RTSP-URL im Feld Address ein und wählen Sie in der Liste Driver den Eintrag RTSP URL aus.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Klicken Sie auf Add Cameras.
3. Klicken Sie auf Add Camera Manually.
4. Geben Sie im Feld Address die IP-Adresse der Kamera ein.
5. Wählen Sie in der Liste Driver den Hersteller der Kamera aus.
6. Geben Sie den Benutzernamen und das Kennwort für die Kamera ein.
7. Klicken Sie auf Connect oder Add without connecting.

Kamera automatisch hinzufügen

Der Server kann Kameras im selben Netzwerk automatisch erkennen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Klicken Sie auf Add Cameras.
3. Klicken Sie auf Begin Automatic Discovery.
4. Geben Sie im Fenster Credentials Required den Benutzernamen und das Kennwort für die Kamera ein und klicken Sie auf Connect.
5. Wählen Sie die Kamera aus und klicken Sie auf Next.
6. Geben Sie im Feld Camera Name einen Namen für die Kamera ein oder verwenden Sie den Standardnamen.
7. Wählen Sie in der Liste Template eine Kameravorlage aus.
8. Wählen Sie in der Liste Group die Gerätegruppe aus, zu der die Kamera gehört.
9. Wählen Sie in der Liste Add-On die Videoanalyse aus, die auf der Kamera verwendet werden soll.
10. Klicken Sie auf Add 1 Selected Camera.

Nach dem Hinzufügen der Kamera öffnet die

Konfigurationsoberfläche des Server

die Bearbeitungsseite der Kamera. Weitere Informationen finden Sie im Thema „Kamera bearbeiten“.

Analoge Kamera hinzufügen

Sie können eine reine Analogkamera zum Server hinzufügen, wenn die Kamera an einen Videoencoder oder eine Capture-Karte angeschlossen ist. Der Server behandelt den Encoder als Netzwerkgerät und adressiert jeden analogen Kanal als separate Kamera.

Vorbereitung:

- Schließen Sie die Analogkamera an einen Kanal eines unterstützten Videoencoders oder einer Capture-Karte an.
- Notieren Sie sich die IP-Adresse des Encoders, die Anmeldedaten für den Encoder und die Kanalnummer, die die Kamera verwendet.
 1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
 2. Klicken Sie auf Add Cameras.
 3. Klicken Sie auf Add Camera Manually.
 4. Geben Sie im Feld Address die IP-Adresse des Videoencoders ein.
 5. Wählen Sie in der Liste Driver den Hersteller des Videoencoders aus.
 6. Geben Sie den Benutzernamen und das Kennwort für den Encoder ein.
 7. Klicken Sie auf Connect.
 8. Wählen Sie den Encoderkanal aus, den die Analogkamera verwendet.
 9. Geben Sie im Feld Camera Name einen Namen für die Analogkamera ein.
 10. Wählen Sie in der Liste Template eine Kameravorlage aus.
 11. Wählen Sie in der Liste Group die Gerätegruppe aus.
 12. Klicken Sie auf Add 1 Selected Camera.

Konfigurieren Sie nach dem Hinzufügen der Kamera auf der Seite Edit Camera das PTZ-Protokoll, falls die Analogkamera eine PTZ-Kamera ist. Weitere Informationen finden Sie im Thema „Kamera bearbeiten“.

Mobile Kamera hinzufügen

Sie können die Kamera eines Mobilgeräts zum Server hinzufügen, wenn Sie die Senstar Symphony Mobile Bridge verwenden. Die mobile Kamera muss eingeschaltet sein, damit der Server Video empfangen kann.

Um eine mobile Kamera zu verwenden, müssen Sie Port 49900 in der Firewall öffnen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Klicken Sie auf Add Cameras.
3. Klicken Sie auf Add Camera Manually.
4. Geben Sie im Feld Address ein.
5. Wählen Sie im Feld Driver den Eintrag Mobile aus.
6. Geben Sie in den Feldern User Name und Password die Anmeldedaten für die Senstar Symphony

Mobile Bridge ein.

7. Klicken Sie auf Connect.
8. Geben Sie im Feld Camera Name einen Namen für die mobile Kamera ein.
9. Wählen Sie im Feld Template eine Vorlage für die mobile Kamera aus.
10. Wählen Sie im Feld Group die Gruppe für die mobile Kamera aus.
11. Wählen Sie im Feld Add-Ons den Eintrag None aus.



Senstar Symphony-Videoanalysen unterstützen keine mobilen Kameras.

1. Wählen Sie im Feld Server den Server für die mobile Kamera aus.
2. Klicken Sie auf Add 1 Selected Camera.
3. Konfigurieren Sie die Einstellungen für die mobile Kamera.



Die Auflösung auf dem Mobilgerät muss mit der in der Konfigurationsoberfläche des Server festgelegten Auflösung übereinstimmen, damit Video übertragen werden kann.

1. Klicken Sie auf Save.

Kamera bearbeiten

Sie können Kameraeinstellungen in der Konfigurationsoberfläche des Server ändern.

Nachdem Sie eine Kamera zum Server hinzugefügt haben (manuell oder automatisch), bearbeiten Sie die Kamera, um die erweiterten Optionen für die Kamera zu konfigurieren.



Einige Einstellungen sind nicht verfügbar, wenn Sie eine Vorlage auf die Kamera anwenden. Sie müssen die Einstellungen in der Kameravorlage ändern.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie eine Kamera aus und klicken Sie auf Edit.
3. Um den Namen der Kamera zu ändern, geben Sie im Feld Name einen neuen Namen ein.
4. Um die auf die Kamera angewendete Vorlage zu ändern, wählen Sie die Vorlage in der Liste Template aus.
5. Geben Sie im Feld Description eine Beschreibung für die Kamera ein.
6. Geben Sie im Feld Code den Text ein, der als Dekoration über dem Video angezeigt wird.
7. Um den RTSP-Port für eine ONVIF-Kamera zu ändern, geben Sie den neuen Port im Feld RTSP Port ein.
8. Um den Server zu ändern, der die Kamera verwaltet, wählen Sie den neuen Server in der Liste Managed By aus.
9. Um zu ändern, wie die Kamera bei einem Serverausfall reagiert, aktivieren oder deaktivieren Sie das Kontrollkästchen Failover enabled.
10. Um die Kamera für die Unterstützung von Direktverbindungen zu konfigurieren, wählen Sie Support Direct Connect aus.

11. Wenn die Kamera über einen Videoencoder angeschlossen ist, wählen Sie aus, ob es sich um eine feste Kamera oder eine PTZ-Kamera handelt.
12. Wenn es sich bei der Kamera um eine PTZ-Kamera handelt, die über einen Videoencoder angeschlossen ist, führen Sie die folgenden Aufgaben aus:
 - a. Stellen Sie im Feld Max Locked Minutes die maximale Zeit ein, für die die Kamera gesperrt werden kann.
 - b. Legen Sie im Feld Auto-PTZ Priority die Priorität fest, die ein Benutzer überschreiten muss, um die PTZ zu steuern, wenn der Server versucht, die PTZ-Kamera für die automatische Verfolgung zu bewegen.
 - c. Legen Sie im Feld Force-PTZ Priority die Priorität fest, die ein Benutzer überschreiten muss, um die PTZ zu steuern, wenn der Server versucht, die PTZ-Kamera aufgrund einer Regel an einen Ort zu zwingen.
 - d. Wählen Sie in der Liste Type das PTZ-Kommunikationsprotokoll für die Kamera aus.
 - e. Wählen Sie im Feld Camera Address die Adresse der Kamera aus. Die Standardkameraadresse ist 1.
 - f. Wählen Sie in der Liste Control Port den Kommunikationsport aus, den der Encoder für die Kamera verwendet. Sie konfigurieren den Kommunikationsport am Videoencoder, wenn Sie die PTZ-Kamera an den Videoencoder anschließen.
13. Klicken Sie auf Save.

Videostream hinzufügen

Sie können einer Kamera einen Videostream hinzufügen, den der Server verwenden kann, um Video mit reduziertem Ressourcenaufwand anzuzeigen.



Einige Einstellungen sind nicht verfügbar, wenn Sie eine Vorlage auf die Kamera anwenden. Die Einstellungen müssen in der Kameravorlage geändert werden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie eine Kamera aus und klicken Sie auf Edit.
3. Klicken Sie im Bereich Video auf Add Stream.
4. Wählen Sie im Feld Resolution die Auflösung für den Stream aus.
5. Wählen Sie im Feld FPS die Bildrate (Bilder pro Sekunde) für den Stream aus.
6. Wählen Sie im Feld Video Codec den Videocodec für den Stream aus.
7. Wählen Sie im Feld Transport aus, wie die Kamera Video aus dem Stream an den Server übermittelt.
8. Wählen Sie im Feld Bitrate die Bitrate für den Stream aus.
9. Wählen Sie in der Liste Key Frame Interval die Häufigkeit der Bilder im Video aus, die der Server als Schlüsselbilder ansieht.
10. Wählen Sie in der Liste Recording Mode aus, wann der Server Video aus dem Stream aufzeichnet.
11. Wählen Sie in der Liste Schedule aus, wann der Aufzeichnungsmodus für den Stream aktiv ist.
12. Klicken Sie auf Save.

Videoanalysestream hinzufügen

Sie können einer Kamera einen Stream hinzufügen, den der Server für die Videoanalyseverarbeitung verwenden kann.

Um einen

Videoanalyse-Stream

hinzuzufügen, müssen Sie zunächst eine

Videoanalyse

für die Kamera konfigurieren.

Der Server legt Auflösung, Bildrate, Videocodec, Transport, Bitrate und Schlüsselbildintervall automatisch fest.



Einige Einstellungen sind nicht verfügbar, wenn Sie eine Vorlage auf die Kamera anwenden. Die Einstellungen müssen in der Kameravorlage geändert werden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie eine Kamera aus und klicken Sie auf Edit.
3. Klicken Sie im Bereich Video auf Add Analytics Stream.
4. Wählen Sie in der Liste Recording Mode aus, wann der Server Video aus dem Stream aufzeichnet.
5. Wählen Sie in der Liste Schedule aus, wann der Aufzeichnungsmodus für den Stream aktiv ist.
6. Klicken Sie auf Save.

Privatsphärenmaske konfigurieren

Sie können eine Privatsphärenmaske verwenden, um Bereiche in der Kameraansicht zu verdecken. Eine Privatsphärenmaske verdeckt Video (Live und historisch), sodass ein Betrachter Objekte nicht identifizieren kann, dem Server aber weiterhin die Analyse des Videos auf Alarme erlaubt.

Eine statische Privatsphärenmaske verdeckt einen festgelegten Bereich der Kameraansicht. Eine dynamische Privatsphärenmaske verdeckt verfolgte Objekte.

Privatsphärenmasken für PTZ-Kameras enthalten zudem eine Standortliste und einen Schieberegler, mit dem Sie ein Bild vergrößern können.

+

Privacy Mask

Enabled: ☒ Static ☒ Dynamic
 Mask Delay (seconds)

% Surrounding Object
 Blur Amount

Drawing Mode: ☒ Hide ☐ Show
 Brush Size:
[Change Image](#)






Zoom:

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie eine Kamera aus und klicken Sie auf Edit.
3. Führen Sie im Abschnitt Privacy Mask die folgenden Schritte aus:
 - a. Wählen Sie in der Liste Enabled aus, ob die Privatsphärenmaske statisch, dynamisch oder beides ist.
 - b. Legen Sie im Feld Mask Delay fest, wie lange (in Sekunden) sich der Server die Position verfolgter Objekte merkt und die vorherige Position eines verfolgten Objekts weiterhin verdeckt. Diese Einstellung gilt nur für dynamische Privatsphärenmasken.
 - c. Wählen Sie auf dem Schieberegler % Surrounding Object den Bereich um ein verfolgtes Objekt

herum aus, auf den der Server die Privatsphärenmaske anwendet. Diese Einstellung gilt nur für dynamische Privatsphärenmasken.

- d. Wählen Sie auf dem Schieberegler Blur Amount aus, wie stark der Server die Kameraansicht verdeckt.
- e. Wählen Sie in der Liste Drawing Mode aus, ob der Pinsel Bereiche markiert, die ausgeblendet oder angezeigt werden sollen. Diese Einstellung gilt nur für statische Privatsphärenmasken.
- f. Wählen Sie auf dem Schieberegler Brush Size die Größe des Pinsels. Diese Einstellung gilt nur für statische Privatsphärenmasken.
- g. Um das Bild der Privatsphärenmaske zu ändern, klicken Sie auf Change Image und wählen Sie das Bild aus. Diese Einstellung gilt nur für statische Privatsphärenmasken.
- h. Verwenden Sie auf dem Bild der Privatsphärenmaske den Pinsel, um die Bereiche zu definieren, die entweder ausgeblendet oder angezeigt werden sollen. Diese Einstellung gilt nur für statische Privatsphärenmasken.

4. Klicken Sie auf Save.

Digitalen Ein- und Ausgang konfigurieren

Sie können konfigurieren, wie digitale Ein- und Ausgänge in der Oberfläche des Windows Client angezeigt werden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie eine Kamera aus und klicken Sie auf Edit.
3. Führen Sie im Abschnitt Digital I/O die folgenden Aufgaben aus:
 - a. Um den Ein- oder Ausgang zu aktivieren, wählen Sie In Use aus.
 - b. Um den Namen festzulegen, der in der Oberfläche des Windows Client angezeigt wird, geben Sie im Feld Output Name oder Input Name einen Namen ein.
 - c. Geben Sie im Feld Activate den Text ein, der in der Oberfläche des Windows Client angezeigt wird, wenn der Ein- oder Ausgang durch Klicken aktiviert wird.
 - d. Geben Sie im Feld Deactivate den Text ein, der in der Oberfläche des Windows Client angezeigt wird, wenn der Ein- oder Ausgang durch Klicken deaktiviert wird.
 - e. Stellen Sie im Feld Auto Deactivate die Zeit (in Millisekunden) ein, nach der der Ein- oder Ausgang automatisch deaktiviert wird.
 - f. Wählen Sie in der Liste Camera Shortcut die Kamera aus, auf der die Steuerelemente für den Ein- oder Ausgang angezeigt werden. Schaltflächen, mit denen Sie den Ein- oder Ausgang steuern können, werden im Kameraansichtspanel der ausgewählten Kamera angezeigt.
4. Klicken Sie auf Save.

Kamera zu einer Gerätegruppe hinzufügen

Sie können eine Kamera im Gerätebaum zu einer Gerätegruppe hinzufügen.

Stellen Sie zunächst sicher, dass Sie Gerätegruppen für den Gerätebaum erstellt haben.

Die Kamera erscheint als Teil der Gruppe im Gerätebaum in der Oberfläche des Windows Client.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.

2. Wählen Sie eine Kamera aus und klicken Sie auf Edit.
3. Wählen Sie im Bereich Groups eine oder mehrere Gruppen aus, denen Sie die Kamera hinzufügen möchten.
4. Klicken Sie auf Save.

Videospeicher für eine Kamera konfigurieren

Was es ist

Jede Kamera schreibt ihr aufgezeichnetes Video in einen Speicherpfad und behält dieses Video für eine Aufbewahrungsdauer. Senstar Symphony löst diese beiden Werte auf drei Ebenen mit klarer Priorität auf:

1. **Kamera** (diese Seite) — die kamerabezogene Überschreibung.
2. **Server** — der Standardwert für jede Kamera auf diesem Server.
3. **Serverfarm** — der Standardwert für alle Server-Instanzen in der Farm.

Die **Kamera**-Einstellung hat Vorrang vor der Server-Einstellung, die wiederum Vorrang vor der Farm-Einstellung hat. Setzen Sie Werte auf der höchsten Ebene, die geteilt werden kann, und überschreiben Sie nur dort, wo eine Kamera etwas anderes benötigt.

Wann Sie es verwenden

- Eine bestimmte Kamera benötigt ein längeres Aufbewahrungsfenster als der Standardwert des Standorts (zum Beispiel ein sensibler Eingangspunkt, der 90 Tage aufbewahren muss, während die meisten Kameras 30 Tage aufbewahren).
- Eine Kamera muss auf ein anderes Volume schreiben, weil das Standardvolume voll, langsam oder für eine andere Speicherebene reserviert ist.
- Das aufgezeichnete Video einer Kamera darf aus Compliance-Gründen nicht zusammen mit anderen Kameras gespeichert werden.

Wenn jede Kamera dieselbe Einstellung benötigt, ändern Sie stattdessen den Standardwert auf Server- oder Farmebene, statt jede Kamera einzeln zu bearbeiten.

Voraussetzungen

- Berechtigung zur Bearbeitung von Kameraeinstellungen.
- Die Kamera ist bereits hinzugefügt. Siehe [Kamera hinzufügen](#).
- Wenn Sie einen benutzerdefinierten Pfad verwenden: Der Pfad existiert, ist durch das Dienstkonto des Server beschreibbar und verfügt über genügend freien Speicherplatz für das geplante Aufbewahrungsfenster.

Über Speicherpfade

Speicherpfade können auf eine lokale Festplatte, ein angeschlossenes Volume oder eine eingebundene Netzwerkfreigabe verweisen. Ein gültiger Pfad:

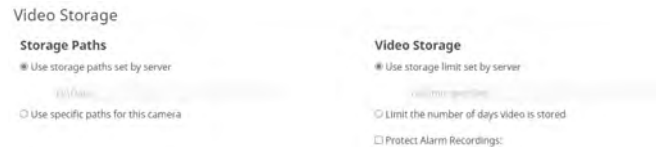
- Existiert, bevor Sie die Einstellung speichern — der Server erstellt das Verzeichnis nicht.
- Ist durch das Dienstkonto, das den Server ausführt, beschreibbar.
- Verfügt über genügend freien Speicherplatz für das Aufbewahrungsfenster. Eine grobe Berechnung: tägliche Bitrate × Aufzeichnungsstunden × Aufbewahrungstage. Wenn dem Server der Speicherplatz auf einem Pfad ausgeht, beginnt er, das älteste Video von diesem Pfad zu löschen, unabhängig von der Aufbewahrungseinstellung.

Über die Aufbewahrung

Die Aufbewahrung legt das maximale Alter von aufgezeichnetem Video fest. Der Server löscht im Rahmen der routinemäßigen Wartung Video, das älter als das Aufbewahrungsfenster ist. Zwei Ausnahmen:

- **Speicherengpass** — wenn ein Speicherpfad voll ist, wird Video von alt nach neu gelöscht, auch bevor das Aufbewahrungsfenster abläuft.
- **Alarmschutz** — alarmbezogenes Video kann länger aufbewahrt werden als die allgemeine Aufbewahrung (siehe **Protect Alarm Recordings** unten).

Vorgehen



1. Klicken Sie in der Konfigurationsoberfläche des Server auf **Devices > Cameras**.
2. Wählen Sie eine Kamera aus und klicken Sie auf **Edit**.
3. Wählen Sie im Abschnitt **Storage Paths** eine der Optionen:
 - **Use storage paths set by server** — die Einstellung von der Server- oder Farmebene übernehmen.
 - **Use specific paths for this camera** — den Überschreibungspfad eingeben.
4. Wählen Sie im Abschnitt **Video Storage** eine der Optionen:
 - **Use storage limit set by server** — die Aufbewahrungsrichtlinie übernehmen.
 - **Limit the number of days video is stored** — ein kameraspezifisches Aufbewahrungsfenster in Tagen festlegen.
5. (Optional) Um alarmbezogenes Video länger als die allgemeine Aufbewahrung beizubehalten, gehen Sie unter **Protect Alarm Recordings** wie folgt vor:
 - a. Wählen Sie **Protect Alarm Recordings** aus.
 - b. Stellen Sie unter **Days** ein, wie lange (in Tagen) der Server alarmbezogenes Video aufbewahrt.
 - c. Stellen Sie unter **Pre Alarm** ein, wie viele Sekunden Video **vor** dem Alarmauslöser eingeschlossen werden sollen.
 - d. Stellen Sie unter **Post Alarm** ein, wie viele Sekunden Video **nach** dem Alarmauslöser eingeschlossen werden sollen.
6. Klicken Sie auf **Save**.

Verwandte Aufgaben

- Videospeicher für einen Server konfigurieren
- Videospeicher für eine Serverfarm konfigurieren
- Kamera bearbeiten

Hilfsbefehl hinzufügen

Sie können Zusatzbefehle zu PTZ-Kameras oder Videoencodern hinzufügen, die Sie zum Server hinzufügen.

Zusatzbefehle sind benutzerdefinierte Befehle, die Sie zu PTZ-Kameras und Encodern hinzufügen können, um zusätzliche Funktionen in der Oberfläche des Windows Client zu nutzen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie eine Kamera aus und klicken Sie auf Edit.
3. Führen Sie im Bereich Auxiliary die folgenden Aufgaben aus:
 - a. Wählen Sie Enable auxiliary commands aus.
 - b. Klicken Sie auf Add.
 - c. Geben Sie im Feld Label einen Namen für den Befehl ein.
 - d. Geben Sie im Feld Command den benutzerdefinierten Befehl ein.
 - e. Wählen Sie im Feld Method aus, ob es sich um einen GET- oder PUT-Befehl handelt.
4. Klicken Sie auf Save.

Um einen Zusatzbefehl zu entfernen, klicken Sie auf das X neben dem Befehl.

Overlay-Befehl hinzufügen

Sie können den Ausgang eines I/O-Geräts als Overlay-Befehl zu einer Kamera hinzufügen. Wenn Sie die Kamera in der Oberfläche des Windows Client anzeigen, erscheint der Befehl als Schaltfläche in der Kameraansicht, die beim Anklicken den Ausgang des I/O-Geräts aktiviert.

Nachdem Sie einen Overlay-Befehl zu einer Kamera hinzugefügt haben, erscheint der Befehl in der Oberfläche des Windows Client so, wie er in der Konfigurationsoberfläche des Server angezeigt wird (einschließlich Aliasen). Sie können einer Kamera mehrere Overlay-Befehle hinzufügen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie eine Kamera aus und klicken Sie auf Edit.
3. Wählen Sie im Bereich Overlay Commands das Hardware-Gerät aus, das Sie ansteuern möchten.
4. Wählen Sie in der Liste Choose a command aus, was der Befehl bewirken soll (z. B. Activate, Deactivate, Toggle State usw.).
5. Klicken Sie auf Save.

Kamera-Failover konfigurieren

Sie können kameraweise auswählen, ob der Server die Kamera bei einem Failover-Ereignis auf einen redundanten Server verschiebt.

Die Redundanz auf Serverebene legt fest, welcher Server übernimmt, wenn ein primärer Server nicht mehr antwortet. Das Failover auf Kameraebene legt fest, ob eine einzelne Kamera an dieser Übergabe teilnimmt. Standardmäßig wird jede Kamera mit ihrem Server umgeschaltet. Sie können die Failover-Einstellung für Kameras deaktivieren, die nicht kritisch sind, eine begrenzte Bandbreite haben oder deren Video auf dem redundanten Server nicht lizenziert ist.

Konfigurieren Sie zuvor die Serverredundanz. Weitere Informationen finden Sie im Thema Serverredundanz.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Um die Kamera in das Failover einzubeziehen, aktivieren Sie das Kontrollkästchen Failover enabled.
4. Um die Kamera vom Failover auszuschließen, deaktivieren Sie das Kontrollkästchen Failover enabled.
5. Klicken Sie auf Save.



Eine Kamera, die vom Failover ausgeschlossen ist, ist nicht verfügbar, während ihr primärer Server offline ist. Der Server setzt die Verarbeitung der Kamera fort, sobald der primäre Server wieder verfügbar ist.

Kameras importieren

Sie können Kameras aus einer CSV-Datei importieren.

Sie können eine CSV-Datei mit Kameras erstellen, indem Sie entweder eine Liste mit Kameras exportieren oder eine leere Importdatei zur Verwendung als Vorlage erstellen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Klicken Sie auf Add Cameras.
3. Klicken Sie auf Import Cameras From File.
4. Navigieren Sie zur Kameralistendatei und klicken Sie auf Open.

Kamera suchen

Um schnell eine bestimmte Kamera zu finden, verwenden Sie Filter und Sortierung.

Filter

Sie können die Kameraliste anhand der folgenden Filter filtern:

- Kamera-ID (ID)
- Kameraname (Name)
- Server, mit dem die Kamera verbunden ist (Server)
- Kameratyp (Type)
- IP-Adresse der Kamera (IP Address)
- Kameramarke (Brand)
- Kameramodell (Model)
- auf die Kamera angewandte Vorlage (Template)
- Kameraauflösung (Resolution)
- Kamera-Bildrate (FPS)
- Gruppen, zu denen die Kamera gehört (Groups)
- auf der Kamera aktive Videoanalyse (Add-on)
 1. Klicken Sie in der Server-Konfigurationsoberfläche auf Devices > Cameras.
 2. Klicken Sie auf die Lupe, um die Filter-Textfelder einzublenden.

3. Definieren Sie die Filterkriterien.
4. Klicken Sie auf Apply filter.

Sortierung

Sie können die Liste der Kameras sortieren, indem Sie auf den Spaltennamen klicken. Durch Klicken auf den Spaltennamen wird zwischen aufsteigender und absteigender Reihenfolge gewechselt.

Zurücksetzen

Um den Filter zurückzusetzen und die Liste der Kameras wiederherzustellen, klicken Sie auf Clear Filter.

Kameras exportieren

Sie können die Kameraliste vom Server in eine CSV-Datei exportieren.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Klicken Sie auf Export.

Sie können die CSV-Datei verwenden, um die Kameras auf einen anderen Server zu importieren.

Leere Importdatei erstellen

Sie können eine leere CSV-Datei erstellen, um sie zum Importieren von Kameras in den Server zu verwenden.

Die leere Importdatei enthält Anweisungen zum Hinzufügen und Importieren von Kameras.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Klicken Sie auf Add Cameras.
3. Klicken Sie auf Create Blank Import File.

Der Server speichert eine Datei namens import.csv an Ihrem Downloadort.

Passwort für Kamera festlegen

Sie können ein neues Kennwort festlegen, das der Server an die Kamera überträgt.

Wenn Sie ein neues Kennwort für eine Kamera festlegen, müssen Sie dieses Kennwort verwenden, wenn Sie sich an der Web-Oberfläche der Kamera anmelden.

1. Klicken Sie in der Server-Konfigurationsoberfläche auf Devices > Cameras.
2. Wählen Sie eine Kamera aus.
3. Klicken Sie auf die Schaltfläche Set Password.
4. Geben Sie das neue Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf die Schaltfläche Set Password.

Kamera verschieben

Sie können eine Kamera auf einen anderen Server in Ihrer Serverfarm verschieben.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie eine Kamera aus.

3. Klicken Sie auf Move to Server.
4. Wählen Sie den Server in der Serverliste aus.
5. Klicken Sie auf OK.

Videoanalyse

Die Videoanalysen von Senstar Symphony bieten Echtzeit-Warmmeldungen, intelligente Videosuche und Berichte.

Um eine Videoanalyse zu verwenden, erwerben Sie die entsprechende Lizenz und installieren die Videoanalyse auf dem Computer, der den Server hostet. Nach der Installation können Sie die Videoanalyse in der Konfigurationsoberfläche des Server auf einer Kamera aktivieren und konfigurieren.

+

Name	Type	Description
☐ TCP Listener	Other	Accepts messages from Symphony.
☐ Analytic Video Signal Loss	PC Analysis	Detects if the video input is one which is not visible or which may indicate signal loss.
☐ Analytics License Plate Recognition (LPR)	PC Analysis	Optical Recognition of license plates from various regions.
☐ Camera Tampering	PC Analysis	Detects if the video has been compromised (loss of video, obstructed, spray painted with, camera position altered).
☐ Crowd Detection	PC Analysis	Detects size and density of crowds of people.
☐ Image Classification	PC Analysis	Maximize the video stream, when experiencing small movements, for use with another video stream or video.
☐ Person Pose Tracking	PC Analysis	Can be used for research, tracking, in outdoor environments.
☐ Left and Rightward Item Detection	PC Analysis	Detects left or rightward items.
☐ Motion Detection	PC Analysis	Detects object changes in the scene.
☐ Outdoor People and Vehicle Tracking	PC Analysis	Can be used for research, tracking, in outdoor environments.

+

Videoanalyse-Lizenz zu einer Kamera hinzufügen

Um eine Videoanalyse auf einer Kamera zu verwenden, müssen Sie der Kamera eine Lizenz hinzufügen, die diese Videoanalyse umfasst.

Vorbereitung:

- Erwerben Sie eine Lizenz für die Videoanalyse.
- Laden Sie die Videoanalyse herunter und installieren Sie sie.
 1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
 2. Wählen Sie eine Kamera aus.
 3. Klicken Sie auf Edit.
 4. Wählen Sie im Bereich Add-Ons in der Liste Analytic License Requested eine geeignete Lizenz aus.
 5. Klicken Sie auf Update License.
 6. Klicken Sie auf Save.

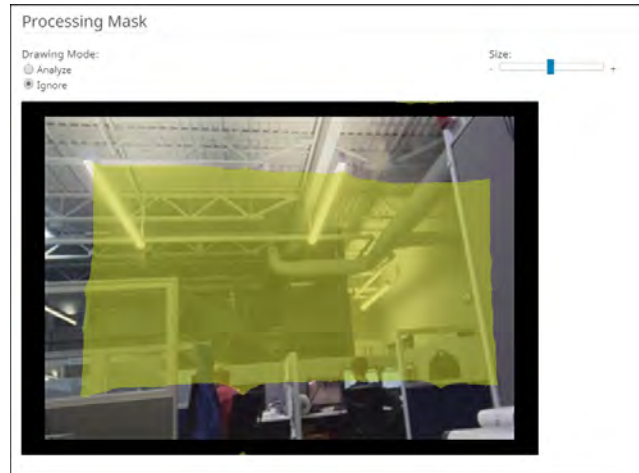
Verarbeitungsmaske zeichnen

Sie können in der Konfigurationsoberfläche des Server eine Verarbeitungsmaske für eine Videoanalyse zeichnen, um den Bereich in der Kameraansicht zu definieren, den die Videoanalyse analysiert.

Das Zeichnen einer Verarbeitungsmaske ist Teil der Konfiguration einer Videoanalyse.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.

3. Klicken Sie in der Liste Add-Ons auf Configure für die Videoanalyse.
4. Führen Sie im Abschnitt Processing die folgenden Aufgaben aus:
 - a. Wählen Sie in der Liste Drawing Mode aus, ob der Pinsel Bereiche im Verarbeitungsmaskenbild markiert, die einbezogen (Analyze) oder ausgeschlossen (Ignore) werden sollen.
 - b. Wählen Sie mit dem Schieberegler Size die Größe des Pinsels aus, den Sie im Verarbeitungsmaskenbild verwenden.
 - c. Zeichnen Sie die Verarbeitungsmaske mit der Maus. Wenn Sie einen Fehler machen, können Sie den Zeichenmodus umkehren und die Verarbeitungsmaske ändern.



5. Klicken Sie auf OK.

Kamera kalibrieren

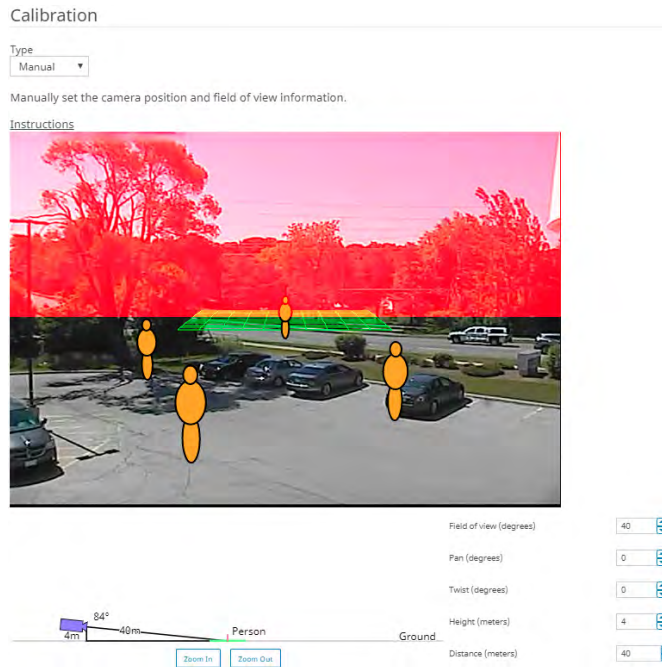
Für einige Videoanalysen müssen Sie die Kamera kalibrieren, um eine optimale Leistung und Genauigkeit zu erzielen.

Das Kalibrieren einer Kamera ist Bestandteil der Konfiguration einer Videoanalyse.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Klicken Sie in der Liste Add-Ons auf Configure für die Videoanalyse.
4. Führen Sie im Bereich Calibration die folgenden Aufgaben aus:
 - a. Klicken Sie auf das Kalibrierungsbild, um Avatare auf dem Bild zu platzieren. Die Avatare helfen Ihnen, Personen im Beispielbild zu visualisieren.
 - b. Geben Sie im Feld Field of view das Sichtfeld der Kamera in Grad ein.
 - c. Geben Sie im Feld Pan den Winkel (in Grad) der horizontalen Drehung um die vertikale Achse der Kamera ein.
 - d. Geben Sie im Feld Twist den Winkel (in Grad) der Drehung um die Längsachse der Kamera ein.
 - e. Geben Sie im Feld Twist den Winkel (in Grad) der Drehung um die Längsachse der Kamera ein.
 - f. Geben Sie im Feld Height die Höhe der Kamera ein.
 - g. Geben Sie im Feld Distance den Abstand zwischen der Kamera und dem Mittelpunkt des

Kalibrierungsrasters ein.

5. Klicken Sie auf Save.



Zusätzlich können Sie die Kamera im Kalibrierungsdiagramm verschieben, um sie in Bezug auf die Szene zu platzieren. Die Schaltflächen Zoom In und Zoom Out passen den Maßstab des Kalibrierungsdiagramms an.

TCP-Listener

Der TCP-Listener ist eine Videoanalyse, die auf eingehende Metadaten über einen TCP-Socket lauscht und die Metadaten mit einem Bild oder Video verknüpft.

Der Server kann die Metadaten verwenden, um nach Bildern und Video zu suchen.

TCP-Listener aktivieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Aktivieren Sie in der Liste Add-Ons die Option TCP Listener.
4. Klicken Sie auf Save.

Verlust des analogen Videosignals

Die Videoanalyse Analog Video Signal Loss kann erkennen, wenn das Video einer Kamera nicht verfügbar ist.

Diese Videoanalyse erfordert keine Konfiguration und beansprucht nur minimale CPU-Ressourcen. Sie wird für alle Kameras empfohlen.

Verlust des analogen Videosignals aktivieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.

3. Aktivieren Sie in der Liste Add-Ons die Option Analog Video Signal Loss.
4. Klicken Sie auf Save.

Automatische Kennzeichenerkennung

Die Videoanalyse Automatische Kennzeichenerkennung ist eine Videoanalyse für den Server, die Kennzeichen erkennen und indexieren kann.

Die Videoanalyse Automatische Kennzeichenerkennung kann Kennzeichen aus verschiedenen Ländern und Regionen an Fahrzeugen mit einer Geschwindigkeit von bis zu 30 km/h (19 mph) erkennen und protokollieren. Sie kann Video in Echtzeit analysieren, ohne dass ein externer Auslöser erforderlich ist.

Mit der Videoanalyse Automatische Kennzeichenerkennung kann eine 720p-Netzwerkamera bis zu zwei Fahrspuren analysieren, sofern die Kennzeichenbilder mindestens 32 Pixel hoch für lateinische Zeichen oder 40 Pixel hoch für nicht-lateinische Zeichen sind.

Typische Einsatzgebiete der Videoanalyse Automatische Kennzeichenerkennung sind:

- Mauterhebung in Parkhäusern
- Verkehrssteuerung
- Grenzübergänge
- Nutzungsmusteranalyse

Automatische Kennzeichenerkennung konfigurieren

Konfigurieren Sie die Videoanalyse Automatische Kennzeichenerkennung für jede Kamera, auf der die Videoanalyse ausgeführt wird.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus, auf der Sie die Videoanalyse Automatische Kennzeichenerkennung ausführen möchten, und klicken Sie auf Edit.
3. Klicken Sie im Abschnitt Add-Ons auf die Schaltfläche neben Automatic License Plate Recognition, um die Funktion zu aktivieren.
4. Klicken Sie auf die Schaltfläche Configure neben Automatic License Plate Recognition.
5. Konfigurieren Sie im Abschnitt Overview die Analyseoptionen und wählen Sie aus, ob die erweiterten Optionen ausgeblendet (Simple Mode an) oder angezeigt (Simple Mode aus) werden sollen.
6. Wenn das Bild in den Abschnitten Processing Mask und Plate Detection kein Bild enthält, das für die Kennzeichenerkennung geeignet ist, aktualisieren Sie das Bild.
 - a. Klicken Sie auf Change Image.
 - b. Verwenden Sie die Zeitleiste und die Videosteuererelemente, um zu einem Bild zu navigieren, das für die Kennzeichenerkennung geeignet ist.
 - c. Klicken Sie auf OK.
7. Definieren Sie im Bild Processing Mask die Bereiche, die die Videoanalyse analysiert und ignoriert.
 - a. Wählen Sie in der Liste Drawing Mode aus, ob ein Bereich zum Analysieren oder Ignorieren gezeichnet werden soll.
 - b. Wählen Sie mit dem Schieberegler Size die Größe des Zeichenkreises aus.

- c. Klicken und ziehen Sie den Zeichenkreis auf dem Bild, um die Bereiche zu definieren, die analysiert oder ignoriert werden sollen.
8. Zeichnen Sie im Bild Plate Detection einen Rahmen um das Kennzeichen, sodass die Kanten des Textes auf dem Kennzeichen innerhalb des grünen Rahmens liegen.
 - a. Klicken und ziehen Sie den Rahmen auf dem Bild.
 - b. Um den Rahmen zu verschieben, klicken Sie in die Mitte des grünen Rahmens und ziehen Sie ihn.
 - c. Um die Größe des Rahmens zu ändern, klicken Sie auf eine Kante des Rahmens und ziehen Sie die Linie, um die Größe anzupassen.
 - d. Um Neigung und Schräglage des Rahmens anzupassen, klicken Sie auf eine Ecke des Rahmens und ziehen Sie die Ecke, um die Neigung oder Schräglage zu ändern.
9. Wählen Sie mit dem Schieberegler Reporting Confidence aus, wie empfindlich die Videoanalyse auf potenzielle Kennzeichen reagiert.
10. Klicken Sie auf OK.

Einstellungen für automatische Kennzeichenerkennung

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Wählen Sie die Auflösung aus, die die Videoanalyse Automatische Kennzeichenerkennung zur Analyse von Videobildern verwendet.
Analysis FPS	Wählen Sie die Anzahl der Bilder pro Sekunde aus, die die Videoanalyse Automatische Kennzeichenerkennung zur Videoanalyse verwendet.
Simple Mode	Deaktivieren Sie diese Option, um die erweiterten Einstellungen sichtbar zu machen.
Region For Plate Analysis	Wählen Sie die regionale Engine aus, die die Videoanalyse Automatische Kennzeichenerkennung zur Analyse der von dieser Kamera erkannten Kennzeichen verwendet. Die Liste enthält die Regionen, die Sie bei der Installation auswählen.
V9 Dongle	Wählen Sie diese Option, wenn Sie eine neue Lizenz mit der Default- oder China-Engine verwenden.
Enable with Motion Detection	Wählen Sie diese Option, um die Analyse nur dann durchzuführen, wenn die Kamera Bewegung erkennt.
Enable with Relay	Wählen Sie diese Option, um die Analyse nur dann durchzuführen, wenn ein Relais-Gerät ein Eingangsereignis aufzeichnet. Wenn Sie diese Option auswählen, erscheinen zusätzliche Felder, in denen Sie das Relais auswählen und konfigurieren können, wie die Videoanalyse Automatische Kennzeichenerkennung auf das Eingangsereignis reagiert.

Verarbeitungsmaske

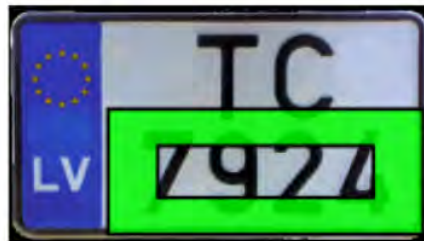
Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob auf der Verarbeitungsmaske zu analysierende oder zu ignorierende Bereiche gezeichnet werden sollen.

Einstellung	Beschreibung
Size	Definieren Sie die Größe des Kreises, der auf der Verarbeitungsmaske gezeichnet wird.

Kennzeichenerkennung

Verwenden Sie das Bild zur Kennzeichenerkennung, um in einem Bild, das eine typische Kennzeichenerkennungssituation darstellt, einen Rahmen um das Kennzeichen zu zeichnen. Der Rahmen darf nur eine Zeichenzeile umschließen, und die äußeren Begrenzungen der Zeichen sollten innerhalb des grünen Rahmens liegen.

Dies ist ein Beispiel für einen guten Kennzeichenrahmen:



+

Dies ist ein Beispiel für einen schlechten Kennzeichenrahmen:



+

Einstellung	Beschreibung
Reporting Confidence	Verwenden Sie den Schieberegler, um die Empfindlichkeit der Videoanalyse Automatische Kennzeichenerkennung festzulegen. Die Reporting Confidence beträgt standardmäßig 50 %. Eine niedrigere Reporting Confidence führt zu mehr Erkennungen und kann die Leistung beeinflussen.
Minimum height	In diesem Feld wird die Höhe des inneren Rechtecks angezeigt.
Maximum height	In diesem Feld wird die Höhe des äußeren Rechtecks angezeigt.
Minimum width	In diesem Feld wird die Breite des inneren Rechtecks angezeigt. Diese Einstellung ist nur für die Videoanalyse Automatic License Plate Recognition Core verfügbar.
Maximum width	In diesem Feld wird die Breite des äußeren Rechtecks angezeigt. Diese Einstellung ist nur für die Videoanalyse Automatic License Plate Recognition Core verfügbar.
Minimum slant	In diesem Feld wird die minimale Neigung der vertikalen Linien angezeigt. Diese Einstellung ist nur für die Videoanalyse Automatic License Plate Recognition Peripheral verfügbar.
Maximum slant	In diesem Feld wird die maximale Neigung der vertikalen Linien angezeigt. Diese Einstellung ist nur für die Videoanalyse Automatic License Plate Recognition Peripheral verfügbar.
Minimum slope	In diesem Feld wird die minimale Steigung der horizontalen Linien angezeigt. Diese Einstellung ist nur für die Videoanalyse Automatic License Plate Recognition Peripheral verfügbar.
Maximum slope	In diesem Feld wird die maximale Steigung der horizontalen Linien angezeigt. Diese Einstellung ist nur für die Videoanalyse Automatic License Plate Recognition Peripheral verfügbar.

Erweitert

Die erweiterten Einstellungen sind sichtbar, wenn der einfache Modus deaktiviert ist.



Das Ändern der erweiterten Einstellungen kann die Leistung der Videoanalyse beeinträchtigen.

Einstellung	Beschreibung
Minimum Plate Length	Definieren Sie die Mindestanzahl an Zeichen, die die Videoanalyse Automatische Kennzeichenerkennung erkennen muss, bevor sie den Text als potenzielles Kennzeichen klassifiziert.

Einstellung	Beschreibung
Plate Dwell Time	Definieren Sie die Zeit (in Sekunden), die ein potenzielles Kennzeichen sichtbar sein muss, bevor die Videoanalyse Automatische Kennzeichenerkennung mit der Analyse des potenziellen Kennzeichens beginnt.
Queue Time	Definieren Sie, wie viel Video die Videoanalyse Automatische Kennzeichenerkennung zur Analyse aufbewahrt. Bilder, die außerhalb der Queue-Zeit liegen, werden von der Videoanalyse ignoriert.
Analysis Timeout	Definieren Sie, wie viel Zeit vergehen darf, bevor die Videoanalyse Automatische Kennzeichenerkennung die Verarbeitung eines Kennzeichens beendet.
Plate Display Time	Definieren Sie, wie lange die Videoanalyse Automatische Kennzeichenerkennung die Kennzeichen-Dekoration in der Oberfläche des Windows Client anzeigt.
Plate Look Time	Definieren Sie die Zeit (in Sekunden), die die Videoanalyse Automatische Kennzeichenerkennung mit der Analyse des Kennzeichens verbringt. Während dieser Zeit zeichnet die Videoanalyse alle erkannten Zeichen auf (zum Beispiel kann die Videoanalyse ein Zeichen als mehrere ähnliche Zeichen erkennen, während sich das Kennzeichen durch die Szene bewegt). Nach Ablauf der Zeit wählt die Videoanalyse das beste Ergebnis aus und meldet es. Alle von der Videoanalyse erkannten Ergebnisse werden jedoch in der Datenbank gespeichert. Wenn Sie diesen Wert auf 0 (null) setzen, meldet die Videoanalyse das erste erkannte Ergebnis.
Import XML	Klicken Sie auf diese Schaltfläche, um eine XML-Konfigurationsdatei zu importieren.
Export XML	Klicken Sie auf diese Schaltfläche, um die XML-Konfigurationsdatei zu exportieren.
Show XML	Klicken Sie auf diese Schaltfläche, um die Konfigurations-XML anzuzeigen.

Kameramanipulation

Die Videoanalyse Kameramanipulation ist eine Videoanalyse, die erkennen kann, wenn das Sichtfeld einer Kamera blockiert wird.

Die Videoanalyse Kameramanipulation kann auf einer Kamera aktiviert werden, auf der bereits eine andere Videoanalyse ausgeführt wird, um den durchgehenden Betrieb der Kamera sicherzustellen. Sie kann erkennen, wenn sich die Ausrichtung der Kamera ändert, wenn die Kamera blockiert wird oder wenn sich die Beleuchtung in der Szene ändert.

Wenn die Videoanalyse Kameramanipulation eine erhebliche Veränderung der Szene erkennt (etwa 25 % der Szene verändert sich), verwendet sie ein vorheriges Bild als Referenz und vergleicht die nachfolgenden Bilder mit diesem Referenzbild. Wenn die Veränderung über die festgelegte Mindestdauer für Manipulation hinaus bestehen bleibt, schließt die Videoanalyse Kameramanipulation darauf, dass die Kamera blockiert ist. Beispielsweise kann die Videoanalyse Kameramanipulation erkennen, wenn das Objektiv einer Kamera mit Sprühfarbe besprüht wird, wenn eine Kamera bewegt wird, wenn ein großer Gegenstand vor einer Kamera platziert wird oder wenn das Licht in der Szene ausgeschaltet wird.

Kameramanipulation konfigurieren

Konfigurieren Sie die Videoanalyse Kameramanipulation in der Konfigurationsoberfläche des Server.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Aktivieren Sie in der Liste Add-Ons Camera Tampering und klicken Sie auf Configure.
4. Passen Sie die Einstellungen für die Videoanalyse Kameramanipulation an.
5. Klicken Sie auf OK.

Einstellungen für Kameramanipulation

Einstellung	Beschreibung
Analysis Resolution	Legen Sie die Auflösung für die Kamera fest, auf der die Videoanalyse Kameramanipulation aktiv ist.
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen. Der einfache Modus ist der Standardmodus. Der erweiterte Modus ist für Systemintegratoren und den technischen Support gedacht.
Minimum tampering time threshold	Legen Sie fest, wie lange eine Kamera blockiert sein muss, bevor ein Alarm ausgelöst wird. Diese Einstellung ist nützlich für Szenen, in denen vorübergehende Verdeckungen vorkommen, etwa wenn Personen an der Kamera vorbeigehen. Sie können den Schwellenwert so festlegen, dass die Videoanalyse vorübergehende Verdeckungen ignoriert.
Scene consistency threshold	Legen Sie die Größe der Szenenänderung fest, die auf eine Kameraverdeckung hinweist. Diese Einstellung ist nützlich für Szenen, in denen Lichtveränderungen auftreten. Sie können den Schwellenwert so festlegen, dass die Videoanalyse das Ein- und Ausschalten der Beleuchtung in der Szene ignoriert, andere Kameraverdeckungen jedoch registriert.

Erkennung von Menschenmengen

Die Videoanalyse Erkennung von Menschenmengen ist eine Videoanalyse, die Erkennung von Menschenmengen, Ereignisauslösung und Alarme bietet.

Sie können den Bereich definieren, den die Videoanalyse Erkennung von Menschenmengen hinsichtlich der Anzahl der Personen im überwachten Bereich (Capacity) und des prozentualen Anteils des überwachten Bereichs mit Personen (Occupancy) überwacht. Die Videoanalyse Erkennung von Menschenmengen kann Alarme auslösen, wenn sie eine bestimmte Capacity oder Occupancy erkennt.

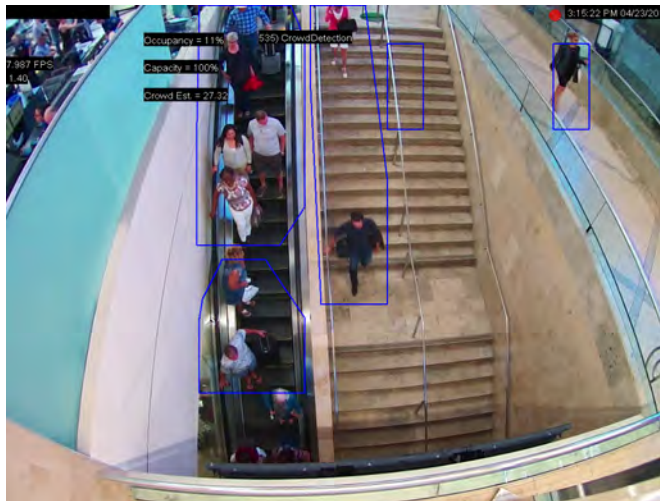
Die Videoanalyse Erkennung von Menschenmengen kann informative Dekorationen im Kameraansichtspanel anzeigen. Zusätzlich zur Anzeige von Verfolgungsboxen um Bereiche, in denen sie Personen erkennt, kann die Videoanalyse Erkennung von Menschenmengen die folgenden Dekorationen anzeigen:

- Die Dekoration Occupancy zeigt den Prozentsatz der Szene an, der Personen enthält.
- Die Dekoration Capacity zeigt die geschätzte Anzahl der Personen in der Szene als Prozentsatz der maximalen Kapazität an.

- Die Dekoration Crowd Est. zeigt die geschätzte Anzahl der Personen in der Szene an.

Die Videoanalyse Erkennung von Menschenmengen kann Personen erkennen, die mindestens 8 Pixel groß in der Szene sind. Beachten Sie beim Platzieren einer Kamera für die Verwendung mit der Videoanalyse Erkennung von Menschenmengen die folgenden Richtlinien.

- Montieren Sie die Kamera so, dass sie einen Überblick über den Bereich hat. Platzieren Sie die Kamera nicht direkt darüber (90°), da die Videoanalyse Erkennung von Menschenmengen Personen nicht direkt von oben erkennen kann, und platzieren Sie die Kamera nicht nahe der Horizontalen (0°), da Personen im Vordergrund die Menschenmenge dahinter verdecken.
- Montieren Sie die Kamera oder verwenden Sie die Verarbeitungsmaske so, dass die Szene keine Menschenmengen mit mehr als 50 Personen enthält. Die Videoanalyse Erkennung von Menschenmengen funktioniert bei Szenen mit mehr als 50 Personen nicht zuverlässig.
- Montieren Sie die Kamera oder verwenden Sie die Verarbeitungsmaske so, dass die Szene keine anderen sich bewegendes Objekte (z. B. Fahrzeuge) oder bewegte Schatten enthält.



Wenn die Videoanalyse Erkennung von Menschenmengen startet, benötigt sie etwa 2 Minuten, um die Szene zu lernen. Während dieser Zeit sind die Ergebnisse ungenau.

Erkennung von Menschenmengen konfigurieren

Konfigurieren Sie die Videoanalyse Erkennung von Menschenmengen in der Konfigurationsoberfläche des Server.

Um die Videoanalyse Erkennung von Menschenmengen zu konfigurieren, sollten Sie ein Bild verwenden, das mindestens eine Person aus der zu konfigurierenden Kamera enthält. Passen Sie die Einstellungen so an, dass die Referenzpersonen und die Rasterlinien im Kalibrierungsbild zur Szene passen. Sie können Referenzpersonen im Kalibrierungsbild verschieben und hinzufügen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Aktivieren Sie in der Liste Add-Ons die Videoanalyse Crowd Detection und klicken Sie auf Configure.
4. Definieren Sie auf der Seite Crowd Detection die Einstellungen für Overview, Processing Mask, Capacity, Calibration und Sensitivity.
5. Klicken Sie auf OK.

Einstellungen für Erkennung von Menschenmengen

Overview

Einstellung	Beschreibung
Analysis Resolution	Stellen Sie die Auflösung für die Kamera ein, auf der die Videoanalyse Erkennung von Menschenmengen aktiv ist.
Automatically Select Resolution Based on Calibration	Wählen Sie diese Option aus, um die Analyseauflösung automatisch auf Basis der Einstellungen im Abschnitt Calibration festzulegen.
Analysis FPS	Stellen Sie die Bilder pro Sekunde für die Kamera ein, auf der die Videoanalyse Erkennung von Menschenmengen aktiv ist.
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen.

Processing Mask

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche im Bild der Verarbeitungsmaske als einzubeziehen (Analyze) oder auszuschließen (Ignore) markiert.
Size	Wählen Sie die Größe des Pinsels aus, den Sie im Bild der Verarbeitungsmaske verwenden.

Capacity

Einstellung	Beschreibung
Maximum Capacity	Verwenden Sie den Schieberegler, um die maximale Kapazität für die Szene zu definieren.

Calibration

Einstellung	Beschreibung
Type	Wählen Sie den Kalibrierungstyp aus. Manual ermöglicht Ihnen, die Kameraposition festzulegen. Automatic ermöglicht es der Videoanalyse Erkennung von Menschenmengen, Kameraposition und Sichtfeld festzulegen. Uncalibrated führt die Videoanalyse ohne Kameraposition und Sichtfeldinformationen aus.
Zoom In	Klicken Sie, um das Kalibrierungsdiagramm zu vergrößern.
Zoom Out	Klicken Sie, um die Kalibrierung zu verkleinern.
Field of view (degrees)	Definieren Sie das horizontale Sichtfeld (in Grad) für die Kamera.
Pan (degrees)	Definieren Sie die Drehung um die vertikale Achse der Kamera in Bezug auf die Szene.
Twist (degrees)	Definieren Sie die Drehung um die horizontale Achse der Kamera in Bezug auf die Szene.
Height (meters)	Definieren Sie den vertikalen Abstand der Kamera zum Boden.
Distance (meters)	Definieren Sie den horizontalen Abstand der Kamera zur Mitte der Szene.

Sensitivity

Einstellung	Beschreibung
Occupancy	Verwenden Sie den Schieberegler, um einzustellen, wie empfindlich die Videoanalyse Erkennung von Menschenmengen auf die von Personen besetzte Fläche reagiert.
Capacity	Verwenden Sie den Schieberegler, um einzustellen, wie empfindlich die Videoanalyse Erkennung von Menschenmengen auf die Anzahl der Personen in der Szene reagiert.

Bildstabilisierung

Die Videoanalyse Bildstabilisierung kann Videos stabilisieren, wenn eine Kamera Vibrationen oder anderen kleinen Bewegungen ausgesetzt ist.

Diese Videoanalyse ist nützlich, wenn Sie sie zur Ergänzung einer anderen Videoanalyse verwenden. Diese Videoanalyse erfordert keine Konfiguration.

Bildstabilisierung aktivieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Aktivieren Sie in der Liste Add-Ons die Option Image Stabilization.
4. Klicken Sie auf Save.

Indoor People Tracking

Die Videoanalyse Indoor People Tracking bietet Personenzählung, Verweilzeiterkennung, Ereignisauslösung und Alarmer.

Für die Personenzählung verwendet die Videoanalyse Indoor People Tracking Zähllinien, die Sie in die Szene zeichnen, um zu zählen, wie viele Personen die Szene passieren.

Die Videoanalyse Indoor People Tracking kann Personen erkennen, die 16 Pixel oder größer in der Szene sind.

+



+

Indoor People Tracking konfigurieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Aktivieren Sie in der Liste Add-Ons Indoor People Tracking und klicken Sie auf Configure.
4. Passen Sie die Einstellungen für die Videoanalyse Indoor People Tracking an. Die Konfiguration im Simple Mode verwendet die Standarderkennungseinstellungen für Indoor People Tracking. Um die Standardeinstellungen anzuzeigen, können Sie den Simple Mode deaktivieren, sodass die Standardeinstellungen im Abschnitt Advanced sichtbar werden.



Das Ändern der erweiterten Einstellungen kann die Leistung der Videoanalyse beeinträchtigen.

1. Klicken Sie auf OK.

Indoor People Tracking Einstellungen**Übersicht**

Einstellung	Beschreibung
Analysis Resolution	Legen Sie die Auflösung für die Kamera fest, an der die Videoanalyse Indoor People Tracking aktiv ist.
Automatically Select Resolution Based on Calibration	Auswählen, um die Analyseauflösung automatisch basierend auf den Einstellungen im Abschnitt Calibration festzulegen.
Analysis FPS	Legen Sie die Bilder pro Sekunde für die Kamera fest, an der die Videoanalyse Indoor People Tracking aktiv ist.
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen. Der einfache Modus ist der Standardmodus. Der erweiterte Modus ist für Systemintegratoren und technisches Support-Personal gedacht.

Verarbeitungsmaske

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche im Verarbeitungsmaskenbild markiert, die einbezogen (Analyze) oder ausgeschlossen (Ignore) werden sollen.
Size	Wählen Sie die Größe des Pinsels aus, den Sie im Verarbeitungsmaskenbild verwenden.

Zähllinie

Einstellung	Beschreibung
Create	Klicken und halten Sie auf dem Bild die linke Maustaste, bewegen Sie die Maus, um die neue Zähllinie zu zeichnen, und lassen Sie die linke Maustaste los.
Delete	Klicken Sie auf eine Zähllinie, um sie auszuwählen, und drücken Sie Entf.

Einstellung	Beschreibung
Move	Halten Sie die STRG-Taste gedrückt, klicken und halten Sie die linke Maustaste auf dem Endpunkt der Zähllinie und ziehen Sie den Endpunkt an die
Add a connected counting line	Klicken und halten Sie die linke Maustaste auf dem Endpunkt einer bestehenden Zähllinie, bewegen Sie die Maus, um die neue Zähllinie zu zeichnen, und lassen Sie die linke Maustaste los.
Change the counting direction	Klicken Sie auf einen Pfeil auf der Zähllinie, um die Zählung für diese Richtung ein- bzw. auszuschalten.

Kalibrierung

Einstellung	Beschreibung
Type	Wählen Sie den Kalibrierungstyp aus. Mit Manual können Sie die Kameraposition festlegen. Mit Automatic kann die Videoanalyse Indoor People Tracking die Kameraposition und das Sichtfeld festlegen. Mit Uncalibrated wird die Videoanalyse Indoor People Tracking ohne Informationen zur Kameraposition und zum Sichtfeld ausgeführt.
Zoom In	Klicken, um das Kalibrierungsdiagramm zu vergrößern.
Zoom Out	Klicken, um die Kalibrierung zu verkleinern.
Field of view (degrees)	Definieren Sie das horizontale Sichtfeld (in Grad) für die Kamera.
Pan (degrees)	Definieren Sie die Drehung um die vertikale Achse der Kamera in Bezug auf die Szene.
Twist (degrees)	Definieren Sie die Drehung um die horizontale Achse der Kamera in Bezug auf die Szene.
Height (meters)	Definieren Sie den vertikalen Abstand von der Kamera zum Boden.
Distance (meters)	Definieren Sie den horizontalen Abstand von der Kamera zur Mitte der Szene.

Empfindlichkeit

Dieser Abschnitt ist nur im einfachen Modus sichtbar.

Einstellung	Beschreibung
Object Contrast	Verwenden Sie den Schieberegler, um festzulegen, wie empfindlich die Videoanalyse Indoor People Tracking auf den Kontrast zwischen Objekten und dem Hintergrund reagiert.
Object Motion	Verwenden Sie den Schieberegler, um festzulegen, wie empfindlich die Videoanalyse Indoor People Tracking auf die Bewegung von Objekten reagiert.
Background Motion	Verwenden Sie den Schieberegler, um festzulegen, wie empfindlich die Videoanalyse Indoor People Tracking auf Bewegungen im Hintergrund reagiert.
Shadow Suppression	Wählen Sie diese Option aus, damit die Videoanalyse Indoor People Tracking das Vorhandensein und die Bewegung von Schatten ignoriert.

Erkennung von zurückgelassenen und entwendeten Gegenständen

Die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen kann erkennen, wenn ein Objekt zur Szene hinzugefügt oder daraus entfernt wird.

Die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen unterscheidet nicht zwischen zurückgelassenen und entwendeten Gegenständen. Die Videoanalyse vergleicht die Pixel in der Szene mit den Pixeln in vorherigen Szenen und verwendet Tracking-Rahmen, um die Bereiche mit Änderungen zu identifizieren.

Erkennung von zurückgelassenen und entwendeten Gegenständen konfigurieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Aktivieren Sie in der Liste Add-Ons Left and Removed Item Detection und klicken Sie auf Configure.
4. Passen Sie die Einstellungen für die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen an. Die Konfiguration im Simple Mode verwendet die Standarderkennungseinstellungen für die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen. Um die Standardeinstellungen anzuzeigen, können Sie den Simple Mode deaktivieren, sodass die Standardeinstellungen im Abschnitt Advanced sichtbar werden.



Das Ändern der erweiterten Einstellungen kann die Leistung der Videoanalyse beeinträchtigen.

1. Klicken Sie auf OK.

Einstellungen für Erkennung von zurückgelassenen und entwendeten Gegenständen

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Legen Sie die Auflösung für die Kamera fest, an der die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen aktiv ist.
Automatically Select Resolution Based on Calibration	Auswählen, um die Analyseauflösung automatisch basierend auf den Einstellungen im Abschnitt Calibration festzulegen.
Analysis FPS	Legen Sie die Bilder pro Sekunde für die Kamera fest, an der die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen aktiv ist.
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen. Der einfache Modus ist der Standardmodus. Der erweiterte Modus ist für Systemintegratoren und technisches Support-Personal gedacht.

Verarbeitungsmaske

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche im Verarbeitungsmaskenbild markiert, die einbezogen (Analyze) oder ausgeschlossen (Ignore) werden sollen.
Size	Wählen Sie die Größe des Pinsels aus, den Sie im Verarbeitungsmaskenbild verwenden.

Kalibrierung

Einstellung	Beschreibung
Zoom In	Klicken, um das Kalibrierungsdiagramm zu vergrößern.
Zoom Out	Klicken, um die Kalibrierung zu verkleinern.
Field of view (degrees)	Definieren Sie das horizontale Sichtfeld (in Grad) für die Kamera.
Pan (degrees)	Definieren Sie die Drehung um die vertikale Achse der Kamera in Bezug auf die Szene.
Twist (degrees)	Definieren Sie die Drehung um die horizontale Achse der Kamera in Bezug auf die Szene.
Height (meters)	Definieren Sie den vertikalen Abstand von der Kamera zum Boden.
Distance (meters)	Definieren Sie den horizontalen Abstand von der Kamera zur Mitte der Szene.

Erweitert

Die erweiterten Einstellungen sind sichtbar, wenn der einfache Modus deaktiviert ist.



Änderungen der erweiterten Einstellungen können die Leistung der Videoanalyse beeinträchtigen.

Einstellung	Beschreibung
Left item duration	Legen Sie die Zeit (Sekunden) fest, die ein Objekt vorhanden oder fehlend sein muss, bevor die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen es als zurückgelassen oder entwendet betrachtet. Die Standardeinstellung ist 15 Sekunden.
Check for object drop-off	Wählen Sie aus, ob die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen Gegenstände ignoriert, die eine Person aufnimmt oder ablegt. Die Standardeinstellung ist ausgewählt.
Initial background model learn time	Legen Sie die Zeit (Sekunden) fest, die die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen benötigt, um den Hintergrund der Szene zu lernen. Während dieser Zeit versucht die Videoanalyse nicht, Objekte zu erkennen. Die Standardeinstellung ist 1 Sekunde.
Reach width	Legen Sie die Entfernung (Pixel) fest, die eine Person in einem Einzelhandelsgeschäft benötigt, um den Gegenstand zu erreichen. Die Standardeinstellung ist 9 Pixel.
Object merge distance	Legen Sie die Entfernung (Pixel) fest, bei der die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen zwei Objekte zu einem Objekt zusammenführt. Die Standardeinstellung ist 20 Pixel.

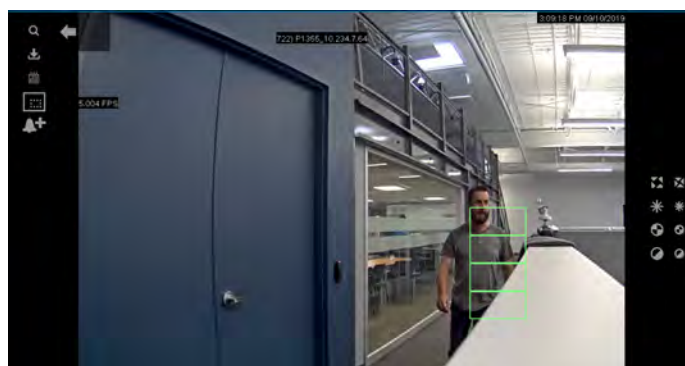
Einstellung	Beschreibung
Reduce false alarms from still people	Wählen Sie aus, ob die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen wartet, um Personen in der Szene als zurückgelassenen oder entwendeten Gegenstand zu erkennen. Diese Einstellung verwendet die Einstellung Time to wait for still people. Die Standardeinstellung ist falsch.
Time to wait for still people	Legen Sie fest, wie lange (Sekunden) die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen wartet, um Personen in der Szene zu erkennen. Diese Einstellung wird durch Auswählen der Einstellung Reduce false alarms from still people aktiviert. Die Standardeinstellung ist 60 Sekunden.
Appearance	
Lower bound	
Upper bound	
Reduce reflection	Wählen Sie aus, ob die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen versucht, Reflexionen zu ignorieren.
Reflection reduction threshold	Legen Sie fest, wie empfindlich die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen auf Reflexionen reagiert. Ein niedrigerer Wert führt dazu, dass die Videoanalyse mehr Reflexionen ignoriert. Ein höherer Wert führt dazu, dass die Videoanalyse mehr Reflexionen verarbeitet.
Camera looking at shelf	Auswählen, wenn die Kamera auf ein Regal gerichtet ist. Diese Einstellung ist nur aktiv, wenn Sie Check for object drop-off auswählen.
Time to clear long-term representation	Legen Sie fest, wie lange (Sekunden) es dauert, bis die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen den Hintergrund löscht.
Time to clear short-term representation	Legen Sie fest, wie lange (Sekunden) es dauert, bis die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen den Cache löscht.
Minimum fill rate	Legen Sie den Prozentsatz des kleinsten Begrenzungsrahmens des Gegenstands fest, den der Gegenstand füllen muss, damit die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen ihn als Gegenstand betrachtet. Der Standardwert ist 10.
Time to remove or drop an item	Legen Sie fest, wie lange (Sekunden) ein Gegenstand vorhanden sein muss, bevor die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen mit der Verarbeitung des Gegenstands beginnt. Eine längere Zeit reduziert die Verarbeitungslast der Videoanalyse.
Background reset time after an object is deleted	Legen Sie fest, wie lange (Sekunden) die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen wartet, bevor sie ein Objekt löscht.

Einstellung	Beschreibung
Minimum valid object dimension	Legen Sie fest, wie groß (Pixel) ein Gegenstand sowohl in der Höhe als auch in der Breite sein muss und wie weit ein Gegenstand vom Rand der Szene entfernt sein muss, damit die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen den Gegenstand als zurückgelassen oder entwendet betrachtet.
Reset camera if this percentage of image becomes foreground in 1 frame	Legen Sie den Prozentsatz des Bildes fest, der sich in einem einzigen Frame ändern muss, bevor die Kamera den Hintergrund zurücksetzt. Dies verhindert, dass die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen plötzliche große Änderungen als Gegenstände betrachtet.
Reset camera if this percentage of image becomes foreground in 5 frames	Legen Sie den Prozentsatz des Bildes fest, der sich in fünf Frames ändern muss, bevor die Kamera den Hintergrund zurücksetzt. Dies verhindert, dass die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen allmähliche große Änderungen als Gegenstände betrachtet.
Merge small objects closer than	Legen Sie die Entfernung (Pixel) zwischen zwei Gegenständen fest, bei der die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen die beiden Gegenstände zu einem einzigen Gegenstand zusammenführt. Der Standardwert ist 8.
Grayscale background update rate	Legen Sie die Rate fest, mit der die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen das Hintergrundbild aktualisiert. Ein niedrigerer Wert erfasst mehr zurückgelassene und entwendete Gegenstände, erhöht aber die Verarbeitungslast. Der Standardwert ist 5.

Bewegungserkennung

Die Videoanalyse Bewegungserkennung bietet Bewegungserkennung, Ereignisauslösung und Alarmer. Die Videoanalyse Bewegungserkennung erkennt Pixeländerungen in der Szene.

+



+

Bewegungserkennung konfigurieren

Was es ist

Die Videoanalyse Bewegungserkennung markiert Pixeländerungen im Videostream einer Kamera als Bewegungsereignisse. Diese Ereignisse werden in die [Regel-Engine](#) eingespeist, sodass Sie Bewegung als Auslöser für Aufzeichnung, Alarme oder Aktionen verwenden können.

Bewegungserkennung ist im Vergleich zu klassifikationsbasierten Analysen ([Verfolgung von Personen und Fahrzeugen im Außenbereich](#), [Senstar Symphony AI Object Detection and Tracking](#)) ressourcenschonend. Sie erkennt, **dass** sich etwas bewegt hat, nicht **was** sich bewegt hat. Wenn Sie zwischen Personen und Fahrzeugen unterscheiden oder Wildtiere herausfiltern müssen, verwenden Sie stattdessen eine klassifikationsbasierte Analyse.

Wann Sie es verwenden

- Eine Kamera muss nur aufzeichnen, wenn sich etwas in der Szene bewegt (bewegungsgesteuerte Aufzeichnung zur Reduzierung des Speicherbedarfs).
- Sie möchten einen einfachen Alarm "Etwas hat sich nach Feierabend bewegt" auf einer wenig frequentierten Kamera.
- Eine Szene ist zu einfach oder die Ressourcen zu knapp, um eine klassifikationsbasierte Analyse zu rechtfertigen.

Verwenden Sie sie nicht allein für Szenen mit hohen Falschalarmraten (Laub im Wind, Schnee, Regen, vorbeifahrender Verkehr außerhalb des interessierenden Bereichs) — passen Sie die Verarbeitungsmaske an, um diese Bereiche auszuschließen, oder wechseln Sie zu einer klassifikationsbasierten Analyse.

Voraussetzungen

- Berechtigung zur Bearbeitung von Kameraeinstellungen.
- Eine bereits zum Server hinzugefügte Kamera. Siehe [Kamera hinzufügen](#).
- Hinweise zur Bedeutung der einzelnen Felder finden Sie unter [Einstellungen der Bewegungserkennung](#).

Vorgehen

1. Klicken Sie in der Konfigurationsoberfläche des Server auf **Devices > Cameras**.
2. Wählen Sie die Kamera aus und klicken Sie auf **Edit**.
3. Aktivieren Sie in der Liste **Add-Ons** die Option **Motion Detection** und klicken Sie auf **Configure**.
4. Passen Sie folgendes an:
 - **Sensitivity** — wie viel Pixeländerung als Bewegung gezählt wird. Beginnen Sie mit dem Standardwert, erhöhen Sie ihn, wenn echte Bewegung übersehen wird, oder verringern Sie ihn, wenn die Analyse durch Rauschen ausgelöst wird (Beleuchtungsänderungen, Komprimierungsartefakte).
 - **Processing mask** — markieren Sie die Bildbereiche, die die Analyse ignorieren soll. Maskieren Sie sich bewegendes Laub, Flaggen, Wasser, irrelevante Straßen sowie Datums-/Zeit-Overlays, die sich jede Sekunde ändern.
 - **Minimum object size** — filtern Sie kleine Pixeländerungen heraus, die zu klein sind, um die für Sie relevanten Objekte zu sein.

Eine vollständige Feldreferenz finden Sie unter [Einstellungen der Bewegungserkennung](#).

5. Klicken Sie auf **OK**.

6. Klicken Sie auf der Kamera auf **Save**, um die Änderung zu übernehmen.

Tipps zur Anpassung

- Optimieren Sie unter den schlechtesten Bedingungen der Szene — Nacht, schlechtes Wetter, Spitzenaktivität — nicht an einem ruhigen Nachmittag.
- Beobachten Sie nach der Anpassung das Ereignisprotokoll für ein bis zwei Schichten (**Ereignisse anzeigen**), um zu bestätigen, dass die Falschalarmrate akzeptabel ist.
- Wenn Sie mit Bewegungserkennung allein nicht sowohl gute Erkennung als auch eine geringe Falschalarmrate erreichen können, wechseln Sie zu einer klassifikationsbasierten Analyse.

Verwandte Aufgaben

- **Bewegungserkennung** — Übersicht über die Analyse.
- **Einstellungen der Bewegungserkennung** — vollständige Feldreferenz.
- **Ereigniseinstellungen der Bewegungserkennung** — Verwendung von Bewegungsereignissen in Regeln.
- **Verarbeitungsmaske zeichnen**

Einstellungen für Bewegungserkennung

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Legen Sie die Auflösung für die Kamera fest, an der die Videoanalyse Bewegungserkennung aktiv ist.
Analysis FPS	Legen Sie die Bilder pro Sekunde für die Kamera fest, an der die Videoanalyse Bewegungserkennung aktiv ist.
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen.

Verarbeitungsmaske

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche im Verarbeitungsmaskenbild markiert, die einbezogen (Analyse) oder ausgeschlossen (Ignore) werden sollen.
Size	Wählen Sie die Größe des Pinsels aus, den Sie im Verarbeitungsmaskenbild verwenden.

Rasteransicht

Einstellung	Beschreibung
Minimum Foreground Fill (percent)	Verwenden Sie den Schieberegler, um zu definieren, welcher Prozentsatz eines Rasterquadrats sich ändern muss, damit die Videoanalyse Bewegungserkennung in diesem Rasterquadrat eine Erkennung durchführt.
Grid Spacing	Verwenden Sie den Schieberegler, um die Größe der Rasterquadrate zu definieren.
Foreground Sensitivity	Verwenden Sie den Schieberegler, um zu definieren, wie empfindlich die Videoanalyse Bewegungserkennung auf Bewegungen bei der Bestimmung der Vordergrundfüllung reagiert.

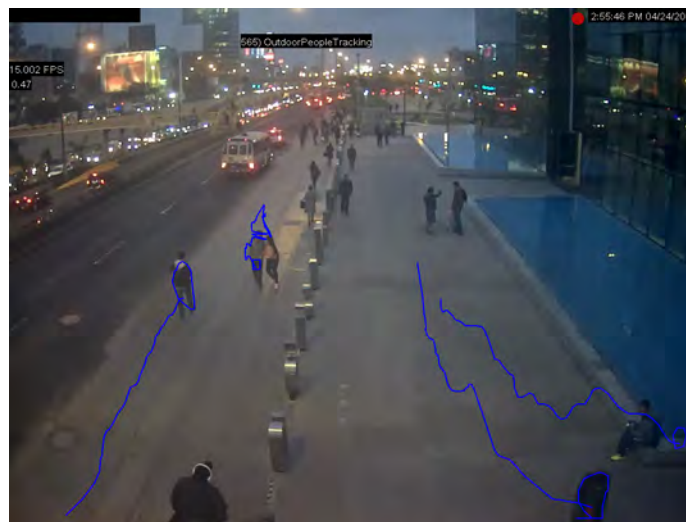
Einstellung	Beschreibung
Adjust sensitivity based on camera noise	Auswählen, um die Vordergrundempfindlichkeit automatisch zu ändern, um zufällige Schwankungen oder Helligkeit oder Farbe von der Kamera zu berücksichtigen.

Verfolgung von Personen und Fahrzeugen im Außenbereich

Die Videoanalyse "Verfolgung von Personen und Fahrzeugen im Außenbereich" ermöglicht die Erkennung von Personen und Fahrzeugen in Außenumgebungen mit wechselnden Wetter- und Lichtverhältnissen.

Die Videoanalyse "Verfolgung von Personen und Fahrzeugen im Außenbereich" kann Objekte in der Szene erkennen, die 8 Pixel oder größer sind.

+



+

Verfolgung von Personen und Fahrzeugen im Außenbereich konfigurieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Aktivieren Sie in der Liste Add-Ons Outdoor People and Vehicle Tracking und klicken Sie auf Configure.
4. Passen Sie die Einstellungen für die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich an. Die Konfiguration im Simple Mode verwendet die Standarderkennungseinstellungen für die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich. Um die Standardeinstellungen anzuzeigen, können Sie den Simple Mode deaktivieren, sodass die Standardeinstellungen im Abschnitt Advanced sichtbar werden.



Das Ändern der erweiterten Einstellungen kann die Leistung der Videoanalyse beeinträchtigen.

1. Klicken Sie auf Save.

Einstellungen für Verfolgung von Personen und Fahrzeugen im Außenbereich

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Legen Sie die Auflösung für die Kamera fest, an der die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich aktiv ist.
Automatically Select Resolution Based on Calibration	Auswählen, um die Analyseauflösung automatisch basierend auf den Einstellungen im Abschnitt Calibration festzulegen.
Analysis FPS	Legen Sie die Bilder pro Sekunde für die Kamera fest, an der die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich aktiv ist.
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen.

Verarbeitungsmaske

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche im Verarbeitungsmaskenbild markiert, die einbezogen (Analyze) oder ausgeschlossen (Ignore) werden sollen.
Size	Wählen Sie die Größe des Pinsels aus, den Sie zum Zeichnen auf dem Verarbeitungsmaskenbild verwenden.

Kalibrierung

Einstellung	Beschreibung
Type	Wählen Sie den Kalibrierungstyp aus. Mit Manual können Sie die Kameraposition festlegen. Mit Automatic kann die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich die Kameraposition und das Sichtfeld festlegen. Mit Uncalibrated wird die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich ohne Informationen zur Kameraposition und zum Sichtfeld ausgeführt.
Zoom In	Klicken, um das Kalibrierungsdiagramm zu vergrößern.
Zoom Out	Klicken, um die Kalibrierung zu verkleinern.
Field of view (degrees)	Definieren Sie das horizontale Sichtfeld (in Grad) für die Kamera.
Pan (degrees)	Definieren Sie die Drehung um die vertikale Achse der Kamera in Bezug auf die Szene.
Twist (degrees)	Definieren Sie die Drehung um die horizontale Achse der Kamera in Bezug auf die Szene.
Height (meters)	Definieren Sie den vertikalen Abstand von der Kamera zum Boden.
Distance (meters)	Definieren Sie den horizontalen Abstand von der Kamera zur Mitte der Szene.

Empfindlichkeit

Die Empfindlichkeitseinstellungen sind sichtbar, wenn der einfache Modus aktiviert ist.

Einstellung	Beschreibung
Object Contrast	Verwenden Sie den Schieberegler, um festzulegen, wie empfindlich die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich auf Unterschiede zwischen Objekten und dem Hintergrund reagiert.
Object Motion	Verwenden Sie den Schieberegler, um festzulegen, wie empfindlich die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich auf Vordergrundbewegungen bei der Objekterkennung reagiert.
Background Motion	Verwenden Sie den Schieberegler, um festzulegen, wie empfindlich die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich auf Hintergrundbewegungen bei der Objekterkennung reagiert.
Shadow Suppression (Simple)	Auswählen, um die einfache Schattenunterdrückung zu verwenden. Die einfache Schattenunterdrückung ist wirksam, wenn helle Schatten in der Szene vorhanden sind.  Verwenden Sie die Schattenunterdrückung nicht mit Wärmebildkameras.
Shadow Suppression (Complex)	Auswählen, um die komplexe Schattenunterdrückung zu verwenden. Die komplexe Schattenunterdrückung ist wirksam, wenn dunkle Schatten in der Szene vorhanden sind.  Verwenden Sie die Schattenunterdrückung nicht mit Wärmebildkameras.
Snow Suppression	Auswählen, damit die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich die Bewegung von Schnee in der Szene ignoriert.
Dynamic Background	Auswählen, damit die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich periodische Bewegungen in der Szene ignoriert. Diese Einstellung ist wirksam für Außenszenen, in denen das Wetter Bewegungen im Hintergrund verursachen kann.
Detect Distant Objects	Auswählen, damit die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich versucht, Objekte in der Ferne zu erkennen.

Automatische PTZ-Verfolgung

Die Videoanalyse "Automatische PTZ-Verfolgung" kann PTZ-Kameras automatisch steuern, wenn Aktivität erkannt wird.

Die Videoanalyse "Automatische PTZ-Verfolgung" setzt voraus, dass die Videoanalyse "Indoor People Tracking" oder die Videoanalyse "Verfolgung von Personen und Fahrzeugen im Außenbereich" auf der Kamera aktiv ist. Sie können die Videoanalyse "Automatische PTZ-Verfolgung" als Aktion für eine Regel hinzufügen.

Automatische PTZ-Verfolgung konfigurieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Aktivieren und konfigurieren Sie für die Kamera entweder die Videoanalyse Indoor People Tracking

oder die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich.

4. Aktivieren Sie in der Liste Add-Ons PTZ Auto-Tracking und klicken Sie auf Configure.
5. Konfigurieren Sie die Videoanalyse.
6. Klicken Sie auf Save.

Einstellungen für automatische PTZ-Verfolgung

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Legen Sie die Auflösung für die Kamera fest, auf der die automatische PTZ-Verfolgung aktiv ist.
Analysis FPS	Legen Sie die Bilder pro Sekunde für die Kamera fest, auf der die Videoanalyse "Automatische PTZ-Verfolgung" aktiv ist.
Simple Mode	Wählen Sie, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden. Der einfache Modus ist der Standardmodus. Der erweiterte Modus ist für Systemintegratoren und technisches Support-Personal gedacht.

Gesichtserkennung

Die Videoanalyse Gesichtserkennung bietet Gesichtserkennung, Ereignisauslösung und Alarme.

Die Videoanalyse Gesichtserkennung verwendet Profile zur Darstellung von Personen. Jedes Profil kann mehrere Bilder des Gesichts einer Person enthalten. Verwenden Sie die Oberfläche des Windows Client, um Profile zu erstellen, Gesichtsbilder hinzuzufügen und festzulegen, ob das Profil gesperrt oder zugelassen ist. Wenn die Videoanalyse Gesichtserkennung ein Gesicht in einem Video identifiziert, kann sie Ereignisse auf dem Server auslösen.

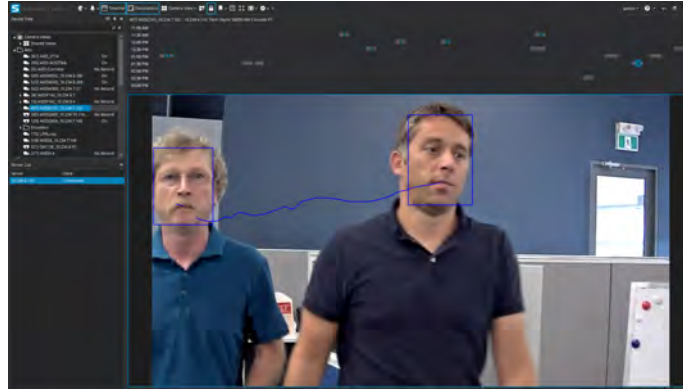
Die Videoanalyse Gesichtserkennung kann Gesichter erkennen, wenn der Abstand zwischen den Augen mehr als 29 Pixel beträgt, und funktioniert am besten, wenn die Auflösung der Kamera mindestens 640 x 480 beträgt.

Die Videoanalyse Gesichtserkennung umfasst die Erkennung von Spoofing-Angriffen. Die Videoanalyse kann den Unterschied zwischen Bildern von Gesichtern und echten Gesichtern erkennen. Sie können die Spoofing-Angriffserkennung verwenden, um Alarme zu generieren, wenn die Videoanalyse gefälschte Gesichter erkennt.



Die Videoanalyse Gesichtserkennung kann nicht gleichzeitig Alarme für echte und gefälschte Gesichter generieren. Sie müssen zwei Regeln erstellen, um Alarme für beide zu generieren.

In der Oberfläche des Windows Client umgibt ein blaues Quadrat ein verfolgtes Gesicht und ein rotes Quadrat umgibt ein verfolgtes Gesicht, das einen Alarm auslöst.



Gesichtserkennung konfigurieren

Was es ist

Die Videoanalyse Gesichtserkennung erkennt Gesichter im Videostream einer Kamera und gleicht sie mit einer Datenbank registrierter Gesichter ab. Treffer steuern [Regeln](#) und erscheinen im [Gesichtserkennungsbericht](#).

Gesichtserkennung ist ressourcenintensiv. Sie eignet sich für eine geringe Anzahl von Kameras, die an Stellen platziert sind, an denen Personen durch ein bekanntes Sichtfeld passieren (Eingänge, Drehkreuze, Engstellen), und nicht für die allgemeine Flächenüberwachung.

Wann Sie es verwenden

- Beobachten bekannter Personen von Interesse an Gebäudeeingängen.
- Erzeugen von Alarmen, wenn ein VIP oder eine gesperrte Person auf Kamera erscheint.
- Erstellen eines Berichts darüber, wer wo und wann gesehen wurde.

Aktivieren Sie die Gesichtserkennung nicht auf Kameras, bei denen die Gesichtsgröße zu klein, der Winkel zu steil oder das Sichtfeld zu weit ist — Erkennungs- und Trefferqualität brechen unter diesen Bedingungen zusammen.

Über die Spoof-Angriffserkennung

Ein Spoof-Angriff ist ein Versuch, die Gesichtserkennung zu täuschen, indem der Kamera ein Foto, eine bedruckte Maske oder eine Videowiedergabe des Gesichts einer anderen Person präsentiert wird. Die Spoof-Angriffserkennung analysiert das präsentierte Gesicht auf Lebendigkeitsmerkmale, sodass ein Foto oder Bildschirm seltener einen Treffer erzeugt.

- **Aktivieren** Sie die Spoof-Angriffserkennung, wenn die Kamera einen hochwertigen Vermögenswert schützt und die zusätzlichen Verarbeitungskosten akzeptabel sind.
- **Deaktivieren** Sie sie, wenn die Verarbeitungskapazität knapp ist und das Spoofing-Risiko gering ist (z. B. eine Decken- oder Fernkamera, bei der das Vorzeigen eines Fotos unplausibel ist).

Über die Verarbeitungsmaske

Die Verarbeitungsmaske teilt der Analyse mit, welche Bildbereiche analysiert werden sollen. Maskieren Sie Bereiche aus, in denen Gesichter nicht plausibel auftreten können (Himmel, Boden, Wände, gedruckte Schilder mit gesichtsähnlichen Mustern). Alles innerhalb der Maske wird ignoriert — die Analyse sucht oder erkennt dort keine Gesichter.

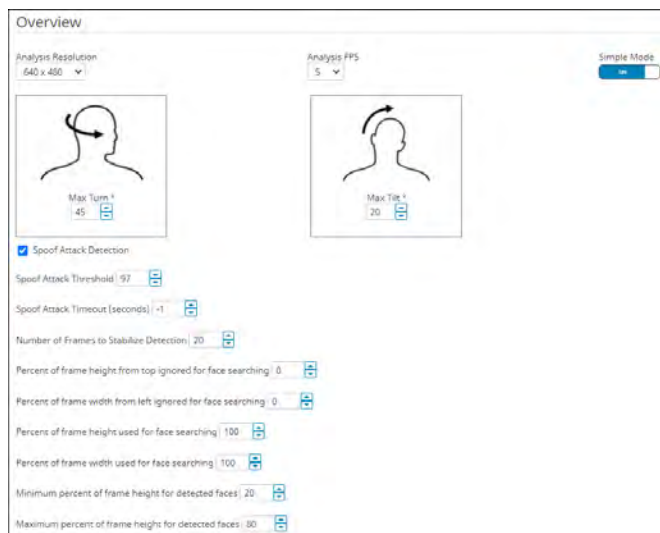
Voraussetzungen

- Berechtigung zur Bearbeitung von Kameraeinstellungen.

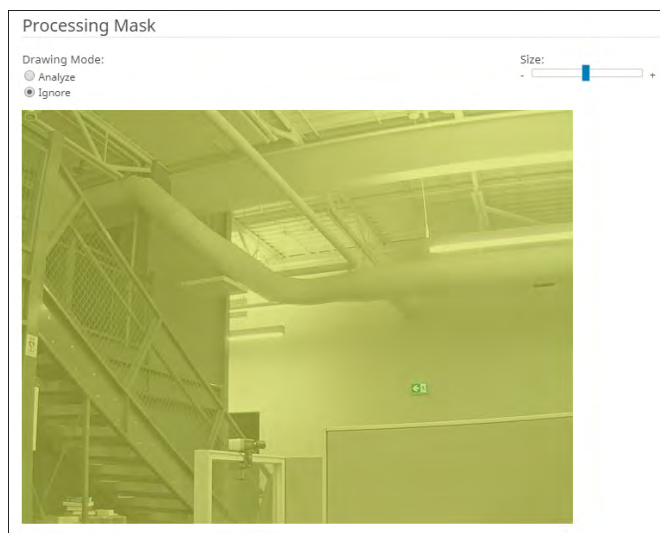
- Eine bereits hinzugefügte Kamera. Siehe [Kamera hinzufügen](#).
- Ausreichend GPU/CPU-Reserven auf dem Server für die Gesichtserkennung bei der geplanten Anzahl von Kameras.
- Eine Datenbank registrierter Gesichter (siehe die Funktionsseiten zur Gesichtserkennung).

Vorgehen

1. Klicken Sie in der Konfigurationsoberfläche des Server auf **Devices > Cameras**.
2. Wählen Sie die Kamera aus und klicken Sie auf **Edit**.
3. Aktivieren Sie in der Liste **Add-Ons** die Option **Face Recognition** und klicken Sie auf **Configure**.
4. Stellen Sie im Abschnitt **Overview** die Erkennungsparameter ein: den Gesichtssuchrahmen (den Bildbereich, in dem die Gesichtserkennung nach Gesichtern sucht) und die Einstellungen für die Spoof-Angriffserkennung.



5. Markieren Sie im Abschnitt **Processing Mask** die Bereiche, die die Analyse ignorieren soll.



Jeder von der Verarbeitungsmaske abgedeckte Bereich wird ignoriert. Wenn ein

Gesicht in einem maskierten Bereich erscheint, wird es weder erkannt noch identifiziert.

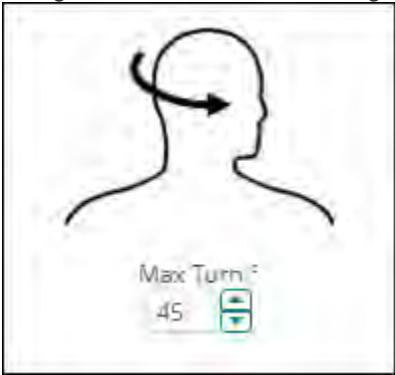
- 6. Klicken Sie auf **OK**.
- 7. Klicken Sie auf **Save**.

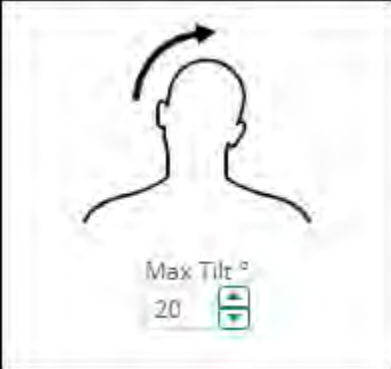
Verwandte Aufgaben

- Gesichtserkennung — Übersicht über die Analyse.
- Einstellungen der Gesichtserkennung — vollständige Feldreferenz.
- Ereignisseinstellungen der Gesichtserkennung — Verwendung von Gesichtserkennungseignissen in Regeln.
- Gesichtserkennungsbericht

Einstellungen für Gesichtserkennung

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Legen Sie die Auflösung für die Kamera fest, an der die Videoanalyse Gesichtserkennung aktiv ist.
Analysis FPS	Legen Sie die Bilder pro Sekunde für die Kamera fest, an der die Videoanalyse Gesichtserkennung aktiv ist.
Face Confidence Threshold	Legen Sie fest, wie sicher die Videoanalyse Gesichtserkennung sein muss, dass Objekte Gesichter sind, bevor sie Objekte verfolgt.
Max Turn	Legen Sie den horizontalen Winkel (in Grad) von der Mitte fest, in dem die Videoanalyse Gesichtserkennung keine Objekte verfolgt. Der empfohlene Wert ist 45 Grad oder weniger. Der maximale Wert beträgt 70 Grad. + 

Einstellung	Beschreibung
Max Tilt	Legen Sie den vertikalen Winkel (in Grad) von der Mitte fest, in dem die Videoanalyse Gesichtserkennung keine Objekte verfolgt. Der empfohlene Wert ist 20 Grad oder weniger. Der maximale Wert beträgt 45 Grad. + 
Spoof Attack Detection	Auswählen, um die Erkennung von Spoofing-Angriffen zu aktivieren. Diese Einstellung ist standardmäßig deaktiviert.
Spoof Attack Threshold	Legen Sie fest, wie sicher die Videoanalyse sein muss, dass ein Gesicht gefälscht ist, um eine Regel auszulösen. Diese Einstellung wird sichtbar, wenn Sie Spoof Attack Detection auswählen. Der Wertebereich liegt zwischen 0 und 100. Der Standardwert ist 99.
Spoof Attack Timeout (seconds)	Legen Sie fest, wie lange die Videoanalyse wartet, bevor der Spoofing-Angriffsstatus zurückgesetzt wird. Diese Einstellung wird sichtbar, wenn Sie Spoof Attack Detection auswählen. Der Bereich für diese Einstellung liegt zwischen -1 (kein Timeout) und 100. Der Standardwert ist -1 (kein Timeout).
Number of Frames to Stabilize Detection	Legen Sie die Anzahl der Frames fest, für die die Videoanalyse von einem gefälschten Gesicht überzeugt sein muss, um eine Regel auszulösen. Diese Einstellung wird sichtbar, wenn Sie Spoof Attack Detection auswählen. Der Bereich für diese Einstellung liegt zwischen 1 und 100. Der Standardwert ist 10.
Percent of frame height from top ignored for face searching	Definieren Sie den Bereich am oberen Rand des Bildes, den die Videoanalyse ignoriert, als Prozentsatz der Höhe des Beispielsbildes.
Percent of frame width from left ignored for face searching	Definieren Sie den Bereich auf der linken Seite des Bildes, den die Videoanalyse ignoriert, als Prozentsatz der Breite des Beispielsbildes.
Percent of frame height used for face searching	Definieren Sie die Höhe des Bereichs, in dem die Videoanalyse versucht, Gesichter zu erkennen, als Prozentsatz der Höhe des Beispielsbildes. Dieser Prozentsatz wird nach dem ignorierten Prozentsatz angewendet.

Einstellung	Beschreibung
Percent of frame width used for face searching	Definieren Sie die Breite des Bereichs, in dem die Videoanalyse versucht, Gesichter zu erkennen, als Prozentsatz der Breite des Beispielbildes. Dieser Prozentsatz wird nach dem ignorierten Prozentsatz angewendet.
Minimum percentage of frame height for detected faces	Definieren Sie die Mindestgröße eines Gesichts, das die Videoanalyse erkennen soll, als Prozentsatz des Beispielbildes.
Maximum percent of frame height for detected faces	Definieren Sie die maximale Größe eines Gesichts, das die Videoanalyse erkennen soll, als Prozentsatz des Beispielbildes.

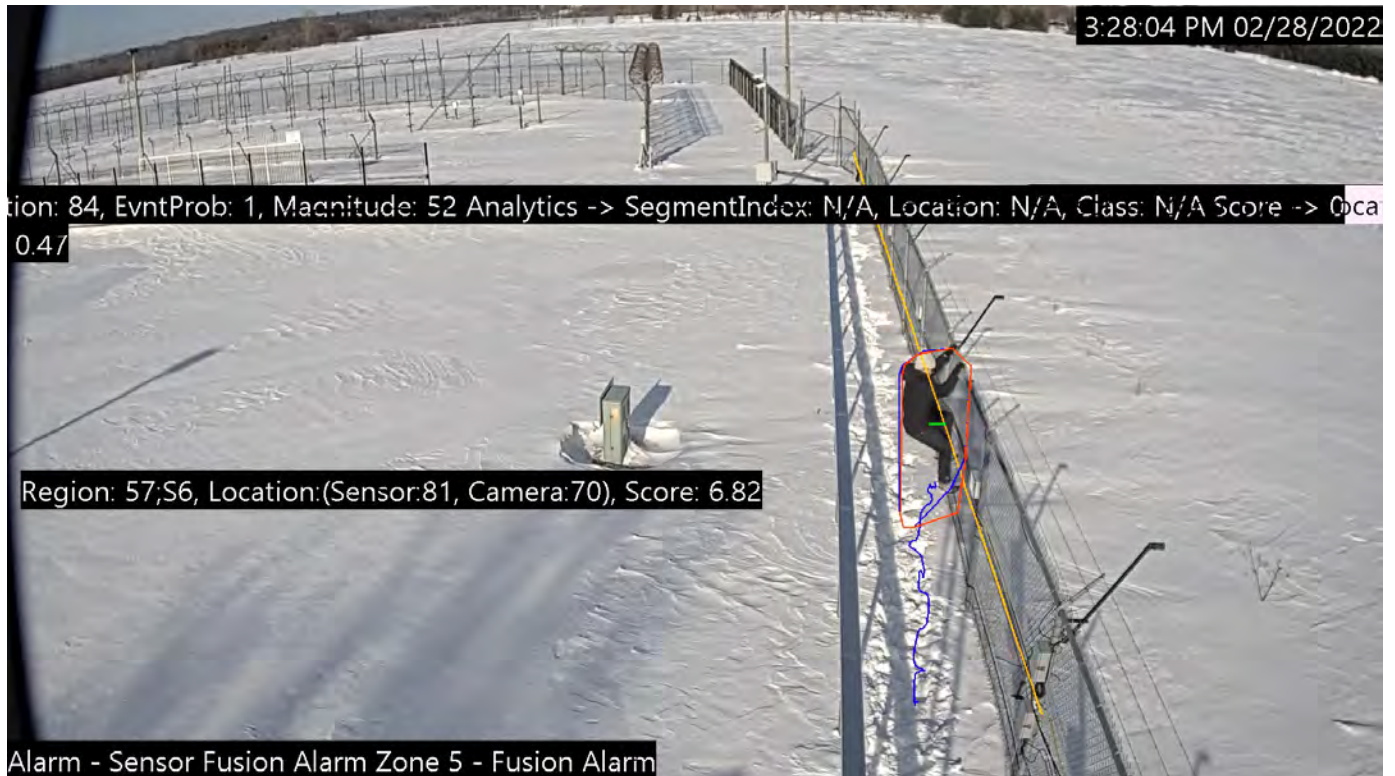
Verarbeitungsmaske

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche im Verarbeitungsmaskenbild markiert, die einbezogen (Analyze) oder ausgeschlossen (Ignore) werden sollen.
Size	Wählen Sie die Größe des Pinsels aus, den Sie im Verarbeitungsmaskenbild verwenden.

Senstar Sensor Fusion

Senstar Sensor Fusion kombiniert die Daten eines Perimeter-Eindringungserkennungssystems mit einer dedizierten Videoanalyse, um die Perimeter-Eindringungserkennung erheblich zu verbessern und gleichzeitig Fehlalarme der einzelnen Sensoren zu reduzieren.

Senstar Sensor Fusion verwendet eine Videoanalyse, um Objekte in der Nähe des Zauns zu analysieren, und korreliert die Ergebnisse mit Daten des Perimeter-Eindringungserkennungssystems. Senstar Sensor Fusion berechnet eine Wahrscheinlichkeit aus der Videoanalyse (Daten einschließlich Zeit, Objektklassifizierung, Verlauf und Standort) und dem Perimeter-Eindringungserkennungssystem (Daten einschließlich Zeit, Standort, Stärke und Frequenz) und verwendet diese Wahrscheinlichkeit, um einen Alarm mit höherer Genauigkeit auszulösen, als wenn jedes System einzeln Alarme auslöst.



Darüber hinaus bietet Senstar Sensor Fusion Redundanz, falls eine der Komponenten ausfällt. Wenn eine Komponente ausfällt, verlagert Senstar Sensor Fusion das Gewicht der Wahrscheinlichkeit auf die funktionierende Komponente und löst Alarme basierend auf dieser Wahrscheinlichkeit aus.

Senstar Sensor Fusion unterstützt derzeit die folgende Senstar-Perimeter-Eindringungserkennungstechnologie:

- Senstar FlexZone

Senstar Sensor Fusion konfigurieren

Konfigurieren Sie Senstar Sensor Fusion in der Konfigurationsoberfläche des Server.

Informationen zu spezifischen Einstellungen von Senstar Sensor Fusion finden Sie im Thema [Einstellungen Senstar Sensor Fusion](#).

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Aktivieren Sie in der Liste Add-Ons Senstar Sensor Fusion und klicken Sie auf Configure.
image::vis_fusion_configure_01.png[]
4. Konfigurieren Sie im Abschnitt Overview die Auflösung und FPS für die Kamera.
5. Legen Sie im Abschnitt Processing Mask die Bereiche im Bild fest, die die Kamera ignoriert oder analysiert. image::vis_fusion_configure_processing_mask.png[]
6. Kalibrieren Sie im Abschnitt Calibration die Kamera auf die Szene. Wählen Sie Automatic, damit die Videoanalyse Kameraposition und Sichtfeldinformationen automatisch ermittelt.

Wählen Sie Uncalibrated, um die Videoanalyse ohne Kameraposition und Sichtfeldinformationen auszuführen.



Die Auswahl dieser Option verringert die Genauigkeit der Videoanalyse erheblich.

Wählen Sie Manual, um Kameraposition und Sichtfeldinformationen manuell festzulegen. Sie können die Kamera an die korrekte Position ziehen oder die Parameter in den entsprechenden Feldern anpassen. Die Referenzperson im Bild sollte möglichst genau der Größe und Position einer realen Person in der Ansicht entsprechen. +

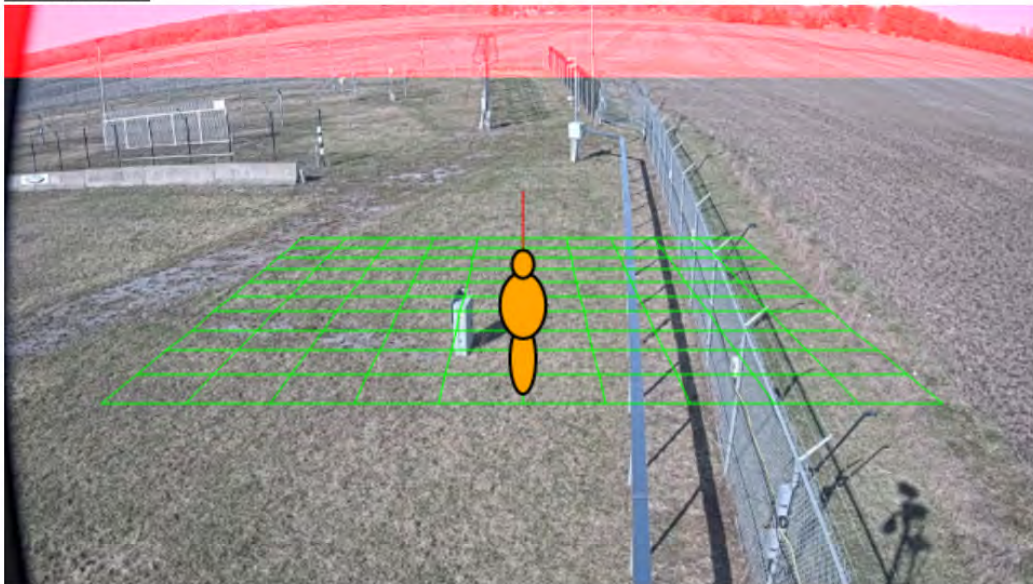
Calibration

Type

Manual ▾

Manually set the camera position and field of view information.

Instructions





Field of view (degrees)

Pan (degrees)

Twist (degrees)

Height (meters)

Distance (meters)

1. Stellen Sie im Abschnitt Sensitivity ein, wie empfindlich Senstar Sensor Fusion auf Kontrast und Bewegung reagiert, und wählen Sie aus, welche Optionen aktiviert werden sollen, um die Kamera für die Umgebung zu optimieren. `image::vis_fusion_configure_sensitivity.png[]`
2. Zeichnen Sie im Abschnitt Sensor Segments die Segmente des Perimeter-Einbruchmeldesystems. `image::vis_fusion_configure_sensor_segments.png[]`

Die Sensorsegmente müssen nicht das gesamte Perimeter-Einbruchmeldesystem abdecken. Die Abdeckung von Senstar Sensor Fusion hängt nicht von der Zonenkonfiguration des Perimeter-

Einbruchmeldesystems ab; die Sensorsegmente können Teil einer einzelnen Zone, Teil mehrerer Zonen oder genau einer Zone entsprechen.

- Klicken und ziehen Sie im Bild, um ein Sensorsegment zu zeichnen, das sowohl der Position als auch dem Standort der entsprechenden Zone des Perimeter-Einbruchmeldesystems entspricht.
- Wählen Sie Show Measures aus. Das Anzeigen von Maßen ist optional, erleichtert aber das Hinzufügen von Sensorsegmenten.
- Geben Sie im Feld Name einen Namen für das Sensorsegment ein.
- Wählen Sie in der Liste Select a Device das Perimeter-Einbruchmeldesystem aus, das Informationen an Senstar Sensor Fusion liefert.
- Wählen Sie in der Liste Zone die Zone des Perimeter-Einbruchmeldesystems aus, der das Sensorsegment entspricht.
- Stellen Sie die Länge des Sensorsegments in den Feldern Range und To ein. Der Wert Range sollte dem Startpunkt der Zone des Perimeter-Einbruchmeldesystems entsprechen.

PIDS-Zone	PIDS-Länge	Range-Wert	To-Wert
1	10	0	10
2	20	10	30
3	10	30	40

- Wählen Sie im Feld Reference Points aus, wie viele Referenzpunkte Sie auf dem Sensorsegment haben möchten. Sie sollten so viele Referenzpunkte hinzufügen, wie Zaunpfosten in der Zone des Perimeter-Einbruchmeldesystems vorhanden sind.



Wenn Sie zusätzliche Referenzpunkte zum Sensorsegment hinzufügen, laufen die gelben Linien, die die Pufferzone markieren, am Ende des Sensorsegments zusammen. Die Pufferzonenlinien kehren zur normalen Darstellung zurück, sobald Sie im nächsten Schritt den Wert Scale festlegen.

- Passen Sie im Feld Scale die Skalierung des Sensorsegments so an, dass die Referenzpunkte den im Sensorsegment enthaltenen Zaunpfosten entsprechen.



Um die Skalierung korrekt einzustellen, konzentrieren Sie sich auf zwei Referenzpunkte und passen Sie die Skalierung so an, dass die Referenzpunkte im Bild den Zaunpfosten entsprechen.

- Stellen Sie im Feld Confidence ein, wie sicher Senstar Sensor Fusion sein muss, um einen Alarm auszulösen.
- Stellen Sie im Feld Buffer Zone Distance ein, wie weit vom Sensorsegment (und der Zone des Perimeter-Einbruchmeldesystems) entfernt die Videoanalyse nach Objekten sucht.
 - Klicken Sie auf OK.
 - Klicken Sie auf Save.

Einstellungen für Senstar Sensor Fusion

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Wählen Sie die Auflösung aus, die die Senstar Sensor Fusion zur Analyse von Videobildern verwendet.
Analysis FPS	Wählen Sie die Anzahl der Bilder pro Sekunde aus, die die Senstar Sensor Fusion zur Videoanalyse verwendet.
Automatically Select Resolution Based on Calibration	Wählen Sie diese Option, um die Analyseauflösung automatisch basierend auf den Einstellungen im Bereich Calibration festzulegen.
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen. Warnung: Das Ändern der erweiterten Einstellungen kann die Leistung der Videoanalyse negativ beeinflussen.

Processing Mask

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche im Verarbeitungsmaskenbild markiert, die einbezogen (Analyse) oder ausgeschlossen (Ignore) werden sollen.
Size	Wählen Sie die Größe des Pinsels aus, mit dem Sie auf dem Verarbeitungsmaskenbild zeichnen.

Calibration

Einstellung	Beschreibung
Type	Wählen Sie den Kalibrierungstyp. Manuell ermöglicht Ihnen, die Kameraposition festzulegen. Automatisch ermöglicht der Videoanalyse, die Kameraposition und das Sichtfeld festzulegen. Unkalibriert führt die Videoanalyse ohne Informationen zur Kameraposition und zum Sichtfeld aus.
Zoom In	Klicken Sie hier, um das Kalibrierungsdiagramm zu vergrößern.
Zoom Out	Klicken Sie hier, um das Kalibrierungsdiagramm zu verkleinern.
Field of view (degrees)	Definieren Sie das horizontale Sichtfeld (in Grad) für die Kamera.
Pan (degrees)	Definieren Sie die Drehung um die vertikale Achse der Kamera in Bezug auf die Szene.
Twist (degrees)	Definieren Sie die Drehung um die horizontale Achse der Kamera in Bezug auf die Szene.
Height (meters)	Definieren Sie den vertikalen Abstand von der Kamera zum Boden.
Distance (meters)	Definieren Sie den horizontalen Abstand von der Kamera zur Mitte der Szene.

Sensitivity

Einstellung	Beschreibung
Object Contrast	Verwenden Sie den Schieberegler, um festzulegen, wie empfindlich die Senstar Sensor Fusion auf Unterschiede zwischen Objekten und dem Hintergrund reagiert.

Einstellung	Beschreibung
Object Motion	Verwenden Sie den Schieberegler, um festzulegen, wie empfindlich die Senstar Sensor Fusion auf Vordergrundbewegungen bei der Objekterkennung reagiert.
Background Motion	Verwenden Sie den Schieberegler, um festzulegen, wie empfindlich die Senstar Sensor Fusion auf Hintergrundbewegungen bei der Objekterkennung reagiert.
Shadow Suppression (Simple)	Wählen Sie diese Option, um die einfache Schattenunterdrückung zu verwenden. Die einfache Schattenunterdrückung ist effektiv, wenn sich helle Schatten in der Szene befinden.  Verwenden Sie keine Schattenunterdrückung mit Wärmebildkameras.
Shadow Suppression (Complex)	Wählen Sie diese Option, um die komplexe Schattenunterdrückung zu verwenden. Die komplexe Schattenunterdrückung ist effektiv, wenn sich dunkle Schatten in der Szene befinden.  Verwenden Sie keine Schattenunterdrückung mit Wärmebildkameras.
Snow Suppression	Wählen Sie diese Option, damit die Videoanalyse die Bewegung von Schnee in der Szene ignoriert.
Dynamic Background	Wählen Sie diese Option, damit die Videoanalyse periodische Bewegungen im Hintergrund der Szene ignoriert. Diese Einstellung ist effektiv für Außenszenen, in denen Wetter Bewegungen im Hintergrund verursachen kann.
Thermal Camera	Wählen Sie diese Option, wenn die Kamera eine Wärmebildkamera ist.
Detect Distant Objects	Wählen Sie diese Option, damit die Videoanalyse versucht, Objekte in der Entfernung zu erkennen.

Sensor Segments

Einstellung	Beschreibung
Show measures	Wählen Sie diese Option, um den Abstand (in Metern) zwischen Referenzpunkten auf dem Bild anzuzeigen.
Segment name	Geben Sie einen Namen für das Sensorsegment ein.
Select a Device	Wählen Sie das Perimeter-Eindringungserkennungssystem aus, das die Daten an die Senstar Sensor Fusion liefert.
Select a Zone	Wählen Sie die Zone des Perimeter-Eindringungserkennungssystems aus, die Sie konfigurieren möchten.
Range Start	Legen Sie den Abstand fest, ab dem die Kamera mit der Überwachung des Zauns beginnt. Dieser Wert entspricht dem Abstand vom Perimeter-Eindringungserkennungssystem.
Range End	Legen Sie den Abstand fest, bei dem die Kamera die Überwachung des Zauns beendet. Dieser Wert entspricht dem Abstand vom Perimeter-Eindringungserkennungssystem.

Einstellung	Beschreibung
Reference Points	Legen Sie fest, wie viele Referenzpunkte sich auf dem Sensorsegment befinden. Die Referenzpunkte müssen äquidistanten Zaunpfosten oder manuell in der Nähe des Zauns platzierten Markierungen entsprechen. Die Senstar Sensor Fusion-Videoanalyse verwendet die Referenzpunkte, um genaue Alarme zu generieren.
Scale	Legen Sie den Maßstab fest, um den Abstand zwischen den Referenzpunkten anzupassen.
Confidence Level	Legen Sie fest, wie sicher die Videoanalyse sein muss, um einen Alarm auszulösen. Der Bereich für diese Einstellung ist 1 bis 10, wobei 1 die niedrigste Vertrauensstufe und 10 die höchste Vertrauensstufe ist. Eine Einstellung von 1 generiert mehr Alarme und eine Einstellung von 10 generiert weniger Alarme.
Buffer Zone Distance (m)	Legen Sie den Abstand (in Metern) vom Sensorsegment fest, ab dem die Videoanalyse mit der Analyse der Szene beginnt. Wenn Sie die Pufferzone beispielsweise auf 5 Meter festlegen, analysiert die Videoanalyse jedes Objekt, das innerhalb von 5 Metern vom Sensorsegment kommt.

Import / Export

Einstellung	Beschreibung
Import XML	Klicken Sie auf diese Schaltfläche, um eine Konfigurations-XML-Datei zu importieren.
Export XML	Klicken Sie auf diese Schaltfläche, um die Konfigurations-XML-Datei zu exportieren.

Senstar Symphony KI-Objekterkennung und -verfolgung

Die Senstar Symphony AI Object Detection and Tracking nutzt maschinelles Lernen mit tiefen neuronalen Netzwerken, um Objekte zu erkennen und zu verfolgen.

Diese Videoanalyse klassifiziert Personen und Fahrzeuge intelligent und ignoriert dabei effektiv Hintergrundbewegungen. Darüber hinaus erhält diese Videoanalyse die Erkennung auch unter ungünstigen Bedingungen aufrecht.

Die Senstar Symphony AI Overhead People Tracking and Counting verwendet ein DNN-Modell, das für die generische Objekterkennung und -verfolgung optimiert ist.

Einstellungen für Senstar Symphony KI-Objekterkennung und -verfolgung

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Wählen Sie die Auflösung aus, die die Videoanalyse verwendet. Hinweis: Diese Einstellung ist nur verfügbar, wenn Sie Automatically Select Resolution Based on Calibration nicht auswählen.
Automatically Select Resolution Based on Calibration	Auswählen, damit der Server die Analyseauflösung auswählt.

Einstellung	Beschreibung
Use GPU instead of CPU	Auswählen, um eine unterstützte GPU für die Analyse zu verwenden. Diese Einstellung erfordert eine NVIDIA-GPU, die CUDA 11.0 oder höher unterstützt.
Analysis FPS	Wählen Sie die Bildrate aus, die die Videoanalyse verwendet.
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen. Warnung: Das Ändern der erweiterten Einstellungen kann die Leistung der Videoanalyse beeinträchtigen.

Verarbeitungsmaske

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche auf dem Bild der Verarbeitungsmaske als zu analysierend (Analyze) oder zu ignorierend (Ignore) markiert.
Size	Wählen Sie die Größe des Pinsels aus, mit dem Sie auf dem Bild der Verarbeitungsmaske zeichnen.

Zähllinie

Einstellung	Beschreibung
Create	Halten Sie auf dem Bild die linke Maustaste gedrückt, bewegen Sie die Maus, um die neue Zähllinie zu zeichnen, und lassen Sie die linke Maustaste los.
Delete	Klicken Sie auf eine Zähllinie, um sie auszuwählen, und drücken Sie Entf.
Move	Halten Sie die STRG-Taste gedrückt, halten Sie die linke Maustaste auf dem Endpunkt der Zähllinie gedrückt und ziehen Sie den Endpunkt an die gewünschte Position.
Add a connected counting line	Halten Sie die linke Maustaste auf dem Endpunkt einer vorhandenen Zähllinie gedrückt, bewegen Sie die Maus, um die neue Zähllinie zu zeichnen, und lassen Sie die linke Maustaste los.
Change the counting direction	Klicken Sie auf einen Pfeil auf der Zähllinie, um die Zählung für diese Richtung ein- oder auszuschalten.

Kalibrierung

Einstellung	Beschreibung
Type	Wählen Sie den Kalibrierungstyp aus. Mit Manual können Sie die Kameraposition selbst festlegen. Mit Automatic kann die Videoanalyse die Kameraposition und das Sichtfeld festlegen. Mit Uncalibrated wird die Videoanalyse ohne Informationen zu Kameraposition und Sichtfeld ausgeführt.
Zoom In	Klicken Sie hier, um das Kalibrierungsdiagramm zu vergrößern.
Zoom Out	Klicken Sie hier, um das Kalibrierungsdiagramm zu verkleinern.

Einstellung	Beschreibung
Field of view (degrees)	Definieren Sie das horizontale Sichtfeld (in Grad) für die Kamera.
Pan (degrees)	Definieren Sie die Drehung um die vertikale Achse der Kamera in Bezug auf die Szene.
Twist (degrees)	Definieren Sie die Drehung um die horizontale Achse der Kamera in Bezug auf die Szene.
Height (meters)	Definieren Sie den vertikalen Abstand zwischen der Kamera und dem Boden.
Distance (meters)	Definieren Sie den horizontalen Abstand zwischen der Kamera und dem Mittelpunkt der Szene.

Empfindlichkeit

Einstellung	Beschreibung
Maximum Hidden Seconds	Legen Sie fest, wie viele Sekunden ein Objekt verdeckt bleiben kann, bevor die Videoanalyse die Verfolgung des Objekts beendet. Wird das Objekt nach Ablauf dieser Zeit erneut erkannt, behandelt die Videoanalyse es als neues Objekt (d. h. es erhält eine neue ID).
Minimum Confidence	Legen Sie fest, wie zuverlässig die Videoanalyse bei der Objekterkennung sein muss, um das Objekt zu klassifizieren.
Minimum Tracking Threshold	Legen Sie fest, wie zuverlässig die Videoanalyse bei der Objekterkennung sein muss, um das Objekt zu verfolgen.

Senstar Symphony KI-Personenverfolgung und -zählung mit Überkopf-Kameras

Die Senstar Symphony AI Overhead People Tracking and Counting nutzt maschinelles Lernen mit tiefen neuronalen Netzwerken, um Personen zu verfolgen und zu zählen.

Diese Videoanalyse erkennt und zählt Personen intelligent über eine Deckenkamera.

Die Senstar Symphony AI Overhead People Tracking and Counting verwendet ein DNN-Modell, das für Deckenkameras optimiert ist.

Einstellungen für Senstar Symphony KI-Wärmeobjekterkennung und -verfolgung

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Wählen Sie die Auflösung aus, die die Videoanalyse verwendet. Hinweis: Diese Einstellung ist nur verfügbar, wenn Sie Automatically Select Resolution Based on Calibration nicht auswählen.
Automatically Select Resolution Based on Calibration	Auswählen, damit der Server die Analyseauflösung auswählt.
Use GPU instead of CPU	Auswählen, um eine unterstützte GPU für die Analyse zu verwenden. Diese Einstellung erfordert eine NVIDIA-GPU, die CUDA 11.0 oder höher unterstützt.
Analysis FPS	Wählen Sie die Bildrate aus, die die Videoanalyse verwendet.

Einstellung	Beschreibung
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen. Warnung: Das Ändern der erweiterten Einstellungen kann die Leistung der Videoanalyse beeinträchtigen.

Verarbeitungsmaske

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche auf dem Bild der Verarbeitungsmaske als zu analysierend (Analyse) oder zu ignorierend (Ignore) markiert.
Size	Wählen Sie die Größe des Pinsels aus, mit dem Sie auf dem Bild der Verarbeitungsmaske zeichnen.

Zähllinie

Einstellung	Beschreibung
Create	Halten Sie auf dem Bild die linke Maustaste gedrückt, bewegen Sie die Maus, um die neue Zähllinie zu zeichnen, und lassen Sie die linke Maustaste los.
Delete	Klicken Sie auf eine Zähllinie, um sie auszuwählen, und drücken Sie Entf.
Move	Halten Sie die STRG-Taste gedrückt, halten Sie die linke Maustaste auf dem Endpunkt der Zähllinie gedrückt und ziehen Sie den Endpunkt an die gewünschte Position.
Add a connected counting line	Halten Sie die linke Maustaste auf dem Endpunkt einer vorhandenen Zähllinie gedrückt, bewegen Sie die Maus, um die neue Zähllinie zu zeichnen, und lassen Sie die linke Maustaste los.
Change the counting direction	Klicken Sie auf einen Pfeil auf der Zähllinie, um die Zählung für diese Richtung ein- oder auszuschalten.

Kalibrierung

Einstellung	Beschreibung
Type	Wählen Sie den Kalibrierungstyp aus. Mit Manual können Sie die Kameraposition selbst festlegen. Mit Automatic kann die Videoanalyse die Kameraposition und das Sichtfeld festlegen. Mit Uncalibrated wird die Videoanalyse ohne Informationen zu Kameraposition und Sichtfeld ausgeführt.
Zoom In	Klicken Sie hier, um das Kalibrierungsdiagramm zu vergrößern.
Zoom Out	Klicken Sie hier, um das Kalibrierungsdiagramm zu verkleinern.
Field of view (degrees)	Definieren Sie das horizontale Sichtfeld (in Grad) für die Kamera.
Pan (degrees)	Definieren Sie die Drehung um die vertikale Achse der Kamera in Bezug auf die Szene.
Twist (degrees)	Definieren Sie die Drehung um die horizontale Achse der Kamera in Bezug auf die Szene.

Einstellung	Beschreibung
Height (meters)	Definieren Sie den vertikalen Abstand zwischen der Kamera und dem Boden.
Distance (meters)	Definieren Sie den horizontalen Abstand zwischen der Kamera und dem Mittelpunkt der Szene.

Empfindlichkeit

Einstellung	Beschreibung
Maximum Hidden Seconds	Legen Sie fest, wie viele Sekunden ein Objekt verdeckt bleiben kann, bevor die Videoanalyse die Verfolgung des Objekts beendet. Wird das Objekt nach Ablauf dieser Zeit erneut erkannt, behandelt die Videoanalyse es als neues Objekt (d. h. es erhält eine neue ID).
Minimum Confidence	Legen Sie fest, wie zuverlässig die Videoanalyse bei der Objekterkennung sein muss, um das Objekt zu klassifizieren.
Minimum Tracking Threshold	Legen Sie fest, wie zuverlässig die Videoanalyse bei der Objekterkennung sein muss, um das Objekt zu verfolgen.

Senstar Symphony KI-Wärmeobjekterkennung und -verfolgung

Die Videoanalyse Senstar Symphony AI Thermal Object Detection and Tracking nutzt maschinelles Lernen mit tiefen neuronalen Netzwerken, um Objekte zu erkennen und zu verfolgen.

Diese Videoanalyse klassifiziert Personen und Fahrzeuge intelligent und ignoriert dabei effektiv Hintergrundbewegungen, wenn Sie Wärmebildkameras verwenden.

Die Senstar Symphony AI Thermal Object Detection and Tracking verwendet ein DNN-Modell, das für Wärmebildkameras optimiert ist.

Einstellungen für Senstar Symphony KI-Wärmeobjekterkennung und -verfolgung

Übersicht

Einstellung	Beschreibung
Analysis Resolution	Wählen Sie die Auflösung aus, die die Videoanalyse verwendet. Hinweis: Diese Einstellung ist nur verfügbar, wenn Sie Automatically Select Resolution Based on Calibration nicht auswählen.
Automatically Select Resolution Based on Calibration	Auswählen, damit der Server die Analyseauflösung auswählt.
Use GPU instead of CPU	Auswählen, um eine unterstützte GPU für die Analyse zu verwenden. Diese Einstellung erfordert eine NVIDIA-GPU, die CUDA 11.0 oder höher unterstützt.
Analysis FPS	Wählen Sie die Bildrate aus, die die Videoanalyse verwendet.
Simple Mode	Wählen Sie aus, ob die erweiterten Einstellungen ausgeblendet oder angezeigt werden sollen. Warnung: Das Ändern der erweiterten Einstellungen kann die Leistung der Videoanalyse beeinträchtigen.

Verarbeitungsmaske

Einstellung	Beschreibung
Drawing Mode	Wählen Sie aus, ob der Pinsel Bereiche auf dem Bild der Verarbeitungsmaske als zu analysierend (Analyze) oder zu ignorierend (Ignore) markiert.
Size	Wählen Sie die Größe des Pinsels aus, mit dem Sie auf dem Bild der Verarbeitungsmaske zeichnen.

Zähllinie

Einstellung	Beschreibung
Create	Halten Sie auf dem Bild die linke Maustaste gedrückt, bewegen Sie die Maus, um die neue Zähllinie zu zeichnen, und lassen Sie die linke Maustaste los.
Delete	Klicken Sie auf eine Zähllinie, um sie auszuwählen, und drücken Sie Entf.
Move	Halten Sie die STRG-Taste gedrückt, halten Sie die linke Maustaste auf dem Endpunkt der Zähllinie gedrückt und ziehen Sie den Endpunkt an die gewünschte Position.
Add a connected counting line	Halten Sie die linke Maustaste auf dem Endpunkt einer vorhandenen Zähllinie gedrückt, bewegen Sie die Maus, um die neue Zähllinie zu zeichnen, und lassen Sie die linke Maustaste los.
Change the counting direction	Klicken Sie auf einen Pfeil auf der Zähllinie, um die Zählung für diese Richtung ein- oder auszuschalten.

Kalibrierung

Einstellung	Beschreibung
Type	Wählen Sie den Kalibrierungstyp aus. Mit Manual können Sie die Kameraposition selbst festlegen. Mit Automatic kann die Videoanalyse die Kameraposition und das Sichtfeld festlegen. Mit Uncalibrated wird die Videoanalyse ohne Informationen zu Kameraposition und Sichtfeld ausgeführt.
Zoom In	Klicken Sie hier, um das Kalibrierungsdiagramm zu vergrößern.
Zoom Out	Klicken Sie hier, um das Kalibrierungsdiagramm zu verkleinern.
Field of view (degrees)	Definieren Sie das horizontale Sichtfeld (in Grad) für die Kamera.
Pan (degrees)	Definieren Sie die Drehung um die vertikale Achse der Kamera in Bezug auf die Szene.
Twist (degrees)	Definieren Sie die Drehung um die horizontale Achse der Kamera in Bezug auf die Szene.
Height (meters)	Definieren Sie den vertikalen Abstand zwischen der Kamera und dem Boden.
Distance (meters)	Definieren Sie den horizontalen Abstand zwischen der Kamera und dem Mittelpunkt der Szene.

Empfindlichkeit

Einstellung	Beschreibung
Maximum Hidden Seconds	Legen Sie fest, wie viele Sekunden ein Objekt verdeckt bleiben kann, bevor die Videoanalyse die Verfolgung des Objekts beendet. Wird das Objekt nach Ablauf dieser Zeit erneut erkannt, behandelt die Videoanalyse es als neues Objekt (d. h. es erhält eine neue ID).
Minimum Confidence	Legen Sie fest, wie zuverlässig die Videoanalyse bei der Objekterkennung sein muss, um das Objekt zu klassifizieren.
Minimum Tracking Threshold	Legen Sie fest, wie zuverlässig die Videoanalyse bei der Objekterkennung sein muss, um das Objekt zu verfolgen.

Multicasting

Multicasting ermöglicht es zahlreichen Windows Client-Instanzen, sich direkt mit Kameras zu verbinden, ohne dass dedizierte Videostreams für jeden Windows Client erforderlich sind.

Multicasting kann die Last sowohl auf dem Server als auch auf der Kamera reduzieren, wenn eine große Anzahl von Windows Client-Instanzen Videos von einer Kamera anzeigen muss. Um Multicasting zu verwenden, müssen sowohl die Kameras als auch die Netzwerk-Switches Multicasting unterstützen. Um zu überprüfen, ob eine Kamera Multicasting unterstützt, prüfen Sie die [Liste der unterstützten Videogeräte](#).

Um Multicasting zu konfigurieren, führen Sie den folgenden Workflow aus:

1. Konfigurieren Sie Multicasting auf dem Netzwerk-Switch.
2. Konfigurieren Sie Multicasting auf der Kamera.
3. Fügen Sie in der Konfigurationsoberfläche des Server die Kamera hinzu und wählen Sie Multicast als Transport für die Kamera aus.
4. Stellen Sie in der Oberfläche des Windows Client den Verbindungsmodus der Kamera auf Connect directly ein, sofern die Kamera dies unterstützt.

Edge-Speicher

Der Edge-Speicher verwendet eine SD-Karte oder einen anderen kameraseitigen Speicher, sodass die Kamera weiter aufzeichnet, wenn sie den Server nicht erreichen kann, und damit der Windows Client dieses Video direkt von der Kamera wiedergeben kann.

Der Edge-Speicher überbrückt Lücken durch Netzerkausfälle, Ausfallzeiten des Server und Wartungsfenster. Die Kamera schreibt Videos nach ihrem eigenen Zeitplan in ihren lokalen Speicher, unabhängig vom Server. Wenn der Server wieder erreichbar ist, kann er die Aufzeichnungen von der Kamera in das reguläre Videoarchiv synchronisieren. Wenn der Server nicht erreichbar ist, kann ein autorisierter Windows Client das Video direkt über eine ONVIF-Verbindung von der Kamera abrufen.

Bevor Sie beginnen:

- Installieren Sie unterstützte Speichermedien (in der Regel eine SD-Karte) in der Kamera.
- Formatieren Sie das Speichermedium über die Weboberfläche der Kamera.
- Stellen Sie sicher, dass die Kamera ONVIF Profile G (Edge-Aufzeichnung und -Abruf) unterstützt.

Edge-Speicher an einer Kamera aktivieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.

2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Wählen Sie im Abschnitt Edge Storage die Option Enable Edge Storage.
4. Wählen Sie den Aufzeichnungsmodus aus:
 - a. Continuous zeichnet Videos jederzeit auf den Speicher der Kamera auf.
 - b. On Connection Loss zeichnet Videos nur dann auf, wenn die Kamera den Server nicht erreichen kann.
5. Legen Sie den Aufzeichnungszeitplan und die Aufbewahrung fest.
6. Klicken Sie auf Save.

Edge-Aufzeichnungen mit dem Server synchronisieren

Wenn der Server die Kamera wieder erreichen kann, kopiert er die auf der Kamera erstellten Aufzeichnungen in das reguläre Videoarchiv. Das synchronisierte Video erscheint in der Zeitleiste neben dem serverseitig aufgezeichneten Video.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Cameras.
2. Wählen Sie die Kamera aus und klicken Sie auf Edit.
3. Wählen Sie im Abschnitt Edge Storage die Option Synchronize on Reconnect.
4. Klicken Sie auf Save.

Edge-Aufzeichnungen in den Windows Client abrufen

Wenn der Server nicht verfügbar ist, kann sich der Windows Client direkt mit der Kamera verbinden und Videos aus dem Edge-Speicher wiedergeben.

1. Öffnen Sie die Kamera im Windows Client in einem Anzeigepanel.
2. Wählen Sie in der Zeitleiste Edge als Wiedergabequelle aus.
3. Ziehen Sie den Zeitleistenindikator auf die Zeit, die Sie anzeigen möchten.

Der Windows Client streamt den angeforderten Zeitbereich über ONVIF von der Kamera. Die Wiedergabe verwendet die Aufzeichnungen auf der Kamera und ist unabhängig vom Server.

Browser

Der Windows Client kann eine Webseite in einem Kameraansichts-Bereich anzeigen.

Wenn Sie in der Konfigurationsoberfläche des Server einen Browser hinzufügen, erscheint dieser in der Oberfläche des Windows Client im Gerätebaum unter der Überschrift Browser. Sie können die Webseite in einem Kameraansichts-Bereich anzeigen.

Der Windows Client verwendet den Microsoft Edge-Browser, um die Webseiten in den Kameraansichts-Bereichen darzustellen, der Bereich enthält jedoch keine Browsersteuerelemente (Navigation, Adressfeld, Einstellungen usw.).

Browser hinzufügen

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Browsers.
2. Klicken Sie auf Add Browser.
3. Geben Sie im Feld Name einen Namen für den Browser ein, der in der Oberfläche des Windows Client angezeigt werden soll.

4. Geben Sie im Feld Url die Adresse der Seite ein.
5. Klicken Sie auf Save.

Browser suchen

Um schnell einen bestimmten Browser zu finden, verwenden Sie Filter und Sortierung.

Filter

Sie können die Browser-Liste anhand der folgenden Filter filtern:

- Browsername (Name)
- Browser-Adresse (Url)
 1. Klicken Sie in der Server-Konfigurationsoberfläche auf Devices > Browsers.
 2. Klicken Sie auf die Lupe, um die Filter-Textfelder einzublenden.
 3. Definieren Sie die Filterkriterien.
 4. Klicken Sie auf Apply filter.

Sortierung

Sie können die Liste der Browser sortieren, indem Sie auf den Spaltennamen klicken. Durch Klicken auf den Spaltennamen wird zwischen aufsteigender und absteigender Reihenfolge gewechselt.

Zurücksetzen

Um den Filter zurückzusetzen und die Liste der Browser wiederherzustellen, klicken Sie auf Clear Filter.

Vorlagen

Eine Vorlage ist eine Sammlung von Konfigurationseinstellungen, die Sie auf Kameras anwenden können.

Wenn Sie eine Vorlage auf eine Kamera anwenden, werden einige der Konfigurationseinstellungen für die Kamera eingeschränkt. Sie können beispielsweise keinen zusätzlichen Stream zu einer Kamera hinzufügen, wenn Sie eine Vorlage auf eine Kamera anwenden.

Vorlage suchen

Um schnell eine bestimmte Vorlage zu finden, verwenden Sie Filter und Sortierung.

Filter

Sie können die Vorlagenliste anhand des folgenden Filters filtern:

- Vorlagenname (Name)
 1. Klicken Sie in der Server-Konfigurationsoberfläche auf Devices > Templates.
 2. Klicken Sie auf die Lupe, um die Filter-Textfelder einzublenden.
 3. Definieren Sie die Filterkriterien.
 4. Klicken Sie auf Apply filter.

Sortierung

Sie können die Liste der Vorlagen sortieren, indem Sie auf den Spaltennamen klicken. Durch Klicken auf den Spaltennamen wird zwischen aufsteigender und absteigender Reihenfolge gewechselt.

Zurücksetzen

Um den Filter zurückzusetzen und die Liste der Vorlagen wiederherzustellen, klicken Sie auf Clear Filter.

Vorlageneinstellungen

General

Einstellung	Beschreibung
Failover enabled	Wählen Sie aus und geben Sie an, ob Failover aktiviert oder deaktiviert ist.
Support Direct Connect	Wählen Sie aus, ob die Kamera direkte Verbindungen über einen Browser zulässt.
Enable Audio Input	Wählen Sie aus, ob die Kamera Audio aufzeichnen kann.
Enable Audio Output	Wählen Sie aus, ob die Kamera Audio wiedergeben kann.
Rotate Degrees	Wählen Sie aus, ob die Aufzeichnungen der Kamera gedreht werden sollen.
Change frame rate on alarm to	Wählen Sie aus, um die Bildrate des Videos der Kamera zu ändern.
Limit the number of days video is stored	Geben Sie die maximale Zeit (in Tagen) an, für die der Server das Video aufbewahrt.
PTZ Maximum Locked Time	Geben Sie die maximale Zeit (in Minuten) an, die PTZ-Kameras im gesperrten Zustand bleiben können.
Enable panoramic technology	Wählen Sie aus, um die Panorama-Technologie für die Kamera zu aktivieren, und geben Sie den Panorama-Typ und die Kameraposition an.

Stream

Einstellung	Beschreibung
Resolution	Geben Sie die Auflösung für die Kamera an.
Frame Rate	Geben Sie die Bildrate für die Kamera an.
Video Codec	Wählen Sie den Video-Codec aus, den die Kamera verwendet.
Bitrate	Geben Sie die Bitrate (in Kilobit pro Sekunde) für die Kamera an.
Key frame interval	Geben Sie das Keyframe-Intervall an.
Video Recording	Wählen Sie aus, wann die Kamera Video aufzeichnet.
Pre Event	Geben Sie an, wie viel Video (in Sekunden) die Kamera vor einem Ereignis aufzeichnet.
Post Event	Geben Sie an, wie viel Video (in Sekunden) die Kamera nach einem Ereignis aufzeichnet.
Schedule	Wählen Sie aus, um den Zeitplan festzulegen.
Audio recording	Wählen Sie aus, wann die Kamera Audio aufzeichnet.

Vorlage erstellen

Erstellen Sie eine Vorlage in der Konfigurationsoberfläche des Server.

1. Klicken Sie auf Devices > Templates.

2. Klicken Sie auf Add Template.
3. Geben Sie im Feld Name einen Namen für die Vorlage ein.
4. Konfigurieren Sie die Einstellungen für die Vorlage.
5. Klicken Sie auf Save.

Vorlage kopieren

Sie können eine Vorlage kopieren, um sie als Ausgangspunkt für eine neue Vorlage zu verwenden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Templates.
2. Wählen Sie die Vorlage aus und klicken Sie auf Clone.
3. Geben Sie im Feld Name einen Namen für die Vorlage ein. Standardmäßig enthält der Name der neuen Vorlage

Clone of

vor dem Namen der ursprünglichen Vorlage.

1. Konfigurieren Sie die Einstellungen für die Vorlage.
2. Klicken Sie auf Save.

Hardware

Die Registerkarte Hardware ermöglicht es Symphony, sich mit bestimmten Geräten wie Einbruchmeldezentralen zu verbinden und diese zu steuern. Für die Verwaltung von Gerätenetzwerken, wie z. B. Lesegeräten zur Zutrittskontrolle oder Perimetersensoren, siehe [Integrationen](#).

Der Server unterstützt die folgenden Hersteller:

- Bosch
- CommBox
- Senstar (nur Legacy, siehe [Integrationen](#))

Hardware-Gerät hinzufügen

Sie können DIO-, Zugangskontroll- und Senstar Thin Client-Geräte über die Registerkarte Hardware in der Konfigurationsoberfläche des Server zum Server hinzufügen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Hardware.
2. Klicken Sie auf Add Hardware.
3. Wählen Sie in der Liste Manufacturer den Hersteller des Hardware-Geräts aus. Wenn der Hersteller nicht in der Liste enthalten ist, versuchen Sie, das Hardware-Gerät als Integration (Add an integration) oder als Zugangskontrollgerät (Add an access control device) hinzuzufügen.
4. Geben Sie im Bereich General die Einstellungen für das Hardware-Gerät an. Die Einstellungen sind sowohl herstellerspezifisch als auch geräteabhängig.
5. Klicken Sie auf Connect to Device, um die Verbindung zu testen.
6. Klicken Sie auf Save.

Hardware-Gerät suchen

Um schnell ein bestimmtes Hardwaregerät zu finden, verwenden Sie Filter und Sortierung.

Filter

Sie können die Hardware-Liste anhand des folgenden Filters filtern:

- Hardware-ID (ID)
- Hardware-Marke (Brand)
- Hardware-Name (Name)
- IP-Adresse des Hardwaregeräts (IP Address)
- Gruppen, zu denen das Hardwaregerät gehört (Groups)
 1. Klicken Sie in der Server-Konfigurationsoberfläche auf Devices > Hardware.
 2. Klicken Sie auf die Lupe, um die Filter-Textfelder einzublenden.
 3. Definieren Sie die Filterkriterien.
 4. Klicken Sie auf Apply filter.

Sortierung

Sie können die Liste der Hardwaregeräte sortieren, indem Sie auf den Spaltennamen klicken. Durch Klicken auf den Spaltennamen wird zwischen aufsteigender und absteigender Reihenfolge gewechselt.

Zurücksetzen

Um den Filter zurückzusetzen und die Liste der Hardwaregeräte wiederherzustellen, klicken Sie auf Clear Filter.

Integrationen

Auf der Registerkarte Integrations in der Konfigurationsoberfläche des Server fügen Sie dem Server Sicherheitslösungen hinzu.

Integrations					
Add Hardware					
Q	ID	Name	Type	Details	Groups
☐	100001	Senstar FP1150	Senstar Network Manager	127.0.0.1, 3	FP1150
☐	100005	Senstar Access Control	Symphony AC	OT-SYMPHONY11(Senstar, VMSAC	Symphony ACS
☐	100006	OmniTrax	Senstar Network Manager	127.0.0.1, 1	PIDS Sensors
☐	100008	Temporary FZ-60	Senstar Network Manager	172.16.58.10, 2	Flexzone-60
☐	100012	NM Simulator on Symphony client	Senstar Network Manager	172.16.58.195, 1	Simulation
☐	100015	NMS SITE MultiSensor	Senstar Network Manager	172.16.56.123, 3	MultiSensors
☐	100019	UW NM	Senstar Network Manager	172.16.56.220, 3	Devices
☐	100020	NM for SITE (Lidar(s)	Senstar Network Manager	127.0.0.1, 6	Devices
☐	100021	NM for SITE PIDS (LM100, FP400, ...	Senstar Network Manager	127.0.0.1, 3	Devices

Über die Registerkarte Integrations können Sie dem Server mehrere Sicherheitslösungen hinzufügen. Sie können beispielsweise mehrere Instanzen von Senstar Symphony Access Control und Senstar Network Manager gleichzeitig zum Server hinzufügen.

Integrations-Hardware hinzufügen

Worum es geht

Eine Integration verbindet ein Drittanbietersystem mit dem Server. Nach der Integration werden die Geräte und Ereignisse des Systems zu vollwertigen Bestandteilen von Senstar Symphony: Sie erscheinen im **Gerätebaum**, ihre Ereignisse können **Regeln** auslösen, und Operatoren können sie im Windows Client sehen.

Integrationen unterscheiden sich von reiner **Hardware** dadurch, dass der Server das Protokoll des

Drittanbieters nativ beherrscht und dessen Ereignismodell versteht. Verwenden Sie eine Integration, wenn eine für Ihr Gerät existiert; greifen Sie nur dann auf den generischen Pfad [Hardware-Gerät hinzufügen](#) zurück, wenn keine vorhanden ist.

Wann Sie es verwenden würden

- Sie stellen ein Zutrittskontrollsystem bereit und möchten, dass Türereignisse Regeln auslösen.
- Sie stellen einen Perimeter-Einbruchssensor (Zaunsensor, Radar) bereit und möchten, dass dessen Erkennungen Alarme erzeugen.
- Sie verfügen über DIO-Hardware, deren Eingänge Regeln auslösen und deren Ausgänge durch Aktionssätze gesteuert werden sollen.

Voraussetzungen

- Berechtigung zum Bearbeiten der Gerätekonfiguration.
- Netzwerkverbindung vom Server zum Drittanbietergerät oder dessen Controller (IP-Adresse und Port).
- Die Anmeldedaten des Geräts (Benutzername, Kennwort, API-Schlüssel oder Zertifikat, je nach Herstelleranforderung).
- Die Herstellerdokumentation zu protokollspezifischen Feldern, Ereigniszuordnungen und Firmwareanforderungen.

Vorgehensweise

1. Klicken Sie in der Konfigurationsoberfläche des Server auf **Devices > Integrations**.
2. Klicken Sie auf **Add Hardware**.
3. Wählen Sie in der Liste **Manufacturer** den Hersteller aus. Wenn der Hersteller nicht aufgeführt ist, versuchen Sie stattdessen [Hardware-Gerät hinzufügen](#) (generisch) oder [Zugangskontrollgerät hinzufügen](#).
4. Füllen Sie im Bereich **General** die Verbindungsfelder aus. Die meisten Hersteller verlangen eine Kombination aus:
 - **Adresse oder Hostname** — wie der Server das Gerät erreicht.
 - **Port** — der Protokollport des Herstellers (siehe Herstellerdokumentation).
 - **Anmeldedaten** — Benutzername und Kennwort oder API-Schlüssel/-Token.
 - **Polling- oder Heartbeat-Intervall** — wie oft der Server das Gerät kontaktiert.
 - **Ereigniszuordnung oder Kanalauswahl** — welche Ereignisse oder Kanäle des Geräts der Server aufgreifen soll.

Pflichtfelder und gültige Werte sind herstellerspezifisch. Schlagen Sie in der Herstellerdokumentation nach, was für Ihr Hardware-Modell und die Firmwareversion erforderlich ist.
5. Klicken Sie auf **Connect to Device**, um die Einstellungen zu überprüfen. Ein erfolgreicher Test bestätigt, dass Adresse, Anmeldedaten und Protokoll korrekt sind. Beheben Sie etwaige Fehler, bevor Sie fortfahren — eine Integration, die keine Verbindung herstellen kann, liefert keine Ereignisse für Regeln.
6. Wählen Sie in der Liste **Groups** die Gerätegruppen des Windows Client aus, zu denen diese Integration gehört. Die Gruppenmitgliedschaft steuert, wo das Gerät im [Gerätebaum](#) erscheint und

welche Sicherheitsprofile es sehen können.

7. Klicken Sie auf **Save**.

Nach dem Hinzufügen

Die Ereignisse der Integration sind nun im [Ereigniskatalog](#) verfügbar. Um aus einem Ereignis einen Alarm oder eine Aktion zu machen, [erstellen Sie eine Regel](#), die das Ereignis verwendet.

Verwandte Aufgaben

- [Kamera mit einer Quelle verknüpfen](#) — Integrationsereignisse mit einer Kamera verbinden, damit Operatoren das Video zum Ereignis sehen.
- [Zugangskontrollgerät hinzufügen](#)
- [Senstar Network Manager](#) — dedizierte Integration für Senstar-Perimetersensoren.
- [Senstar Symphony Access Control](#)

Integrations-Hardware suchen

Um schnell eine bestimmte Integration zu finden, verwenden Sie Filter und Sortierung.

Filter

Sie können die Integrationsliste anhand des folgenden Filters filtern:

- Integrations-ID (ID)
- Integrationsname (Name)
- Integrationstyp (Type)
- Informationen zur Integration (Details)
- Gruppen, zu denen die Integration gehört (Groups)
 1. Klicken Sie in der Server-Konfigurationsoberfläche auf [Devices > Integrations](#).
 2. Klicken Sie auf die Lupe, um die Filter-Textfelder einzublenden.
 3. Definieren Sie die Filterkriterien.
 4. Klicken Sie auf [Apply filter](#).

Sortierung

Sie können die Liste der Integrationen sortieren, indem Sie auf den Spaltennamen klicken. Durch Klicken auf den Spaltennamen wird zwischen aufsteigender und absteigender Reihenfolge gewechselt.

Zurücksetzen

Um den Filter zurückzusetzen und die Liste der Integrationen wiederherzustellen, klicken Sie auf [Clear Filter](#).

Gerätealias

Sie können die Sensoren, Befehle, Ereignisse und Zustände eines Hardware- oder Integrationsgeräts umbenennen, sodass sie mit aussagekräftigen, beschreibenden Namen im [Gerätebaum](#), im [Gerätebaum](#), in [Regeln](#) und in [Alarmen](#) angezeigt werden.

Standardmäßig stellen Geräte ihre Sensoren, Befehle, Ereignisse und Zustände unter den vom Gerät gemeldeten Bezeichnungen bereit, die oft generisch sind (z. B. [Input 1](#), [Relay 2](#)). Sie können diese Bezeichnungen durch Aliase ersetzen, die die Rolle des Elements an Ihrem Standort beschreiben (z. B.

Front Door Contact oder Lobby Strobe).

So verwenden Sie einen Gerätealias:

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Device Tree.
2. Erweitern Sie das Gerät.
3. Klicken Sie mit der rechten Maustaste auf den Sensor, Befehl, das Ereignis oder den Zustand, den Sie umbenennen möchten.
4. Klicken Sie auf Rename.
5. Geben Sie den Alias ein und drücken Sie die Eingabetaste.

Um die ursprüngliche Bezeichnung wiederherzustellen, klicken Sie mit der rechten Maustaste auf das Element, klicken Sie auf Rename, löschen Sie den Alias und drücken Sie die Eingabetaste.

Symphony AC

Senstar Symphony Access Control ist eine eigenständige Anwendung, die in den Server integriert wird, um Hardware-Controller für Zutrittskontroll-, Einbruch- und HLK-Systeme zu verwalten.

Sie können Senstar Symphony Access Control in den Server integrieren, um Ereignisse von Senstar Symphony Access Control-Knoten für die Alarmierung und Überwachung zu nutzen.

Damit der Server Alarme von Senstar Symphony Access Control empfangen kann, müssen die Regions- und Zeiteinstellungen auf dem Computer, der Senstar Symphony Access Control hostet, mit den Regions- und Zeiteinstellungen auf dem Computer übereinstimmen, der den Server hostet.

Mit Senstar Symphony Access Control verbinden

Verbinden Sie den Server mit Senstar Symphony Access Control, um Ereignisse aus Senstar Symphony Access Control als Auslöser für Aktionen zu verwenden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Integrations.
2. Klicken Sie auf Add Hardware.
3. Wählen Sie in der Liste Device Type den Eintrag Symphony AC aus.
4. Geben Sie im Feld Name einen aussagekräftigen Namen für Senstar Symphony Access Control ein. Dieser Name erscheint in der Geräteliste in der

Konfigurationsoberfläche des Server

und im Gerätebaum in der

Oberfläche des Windows Client

.

1. Geben Sie im Feld Database Server die vollständige Adresse der Microsoft SQL Server-Instanz für Senstar Symphony Access Control ein. Zum Beispiel

COMPUTER1\SQLEXPRESS2012

.

1. Geben Sie im Feld Database Name den Namen der Datenbank von Senstar Symphony Access Control ein.
2. Geben Sie im Feld Username den Benutzernamen ein, mit dem der Server auf die Datenbank von

Senstar Symphony Access Control zugreift.

3. Geben Sie im Feld Password das Kennwort ein, mit dem der Server auf die Datenbank von Senstar Symphony Access Control zugreift.
4. Klicken Sie auf Connect to Device.
5. Wählen Sie in der Liste Sources die Knoten aus, die Sie zum Server hinzufügen möchten. Wenn Ihre Auswahl auch für alle untergeordneten Knoten gelten soll, schalten Sie den Schalter

Cascade Selection

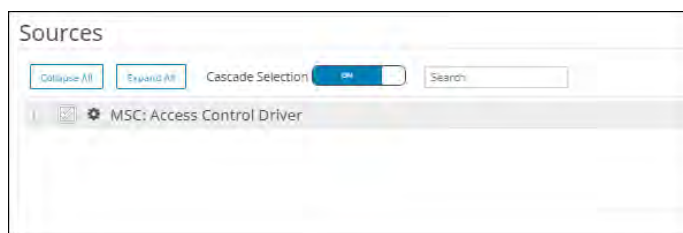
ein. Um zu verhindern, dass Ihre Auswahl andere Knoten beeinflusst, schalten Sie den Schalter

Cascade Selection

aus. Um nach einem Knoten zu suchen, geben Sie die Begriffe in das Feld

Search

ein — die Quellenliste wird nach den Suchbegriffen gefiltert.



1. Wählen Sie in der Liste Groups den Gerätebaumordner aus, in dem Senstar Symphony Access Control angezeigt werden soll.
2. Klicken Sie auf Save.

Einstellungen für Senstar Symphony Access Control

General

Einstellung	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen für die Senstar Symphony Access Control-Instanz ein. Dieser Name erscheint im Gerätebaum.
Type	In diesem Feld wird der Integrationstyp angezeigt. Den Typ wählen Sie beim Hinzufügen von Hardware aus.
Database Server	Geben Sie die vollständige Adresse der Microsoft SQL Server-Instanz für Senstar Symphony Access Control ein.
Database Name	Geben Sie den Namen der Senstar Symphony Access Control-Datenbank ein.
Username	Geben Sie den Benutzernamen ein, mit dem der Server auf die Senstar Symphony Access Control-Datenbank zugreift.
Password	Geben Sie das Kennwort ein, mit dem der Server auf die Senstar Symphony Access Control-Datenbank zugreift.
Import XML	Klicken Sie hier, um eine XML-Datei mit Konfigurationsinformationen zu importieren.
Export XML	Klicken Sie hier, um eine XML-Datei mit Konfigurationsinformationen zu exportieren.

Einstellung	Beschreibung
Show XML	Klicken Sie hier, um die Konfigurationsinformationen anzuzeigen.

Connect

Einstellung	Beschreibung
Save and Reconnect	Klicken Sie hier, um die Änderungen an den allgemeinen Einstellungen zu speichern und eine Verbindung zu Senstar Symphony Access Control herzustellen.

Sources

Einstellung	Beschreibung
Collapse All	Klicken Sie hier, um den Quellbaum zuzuklappen und nur die obersten Ebenen anzuzeigen.
Expand All	Klicken Sie hier, um den Quellbaum aufzuklappen und alle Ebenen anzuzeigen.
Cascade Selection	Aktivieren Sie diese Option, um beim Auswählen eines Geräts automatisch alle untergeordneten Ebenen auszuwählen. Deaktivieren Sie sie, um nur das ausgewählte Gerät zu markieren.
Search	Geben Sie Suchbegriffe ein, um die Quellliste zu filtern.

Senstar Network Manager

Der Senstar Network Manager verbindet Senstar-Sicherheitsnetzwerke mit dem Server. Der Server unterstützt den Senstar Network Manager 2.32 und neuer.

Sie können den Senstar Network Manager mit dem Server integrieren, um Ereignisse von Senstar Network Manager-Knoten für Alarmierung und Überwachung zu nutzen. Sie verwenden die Registerkarte Integration in der Server-Konfigurationsoberfläche, um den Senstar Network Manager zu verbinden und zu konfigurieren.

Mit dem Senstar Network Manager verbundene Geräte erscheinen im Gerätebaum in der Windows Client-Oberfläche. Darüber hinaus zeigt der Gerätebaum den Status der mit dem Senstar Network Manager verbundenen Geräte an.

Sie können mehrere Instanzen des Senstar Network Manager mit dem Server verbinden.

Automatisch generierte Regeln

Wenn Sie eine Senstar Network Manager-Integration hinzufügen, kann der Server automatisch Regeln für die mit dem Senstar Network Manager verbundenen Sensoren und Geräte generieren. Das automatische Generieren von Regeln kann Zeit sparen, wenn Sie einen Senstar Network Manager mit zahlreichen Geräten oder Sensoren hinzufügen. Standardmäßig generiert der Server Sensoralarme für Trouble-, Alarm- und Tamper-Vorfälle sowie für Communication Fail-, Communication Fault-, Diagnostic Warnings-, Diagnostic Fatal- und Enclosure Tamper-Vorfälle.

Beim automatischen Generieren von Regeln wählt der Server aus, Alarme auf der ersten Kamera nach Kamera-ID auszulösen. Wenn keine Kameras mit dem Server verbunden sind, wählt der Server aus, Alarme auf dem alphabetisch ersten Lageplan auszulösen. Wenn keine Kameras und Lagepläne mit dem Server verbunden sind, wählt der Server aus, Alarme auf allen Geräten auszulösen.

Sie können die automatische Regelgenerierung konfigurieren, wenn Sie den Senstar Network Manager

als Integration zum Server hinzufügen, oder Sie können die Integration nachträglich bearbeiten.



Wenn Sie die Generierungseinstellungen der Senstar Network Manager-Integration bearbeiten und das Kontrollkästchen "Automatically generate rules" ausgewählt ist, löscht der Server die vorhandenen automatisch generierten Regeln und generiert neue Regeln. Um Ihre ursprünglichen automatisch generierten Regeln beizubehalten, deaktivieren Sie das Kontrollkästchen "Automatically generate rules", bevor Sie Ihre Änderungen speichern.

Mit Senstar Network Manager verbinden

Verbinden Sie den Server mit dem Senstar Network Manager, um Ereignisse aus dem Senstar Network Manager als Auslöser für Aktionen zu verwenden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Integrations.
2. Klicken Sie auf Add Hardware.
3. Wählen Sie in der Liste Device Type den Eintrag Senstar Network Manager aus.
4. Geben Sie im Feld Name einen aussagekräftigen Namen für den Senstar Network Manager ein. Dieser Name erscheint in der Geräteliste in der

Konfigurationsoberfläche des Server

und im Gerätebaum in der

Oberfläche des Windows Client

.

1. Geben Sie im Feld IP Address die IP-Adresse des Senstar Network Manager ein.
2. Geben Sie im Feld Secondary IP Address die IP-Adresse eines sekundären (redundanten) Senstar Network Manager ein.
3. Geben Sie im Feld Unit ID die ID des Senstar Network Manager ein.
4. Klicken Sie auf Connect to Device.
5. Wählen Sie in der Liste Sources die Knoten aus, die Sie zum Server hinzufügen möchten. Wenn Ihre Auswahl auch für alle untergeordneten Knoten gelten soll, schalten Sie den Schalter

Cascade Selection

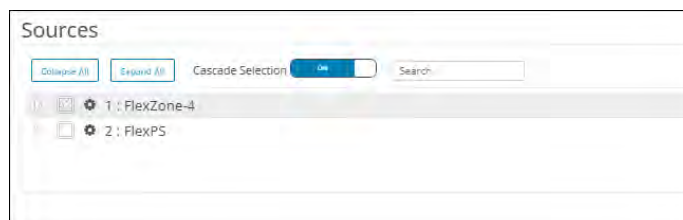
ein. Um zu verhindern, dass Ihre Auswahl andere Knoten beeinflusst, schalten Sie den Schalter

Cascade Selection

aus. Um nach einem Knoten zu suchen, geben Sie die Begriffe in das Feld

Search

ein — die Quellenliste wird nach den Suchbegriffen gefiltert.



1. Konfigurieren Sie im Abschnitt Rules, ob und wie der Server automatisch Regeln für die Integration des Senstar Network Manager erstellt. image::air_network_manager_connect_rules.png[]

Sie können sowohl Sensorregeln als auch Geräteregeeln automatisch erstellen.

Für Sensorregeln können Sie die Granularität auswählen: global, Gerät oder Sensor. Wenn Sie Global rule auswählen, erstellt der Server eine einzelne Regel für alle ausgewählten Sensoren. Wenn Sie Device alarm rules auswählen, erstellt der Server eine Regel für jedes der ausgewählten Geräte. Wenn Sie Sensor alarm rules auswählen, erstellt der Server eine Regel für jeden der ausgewählten Sensoren. Zusätzlich können Sie auswählen, ob alle Vorfallstypen in einer einzigen Regel zusammengefasst werden, oder Sie können separate Sensorregeln für jeden Vorfallstyp erstellen.

Für Geräteregeeln können Sie wählen, eine globale Diagnoseregel für alle ausgewählten Geräte zu erstellen, oder eine Gerätediagnoseregel für jedes ausgewählte Gerät zu erstellen.

1. Wählen Sie in der Liste Groups den Gerätebaumordner aus, in dem der Senstar Network Manager angezeigt werden soll.
2. Klicken Sie auf Save.

Einstellungen für Senstar Network Manager

General

+



+

Einstellung	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen für die Senstar Network Manager-Instanz ein. Dieser Name erscheint im Gerätebaum.
Type	Dieses Feld zeigt den Integrationstyp an. Sie wählen den Typ beim Hinzufügen der Hardware aus.
IP Address	Geben Sie die IP-Adresse des Senstar Network Manager ein.
Secondary IP Address	Geben Sie die sekundäre IP-Adresse des Senstar Network Manager ein. Die sekundäre IP-Adresse ist die IP-Adresse des sekundären Senstar Network Manager, wenn Redundanz konfiguriert ist.
Unit ID	Geben Sie die Unit-ID des Senstar Network Manager ein. Die Unit-ID wird bei der Installation des Senstar Network Manager festgelegt. Wenden Sie sich für weitere Informationen an den Senstar Network Manager-Administrator.
Import XML	Klicken Sie hier, um eine XML-Datei mit Konfigurationsinformationen zu importieren.
Export XML	Klicken Sie hier, um eine XML-Datei mit Konfigurationsinformationen zu exportieren.
Show XML	Klicken Sie hier, um die Konfigurationsinformationen anzuzeigen.

Connect

Einstellung	Beschreibung
Save and Reconnect	Klicken Sie hier, um die Änderungen an den allgemeinen Einstellungen zu speichern und zu versuchen, eine Verbindung zum Senstar Network Manager herzustellen.

Sources

Einstellung	Beschreibung
Collapse All	Klicken Sie hier, um den Quellbaum zu reduzieren und nur die obersten Ebenen anzuzeigen.
Expand All	Klicken Sie hier, um den Quellbaum zu erweitern und alle Ebenen anzuzeigen.
Cascade Selection	Aktivieren Sie diese Option, um beim Auswählen eines Geräts automatisch alle untergeordneten Ebenen mit auszuwählen. Deaktivieren Sie diese Option, um nur das ausgewählte Gerät auszuwählen.
Search	Geben Sie Suchbegriffe ein, um die Quellliste zu filtern.

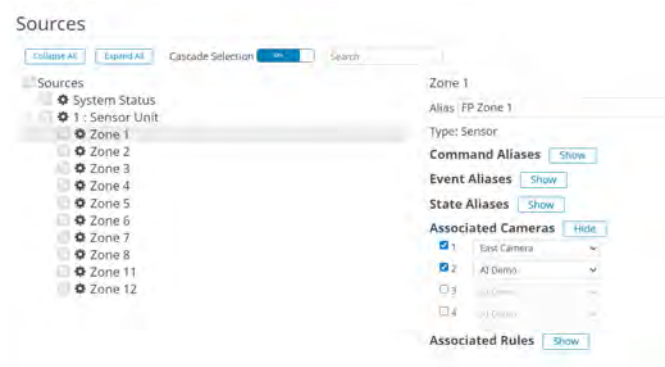
Rules

Einstellung	Beschreibung
Automatically generate rules	Wählen Sie diese Option, damit der Server automatisch Regeln für die Senstar Network Manager-Integration generiert.
No sensor rules	Wählen Sie diese Option, um zu verhindern, dass der Server automatisch Regeln für an den Senstar Network Manager angeschlossene Sensoren generiert, oder damit der Server alle vorhandenen automatisch generierten Sensorregeln löscht.
Global rule	Wählen Sie diese Option, damit der Server automatisch eine einzige Regel generiert, die für alle an den Senstar Network Manager angeschlossenen Sensoren gilt. Sie können eine einzige Regel für alle Vorfalltypen erstellen (gruppiert) oder Regeln für jeden Vorfalltyp erstellen (separat).
Device alarm rules	Wählen Sie diese Option, damit der Server automatisch eine separate Regel für jedes in der Sources-Liste ausgewählte Gerät generiert. Sie können eine einzige Regel für alle Vorfalltypen erstellen (gruppiert) oder Regeln für jeden Vorfalltyp erstellen (separat).
Sensor alarm rules	Wählen Sie diese Option, damit der Server automatisch eine separate Regel für jeden in der Sources-Liste ausgewählten Sensor generiert. Sie können eine einzige Regel für alle Vorfalltypen erstellen (gruppiert) oder Regeln für jeden Vorfalltyp erstellen (separat).
No diagnostic rules	Wählen Sie diese Option, um zu verhindern, dass der Server automatisch Diagnoseregeln für an den Senstar Network Manager angeschlossene Geräte generiert, oder damit der Server alle vorhandenen automatisch generierten Geräteregele löscht.
Global diagnostic rule	Wählen Sie diese Option, damit der Server automatisch eine einzige Diagnoseregeln generiert, die für alle an den Senstar Network Manager angeschlossenen Geräte gilt.

Einstellung	Beschreibung
Device diagnostic rules	Wählen Sie diese Option, damit der Server automatisch eine separate Diagnoseregeln für jedes in der Sources-Liste ausgewählte Gerät generiert.

Kamera mit einer Quelle verknüpfen

Sie können bis zu vier Kameras mit einer Hardwarequelle verknüpfen, um den Bereich, in dem sich die Hardwarequelle befindet, zu überwachen.



1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Integrations.
2. Wählen Sie die Hardware aus.
3. Klicken Sie auf Edit.
4. Wählen Sie im Bereich Sources die Hardwarequelle aus, mit der Sie Kameras verknüpfen möchten. Wenn Sie mehrere Hardwarequellen auswählen und die Kameras mit allen ausgewählten Quellen verknüpfen möchten, klicken Sie auf das Kontrollkästchen

Selected

- .
1. Klicken Sie neben Associated Cameras auf Show.
 2. Wählen Sie für jede zu verknüpfende Kamera den Kameraplatz aus und wählen Sie die Kamera aus der Liste aus. image::air_server_integrations_sources_camera_associate_01.png[]
 3. Klicken Sie auf Save.

Zugangskontrollgerät

Der Server kann Daten von Zugangskontrollgeräten verwenden, um Ereignisse auszulösen. Sie können die Konfigurationsoberfläche des Server verwenden, um ein Zugangskontrollgerät in den Server zu integrieren. Nachdem Sie das Zugangskontrollgerät hinzugefügt haben, können Sie die Zugangskontrollgeräte in der Lösung auswählen, die als Quellen für Ereignisse verwendet werden sollen.

Der Server unterstützt die folgenden Hersteller:

- Axiom
- Axis PACS
- Gallagher

- JCI P2000
- Siemens SPC
- Software House

Zugangskontrollgerät hinzufügen

Sie können Zugangskontrollgeräte über die Registerkarte Access Devices in der Konfigurationsoberfläche des Server zum Server hinzufügen.

In manchen Fällen müssen Sie möglicherweise zusätzliche Aufgaben am Zugangskontrollgerät durchführen. Informationen zu einem bestimmten Zugangskontrollgerät finden Sie im Senstar Xnet, indem Sie nach dem Hersteller des Zugangskontrollgeräts suchen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Access Devices.
2. Wählen Sie in der Liste Manufacturer den Hersteller des Zugangskontrollsystems aus. Welche Felder angezeigt werden, hängt vom ausgewählten Hersteller ab. Wenn der Hersteller nicht in der Liste enthalten ist, versuchen Sie, das Zugangskontrollgerät als Hardware (Add hardware) oder als Integration (Add an integration) hinzuzufügen.
3. Wählen Sie in der Liste Server den Server aus, dem Sie das Zugangskontrollgerät hinzufügen möchten.
4. Geben Sie im Feld IP Address die IP-Adresse des Zugangskontrollsystems ein.
5. Geben Sie in den Feldern Username und Password die Anmeldedaten für das Zugangskontrollsystem ein.
6. Klicken Sie auf Connect.
7. Wählen Sie in der Liste Sources die Geräte im Zugangskontrollsystem aus, die Ereignisse auf dem Server auslösen können.
8. Klicken Sie auf Save.

Gerätebaum

Der Gerätebaum organisiert und zeigt Geräte in der Oberfläche des Windows Client an.

Gerät finden

Um ein bestimmtes Gerät schnell zu finden, verwenden Sie einen Filter.

Filtern

Verwenden Sie das Filterfeld oben im Gerätebaum, um die Liste auf Geräte einzugrenzen, deren Name mit dem eingegebenen Text übereinstimmt.

Zurücksetzen

Um den Filter zurückzusetzen und die Liste der Geräte wiederherzustellen, klicken Sie auf Clear Filter.

Gerätegruppen verwalten

Sie können die Geräte in Gruppen organisieren. Änderungen, die Sie vornehmen, werden sofort in der Oberfläche des Windows Client angezeigt.

Gerätegruppe erstellen

Sie können Gerätegruppen verwenden, um Ihre Geräte zu organisieren.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Device Tree.
2. Klicken Sie auf Create Group. Ein neuer Ordner mit dem Namen

New Group

erscheint im Gerätebaum.

1. Geben Sie einen Namen für die Gruppe ein und drücken Sie die Eingabetaste.
2. Ziehen Sie Geräte in die Gruppe.
3. Klicken Sie auf Save.

Gerätegruppe ändern

Sie können den Namen der Gerätegruppe ändern oder Geräte zur Gerätegruppe hinzufügen und entfernen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Device Tree.
2. Um den Namen der Gerätegruppe zu ändern, führen Sie die folgenden Aufgaben aus:
 - a. Wählen Sie die Gerätegruppe aus.
 - b. Klicken Sie auf Edit.
 - c. Geben Sie einen Namen für die Gerätegruppe ein.
 - d. Klicken Sie auf Save.
3. Um ein Gerät in die Gerätegruppe zu verschieben, führen Sie die folgenden Aufgaben aus:
 - a. Klicken Sie auf ein Gerät und ziehen Sie es in die Gerätegruppe.
 - b. Klicken Sie auf Save.

Gerätegruppe kopieren

Sie können eine Gerätegruppe kopieren, um sie als Vorlage für eine neue Gerätegruppe zu verwenden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Device Tree.
2. Wählen Sie eine Gerätegruppe aus.
3. Klicken Sie auf Clone.
4. Geben Sie einen Namen für die neue Gerätegruppe ein.
5. Klicken Sie auf Save.

Gerätegruppe löschen

Sie können eine Gerätegruppe aus dem Gerätebaum löschen. Wenn Sie eine Gerätegruppe löschen, werden die Geräte in der Gruppe in den Stammordner des Gerätebaums verschoben.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Device Tree.
2. Wählen Sie eine Gerätegruppe aus.
3. Klicken Sie auf Delete.

Kameras mit Sensoren und Zonen verknüpfen

Sie können eine oder mehrere Kameras und Regeln mit einem Sensor oder einer Zone verknüpfen, sodass der Windows Client das zugehörige Video und die Regeln anzeigt, sobald der Sensor oder die Zone ausgewählt wird.

Wenn ein Sensor oder eine Zone aktiviert wird, kann ein Operator das Video, das den Bereich abdeckt, schnell aufrufen, ohne zuerst die richtige Kamera im Gerätebaum suchen zu müssen. Die Verknüpfung wird auf dem Server gespeichert und gilt für jeden Windows Client, der mit dem Server verbunden ist.

Kameras im Gerätebaum mit einem Sensor oder einer Zone verknüpfen

1. Öffnen Sie in der Konfigurationsoberfläche des Server oder im Windows Client den Gerätebaum.
2. Klicken Sie mit der rechten Maustaste auf den Sensor oder die Zone.
3. Klicken Sie auf Associate Cameras.
4. Wählen Sie eine oder mehrere Kameras aus der Liste aus.
5. Klicken Sie auf Save.

Regeln mit einem Sensor oder einer Zone verknüpfen

1. Klicken Sie im Gerätebaum mit der rechten Maustaste auf den Sensor oder die Zone.
2. Klicken Sie auf Associate Rules.
3. Wählen Sie eine oder mehrere Regeln aus der Liste aus.
4. Klicken Sie auf Save.

Kameras auf einem Lageplan mit einem Sensor oder einer Zone verknüpfen

1. Öffnen Sie im Windows Client den Lageplan, der den Sensor oder die Zone enthält.
2. Klicken Sie mit der rechten Maustaste auf das Symbol des Sensors oder der Zone.
3. Klicken Sie auf Associate Cameras.
4. Wählen Sie eine oder mehrere Kameras aus der Liste aus.
5. Klicken Sie auf Save.

Nachdem Sie Kameras mit einem Sensor oder einer Zone verknüpft haben, erscheinen die verknüpften Kameras im Rechtsklick-Menü dieses Sensors oder dieser Zone. Beim Auswählen einer verknüpften Kamera wird die Kamera im aktiven Anzeigebereich geöffnet.

Sequenzen

Sequenzen sind Konfigurationen für Videopaneln in der Oberfläche des Windows Client, die mehrere Kameras durchlaufen und Video für eine festgelegte Zeit anzeigen können.

In der Konfigurationsoberfläche des Server fügen Sie Kameras zur Sequenz hinzu und legen anschließend fest, wie lange das Videopanel in der Oberfläche des Windows Client Video anzeigt, bevor es zur nächsten Kamera wechselt. Der Gerätebaum in der Oberfläche des Windows Client listet alle verfügbaren Sequenzen auf. Sie können eine Sequenz in einem beliebigen Videopanel öffnen.

Sequenz suchen

Um schnell eine bestimmte Sequenz zu finden, verwenden Sie Filter und Sortierung.

Filter

Sie können die Sequenzliste anhand des folgenden Filters filtern:

- Sequenzname (Name)
 1. Klicken Sie in der Server-Konfigurationsoberfläche auf Devices > Carousels.
 2. Klicken Sie auf die Lupe, um die Filter-Textfelder einzublenden.
 3. Definieren Sie die Filterkriterien.
 4. Klicken Sie auf Apply filter.

Sortierung

Sie können die Liste der Sequenzen sortieren, indem Sie auf den Spaltennamen klicken. Durch Klicken auf den Spaltennamen wird zwischen aufsteigender und absteigender Reihenfolge gewechselt.

Zurücksetzen

Um den Filter zurückzusetzen und die Liste der Sequenzen wiederherzustellen, klicken Sie auf Clear Filter.

Sequenzen verwalten

Sie können Sequenzen erstellen, ändern, kopieren und löschen.

Sequenz erstellen

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Carousels.
2. Klicken Sie auf Add Carousel.
3. Geben Sie einen Namen für die Sequenz ein.
4. Wählen Sie in der Liste Available Cameras on Servers die Kameras aus, die der Sequenz hinzugefügt werden sollen, und klicken Sie auf Add Selected.
5. Ziehen Sie in der Liste Camera die Kameras per Drag & Drop, um die Reihenfolge der Sequenz festzulegen, und definieren Sie die Anzahl der Sekunden, für die das Kameraansichtspanel die Kamera anzeigt.
6. Klicken Sie auf Save.

Sequenz ändern

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Carousels.
2. Wählen Sie die Sequenz aus und klicken Sie auf Edit.
3. Führen Sie eine der folgenden Aufgaben aus:
 - a. Um den Namen der Sequenz zu ändern, geben Sie im Feld Name einen neuen Namen ein.
 - b. Um eine Kamera zur Sequenz hinzuzufügen, wählen Sie die Kamera in der Liste Available Cameras on Servers aus und klicken Sie auf Add Selected.
 - c. Um eine Kamera aus der Sequenz zu entfernen, markieren Sie die Kamera in der Liste Camera und klicken Sie auf die Schaltfläche X.
 - d. Um die Zeitdauer für jede Kamera zu ändern, geben Sie neue Werte in die Felder Seconds ein.
4. Klicken Sie auf Save.

Sequenz kopieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Carousels.
2. Wählen Sie die Sequenz aus und klicken Sie auf Clone.
3. Ändern Sie die Sequenz.
4. Klicken Sie auf Save.

Sequenz löschen

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Carousels.
2. Wählen Sie die Sequenz aus und klicken Sie auf Delete.

Sicherheit

Die Sicherheitseinstellungen auf dem Server ermöglichen es Ihnen, die Authentifizierung für Benutzer zu konfigurieren, Berechtigungen für Benutzer und Gruppen schnell festzulegen und zu ändern sowie Wasserzeichen zu Videos hinzuzufügen.

Sie greifen auf die Sicherheitseinstellungen über die Registerkarte Security in der Server-Konfigurationsoberfläche zu. Die Registerkarte Security enthält die Registerkarten Users, Groups, Security Profiles und Logins.

Benutzer

Benutzer sind Personen mit Berechtigung zum Zugriff auf und zur Verwendung des Server, Windows Client und des Web Client.

Benutzer hinzufügen

Worum es geht

Ein Benutzer in Senstar Symphony ist eine Identität, die sich beim Server oder bei einer Clientanwendung anmelden kann. Benutzer erben Berechtigungen aus den [Gruppen](#), denen sie angehören, und nicht direkt von sich selbst — das Hinzufügen eines Benutzers besteht im Wesentlichen darin, die Identität zu erstellen und sie den richtigen Gruppen zuzuordnen.

Wenn Ihr Standort Active Directory verwendet, ist es vorzuziehen, eine [Active Directory-Gruppe zu verknüpfen](#), anstatt Benutzer einzeln im Server zu verwalten.

Wann Sie es verwenden würden

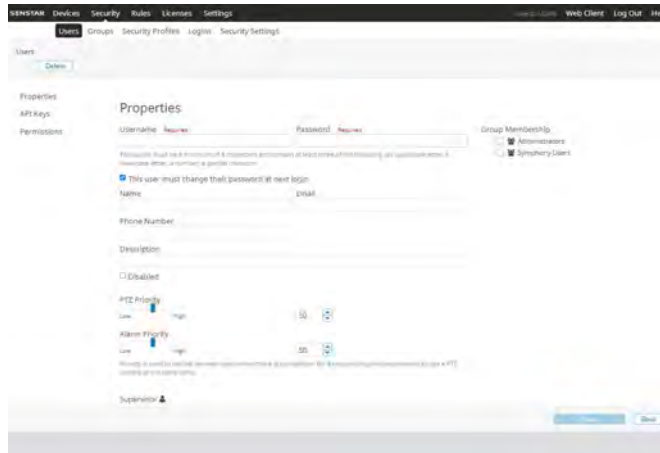
- Eine neue Person tritt dem Team bei und benötigt eine Anmeldemöglichkeit.
- Sie initialisieren eine neue Bereitstellung mit Dienstkonten, Schichtoperatoren und Administratoren.
- Sie benötigen ein temporäres Konto für einen kurzfristigen Auftragnehmer — setzen Sie am Ende des Engagements **Disabled** mit einer Begründung, anstatt den Datensatz zu löschen, damit Berichte konsistent bleiben.

Voraussetzungen

- Berechtigung zum Hinzufügen von Benutzern (siehe [Benutzerberechtigungen](#)).
- Die [Gruppen](#), die den neuen Benutzer aufnehmen sollen, sind bereits vorhanden.
- Wenn der Benutzer andere überwachen wird, ist die [Supervisor-Gruppe](#) vorhanden.

Vorgehensweise

1. Klicken Sie in der Konfigurationsoberfläche des Servers auf **Security > Users**.
2. Klicken Sie auf **Add**.
3. Geben Sie die Identitätsfelder des Benutzers ein (Name, Anmeldename, Kennwort, E-Mail, Telefon, Beschreibung).



4. (Optional) Um den Benutzer zu deaktivieren, ohne den Datensatz zu löschen, wählen Sie **Disabled** und geben Sie einen Grund ein. Deaktivierte Benutzer können sich nicht anmelden, bleiben aber in Berichten und Audit-Protokollen erhalten.
5. Legen Sie **PTZ Priority** fest. Wenn zwei Benutzer gleichzeitig versuchen, dieselbe PTZ-Kamera zu steuern, gewinnt der Benutzer mit der höheren Priorität; ein Benutzer mit gleicher oder niedrigerer Priorität wird blockiert, bis der Benutzer mit höherer Priorität die Steuerung freigibt. Der Schieberegler reicht von 1 (niedrigste) bis 10 (höchste). Verwenden Sie 10 nur für Vorgesetzte oder Disponenten, die die Kontrolle jederzeit übernehmen können müssen.
6. Legen Sie **Alarm Priority** fest. Wenn **zweistufige erweiterte Alarme** verwendet werden, sieht der Benutzer mit der höheren Priorität den Alarm zuerst. Verwenden Sie dieselbe 1–10-Skala; die meisten Operatoren bleiben beim Standardwert.
7. Wählen Sie unter **Group Membership** die Gruppen aus, denen der Benutzer angehört. Berechtigungen werden aus diesen Gruppen abgeleitet — ein Benutzer ohne Gruppenmitgliedschaften kann sich anmelden, aber kaum etwas tun.
8. Wählen Sie unter **Supervisor** die Gruppe aus, deren Mitglieder diesen Benutzer **imitieren** dürfen. Lassen Sie das Feld leer, wenn der Standort keine Supervisor-Imitation verwendet.
9. Klicken Sie auf **Save**.

Nach dem Hinzufügen

Geben Sie die Anmeldedaten dem Benutzer über den sicheren Kanal Ihrer Organisation weiter (nicht im Klartext per E-Mail). Wenn die Standortrichtlinie eine Änderung bei der ersten Anmeldung erfordert, verwenden Sie **Kennwortänderung erzwingen**.

Verwandte Aufgaben

- **Benutzer kopieren** — schneller als das erneute Eingeben von Feldern für einen ähnlichen Benutzer.
- **Benutzer zu einer Gruppe hinzufügen**
- **Kennwortänderung erzwingen**

- **Benutzerberechtigungen**

Benutzer kopieren

Sie können einen Benutzer kopieren, um ihn als Vorlage für einen neuen Benutzer zu verwenden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Security > Users.
2. Wählen Sie einen Benutzer aus und klicken Sie auf Clone.
3. Geben Sie Informationen für den Benutzer ein.
4. Um den Benutzer zu deaktivieren, aktivieren Sie das Kontrollkästchen Disabled und geben Sie einen Grund ein.
5. Definieren Sie mit dem Schieberegler Priority oder dem Textfeld eine Priorität für den Benutzer, um Ressourcenkonflikte aufzulösen.
6. Wählen Sie im Bereich Group Membership die Gruppen aus, denen der Benutzer angehört.
7. Wählen Sie in der Liste Supervisor die Gruppe aus, die Benutzer enthält, die diesen Benutzer imitieren können.
8. Klicken Sie auf Save.

Benutzer zu einer Gruppe hinzufügen

Sie können einen Benutzer jederzeit zu einer Gruppe hinzufügen, um ihm die Berechtigungen dieser Gruppe zuzuweisen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Security > Users.
2. Wählen Sie einen Benutzer aus und klicken Sie auf Edit.
3. Wählen Sie im Bereich Group Membership die Gruppe aus, zu der Sie den Benutzer hinzufügen möchten. image::air_server_user_group_add_8_group_membership.png[]
4. Klicken Sie auf Save.

Passwortänderung erzwingen

Sie können einen Benutzer zwingen, ein Kennwort zu ändern, wenn er sich das nächste Mal beim Server, beim Windows Client oder beim Web Client anmeldet.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Security > Users.
2. Wählen Sie den Benutzer aus und klicken Sie auf Edit.
3. Wählen Sie This user must change their password at next login.
4. Klicken Sie auf Save.

Wenn sich der Benutzer das nächste Mal anmeldet, wird er zur Änderung des Kennworts aufgefordert.

Supervisor-Imitation

Supervisor-Impersonation ermöglicht zwei Benutzern mit geringeren Berechtigungen, sich gleichzeitig anzumelden, um einen einzelnen Benutzer mit höheren Berechtigungen zu impersonifizieren.

Supervisor-Impersonation ist die Anwendung des Vier-Augen-Prinzips, um zusätzliche Sicherheit für den Windows Client zu schaffen. Sie können diese Funktion verwenden, um sicherzustellen, dass zwei Personen anwesend sind, wenn ein Benutzer eine Operation in der Windows Client-Oberfläche

ausführt.

Benutzer für Supervisor-Imitation konfigurieren

Um die Supervisor-Imitation zu verwenden, müssen Sie einen Benutzer konfigurieren, den die zwei anderen Benutzer imitieren können.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Security > Users.
2. Führen Sie eine der folgenden Aufgaben aus:
 - Um einen neuen Benutzer für die Supervisor-Imitation zu erstellen, klicken Sie auf Add.
 - Um einen vorhandenen Benutzer für die Supervisor-Imitation zu verwenden, wählen Sie den Benutzer aus und klicken Sie auf Edit.
3. Wählen Sie im Abschnitt Properties die Option Enable Two Person Rule aus.
4. Wählen Sie in jeder Gruppenliste die Gruppen aus, aus denen die Benutzer den Benutzer imitieren dürfen.
5. Klicken Sie auf Save.

Supervisor-Imitation aktivieren

Um die Option zur Supervisor-Imitation im Windows Client verfügbar zu machen, müssen Sie die Funktion zur Konfigurationsdatei hinzufügen.

1. Öffnen Sie die Datei acc.ini unter %appdata%\Senstar8.
2. Fügen Sie im Abschnitt **[Main]** den folgenden Text hinzu:

```
ShowTwoManRule=True
```

1. Speichern und schließen Sie die Datei acc.ini.

Die Option

Supervisor Logon

ist auf der Anmeldeseite des

Windows Client

sichtbar.

Supervisor imitieren

Zwei Benutzer können sich am Windows Client anmelden, um einen Benutzer zu imitieren und Zugriff auf zusätzliche Funktionen zu erhalten.

1. Klicken Sie in der Oberfläche des Windows Client auf den Benutzernamen und dann auf Log On/Switch User, um das Anmeldefenster zu öffnen.
2. Wählen Sie in der Liste Server den Server aus, für den Sie die Supervisor-Imitation konfiguriert haben.
3. Geben Sie die Anmeldedaten des ersten Benutzers ein.
4. Aktivieren Sie das Kontrollkästchen Supervisor Logon.
5. Geben Sie die Anmeldedaten des zweiten Benutzers ein.

6. Geben Sie den Namen des Supervisor-Imitationsbenutzers ein.
7. Geben Sie im Feld Reason den Grund für die Imitation eines Supervisors ein.
8. Klicken Sie auf OK.

Gruppen

Gruppen sind Sammlungen von Benutzern mit ähnlichen Berechtigungen für den Server und Windows Client.

Gruppen können Benutzer enthalten, die Sie auf dem Server erstellen und verwalten, oder, wenn Sie die Active Directory-Authentifizierung verwenden, können Gruppen ihre Mitgliedschaft mit einer zugeordneten Active Directory-Gruppe synchronisieren.

Gruppe hinzufügen

Sie können eine Gruppe hinzufügen, um eine Sammlung von angepassten Berechtigungen für Benutzer zu erstellen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Security > Groups.
2. Klicken Sie auf Add.
3. Geben Sie einen Namen für die Gruppe ein.
4. Wählen Sie die übergeordnete Gruppe aus.
5. Geben Sie eine Beschreibung für die Gruppe ein.
6. Um die Gruppe mit einer Active Directory-Gruppe zu verknüpfen, führen Sie die folgenden Schritte aus:
 - a. Klicken Sie auf Associate.
 - b. Suchen Sie die Active Directory-Gruppe und wählen Sie sie aus.
 - c. Klicken Sie auf OK.
7. Klicken Sie auf Save.

Nachdem Sie eine Gruppe erstellt haben, müssen Sie die Berechtigungen für jedes verwendete Sicherheitsprofil festlegen.

Gruppe kopieren

Sie können eine Gruppe kopieren, um sie als Vorlage für eine neue Gruppe zu verwenden.

Wenn Sie eine Gruppe kopieren, werden die Berechtigungen für alle Sicherheitsprofile in die neue Gruppe geklont.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Security > Groups.
2. Wählen Sie eine Gruppe aus und klicken Sie auf Clone.
3. Geben Sie im Feld Name einen Namen für die Gruppe ein.
4. Wählen Sie im Feld Group Parents die Gruppen aus, die als übergeordnete Gruppen fungieren.
5. Geben Sie im Feld Description eine Beschreibung für die Gruppe ein.
6. Um die Gruppe einer Active Directory-Gruppe zuzuordnen, gehen Sie wie folgt vor:

- a. Klicken Sie auf Associate.
 - b. Suchen Sie nach der Active Directory-Gruppe und wählen Sie sie aus.
 - c. Klicken Sie auf OK.
7. Klicken Sie auf Save.
 8. Wählen Sie im Bereich Group Membership die Gruppen aus, denen der Benutzer angehört.
 9. Wählen Sie in der Liste Supervisor die Gruppe aus, die Benutzer enthält, die diesen Benutzer imitieren können.
 10. Klicken Sie auf Save.

Sicherheitsprofile

Ein Sicherheitsprofil ist eine Sammlung von Berechtigungen, die Sie auf alle Benutzer und Gruppen anwenden können. Sicherheitsprofile machen es einfach, die Berechtigungen für Benutzer und Gruppen im Server zu wechseln.

Üblicherweise fügen Sie Sicherheitsprofile zum Server hinzu, um schneller auf externe Änderungen reagieren zu können. Jeder Benutzer und jede Benutzergruppe kann innerhalb jedes Sicherheitsprofils einen bestimmten Satz von Berechtigungen haben. Wenn Sie ein Sicherheitsprofil aktivieren, wechseln alle Benutzer und Benutzergruppen zu den Berechtigungen in diesem Sicherheitsprofil.

Workflow für Sicherheitsprofile

1. Fügen Sie ein Sicherheitsprofil hinzu, um einen neuen Container für Benutzer- und Gruppenberechtigungen zu erstellen.
2. Legen Sie die Sicherheitsprofil-Berechtigungen fest, um die Berechtigungen zu definieren, die Benutzer und Gruppen haben, wenn das Sicherheitsprofil aktiv ist.
3. Aktivieren Sie das Sicherheitsprofil, um die Berechtigungen auf Benutzer und Gruppen anzuwenden.

Anwendungsbeispiel

Sie können beispielsweise ein Standard-Sicherheitsprofil und ein Sicherheitsprofil für die Brandbekämpfung erstellen. Im Normalbetrieb ist das Standard-Sicherheitsprofil aktiv und die den Benutzern und Benutzergruppen zugewiesenen Berechtigungen sind ebenfalls aktiv. Im Falle eines Brandereignisses aktivieren Sie das Brandbekämpfungs-Sicherheitsprofil, das einer Brandbekämpfungsgruppe die Berechtigung erteilt, alle Kameras der Anlage anzuzeigen, Audio von Kameras zu übertragen und Aufzeichnungen zu durchsuchen, um die Notfallreaktion zu unterstützen. Wenn die Brandbekämpfungsmannschaft den Vorfall behoben hat, reaktivieren Sie das Standard-Sicherheitsprofil und kehren zum Normalbetrieb zurück.

Sicherheitsprofil hinzufügen

Sie können ein vorhandenes Sicherheitsprofil kopieren, um ein weiteres Sicherheitsprofil zum Server hinzuzufügen.

Der Server enthält das Sicherheitsprofil Default. Sie können dieses Sicherheitsprofil als Vorlage für andere Sicherheitsprofile verwenden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Security > Security Profiles.
2. Wählen Sie ein Sicherheitsprofil aus und klicken Sie auf Copy.

3. Geben Sie im Feld Name einen Namen für das Sicherheitsprofil ein.
4. (Optional) Geben Sie im Feld Description eine Beschreibung für das Sicherheitsprofil ein.
5. Klicken Sie auf Save.

Berechtigungen für Sicherheitsprofil festlegen

Sie können die Sicherheitsprofil-Berechtigungen für einen Benutzer oder eine Gruppe festlegen. Wenn Sie das Sicherheitsprofil aktivieren, wendet der Server die mit dem Sicherheitsprofil verknüpften Berechtigungen auf die Benutzer und Gruppen an.

In den meisten Fällen legen Sie die Berechtigungen für das Standard-Sicherheitsprofil fest. Wenn Sie jedoch mehrere Sicherheitsprofile verwenden, müssen Sie möglicherweise benutzerdefinierte Berechtigungen für jedes Sicherheitsprofil festlegen.



Wenn Sie umfangreiche Änderungen am Standard-Sicherheitsprofil vornehmen möchten, sollten Sie ein neues Sicherheitsprofil für den regulären Gebrauch erstellen und das Standard-Sicherheitsprofil als Vorlage für zusätzliche Sicherheitsprofile beibehalten.

1. Führen Sie in der Server-Konfigurationsoberfläche eine der folgenden Aufgaben aus:
 - Um die Sicherheitsprofil-Berechtigungen für einen Benutzer festzulegen, klicken Sie auf Security > Users.
 - Um die Sicherheitsprofil-Berechtigungen für eine Gruppe festzulegen, klicken Sie auf Security > Groups.
2. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf Edit.
3. Wählen Sie in der Liste Security Profile das Sicherheitsprofil aus, für das Sie Berechtigungen festlegen möchten.
4. Klicken Sie im Berechtigungsbaum auf die Berechtigungskategorie, die Sie festlegen möchten.
image::ROOT:air_server_security_profile_permissions_set_8_permissions.png[]
5. Legen Sie in der Berechtigungsliste die Berechtigungen fest.
image::ROOT:air_server_security_profile_permissions_set_8_permission_list.png[]
6. Klicken Sie auf Save.

Standortberechtigungen

General

Berechtigung	Beschreibung
Change IO State	Diese Berechtigung erlaubt einem Benutzer, den IO-Zustand von Geräten in der Windows Client-Oberfläche zu ändern.
Configure Maps	Diese Berechtigung erlaubt einem Benutzer, Lagepläne in der Windows Client-Oberfläche zu konfigurieren.
Connect	Diese Berechtigung erlaubt einem Benutzer, sich mit Servern zu verbinden.
Delete Footage	Diese Berechtigung erlaubt einem Benutzer, Videoaufzeichnungen in der Windows Client-Oberfläche zu löschen.

Berechtigung	Beschreibung
Export Video	Diese Berechtigung erlaubt einem Benutzer, Video aus der Windows Client-Oberfläche zu exportieren.
Get Logs	Diese Berechtigung erlaubt einem Benutzer, Protokolle in der Windows Client-Oberfläche anzuzeigen und herunterzuladen.
Manage Bookmarks	Diese Berechtigung erlaubt einem Benutzer, Lesezeichen in der Windows Client-Oberfläche zu erstellen und zu bearbeiten.
Manage Services	Diese Berechtigung erlaubt einem Benutzer, Senstar Symphony-Dienste in der Windows Client-Oberfläche zu starten, zu beenden und neu zu starten.
Play Sounds	Diese Berechtigung erlaubt einem Benutzer, Audio in der Windows Client-Oberfläche abzuspielen.

Configuration

Berechtigung	Beschreibung
Add Devices	Diese Berechtigung erlaubt einem Benutzer, Geräte in der Server-Konfigurationsoberfläche hinzuzufügen.
Change Access Control	Diese Berechtigung erlaubt einem Benutzer, Zugangskontrollgeräte in der Server-Konfigurationsoberfläche zu konfigurieren.
Change Settings	Diese Berechtigung erlaubt einem Benutzer, die allgemeinen Einstellungen in der Server-Konfigurationsoberfläche zu ändern.

Alarm

Berechtigung	Beschreibung
Add Alarm	Diese Berechtigung erlaubt einem Benutzer, Alarme in der Windows Client-Oberfläche zu erstellen.
Manage Alarms	Diese Berechtigung erlaubt einem Benutzer, Alarme in der Windows Client-Oberfläche zu bearbeiten und zu löschen.
Mark Alarms	Diese Berechtigung erlaubt einem Benutzer, Alarme in der Windows Client-Oberfläche als Alarm, Fehlalarm oder echt-handlungsrelevant zu markieren.
View Alarms	Diese Berechtigung erlaubt einem Benutzer, Alarme in der Windows Client-Oberfläche anzuzeigen.

Backup

Berechtigung	Beschreibung
Backup	Diese Berechtigung erlaubt einem Benutzer, Backup-Optionen in der Server-Konfigurationsoberfläche zu konfigurieren.
Restore	Diese Berechtigung erlaubt einem Benutzer, eine Konfiguration in der Server-Konfigurationsoberfläche wiederherzustellen.

Face Recognition

Berechtigung	Beschreibung
Change faces/people	Diese Berechtigung erlaubt einem Benutzer, Gesichter und zugehörige Informationen für die Videoanalyse "Gesichtserkennung" in der Windows Client-Oberfläche zu bearbeiten.
Manage Face Lists	Diese Berechtigung erlaubt einem Benutzer, Gesichter zu einer Liste hinzuzufügen oder daraus zu entfernen.
View faces/people	Diese Berechtigung erlaubt einem Benutzer, Gesichter und zugehörige Informationen für die Videoanalyse "Gesichtserkennung" in der Windows Client-Oberfläche anzuzeigen.

LPR

Berechtigung	Beschreibung
Add or Edit License Plate Metadata	Diese Berechtigung erlaubt einem Benutzer, Kennzeicheninformationen für die Videoanalyse "Automatische Kennzeichenerkennung" in der Windows Client-Oberfläche hinzuzufügen oder zu bearbeiten.
Delete License Plate	Diese Berechtigung erlaubt einem Benutzer, Kennzeicheninformationen aus der Videoanalyse "Automatische Kennzeichenerkennung" in der Windows Client-Oberfläche zu löschen.
Export License Plates	Diese Berechtigung erlaubt einem Benutzer, Kennzeicheninformationen aus der Videoanalyse "Automatische Kennzeichenerkennung" in der Windows Client-Oberfläche zu exportieren.
Manage License Plate Lists	Diese Berechtigung erlaubt einem Benutzer, Kennzeichenlisten für die Videoanalyse "Automatische Kennzeichenerkennung" in der Windows Client-Oberfläche zu erstellen und zu bearbeiten.
Manage Special Characters	Diese Berechtigung erlaubt einem Benutzer, Sonderzeichenzuordnungen für die Videoanalyse "Automatische Kennzeichenerkennung" in der Windows Client-Oberfläche hinzuzufügen.
Perform License Plate Search	Diese Berechtigung erlaubt einem Benutzer, nach Kennzeicheninformationen aus der Videoanalyse "Automatische Kennzeichenerkennung" in der Windows Client-Oberfläche zu suchen.
View License Plate Log	Diese Berechtigung erlaubt einem Benutzer, das Kennzeichenprotokoll der Videoanalyse "Automatische Kennzeichenerkennung" in der Windows Client-Oberfläche anzuzeigen.
View License Plate Metadata Configuration	Diese Berechtigung erlaubt einem Benutzer, die Konfiguration der Kennzeichen-Metadaten für die Videoanalyse "Automatische Kennzeichenerkennung" in der Windows Client-Oberfläche anzuzeigen.

Messenger

Berechtigung	Beschreibung
Modify Pre-written Messages	Diese Berechtigung erlaubt einem Benutzer, die vorgefertigten Nachrichten im Messenger in der Windows Client-Oberfläche zu bearbeiten.

Berechtigung	Beschreibung
Send Messages	Diese Berechtigung erlaubt einem Benutzer, Nachrichten über den Messenger in der Windows Client-Oberfläche zu senden.

Point of Sale

Berechtigung	Beschreibung
Change POS data	Diese Berechtigung erlaubt einem Benutzer, die Point-of-Sale-Daten in der Windows Client-Oberfläche zu ändern.
View POS data	Diese Berechtigung erlaubt einem Benutzer, Point-of-Sale-Daten in der Windows Client-Oberfläche anzuzeigen.

Report

Berechtigung	Beschreibung
Execute Report	Diese Berechtigung erlaubt einem Benutzer, Berichte in der Windows Client-Oberfläche auszuführen.

Rule

Berechtigung	Beschreibung
Add Rules	Diese Berechtigung erlaubt einem Benutzer, Regeln in der Server-Konfigurationsoberfläche zu erstellen.

Search

Berechtigung	Beschreibung
Convert Searches	Diese Berechtigung erlaubt einem Benutzer, Suchergebnisse in der Windows Client-Oberfläche in AVI- oder MPEG-Dateien zu konvertieren.
Delete Searches	Diese Berechtigung erlaubt einem Benutzer, Suchen in der Windows Client-Oberfläche zu löschen.
Search	Diese Berechtigung erlaubt einem Benutzer, Suchen in der Windows Client-Oberfläche durchzuführen.

Security

Berechtigung	Beschreibung
Activate Security Profile	Diese Berechtigung erlaubt einem Benutzer, Sicherheitsprofile in der Server-Konfigurationsoberfläche zu aktivieren.
Change Authentication Mode	Diese Berechtigung wird nicht verwendet.
Edit Security	Diese Berechtigung erlaubt einem Benutzer, Sicherheitseinstellungen in der Server-Konfigurationsoberfläche zu bearbeiten.
Manage Security Profiles	Diese Berechtigung erlaubt einem Benutzer, Sicherheitsprofile in der Server-Konfigurationsoberfläche hinzuzufügen, zu bearbeiten und zu löschen.

Subscription

Berechtigung	Beschreibung
Change Subscriptions	Diese Berechtigung erlaubt einem Benutzer, die Benachrichtigungseinstellungen in der Server-Konfigurationsoberfläche zu ändern.
View Subscriptions	Diese Berechtigung erlaubt einem Benutzer, die Benachrichtigungseinstellungen in der Server-Konfigurationsoberfläche anzuzeigen.

UI

Berechtigung	Beschreibung
Change Carousels	Diese Berechtigung erlaubt einem Benutzer, Kamerasequenzen in der Server-Konfigurationsoberfläche zu bearbeiten.
Configure Visual Tracking	Diese Berechtigung erlaubt einem Benutzer, visuelle Tracking-Verknüpfungen in der Windows Client-Oberfläche hinzuzufügen, zu bearbeiten und zu löschen.
Lock UI	Diese Berechtigung erlaubt einem Benutzer, die Windows Client-Oberfläche zu sperren.
Manage Shared Views	Diese Berechtigung erlaubt einem Benutzer, freigegebene Ansichten in der Windows Client-Oberfläche zu bearbeiten und zu speichern.
View Carousels	Diese Berechtigung erlaubt einem Benutzer, Kamerasequenzen in der Windows Client-Oberfläche anzuzeigen.

User

Berechtigung	Beschreibung
Add Users	Diese Berechtigung erlaubt einem Benutzer, Benutzer in der Server-Konfigurationsoberfläche zu erstellen.
Multiple Logins	Diese Berechtigung erlaubt einem Benutzer, sich gleichzeitig an mehreren Windows Client- und Server-Konfigurationsoberflächen-Instanzen anzumelden.

Video Wall

Berechtigung	Beschreibung
Change Video Wall Client	Diese Berechtigung erlaubt einem Benutzer, Videowand-Clients in der Windows Client-Oberfläche zu konfigurieren.
Control Video Walls	Diese Berechtigung erlaubt einem Benutzer, Videowand-Clients in der Windows Client-Oberfläche fernzusteuern.
Create Video Walls	Diese Berechtigung erlaubt einem Benutzer, Videowände in der Windows Client-Oberfläche zu erstellen.

Geräteberechtigungen

General

Berechtigung	Beschreibung
Basic Access	Diese Berechtigung erlaubt einem Benutzer den Zugriff auf Kameras oder andere Geräte.

Berechtigung	Beschreibung
View Group	Diese Berechtigung erlaubt einem Benutzer, die Geräte in Gerätegruppen anzuzeigen.
View IO State	Diese Berechtigung erlaubt einem Benutzer, den Eingangs-/Ausgangszustand von Geräten anzuzeigen.

Configuration

Berechtigung	Beschreibung
Add Members	Diese Berechtigung erlaubt einem Benutzer, Geräte zu einer Gerätegruppe hinzuzufügen.
Change IO State	Diese Berechtigung erlaubt einem Benutzer, den Eingangs- und Ausgangszustand eines Geräts zu ändern.
Change Settings	Diese Berechtigung erlaubt einem Benutzer, die Einstellungen für ein Gerät zu ändern.
Configure Analytics	Diese Berechtigung erlaubt einem Benutzer, Analysen für ein Gerät zu konfigurieren.
Delete	Diese Berechtigung erlaubt einem Benutzer, ein Gerät vom Server zu entfernen.
Delete Group	Diese Berechtigung erlaubt einem Benutzer, eine Gerätegruppe zu löschen.
Edit Device Security	Diese Berechtigung erlaubt einem Benutzer, die Authentifizierungseinstellungen für Geräte zu ändern.
Edit Group Membership	Diese Berechtigung erlaubt einem Benutzer zu ändern, zu welchen Gruppen eine Gerätegruppe gehört.
Edit Group Properties	Diese Berechtigung erlaubt einem Benutzer, die Eigenschaften für Gerätegruppen zu ändern.
Edit Group Security	Diese Berechtigung erlaubt einem Benutzer, die Sicherheitsprofile für Gerätegruppen zu ändern.
Edit Membership	Diese Berechtigung erlaubt einem Benutzer zu ändern, welche Geräte sich in einer Gerätegruppe befinden.
Remove Members	Diese Berechtigung erlaubt einem Benutzer, ein Gerät aus einer Gerätegruppe zu entfernen.

Alarm

Berechtigung	Beschreibung
Manage Alarms	Diese Berechtigung erlaubt einem Benutzer, einen Alarm als Alarm, Fehlalarm oder als echt und handlungsrelevant zu markieren sowie Alarmdetails in der Oberfläche des Windows Client anzuzeigen und zu bearbeiten.
Trigger Manual Alarm	Diese Berechtigung erlaubt einem Benutzer, in der Oberfläche des Windows Client einen Alarm zu einer Kamerazeile hinzuzufügen.

Audio

Berechtigung	Beschreibung
Listen to camera	Diese Berechtigung erlaubt einem Benutzer, das von einer Kamera aufgezeichnete Audio über die Oberfläche des Windows Client anzuhören.

Berechtigung	Beschreibung
Talk through camera	Diese Berechtigung erlaubt einem Benutzer, Audio über eine Kamera mit der Oberfläche des Windows Client zu übertragen.

LPR

Berechtigung	Beschreibung
Edit License Plate	Diese Berechtigung erlaubt einem Benutzer, von Kameras erkannte Kennzeichen über die Oberfläche des Windows Client zu bearbeiten.

PTZ

Berechtigung	Beschreibung
Calibrate PTZ Camera	Diese Berechtigung erlaubt einem Benutzer, eine PTZ-Kamera in der Oberfläche des Windows Client zu kalibrieren.
Control PTZ	Diese Berechtigung erlaubt einem Benutzer, eine PTZ-Kamera über die Oberfläche des Windows Client zu schwenken und zu neigen.
Control zoom via clients	Diese Berechtigung erlaubt einem Benutzer, eine PTZ-Kamera über die Oberfläche des Windows Client zu zoomen.
PTZ Presets	Diese Berechtigung erlaubt einem Benutzer, eine PTZ-Kamera über die Oberfläche des Windows Client in eine voreingestellte Position zu bewegen.

Search

Berechtigung	Beschreibung
Search Footage	Diese Berechtigung erlaubt einem Benutzer, Videoaufnahmen über die Oberfläche des Windows Client zu durchsuchen.

Video

Berechtigung	Beschreibung
Manage Recording	Diese Berechtigung erlaubt einem Benutzer, Aufzeichnungen zu verwalten.
Protect Footage	Diese Berechtigung erlaubt einem Benutzer, Aufnahmen über die Oberfläche des Windows Client vor dem Löschen zu schützen.
Unprotect Footage	Diese Berechtigung erlaubt einem Benutzer, den Schutz von Aufnahmen auf der Seite Settings > Protected Footage in der Konfigurationsoberfläche des Server aufzuheben.
View Historical Video	Diese Berechtigung erlaubt einem Benutzer, historisches Video anzuzeigen.
View Live Video	Diese Berechtigung erlaubt einem Benutzer, Live-Video anzuzeigen.
View Private Video	Diese Berechtigung erlaubt einem Benutzer, Video anzuzeigen, das durch eine Privatsphärenmaske ausgeblendet ist.

Berechtigung	Beschreibung
View Restricted Historical Video	Diese Berechtigung erlaubt einem Benutzer, Video anzuzeigen, das als eingeschränkt markiert wurde. Der Server kann historisches Video als eingeschränkt markieren, basierend auf der Einstellung Time based video playback restriction applied at auf der Seite Settings > General Settings in der Konfigurationsoberfläche des Server.

Benutzerberechtigungen

Diese Seite listet die Berechtigungen in der Kategorie **User** auf. Diese Berechtigungen sind an **Sicherheitsprofile** gebunden; Sicherheitsprofile sind an **Gruppen** gebunden; Benutzer erhalten ihre Berechtigungen, indem sie zu Gruppen gehören. Andere Berechtigungskategorien (**Standort**, **Gerät**, **Regel**, **Videowand**, **freigegebene Ansicht**) folgen demselben Modell.

Rollenvorlagen

Die meisten Bereitstellungen müssen keine einzelnen Berechtigungen manuell auswählen. Beginnen Sie mit einer der unten stehenden Rollenvorlagen und passen Sie sie an.

Rolle	Empfohlene Berechtigungen der Kategorie User
Operator nur zur Anzeige — beobachtet Video, reagiert nicht auf Alarme	Keine aus dieser Kategorie.
Voll-Operator — reagiert auf Alarme, generiert Berichte, arbeitet eine Überwachungsschicht	View User, View Group.
Supervisor — verwaltet Operatoren während einer Schicht, kann eine festsitzende Sitzung beenden	View User, View Group, Terminate user session.
Benutzeradministrator — verwaltet die tägliche Benutzerliste für den Standort	Alle View - und Configuration -Berechtigungen unten außer Edit Group Security und Edit Security .
Standortadministrator — verwaltet Benutzer, Sicherheitsprofile und das vollständige Berechtigungsmodell	Alle Berechtigungen in dieser Kategorie.

Gewähren Sie standort- und geräteebenen-bezogene Berechtigungen separat; siehe die oben verlinkten verwandten Seiten.

General

Berechtigung	Beschreibung
View User	Benutzer in der Benutzerliste sehen. Erforderlich für jeden, der wissen muss, wer ein Konto hat — einschließlich der meisten Operatoren, damit sie sehen können, wer Schicht hat.
View Group	Gruppen in der Gruppenliste sehen.
Terminate user session	Die aktive Sitzung eines anderen Benutzers beenden. Typische Verwendung: Ein Schichtleiter beendet eine festsitzende Sitzung, damit sich ein anderer Operator anmelden kann.

Configuration

Berechtigung	Beschreibung
Add Members	Vorhandene Benutzer zu einer Gruppe hinzufügen.
Remove Members	Benutzer aus einer Gruppe entfernen.

Berechtigung	Beschreibung
Edit Membership	Benutzer in Gruppen hinzufügen oder entfernen. Eine Obermenge von Add Members + Remove Members für die Benutzermitgliedschaft.
Edit Group Membership	Gruppen innerhalb anderer Gruppen hinzufügen oder entfernen (Gruppenverschachtelung). Unterscheidet sich von Edit Membership: Diese steuert die Beziehung von Gruppen-zu-Gruppen, nicht Benutzer-zu-Gruppe.
Edit Group Properties	Den Namen, die Beschreibung und die Active Directory-Verknüpfung einer Gruppe ändern.
Edit User Properties	Telefonnummer, E-Mail, Beschreibung und ähnliche nicht sicherheitsrelevante Eigenschaften eines Benutzers ändern.
Edit Group Security	Das mit einer Gruppe verknüpfte Sicherheitsprofil ändern. Hohe Auswirkung — diese Berechtigung zu erteilen entspricht der Erteilung jeder Berechtigung, die ein beliebiges Sicherheitsprofil verleiht.
Edit Security	Das mit einem einzelnen Benutzer verknüpfte Sicherheitsprofil ändern. Gleicher Vorbehalt wie bei Edit Group Security.
Delete Group	Eine Gruppe aus dem Server entfernen. Benutzer in der Gruppe verlieren die Berechtigungen, die die Gruppe gewährt hat.
Delete User	Einen Benutzer aus dem Server entfernen.

Hinweise

- **Edit Group Security** und **Edit Security** sind Berechtigungen zur Berechtigungseskalation. Erteilen Sie diese nur Administratoren, denen Sie das vollständige Berechtigungsmodell anvertrauen.
- **Edit Group Membership** wird oft mit **Edit Membership** verwechselt. Verwenden Sie ersteres, wenn Sie hierarchische Gruppenstrukturen aufbauen; verwenden Sie letzteres für den häufigeren Fall, dass Sie Benutzer aus einer flachen Menge von Gruppen hinzufügen und entfernen.
- Berechtigungen sind über die Gruppenmitgliedschaften eines Benutzers additiv. Wenn ein Benutzer zu zwei Gruppen gehört, ist der effektive Berechtigungssatz die Vereinigung beider.

Verwandte Aufgaben

- Benutzer hinzufügen
- Gruppe hinzufügen
- Sicherheitsprofil hinzufügen
- Sicherheitsprofil-Berechtigungen festlegen

Videowand-Berechtigungen

General

Berechtigung	Beschreibung
Change Panel	Diese Berechtigung erlaubt einem Benutzer, die Kameraansichten in einem Videowand-Panel zu ändern.
Change Window	Diese Berechtigung erlaubt einem Benutzer, die Panels in einem Videowand-Fenster zu ändern.
Move Window	Diese Berechtigung erlaubt einem Benutzer, Videowand-Panels in der Videowand zu verschieben.
Use Panel Context Menu	Diese Berechtigung erlaubt einem Benutzer, das Kontextmenü für Videowand-Panels anzuzeigen und zu verwenden.

Berechtigung	Beschreibung
Use Window Context Menu	Diese Berechtigung erlaubt einem Benutzer, das Kontextmenü für Videowand-Fenster anzuzeigen und zu verwenden.
View	Diese Berechtigung erlaubt einem Benutzer, Videowände anzuzeigen.
View Group	Diese Berechtigung erlaubt einem Benutzer, Videowand-Gruppen anzuzeigen.

Configuration

Berechtigung	Beschreibung
Add Members	Diese Berechtigung erlaubt einem Benutzer, Benutzer zu einer Videowand-Gruppe hinzuzufügen.
Delete	Diese Berechtigung erlaubt einem Benutzer, eine Videowand aus dem Server zu entfernen.
Delete Group	Diese Berechtigung erlaubt einem Benutzer, eine Videowand-Gruppe zu löschen.
Edit Group Membership	Diese Berechtigung erlaubt einem Benutzer, zu ändern, zu welchen Gruppen eine Videowand-Gruppe gehört.
Edit Group Properties	Diese Berechtigung erlaubt einem Benutzer, die Eigenschaften für Videowand-Gruppen zu ändern.
Edit Group Security	Diese Berechtigung erlaubt einem Benutzer, die Sicherheitsprofile für Videowand-Gruppen zu ändern.
Edit Security	Diese Berechtigung erlaubt einem Benutzer, die Sicherheitsprofile von Benutzern zu ändern.
Modify	Diese Berechtigung erlaubt einem Benutzer, die Konfiguration von Videowänden zu ändern.
Remove Members	Diese Berechtigung erlaubt einem Benutzer, einen Benutzer aus einer Videowand-Gruppe zu entfernen.

Regelberechtigungen

General

Berechtigung	Beschreibung
View Rule	Diese Berechtigung erlaubt einem Benutzer, Regeln in der Server-Konfigurationsoberfläche anzuzeigen.

Configuration

Berechtigung	Beschreibung
Change Rule	Diese Berechtigung erlaubt einem Benutzer, Regeln in der Server-Konfigurationsoberfläche zu ändern.

Berechtigungen für freigegebene Ansicht

General

Berechtigung	Beschreibung
View Shared View	Diese Berechtigung erlaubt einem Benutzer, freigegebene Ansichten in der Windows Client-Oberfläche anzuzeigen.

Sicherheitsprofil aktivieren

Sie können ein Sicherheitsprofil aktivieren, um alle Berechtigungen anzuwenden, die Sie für Benutzer und Gruppen unter diesem Sicherheitsprofil konfigurieren.

Wenn Sie ein Sicherheitsprofil aktivieren, ersetzen die Berechtigungen des Sicherheitsprofils die Berechtigungen des vorherigen Sicherheitsprofils. Die für Benutzer verfügbaren Funktionen in der Konfigurationsoberfläche des Server und in der Oberfläche des Windows Client können sich beim Aktivieren eines Sicherheitsprofils erheblich ändern.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Security > Security Profiles.
2. Wählen Sie ein Sicherheitsprofil aus und klicken Sie auf Activate Security Profile.

Sicherheitsprofil entfernen

Sie können ein Sicherheitsprofil aus dem Server entfernen, sofern das Sicherheitsprofil nicht aktiv ist. Sie können das Standard-Sicherheitsprofil nicht entfernen.

Das Entfernen eines Sicherheitsprofils aus dem Server ändert nicht die aktiven Berechtigungen für Benutzer oder Gruppen.

1. Klicken Sie in der Server-Konfigurationsoberfläche auf Security > Security Profiles.
2. Wählen Sie ein Sicherheitsprofil aus und klicken Sie auf Delete.

Benutzeranmeldungen

Auf der Seite Logins werden Sitzungen sowohl für den Server als auch für den Windows Client angezeigt.

Im Abschnitt Active Sessions werden Informationen zu Benutzern angezeigt, die derzeit an der Konfigurationsoberfläche des Server und der Oberfläche des Windows Client angemeldet sind.

Im Abschnitt Historical Sessions werden Informationen zu Benutzern angezeigt, die sich zuvor an der Konfigurationsoberfläche des Server und der Oberfläche des Windows Client angemeldet haben.

Im Abschnitt Banned Devices and Groups werden die Geräte und Gerätegruppen angezeigt, für die Sie Videos ausgesetzt haben. Wenn Sie den Zugriff auf Videos in der Oberfläche des Windows Client nicht aussetzen, ist dieser Abschnitt leer.

Aktive Sitzung beenden

Sie können die aktiven Sitzungen für Benutzer beenden, die am Windows Client angemeldet sind.

Administratorbenutzer können die aktiven Sitzungen aller anderen Benutzer beenden. Benutzer, die keine Administratorbenutzer sind, können nur ihre eigenen Sitzungen beenden.

1. Klicken Sie in der Server-Konfigurationsoberfläche auf Security > Logins.
2. Klicken Sie neben der aktiven Sitzung, die Sie beenden möchten, auf Terminate.

Sitzungsverlauf anzeigen

1. Klicken Sie in der Server-Konfigurationsoberfläche auf Security > Logins.
2. Klicken Sie auf Load Historical Sessions.
3. Um die historischen Sitzungen in eine CSV-Datei zu exportieren, klicken Sie auf Export CSV file und öffnen oder speichern Sie die Datei.

Security Settings

Sie können die Kennwortrichtlinie für den Server in den Security Settings konfigurieren.



Informationen zur Verwaltung von Konten mit Active Directory finden Sie unter [Active Directory Integration](#).

Passwords

Verwenden Sie die Seite Passwords, um die Kennwortrichtlinie zu definieren, die für Benutzerkonten des Servers gilt.

Password expiry (days)

Wenn ausgewählt, laufen Kennwörter nach der angegebenen Anzahl von Tagen ab. Der Standardwert ist 90.

Require complex passwords

Wenn ausgewählt, müssen Kennwörter Komplexitätsanforderungen erfüllen.

Minimum password length

Wenn "Require complex passwords" ausgewählt ist, gibt dies die Mindestanzahl an Zeichen in einem Kennwort an. Der Standardwert ist 8.

Password history length

Gibt die maximale Anzahl früherer Kennwörter an, die der Server speichert und prüft, wenn ein Benutzer sein Kennwort ändert. Benutzer können ihr Kennwort nicht zu einem ihrer letzten Kennwörter ändern. Der Mindestwert ist 1, wodurch nur das aktuelle Kennwort geprüft wird.

Password attempts before lockout

Gibt die Anzahl fehlgeschlagener Anmeldeversuche an, bevor der Server das Benutzerkonto sperrt. Der Standardwert ist 3.

Password lockout (minutes)

Gibt die Anzahl der Minuten an, die ein gesperrtes Benutzerkonto gesperrt bleibt. Der Standardwert ist 15.

Active-Directory-Integration

Der Active Directory-Authentifizierungsmodus verwendet Active Directory zur Authentifizierung von Benutzern.

Bei dieser Authentifizierungsmethode speichert die Senstar Symphony-Datenbank Benutzernamen und Sicherheitskennungen für Benutzerkonten, jedoch keine Kennwörter. Wenn ein Benutzer versucht, sich anzumelden, prüft der Server die Anmeldedaten gegen Active Directory. Wenn Sie ein Benutzerkonto zum Server hinzufügen, müssen Sie das Benutzerkonto mit einem Benutzerkonto in Active Directory verknüpfen.

Wenn Sie den Benutzer anschließend aus Active Directory entfernen, löscht der Server den Benutzer.

Der Server synchronisiert sich automatisch einmal täglich um 12:00 Uhr Serverzeit mit Active Directory. Zusätzlich können Sie den Server manuell synchronisieren.

Mit Active Directory integrieren

Sie können den Server so konfigurieren, dass er in die Active Directory-Domäne integriert wird.

Sie können den Server während der Installation des Server oder nach der Installation mithilfe des Senstar Symphony-Setup-Assistenten in Active Directory integrieren.

Der Server stellt eine Verbindung zum globalen Active Directory-Katalog für die Benutzer- und Gruppensynchronisierung her. In der Konfigurationsoberfläche des Server erstellen Sie Gruppen und ordnen diese Gruppen den Gruppen in Active Directory zu.

Darüber hinaus stellt der Server eine Verbindung zu einem Active Directory-Benutzer als standardmäßigem administrativen Benutzer her.

1. Klicken Sie im Abschnitt Symphony Security Security auf der Registerkarte Farm Configuration auf Edit. 
2. Wählen Sie Active Directory Integration. 
3. Führen Sie im Feld LDAP URL eine der folgenden Aufgaben aus:
 - Geben Sie die URL für den globalen LDAP-Katalog ein.
 - Klicken Sie auf Auto Discover, um den globalen LDAP-Katalog automatisch zu erkennen.
4. Geben Sie einen Benutzernamen und ein Kennwort des Active Directory-Benutzers ein, der als standardmäßiger administrativer Benutzer für den Server fungiert.
5. Klicken Sie auf Verify.

Gruppe verknüpfen

Wenn Sie die Active Directory-Authentifizierung verwenden, müssen Sie die in Senstar Symphony erstellten Gruppen mit Gruppen in Active Directory verknüpfen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Security > Groups.
2. Wählen Sie eine Gruppe aus und klicken Sie auf Edit.
3. Klicken Sie auf Associate. 
4. Geben Sie im Feld Search For einen Gruppennamen ein und klicken Sie auf Search. 
5. Klicken Sie auf die Gruppe und klicken Sie auf OK. 

Gruppen mit Active Directory synchronisieren

Sie können Gruppen, die mit Active Directory-Gruppen verknüpft sind, manuell synchronisieren, um Änderungen in Active Directory zu übernehmen.

1. Klicken Sie in der Server-Konfigurationsoberfläche auf Security > Groups.
2. Klicken Sie auf Synchronize.

Sicherheitsauthentifizierung

Der Senstar Symphony-Sicherheitsauthentifizierungsmodus authentifiziert Benutzernamen und Kennwörter, die Sie für Benutzer in der Server-Konfigurationsoberfläche erstellen.

Bei dieser Authentifizierungsmethode speichert die Senstar Symphony-Datenbank Benutzernamen und Kennwörter für Benutzerkonten. Wenn ein Benutzer versucht, sich anzumelden, prüft Senstar Symphony die Anmeldedaten gegen die Senstar Symphony-Datenbank.

Wasserzeichen

Senstar Symphony verwendet Wasserzeichen, um manipuliertes Video und Audio zu erkennen. Wasserzeichen funktionieren im Windows Client, Player und Web Client.

Wenn Senstar Symphony das Wasserzeichen erfolgreich verifiziert, wird das Video normal abgespielt. Schlägt die Wasserzeichenverifizierung fehl, zeigt das Video eine Fehlermeldung an, wenn Sie versuchen, Video im Web Client oder Player anzusehen.

Wasserzeichen aktivieren

Wenn Sie Wasserzeichen aktivieren, fügt der Server aufgezeichnetem Video Wasserzeichen hinzu, und der Windows Client verifiziert Wasserzeichen beim Abspielen von Video.

1. Klicken Sie in der Windows Client-Oberfläche auf Server Configuration > Manual Configuration Editor.
2. Klicken Sie auf Add a new setting.
3. Fügen Sie die folgenden Werte hinzu:

```
Type: Global
Section: Main
Key: EnableWatermark
Value: True
```

1. Klicken Sie auf OK.
2. Starten Sie die Senstar Symphony-Dienste neu.

Regeln

Der Server kann Alarme aus Regeln generieren. Regeln umfassen Ereignisse, Aktionssätze und Zeitpläne.

Alarmgenerierung

Alarme treten nicht isoliert auf; sie sind das Ergebnis einer logischen Kette innerhalb des Symphony Server:

- **Ereignis:** Ein roher Auslöser (z. B. eine Analyseerkennung "Linienüberschreitung", eine gewaltsam geöffnete Tür oder ein Zaunsensor, der einen Schnitt erkennt).
- **Aktionssatz:** Die spezifischen Folgen des Ereignisses, die das Erstellen eines Alarms, das Senden von E-Mails oder das Verschieben einer PTZ-Kamera in eine Voreinstellung umfassen.
- **Zeitplan:** Ein Zeitrahmen, in dem die Regel aktiv ist (z. B. "Außerhalb der Geschäftszeiten").
- **Schweregrad:** Die Bedeutung des Alarms auf einer Skala von 1 (höchste) bis 5 (niedrigste).

Sie erstellen Regeln in der Server-Konfigurationsoberfläche. Wenn Sie eine Regel erstellen, verknüpfen Sie entweder vorhandene Ereignisse, Aktionssätze und einen Zeitplan mit der Regel oder Sie erstellen neue Ereignisse, Aktionssätze und einen Zeitplan für die Regel.

Ein Aktionssatz definiert die Aktionen, die der Server ausführt, wenn ein Ereignis eine Regel auslöst. Beispiele sind das Anzeigen oder Aufzeichnen von Material einer Kamera, das Senden einer E-Mail und das Schalten eines Relais. Sie können auswählen, wie der Server alle Aktionen für mehrere Alarme

desselben Typs ausführt, indem Sie die Einstellungen für das Mehrfachaufruf-Verhalten verwenden: "Append actions sets" führt alle Aktionen für jeden Alarm aus, und "Replace queued actions" führt alle Aktionen nur für den letzten Alarm aus.

Ein Zeitplan definiert, wann eine Regel aktiv ist. Ein Ereignis muss während einer aktiven Zeit im Zeitplan eintreten, um eine Regel auszulösen.

Wenn eine Regel aktiviert ist, führt das Auftreten eines mit der Regel verknüpften Ereignisses während eines aktiven Zeitraums im Zeitplan der Regel dazu, dass der Server die im Aktionssatz der Regel definierten Aktionen ausführt.

Metadaten

Metadaten sind strukturierte Daten, die Videoanalysen und Integrationen zusammen mit Videos erzeugen. Die Regel-Engine auf dem Server wertet Metadaten aus, um zu entscheiden, ob ein Ereignis ausgelöst werden soll.

Was Metadaten sind

Eine Kamera erzeugt Videoframes. Eine Videoanalyse, ein Zutrittskontrollgerät oder eine andere Integration erzeugt Metadaten, die beschreiben, was diese Frames oder Ereignisse bedeuten. Metadaten sind strukturierte Daten (im XML-Stil), die zusammen mit dem Video übertragen und auf dem Server gespeichert werden. Beispiele für Metadaten sind die folgenden:

- Der Begrenzungsrahmen, die Klassifizierung (Person, Fahrzeug, Tier) und die Flugbahn eines Objekts, das eine Analyse erkennt.
- Der Kennzeichentext, der Vertrauenswert und die Region, die die Analyse Automatische Kennzeichenerkennung meldet.
- Die übereinstimmende Identität und der Vertrauenswert, die die Analyse Gesichtserkennung meldet.
- Der Karteninhaber, die Tür und das Ergebnis (gewährt oder verweigert), das ein Zutrittskontrollereignis meldet.
- Der Sensorname, die Zone und die Statusänderung, die eine Perimeter-Integration meldet.

Metadaten werden kontinuierlich erzeugt, während die Quelle aktiv ist. Der Server speichert Metadaten neben dem Video, das sie beschreiben, sodass Sie beide gleichzeitig durchsuchen, filtern und wiedergeben können.

Wie die Regel-Engine Metadaten verwendet

Wenn Sie ein Ereignis auf dem Server erstellen, wählen Sie eine Metadatenquelle (z. B. eine Videoanalyse oder eine Integration) aus und geben Sie die Bedingungen an, unter denen das Ereignis ausgelöst wird. Die Regel-Engine wertet eingehende Metadaten in Echtzeit gegen diese Bedingungen aus. Wenn die Bedingungen übereinstimmen, löst die Regel-Engine das Ereignis aus, und die Regel, die dieses Ereignis verwendet, führt ihren Aktionssatz aus.

Beispielsweise erzeugt eine Analyse Verfolgung von Personen und Fahrzeugen im Außenbereich Metadaten für jedes verfolgte Objekt. Eine Regel, die ein Linienüberschreitungs-Ereignis verwendet, untersucht die Trajektorienmetadaten für jedes Objekt und wird ausgelöst, wenn ein Objekt während eines aktiven Zeitplans die konfigurierte Linie überschreitet.

Metadaten sind auch das, was die Suche im Windows Client ermöglicht. Wenn Sie nach einer Person, einem Fahrzeug oder einem Kennzeichen suchen, fragt der Windows Client die vom Server gespeicherten Metadaten ab, nicht die Videopixel.

Woher Metadaten stammen

Die folgenden Quellen erzeugen Metadaten:

- **Videoanalysen**, die auf einer Kamera oder auf dem Server ausgeführt werden.
- **Integrationen** mit Zutrittskontrolle, Perimetererkennung und anderen externen Systemen.
- **Der TCP-Listener**, der Metadaten von Drittanbieterquellen über das Netzwerk akzeptiert.

Regel erstellen

Sie können eine Regel erstellen, um den Server Aktionen ausführen zu lassen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Rules.
2. Klicken Sie auf Add.
3. Geben Sie einen Namen für die Regel ein.
4. Aktivieren oder deaktivieren Sie die Regel.
5. Fügen Sie der Regel ein vorhandenes Ereignis hinzu oder erstellen Sie ein neues Ereignis, das der Regel hinzugefügt werden soll.
6. Wenn Sie der Regel mehrere Ereignisse hinzufügen, wählen Sie aus, wie die Ereignisse auftreten müssen, um die Regel auszulösen.
 - Wählen Sie in sequence, um eine Regel auszulösen, wenn die Ereignisse in der Reihenfolge auftreten, in der die Konfigurationsoberfläche des Server die Ereignisse auflistet.
 - Wählen Sie within a time period of und geben Sie die Anzahl der Sekunden an, um eine Regel auszulösen, wenn alle Ereignisse innerhalb des angegebenen Zeitraums auftreten.
7. Um der Regel Aktionssätze hinzuzufügen, führen Sie die folgenden Aufgaben aus:
 - a. Wählen Sie in der Liste den Aktionssatz aus und klicken Sie auf Add.
 - b. Stellen Sie im Feld Delay ein, wie viel Zeit nach dem Eintreten der Regel verstreichen muss, bevor die Aktion ausgelöst wird.
 - c. Wählen Sie in der Liste Multiple Invocation behavior Append action sets aus, um die Aktionen für jedes Auftreten der Regel auszulösen, oder Replace queued actions, um die Aktionen nur für das jüngste Auftreten der Regel auszulösen.

Sie können jeder Regel mehrere Aktionen hinzufügen.

1. Fügen Sie der Regel einen vorhandenen Zeitplan hinzu oder erstellen Sie einen neuen Zeitplan, der der Regel hinzugefügt werden soll.
2. Wählen Sie im Feld Severity den Schweregrad für den Alarm aus.
 - 1 gilt im Windows Client als hoher Schweregrad
 - 2 und 3 gelten im Windows Client als mittlerer Schweregrad
 - 4 und 5 gelten im Windows Client als niedriger Schweregrad

Sie können den Alarmschweregrad verwenden, um Alarme im Windows Client zu sortieren.

1. Klicken Sie auf Save.

Regel bearbeiten

Sie können eine Regel bearbeiten, um die Ereignisse, den Aktionssatz und den Zeitplan zu ändern, die der Regel zugeordnet sind.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Rules.
2. Wählen Sie eine Regel aus.
3. Klicken Sie auf Edit.
4. Ändern Sie die Regel.
5. Klicken Sie auf Save.

Regel löschen

Sie können eine Regel entfernen, um zu verhindern, dass Ereignisse auf dem Server ausgelöst werden.

Wenn Sie eine Regel löschen, werden die Ereignisse, der Aktionssatz und der Zeitplan, die mit der Regel verknüpft sind, nicht gelöscht.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Rules.
2. Wählen Sie eine Regel aus.
3. Klicken Sie auf Delete.
4. Klicken Sie auf Yes.

Ereignisse

Ereignisse definieren die Bedingung, die erfüllt sein muss, damit eine Regel einen Alarm auf dem Server auslöst.

Ereignis erstellen

Sie können ein Ereignis erstellen, das eine Regel auf dem Server auslöst.

Wenn der Server eine Eingabe von einer Quelle empfängt, kann er eine Regel auslösen. Verschiedene Quellen können Regeln auf unterschiedliche Weise auslösen. Weitere Informationen zu Geräten finden Sie in der Dokumentation des Herstellers.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Events.
2. Klicken Sie auf New Event.
3. Geben Sie einen Namen für das Ereignis ein.
4. Um eine Quelle hinzuzufügen, führen Sie die folgenden Aufgaben aus:
 - a. Klicken Sie auf Add Sources.
 - b. Wählen Sie das Gerät, die Regel oder den Zeitplan aus, mit dem die Regel ausgelöst werden soll.
 - c. Klicken Sie auf OK.
5. Führen Sie eine der folgenden Aufgaben aus:
 - Wenn Sie eine Kamera hinzufügen, wählen Sie die Video-Engine aus und konfigurieren Sie, wie

sie eine Regel auslöst.

- Wenn Sie ein Metadatengerät hinzufügen, wählen Sie den Eingang aus und konfigurieren Sie, wie er eine Regel auslöst.
- Wenn Sie ein Zugangskontrollgerät hinzufügen, wählen Sie die Lesegeräte und Eingänge aus und konfigurieren Sie, wie sie eine Regel auslösen.
- Wenn Sie eine Regel hinzufügen, wählen Sie die Aktion aus, die eine Regel auslöst.
- Wenn Sie einen Zeitplan hinzufügen, wählen Sie aus, wann eine Regel ausgelöst werden soll.

6. Klicken Sie auf Save.

Ereignis bearbeiten

Sie können ein Ereignis bearbeiten, um zu ändern, was eine Regel auslöst.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Events.
2. Wählen Sie ein Ereignis aus.
3. Klicken Sie auf Edit.
4. Ändern Sie das Ereignis.
5. Klicken Sie auf Save.

Ereignis löschen

Sie können ein Ereignis löschen, um es vom Server zu entfernen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Events.
2. Wählen Sie ein Ereignis aus.
3. Klicken Sie auf Delete.
4. Klicken Sie auf Yes.

Ereigniseinstellungen für automatische Kennzeichenerkennung

Die Ereigniseinstellungen für die Videoanalyse Automatische Kennzeichenerkennung sind sichtbar, wenn Sie sie als Video-Engine für ein Ereignis auswählen.

Einstellung	Beschreibung
Alarm type	Wählen Sie aus, ob das Ereignis die Regel auslöst, wenn die Videoanalyse Automatische Kennzeichenerkennung ein Kennzeichen erkennt, ein Kennzeichen erkennt, das nicht auf der Liste (Whitelist) steht, oder ein Kennzeichen erkennt, das auf der Liste (Blacklist) steht.

Ereigniseinstellungen für Erkennung von Menschenmengen

Die Ereigniseinstellungen für die Videoanalyse Erkennung von Menschenmengen sind sichtbar, wenn Sie sie als Video-Engine für ein Ereignis auswählen.

Einstellung	Beschreibung
Alarm type	Wählen Sie aus, ob das Ereignis auf Capacity (Anzahl der Personen) oder Occupancy (von Personen besetzte Fläche) reagiert.

Einstellung	Beschreibung
Duration	Stellen Sie die Zeitdauer ein, über die die Videoanalyse Erkennung von Menschenmengen Werte mittelt. Eine längere Dauer reduziert die Anzahl der Alarme, erhöht aber die Wahrscheinlichkeit, Alarme zu verpassen. Eine kürzere Dauer erhöht die Anzahl der Alarme, erhöht aber die Wahrscheinlichkeit von Fehlalarmen.
Threshold	Verwenden Sie den Schieberegler, um die Werte zu definieren, die das Ereignis auslösen. Werte, die außerhalb des Schwellenwerts liegen, lösen das Ereignis aus. Für den Alarmtyp Capacity stellt der Schieberegler den Prozentsatz der maximalen Kapazität dar, die Sie für die Videoanalyse Erkennung von Menschenmengen konfigurieren. Für den Alarmtyp Occupancy stellt der Schieberegler den Prozentsatz der Szene (definiert durch die Verarbeitungsmaske) dar, der von Personen besetzt ist.

Ereigniseinstellungen für Gesichtserkennung

+

Select video engine from those running on camera

Face Recognition ▼

Match Threshold 50

Max Spoof Score 30

Alarm type

☒ Alarm on all real faces

☐ Alarm only on real faces not in the list(s)

☐ Alarm only on real faces in the list(s)

☐ Alarm only on spoofing attacks

+

Einstellung	Beschreibung
Match Threshold	Legen Sie fest, wie genau das erkannte Gesicht mit einem Gesicht auf der Sperrliste übereinstimmen muss, um einen Alarm auszulösen, oder mit einem Gesicht auf der Zulassungsliste, um keinen Alarm auszulösen. Diese Einstellung gilt nicht, wenn Sie Alarm on all faces auswählen.
Max Spoof Score	Legen Sie den Wert fest, den ein Gesicht überschreiten muss, damit die Videoanalyse Gesichtserkennung das Gesicht als Spoofing einstuft. Der Standardwert ist 30.
Alarm on all real faces	Auswählen, um einen Alarm auszulösen, wenn die Videoanalyse Gesichtserkennung ein Gesicht erkennt.

Einstellung	Beschreibung
Alarm only on real faces not in the list(s)	Auswählen, um einen Alarm auszulösen, wenn die Videoanalyse Gesichtserkennung ein Gesicht erkennt, das nicht auf den von Ihnen ausgewählten Listen steht. Zu den Listenoptionen gehören die Standardlisten (Allowed und Blocked) sowie alle von Ihnen erstellten benutzerdefinierten Listen.
Alarm only on real faces in the list(s)	Auswählen, um einen Alarm auszulösen, wenn die Videoanalyse Gesichtserkennung ein Gesicht erkennt, das auf den von Ihnen ausgewählten Listen steht. Zu den Listenoptionen gehören die Standardlisten (Allowed und Blocked) sowie alle von Ihnen erstellten benutzerdefinierten Listen.
Alarm only on spoofing attacks	Auswählen, um einen Alarm nur dann auszulösen, wenn die Videoanalyse Gesichtserkennung ein Gesicht mit einem Spoof-Wert erkennt, der den maximalen Spoof-Wert überschreitet.

Ereigniseinstellungen für Erkennung von zurückgelassenen und entwendeten Gegenständen

Die Ereigniseinstellungen für die Videoanalyse Erkennung von zurückgelassenen und entwendeten Gegenständen sind sichtbar, wenn Sie diese als Video-Engine für ein Ereignis auswählen.

Einstellung	Beschreibung
Processing mask	Zeichnen Sie eine Verarbeitungsmaske, um zu bestimmen, welche Bereiche ein Ereignis auslösen können.
Alarm based on percentage of object inside alarm mask	Auswählen, wenn das Ereignis Regeln basierend auf dem Prozentsatz des Objekts innerhalb der Verarbeitungsmaske auslöst.
Alarm size	Definieren Sie die maximale und minimale Größe von Objekten, die die Regel auslösen können.
Alarm only if	Auswählen, um nur dann einen Alarm auszulösen, wenn mehrere Alarmer in einer bestimmten Zeit auftreten. Sie können sowohl die Anzahl der Alarmer als auch die Zeit definieren.
Or at least	Auswählen, um einen Alarm auszulösen, wenn sich eine bestimmte Anzahl von Pixeln in einer bestimmten Zeit ändert. Sie können sowohl die Anzahl der Pixel als auch die Zeit definieren.

Ereigniseinstellungen für Bewegungserkennung

Die Ereigniseinstellungen für Bewegungserkennung sind sichtbar, wenn Sie diese als Video-Engine für ein Ereignis auswählen.

Einstellung	Beschreibung
Processing mask	Zeichnen Sie eine Verarbeitungsmaske, um zu bestimmen, welche Bereiche ein Ereignis auslösen können.

Ereigniseinstellungen für Verfolgung von Personen und Fahrzeugen im Außenbereich

Die Ereigniseinstellungen für die Videoanalyse Verfolgung von Personen und Fahrzeugen im Außenbereich sind sichtbar, wenn Sie diese als Video-Engine für ein Ereignis auswählen.

Einstellung	Beschreibung
Class	Wählen Sie die Klasse des Objekts aus, das die Regel auslöst.
Behavior	Wählen Sie aus, ob ein sich für eine bestimmte Zeit bewegendes oder ein sich für eine bestimmte Zeit aufhaltendes Objekt die Regel auslöst, und legen Sie die Zeit fest.
Use Mask	Wählen Sie aus, welche Bewegung beim Auslösen der Regel verwendet werden soll. Wählen Sie aus, ob der Anfang, das Ende oder ein beliebiger Teil der Bewegungsspur den Alarm auslöst, und wählen Sie aus, ob ein beliebiger Teil des Objekts die Regel auslösen kann.
Use Fences	Wählen Sie aus, ob Regeln ausgelöst werden sollen, wenn ein Objekt eine der Begrenzungen überschreitet, oder wenn ein Objekt alle Begrenzungen überschreitet.

Ereigniseinstellungen für TCP-Listener

Die Ereigniseinstellungen für die Videoanalyse "TCP-Listener" sind sichtbar, wenn Sie sie als Video-Engine für ein Ereignis auswählen.

Einstellung	Beschreibung
Alarm type	Wählen Sie aus, ob das Ereignis auf beliebige Metadaten oder auf Metadaten reagiert, die einen bestimmten Text enthalten.
Alarm on metadata that contains	Geben Sie den Text an, der das Ereignis auslöst, wenn Sie auswählen, bei Metadaten mit bestimmtem Text einen Alarm auszulösen.

Ereigniseinstellungen für Senstar Network Manager

Ereignisse vom Senstar Network Manager können Regeln auf dem Server auslösen.

Einstellung	Beschreibung
Activated	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundener Ausgang aktiviert wird.
Deactivated	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundener Ausgang deaktiviert wird.
Alarm	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundener Eingang in einen Alarmzustand wechselt.
Alarm Secure	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundener Eingang einen Alarmzustand verlässt.
Communication Fail	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät in einen Kommunikationsfehlerzustand wechselt.
Communication Fail Secure	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät einen Kommunikationsfehlerzustand verlässt.

Einstellung	Beschreibung
Communication Fault	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät in einen Kommunikationsstörungszustand wechselt.
Communication Fault Secure	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät einen Kommunikationsstörungszustand verlässt.
Diagnostic Warning	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät in einen Diagnosewarnungszustand wechselt.
Diagnostic Warning Secure	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät einen Diagnosewarnungszustand verlässt.
Diagnostic Fatal	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät in einen schwerwiegenden Diagnosezustand wechselt.
Diagnostic Fatal Secure	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät einen schwerwiegenden Diagnosezustand verlässt.
Enclosure Tamper	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät in einen Gehäusemanipulationszustand wechselt.
Enclosure Tamper Secure	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundenes Gerät einen Gehäusemanipulationszustand verlässt.
Tamper	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundener Eingang in einen Manipulationszustand wechselt.
Tamper Secure	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundener Eingang einen Manipulationszustand verlässt.
Trouble	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundener Eingang in einen Störungszustand wechselt.
Trouble Secure	Wählen Sie diese Option, um eine Regel auf dem Server auszulösen, wenn ein mit dem Senstar Network Manager verbundener Eingang einen Störungszustand verlässt.

Ereigniseinstellungen für Senstar Symphony Access Control

Ereignisse von Senstar Symphony Access Control können Regeln auf dem Server auslösen.

Einige Ereignisse sind in der Konfigurationsoberfläche des Server doppelt aufgeführt, um sowohl Proximity-Kartenleser als auch Magnetstreifen-Kartenleser abzudecken. Ereignisse mit der Kennzeichnung >> sind die Standardeinstellung für Proximity-Kartenleser und Abwärtsbewegungen bei Magnetstreifen-Kartenlesern. Ereignisse mit der Kennzeichnung << gelten für Aufwärtsbewegungen bei Magnetstreifen-Kartenlesern.

Einstellung	Beschreibung
Door Forced Open	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossener Türkontakt ein gewaltsames Öffnen der Tür erkennt.
Door Held Open	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossener Türkontakt erkennt, dass die Tür offen gehalten wird.
Door is Closed	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossener Türkontakt erkennt, dass die Tür geschlossen ist.
Door is Opened	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossener Türkontakt erkennt, dass die Tür offen ist.
Request To Exit	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossener Türkontakt oder ein Anforderungsgerät zum Verlassen eine Anforderung zum Verlassen erkennt.
Request To Exit (Door Used)	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Anforderungsgerät zum Verlassen eine Anforderung zum Verlassen mit benutzter Tür erkennt.
Request to Exit (Door Not Used)	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Anforderungsgerät zum Verlassen eine Anforderung zum Verlassen ohne benutzte Tür erkennt.
Door is Locked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass die Tür verriegelt ist.
Door is Unlocked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass die Tür entriegelt ist.
Deadbolt Disengaged	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass der Riegel ausgerückt ist.
Deadbolt Engaged	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass der Riegel eingerückt ist.
Door Schedule is Disabled	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass der Türzeitplan deaktiviert ist.
Door Schedule is Enabled	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass der Türzeitplan aktiviert ist.
Door is Momentarily Unlocked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass die Tür kurzzeitig entriegelt ist.
Double Locked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass sowohl der Riegel als auch das Griffschloss eingerückt sind. Dieses Ereignis gilt nur für Funkschlösser von Assa Abloy.

Einstellung	Beschreibung
Locked Down	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass ein Befehl zum Verriegeln der Tür und Deaktivieren des Lesegerätemodus ausgegeben wird. Dieses Ereignis gilt nur für Funkschlösser von Assa Abloy.
Locked Open	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türschlossgerät erkennt, dass ein Befehl zur Wiederherstellung des Normalbetriebs von Tür und Lesegerät nach einem Locked-Down-Ereignis ausgegeben wird. Dieses Ereignis gilt nur für Funkschlösser von Assa Abloy.
Control Point Deactivated	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türsignalgerät erkennt, dass ein Steuerpunkt deaktiviert wird.
Control Point Activated	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Türsignalgerät erkennt, dass ein Steuerpunkt aktiviert wird.
Control Point Pulse	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Steuerpunktgerät erkennt, dass der Steuerpunkt einen Befehl zum kurzzeitigen Aktivieren eines Relais oder Ausgangs erhält.
Reader Mode: Disabled	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät deaktiviert ist.
Reader Mode: Unlocked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät entriegelt ist.
Reader Mode: Locked (REX Only)	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät verriegelt ist und nur durch eine Anforderung zum Verlassen (REX) entriegelt werden kann.
Reader Mode: Facility Code Only	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät nur entriegelt werden kann, wenn der Facility Code auf einer Karte mit dem Facility Code in der Systemkonfiguration übereinstimmt.
Reader Mode: Card Only	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät so eingestellt ist, dass es nur Karten akzeptiert.
Reader Mode: PIN Only	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät so eingestellt ist, dass es nur PINs akzeptiert.
Reader Mode: Card and PIN	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät so eingestellt ist, dass es nur Karten mit PINs akzeptiert.
Reader Mode: Card or PIN	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät so eingestellt ist, dass es Karten oder PINs akzeptiert.

Einstellung	Beschreibung
User Command Requested	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät erkennt, dass die Terminaltastatur einen Benutzercode anfordert.
Reader Mode: Fingerprint Only	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät so eingestellt ist, dass es nur Fingerabdrücke akzeptiert.
Reader Mode: Card and Fingerprint	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät so eingestellt ist, dass es nur Karten mit Fingerabdrücken akzeptiert.
Reader Mode: Card or Fingerprint	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät so eingestellt ist, dass es Karten oder Fingerabdrücke akzeptiert.
Reader Mode: Office First	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät so eingestellt ist, dass es auf die First-Person-In-Situation reagiert.
Reader Mode: Blocked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät deaktiviert ist. Dieses Ereignis gilt nur für Funkschlösser von Assa Abloy.
Reader Mode: Emergency Lock	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät in den Notfall-Verriegelungszustand wechselt.
Reader Mode: Emergency Unlock	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Notfall-Verriegelungszustand verlässt.
Access Granted	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt gewährt.
Access Denied: Level	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät einer Karte aufgrund einer unzureichenden Zugangsstufe den Zutritt verweigert.
Access Denied: Time	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät einer Karte aufgrund einer unzureichenden Zugangsstufe zu einer bestimmten Zeit den Zutritt verweigert.
Access Denied: Locked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert und die Tür verriegelt.
Access Denied: Card	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät einer Karte den Zutritt verweigert.
Access Denied: Facility	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät einer Karte aufgrund eines falschen Facility Codes den Zutritt verweigert.

Einstellung	Beschreibung
Access Denied: Passback	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt aufgrund eines Karten-Passbacks verweigert.
Access Denied: Issue Code	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt aufgrund eines falschen Issue Codes verweigert. Ein Issue Code besteht aus einem Facility Code, einem Re-Issue Code und einer Kartennummer. Issue Codes werden mit Mercury-Controllern verwendet, um zu verfolgen, wie oft eine Karte neu ausgegeben wird.
Access Denied: Invalid	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt aufgrund eines ungültigen Kartenformats verweigert.
Card Information Event	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät ein Karteninformationseignis erkennt. Karteninformationseignisse sind spezielle Ereignisse, die Informationen zu einem vorherigen Ereignis anzeigen. Wenn beispielsweise einer Karte aufgrund eines falschen Facility Codes der Zutritt verweigert wird, zeigt das Karteninformationseignis den falschen Facility Code an.
Access Granted: Unlocked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt gewährt und die Tür entriegelt.
Access Granted: Door Not Used	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt gewährt, aber die Tür nicht benutzt wurde.
Access Granted: Door Used	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt gewährt und die Tür benutzt wurde.
Access Denied: Deactivated Card	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt aufgrund einer deaktivierten Karte verweigert.
Access Denied: Before Activation Date	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil die Karte noch nicht aktiv ist.
Access Denied: After Expiration Date	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil die Karte abgelaufen ist.
Access Denied: Invalid PIN	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt aufgrund einer ungültigen PIN verweigert.

Einstellung	Beschreibung
Access Denied: 2nd Card not Presented	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil die zweite Karte (für die Zwei-Personen-Authentifizierung erforderlich) nicht vorgelegt wurde.
Access Denied: Occupancy Limit Reached	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät erkennt, dass das Lesegerät den Zutritt verweigert hat, weil die Belegungsgrenze erreicht wurde.
Access Denied: Area not Enabled	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil der Bereich nicht aktiviert ist.
Access Denied: Use Limit	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil die Karte die maximal zulässige Anzahl an Verwendungen überschritten hat.
Access Denied: Duress Code Detected	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil ein Notfallcode verwendet wurde.
Access Denied: Duress (Door Used)	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil ein Notfallcode verwendet und die Tür benutzt wurde.
Access Denied: Duress (Door Not Used)	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät erkennt, dass das Lesegerät den Zutritt verweigert hat, weil ein Notfallcode verwendet und die Tür nicht benutzt wurde.
Access Denied: Unauthorized Assets	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil die Assets für die Karte nicht autorisiert sind.
Access Denied: Biometric Verification Error	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil ein Notfallcode verwendet und die Tür nicht benutzt wurde.
Access Granted: Verification Confirmed	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt gewährt, weil die Verifizierung bestätigt wurde.
Access Denied: No Biometric Record	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil der Benutzer keinen biometrischen Datensatz hat.
Access Denied: No Biometric Device	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät, das keine biometrische Funktion besitzt, in den biometrischen Modus versetzt und eine Karte vorgelegt wird. Dieses Ereignis gilt nur für ZK-Geräte.

Einstellung	Beschreibung
Intrusion Area: Armed	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät erkennt, dass der Bereich scharfgeschaltet und alarmbereit ist.
Intrusion Area: Disarmed	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät erkennt, dass der Bereich unscharf geschaltet und nicht alarmbereit ist.
Intrusion Request Attempt: Denied	Dieses Ereignis ist nicht anwendbar.
Intrusion Disarm Attempt: Denied	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät einen Unscharfschaltungsversuch aufgrund unzureichender Berechtigungen verweigert.
Access Granted: Office First Door Unlocked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt gewährt und entriegelt wird, weil die First-Person-In-Situation eintritt.
Access Granted: Office First Door Locked	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt gewährt und verriegelt wird, weil die First-Person-In-Situation eintritt.
Access Denied: Punch Interval	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt verweigert, weil das Intervall zwischen zwei Karten zu kurz ist. Dieses Ereignis gilt nur für ZK-Geräte.
Access Granted: Passback (Door Not Used)	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt bei einem Karten-Passback gewährt und die Tür nicht benutzt wurde.
Access Granted: Passback (Door Used)	Auswählen, um eine Regel auf dem Server auszulösen, wenn ein an Senstar Symphony Access Control angeschlossenes Lesegerät den Zutritt bei einem Karten-Passback gewährt und die Tür benutzt wurde.

Ereigniseinstellungen für Senstar Sensor Fusion

Die folgenden Einstellungen bestimmen, wann die Senstar Sensor Fusion Ereignisse auf dem Server auslöst.

Sie können die Senstar Sensor Fusion so konfigurieren, dass Ereignisse von der Videoanalyse, dem Perimeter-Eindringungserkennungssystem oder beiden ausgelöst werden.

SENSTAR

Devices

Security

Rules

Licenses

Settings

Farm ID: 139470

Web Client

Log Out

Help

Rules

Events

Action Sets

Schedules

Rules > Events

Properties

Fusion Events

SensorFusionWindow

Add Sources

Properties

Name Required

Enter a name here...

SensorFusionWindow

Class

☒ People

☒ Vehicles

☒ Unknown

Segments

☒ Sensor Segment 1

Save

Cancel

Einstellung	Beschreibung
People	Wählen Sie aus, ob die Senstar Sensor Fusion Ereignisse auslösen soll, wenn sie eine Person erkennt.
Vehicles	Wählen Sie aus, ob die Senstar Sensor Fusion Ereignisse auslösen soll, wenn sie ein Fahrzeug erkennt.
Unknown	Wählen Sie aus, ob die Senstar Sensor Fusion Ereignisse auslösen soll, wenn sie ein unbekanntes Objekt erkennt.
Segments	Wählen Sie die Sensorsegmente aus, für die die Senstar Sensor Fusion Ereignisse auslösen soll.

Aktionssätze

Aktionssätze sind Kombinationen von Aktionen, die der Server ausführt, wenn eine Regel einen Alarm auslöst.

Aktionssatz erstellen

Sie können einen Aktionssatz erstellen, um festzulegen, welche Aktionen der Server ausführt, wenn eine Regel ausgelöst wird.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Action Sets.
2. Klicken Sie auf New Action Set.

3. Geben Sie einen Namen für den Aktionssatz ein.

4. Führen Sie im Abschnitt Alarm die folgenden Aufgaben aus:

- a. Wählen Sie in der Geräteliste die Geräte aus, die Sie in Ansichtspanels in der Oberfläche des Windows Client anzeigen möchten. Die Geräteliste ist standardmäßig in Gerätegruppen gruppiert. Wenn Sie die Geräte in einer alphabetischen Liste anzeigen möchten, wählen Sie

Hide Device Groups

aus.

- a. Geben Sie im Feld neben dem ausgewählten Gerät einen Namen für das Panel ein, in dem Sie das Gerät anzeigen möchten. Wenn Sie keinen Panel-Namen eingeben, zeigt der

Windows Client

das Gerät im Standardansichtspanel an.

1. Um auszuwählen, wo der Alarm angezeigt wird, führen Sie eine der folgenden Aufgaben aus:

- Um den Alarm einer Kamera zuzuordnen und den Alarm in einer Kamerazeitleiste anzuzeigen, wählen Sie die Kamera in der Liste Choose a Camera aus.
- Um den Alarm einem Lageplan zuzuordnen und den Alarm auf dem Lageplan anzuzeigen, wählen Sie den Lageplan in der Liste Choose a Map aus.

2. Wählen Sie in der Liste Record die Kameras aus, die Aufnahmen erstellen, wenn ein Alarm auftritt.

3. Um weitere Aktionen hinzuzufügen, führen Sie die folgenden Aufgaben aus:

- a. Wählen Sie in der Liste Pick an item eine Aktion aus.
image::air_server_rules_action_set_create.png[]
- b. Klicken Sie auf Add.
- c. Konfigurieren Sie die Einstellungen für die Aktion.

4. Klicken Sie auf Save.

Aktionssatz bearbeiten

Sie können einen Aktionssatz bearbeiten, um zu ändern, welche Aktionen der Server ausführt, wenn eine Regel ausgelöst wird.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Action Sets.
2. Wählen Sie einen Aktionssatz aus.
3. Klicken Sie auf Edit.
4. Ändern Sie den Aktionssatz.
5. Klicken Sie auf Save.

Aktionssatz löschen

Sie können einen Aktionssatz löschen, um ihn vom Server zu entfernen.

Wenn der Aktionssatz einer Regel zugeordnet ist, sehen Sie beim Löschen eines Aktionssatzes eine zusätzliche Warnmeldung und eine Bestätigungsaufforderung. Wenn Sie den Aktionssatz in diesem Fall entfernen, funktioniert die Regel nicht wie erwartet.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Action Sets.

2. Wählen Sie einen Aktionssatz aus.
3. Klicken Sie auf Delete.
4. Klicken Sie auf Yes.

Zeitpläne

Zeitpläne bestimmen, wann Regeln im Server aktiv sind.

Sie können einen Zeitplan als Teil des Regelerstellungsprozesses oder unabhängig in der Server-Konfigurationsoberfläche erstellen. Zeitpläne arbeiten in Halbstundenblöcken und unterstützen tägliche Ausnahmen, die jährlich wiederkehren können.

Zeitplan erstellen

Sie können einen Zeitplan erstellen, um festzulegen, wann eine Regel aktiv ist.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Schedules.
2. Klicken Sie auf Add Schedule.
3. Geben Sie einen Namen für den Zeitplan ein.
4. Definieren Sie die aktiven und inaktiven Zeiten für den Zeitplan.
5. Fügen Sie bei Bedarf Ausnahmen zum Zeitplan hinzu.
 - a. Wählen Sie ein Datum aus.
 - b. Wählen Sie aus, ob die Ausnahme jedes Jahr an diesem Datum wiederholt werden soll.
 - c. Klicken Sie auf Add Exception.
 - d. Definieren Sie die aktiven und inaktiven Zeiten für die Ausnahme.
6. Klicken Sie auf Save.

Zeitplan bearbeiten

Sie können einen Zeitplan bearbeiten, um zu ändern, wann eine Regel aktiv ist.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Schedules.
2. Wählen Sie einen Zeitplan aus.
3. Klicken Sie auf Edit.
4. Ändern Sie den Zeitplan.
5. Klicken Sie auf Save.

Zeitplan klonen

Sie können einen Zeitplan klonen, um ihn als Vorlage für einen neuen Zeitplan zu verwenden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Schedules.
2. Wählen Sie einen Zeitplan aus.
3. Klicken Sie auf Clone.
4. Ändern Sie den Zeitplan.

5. Klicken Sie auf Save.

Zeitplan löschen

Sie können einen Zeitplan löschen, um ihn vom Server zu entfernen.

Sie können einen Zeitplan nicht löschen, wenn er einer Regel zugeordnet ist.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Rules > Schedules.
2. Wählen Sie einen Zeitplan aus.
3. Klicken Sie auf Delete.
4. Klicken Sie auf Yes.

Lizenzen

Mit den Lizenzeinstellungen für den Server können Sie Lizenzen anzeigen und aktualisieren.

Sie greifen auf die Lizenzeinstellungen über die Registerkarte Licenses in der Konfigurationsoberfläche des Server zu.

Im Abschnitt Properties werden die Eigenschaften Ihrer Server-Lizenz angezeigt. Der Abschnitt zeigt das Ablaufdatum der Lizenz und die Softwareversion an, für die die Lizenz gilt.

Im Abschnitt Licenses in Farm werden die Lizenzen für Videoanalysen, die Kameralizenzen und die MAC-Adressen der in der Serverfarm zulässigen Server angezeigt.

Im Abschnitt Unlicensed Devices werden die Kameras im Netzwerk angezeigt, die keiner Lizenz zugeordnet sind.

Lizenzen aktualisieren

Sie können Ihre Lizenzen aktualisieren, um nach neueren Versionen aus dem Senstar Xnet zu suchen oder Aktualisierungen manuell anzuwenden.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Licenses.
2. Klicken Sie auf Refresh Licenses.
3. Führen Sie eine der folgenden Aufgaben aus:
 - a. Um die Lizenz von senstar.com zu aktualisieren, wählen Sie Refresh license from senstar.com aus.
 - b. Um die Lizenz aus einer Datei zu aktualisieren, wählen Sie Refresh license from file aus, navigieren Sie zur Lizenzdatei oder ziehen Sie die Lizenzdatei in das Fenster.
4. Klicken Sie auf OK.

Lizenz-XML anzeigen

Sie können das XML für Ihre Lizenz anzeigen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Licenses.
2. Klicken Sie auf Show Raw License.

Einstellungen

Die Einstellungen für den Server ermöglichen es Ihnen, Server, allgemeine Einstellungen, Cloud-Dienste, Alarmsummen, Updates, Backup und Wiederherstellung, Lagepläne sowie geschützte Aufnahmen zu konfigurieren.

Sie greifen auf die Einstellungen über die Registerkarte Settings in der Server-Konfigurationsoberfläche zu. Die Registerkarte Settings enthält die Registerkarten Servers, General Settings, Cloud Services, Aggregates, Maintenance, Backup & Restore, Maps und Protected Footage.

Server

Die Registerkarte „Servers“ der Konfigurationsoberfläche des Server dient zum Konfigurieren von Einstellungen, die für einzelne Server-Instanzen in der Serverfarm spezifisch sind.

Auf der Registerkarte „Servers“ können Sie Servereinstellungen bearbeiten, den Videospeicher konfigurieren und Serverredundanz einrichten.

+



+

Videospeicher für einen Server konfigurieren

Sie können konfigurieren, wie der Server Videoaufnahmen speichert und verwaltet. Diese Einstellungen gelten für den ausgewählten Server.

Sie können konfigurieren, wo der Server Videoaufnahmen speichert, wie viele Videoaufnahmen der Server speichert und unter welchen Bedingungen der Server Videoaufnahmen löscht. Außerdem können Sie Sicherungspfade für Videoaufnahmen festlegen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie einen Server aus und klicken Sie auf Edit.
3. Um einen Speicherpfad festzulegen, führen Sie im Abschnitt Video Storage die folgenden Aufgaben aus:
 - a. Geben Sie den Pfad an, in dem der Server Videodateien speichern soll.
 - b. Um einen weiteren Speicherpfad hinzuzufügen, klicken Sie auf Add Another Path und geben Sie den Pfad an.

c. Um Videodateien nur in einem Speicherpfad zu speichern, wählen Sie Failover. Der Server

versucht, Videodateien zuerst in den ersten Pfad der Liste zu speichern. Wenn dieser Pfad nicht verfügbar ist, versucht der

Server

, die Videodateien in den nächsten Pfad der Liste zu speichern.

- a. Um Videodateien in alle Speicherpfade zu speichern, wählen Sie Redundant.
- b. Wählen Sie unter Force disk reads from den Pfad aus, von dem der Server Videodateien lesen soll.
 1. Um einen sekundären (Archiv-)Speicherpfad festzulegen, führen Sie die folgenden Aufgaben aus:
 - c. Wählen Sie Archive video to secondary storage path.
 - d. Geben Sie den Pfad ein, in dem der Server Videodateien speichern soll. Sie müssen für jeden primären Speicherpfad einen sekundären (Archiv-)Speicherpfad eingeben.
 - e. Stellen Sie im Feld Days to store before archiving ein, wie viele Tage vergehen müssen, bevor der Server die Videodateien in den sekundären (Archiv-)Speicherpfad speichert. Dieser Wert muss kleiner sein als der Wert

Limit the number of days video is stored

.

1. Um eine Begrenzung basierend auf dem verbleibenden Speicherplatz festzulegen, stellen Sie den Speicherplatz im Feld MB oder den Prozentsatz des Speicherplatzes im Feld % ein.
2. Um die maximale Anzahl von Tagen festzulegen, für die der Server Videodateien aufbewahren kann, wählen Sie Limit the number of days video is stored und stellen Sie die Anzahl der Tage ein.
3. Um Metadaten beizubehalten, nachdem der Server Videodateien gelöscht hat, wählen Sie Keep metadata longer und stellen Sie die Anzahl der Tage ein.
4. Um Videodateien, die während eines Failover erzeugt werden, vom redundanten Server zurück auf den wiederhergestellten primären Server zu kopieren, wählen Sie SAN Failover mode: Copy files to owner server. Sowohl der primäre

Server

als auch der redundante

Server

müssen Lese- und Schreibberechtigungen für die Speicherpfade auf jedem

Server

besitzen.

1. Definieren Sie in der Liste Cameras alle kamerabezogenen Speicherpfade. Standardmäßig speichert der

Server

Videodateien aller Kameras in den Speicherpfaden.

1. Klicken Sie auf Save.

SAN-Failover-Modus

Der SAN-Failover-Modus arbeitet zusammen mit der Server-Redundanz, um lokale Aufzeichnungsdateien vom redundanten Server zurück auf den primären Server zu verschieben, wenn sich der primäre Server vom Ausfall erholt.

Wenn sich der primäre Server vom Ausfall erholt, versucht er, Aufzeichnungsdateien vom redundanten Server zu kopieren und diese Dateien mit den vorhandenen Aufzeichnungsdateien im lokalen Speicher zusammenzuführen.

Um den SAN-Failover-Modus zu nutzen, führen Sie folgenden Workflow aus:

1. Erstellen Sie in der Server-Konfigurationsoberfläche eine Redundanzgruppe und fügen Sie jeden Server der Redundanzgruppe hinzu.
2. Stellen Sie auf jedem Computer, der einen Server in der Redundanzgruppe hostet, sicher, dass der Datenordner denselben Laufwerksbuchstaben wie alle anderen Computer hat.
3. Erstellen Sie auf jedem Computer, der einen Server in der Redundanzgruppe hostet, eine Freigabe für den Datenordner und benennen Sie die Freigabe DATA_X, wobei X der Laufwerksbuchstabe ist. Benennen Sie die Freigabe beispielsweise DATA_G, wenn sich die Freigabe auf dem Laufwerk G befindet.
4. Gewähren Sie den Benutzerkonten, die die Senstar Symphony-Dienste auf jedem anderen Server in der Redundanzgruppe ausführen, Lese- und Schreibberechtigungen für die Datenordner-Freigabe.
5. Aktivieren Sie in der Server-Konfigurationsoberfläche das Kontrollkästchen "SAN failover mode" für jeden Server in der Redundanzgruppe. +
image::ROOT:air_server_san_failover_01.png[]

Sie müssen den SAN-Failover-Modus normalerweise nicht verwenden, wenn Sie einen gemeinsamen Netzwerkstandort für die Speicherung der Datenordner jedes Server in der Redundanzgruppe verwenden.

Überlastschutz konfigurieren

Sie können einen Server so konfigurieren, dass Kameras automatisch auf einen anderen Server verschoben werden, wenn die CPU-Last zu hoch wird.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie einen Server aus und klicken Sie auf Overload Protection.
3. Wählen Sie aus, ob Kameras auf einen anderen Server verschoben werden sollen, wenn die CPU-Last zu hoch ist.
4. Wählen Sie aus, ob redundante Server verwendet werden sollen. Wenn Sie redundante Server verwenden, um Kameras im Falle einer Überlastung aufzunehmen, können Sie die Funktion Serverredundanz nicht verwenden.
5. Stellen Sie den CPU-Schwellenwert (in Prozent) ein, ab dem sich der Server als überlastet betrachtet.
6. Stellen Sie die Abfragefrequenz (in Sekunden) ein, um festzulegen, wie oft der Server die CPU-Last überwacht.
7. Stellen Sie die maximale Anzahl von Kameras ein, die auf den neuen Server verschoben werden sollen.
8. Klicken Sie auf Save.

Dienste verwalten

Sie können konfigurieren, wie der Server die Senstar Symphony-Dienste verwaltet.

Mit der Verwaltung von Diensten können Sie Massenänderungen an Senstar Symphony-Diensten vornehmen. Sie können mehrere Senstar Symphony-Dienste gleichzeitig starten und stoppen, die Senstar Symphony-Dienste auf automatischen Start einstellen und das Benutzerkonto ändern, das der Server zum Ausführen des Server verwendet.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie einen Server aus und klicken Sie auf Edit.
3. Führen Sie im Abschnitt Services die folgenden Aufgaben aus:
 - a. Um den Status eines Senstar Symphony-Dienstes zu ändern, wählen Sie den Dienst aus und klicken Sie auf Toggle Selected. Durch das Ausführen dieser Aufgabe wird ein laufender Dienst gestoppt oder ein gestoppter Dienst gestartet.
 - b. Um die Dienstliste zu aktualisieren, klicken Sie auf die Schaltfläche Refresh.
 - c. Um die Senstar Symphony-Dienste automatisch zu starten, wenn der Computer, auf dem der Server gehostet wird, startet, wählen Sie Automatically start Symphony services on system startup aus.
 - d. Um das Benutzerkonto festzulegen, das die Senstar Symphony-Dienste ausführt, wählen Sie entweder Log on as Local System account, um das lokale Systemkonto zu verwenden, oder wählen Sie This account und geben Sie die Anmeldedaten des Kontos ein, um ein anderes Konto zu verwenden. Das lokale Systemkonto ist das Standardkonto, das der

Server

verwendet, um

Senstar Symphony

-Dienste auszuführen, aber Sie ändern das Konto, um auf Daten an einem freigegebenen Netzwerkstandort zuzugreifen.

1. Klicken Sie auf Save.

Server-Redundanz

Der Server unterstützt Server-Redundanz in Serverfarmen. Wenn der primäre Server nicht mehr reagiert, wird die Kamera- und Geräteverarbeitung auf einen redundanten Server verschoben.

Um Server-Redundanz zu nutzen, benötigen Sie mindestens einen primären Server und einen redundanten Server in einer Redundanzgruppe. Der primäre Server führt aktiv die Kamera- und Geräteverarbeitung durch. Der redundante Server ist aktiv, hat aber keine Kameras oder Geräte zugewiesen. Es muss jederzeit mindestens ein redundanter Server in der Serverfarm verfügbar sein.

Wenn ein Failover auftritt, übernimmt der redundante Server die Kamera- und Geräteverarbeitung vom primären Server, solange dieser nicht verfügbar ist. Wenn sich der primäre Server vom Ausfall erholt, geschieht eines der folgenden Dinge:

- Sie können die Kamera- und Geräteverarbeitung automatisch auf den primären Server zurückverschieben, indem Sie Failback in der Server-Konfigurationsoberfläche aktivieren.
- Sie können die Kamera- und Geräteverarbeitung manuell auf den primären Server zurückverschieben, indem Sie die Server in der Server-Konfigurationsoberfläche tauschen.

- Sie können den primären Server als redundanten Server verwenden.

Master-Server

In einer Serverfarm ist ein Server der Master-Server. Der Master-Server ist der Server, der die Farm koordiniert und entscheidet, wann Failover und Failback auftreten.

Der Master-Server ist für die folgenden Aufgaben verantwortlich:

- Erkennen, wenn ein primärer Server nicht mehr reagiert, und Auslösen eines Failover-Ereignisses.
- Auswahl des redundanten Server, der die Kamera- und Geräteverarbeitung übernimmt.
- Koordination des Failbacks, wenn der primäre Server wieder in Betrieb ist.
- Vorhalten der maßgeblichen Kopie der Konfiguration, sodass jeder Server in der Farm die gleichen Einstellungen sieht.

Der Master-Server führt seine eigene Kamera- und Geräteverarbeitung weiter aus, während er diese Aufgaben wahrnimmt.

Wenn der Master-Server nicht mehr verfügbar ist, wählen die verbleibenden Server in der Farm automatisch einen neuen Master-Server, sodass Failover-Entscheidungen ohne Eingreifen des Administrators weiterhin möglich sind. Wenn der ursprüngliche Master-Server wieder in Betrieb ist, übernimmt er die Rolle nicht automatisch zurück.

Sie können manuell auswählen, welcher Server der Master-Server ist, indem Sie auf das Sternsymbol neben dem Server auf der Seite "Servers" in der Server-Konfigurationsoberfläche klicken.

Server zu einer Redundanzgruppe hinzufügen

Sie können einen Server zu einer Redundanzgruppe hinzufügen oder eine neue Redundanzgruppe erstellen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie einen Server aus und klicken Sie auf Edit.
3. Führen Sie in der Liste Server Group eine der folgenden Aktionen aus:
 - Um den Server zu einer vorhandenen Redundanzgruppe hinzuzufügen, wählen Sie die Gruppe aus.
 - Um den Server zu einer neuen Redundanzgruppe hinzuzufügen, wählen Sie <New> aus.
4. Klicken Sie auf Save.

Failover konfigurieren

Sie können den Server so konfigurieren, dass Kameras auf einen sekundären Server verschoben werden, wenn der primäre Server offline geht.

Konfigurieren Sie zuvor den Videospeicher für den Server.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie einen Server aus und klicken Sie auf Edit.
3. Wählen Sie in der Liste Server Group eine Servergruppe aus, die einen Server enthält, der keine Kameras besitzt.
4. Klicken Sie auf Enable Failover.

Failback konfigurieren

Sie können den Server so konfigurieren, dass Kameras nach einem Failover wieder auf den primären Server verschoben werden, sobald der primäre Server wieder online ist.

Konfigurieren Sie zuvor das Failover für den Server.

Wenn Sie kein Failback konfigurieren, müssen Sie die Kameras manuell auf den primären Server zurück verschieben.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie einen Server aus und klicken Sie auf Edit.
3. Klicken Sie auf Enable Failback.

Kameras verschieben

Sie können alle Kameras von einem Server auf einen anderen Server in Ihrer Serverfarm verschieben.

Sie können nur dann alle Kameras von einem Server auf einen anderen Server verschieben, wenn dem Zielservers keine Kameras zugeordnet sind.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie in der Serverliste den Server aus, von dem Kameras verschoben werden sollen.
3. Wählen Sie in der Serverliste den Server aus, auf den die Kameras verschoben werden sollen.
4. Klicken Sie auf Swap Servers.

Alternative Serveradresse hinzufügen

Sie können mehrere IP-Adressen für den Server hinzufügen, um die Kommunikation mit dem Server zu erleichtern, wenn er Teil einer Multi-Server-Farm ist.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie einen Server aus und klicken Sie auf Edit.
3. Klicken Sie auf das Pluszeichen neben Alternate Server Addresses.
4. Geben Sie im Feld Alternate Server Addresses die alternative Adresse für den Server ein.
5. Wählen Sie den Port aus.
6. Klicken Sie auf Save.

SSL-Zertifikat hinzufügen

Sie können ein SSL-Zertifikat in der Konfigurationsoberfläche des Server zum Server hinzufügen. Dieses Thema gilt nur für Server 8.6.0. In Server 8.6.1 wurden die SSL-Zertifikatseinstellungen in den Einrichtungsassistenten verschoben. Weitere Informationen finden Sie im Senstar Symphony-Installationshandbuch.

Der Server verwendet das SSL-Zertifikat, um Verbindungen von Browsern und der Senstar Symphony Mobile Application zu sichern. Der Server unterstützt PFX-Zertifikatsdateien.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie den Server aus und klicken Sie auf Edit.
3. Navigieren Sie zum Bereich SSL Certificate.

4. Geben Sie im Feld Password das Kennwort für das Zertifikat ein.
5. Ziehen Sie die Zertifikatsdatei in das Feld oder suchen Sie nach der Zertifikatsdatei.
6. Klicken Sie auf Save.

Mobile Verbindungen konfigurieren

Sie können den Server so konfigurieren, dass er Verbindungen mit der Senstar Symphony Mobile Application auf mobilen Geräten unterstützt.

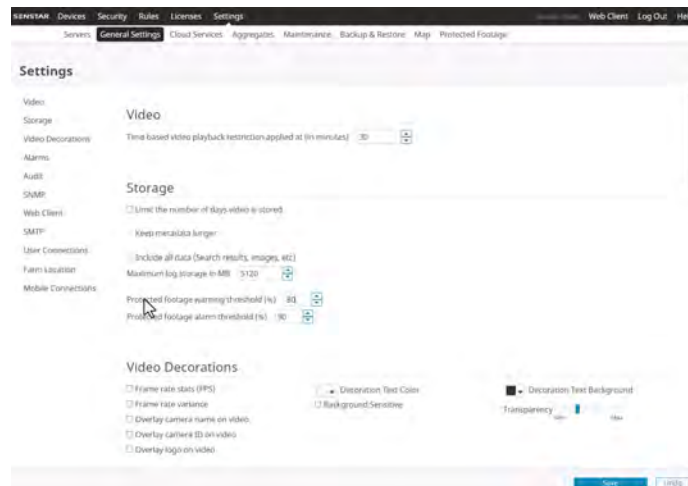
Sie konfigurieren das SSL-Zertifikat, das der Server für mobile Verbindungen verwendet, im Setup-Assistenten von Senstar Symphony.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Servers.
2. Wählen Sie den Server aus und klicken Sie auf Edit.
3. Navigieren Sie zum Abschnitt Mobile Connections.
4. Um das SSL-Zertifikat auszuwählen, klicken Sie auf Change, wählen Sie das Zertifikat aus und klicken Sie auf OK.
5. Um den Netzwerkadapter für mobile Verbindungen auszuwählen, klicken Sie auf Change, wählen Sie den Netzwerkadapter aus und klicken Sie auf OK.
6. Stellen Sie im Feld Mobile Port den Port ein, den der Server verwendet, um auf Anfragen von mobilen Geräten zu lauschen.
7. Stellen Sie im Feld Video Proxy Port den Port ein, den der Server verwendet, um Video an mobile Geräte zu streamen und Video von ihnen zu empfangen.
8. Klicken Sie auf Save.

Allgemeine Einstellungen

Die Registerkarte General Settings wird verwendet, um Einstellungen zu konfigurieren, die für alle Serverinstanzen in der Serverfarm gelten.

Um die Registerkarte General Settings anzuzeigen, klicken Sie in der Konfigurationsoberfläche des Server auf Settings > General Settings. Die Registerkarte General Settings enthält die Abschnitte Video, Storage, Video Decorations, Alarms, Audit, SNMP, Web Client, SMTP, User Connections, Farm Location und Mobile Connections.



Der Abschnitt Storage enthält die Einstellungen für die Videoaufbewahrung sowie die Warn- und Alarmschwellenwerte für geschützte Aufnahmen. Weitere Informationen finden Sie unter [Speicher](#) und [Geschützte Aufnahmen](#).

Video

Der Bereich Video in den Allgemeinen Einstellungen bestimmt, wie lange nach der Aufzeichnung eines Videos ein Benutzer es ansehen kann, bevor es als eingeschränkt markiert wird.

Einstellung	Beschreibung
Time based video playback restriction applied at	Wie lange (in Minuten) nach der Aufzeichnung eines Videos ein Benutzer das Video im Windows Client ansehen kann. Nach Ablauf der Zeit markiert der Server das Video als eingeschränkt, und ein Benutzer benötigt die Berechtigung "View Restricted Historical Video", um das eingeschränkte historische Video anzuzeigen.

Speicher

Der Storage-Bereich in den Allgemeinen Einstellungen bestimmt, wie lange die Serverfarm Video, Video-Metadaten und Protokolldateien aufbewahrt. Diese globale Einstellung tritt in Kraft, wenn Sie keine Videospeichereinstellungen für einzelne Serverinstanzen konfigurieren.

Der Server löscht geschützte Aufnahmen nicht automatisch. Die Schwellenwerte für geschützte Aufnahmen bestimmen, wann der Server Sie warnt, dass geschützte Aufnahmen den Videospeicher füllen. Weitere Informationen finden Sie unter [Geschützte Aufnahmen](#).

Einstellung	Beschreibung
Limit the number of days video is stored	Löscht Video, das älter als die konfigurierte Anzahl von Tagen ist.
Keep metadata longer	Behält Metadaten von Video für die konfigurierte Anzahl von Tagen nach dem Löschen des zugehörigen Videos.
Include all data	Behält alle Daten (z. B. Suchergebnisse, Bilder usw.) für die konfigurierte Anzahl von Tagen.
Maximum log storage in MB	Die maximale Größe der Protokolldateien in Megabyte.
Protected footage warning threshold (%)	Der Prozentsatz des Videospeichers, den geschützte Aufnahmen belegen können, bevor der Server eine Warnung auslöst. Der Standardwert ist 80.
Protected footage alarm threshold (%)	Der Prozentsatz des Videospeichers, den geschützte Aufnahmen belegen können, bevor der Server einen Alarm auslöst. Der Standardwert ist 90.

Videodekorationen

Der Bereich Video Decorations in den Allgemeinen Einstellungen bestimmt, welche Overlay-Informationen im Video erscheinen und wie sie gestaltet sind. Sie können Farbe, Hintergrundfarbe und Hintergrundtransparenz der Videodekos festlegen.

Einstellung	Beschreibung
Frame rate stats	Bildrate (in Bildern pro Sekunde)
Frame rate variance	Zeigt an, wie stark sich die Bildrate über die letzten 50 Bilder ändert
Overlay camera name on video	Kameraname

Einstellung	Beschreibung
Overlay camera ID on video	Kamera-ID
Overlay logo on video	Verwenden Sie ein bereitgestelltes Bild als Logo. Das Bild wird von der TBD-Seite hochgeladen.
Decoration Text Color	Farbe des Texts
Background Sensitive	Passt die Textfarbe automatisch basierend auf den Farben im Video an, um mehr Kontrast zu bieten
Decoration Text Background	Hintergrundfarbe für Text
Transparency	Transparenz des Texthintergrunds (Min ist deckend, Max ist transparent)

Alarme

Der Bereich Alarms in den allgemeinen Einstellungen konfiguriert die Alarmaggregation und die erweiterte Alarmverarbeitung für die Serverfarm. Die Alarmaggregation fasst mehrere Alarms aus derselben Quelle (z. B. Zone) zusammen, um die Belastung des Operators zu verringern. Die erweiterte Alarmverarbeitung legt die Bedingungen fest, unter denen ein Alarm von einem Operator bearbeitet werden kann.

Alarmaggregation

Einstellung	Beschreibung
No Aggregation	Deaktiviert die Alarmaggregation.
Aggregate	Aktiviert die Alarmaggregation. Nach der Bestätigung lösen nachfolgende Alarms keinen neuen Alarmzustand mehr aus.
Aggregate and Re-Alarm	Aktiviert die Alarmaggregation, lässt jedoch nachfolgende Alarms einen neuen Alarmzustand auslösen.
Aggregation Maximum Alarms	Konfiguriert die maximale Anzahl an Alarms, die in einer Alarmaggregation enthalten sein können.
Aggregation Timeout	Auswählen, um festzulegen, wie viel Zeit zwischen Alarms vergehen darf, bevor neue Alarms einer neuen Alarmaggregation zugeordnet werden.

Erweiterte Alarmverarbeitung

Einstellung	Beschreibung
Enable advanced alarm processing	Wählen Sie diese Option, um die erweiterte Alarmverarbeitung im Windows Client zu aktivieren. Die erweiterte Alarmverarbeitung ermöglicht es einem Benutzer, einen Alarm zu bestätigen, um den Alarm vor der Bearbeitung zu beanspruchen.
Reason text field is optional for masking hardware nodes	Legt fest, ob beim Maskieren von Hardware-Knoten eine Begründung erforderlich ist. Diese Option ist verfügbar, wenn Sie die erweiterte Alarmverarbeitung aktivieren.

Einstellung	Beschreibung
Require Integration State Change	Wählen Sie diese Option, um zu verlangen, dass sich der Zustand des Hardware-Knotens ändert, bevor Sie den Alarm zurücksetzen können. Diese Option erfordert, dass Sie das Problem mit dem Hardware-Knoten beheben, bevor Sie den Alarm zurücksetzen können. Diese Option ist verfügbar, wenn Sie die erweiterte Alarmverarbeitung aktivieren.
Acknowledgement Timeout	Auswählen, um festzulegen, wie viel Zeit ohne Markierung eines bestätigten Alarms vergehen darf, bevor er in den Zustand „nicht bestätigt“ zurückkehrt.

Audit

Der Bereich Audit in den allgemeinen Einstellungen legt fest, ob der Server Ereignisse protokolliert und wie er Audit-Protokolle archiviert.

Einstellung	Beschreibung
Enable Audit	Aktiviert/deaktiviert die Protokollierung von Ereignissen.
Never archive audit	Verhindert, dass der Server Audits archiviert.
Archive audit weekly	Archiviert Audits wöchentlich.
Audit archive retention	Wie lange (in Tagen) der Server archivierte Audits aufbewahrt.

SNMP

Der SNMP-Bereich in den Allgemeinen Einstellungen konfiguriert den Server, um Telemetriedaten an einen Simple Network Management Protocol (SNMP)-Client zu liefern.

Einstellung	Beschreibung
Enable SNMP	SNMP-Unterstützung aktivieren/deaktivieren.
Data polling rate	Wie oft (in Sekunden) der SNMP-Agent den Server nach Daten abfragt.
Footage size polling rate	Wie oft (in Sekunden) der SNMP-Agent den Server nach der Größe der Videoaufzeichnungen abfragt.

SNMP konfigurieren

Sie können den Server so konfigurieren, dass er SNMP-Daten an einen SNMP-Client sendet.

1. Klicken Sie in der Server-Konfigurationsoberfläche auf Settings > General Settings.
2. Wählen Sie Enable SNMP aus.
3. Legen Sie unter Data polling rate fest, wie oft (in Sekunden) SNMP-Sub-Agents Daten abfragen.
4. Legen Sie unter Footage size polling fest, wie oft (in Sekunden) der Server die Größe der Aufzeichnungen aktualisiert.
5. Klicken Sie auf Save.
6. Starten Sie die Senstar Symphony-Dienste neu.
7. Konfigurieren Sie den Windows SNMP Agent Service auf dem Computer, der den Server hostet.

SNMP-Objektkennungen**Server Information**

Objekt	Beschreibung	Trap
serverId	Eindeutige Kennung des Server.	Nein
serverName	Name des Server.	Nein

Version Information

Objekt	Beschreibung	Trap
serverVersion	Assembly-Version der Server-Software.	Nein
webserviceVersion	Version des Web-Service-Protokolls des Server.	Nein
cameraMessageVersion	Version des Kamera-Nachrichtenprotokolls des Server.	Nein
streamingVersion	Version des Streaming-Protokolls des Server.	Nein

Client Bandwidth

Objekt	Beschreibung	Trap
connectedClientNumber	Anzahl der Windows Client-Instanzen, die mit dem Server verbunden sind.	Nein
connectedClientIndex	Eindeutige Kennung des Windows Client.	Nein
connectedClientIpAddress	IP-Adresse des Windows Client.	Nein
connectedClientUsername	Benutzername, den der Windows Client zur Verbindung mit dem Server verwendet.	Nein
connectedClientDuration	Wie lange der Windows Client mit dem Server verbunden ist.	Nein
connectedClientDataReceived	Wie viele Daten (in Kilobyte) der Windows Client vom Server empfangen hat.	Nein
connectedClientCurrentBandwidth	Datenmenge (in Kilobyte pro Sekunde), die zwischen dem Windows Client und dem Server übertragen wird.	Nein

Camera Information

Objekt	Beschreibung	Trap
cameraNumber	Anzahl der Kameras, die mit dem Server verbunden sind.	Nein
cameraId	Eindeutige Kennung der Kamera.	Nein
cameraName	Name der Kamera.	Nein
footagePath	Speicherpfad für Aufzeichnungen der Kamera.	Nein
footageSize	Größe (in Bytes) der Aufzeichnungen am Speicherpfad.	Nein

Storage Information

Objekt	Beschreibung	Trap
storagePoolNumber	Anzahl der Speicherpools, die mit dem Server verbunden sind.	Nein
storagePath	Der Pfad des Speicherpools.	Nein
storageCapacity	Gesamtkapazität (in Megabyte) des Speicherpools.	Nein
storagePercentAvailable	Verfügbare Kapazität (in Megabyte) des Speicherpools.	Nein
storageFootageSize	Größe (in Megabyte) der Aufzeichnungen im Speicherpool.	Nein
storageFootageFiles	Anzahl der Aufzeichnungsdateien im Speicherpool.	Nein

Service Information

Objekt	Beschreibung	Trap
infoServiceStatus	Status des AI InfoService-Dienstes.	Nein
netSendHistStatus	Status des AI NetSendHist-Dienstes.	Nein
schedulerStatus	Status des AI Scheduler-Dienstes.	Nein
trackNumber	Anzahl der aktiven AI Tracker-Dienste.	Nein
trackerId	Eindeutige Kennung des AI Tracker-Dienstes.	Nein
trackerStatus	Status des AI Tracker-Dienstes.	Nein

Login Monitor Information

Objekt	Beschreibung	Trap
authorizedLoginNotif	Benachrichtigung, die bei erfolgreicher Anmeldung gesendet wird.	Ja
unauthorizedLoginNotif	Benachrichtigung, die bei erfolgloser Anmeldung gesendet wird.	Ja
loginNotifyIpAddress	IP-Adresse des Windows Client.	Nein
loginNotifyUsername	Benutzername, den der Windows Client zur Verbindung mit dem Server verwendet hat.	Nein
loginNotificationMessage	Zusätzliche Details zur Anmeldung.	Nein

Alarm Monitor Information

Objekt	Beschreibung	Trap
alarmNotif	Benachrichtigung, die beim Auftreten eines Alarms gesendet wird.	Ja
alarmNotifyCameraId	Kennung der Kamera, die den Alarm aufgezeichnet hat.	Nein
alarmNotifyCameraName	Name der Kamera, die den Alarm aufgezeichnet hat.	Nein

Objekt	Beschreibung	Trap
<code>alarmNotifyUserId</code>	Kennung des Benutzers, der den Alarm markiert hat.	Nein
<code>alarmNotifyUserName</code>	Name des Benutzers, der den Alarm markiert hat.	Nein
<code>alarmNotifyMarkedDelay</code>	Zeit, zu der der Alarm markiert wurde.	Nein
<code>alarmNotifyFalseAlarm</code>	Ist der Alarm ein Fehlalarm.	Nein
<code>alarmNotifyRuleId</code>	Kennung der Regel, die den Alarm verursacht.	Nein
<code>alarmNotifyRuleName</code>	Name der Regel, die den Alarm verursacht.	Nein
<code>alarmNotifyDBId</code>	Kennung des Alarms.	Nein
<code>alarmNotifyComment</code>	Kommentar zu diesem Alarm.	Nein
<code>alarmNotifyMSSinceChange</code>	Anzahl der Millisekunden zwischen dem Auftreten des Alarms und seiner Erkennung.	Nein

Device Movement Monitor Information

Objekt	Beschreibung	Trap
<code>devicesMovedNotif</code>	Benachrichtigung, die gesendet wird, wenn ein Gerät von einem Server auf einen anderen Server verschoben wird.	Ja
<code>sourceServerId</code>	Kennung des Servers, von dem das Gerät verschoben wurde.	Nein
<code>destinationServerId</code>	Kennung des Servers, auf den das Gerät verschoben wurde.	Nein
<code>numberDevicesMoved</code>	Anzahl der Geräte, die vom Quellserver auf den Zielservers verschoben wurden.	Nein

Health Monitor Information

Objekt	Beschreibung	Trap
<code>healthMonitorFaultNotification</code>	Benachrichtigung, die gesendet wird, wenn der Health Monitor einen Fehler erkennt.	Ja
<code>healthMonitorActionNotification</code>	Benachrichtigung, die gesendet wird, wenn der Health Monitor als Reaktion auf einen Fehler eine Aktion ausführt.	Ja
<code>healthMonitorName</code>	Name des zugehörigen Health Monitors.	Nein
<code>healthMonitorAction</code>	Die Aktion, die der Health Monitor als Reaktion auf einen Fehler ausgeführt hat.	Nein

Web Client

Der Bereich Web Client in den Allgemeinen Einstellungen konfiguriert Lastverteilung, Aktualisierungsrate (wie oft der Client Updates vom Server erhält) und ICE-Server-Einstellungen für den Web Client.

Einstellung	Beschreibung
Randomly redirect master server logins to other available servers in the farm	Konfiguriert, ob der Master-Server Benutzer an andere Server in der Serverfarm umleitet. Dies bietet Lastverteilung für den Web Client.
Refresh rate	Wie oft der Web Client Informationen vom Server aktualisiert.
Use an ICE Server	Wählen Sie aus, ob Sie einen Interactive Connectivity Establishment (ICE)-Server mit dem Web Client verwenden.
Type	Der Typ des verwendeten ICE-Servers, STUN oder TURN. Diese Einstellung ist verfügbar, wenn Sie "Use an ICE Server" auswählen.
URL	URL des ICE-Servers. Diese Einstellung ist nur verfügbar, wenn Sie "Use an ICE Server" auswählen.
Username	Benutzername für den ICE-Server. Diese Einstellung ist nur verfügbar, wenn Sie "Use an ICE Server" auswählen.
Password	Kennwort für den ICE-Server. Diese Einstellung ist verfügbar, wenn Sie "Use an ICE Server" auswählen.

SMTP

Der SMTP-Bereich in den Allgemeinen Einstellungen konfiguriert den E-Mail-Server, den der Server zum Versenden von E-Mail-Benachrichtigungen verwendet.

Einstellung	Beschreibung
SMTP server	URL des SMTP-Servers.
Use Secure Sockets Layer	SSL für die Kommunikation mit dem SMTP-Server verwenden.
Sender email account	Definiert das E-Mail-Konto, das der Server zum Versenden von E-Mails verwendet.
SMTP server requires authentication	Konfiguriert, ob der SMTP-Server eine Authentifizierung erfordert.
Username	Benutzername, den der Server zur Authentifizierung am SMTP-Server verwendet. Diese Einstellung ist nur verfügbar, wenn Sie "SMTP server requires authentication" auswählen.
Password	Kennwort, das der Server zur Authentifizierung am SMTP-Server verwendet. Diese Einstellung ist nur verfügbar, wenn Sie "SMTP server requires authentication" auswählen.
Send a test email to address	Verwenden Sie dieses Feld, um die SMTP-Einstellungen zu testen. Geben Sie eine E-Mail-Adresse ein und klicken Sie auf Send Test, um eine Test-E-Mail zu senden.

Benutzerverbindungen

Der Bereich User Connections in den Allgemeinen Einstellungen schränkt gleichzeitige Anmeldungen und inaktive Sitzungen an der Server-Konfigurationsoberfläche ein.

Einstellung	Beschreibung
Do not allow more than one concurrent connection per user	Konfiguriert, ob sich Benutzer pro Serverfarm gleichzeitig an mehr als einer Server-Konfigurationsoberfläche anmelden können.
Automatically log out inactive Server Configuration users	Konfiguriert, ob der Server Benutzer nach einer Zeit der Inaktivität automatisch von der Server-Konfigurationsoberfläche abmeldet.

Einstellung	Beschreibung
Minutes of Inactivity	Die Timeout-Periode für die Server-Konfigurationsoberfläche.

Standort der Serverfarm

Der Abschnitt Farm Location in General Settings legt die GPS-Koordinaten der Server-Serverfarm fest.

Einstellung	Beschreibung
GPS Latitude	Breitengrad der Server-Serverfarm.
GPS Longitude	Längengrad der Server-Serverfarm.

Mobile Verbindungen

Im Abschnitt Mobile Connections in General Settings werden Push-Benachrichtigungen für iOS-Geräte (z. B. iPhone) aktiviert.

Einstellung	Beschreibung
Enable iOS Notifications	Push-Benachrichtigungen für iOS-Geräte aktivieren/deaktivieren.



Server-spezifische Einstellungen für mobile Verbindungen (Mobilport, Videoproxyport und SSL-Zertifikat) werden unter [Einstellungen > Server](#) konfiguriert. Siehe [Mobile Verbindungen konfigurieren](#) und [SSL-Zertifikat hinzufügen](#).

Cloud-Dienste

Die Registerkarte Cloud Services in der Konfigurationsoberfläche des Server ist die Schnittstelle zur Konfiguration von Cloud-Diensten, die zusätzliche Funktionen für die Serverfarm bereitstellen.

Health Monitoring

Wenn Sie die Option Maintenance and Support erworben haben, können Sie Health Monitoring aktivieren. Health Monitoring sendet Telemetriedaten vom Server an das Senstar Xnet. Sie können sich am Senstar Xnet anmelden und den Status aller Server anzeigen.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Cloud Services.
2. Stellen Sie im Abschnitt Health Monitoring den Schalter Send Packets to Senstar XNet auf On.

Um Health Monitoring zu deaktivieren, stellen Sie den Schalter Send Packets to Senstar XNet auf Off.

Senstar Enterprise Manager

Sie können den Server oder die Farm mit dem Senstar Enterprise Manager verwalten.



Wenn Sie Benutzer oder Gruppen erstellt haben, werden diese Benutzer und Gruppen durch die Benutzer aus dem Senstar Enterprise Manager ersetzt, sobald Sie den Server zum Senstar Enterprise Manager hinzufügen. Dies schließt Administratorbenutzer ein. Senstar empfiehlt, Ihre Konfigurationseinstellungen oder Datenbank zu sichern, bevor Sie Ihren Server oder Ihre Serverfarm mit dem Senstar Enterprise Manager verwalten.

1. Klicken Sie auf Settings > Cloud Services.

2. Stellen Sie im Abschnitt Enterprise Manager den Schalter Current State auf On.
3. Geben Sie im Feld Address die IP-Adresse des Senstar Enterprise Manager ein.
4. Geben Sie im Feld Site Name einen Namen für den Standort ein. Der Senstar Enterprise Manager verwendet diesen Standortnamen, um den Server oder die Serverfarm zu identifizieren.
5. Geben Sie im Feld Organization Name den Organisationsnamen für den Senstar Enterprise Manager ein.
6. Geben Sie im Feld Passphrase das Kennwort für den Senstar Enterprise Manager ein.
7. Klicken Sie auf Save.

Cloud Proxy

Sie können den Server mit der Senstar Cloud verbinden, um die Authentifizierung und die Kommunikation zwischen dem Server und mobilen Geräten zu erleichtern. Konfigurieren Sie zuvor die Senstar Cloud und beziehen Sie den API-Schlüssel.

1. Klicken Sie auf Settings > Cloud Services.
2. Klicken Sie auf den Schalter Enable Cloud Proxy heartbeat, um den Heartbeat zu aktivieren.
3. Geben Sie im Feld Cloud Proxy API key den API-Schlüssel aus der Senstar Cloud ein.
4. Klicken Sie auf Save.

Nachdem Sie den Server mit der Senstar Cloud verbunden haben, können Sie sich an der Senstar Cloud anmelden, um zu bestätigen, dass die Verbindung aktiv ist.

Summen

Eine Summe ist eine Sammlung von Kameras, die die Personenzählungen aller Kameras kombinieren und diese Informationen auf einer HTML-Seite darstellen kann. Sie können Summen verwenden, um umfassende Belegungszahlen und Anweisungen für Kunden bereitzustellen.



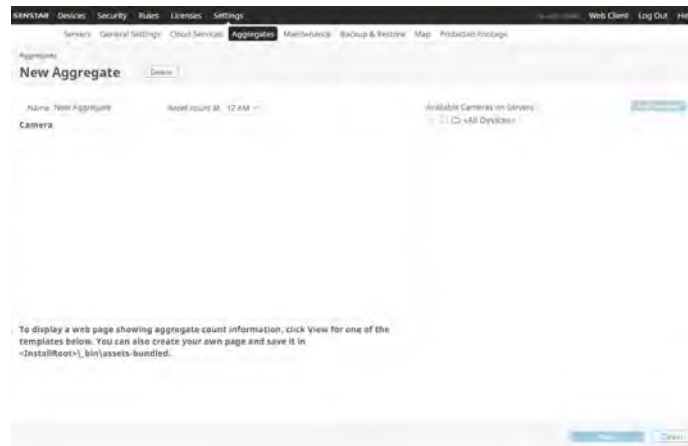
Summen verwalten

Sie können Summen erstellen, ändern, kopieren und löschen und die HTML-Seite des aggregierten Personenzählers anpassen.

Summe erstellen

Konfigurieren Sie die Videoanalyse des aggregierten Personenzählers in der Konfigurationsoberfläche des Server.

Eine Kamera muss die Videoanalyse Indoor People Tracking ausführen, um in der Liste Available Cameras on Servers sichtbar zu sein.



1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Aggregates.
2. Klicken Sie auf Add Aggregate.
3. Geben Sie im Feld Name einen aussagekräftigen Namen für die Summenzählung ein.
4. Wählen Sie in der Liste Reset count at die Stunde aus, zu der die Summenzählung auf null zurückgesetzt wird. Die Liste enthält die 24 Stunden des Tages (12 AM bis 11 PM). Das tägliche Zurücksetzen der Zählung trägt zur Aufrechterhaltung der Genauigkeit bei.
5. Erweitern Sie in der Baumstruktur Available Cameras on Servers den Gerätebaum, wählen Sie die Kameras aus, die Sie in die Summenzählung einbeziehen möchten, und klicken Sie auf Add Selected. Die ausgewählten Kameras werden in der Liste Camera angezeigt. Nur Kameras, die die Videoanalyse Indoor People Tracking ausführen, sind verfügbar.
6. (Optional) Um eine Kamera aus der Summe zu entfernen, wählen Sie sie in der Liste Camera aus und klicken Sie auf die Schaltfläche X daneben.
7. (Optional) Klicken Sie in der Vorlagenliste unter der Liste Camera auf View neben einer Vorlage (z. B. Aggregate-en), um die HTML-Seite zu betrachten, die der Server zur Anzeige der Summenzählung verwendet. Sie können Ihre eigene Seite erstellen und unter `<InstallRoot>\_bin\assets-bundled` speichern, um sie als Vorlage verfügbar zu machen.
8. Klicken Sie auf Save.

Nachdem Sie eine Summe hinzugefügt haben, erstellt der Server eine HTML-Seite, mit der Sie Belegungsinformationen und Anweisungen anzeigen können. Um die HTML-Seite zu öffnen, klicken Sie auf den Link unten auf der Seite Aggregates.

Summe ändern

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Aggregates.
2. Wählen Sie die Summe aus und klicken Sie auf Edit.
3. Führen Sie eine der folgenden Aufgaben aus:
 - a. Um den Namen der Summe zu ändern, geben Sie im Feld Name einen neuen Namen ein.
 - b. Um die Rücksetzzeit zu ändern, wählen Sie einen neuen Wert in der Liste Reset count at aus.
 - c. Um eine Kamera zur Summe hinzuzufügen, wählen Sie die Kamera in der Liste Available Cameras on Servers aus und klicken Sie auf Add Selected.
 - d. Um eine Kamera aus der Summe zu entfernen, markieren Sie die Kamera in der Liste Camera

und klicken Sie auf die Schaltfläche X.

4. Klicken Sie auf Save.

Summe kopieren

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Aggregates.
2. Wählen Sie die Summe aus und klicken Sie auf Clone.
3. Ändern Sie die Summe.
4. Klicken Sie auf Save.

Summe löschen

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Aggregates.
2. Wählen Sie die Summe aus und klicken Sie auf Delete.

HTML des aggregierten Personenzählers ändern

Sie können die HTML-Seite ändern, die die Videoanalyse des aggregierten Personenzählers zur Anzeige von Belegungszählungen und Anweisungen für Kunden verwendet.

Sie können auch eine vorhandene HTML-Datei kopieren, um mehrere HTML-Dateien zu erstellen, die unterschiedliche Belegungszählungen und Anweisungen für andere Summen oder Situationen anzeigen.

1. Navigieren Sie auf dem Computer, der den Server hostet, zu `_bin\assets-bundled`.
2. Öffnen Sie die HTML-Datei (z. B. `Aggregate-en.html`) mit einem Texteditor.
3. Um die Belegungsschwellenwerte zu ändern, ändern Sie den folgenden Code:

```
var thresholdYellow = 50;
var thresholdRed = 75;
```

1. Um die Meldungen zu ändern, ändern Sie den folgenden Code:

```
function showGreen(difference) {
    document.getElementById("message").innerHTML = "LIMITED STORE<br />CAPACITY";
    document.getElementById("instructions").innerHTML = "PLEASE PROCEED WITH
CAUTION";
```

```
function showYellow(difference) {
    document.getElementById("message").innerHTML = "LIMITED STORE<br />CAPACITY";
    document.getElementById("instructions").innerHTML = "PLEASE MAINTAIN SOCIAL
DISTANCING";
```

```
function showRed(difference) {
    document.getElementById("message").innerHTML = "MAXIMUM<br />CAPACITY";
    document.getElementById("instructions").innerHTML = "PLEASE WAIT FOR
ASSISTANCE";
```

```
<div style="padding-top: 2vw; font-size: 1.5vw; ">CURRENT NUMBER<br />OF PEOPLE</div>
```

```
<div style="padding-top: 2vw; font-size: 1.5vw; ">MAXIMUM NUMBER<br />OF PEOPLE  
ALLOWED</div>
```

1. Speichern und schließen Sie die HTML-Datei.

Summe suchen

Um eine bestimmte Summe schnell zu finden, verwenden Sie Filter und Sortierung.

Filtern

Sie können die Liste der Summen mit dem folgenden Filter filtern:

- Name der Summe (Name)
 1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Aggregates.
 2. Klicken Sie auf die Lupe, um die Filtertextfelder anzuzeigen.
 3. Definieren Sie die Filterkriterien.
 4. Klicken Sie auf Apply filter.

Sortieren

Sie können die Liste der Summen sortieren, indem Sie auf den Spaltennamen klicken. Das Klicken auf den Spaltennamen wechselt zwischen aufsteigender und absteigender Reihenfolge.

Zurücksetzen

Um den Filter zurückzusetzen und die Liste der Summen wiederherzustellen, klicken Sie auf Clear Filter.

Wartung

Auf der Registerkarte Maintenance in der Konfigurationsoberfläche des Server wird konfiguriert, wann der Windows Client Software-Updates anwendet und wann der Server Updates herunterlädt und installiert.

Client-Updates

Der Abschnitt Client Updates legt fest, wann mit dieser Serverfarm verbundene Windows Client-Instanzen Software-Updates anwenden.

Einstellung	Beschreibung
Immediately	Aktualisieren Sie den Windows Client, sobald ein Update verfügbar ist.
During time frame	Aktualisieren Sie den Windows Client nur zwischen den Zeiten Begin und End.
Never	Verhindern Sie automatische Updates für den Windows Client.

Server-Updates

Der Abschnitt Server Updates zeigt an, wann der Server zuletzt nach Updates gesucht hat, ermöglicht

eine manuelle Prüfung und konfiguriert automatische Updates.

Einstellung	Beschreibung
Last check for updates	Datum und Uhrzeit der letzten Update-Prüfung oder Never, wenn keine Prüfung durchgeführt wurde.
Check for Updates	Manuelle Prüfung auf verfügbare Updates. Diese Option ist nur für eigenständige Serverfarmen (mit einem einzelnen Server) verfügbar.
Enable automatic updates	Ob der Server Updates automatisch herunterlädt und installiert.
Automatically download and install at	Die Tageszeit, zu der Updates heruntergeladen und installiert werden.
Update from the following location	Verwenden Sie einen lokalen Dateipfad als Update-Quelle.
Update from product web site	Verwenden Sie die Senstar-Produktwebsite als Update-Quelle. Diese Einstellung ist verfügbar, wenn Sie Enable automatic updates auswählen.



Wenn automatische Updates mit installierten Komponenten (z. B. Gesichtserkennung) inkompatibel sind, werden diese Komponenten auf der Seite aufgeführt und Sie müssen sie manuell aktualisieren, bevor automatische Updates ausgeführt werden können.

Backup & Wiederherstellen

Die Registerkarte Backup & Restore in der Konfigurationsoberfläche des Server ist die Schnittstelle zum Sichern und Wiederherstellen von Server-Konfigurationen.

Sie können Konfigurationen verwenden, um Einstellungen zwischen verschiedenen Server-Instanzen zu übertragen oder einen vorhandenen Server wiederherzustellen.

Wenn Sie eine Server-Farm betreiben, wird dringend empfohlen, die Sicherungen an einem Ort zu speichern, der sich nicht auf einem der Server in der Farm befindet, aber für alle Server in der Farm zugänglich ist (z. B. ein NAS). Dies erleichtert die Wiederherstellung von Servern in Notfallwiederherstellungssituationen. Wenn Sie eine Maintenance & Support-Lizenz besitzen, können Sie Sicherungen zusätzlich online im Senstar Xnet speichern.

Der Server unterstützt nicht das Wiederherstellen einer Konfiguration aus einer früheren Version des Server.

Backups konfigurieren

Was es ist

Ein Backup des Server ist eine Momentaufnahme der Serverkonfiguration — Standortlayout, Geräte, Regeln, Ereignisse, Aktionssätze, Zeitpläne, Benutzer, Gruppen, Sicherheitsprofile, Lizenzen und allgemeine Einstellungen. Es enthält **keine** aufgezeichneten Videos. Aufgezeichnete Videos befinden sich unter den Videospeicherpfaden und werden gemäß der Aufbewahrungsrichtlinie jeder Kamera aufbewahrt; siehe [Videospeicher für eine Kamera](#).

Sie können Backups lokal speichern (an einem Pfad auf dem Server oder einer eingebundenen Freigabe) und mit einer Maintenance & Support-Lizenz auch im Senstar Xnet zur externen Wiederherstellung.

Wann Sie es verwenden

- **Wiederherstellung nach Hardwareausfall** — Wiederherstellung der Konfiguration auf Ersatzhardware, anstatt sie manuell neu aufzubauen.
- **Änderung rückgängig machen** — Rücknahme einer fehlerhaften Regel, eines Sicherheitsprofils oder einer Integrationsänderung.
- **Migrieren** — Übertragen einer Konfiguration auf einen neuen Server.
- **Einhaltung der Backup-Richtlinie Ihrer Organisation** — Einbeziehung des Server in nächtliche oder wöchentliche Backups.

Voraussetzungen

- Berechtigung zur Bearbeitung von Einstellungen des Server.
- Ein beschreibbarer Pfad für lokale Backups (ein lokales Laufwerk, ein angeschlossenes Volume oder eine eingebundene Netzwerkfreigabe mit Anmeldedaten, die das Dienstkonto des Server verwenden kann).
- Für Online-Backup eine Maintenance & Support-Lizenz und Internetzugang vom Server zum Senstar Xnet.

Wie häufig auszuführen

Der Standardzeitplan ist ein einzelnes tägliches Backup um 23:00 Uhr Serverzeit. Die meisten Standorte behalten den täglichen Rhythmus bei und ändern nur die Uhrzeit, sodass das Backup außerhalb der Hauptaufzeichnungszeiten ausgeführt wird. Bei Standorten, an denen die Konfiguration häufig geändert wird (neue Kameras, häufige Regelanpassungen), sollten Sie das nächtliche Backup mit einem manuellen **Back up now** vor und nach wesentlichen Änderungen kombinieren.

Vorgehen

Backup Configuration

Backup configuration daily at
10:58 pm

Local backup path
D:\Data_backups

Last local backup: Yesterday at 10:57 PM
☐ Protect Backups with a Password

Password for the Backup

Confirm Backup Password

Enable online backup ☒ ON
Last online backup: Yesterday at 10:57 PM

Back up now Test configuration

1. Klicken Sie in der Konfigurationsoberfläche des Server auf **Settings > Backup & Restore**.
2. Stellen Sie im Feld **Backup configuration daily at** die Uhrzeit ein, zu der der Server das Backup

erstellt. Wählen Sie eine Uhrzeit, zu der der Server nicht stark ausgelastet ist.

3. Stellen Sie im Feld **Local backup path** den Pfad ein, in den der Server das Backup schreibt. Verwenden Sie ein Volume oder eine Freigabe, die als Teil Ihrer übergeordneten IT-Backup-Richtlinie gesichert wird — ein Backup, das nur auf dem Server liegt, übersteht keinen Festplattenausfall.

4. Um die Backup-Datei mit einem Kennwort zu verschlüsseln, gehen Sie wie folgt vor:
 - a. Wählen Sie **Protect Backups with a Password** aus.
 - b. Geben Sie das Kennwort in **Password for the Backup** ein. Das Kennwort muss die für den Server konfigurierten Komplexitätsanforderungen erfüllen.
 - c. Geben Sie das Kennwort in **Confirm Backup Password** erneut ein.

Speichern Sie das Kennwort im Kennwortmanager Ihrer Organisation. Ohne das Kennwort kann das Backup nicht wiederhergestellt werden.

5. Um Backups zusätzlich in das Senstar Xnet hochzuladen, aktivieren Sie **Enable online backup**.



Online-Backup erfordert eine Maintenance & Support-Lizenz.

6. Klicken Sie auf **Test configuration**, um zu bestätigen, dass der Pfad beschreibbar ist und, falls Online-Backup aktiviert ist, dass der Server das Senstar Xnet erreichen kann.
7. Klicken Sie auf **Back up now**, um sofort ein Backup zu erstellen.

Verwandte Aufgaben

- Aus einem lokalen Backup wiederherstellen
- Aus einem Online-Backup wiederherstellen
- Aus Datei wiederherstellen

Aus lokalem Backup wiederherstellen

Sie können die Konfigurationseinstellungen für den Server aus dem lokalen Backup-Pfad wiederherstellen.

1. Klicken Sie in der Server-Konfigurationsoberfläche auf Settings > Backup & Restore.
2. Um die Konfigurationseinstellungen von einem Server wiederherzustellen, der nicht Teil der Serverfarm ist, wählen Sie Restore backup from different hardware, excluding license.
3. Klicken Sie auf die Registerkarte Restore local backup.
4. Um kompatible Backup-Dateien im lokalen Pfad anzuzeigen, wählen Sie Show only compatible versions.
5. Wählen Sie die Backup-Datei aus.
6. Klicken Sie auf Restore.

Aus Online-Backup wiederherstellen

Sie können die Konfigurationseinstellungen für einen Server aus dem Senstar Xnet wiederherstellen.



Diese Funktion erfordert eine Maintenance & Support-Lizenz.

1. Klicken Sie in der Server-Konfigurationsoberfläche auf Settings > Backup & Restore.
2. Klicken Sie auf Restore online backup.
3. Um kompatible Backup-Dateien im lokalen Pfad anzuzeigen, wählen Sie Show only compatible versions.
4. Wählen Sie die Backup-Datei aus.
5. Klicken Sie auf Restore.

Aus Datei wiederherstellen

Sie können die Konfigurationseinstellungen für einen Server aus einer Datei wiederherstellen.

1. Klicken Sie in der Server-Konfigurationsoberfläche auf Settings > Backup & Restore.
2. Um die Konfigurationseinstellungen von einem Server wiederherzustellen, der nicht Teil der Serverfarm ist, wählen Sie Restore backup from different hardware, excluding license.
3. Klicken Sie auf Restore from file.
4. Ziehen Sie die Datei in die Oberfläche oder navigieren Sie zur Backup-Datei.
5. Klicken Sie auf Restore.

Lageplan

Mit den Lageplaneinstellungen können Sie die auf einem Lageplan platzierten Symbole an die spezifisch eingesetzten Geräte anpassen und die Farben anpassen, die zur Darstellung von Gerätezuständen wie Alarm, Supervision, Mask, Fault, Warning und Normal verwendet werden.

Lageplansymbole

Verwenden Sie die Einstellungen Map Icons, um das Symbol auszuwählen, das jeden Gerätetyp auf einem Lageplan darstellt. Wählen Sie für jeden Gerätetyp ein Symbol aus der Liste aus, das zu den eingesetzten Geräten passt.

Map Icons

Fixed Camera		Fixed
PTZ Camera		PTZ
Controller		Flexzone_1
Closed Door		Door_Closed
Open Door		Door_Open
Input (Activated)		Input_Activated
Input (Deactivated)		DIO_Input_1

Lageplan-Statusfarben

Verwenden Sie die Einstellungen Map State Colors, um die Farbe zu ändern, die jeden Geräte-Zustand auf einem Lageplan darstellt. Klicken Sie auf das Farbfeld neben einem **Zustand**, um eine neue Farbe auszuwählen, oder klicken Sie auf Reset Color, um die Standardfarbe wiederherzustellen.

Map State Colors

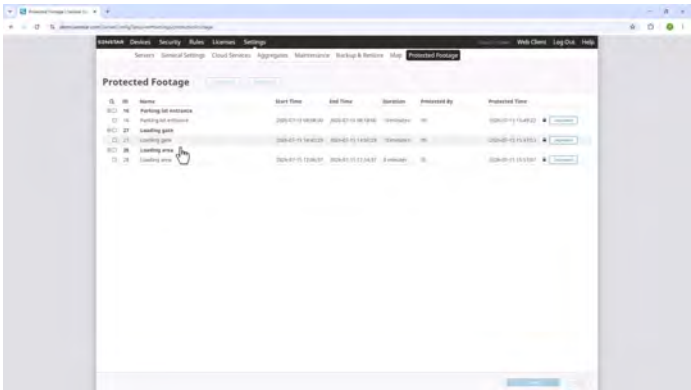
Supervision		Reset Color
Mask		Reset Color
Alarm		Reset Color
Fault		Reset Color
Warning		Reset Color
Normal		Reset Color

Geschützte Aufnahmen

Geschützte Aufnahmen sind aufgezeichnetes Video, das ein Benutzer geschützt hat, damit der Server es nicht löscht. Der Server schließt geschützte Aufnahmen von der automatischen Speicherbereinigung und den Aufbewahrungseinstellungen aus. Geschützte Aufnahmen verbleiben auf dem Server, bis ein Benutzer den Schutz aufhebt.

Benutzer schützen Aufnahmen über die Kamerazeitleiste in der Oberfläche des Windows Client. Weitere Informationen finden Sie unter [Aufnahmen schützen](#). Informationen zum Aufheben oder Wiederherstellen des Schutzes finden Sie unter [Aufnahmenschutz aufheben](#).

Die Seite Protected Footage listet jeden geschützten Abschnitt auf dem Server auf, gruppiert nach Kamera. Um die Seite Protected Footage anzuzeigen, klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Protected Footage.



Spalte	Beschreibung
ID	Die Kennung der Kamera.
Name	Der Name der Kamera.
Start Time	Der Beginn des geschützten Zeitbereichs.

Spalte	Beschreibung
End Time	Das Ende des geschützten Zeitbereichs.
Duration	Die Länge des geschützten Zeitbereichs.
Protected By	Der Benutzer, der die Aufnahmen geschützt hat.
Protected Time	Der Zeitpunkt, zu dem der Benutzer die Aufnahmen geschützt hat.

Die Spalten Protected By und Protected Time bieten einen Prüfpfad für geschützte Aufnahmen. Verwenden Sie zur Unterstützung des Prüfpfads individuelle Benutzerkonten anstelle gemeinsam genutzter Anmeldungen.

Da der Server geschützte Aufnahmen von der automatischen Speicherbereinigung ausschließt, können sich geschützte Aufnahmen ansammeln und den Videospeicher füllen. Der Server kann eine Warnung und einen Alarm auslösen, wenn geschützte Aufnahmen einen konfigurierten Prozentsatz des Videospeichers erreichen. Weitere Informationen finden Sie unter [Speicher](#).

Das Schützen von Aufnahmen und das Aufheben des Schutzes sind separate Berechtigungen. Sie können Bedienern erlauben, Aufnahmen zu schützen, und das Aufheben des Schutzes Administratoren vorbehalten. Weitere Informationen finden Sie unter [Geräteberechtigungen](#).

Aufnahmenschutz aufheben

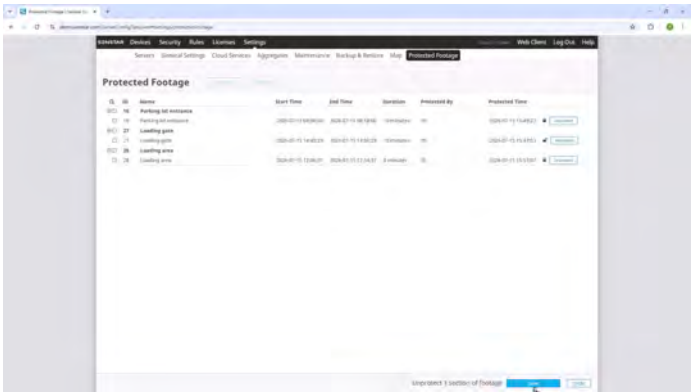
Sie können den Schutz von Aufnahmen aufheben, damit der Server seine normalen Aufbewahrungseinstellungen auf das Videomaterial anwendet. Sobald Sie den Schutz aufheben, kann die automatische Speicherbereinigung das Videomaterial löschen. Weitere Informationen zu den Aufbewahrungseinstellungen finden Sie unter [Speicher](#).

Benutzer schützen Aufnahmen über die Kamerazeitleiste in der Oberfläche des Windows Client. Weitere Informationen finden Sie unter [Aufnahmen schützen](#).

Überprüfen Sie die Seite Protected Footage regelmäßig und heben Sie den Schutz von Aufnahmen auf, die Sie nicht mehr benötigen, damit der Server den Speicherplatz freigeben kann. Die Schaltflächen Unprotect und Reprotect sind nur verfügbar, wenn Ihre Gruppe über die Berechtigung Unprotect Footage verfügt. Weitere Informationen finden Sie unter [Geräteberechtigungen](#).

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Settings > Protected Footage.
2. Führen Sie eine der folgenden Aufgaben aus:
 - Um den Schutz eines Abschnitts aufzuheben, klicken Sie in der Zeile dieses Abschnitts auf Unprotect.
 - Um den Schutz mehrerer Abschnitte aufzuheben, aktivieren Sie das Kontrollkästchen für jeden Abschnitt und klicken Sie oben in der Liste auf Unprotect.
3. Klicken Sie auf Save.

Der Server zeigt die ausstehende Änderung unten auf der Seite an (zum Beispiel Unprotect 1 section of footage). Bevor Sie auf Save klicken, können Sie in einer Zeile auf Reprotect klicken, um die Änderung für diesen Abschnitt abubrechen, oder auf Undo klicken, um alle ausstehenden Änderungen zu verwerfen.



Serververwaltung

Der Server führt die folgenden Dienste aus.

Dienst	Funktion
AI Authentication Service	- Führt die Single-Sign-On-Authentifizierung durch - Protokolldateipräfix: - SSO
AI AxisPACSListenerService	- Kommuniziert mit Axis-Zugangskontrollgeräten - Optionaler Dienst/Manuelle Installation - Protokolldateipräfix: - aac1
AI DataAccessService	- Kommuniziert mit der Senstar Symphony-Datenbank - Protokolldateipräfix: - da
AI Enterprise Management Service	- Kommuniziert mit dem Senstar Enterprise Manager - Aktualisiert die Server-Software automatisch, wenn Konfigurationsänderungen über den Senstar Enterprise Manager vorgenommen werden - Protokolldateipräfix: - fs
AI InfoService	- Hostet den Senstar Symphony-Web-Service, der alle Anfragen vom Windows Client empfängt - Hostet den Webserver für die Server-Konfigurationsoberfläche - Ruft Zeitleistendaten aus dem Aufzeichnungsspeicher ab - Protokolldateipräfixe: - is (information service) - isac (access control) - isbk (automatic backup)

Dienst	Funktion
AI Mobile Bridge	• Ermöglicht die Kommunikation zwischen Mobilgeräten und dem Server • Ermöglicht die Kommunikation zwischen dem Senstar Thin Client und dem Server • Protokolldateipräfix: ◦ mo
AI NetSendHist	• Ruft historisches Video aus dem Aufzeichnungsspeicher ab • Streamt Video • Erstellt historische Bilder • Protokolldateipräfix: ◦ hs
AI OPCServer	• Kommuniziert mit dem OPC-Server • Optionaler Dienst/Manuelle Installation • Protokolldateipräfix: ◦ op
AI Scheduler	• Fragt Hardware-Alarমেingänge ab • Generiert Alarमे • Generiert Berichte • Entfernt abgelaufene Videodateien • Ruft Suchergebnisse (Video und XML) vom NAS ab • Protokolldateipräfixe: ◦ sc (scheduler) ◦ scac (actions) ◦ scax (access) ◦ scc1 (cleaner) ◦ sccp (CPU/memory) ◦ scis (multicaster) ◦ scpm (PTZ) ◦ scse (searches)
AI SNMP Registry	• Registriert Sub-Agents
AI Tracker	• Analysiert Video • Speichert Video im Speicher • Protokolldateipräfix: ◦ cs Der Server erstellt eine Instanz des AI Tracker-Dienstes für jede Kamera. Die Namen der AI Tracker-Dienstinstanzen enthalten die ID der Kamera.

Dienst	Funktion
AI Watchdog	- Überwacht und startet Senstar Symphony-Dienste - Protokolldateipräfixe: - hm (health monitoring) - nu (health monitor)

CPU-Auslastung prüfen

Sie können den Befehl **ShowCPUUsage** verwenden, um die CPU-Auslastung auf dem Computer zu prüfen, der den Server hostet.

Der Befehl **ShowCPUUsage** zeigt die CPU-Auslastung als Prozentsatz der Kapazität eines einzelnen Kerns an. Wenn der Computer beispielsweise vier Kerne hat und der Server 30 % jedes Kerns nutzt, beträgt das Ergebnis 120.



Vor Senstar Symphony 8.5 konnten Sie die CPU-Auslastung mit dem Befehl **KillAll 8** prüfen.

- Führen Sie auf dem Computer, der den Server hostet, eine Eingabeaufforderung als Administrator aus.
- Geben Sie in der Eingabeaufforderung `ShowCPUUsage` ein und drücken Sie die Eingabetaste.

Dienste verwalten

Sie können den Befehl **KillAll** verwenden, um Senstar Symphony-Dienste zu stoppen, zu starten und neu zu starten.

Die folgenden Parameter werden mit dem Befehl **KillAll** verwendet, um die Senstar Symphony-Dienste zu verwalten.

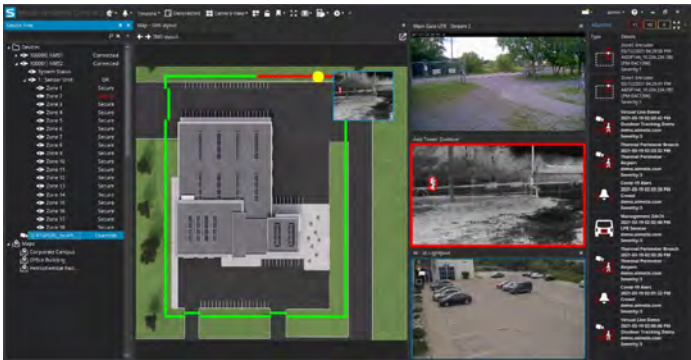
Parameter	Beschreibung
1	Senstar Symphony-Dienste ordnungsgemäß stoppen.
2	Senstar Symphony-Dienste beenden.
4	Senstar Symphony-Dienste nur bei Bedarf beenden (ausgenommen den AI InfoService-Dienst).
5	Senstar Symphony-Dienste ordnungsgemäß starten (ausgenommen den AI InfoService-Dienst).
6 pid	Den Senstar Symphony-Dienst mit der Prozess-ID gleich pid beenden.
7	Den AI InfoService-Dienst neu starten.
9	Senstar Symphony-Dienste nur bei Bedarf beenden (einschließlich des AI InfoService-Dienstes).
a	Senstar Symphony-Dienste starten.
d	Alle Senstar Symphony-Dienste deaktivieren.
e	Alle Senstar Symphony-Dienste aktivieren. Der AI Tracker-Dienst wird auf manuell gesetzt und alle anderen Senstar Symphony-Dienste werden auf automatisch gesetzt.

Parameter	Beschreibung
r	Senstar Symphony-Dienste nur bei Bedarf beenden (einschließlich des AI InfoService-Dienstes) und Senstar Symphony-Dienste ordnungsgemäß starten (ausgenommen den AI InfoService-Dienst).
s	Die Senstar Symphony-Dienste der Reihe nach neu starten.
t tracker_id	Den AI Tracker-Dienst mit der ID gleich tracker_id neu starten.
x	Senstar Symphony-Dienste nur bei Bedarf beenden (einschließlich des AI InfoService-Dienstes) und alle Instanzen des Windows Client stoppen, die auf dem Computer ausgeführt werden.

1. Führen Sie auf dem Computer, der den Server hostet, eine Eingabeaufforderung als Administrator aus.
2. Geben Sie in der Eingabeaufforderung `KillAll` `parameter` ein und drücken Sie die Eingabetaste.
Wobei *parameter* die Zahl oder der Buchstabe ist, der die spezifische Funktion des Befehls **KillAll** definiert.

Windows Client

Der Windows Client ist eine Anwendung, mit der Operatoren Kameras und Alarmer überwachen, während Administratoren den Client zur Videoverwaltung, zum Erstellen von Berichten und zur Konfiguration der Alarmanzeige nutzen können. Er wird automatisch zusammen mit dem Server installiert, kann aber auch separat auf Arbeitsstationen installiert werden. Da Senstar Symphony pro Kamera bzw. Gerät lizenziert wird, können Sie den Windows Client auf beliebig vielen Rechnern installieren.



Erste Schritte

Aktion	Thema
Grundlagen kennenlernen	User Interface (EN)
Mit einem Symphony-Server verbinden	Connect to a Server (EN)
Videostream einer Kamera ansehen	Viewing a Camera's Video Stream (EN)
Alarmer überwachen und beantworten	Managing Alarms (EN)
Aufgezeichnetes Video als Datei speichern	Exporting Video (EN)
Layout und Erscheinungsbild des Clients anpassen	Interface Customizations (EN)

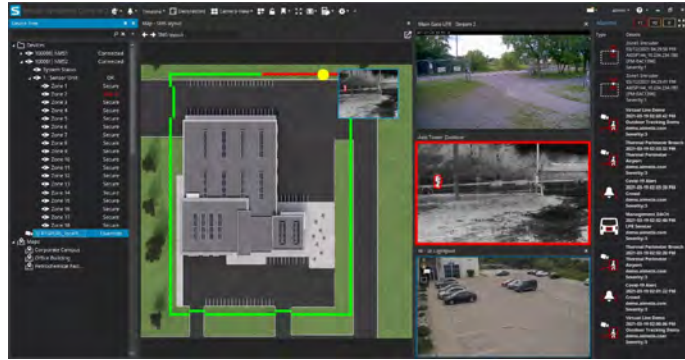
Kennwort ändern

Sie können Ihr Kennwort im Windows Client ändern.

1. Klicken Sie in der Symbolleiste oben rechts auf **Anmelden**.
2. Wählen Sie **Kennwort ändern**.
3. Geben Sie Ihr aktuelles Kennwort ein.
4. Geben Sie Ihr neues Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf **OK**.

Benutzeroberfläche

Die Windows Client-Oberfläche ist in mehrere Bereiche und Bedienfelder unterteilt, die Sie zur Überwachung von Kameras, zur Reaktion auf Alarmer, zur Navigation in Lageplänen und zur Konfiguration des Systems verwenden.



Gerätebaum

Der Gerätebaum listet die Server, Kameras, Kameraansichten, Sequenzen, Lagepläne und andere Geräte auf, die auf den verbundenen Servern verfügbar sind. Verwenden Sie den Gerätebaum, um ein Gerät zur Anzeige auszuwählen, nach einem Gerät zu suchen oder den Status eines Geräts zu ändern.

Ansichts-Panels

Ansichts-Panels zeigen Videos von Kameras, Lagepläne, Webbrowser und andere Inhalte an. Sie können Ansichts-Panels im Arbeitsbereich anordnen, Layouts als Kameraansichten speichern und zusätzliche Panels in freischwebenden oder angedockten Fenstern öffnen.

Symbolleiste

Die Symbolleiste bietet schnellen Zugriff auf häufig verwendete Befehle wie das Öffnen von Ansichten, das Wechseln von Layouts und die Verwaltung von Alarmen. Sie können die Symbolleiste anpassen, um die am häufigsten verwendeten Befehle anzuzeigen.

Alarmkonsole

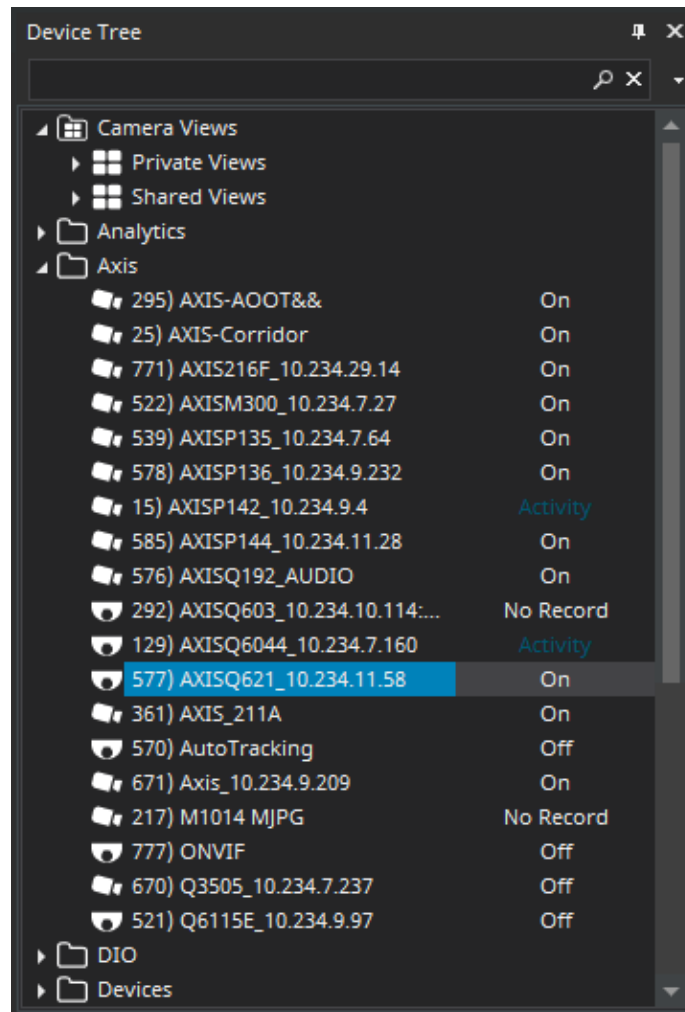
Die Alarmkonsole listet aktive und vergangene Alarme der verbundenen Server auf. Verwenden Sie die Alarmkonsole, um Alarme anzuzeigen, zu bestätigen und zu teilen.

Zeitleiste

Die Zeitleiste zeigt aufgezeichnete Videos, Alarme und Ereignisse für die Kameras an, die Sie gerade ansehen. Verwenden Sie die Zeitleiste, um durch aufgezeichnete Videos zu navigieren und Aktivitäten über einen bestimmten Zeitraum zu überprüfen.

Gerätebaum

Der Gerätebaum in der Oberfläche des Windows Client listet die auf dem Server verfügbaren Kameras, Geräte und Sequenzen auf.



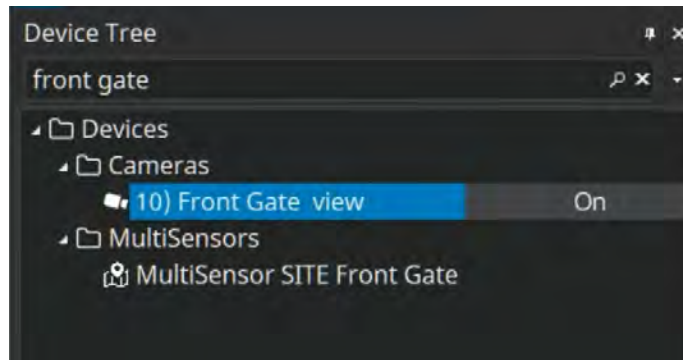
Sie können im Gerätebaum nach Kameras, Geräten und Sequenzen suchen. Geben Sie zur Suche Ihre Suchkriterien in das Suchfeld ein und klicken Sie auf Suchen. Der Windows Client filtert den Gerätebaum so, dass nur die Ergebnisse angezeigt werden, die Ihren Suchkriterien entsprechen. Um den Gerätebaum wiederherzustellen, drücken Sie das X im Suchfeld.

Der Gerätebaum zeigt auch die Status der mit dem Server verbundenen Kameras und Geräte an.

Der Gerätebaum enthält ein Kontextmenü, mit dem Sie Befehle an Geräte senden können. Wenn Sie mit der rechten Maustaste auf ein Gerät im Gerätebaum klicken, zeigt der Windows Client die anwendbaren Befehle an.

Im Gerätebaum suchen

Sie können den Gerätebaum nach Kameras, Geräten, Eingängen und Ausgängen sowie Sequenzen durchsuchen.



Wenn Sie den Gerätebaum durchsuchen, filtert der Windows Client den Gerätebaum so, dass nur Geräte enthalten sind, die Ihren Suchkriterien entsprechen.

1. Geben Sie in der Oberfläche des Windows Client den Suchbegriff in das Suchfeld des Gerätebaums ein.
2. Wählen Sie in der Liste die Eigenschaften aus, nach denen Sie suchen möchten. Sie können nach Kamera-ID, Kameraname, Kameracode und Beschreibung suchen.
3. Um die Ergebnisse auf Elemente zu beschränken, die exakt mit Ihren Suchbegriffen übereinstimmen, wählen Sie Nur exakte Übereinstimmungen aus.
4. Um Elemente, die mit Ihren Suchbegriffen übereinstimmen, aus den Suchergebnissen auszuschließen, wählen Sie Übereinstimmungen ausschließen aus. Sie können beispielsweise

On

als Suchbegriff verwenden und

Übereinstimmungen ausschließen

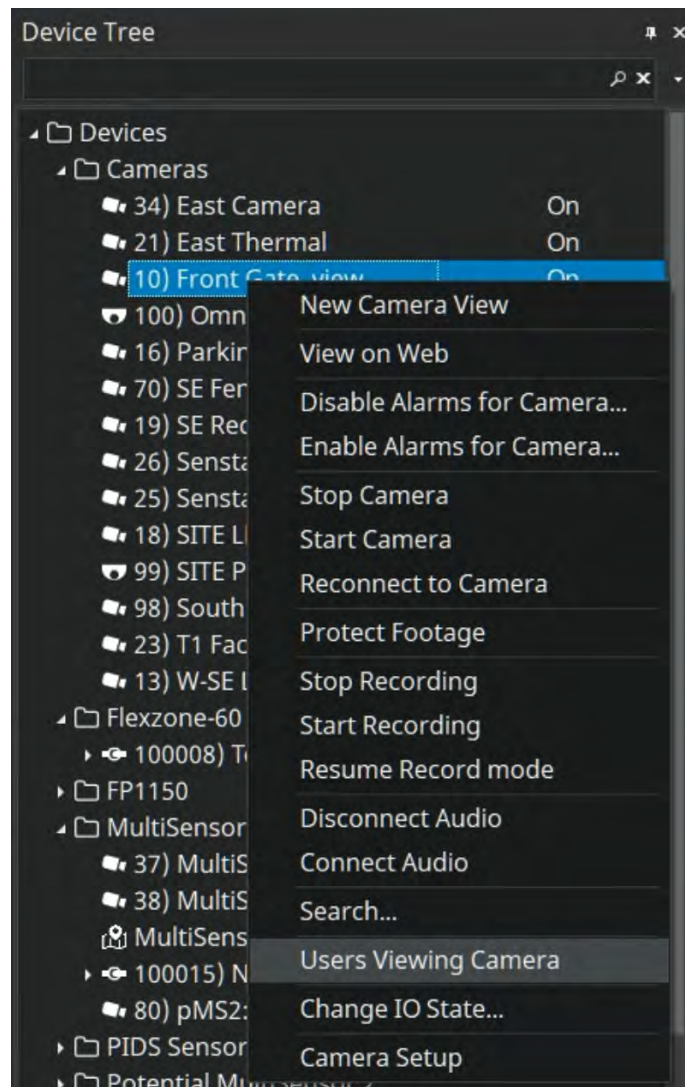
auswählen, um alle Elemente anzuzeigen, die nicht den Status On haben.

1. Klicken Sie auf das Suchsymbol.

Um die Liste des Gerätebaums wiederherzustellen, klicken Sie auf das X-Symbol.

Liste der Benutzer anzeigen, die eine Kamera ansehen

Sie können eine Liste der Benutzer anzeigen, die bei einem Windows Client angemeldet sind, in dem eine Kamera in einem Kameraansichts-Panel aktiv ist.



Um eine Liste der Benutzer anzuzeigen, die eine Kamera ansehen, müssen Sie ein Administratorbenutzer sein.

1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf eine Kamera.
2. Klicken Sie auf Users Viewing Camera.
3. Um die Liste der Benutzer, die die Kamera ansehen, zu aktualisieren, klicken Sie auf Refresh.

Videozugriff aussetzen

Der Server bietet Funktionen, mit denen der Videozugriff (Video sperren) auf eine Kamera oder eine Kameragruppe für eine bestimmte Benutzergruppe ausgesetzt werden kann.

Um diese Funktion zu verwenden, müssen Sie eine Benutzergruppe mit dem Namen UserBanGroup erstellen. Wenn Sie den Videozugriff aussetzen, können die Benutzer in der Gruppe UserBanGroup keine Videos der Kamera ansehen, während andere Benutzer die Videos der Kamera ansehen können. Die Benutzer in der Gruppe UserBanGroup können erst dann wieder Videos ansehen, wenn Sie den Videozugriff wieder aufheben (Video entsperren).

Wenn Sie den Videozugriff auf eine Kamera oder eine Kameragruppe aussetzen, wird die Kamera oder

Kameragruppe in der Server-Konfigurationsoberfläche angezeigt.

Benutzergruppe zum Aussetzen des Videozugriffs erstellen

Um den Zugriff auf Video auszusetzen, müssen Sie eine Benutzergruppe erstellen und die Gruppe zum Server hinzufügen.

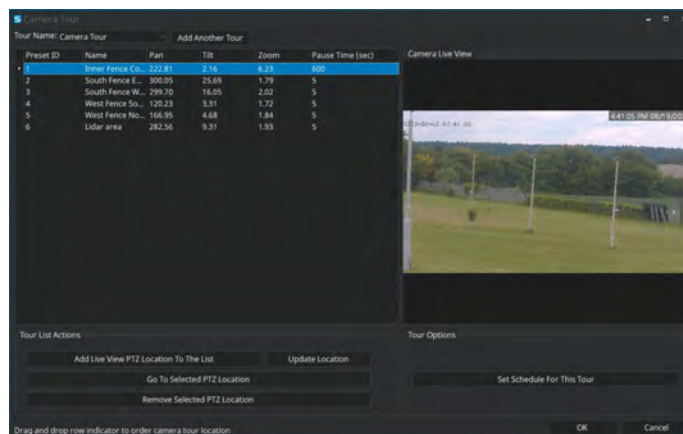
1. Führen Sie in der Oberfläche des Windows Client die folgenden Aufgaben aus:
 - a. Erstellen Sie eine Gruppe namens UserBanGroup.
 - b. Fügen Sie alle Benutzer, die Sie am Anzeigen von Video hindern möchten, zur UserBanGroup hinzu.
 - c. Wenn Sie den Zugriff auf Video auf Videowänden aussetzen möchten, fügen Sie Benutzer, die sich bei Videowand-Clients anmelden können, zur UserBanGroup hinzu.
2. Führen Sie in der Oberfläche des Windows Client die folgenden Aufgaben aus:
 - a. Klicken Sie auf Server Configuration > Manual Configuration Editor.
 - b. Klicken Sie auf Add a new setting.
 - c. Geben Sie die folgenden Werte ein:

```
Type = Global
Section = Main
ID = <empty>
Key = LiveBanGroup
Value = UserBanGroup
```

- a. Drücken Sie die Eingabetaste.
- b. Klicken Sie auf OK.

Kameratour erstellen

Sie können eine Tour mit voreingestellten Positionen erstellen, die eine PTZ-Kamera in der Oberfläche des Windows Client ansteuert.

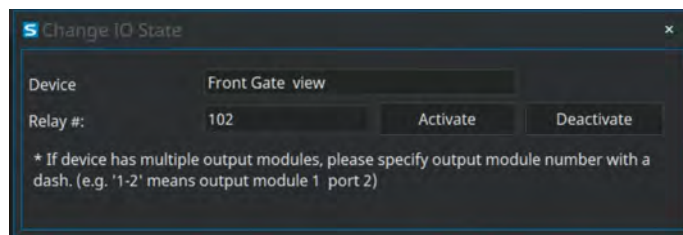


1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf eine Kamera im Gerätebaum.

2. Klicken Sie auf Camera Tour.
3. Führen Sie für jede Position in der Kameratour die folgenden Aufgaben aus:
 - a. Verwenden Sie die PTZ-Steuerelemente, um die Kamera an die gewünschte Position zu bewegen und zu zoomen.
 - b. Klicken Sie auf Add Live View PTZ Location To The List.
 - c. Klicken Sie auf die Tour-Position und bearbeiten Sie ihre Details.
4. Um den Zeitplan für die Kameratour festzulegen, führen Sie die folgenden Aufgaben aus:
 - a. Klicken Sie auf Set Schedule For This Tour.
 - b. Wählen Sie in der Zeitplanliste einen vorhandenen Zeitplan oder Create new schedule aus.
 - c. Wenn Sie einen neuen Zeitplan erstellen, geben Sie einen Namen für den Zeitplan ein.
 - d. Markieren Sie die Zellen entweder als aktiv oder inaktiv.
 - e. Klicken Sie auf OK.
5. Klicken Sie auf OK.

IO-Zustand ändern

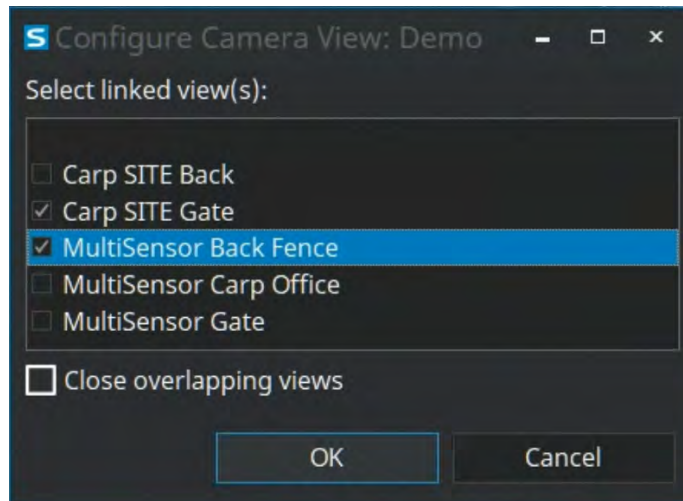
Sie können den Status der Ausgänge an Geräten in der Oberfläche des Windows Client ändern.



1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf eine Kamera im Gerätebaum.
2. Klicken Sie auf Change IO state.
3. Wählen Sie in der Liste Device das Gerät aus, an dem der Ausgangsstatus geändert werden soll.
4. Geben Sie im Feld Relay # das Modul und den Port für den Ausgang an.
5. Klicken Sie auf Activate oder Deactivate.

Kameraansicht verknüpfen

Sie können Kameraansichten verknüpfen, sodass mehrere Kameraansichten geöffnet werden, wenn Sie eine Kameraansicht öffnen. Wenn Sie die primäre Kameraansicht öffnen, öffnet der Windows Client die verknüpften Kameraansichten in neuen schwebenden Ansichten.



Bevor Sie beginnen, speichern Sie mindestens zwei Kameraansichten (eine primäre und eine sekundäre).

Das Verknüpfen von Kameraansichten ist eine einfache Möglichkeit, zahlreiche Kameraansichts-Panels zu öffnen.

1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf eine Kameraansicht im Gerätebaum.
2. Klicken Sie auf Configure Camera View.
3. Wählen Sie in der Liste Select linked view die sekundären Kameraansichten aus, die geöffnet werden sollen, wenn Sie die primäre Kameraansicht öffnen.
4. Um nicht verwendete Kameraansichts-Panels zu schließen, wenn Sie eine neue Kameraansicht öffnen, wählen Sie Close overlapping views.
5. Klicken Sie auf OK.

Audio trennen

Sie können das Audio einer Kamera trennen, sodass der Windows Client kein Audio von der Kamera empfängt.

Wenn Sie Audio trennen, wird die Einstellung Enable Audio Input für die Kamera in der Konfigurationsoberfläche des Server deaktiviert.



Das Verbinden und Trennen von Audio führt dazu, dass der Windows Client die Verbindung zur Kamera neu startet.

1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf eine Kamera im Gerätebaum.
2. Klicken Sie auf Disconnect audio. Jegliches Video, das der

Windows Client

von der Kamera anzeigt oder aufzeichnet, während das Audio getrennt ist, enthält kein Audio.

Um das Audio wieder zu verbinden, klicken Sie auf

Connect audio

Zwei-Wege-Audio

Sie können Zwei-Wege-Audio im Windows Client verwenden, um über eine Kamera mit angeschlossenem Lautsprecher zu sprechen, während Sie weiterhin das Mikrofon der Kamera mithören.

Bevor Sie beginnen:

- Die Kamera muss Zwei-Wege-Audio unterstützen und über ein angeschlossenes Mikrofon und einen Lautsprecher verfügen.
- Bei der Kamera müssen Audioeingang und Audioausgang in der Server-Konfigurationsoberfläche aktiviert sein.
- An Ihrer Windows Client-Arbeitsstation muss ein Mikrofon angeschlossen sein.
- Ihr Sicherheitsprofil muss Audioausgabe zulassen.

Eine Zwei-Wege-Audio-Sitzung starten

1. Öffnen Sie in der Oberfläche des Windows Client die Kamera in einem Ansichts-Panel.
2. Klicken Sie mit der rechten Maustaste auf die Kamera im Ansichts-Panel oder im Gerätebaum.
3. Klicken Sie auf Mit Kamera sprechen.
4. Halten Sie die Schaltfläche Push-to-Talk gedrückt oder drücken Sie das konfigurierte Tastaturkürzel, während Sie sprechen.

Der Windows Client sendet Audio von Ihrem Mikrofon an den Lautsprecher der Kamera, solange Sie die Schaltfläche gedrückt halten. Das Mikrofonaudio der Kamera wird die ganze Zeit über im Windows Client weiter wiedergegeben.

Eine Zwei-Wege-Audio-Sitzung beenden

1. Klicken Sie mit der rechten Maustaste auf die Kamera im Ansichts-Panel oder im Gerätebaum.
2. Klicken Sie auf Sprechen beenden.



Es kann immer nur ein Windows Client gleichzeitig mit einer Kamera sprechen. Wenn ein anderer Bediener bereits Zwei-Wege-Audio mit der Kamera nutzt, ist die Option Mit Kamera sprechen nicht verfügbar, bis der andere Bediener beendet.

Gerätestatus ausblenden

Sie können den Status von Geräten im Gerätebaum ausblenden.

1. Klicken Sie in der Oberfläche des Windows Client auf View > Settings.
2. Klicken Sie auf die Registerkarte Customize.
3. Deaktivieren Sie im Bereich Device Tree das Kontrollkästchen Show Device Status.
4. Klicken Sie auf OK. /

Serverliste

Die Oberfläche des Windows Client listet die Server-Instanzen auf, mit denen der Windows Client verbunden ist, sowie deren Status. Sie können einen Server auswählen, um auf die Kameras und Geräte

zuzugreifen, die mit dieser Instanz verbunden sind.

Standardmäßig zeigt die Oberfläche des Windows Client die Server-Instanzen, auf die der Windows Client zugreifen kann, in der Serverfarmliste in der Symbolleiste an.

Optional können Sie die Oberfläche des Windows Client so konfigurieren, dass die Server-Instanzen, mit denen sich der Windows Client verbinden kann, in einem Serverlisten-Bedienfeld angezeigt werden. Wenn Sie das Serverlisten-Bedienfeld aktivieren, wird die Serverliste in der Symbolleiste ausgeblendet.

Die Serverfarmliste und das Serverlisten-Bedienfeld enthalten alle Server-Instanzen, für die Sie eine Verbindung konfiguriert haben.

Aktiven Server über die Serverfarmliste auswählen

Sie können den aktiven Server in der Serverfarmliste in der Symbolleiste auswählen.

Die Serverfarmliste ist standardmäßig in der Oberfläche des Windows Client sichtbar.

1. Klicken Sie in der Oberfläche des Windows Client auf den Pfeil nach unten in der Serverfarmliste.
2. Klicken Sie in der Serverliste auf den Server, der im Windows Client aktiv sein soll.

Serverlisten-Bereich aktivieren

Sie können die Dienstliste als Panel in der Oberfläche des Windows Client anzeigen.

1. Öffnen Sie die Datei acc.ini unter %appdata%\Senstar8.
2. Setzen Sie den Wert **ShowFarmDropDown** im Abschnitt **Main** auf **False**.
3. Speichern und schließen Sie die Datei acc.ini.
4. Starten Sie den Windows Client.
5. Klicken Sie in der Oberfläche des Windows Client auf View > Server List.

Aktiven Server über die Serverliste auswählen

Bevor Sie beginnen, müssen Sie das Bedienfeld der Serverliste aktivieren.

Klicken Sie im Bedienfeld Serverliste der Oberfläche des Windows Client auf den Server, der im Windows Client aktiv sein soll.

Ansichts-Panels

Ansichts-Panels können Live-Video, aufgezeichnete Videos, Dekos von Kameras, Browserseiten und Lagepläne in der Oberfläche des Windows Client anzeigen.

Ansichts-Panels können Overlays mit Steuerelementen für die Kamera anzeigen. Um die Overlays auszublenden, können Sie die Umschalttaste gedrückt halten, während Sie Aktionen (z. B. Kasten-Zoom) im Kameraansichts-Panel ausführen.

+



+

Kamera anzeigen

Sie können in jedem Kameraansichts-Panel in der Oberfläche des Windows Client eine Kamera anzeigen.

Bevor Sie beginnen:

- Fügen Sie eine Kamera zum Server hinzu
- Öffnen Sie eine freischwebende oder angedockte Kameraansicht
 1. Klicken Sie in der Oberfläche des Windows Client auf eine Kameraansicht.
 2. Klicken Sie im Gerätebaum auf die Kamera, die Sie anzeigen möchten.

Browser anzeigen

Sie können in jedem Kameraansichts-Panel in der Oberfläche des Windows Client einen Browser anzeigen.

Bevor Sie beginnen:

- Fügen Sie einen Browser zum Server hinzu
- Öffnen Sie eine freischwebende oder angedockte Kameraansicht
 1. Klicken Sie in der Oberfläche des Windows Client auf ein Kameraansichts-Panel.
 2. Klicken Sie im Gerätebaum auf den Browser, den Sie anzeigen möchten.

Lageplan anzeigen

Sie können in jedem Kameraansichts-Panel in der Oberfläche des Windows Client einen Lageplan anzeigen.

Bevor Sie beginnen:

- Fügen Sie einen Lageplan zum Windows Client hinzu
- Öffnen Sie eine freischwebende oder angedockte Kameraansicht
 1. Klicken Sie in der Oberfläche des Windows Client auf ein Kameraansichts-Panel.
 2. Klicken Sie im Gerätebaum auf den Browser, den Sie anzeigen möchten.

Senstar Thin Client anzeigen

Sie können ein Gerät in der Windows Client-Oberfläche in der Oberfläche des Windows Client anzeigen.

Bevor Sie beginnen:

- Fügen Sie einen Senstar Thin Client zum Server hinzu

Wenn Sie einen Senstar Thin Client in der Oberfläche des Windows Client anzeigen, wird der Senstar Thin Client in einer neuen freischwebenden Ansicht geöffnet.

Klicken Sie im Gerätebaum auf den Senstar Thin Client, den Sie anzeigen möchten.

Bild-im-Bild anzeigen

Sie können Live-Video in einem eingebetteten Fenster anzeigen, während Sie aufgezeichnete Videos ansehen.

Das Bild-im-Bild-Fenster zeigt Live-Video an, während im Haupt-Kameraansichts-Panel historisches Video angezeigt wird.

1. Führen Sie in einem Kameraansichts-Panel der Oberfläche des Windows Client eine der folgenden Aufgaben aus:
 - a. Klicken Sie mit der rechten Maustaste in das Kameraansichts-Panel und klicken Sie auf Bild-im-Bild anzeigen.
 - b. Bewegen Sie den Mauszeiger über das Kameraansichts-Panel und klicken Sie auf das Bild-im-Bild-Symbol.
2. Sehen Sie aufgezeichnete Videos im Haupt-Kameraansichts-Panel an, um Live-Video im Bild-im-Bild-Fenster anzuzeigen.
3. Um das Bild-im-Bild-Fenster zu verschieben, klicken Sie auf eines der Symbole in der Ecke des Bild-im-Bild-Fensters, um das Fenster in diese Ecke des Kameraansichts-Panels zu verschieben.

Sofortwiedergabe anzeigen

Sie können historische Videos entweder 5 oder 10 Sekunden hinter dem Live-Video im Windows Client abspielen.

Sie können die Dauer der Sofortwiedergabe auf der Seite Videoeinstellungen in den Einstellungen des Windows Client auswählen.

1. Stellen Sie in der Oberfläche des Windows Client die Dauer der Sofortwiedergabe ein.
2. Klicken Sie in einem Video-Bereich der Oberfläche des Windows Client auf das Symbol Sofortwiedergabe.
3. Sehen Sie sich das aufgezeichnete Video an.

Um die Sofortwiedergabe zu beenden, klicken Sie auf das Symbol

Zur Live-Ansicht wechseln

.

Kameraansicht speichern

Sie können das Layout einer andockten oder freischwebenden Ansicht speichern, um einen einfachen Zugriff auf die Ansichtskonfiguration zu ermöglichen.

1. Klicken Sie in der Oberfläche des Windows Client auf Kameraansicht > Aktuelle Ansicht speichern.
2. Führen Sie im Fenster Speichern unter eine der folgenden Aufgaben aus:
 - Um eine vorhandene Kameraansicht zu überschreiben, wählen Sie Vorhandene Kameraansicht aus und wählen Sie die zu überschreibende vorhandene Kameraansicht aus.
 - Um sie als neue Kameraansicht zu speichern, wählen Sie Neue Kameraansicht aus und geben Sie einen Namen für die Kameraansicht ein.
3. Um die gespeicherte Kameraansicht öffentlich zu machen, wählen Sie Mit anderen Benutzern geteilt aus.
4. Klicken Sie auf OK.

Kameraansicht laden

1. Klicken Sie in der Oberfläche des Windows Client auf Camera View > Load Camera View.
2. Wählen Sie die zu ladende Kameraansicht aus.

Angedockte Kameraansicht öffnen

Sie können eine Kameraansicht in der Oberfläche des Windows Client öffnen.

Der Windows Client enthält Kameraansichten mit 1, 4, 6, 9, 16 und 25 Kameraansichts-Panels.

1. Klicken Sie in der Oberfläche des Windows Client auf Camera View > New Docked View.
2. Klicken Sie auf die Kameraansicht, die Sie öffnen möchten.

Schwebende Kameraansicht öffnen

Sie können eine Kameraansicht in einem neuen Fenster öffnen.

Der Windows Client enthält Kameraansichten mit 1, 4, 6, 9, 16 und 25 Kameraansichts-Panels.

Um zu verhindern, dass sich die Ansichts-Panels in der schwebenden Ansicht ändern, klicken Sie in der schwebenden Ansicht auf das Symbol Prevent panel selection (Schloss). Obwohl Sie das Panel nicht auswählen können, können Sie den Fokus weiterhin auf das Panel legen, indem Sie in das Panel klicken.

1. Klicken Sie in der Oberfläche des Windows Client auf Camera View > New Floating View.
2. Klicken Sie auf die Kameraansicht, die Sie öffnen möchten.

Kameraansichts-Panel hinzufügen

Sie können der Oberfläche des Windows Client ein Ansichts-Panel für Kamera hinzufügen. Ein neues Ansichts-Panel für Kamera erscheint als schwebendes Ansichts-Panel, Sie können es jedoch in der Oberfläche des Windows Client andocken.

1. Klicken Sie in der Oberfläche des Windows Client auf Add Camera View Panel.
2. Ziehen Sie das Ansichts-Panel für Kamera an die gewünschte Position.

Alarm hinzufügen

Sie können im Windows Client einen manuellen Alarm zu einer Kamera hinzufügen.

Sie können manuelle Alarmer verwenden, um den mit der manuellen Regel verknüpften Aktionssatz zu

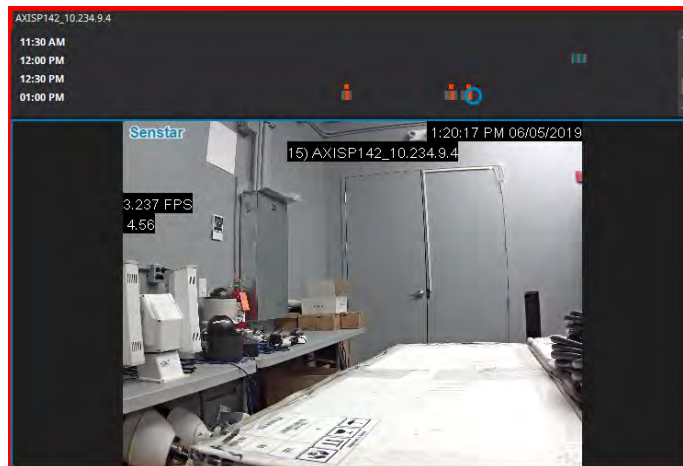
aktivieren.

1. Öffnen Sie in der Oberfläche des Windows Client die Kamera, der Sie einen Alarm hinzufügen möchten, in einem Ansichts-Panel für Kamera.
2. Bewegen Sie den Mauszeiger über das Ansichts-Panel für Kamera, das die Kamera enthält, der Sie einen Alarm hinzufügen möchten, und klicken Sie auf das Alarmsymbol.

Alarmanzeige hinzufügen

Sie können einen Alarmindikator um ein Ansichts-Panel für Kamera anzeigen. Der Alarmindikator blinkt für eine bestimmte Zeit oder bis Sie den Alarm bestätigen.

+



+

1. Klicken Sie in der Oberfläche des Windows Client auf View > Settings.
2. Klicken Sie auf die Registerkarte Alarms.
3. Wählen Sie Flash panel on alarm.
4. Geben Sie im Feld Number of seconds to flash alarm ein, wie lange das Ansichts-Panel für Kamera blinkt, wenn die Kamera einen Alarm aufzeichnet.
5. Klicken Sie auf OK.

Kameraansichts-Panel konfigurieren

1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf ein Ansichts-Panel für Kamera.
2. Klicken Sie auf Settings.
3. Konfigurieren Sie die Einstellungen für das Ansichts-Panel für Kamera.
4. Um die Einstellungen auf alle Ansichts-Panels für Kamera anzuwenden, klicken Sie auf Other > Apply To All.
5. Klicken Sie auf Apply.
6. Klicken Sie auf OK.

Name des Ansichts-Panels ändern

Sie können den Namen der Panels im Windows Client ändern.

Standardmäßig enthalten Panel-Namen den Namen des Computers, den Port, eine Beschriftung für eine angedockte Ansicht oder eine schwebende Ansicht und einen Bezeichner für das Panel.

1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste in das Panel.
2. Klicken Sie auf Settings.
3. Geben Sie auf der Registerkarte Child den neuen Namen im Feld Panel Name ein.
4. Klicken Sie auf OK.

Alarmkameras im Panel anzeigen

Sie können das Ansichts-Panel auswählen, in dem standardmäßig die Kamera angezeigt wird, die Sie bei einem Alarm anzeigen möchten.

Wenn Sie mehr als eine Kamera für die Anzeige bei einem Alarm auswählen, wird das Bedienfeld, das Sie zum Anzeigen von Alarmkameras ausgewählt haben, zum Startbedienfeld; weitere Bedienfelder von links nach rechts und von oben nach unten in der Oberfläche des Windows Client zeigen alle weiteren Kameras an, die Sie für die Anzeige bei einem Alarm ausgewählt haben.

1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf das Ansichts-Panel, in dem die Kameras des Alarms angezeigt werden sollen.
2. Klicken Sie auf Einstellungen.
3. Wählen Sie auf der Registerkarte Aktivität die Option Ansicht beim Auftreten eines Alarms wechseln aus.
4. Um andere Kameras, die in der Liste der Ansicht-bei-Alarm aufgeführt sind, in anderen Ansichts-Panels anzuzeigen, wählen Sie Alarmkameras in anderen Bedienfeldern anzeigen aus.
5. Um Änderungen auf bestimmte Kameras und Alarmer zu beschränken, wählen Sie Aktion auf bestimmte Kameras oder Alarmer beschränken aus und wählen Sie die Kameras und Alarmer in der Liste aus.
6. Klicken Sie auf Anwenden.
7. Klicken Sie auf OK.

Inhalt des Ansichts-Panels gegen Änderungen schützen

Im Windows Client können Sie verhindern, dass ein Ansichts-Panel den angezeigten Inhalt (z. B. Kamera, Lageplan oder Browser) ändert.

Sie können Inhaltsänderungen in Ansichts-Panels über das Kontextmenü jedes Ansichts-Panels verhindern. Um zu verhindern, dass sich der Inhalt eines Ansichts-Panels in einer angedockten Ansicht ändert, können Sie in der Symbolleiste des Fensters der angedockten Ansicht auf das Symbol Prevent panel content changes (Schloss) klicken.

1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf das Ansichts-Panel.
2. Klicken Sie auf Prevent panel content changes.

Um diese Einstellung umzuschalten, klicken Sie auf
Allow panel content changes

Einstellungen für Kameraansicht

Erscheinungsbild

Einstellung	Beschreibung
Lock Timeline Height When Resize Occurs	Wählen Sie diese Option aus, um zu verhindern, dass die Größe der Zeitleiste geändert wird, wenn Sie die Größe des Ansichts-Panels für Kamera ändern.
Overlay Camera Messages	Wählen Sie diese Option aus, um Nachrichten von der Kamera im Ansichts-Panel für Kamera anzuzeigen.
Overlay Time	Wählen Sie diese Option aus, um die Uhrzeit im Ansichts-Panel für Kamera anzuzeigen.
Overlay Tracking Boxes	Wählen Sie diese Option aus, um Boxen für Videoanalysen im Ansichts-Panel für Kamera anzuzeigen.
Overlay video retention on video	Wählen Sie diese Option aus, um die Anzahl der Tage des Videos für die Kamera anzuzeigen.
Overlay Messenger Messages	Wählen Sie diese Option aus, um Nachrichten im Ansichts-Panel für Kamera anzuzeigen, und legen Sie fest, wie viele Sekunden die Nachrichten sichtbar bleiben.
Overlay Tracking Paths	Wählen Sie diese Option aus, um Pfade für Videoanalysen im Ansichts-Panel für Kamera anzuzeigen.
Overlay Date	Wählen Sie diese Option aus, um das Datum im Ansichts-Panel für Kamera anzuzeigen.
Overlay Thick Decoration	Wählen Sie diese Option aus, um Tracking-Boxen und -Pfade als breitere Linien anzuzeigen.
Overlay Recording Indicator	Wählen Sie diese Option aus, um den Aufnahmeindikator im Ansichts-Panel für Kamera anzuzeigen.
Video Quality	Wählen Sie die Auflösung für das Ansichts-Panel für Kamera aus. Die Standardauflösung ist die für die Kamera eingestellte Auflösung.
Display Mode	Wählen Sie die Größe und das Seitenverhältnis des im Ansichts-Panel für Kamera anzuzeigenden Videos aus.

Aktivität

Einstellung	Beschreibung
Switch view when an alarm occurs	Wählen Sie diese Option aus, um das Ansichts-Panel für Kamera zu wechseln, wenn ein Alarm auftritt.
Switch view when motion occurs	Wählen Sie diese Option aus, um das Ansichts-Panel für Kamera zu wechseln, wenn Bewegung auftritt.
Show alarm cameras in other panels	Wenn die Regel für den Alarm die Option View other cameras on alarm enthält, wählen Sie diese Option aus, um die anderen Ansichts-Panels für Kamera auf diese Kameras umzuschalten. Diese Einstellung wird sichtbar, wenn Sie Switch view when an alarm occurs auswählen.

Einstellung	Beschreibung
Limit action to specific cameras or alarms	Wählen Sie diese Option aus und geben Sie die Kameras an, um die Aktivität des Ansichts-Panels für Kamera auf bestimmte Kameras oder Alarmer zu beschränken. Diese Einstellung wird sichtbar, wenn Sie Switch view when an alarm occurs oder Switch view when motion occurs auswählen.
Ensure Visible	Wählen Sie diese Option aus, um das Ansichts-Panel für Kamera in den Fokus zu bringen, wenn ein Alarm oder eine Bewegung auftritt.
Display	Wählen Sie aus, ob das Ansichts-Panel für Kamera zu Video oder einem Standbild wechselt.
Perform action after switch	Wählen Sie diese Option aus, um eine Aktion auszuführen, wenn ein Alarm oder eine Bewegung auftritt.
Disable switching after switch occurs	Wählen Sie diese Option aus, um zu verhindern, dass das Ansichts-Panel für Kamera nach einem nachfolgenden Alarm oder einer Bewegung zu einer anderen Kamera wechselt.
Hide switched view after seconds	Legen Sie fest, wie viele Sekunden das Ansichts-Panel für Kamera die umgeschaltete Kameraansicht anzeigt.
Go back to previous state after seconds	Wählen Sie diese Option aus und geben Sie die Anzahl der Sekunden an, um das Ansichts-Panel für Kamera in den Zustand vor dem Alarmwechsel zurückzusetzen.

Untergeordnet

Einstellung	Beschreibung
Show latest alarm when the camera displayed in another panel changes	Wählen Sie diese Option aus, um den letzten Alarm vom primären Ansichts-Panel für Kamera anzuzeigen.
Panel Name	Sie können den Panel-Namen mit der Videowand-Funktion und dem Senstar Symphony SDK verwenden. Sie können den Standardnamen verwenden oder ihn in einen aussagekräftigeren Namen ändern.

Verfolgung

Einstellung	Beschreibung
Digitally zoom in on hot spots	Wählen Sie diese Option aus, um automatisch in Objekte hineinzuzoomen, die durch Videoanalysen erkannt werden. Diese Einstellung funktioniert sowohl für Live- als auch für aufgezeichnetes Video.

Sonstiges

Einstellung	Beschreibung
Apply To All	Klicken Sie hier, um Ihre Änderungen auf alle aktiven Ansichts-Panels für Kamera anzuwenden.

Suchen

Sie können Videoaufnahmen einer Kamera nach Objekten und Ereignissen durchsuchen.

- Führen Sie in der Oberfläche des Windows Client eine der folgenden Aufgaben aus:
 - Klicken Sie mit der rechten Maustaste auf das Kameraansichts-Panel und klicken Sie auf

Suchen.

- Bewegen Sie den Mauszeiger über das Kameraansichts-Panel und klicken Sie auf das Suchsymbol.

2. Wählen Sie im Bereich Klasse die Art des Objekts aus, nach dem gesucht werden soll.
3. Wählen Sie im Bereich Verhalten aus, ob sich das Objekt bewegen oder verweilen soll und wie lange es das Verhalten zeigen soll.
4. Legen Sie fest, ob der Suchbereich durch eine Maske oder Zäune definiert werden soll.
5. Wählen Sie im Bereich Einschließen die Teile des Objekts oder der Objektbewegung aus, die den Suchbereich passieren müssen, damit das Objekt in die Suchergebnisse aufgenommen wird.
6. Wählen Sie im Bereich Zeichnen aus, ob Maskenbereich oder Zäune hinzugefügt oder entfernt werden sollen.
7. Definieren Sie den Suchzeitraum in den Feldern Von und Bis.
8. Wählen Sie im Bereich Suchen nach aus, ob nach allen Ereignissen oder nur nach Ereignissen gesucht werden soll, die Alarme auslösen. Wenn Sie diese Auswahl ändern, werden die im Fenster

Suchen

verfügbaren Einstellungen geändert.

1. Wählen Sie im Bereich Add-Ons (verfügbar, wenn Sie nach allen Ereignissen suchen) die Videoanalyse-Ereignisse aus, nach denen gesucht werden soll.
2. Wählen Sie im Bereich Regeln die Regelereignisse aus, nach denen gesucht werden soll.
3. Wählen Sie in der Liste Stream den zu durchsuchenden Stream aus.
4. Klicken Sie auf Suchen.

Video nach Datum anzeigen

Sie können in einem Kameraansichts-Panel Videos eines bestimmten Datums und einer bestimmten Uhrzeit anzeigen.

Daten, für die die Kamera Video aufweist, werden im Kalender fett dargestellt.

1. Führen Sie in einem Kameraansichts-Panel der Oberfläche des Windows Client eine der folgenden Aufgaben aus:
 - a. Klicken Sie mit der rechten Maustaste in das Kameraansichts-Panel und klicken Sie auf Datum.
 - b. Bewegen Sie den Mauszeiger über das Kameraansichts-Panel und klicken Sie auf das Datumssymbol.
2. Geben Sie ein Datum und eine Uhrzeit an.
3. Klicken Sie auf Auswählen.

Video manuell aufzeichnen

Sie können die Aufzeichnung von Video von einer Kamera manuell starten, die nicht auf permanente Aufzeichnung eingestellt ist.

Sie können die Aufzeichnung über das Ansichts-Panel starten, das das Video der Kamera in der Oberfläche des Windows Client anzeigt. Wenn Sie die Aufzeichnung über das Ansichts-Panel starten, wird das Video in 10-minütigen Intervallen aufgezeichnet.

Darüber hinaus können Sie die Aufzeichnung für eine Kamera über das Kontextmenü (Rechtsklick) im Gerätebaum in der Oberfläche des Windows Client starten und stoppen. Wenn Sie die Aufzeichnung über das Kontextmenü starten, gibt es keine Zeitbegrenzung und die Kamera zeichnet weiter auf, bis Sie die Aufzeichnung manuell über das Kontextmenü stoppen.

1. Klicken Sie in der Oberfläche des Windows Client auf die Schaltfläche Start Recording, um 10 Minuten Video von der Kamera aufzuzeichnen.
2. Um weitere 10 Minuten hinzuzufügen, klicken Sie erneut auf die Schaltfläche Start Recording. Sie können die Schaltfläche mehrmals anklicken, um mehrere 10-Minuten-Intervalle hinzuzufügen.

Das Kameraansichts-Panel zeigt ein Symbol an, um anzuzeigen, dass der

Server

Video aufzeichnet.

Über Adresse öffnen

Sie können einen Alarm, eine Kamera oder Video aus einer bestimmten Zeit im aktiven Kameraansichts-Panel öffnen.

Nachdem Sie eine gültige Adresse eingegeben haben, zeigt das aktive Kameraansichts-Panel das von Ihnen angegebene Video an.

1. Drücken Sie in der Oberfläche des Windows Client die Taste F5.
2. Führen Sie im Fenster Enter address eine der folgenden Aufgaben aus:
 - Geben Sie eine Alarm-ID ein.
 - Geben Sie eine Kamera-ID ein.
 - Geben Sie den Servernamen und die Kamera-ID ein. Verwenden Sie das Format `http://computer_name/camera_id/date_time`.
3. Klicken Sie auf OK.

Zusammenfassungsvideo anzeigen

Sie können ein Zusammenfassungsvideo einer Kamera anzeigen, auf der eine Videoanalyse ausgeführt wird.

Das Zusammenfassungsvideo überspringt Material, in dem die Videoanalyse keine Ereignisse erkennt, und zeigt Material, in dem die Videoanalyse Ereignisse erkennt, mit 16-facher Geschwindigkeit an.

1. Sehen Sie sich in der Oberfläche des Windows Client ein Video einer Kamera an, auf der eine Videoanalyse ausgeführt wird.
2. Navigieren Sie in der Zeitleiste zu historischem Video.
3. Klicken Sie auf das Symbol Video zusammenfassen, um das Zusammenfassungsvideo abzuspielen.

Videosteuerung

Steuerelement	Beschreibung
	Verringert die Wiedergabegeschwindigkeit.
	Schieber zum Anpassen der Wiedergabegeschwindigkeit.

Steuerelement	Beschreibung
	Erhöht die Wiedergabegeschwindigkeit.
	Navigiert zum vorherigen Lesezeichen.
	Navigiert zum vorherigen Alarm.
	Navigiert zur vorherigen Aktivität.
	Geht zehn Sekunden zurück.
	Geht eine Sekunde zurück.
	Geht ein Bild zurück.
	Video abspielen.
	Video pausieren.
	Geht ein Bild vorwärts.
	Geht eine Sekunde vorwärts.
	Geht zehn Sekunden vorwärts.
	Navigiert zur nächsten Aktivität.
	Navigiert zum nächsten Alarm.
	Navigiert zum nächsten Lesezeichen.
	Live-Video anzeigen

PTZ-Steuerung

Steuerelement	Beschreibung
	Bewegen Sie die PTZ-Kamera zu einer voreingestellten Position.
	Vergrößern Sie den Zoom auf der PTZ-Kamera.
	Verkleinern Sie den Zoom auf der PTZ-Kamera.
	Bewegen Sie die PTZ-Kamera in die Ausgangsposition.
	Bewegen Sie die PTZ-Kamera.
	Sperren oder Entsperren der PTZ-Kamerabewegung.
	Öffnen Sie die Konfigurationsseite für die Kameratour.
	Erweitern oder Reduzieren der Kamerasteuerelemente.

Kamerasteuerung

Steuerung	Beschreibung
	Öffnen oder schließen Sie die Blende der Kamera, um anzupassen, wie viel Licht in das Objektiv der Kamera einfällt.
	Erhöhen oder verringern Sie die Helligkeit der Kamera.
	Stellen Sie den Fokus der Kamera ein.
	Stellen Sie den Kontrast der Kamera ein.

Lagepläne

Lagepläne können den Standort von Kameras, Kameraansichten, digitalen Ein- und Ausgabegeräten, Links und Beschriftungen in der Oberfläche des Windows Client anzeigen.

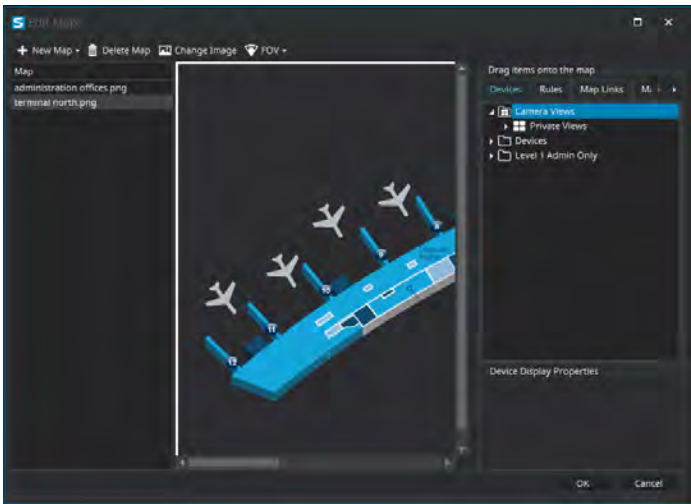
Lageplaneditor

Der Lageplaneditor ist eine Komponente im Windows Client, die Sie zur Verwaltung von Lageplänen verwenden.

Sie können den Lageplaneditor verwenden, um Lagepläne dem Windows Client hinzuzufügen. Ein Lageplan kann eine Bilddatei (jpg-, gif- oder bmp-Datei), eine CAD-Datei (DWG-Format 2013 oder früher) oder ein von einem GIS-Dienst bereitgestellter Lageplan sein.

Sie können den Lageplaneditor verwenden, um Kameras, Kameraansichten, digitale Ein- und Ausgabegeräte, Links und Beschriftungen einem Lageplan hinzuzufügen. Elemente, die Sie einem Lageplan hinzufügen, erscheinen im Lageplan-Bereich der Oberfläche des Windows Client und können dort Funktionalität hinzufügen.

+



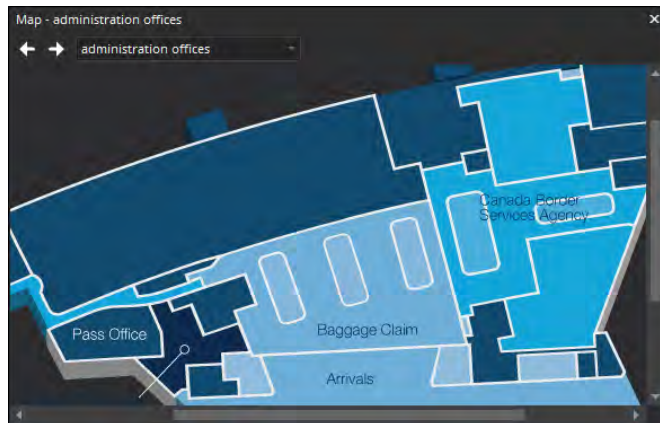
+

Lageplan-Navigation

Wenn Sie die Lageplan-Navigation einschalten, zeigt die Oberfläche des Windows Client den Lageplan-Bereich an.

Das Klicken auf ein Symbol im Lageplan-Bereich führt die folgenden Aktionen aus:

- Klicken auf ein Kamerasymbol zeigt die Kameraansicht im aktiven Video-Panel an.
- Klicken auf ein Kameraansichts-Symbol lädt die Kameraansicht in der Oberfläche des Windows Client.
- Rechtsklick auf ein Ausgabegerät öffnet ein Kontextmenü mit Befehlen, die Sie an das Gerät senden können.



===== Lageplan hinzufügen

Sie können dem Windows Client einen Lageplan hinzufügen.

1. Klicken Sie in der Oberfläche des Windows Client auf View > Map Editor.
2. Klicken Sie auf New Map > Upload File.
3. Navigieren Sie zur Lageplandatei und klicken Sie auf Open.
4. Um den Namen des Lageplans zu ändern, klicken Sie auf den Namen des Lageplans in der Liste und geben Sie den neuen Namen ein.
5. Klicken Sie auf OK.

GIS-Lageplan hinzufügen

Sie können einen Lageplan vom ArcGIS-Dienst zum Windows Client hinzufügen.

1. Klicken Sie in der Oberfläche des Windows Client auf View > Map Editor.
2. Klicken Sie auf New Map > GIS Map.
3. Geben Sie im Feld Map Name einen Namen für den Lageplan ein, der in der Lageplanliste erscheinen soll.
4. Geben Sie im Feld Server Address die URL des Lageplandienstes ein.
5. Klicken Sie auf Add Map.
6. Klicken Sie auf OK.

Lageplan anzeigen

Sie können das Lageplan-Bedienfeld öffnen und einen Lageplan in der Oberfläche des Windows Client anzeigen.

Sie können auf dem Lageplan navigieren, indem Sie die Bildlaufleisten verwenden oder den Lageplan klicken und ziehen.

1. Klicken Sie in der Oberfläche des Windows Client auf Ansicht > Lageplan-Navigation.
2. Verwenden Sie im Lageplan-Bedienfeld die Pfeile, um durch die Lagepläne zu navigieren, oder wählen Sie den Lageplan in der Liste aus.

Gerät zu einem Lageplan hinzufügen

Sie können Kameras, Kameraansichten, Zutrittskontrollgeräte, Senstar Symphony Access Control und Senstar Network Manager zu einem Lageplan hinzufügen.

Wenn Sie ein Gerät zu einem Lageplan hinzufügen, zeigt der Lageplan einen Link an, der entweder die Kamera oder die Kameraansicht öffnet oder den Status des Zutrittskontrollgeräts anzeigt.

1. Klicken Sie in der Oberfläche des Windows Client auf View > Map Editor.
2. Wählen Sie einen Lageplan aus.
3. Klicken Sie auf die Registerkarte Devices.
4. Ziehen Sie ein Gerät auf den Lageplan.
5. Um das Kamerasymbol zu drehen, führen Sie die folgenden Schritte aus:
 - a. Klicken Sie mit der rechten Maustaste auf das Kamerasymbol.
 - b. Klicken Sie auf Rotate.
 - c. Bewegen Sie die Maus, bis die Kamera in die richtige Richtung zeigt, und klicken Sie auf die Maustaste.
6. Klicken Sie auf OK.

Beschriftung zu einem Lageplan hinzufügen

Sie können einem Lageplan eine Beschriftung hinzufügen.

Zusätzlich zur Definition des Textes und der Formatierung der Beschriftung können Sie der Beschriftung auch einen Hyperlink hinzufügen.

1. Klicken Sie in der Oberfläche des Windows Client auf View > Map Editor.
2. Wählen Sie einen Lageplan aus.
3. Klicken Sie auf die Registerkarte Map Labels.
4. Um eine neue Beschriftung zu erstellen, führen Sie die folgenden Aufgaben im Bereich Map Label aus:
 - a. Geben Sie im Feld Name den Namen ein, den der Map Editor in der Liste der Beschriftungen anzeigt.
 - b. Geben Sie im Feld Text den Text ein, der auf dem Lageplan erscheinen soll.
 - c. Wählen Sie im Feld Font Name die Schriftart aus, die für die Beschriftung verwendet werden soll.
 - d. Wählen Sie im Feld Font Size die Größe des Textes auf dem Lageplan aus.
 - e. Wählen Sie im Feld Foreground die Farbe des Textes auf dem Lageplan aus.
 - f. Wählen Sie im Feld Background die Farbe und Deckkraft des Banners hinter dem Text aus.

- g. Legen Sie im Feld Width die Breite des Banners hinter dem Text fest.
- h. Legen Sie im Feld Height die Höhe des Banners hinter dem Text fest.
- i. Geben Sie im Feld URL den Hyperlink ein.
- j. Klicken Sie auf Save.

Nachdem Sie eine neue Beschriftung gespeichert haben, erscheint die Beschriftung in der Beschriftungsliste.

1. Klicken und ziehen Sie eine Beschriftung aus der Beschriftungsliste an die gewünschte Position auf dem Lageplan.
2. Klicken Sie auf OK.

Um eine Beschriftung von einem Lageplan zu entfernen, klicken Sie mit der rechten Maustaste auf die Beschriftung, klicken Sie auf

Remove from Map

und klicken Sie auf

OK

.

Regel zu einem Lageplan hinzufügen

Sie können einem Lageplan eine Beschriftung hinzufügen.

Zusätzlich zur Definition des Textes und der Formatierung der Beschriftung können Sie der Beschriftung auch einen Hyperlink hinzufügen.

1. Klicken Sie in der Oberfläche des Windows Client auf View > Map Editor.
2. Wählen Sie einen Lageplan aus.
3. Klicken Sie auf die Registerkarte Map Labels.
4. Um eine neue Beschriftung zu erstellen, führen Sie die folgenden Aufgaben im Bereich Map Label aus:
 - a. Geben Sie im Feld Name den Namen ein, den der Map Editor in der Liste der Beschriftungen anzeigt.
 - b. Geben Sie im Feld Text den Text ein, der auf dem Lageplan erscheinen soll.
 - c. Wählen Sie im Feld Font Name die Schriftart aus, die für die Beschriftung verwendet werden soll.
 - d. Wählen Sie im Feld Font Size die Größe des Textes auf dem Lageplan aus.
 - e. Wählen Sie im Feld Foreground die Farbe des Textes auf dem Lageplan aus.
 - f. Wählen Sie im Feld Background die Farbe und Deckkraft des Banners hinter dem Text aus.
 - g. Legen Sie im Feld Width die Breite des Banners hinter dem Text fest.
 - h. Legen Sie im Feld Height die Höhe des Banners hinter dem Text fest.
 - i. Geben Sie im Feld URL den Hyperlink ein.
 - j. Klicken Sie auf Save.

Nachdem Sie eine neue Beschriftung gespeichert haben, erscheint die Beschriftung in der Beschriftungsliste.

1. Klicken und ziehen Sie eine Beschriftung aus der Beschriftungsliste an die gewünschte Position auf dem Lageplan.
2. Klicken Sie auf OK.

Um eine Beschriftung von einem Lageplan zu entfernen, klicken Sie mit der rechten Maustaste auf die Beschriftung, klicken Sie auf

Remove from Map
und klicken Sie auf
OK

.

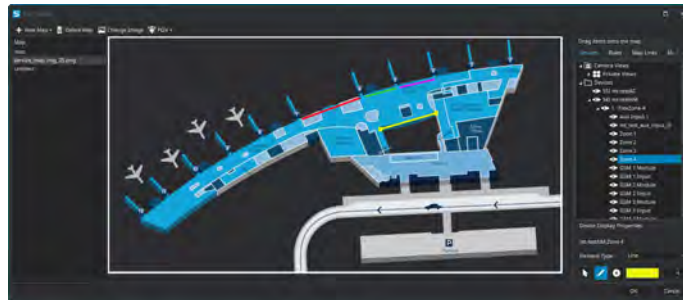
Alarmzone zu einem Lageplan hinzufügen

Sie können von Hardware-Knoten gemeldete Alarmzonen zu einem Lageplan hinzufügen.

Eine Zone erscheint als Linie auf dem Lageplan. Sie können die Position, Farbe und Stärke der Linie festlegen. Außerdem können Sie der Linie mehrere Segmente hinzufügen, um ihre Position genau darzustellen.

Wenn der Hardware-Knoten einen Zonenalarm meldet, wechselt die entsprechende Zone auf dem Lageplan in den Alarmzustand.

+



+

1. Klicken Sie in der Oberfläche des Windows Client auf View > Map Editor.
2. Wählen Sie einen Lageplan aus.
3. Klicken Sie auf die Registerkarte Devices.
4. Ziehen Sie eine Alarmzone auf den Lageplan.
5. Klicken Sie auf das Symbol für die Alarmzone.
6. Klicken Sie im Feld Element Type auf die Auslassungspunkte und klicken Sie auf Line. Das Symbol ändert sich zu einer Linie.
7. Um die Linie zu ändern, führen Sie eine der folgenden Aufgaben aus:
 - Um die Farbe der Linie zu ändern, wählen Sie die Linie aus, klicken Sie auf die Auslassungspunkte im Farbfeld, wählen Sie eine neue Farbe aus und klicken Sie auf OK.

- Um die Stärke der Linie zu ändern, wählen Sie die Linie aus und klicken Sie auf die Pfeile nach oben oder unten im Stärkefeld.
 - Um die Position oder Größe der Linie zu ändern, klicken und halten Sie den Endpunkt der Linie und verschieben Sie ihn an die neue Position.
8. Um der Zone ein Segment hinzuzufügen, führen Sie die folgenden Aufgaben aus:
- a. Klicken Sie auf das Stiftsymbol, um das Draw Tool zu aktivieren.
 - b. Bewegen Sie das Stiftsymbol zu einem Endpunkt einer vorhandenen Linie.
 - c. Klicken Sie auf den Endpunkt.
 - d. Bewegen Sie die Maus, um das neue Segment zu zeichnen, und klicken Sie, um das Segment zu beenden. Ein Endpunkt erscheint und ein neues Segment beginnt.
 - e. Wiederholen Sie Schritt d, um zusätzliche Segmente zu zeichnen.
 - f. Drücken Sie die ESC-Taste oder klicken Sie auf das Pfeilsymbol, um das Draw Tool zu deaktivieren.
9. Um ein Segment aus der Zone zu entfernen, führen Sie die folgenden Aufgaben aus:
- a. Klicken Sie auf das X-Symbol, um das Delete Tool zu aktivieren.
 - b. Bewegen Sie das X-Symbol zu einem Endpunkt einer vorhandenen Linie.
 - c. Klicken Sie auf den Endpunkt. Die mit dem Endpunkt verbundenen Segmente werden aus der Zone entfernt. Wenn der Endpunkt das Ende der Zone ist, wird das Segment entfernt. Wenn der Endpunkt eine Verbindung zwischen zwei Segmenten ist, werden beide Segmente entfernt und ein neues Segment erscheint zwischen den verbleibenden Endpunkten.
 - d. Wiederholen Sie Schritt c, um zusätzliche Segmente zu entfernen.
 - e. Drücken Sie die ESC-Taste oder klicken Sie auf das Pfeilsymbol, um das Delete Tool zu deaktivieren.
10. Klicken Sie auf OK.

Standortinformationen zu einem Lageplan hinzufügen

Sie können Standortinformationen hinzufügen, die auf einem Lageplan im Lageplan-Navigationsbereich in der Oberfläche des Windows Client erscheinen.

Um einem Lageplan Standortinformationen hinzuzufügen, fügen Sie eine Beschriftung hinzu und verwenden dann einen Inhaltseditor, um die Informationen einzugeben. Der Lageplaneditor in der Oberfläche des Windows Client enthält vier Felder für Standortinformationen, drei Größen für den Text und zwei Positionen für den Inhalt.

1. Klicken Sie in der Oberfläche des Windows Client auf View > Map Editor.
2. Wählen Sie einen Lageplan aus.
3. Klicken Sie auf die Registerkarte Map Properties.
4. Führen Sie im Bereich Site Information die folgenden Aufgaben aus:
 - a. Wählen Sie Display Site Information.
 - b. Geben Sie im Beschriftungsfeld eine Beschriftung für die Informationen ein.
 - c. Um den Inhaltseditor zu öffnen, klicken Sie auf die Auslassungspunkt-Schaltfläche.

- d. Geben Sie die Informationen ein, die Sie dem Lageplan hinzufügen möchten, und klicken Sie auf save.
 - e. Wählen Sie in der Liste Format Size die Schriftgröße aus.
 - f. Wählen Sie in der Liste Position aus, wo auf dem Lageplan die Informationen erscheinen sollen.
5. Klicken Sie auf OK.

Nachdem Sie einem Lageplan Standortinformationen hinzugefügt haben, erscheinen sie im Lageplan-Navigationsbereich in der

Oberfläche des Windows Client

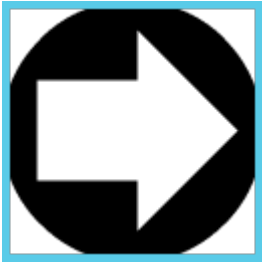
als

Site Information

- 1. Durch Klicken auf die Schaltfläche werden die Standortinformationen ein- (und aus-)geblendet.

Lageplan-Symbole

Symbol	Beschreibung
	Regel
	Digitaler Eingang • Aktiviert: gelber Hintergrund • Nicht aktiviert: weißer Hintergrund
	Digitaler Ausgang • Aktiviert: gelber Hintergrund • Nicht aktiviert: weißer Hintergrund

Symbol	Beschreibung
	Kamera • Online-Kamera: grauer Pfeil • Offline-Kamera: weißer Pfeil • Bewegung erkannt: blauer Pfeil • Alarm: oranger Pfeil • Ausgewählte Kamera: oranger Kreis
	PTZ-Kamera • Online-Kamera: grauer Pfeil • Offline-Kamera: weißer Pfeil • Bewegung erkannt: blauer Pfeil • Alarm: oranger Pfeil
	Zutrittskontrollgerät • Zutritt gewährt: grün • Zutritt verweigert: rot
	Senstar Symphony Access Control- und Senstar Network Manager-Geräte

Sichtfeld anzeigen

Sie können das Sichtfeld für Kameras auf Lageplänen in der Oberfläche des Windows Client anzeigen.

Wenn Sie das Sichtfeld für eine PTZ-Kamera anzeigen, ändert sich die Grafik auf dem Lageplan, wenn Sie die Kamera bewegen.

1. Klicken Sie in der Oberfläche des Windows Client auf View > Map Editor.
2. Wählen Sie einen Lageplan aus.
3. Klicken Sie auf FOV > Show FOV.
4. Um die Farbe der Sichtfeld-Grafik zu ändern, führen Sie die folgenden Aufgaben aus:
 - a. Klicken Sie auf FOV > Change Color.
 - b. Wählen Sie die Farbe mit der Farbauswahl aus oder definieren Sie die Farbe über die RGB-Werte oder Hex-Farbcodes.
 - c. Klicken Sie auf OK.
5. Klicken Sie auf OK.

Senstar Symphony Messenger

Mit dem Senstar Symphony Messenger können Sie Nachrichten an alle Benutzer senden, die beim Windows Client oder Web Client angemeldet sind.

Nachricht senden

Sie können Nachrichten an Benutzer oder Gruppen senden.

1. Klicken Sie in der Oberfläche des Windows Client auf Einstellungen > Messenger, um das Fenster Senstar Symphony Messenger zu öffnen.
2. Wählen Sie in der Benutzer- und Gruppenliste die Empfänger der Nachricht aus.
3. Geben Sie Ihre Nachricht in das Textfeld ein.
4. Klicken Sie auf Senden.

Sequenzen

Sequenzen können mehrere Kameras über mehrere Server in derselben Serverfarm durchlaufen und dabei für eine festgelegte Zeit auf jeder Kamera pausieren.

Sie können einem Video-Panel in der Oberfläche des Windows Client eine Sequenz zuweisen. Das Video-Panel durchläuft die Kameras automatisch und enthält Steuerelemente zum Pausieren und Vor- und Zurückbewegen durch die Kameras in der Sequenz.

Sie können eine Sequenz in der Konfigurationsoberfläche des Server erstellen. Nach der Erstellung erscheinen Sequenzen im Gerätebaum in der Oberfläche des Windows Client.

Sequenz hinzufügen

Fügen Sie eine Sequenz in der Konfigurationsoberfläche des Server hinzu.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Carousels.
2. Klicken Sie auf Add Carousel.
3. Geben Sie im Feld Name einen Namen für die Sequenz ein. Der Name der Sequenz erscheint im Gerätebaum in der

Oberfläche des Windows Client

.

1. Führen Sie eine der folgenden Aufgaben aus:
 - Wählen Sie Add to bottom of list, um Kameras am unteren Ende der Kameraliste der Sequenz hinzuzufügen.
 - Wählen Sie Insert below currently selected camera in list, um Kameras unterhalb der ausgewählten Kamera in der Kameraliste der Sequenz hinzuzufügen.
2. Wählen Sie in der Liste Available Cameras on Servers die Kameras aus, die in die Sequenz aufgenommen werden sollen, und klicken Sie auf Add Selected.
3. Führen Sie in der Kameraliste der Sequenz die folgenden Aufgaben aus:
 - a. Legen Sie die Reihenfolge der Kameras fest, indem Sie die Pfeilschaltfläche neben einer Kamera klicken und gedrückt halten, die Kamera an die gewünschte Position ziehen und die Maustaste loslassen.
 - b. Stellen Sie die Zeit ein, die die Sequenz auf der Kamera pausiert, bevor sie zur nächsten Kamera in der Sequenz wechselt.
4. Klicken Sie auf Save.

Sequenz bearbeiten

Bearbeiten Sie eine Sequenz in der Konfigurationsoberfläche des Server.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Carousels.
2. Wählen Sie die Sequenz aus und klicken Sie auf Edit.
3. Führen Sie eine der folgenden Aufgaben aus:
 - Um eine Kamera aus der Sequenz zu entfernen, fahren Sie mit dem Mauszeiger über die Kamera und klicken Sie auf die Schaltfläche X.
 - Um eine Kamera hinzuzufügen, wählen Sie die Kamera in der Liste Available Cameras on Servers aus und klicken Sie auf Add Selected.
 - Um die Zeit zu ändern, die die Sequenz bei der Kamera pausiert, bearbeiten Sie die Zahl im Feld Seconds.
4. Klicken Sie auf Save.

Sequenz löschen

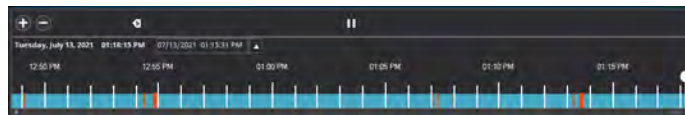
Entfernen Sie eine Sequenz in der Konfigurationsoberfläche des Server.

1. Klicken Sie in der Konfigurationsoberfläche des Server auf Devices > Carousels.
2. Wählen Sie die Sequenz aus.
3. Klicken Sie auf Delete.
4. Um den Löschvorgang zu bestätigen, klicken Sie auf Yes.

Zeitleiste

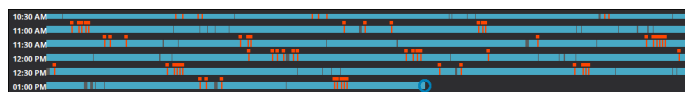
Eine Zeitleiste zeigt Aktivitäten und Alarmer für Kameras in der Oberfläche des Windows Client an. Der Windows Client enthält eine konsolidierte Zeitleiste, die Informationen von zahlreichen Kameras anzeigt, sowie eine Kamera-Zeitleiste, die Informationen von einer einzelnen Kamera anzeigt.

Die konsolidierte Zeitleiste zeigt Informationen von zahlreichen Kameras an und ist verfügbar, wenn Locked Times on Navigation aktiviert ist.



+

Die Kamera-Zeitleiste zeigt Informationen einer bestimmten Kamera an.



+

Sie können auf eine Zeitleiste klicken, um zu einem bestimmten Zeitpunkt oder Ereignis im Filmmaterial zu navigieren.

Zeitleisten-Farben

Die Oberfläche des Windows Client verwendet die folgenden Farben, um Ereignisse auf der Zeitleiste zu kennzeichnen.

Farbe	Ereignis
Dunkelblau (#005670)	Aktivität
Dunkelgrün (#008080)	Von der Kamera heruntergeladenes Video
Hellgelb (#FFFF00)	Zugriff verweigert
Weiß (#FFFFFF)	Zugriff gewährt
Rot (#FF0000)	Zugriff sonstiges Alarme
Grau (#5C5C5C)	Keine Aktivität
Dunkelgrau (#231F20)	Kein Signal
Hellgrau (#808080)	Nicht verwendet
Transparent (#00FFFFFF)	Keine Aufzeichnung
Hellblau (#59CBE8)	Zoom

Kamera-Zeitleiste anzeigen

Sie können eine Kamera-Zeitleiste anzeigen, um die Informationen für eine einzelne Kamera in einem Kameraansichts-Panel anzuzeigen.

- Um eine Kamera-Zeitleiste für eine einzelne Kamera einzuschalten, führen Sie die folgenden Schritte aus:
 - Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf ein Video-Panel.
 - Klicken Sie auf Show Timeline.
- Um die Kamera-Zeitleisten für alle Kameras in einer Ansicht einzuschalten, führen Sie die folgenden Schritte aus:
 - Klicken Sie in der Oberfläche des Windows Client auf Timeline.
 - Klicken Sie auf Show panels.

Die Kamera-Zeitleiste wird für die ausgewählten Kameras angezeigt.

Um eine Zeitleiste auszublenden, klicken Sie mit der rechten Maustaste auf das Video-Panel und klicken Sie erneut auf Show Timeline.

Konsolidierte Zeitleiste anzeigen

Sie können die konsolidierte Zeitleiste anzeigen, um Informationen aller Kameras in einer Ansicht anzuzeigen.

Um die konsolidierte Zeitleiste anzuzeigen, müssen Sie

Lock Times On Navigation

einschalten.

- Klicken Sie in der Oberfläche des Windows Client auf Timeline.

2. Klicken Sie auf Show consolidated.

Die konsolidierte Zeitleiste wird unten in der Kameraansicht angezeigt.

Anpassungen der Oberfläche

Sie können die Oberfläche des Windows Client auf verschiedene Weise anpassen, einschließlich der Änderung der Symbolleiste, der Anpassung von Anzeige- und regionalen Einstellungen, der Sperrung des Layouts und der Konfiguration, wie Alarme, Video und Ton dargestellt werden.

Symbolleiste

Passen Sie die Symbolleiste an, um die Befehle anzuzeigen, die Sie am häufigsten verwenden. Weitere Informationen finden Sie unter [Symbolleiste anpassen](#).

Einstellungen

Der Windows Client bietet Einstellungen, die das Erscheinungsbild und Verhalten der Oberfläche steuern, darunter:

- [Anzeigeeinstellungen](#)
- [Einstellungen anpassen](#)
- [Regionale Einstellungen](#)
- [Starteinstellungen](#)
- [Alarmeinstellungen](#)
- [Videoeinstellungen](#)
- [Toneinstellungen](#)

Layout

Sie können das Layout des Windows Client sperren, um Änderungen an der Anordnung der Ansichtspanel zu verhindern. Weitere Informationen finden Sie unter [Sperreinstellungen](#) und [Sperrzeiten](#).

Symbolleiste anpassen

Sie können die Symbole ändern, die in der Symbolleiste der Oberfläche des Windows Client angezeigt werden.

1. Klicken Sie in der Oberfläche des Windows Client auf den Pfeil nach unten.
2. Klicken Sie auf Add or Remove Buttons > Main Menu
3. Wählen Sie die Symbole aus, die zur Symbolleiste hinzugefügt oder daraus entfernt werden sollen.
4. Um die Symbolleiste auf die Standardeinstellung zurückzusetzen, klicken Sie auf Reset Toolbar und dann auf OK.

Mehrere Monitore

Sie können den Windows Client über mehrere Monitore an einer einzigen Arbeitsstation verwenden, sodass ein Bediener gleichzeitig mehr Video und Werkzeuge sehen kann.

Mehrere Monitore unterscheiden sich von einer Videowand. Eine Videowand ist eine verwaltete Anzeigefläche, auf die Bediener von jedem registrierten Windows Client aus Ansichten übertragen können. Mehrere Monitore sind einfach zusätzliche Bildschirme, die an die Arbeitsstation des Bedieners

angeschlossen sind.

Hauptfenster über Monitore strecken

1. Ziehen Sie das Hauptfenster des Windows Client so, dass es sich über die Monitore erstreckt.
2. Klicken Sie auf die Schaltfläche zum Maximieren.

Das Raster der Ansichts-Panels erweitert sich, um die neue Fenstergröße auszufüllen.

Schwebende Kameraansichten auf anderen Monitoren öffnen

Sie können schwebende Kameraansichten öffnen und auf einen beliebigen Monitor verschieben. Jede schwebende Ansicht ist unabhängig vom Hauptfenster.

1. Klicken Sie in der Oberfläche des Windows Client auf View > New Floating Camera View.
2. Ziehen Sie die schwebende Ansicht auf den gewünschten Monitor.
3. Fügen Sie der schwebenden Ansicht Kameras, Lagepläne, Alarmer oder andere Inhalte hinzu.

Weitere Informationen finden Sie im Thema [Schwebende Kameraansicht öffnen](#).

Mehrere Instanzen des Windows Client ausführen

Sie können mehr als eine Instanz des Windows Client an derselben Arbeitsstation ausführen, jede auf einem eigenen Monitor und jede mit demselben oder verschiedenen Servern verbunden.

1. Starten Sie den Windows Client.
2. Ziehen Sie das Fenster auf den ersten Monitor.
3. Starten Sie den Windows Client erneut über das Startmenü.
4. Ziehen Sie das zweite Fenster auf einen anderen Monitor.
5. Melden Sie sich in jeder Instanz an.



Jede Instanz verwendet ihre eigenen Ressourcen. Die Anzahl der Instanzen, die Sie ausführen können, wird durch die an der Arbeitsstation verfügbare CPU, GPU und Bandbreite begrenzt.

Video verwalten

Der Windows Client bietet Werkzeuge zum Anzeigen von Live- und aufgezeichnetem Video, zum manuellen Aufzeichnen von Video, zum Suchen nach Ereignissen, zum Exportieren von Video zur Verwendung außerhalb des Windows Client und zum Schützen von Video vor dem Löschen.

Videoexport

Der Windows Client bietet Funktionen zum Exportieren von Videos. Der Player kann das exportierte Video abspielen.

Standardmäßig umfasst der Videoexport die zwei Minuten Video vor dem Klick auf Exportieren (für die aktive Kamera) oder Alle exportieren (für alle Kameras in den Ansichts-Panels). Um Videos mit längerer Dauer zu exportieren, können Sie den Anfang und das Ende des Videos auf der Zeitleiste des Panels markieren.



Je länger das Video ist, das Sie exportieren möchten, desto länger dauert der

Exportvorgang im Windows Client.

Der Windows Client kann Videos in eine Datei oder zum Senstar Xnet exportieren, von wo aus Benutzer das Video herunterladen können. Der Export kann Videos einer oder mehrerer Kameras enthalten, und der Windows Client kann ein Zusammenfassungsvideo erzeugen, das das Video mit höherer Geschwindigkeit abspielt, um Ereignisse hervorzuheben.

Der Windows Client bietet außerdem Funktionen zum Anzeigen des Status von Videoexporten.

Video in die Cloud exportieren

Sie können Video aus dem Windows Client in die Cloud exportieren und einen Link zum Herunterladen des Videos erhalten.

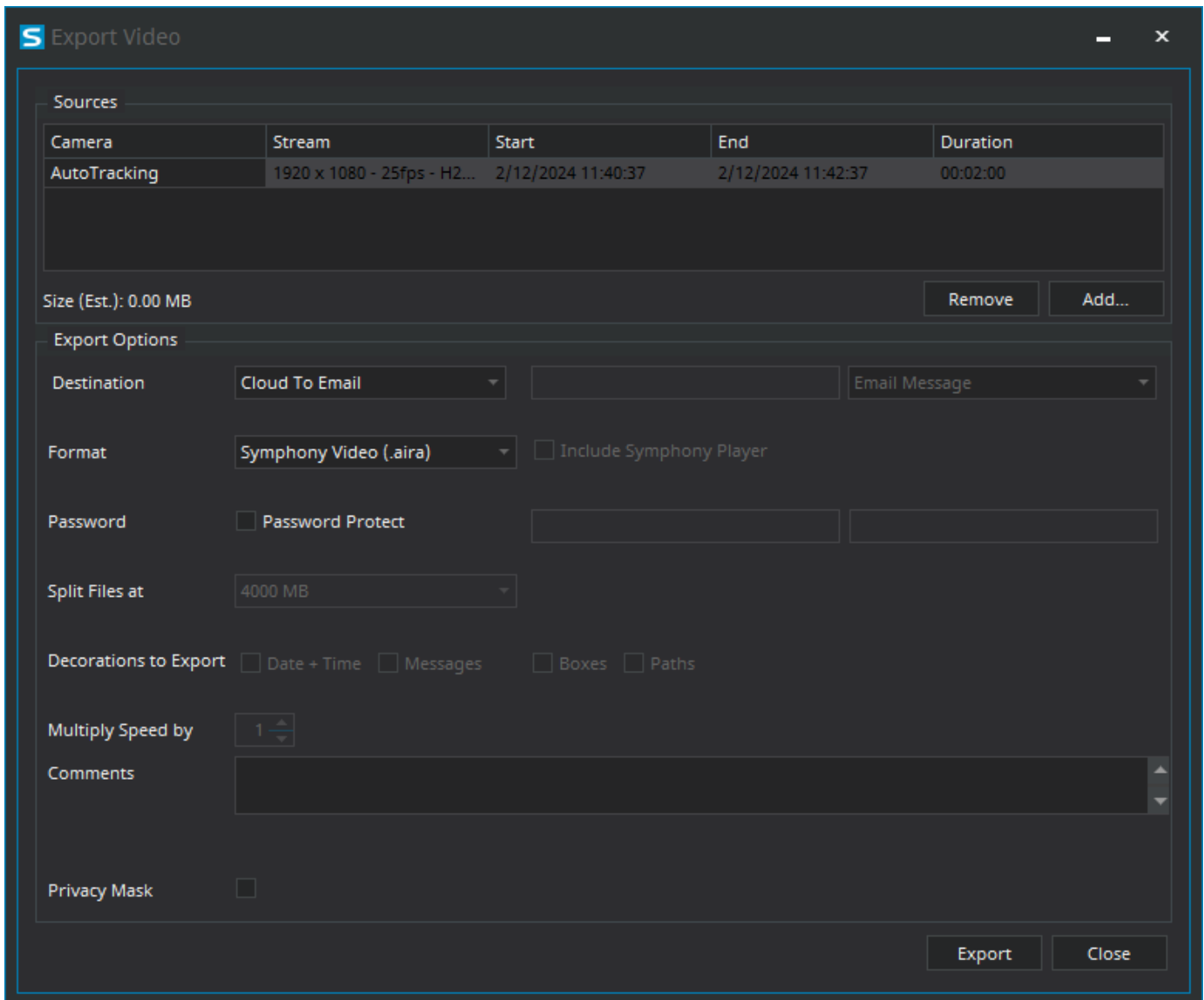
Um Video in die Cloud zu exportieren, müssen Sie eine E-Mail-Adresse mit Ihrem Senstar Symphony

-Benutzerkonto verknüpfen.

Der Windows Client lädt die Videodateien in das Senstar Xnet hoch und sendet eine E-Mail mit einem Link zum Herunterladen der Videodateien an die mit Ihrem Senstar Symphony-Benutzerkonto verknüpfte E-Mail-Adresse. Sie können den Link dann an andere Empfänger weiterleiten.

Beim Exportieren von Video in die Cloud teilt der Windows Client das Video in Dateien mit einer maximalen Größe von 4000 MB auf, schließt keine Dekorationen ein und unterstützt keine Erhöhung der Videogeschwindigkeit.

+



1. Führen Sie in der Oberfläche des Windows Client eine der folgenden Aufgaben aus:
 - Klicken Sie mit der rechten Maustaste auf das Ansichts-Panel und klicken Sie auf Export, um Video von der im Ansichts-Panel aktiven Kamera zu exportieren, oder auf Export All, um Video von allen Kameras zu exportieren, die in Ansichts-Panels aktiv sind.
 - Fahren Sie mit dem Mauszeiger über das Ansichts-Panel und klicken Sie auf das Symbol Export.
 - Klicken Sie mit der rechten Maustaste auf die Zeitleiste, um den Exportstart und das Exportende zu markieren, und klicken Sie auf Export, um Video von der im Ansichts-Panel aktiven Kamera zu exportieren, oder auf Export All, um Video von allen in Ansichts-Panels aktiven Kameras zu exportieren.
2. Um einen Kamera-Stream zum Export hinzuzufügen, führen Sie die folgenden Aufgaben aus:
 - a. Klicken Sie auf Add.
 - b. Wählen Sie die Kamera aus und klicken Sie auf Add.
 - c. Wählen Sie in der Quellenliste den Stream in der Spalte Stream aus.

- d. Ändern Sie bei Bedarf die Start- und Endzeit für den Export.
3. Wählen Sie in der Liste Destination den Eintrag Cloud To Email aus.
4. Um eine benutzerdefinierte Nachricht zur E-Mail hinzuzufügen, führen Sie die folgenden Aufgaben aus:
 - a. Klicken Sie in das Feld Email Message.
 - b. Geben Sie im Textfenster die E-Mail-Nachricht ein.
 - c. Klicken Sie auf OK.
5. Um die Videoexportdateien mit einem Kennwort zu schützen, führen Sie die folgenden Aufgaben aus:
 - a. Wählen Sie Password Protect.
 - b. Geben Sie das Kennwort ein und bestätigen Sie es.
6. Geben Sie im Feld Comments einen beliebigen Text ein, den Sie in die Textdatei einbeziehen möchten, die mit dem Videoexport verknüpft ist.
7. Um eine Privatsphärenmaske zum Videoexport hinzuzufügen, führen Sie die folgenden Aufgaben aus:
 - a. Wählen Sie Privacy Mask.
 - b. Zeichnen Sie im Bereich Privacy Mask die Privatsphärenmaske auf das Beispielbild.
8. Klicken Sie auf Export.

Der

Server

sendet Ihnen eine E-Mail mit einem Link zur Verwaltung Ihres exportierten Videos. Sie können den Link verwenden, um exportierte Videos zu löschen.

Sperrzeiten

Sie können in der Oberfläche des Windows Client Zeiten bei der Navigation sperren, damit alle Kameraansichts-Panels Video aus derselben Zeit anzeigen.

Wenn Sie beispielsweise vier Kameraansichts-Panels in der Oberfläche des Windows Client geöffnet haben und auf ein Lesezeichen für Video vom Vortag klicken, versuchen alle Kameras in den Kameraansichts-Panels, Video aus der Zeit des Lesezeichens anzuzeigen.

Das Sperren von Zeiten bei der Navigation unterstützt maximal vier Kameraansichts-Panels.

Klicken Sie in der Oberfläche des Windows Client auf das Symbol Lock Times On Navigation (Uhr).

Anzahl der gesperrten Kameraansichts-Panels anpassen

Sie können die maximale Anzahl der Kamera-Panels festlegen, auf die Sie die Funktion Lock Times On Navigation anwenden können.

Standardmäßig liegt die Grenze bei vier Ansichts-Panels für Kamera. Das Erhöhen der Grenze und das Anwenden der Funktion Lock Times On Navigation auf weitere Ansichts-Panels für Kamera erhöht die Systemressourcen, die der Windows Client verwendet.

1. Öffnen Sie die Datei acc.ini unter %appdata%\Senstar7.

2. Fügen Sie die folgenden Werte hinzu:

```
[VideoRecvCTRL]
LockTimesPanelLimit=number_of_panels
```

Wobei number_of_panels die maximale Anzahl der Ansichts-Panels für Kamera ist, bei denen Sie die Funktion Lock Times On Navigation verwenden können.

1. Speichern und schließen Sie die Datei acc.ini.

Lesezeichen

Ein Lesezeichen kennzeichnet bestimmte Aufnahmen, zu denen Sie später zurückkehren können. Lesezeichen können sich auf Live-Videos, aufgezeichnete Videos oder Standbilder beziehen.

Wenn Sie ein Lesezeichen hinzufügen, bezieht es sich auf das Video einer bestimmten Kamera zu einer bestimmten Zeit. Lesezeichen erscheinen in der Lesezeichenliste in der Oberfläche des Windows Client.

Lesezeichen erstellen

Sie können ein Lesezeichen erstellen, um auf Video von einer bestimmten Zeit und Kamera zu verweisen.

Wenn Sie ein Lesezeichen erstellen, wird eine Verbindung zur Kamera hergestellt, die zu dem Zeitpunkt, der im Anzeigebereich angezeigt wird, in der Oberfläche des Windows Client aktiv ist, wenn Sie das Lesezeichen erstellen.



Wenn Sie ein Lesezeichen für eine Kamera erstellen, die nicht aufzeichnet, können Sie später nicht mehr auf das Video zugreifen.

Sie können ein Lesezeichen freigeben, sodass andere Benutzer das von Ihnen markierte Video öffnen können.

1. Klicken Sie in der Oberfläche des Windows Client auf Bookmarks > Add Bookmark.
2. Geben Sie einen Namen für das Lesezeichen ein.
3. Wählen Sie aus, ob Sie das Lesezeichen für andere Benutzer freigeben möchten.
4. Klicken Sie auf OK.

Lesezeichen löschen

Sie können von Ihnen erstellte Lesezeichen entfernen.

1. Klicken Sie in der Oberfläche des Windows Client auf Bookmarks > Manage Bookmarks.
2. Wählen Sie Delete für das Lesezeichen aus.
3. Klicken Sie auf OK.

Visuelle Verfolgung

Mit der Funktion Visuelle Verfolgung können Sie Verknüpfungen zu Kameras hinzufügen, die das Kameraansichts-Panel automatisch zu einer benachbarten Kamera wechseln. Sie können diese

Funktion verwenden, um ein sich bewegendes Subjekt über mehrere Kameras hinweg zu verfolgen.

Verknüpfungen für die visuelle Verfolgung werden als transparente Overlays im Kameraansichts-Panel angezeigt. Die Verknüpfung enthält die Kamera-Identifikationsnummer der Kamera, zu der die Verknüpfung führt. Sie können sowohl die Position als auch die Form der Verknüpfungen zu benachbarten Kameras anpassen, um die Verknüpfungen in der Szene aussagekräftiger zu gestalten. Sie können beispielsweise die Position und Form einer Verknüpfung so anpassen, dass sie eine Tür abdeckt, die in einen Bereich der Szene der benachbarten Kamera führt.

Wenn Sie auf eine Verknüpfung der visuellen Verfolgung klicken, wechselt das Kameraansichts-Panel zu der Kamera, auf die die Verknüpfung verweist.

Link für visuelle Verfolgung hinzufügen

Sie können einem Ansichts-Panel für Kamera in der Oberfläche des Windows Client eine Verknüpfung für die visuelle Verfolgung hinzufügen.

1. Öffnen Sie in der Oberfläche des Windows Client die Kamera, zu der Sie die Verknüpfung für die visuelle Verfolgung hinzufügen möchten, in einem Ansichts-Panel für Kamera.
2. Halten Sie die Alt-Taste gedrückt.
3. Klicken Sie im Gerätebaum mit der linken Maustaste auf die Kamera, mit der Sie verknüpfen möchten, und halten Sie diese gedrückt.
4. Ziehen Sie die Zielkamera an die gewünschte Position.
5. Lassen Sie die Alt-Taste und die Maustaste los.
6. Um die Verknüpfung zu verschieben, führen Sie die folgenden Schritte aus:
 - a. Halten Sie die Alt-Taste gedrückt.
 - b. Klicken Sie auf die Verknüpfung.
 - c. Klicken Sie mit der linken Maustaste auf das Hand-Symbol und halten Sie es gedrückt.
 - d. Ziehen Sie die Verknüpfung an die gewünschte Position.
 - e. Lassen Sie die Alt-Taste und die Maustaste los.
7. Um die Form der Verknüpfung zu ändern, führen Sie die folgenden Schritte aus:
 - a. Halten Sie die Alt-Taste gedrückt.
 - b. Klicken Sie auf die Verknüpfung.
 - c. Klicken Sie mit der linken Maustaste auf einen Ankerpunkt und halten Sie ihn gedrückt.
 - d. Ziehen Sie den Ankerpunkt an die gewünschte Position.
 - e. Lassen Sie die Alt-Taste und die Maustaste los.

Aufnahmen schützen

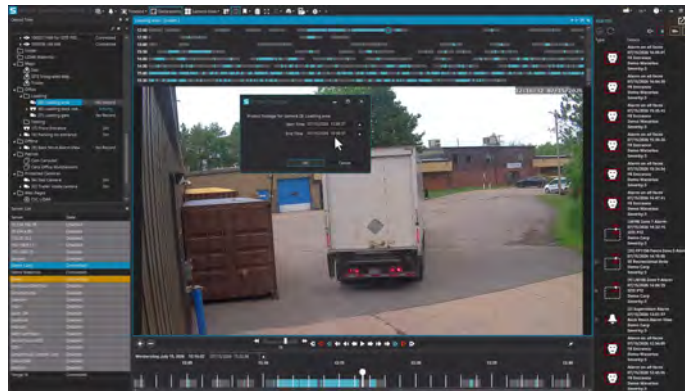
Sie können einen Abschnitt von aufgezeichnetem Video schützen, damit der Server ihn nicht löscht. Der Server schließt geschützte Aufnahmen von der automatischen Speicherbereinigung und den Aufbewahrungseinstellungen aus, und das Videomaterial verbleibt auf dem Server, bis ein Benutzer den Schutz aufhebt.

Schützen Sie Aufnahmen, um Video von Vorfällen und Ermittlungen zu bewahren, ohne das Video zu exportieren oder die Aufbewahrungseinstellungen zu ändern. Der Schutz gilt für eine bestimmte

Kamera und einen bestimmten Zeitbereich. Der Server zeichnet den Benutzer, der jeden Abschnitt schützt, und den Zeitpunkt des Schutzes auf.

Die Option Protect Footage ist nur verfügbar, wenn Ihre Gruppe über die Berechtigung Protect Footage verfügt. Weitere Informationen finden Sie unter [Geräteberechtigungen](#).

1. Wählen Sie in der Oberfläche des Windows Client eine Kamera im Gerätebaum aus.
2. Navigieren Sie mit der Zeitleiste zu den Aufnahmen, die Sie schützen möchten.
3. Klicken Sie mit der rechten Maustaste auf die Zeitleiste und wählen Sie Protect Footage.
4. Legen Sie im Fenster Protect Footage die Startzeit und die Endzeit für den zu schützenden Abschnitt fest.
5. Klicken Sie auf OK.



Wählen Sie den kürzesten Zeitbereich, der das Ereignis abdeckt. Der Server löscht geschützte Aufnahmen nicht automatisch, sodass große geschützte Abschnitte Speicherplatz belegen, bis ein Benutzer den Schutz aufhebt.

Administratoren können geschützte Aufnahmen auf der Seite Protected Footage in der Konfigurationsoberfläche des Server anzeigen und den Schutz aufheben, wenn das Videomaterial nicht mehr benötigt wird. Weitere Informationen finden Sie unter [Geschützte Aufnahmen](#) und [Aufnahmenschutz aufheben](#).

Aufgezeichnetes Video löschen

Sie können aufgezeichnetes Video für einen bestimmten Zeitraum oder das gesamte aufgezeichnete Video löschen.

1. Klicken Sie in der Oberfläche des Windows Client auf Server Configuration > Delete Recorded Video.
2. Führen Sie eine der folgenden Aufgaben aus:
 - Geben Sie einen Datumsbereich an und klicken Sie auf Delete Footage in Above Date Range On All Cameras.
 - Klicken Sie auf Delete everything.
3. Klicken Sie auf Yes.

Alarmer verwalten

Ein Alarm ist ein Ereignis mit hoher Priorität, das ausgelöst wird, wenn eine Videoanalyse oder ein integriertes Sicherheitsgerät (z. B. ein Zunsensor oder ein Zutrittskontrollleser) Bedingungen erkennt, die einer vordefinierten Regel entsprechen. Alarmer sind der Mechanismus, der das System von der passiven Überwachung zur aktiven Reaktion überführt: Sobald eine Regel einen Alarm auslöst, zeichnet das System ihn auf, zeigt ihn an und erwartet, dass ein Bediener ihn klassifiziert.

Alarmlebenszyklus

Jeder Alarm durchläuft dieselben Phasen. Es ist die Aufgabe eines Bedieners, ihn zügig durch diese zu bewegen.

1. **Ausgelöst** — eine Regel löst aus. Der Server zeichnet den Alarm auf, erfasst das umgebende Video (Vor- und Nach-Alarm-Dauer in der Regel festgelegt) und sendet ihn an den Windows Client.
2. **Angezeigt** — der Alarm wird in der Alarmkonsole, im Alarmer-Panel und auf Lageplänen und Zeitleisten gemäß Konfiguration angezeigt.
3. **Bestätigt** — ein Bediener übernimmt die Verantwortung und klassifiziert den Alarm. Bis zur Bestätigung verlangt der Alarm weiterhin Aufmerksamkeit (Audio, blinkende Anzeigen, Pop-ups).
4. **Gelöst** — alle Folgemaßnahmen (Entsendung, Bericht, Eskalation) sind abgeschlossen.
5. **Archiviert** — der Alarm wird in der Alarmedatenbank für spätere Abfragen und Berichte gespeichert.

Wenn kein Bediener innerhalb des konfigurierten Zeitlimits bestätigt (siehe [Alarmerinstellungen](#) und die zweistufigen Einstellungen der Regel), wird der Alarm eskaliert. Administratoren legen fest, was Eskalation für jede Regel bedeutet.

Alarmer anzeigen

Je nach Konfiguration des Standorts zeigt der Windows Client Alarmer gleichzeitig an mehreren Stellen an. Ein Bediener beobachtet während der aktiven Überwachung in der Regel die Alarmkonsole und verlässt sich auf die anderen Anzeigen als Hintergrundsignale.

Ort	Was angezeigt wird
Alarmer-Panel	Live-Liste unbestätigter Alarmer in der aktuellen Ansicht. Klicken Sie auf einen Alarm, um zur zugehörigen Kamera zu springen.
Alarmkonsole	Der primäre Arbeitsbereich für die Reaktion auf Alarmer. Enthält die Alarmliste, das Video des Vorfalls, alle Anweisungen, die Administratoren der Regel angehängt haben, und die Bestätigungssteuerelemente.
Zeitleistenanzeige	Farbige Markierungen auf der Zeitleiste zeigen, wann Alarmer für die ausgewählte Kamera aufgetreten sind. Nützlich bei Untersuchungen.
Blinken des Video-Panels	Ein Ansichts-Panel kann seinen Rahmen blinken lassen, wenn die zugehörige Kamera einen Alarm auslöst. Konfigurieren Sie dies in Ansichts-Panels .
Blinken von Lageplan-Symbolen/-Linien	Symbole und Zonen auf einem Lageplan blinken, wenn das entsprechende Gerät einen Alarm auslöst.
Pop-up-Fenster	Optionales Pop-up, das einen eingehenden Alarm unabhängig vom aktuellen Arbeitsbereich anzeigt. Konfigurieren Sie dies in Alarmerinstellungen .
Gerätebaum-Status	Der Gerätebaum zeigt den Alarmstatus jedes Geräts als Symbol-Overlay an.

Auf Alarme reagieren

Es ist die Aufgabe eines Bedieners, einen Alarm zu bestätigen und korrekt zu klassifizieren. Die Klassifizierung steigert die Genauigkeit der Berichte und, bei Regeln, die sie verwenden, die nachgelagerte Automatisierung.

Bestätigen

Siehe [Alarm bestätigen](#) für die schrittweise Anleitung. Auf hoher Ebene:

1. Öffnen Sie den Alarm in der [Alarmkonsole](#).
2. Sehen Sie sich den Videoclip an (das Vor-Alarm-Material zeigt, was zur Auslösung führte).
3. Lesen Sie alle Anweisungstexte, die der Regel angehängt sind.
4. Klassifizieren Sie den Alarm (siehe unten).
5. Fügen Sie einen Kommentar hinzu, der beschreibt, was Sie gesehen und getan haben.

Klassifizieren

Die Klassifizierung ist eine Ermessensentscheidung. Die typischen Optionen und wann Sie sie verwenden:

Klassifizierung	Verwenden, wenn
Echter Alarm	Das Ereignis trat wie von der Regel beabsichtigt auf, und jemand (Sicherheitspersonal, Polizei, Standortpersonal) hat darauf reagiert.
Echte Maßnahme erforderlich	Das Ereignis trat wie beabsichtigt auf, und Sie haben die erforderliche Maßnahme selbst ergriffen (einen Wachmann entsandt, eine Tür verriegelt, einen Fahrer kontaktiert).
Falscher Alarm	Das Ereignis entsprach nicht der Absicht der Regel — Wetter, Beleuchtung, ein Tier, ein bekanntes Fahrzeug oder ein Abstimmungsproblem verursachten die Auslösung.

Wenn Sie wiederholt falsche Alarme von derselben Regel oder Kamera bemerken, melden Sie dies einem Administrator. Dauerhaft falsche Alarme deuten in der Regel auf eine Abstimmung der [Bewegungserkennung](#) oder einen Schwellenwert einer [Videoanalyse](#) hin, der angepasst werden muss.

Teilen oder eskalieren

Wenn der Alarm die Aufmerksamkeit eines Kollegen erfordert — eines anderen Bedieners, eines Vorgesetzten oder eines Spezialisten — verwenden Sie [Alarm teilen](#), um ihn weiterzuleiten. Beim Teilen bleiben der Bestätigungsstatus und die angehängten Kommentare erhalten.

Alarme konfigurieren

Administratoren konfigurieren Alarme auf dem Server. Ein Alarm ist einfach eine [Regel](#), deren Aktionssatz die Aktion „Alarm erstellen“ enthält.

- [Regeln](#) — das Modell: Ereignis + Aktionssatz + Zeitplan + Schweregrad.
- [Regel erstellen](#) — erstellen Sie eine Regel, die einen Alarm auslöst.
- [Ereignisse](#) — die verfügbaren Auslöser (Bewegung, Analyseerkennung, Integrationsereignis, digitaler Eingang usw.).
- [Aktionssätze](#) — was passiert, wenn die Regel auslöst (Aufzeichnen, Alarm, E-Mail, Ausgang usw.).
- [Zeitpläne](#) — wann die Regel aktiv ist (immer, Geschäftszeiten, außerhalb der Geschäftszeiten, benutzerdefiniert).

Auf Seiten des Windows Client stimmen Bediener das Erscheinungsbild von Alarmen mithilfe der **Alarmeinstellungen** und **Toneinstellungen** ab.

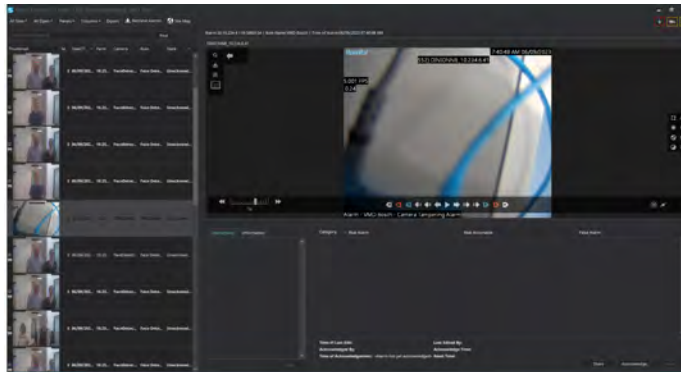
Alarmkonsole

Die Alarmkonsole im Windows Client bietet Funktionen zum Anzeigen und Verwalten von Alarmen.

Die Alarmkonsole erscheint in der Oberfläche des Windows Client standardmäßig als zusammenklappbare Seitenleiste. In der Seitenleiste zeigt die Alarmkonsole eine Liste von Alarmen an, die ein Symbol zur Veranschaulichung des Alarmtyps und Alarmdetails enthält. Durch Klicken auf einen Alarm in der Liste wird das Alarmvideo im aktiven Ansichts-Panel für Kamera angezeigt. Die Alarmkonsole enthält Schaltflächen zum Bestätigen und Zurücksetzen von Alarmen (für zweistufige Alarme) sowie Zähler zur Anzeige der Anzahl und des Typs der Alarme.

Die Alarmkonsole enthält außerdem einen erweiterten Modus, der die Alarmkonsole in einem eigenen Fenster öffnet. Im erweiterten Modus enthält die Alarmkonsole zusätzliche Funktionen zum Filtern, Exportieren und Verwalten von Alarmen. Wenn sich die Alarmkonsole im erweiterten Modus befindet, erscheint sie nicht als Seitenleiste in der Oberfläche des Windows Client.

+



+

Die erweiterte Alarmkonsole umfasst die folgenden Komponenten:

- Alarmliste
 - Zeigt die Alarme an, die Ihren Auswahlkriterien entsprechen
- Ansichts-Panels
 - Zeigt ein bis vier Ansichts-Panels in der erweiterten Alarmkonsole an (Konfiguration auf der Seite Action Sets in der Konfigurationsoberfläche des Server)
- Anweisungsbereich
 - Zeigt Anweisungen (als Text oder angehängte Datei) für den Alarm an (Anweisungen werden auf der Seite Action Sets in der Konfigurationsoberfläche des Server definiert)
 - Wenn Sie eine Datei hinzufügen, können Sie die Datei vergrößern, indem Sie die STRG-Taste gedrückt halten und das Mausrad verwenden
- Informationsbereich
 - Zeigt zusätzliche Informationen über den Alarm aus Zutrittskontrollsystemen oder dem Senstar Network Manager an

- Bestätigungsbereich
 - Alarm freigeben, bestätigen oder zurücksetzen
 - Einen Alarm als echt, echt zu bearbeiten oder falsch markieren
 - Mit dem Alarm verknüpfte Kommentare hinzufügen oder anzeigen
 - Zeigt Informationen und Alarmbearbeitung an

Alarmer anzeigen

Sie können die Liste der Alarmer verfeinern, die in der erweiterten Alarmkonsole angezeigt werden.

1. Klicken Sie in der Oberfläche des Windows Client auf Erweiterter Modus, um die erweiterte Alarmkonsole zu öffnen.
2. Wählen Sie in der Liste der Standorte die Standorte aus, von denen Sie Alarmer anzeigen möchten.
3. Wählen Sie in der Liste der Typen aus, welche Art von Alarmen Sie anzeigen möchten.
4. Wählen Sie in der Liste der Bedienfelder aus, ob Sie ein Ansichts-Panel oder vier Ansichts-Panels anzeigen möchten.
5. Wählen Sie in der Spaltenliste aus, welche Spalten Sie in der Alarmliste anzeigen möchten.

Während Sie Änderungen vornehmen, wird die Alarmliste aktualisiert, um Alarmer einzubeziehen, die mit den von Ihnen ausgewählten Parametern übereinstimmen.

Alarmer abrufen

Sie können Alarmer für Daten abrufen, die nicht in der Alarmliste enthalten sind.

Je nachdem, wie Sie die Alarmliste sortieren, werden die abgerufenen Alarmer möglicherweise nicht oben in der Liste angezeigt.

1. Klicken Sie in der Oberfläche des Windows Client auf Erweiterter Modus, um die erweiterte Alarmkonsole zu öffnen.
2. Klicken Sie auf Alarmer abrufen.
3. Wählen Sie ein Datum aus.

Die Alarmliste in der erweiterten Alarmkonsole

zeigt die Alarmer für das ausgewählte Datum an.

Alarmliste exportieren

Sie können Alarmer aus der Oberfläche des Windows Client exportieren.

Beim Exportieren von Alarmen unterstützt der Server die folgenden Formate:

- PDF
- HTML
- MHT
- RTF
- DOCX

- XLS
 - XLSX
 - CSV
 - Text
 - Bild
1. Klicken Sie in der Oberfläche des Windows Client auf Advanced Mode, um die erweiterte Alarmkonsole zu öffnen.
 2. Filtern und sortieren Sie die Alarme, bis Sie die gewünschte Liste zum Exportieren erhalten.
 3. Klicken Sie auf Export. Die Zeit, die der

Server

zum Verarbeiten der Exportdatei benötigt, steigt mit der Anzahl der zu exportierenden Alarme.

1. Klicken Sie im Vorschaufenster auf File > Export Document.
2. Klicken Sie auf das Dateiformat.
3. Geben Sie die Optionen für die Ausgabe an und klicken Sie auf OK.
4. Wählen Sie im Fenster Save As den Speicherort für die Datei aus und klicken Sie auf Save.

Alarm freigeben

Sie können einen Alarm mit jedem Benutzer teilen, der am Windows Client angemeldet ist.

Wenn Sie einen Alarm mit einem Benutzer teilen, zeigt der Windows Client dem Benutzer eine Nachricht in der Oberfläche des Windows Client an.

1. Klicken Sie in der Seitenleiste der Alarmkonsole auf Erweiterter Modus.
2. Wählen Sie den Alarm aus.
3. Klicken Sie auf Teilen.
4. Wählen Sie im Fenster Ereignis teilen einen Benutzer aus.
5. Klicken Sie auf Teilen.

Alarm bestätigen

Sie können einen Alarm bestätigen, um den Alarm während der Bearbeitung für sich zu beanspruchen.

Wenn die zweistufige Alarmbearbeitung aktiviert ist, beanspruchen Sie den Alarm, indem Sie ihn bestätigen, sodass Sie den Alarm bearbeiten können. Wenn die erweiterte zweistufige Alarmbearbeitung aktiviert ist, kann ein Benutzer mit höherer Priorität (in der Konfigurationsoberfläche des Server festgelegt) den Alarm von einem Benutzer mit niedrigerer Priorität übernehmen.

Sie haben bis zum Ablauf des Bestätigungs-Timeouts (in der Konfigurationsoberfläche des Server festgelegt) Zeit, ihn zu bearbeiten. Sobald das Bestätigungs-Timeout abgelaufen ist, kehrt der Alarm in den unbestätigten Zustand zurück.

1. Klicken Sie in der Seitenleiste der Alarmkonsole auf Advanced Mode.
2. Wählen Sie den Alarm aus.
3. Klicken Sie auf Acknowledge.

4. Um die mit dem Alarm verknüpften Anweisungen anzuzeigen, klicken Sie auf die Registerkarte Instructions.
5. Um Standortinformationen anzuzeigen, klicken Sie auf die Registerkarte Information.
6. Wählen Sie den Typ des Alarms aus.
 - Real Alarm
 - Real Actionable
 - False Alarm
7. Geben Sie alle Kommentare ein, die Sie dem Alarm hinzufügen möchten.
8. Klicken Sie auf Reset, um den Alarm zu schließen und zu archivieren.

Client-Optionen

Alarmer deaktivieren

Sie können Alarmer auf Kamera-/Geräte- oder Serverebene deaktivieren, wenn Ihr Konto über die erforderlichen Berechtigungen verfügt.



Beim Deaktivieren von Alarmen werden von einer Kamera erzeugte Alarmer ausgeblendet. Um von einem Gerät erzeugte Alarmer auszublenden, siehe Abschnitt Mask.

Alarmer für eine Kamera deaktivieren

Sie können die Alarmer für eine Kamera im Windows Client deaktivieren.

1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf eine Kamera im Gerätebaum.
2. Klicken Sie auf Disable Alarms for Camera.
3. Geben Sie die Zeit (in Minuten) an, für die die Alarmer deaktiviert werden.
4. Klicken Sie auf OK.

Um den Alarm wieder zu aktivieren, klicken Sie mit der rechten Maustaste auf die Kamera und klicken Sie auf Enable Alarms for Camera.

Alarmer für einen Server deaktivieren

Sie können die Alarmer für Kameras auf dem Server deaktivieren, mit dem der Windows Client verbunden ist.

1. Klicken Sie in der Oberfläche des Windows Client auf Alarms > Disable Alarms for Server.
2. Geben Sie die Anzahl der Minuten an, für die die Alarmer deaktiviert werden sollen.
3. Klicken Sie auf OK.

Um Alarmer manuell zu aktivieren, ohne auf den Ablauf der Zeit zu warten, klicken Sie auf Alarms > Enable Alarms for Server.

Einstellungen

Sie können die Einstellungen im Windows Client verwenden, um die Oberfläche des Windows Client anzupassen.

Kameraaktivität anzeigen

Sie können die Aktivität für mehrere Kameras anzeigen und Kameraansichts-Panels für bestimmte Zeiten aus der Zeitleiste jeder Kamera öffnen.

Durch das Anzeigen der Kameraaktivität können Sie die Zeitleisten vergleichen und Aktivitäten über mehrere Kameras hinweg verfolgen. Sie können Videos aus unterschiedlichen Zeiten und von verschiedenen Kameras öffnen, um das vollständige Video für eine Aktivität oder einen Alarm anzuzeigen.

1. Klicken Sie in der Oberfläche des Windows Client auf Ansicht > Aktivität für Kameras.
2. Geben Sie das Start- und Enddatum für die anzuzeigende Aktivität an und klicken Sie auf Neu laden.
3. Wählen Sie in der Liste Kameras auswählen die Kameras aus, für die Sie die Aktivität anzeigen möchten.
4. Verwenden Sie Hineinzoomen und Herauszoomen, um die richtige Auflösung einzustellen.
5. Führen Sie eine der folgenden Aufgaben aus:
 - Um bei jedem Klick auf eine Kamera-Zeitleiste das Video in einem einzelnen angedockten Kameraansichts-Panel zu öffnen, schalten Sie die Schaltfläche Eine Kameraansicht ein.
 - Um bei jedem Klick auf eine Kamera-Zeitleiste das Video in einem neuen freischwebenden Kameraansichts-Panel zu öffnen, schalten Sie die Schaltfläche Eine Kameraansicht aus.
6. Klicken Sie auf eine Kamera-Zeitleiste, um Video anzuzeigen.

Symbolleiste anpassen

Sie können Symbole zur Symbolleiste in der Oberfläche des Windows Client hinzufügen oder daraus entfernen.

1. Klicken Sie auf den Pfeil nach unten in der Symbolleiste.
2. Klicken Sie auf Add or Remove Buttons > Main Menu.
3. Klicken Sie, um die Schaltflächen anzuzeigen oder auszublenden, oder klicken Sie auf Reset Toolbar.

Zeitleisten-Farben ändern

Sie können die Farben ändern, die der Windows Client in der Zeitleiste verwendet.

Wenn Sie die Farben der Zeitleiste ändern, ändern Sie auch die Farben, die der Windows Client für Lageplansymbole verwendet.

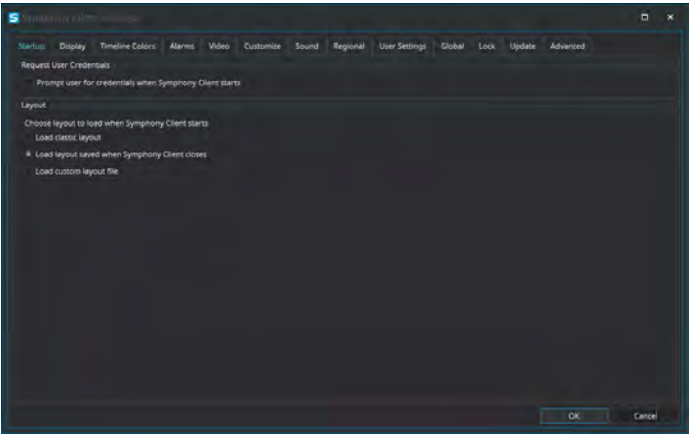
1. Klicken Sie in der Oberfläche des Windows Client auf View > Settings.
2. Klicken Sie auf die Registerkarte Timeline Colors.
3. Wählen Sie die Farben für jedes Zeitleistenereignis aus.
4. Klicken Sie auf OK.

Sie können die Farben auch jederzeit auf die Standardfarben zurücksetzen oder die klassischen Farben aus Senstar Symphony 6.14 verwenden.

Starteinstellungen

Die Starteinstellungen legen das Verhalten des Windows Client beim Start fest.

+



+

Benutzeranmeldedaten anfordern

Einstellung	Beschreibung
Benutzer beim Start des Windows Client zur Eingabe von Anmeldedaten auffordern	Auswählen, damit Benutzer einen gültigen Benutzernamen und ein gültiges Kennwort eingeben müssen, bevor sie den Windows Client verwenden können.

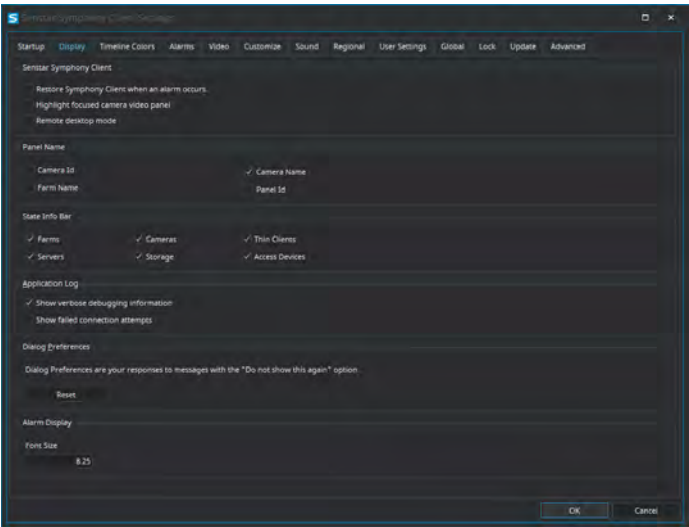
Layout

Einstellung	Beschreibung
Klassisches Layout laden	Auswählen, um beim Start des Windows Client das Standardlayout zu laden.
Layout laden, das beim Schließen des Windows Client gespeichert wurde	Auswählen, um beim Start des Windows Client das Layout der letzten Sitzung zu laden.
Benutzerdefinierte Layoutdatei laden	Auswählen, um beim Start des Windows Client das Layout aus einer gespeicherten Layoutdatei zu laden.

Anzeigeeinstellungen

Die Anzeigeeinstellungen bestimmen, welche Informationen der Windows Client anzeigt und was in Protokolldateien enthalten ist.

+



+

Windows Client

Einstellung	Beschreibung
Restore Windows Client when an alarm occurs	Wählen Sie diese Option, um die Oberfläche des Windows Client bei einem Alarm in voller Größe wiederherzustellen.
Highlight focused camera video panel	Wählen Sie diese Option, um das fokussierte Kameraansichts-Panel hervorzuheben.
Remote desktop mode	Wählen Sie diese Option, wenn Sie einen Remotedesktop oder eine virtuelle Maschine verwenden, um auf den Windows Client zuzugreifen. Diese Einstellung entfernt die Abhängigkeit von Overlays und Navigationssteuerelementen in der Oberfläche des Windows Client von DirectX.

Panelname

Einstellung	Beschreibung
Camera Id	Wählen Sie diese Option, um die Kamera-ID im Namen des Kameraansichts-Panels anzuzeigen.
Farm Name	Wählen Sie diese Option, um den Farmnamen im Namen des Kameraansichts-Panels anzuzeigen.
Camera Name	Wählen Sie diese Option, um den Kameranamen im Namen des Kameraansichts-Panels anzuzeigen.
Panel Id	Wählen Sie diese Option, um die Panel-ID im Namen des Kameraansichts-Panels anzuzeigen.

Statusinformationsleiste

Einstellung	Beschreibung
Farms	Wählen Sie diese Option, um Warnmeldungen für Farmen in der Benachrichtigungsleiste anzuzeigen.
Servers	Wählen Sie diese Option, um Warnmeldungen für Server in der Benachrichtigungsleiste anzuzeigen.

Einstellung	Beschreibung
Cameras	Wählen Sie diese Option, um Warnmeldungen für Kameras in der Benachrichtigungsleiste anzuzeigen.
Storage	Wählen Sie diese Option, um Warnmeldungen für die Videospeicherung in der Benachrichtigungsleiste anzuzeigen.
Senstar Thin Clients	Wählen Sie diese Option, um Warnmeldungen für Senstar-Thin-Client-Geräte in der Benachrichtigungsleiste anzuzeigen.
Access Devices	Wählen Sie diese Option, um Warnmeldungen für Zutrittskontrollgeräte in der Benachrichtigungsleiste anzuzeigen.

Anwendungsprotokoll

Einstellung	Beschreibung
Show verbose debugging information	Wählen Sie diese Option, um ausführliche Debugging-Informationen im Anwendungsprotokoll anzuzeigen.
Show failed connection attempts	Wählen Sie diese Option, um fehlgeschlagene Verbindungsversuche im Anwendungsprotokoll anzuzeigen.

Dialogeinstellungen

Einstellung	Beschreibung
Reset	Klicken Sie hier, um alle ausgeblendeten Dialogfelder in der Oberfläche des Windows Client zurückzusetzen.

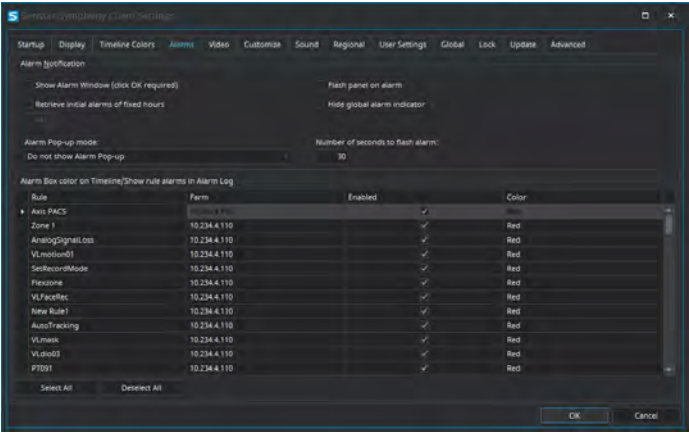
Alarmanzeige

Einstellung	Beschreibung
Font Size	Wählen Sie die Größe (in Pixel) der Schriftart in der Alarmkonsole aus.

Alarmeinstellungen

Die Alarmeinstellungen legen fest, wie Alarme im Windows Client angezeigt werden.

+

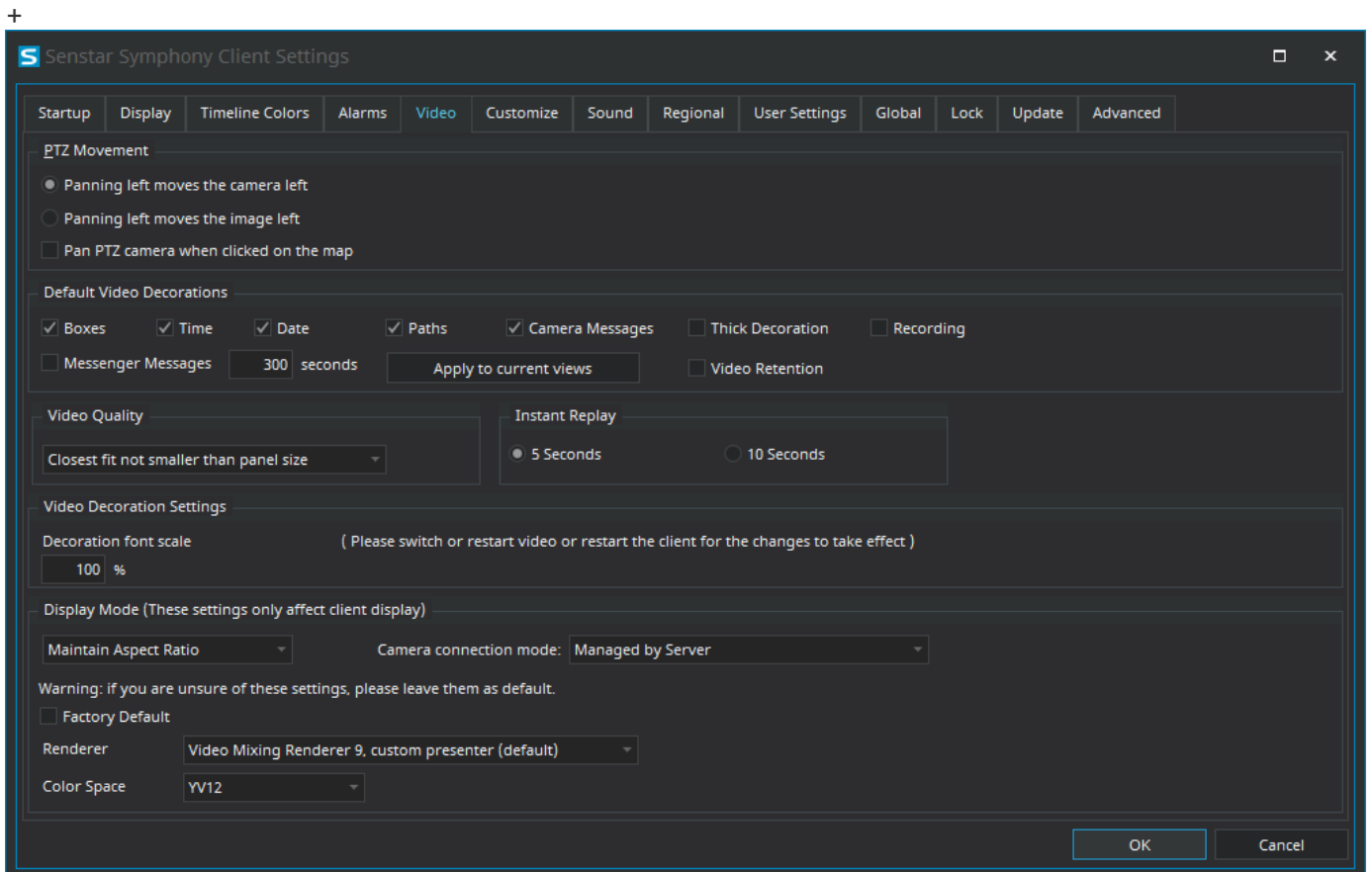


+

Einstellung	Beschreibung
Show Alarm Window (click OK required)	Wählen Sie diese Option aus, damit der Windows Client ein Dialogfeld anzeigt, wenn ein Alarm auftritt.
Retrieve initial alarms of fixed hours	Wählen Sie diese Option aus, um Alarme aus dem Zeitraum abzurufen, den Sie im darunter liegenden Stundenfeld angeben (1 bis 24 Stunden).
Alarm Pop-up mode	Wählen Sie aus, wie der Windows Client Alarm-Dialogfelder anzeigt.
Flash panel on alarm	Wählen Sie diese Option aus, um einen Alarmindikator um Ansichts-Panels für Kamera anzuzeigen, wenn Kameras Alarme aufzeichnen.
Hide global alarm indicator	Wählen Sie diese Option aus, um die farbigen Alarmindikatoren in der Oberfläche des Windows Client auszublenden.
Number of seconds to flash alarm	Geben Sie an, wie lange der Alarmindikator blinkt, wenn Kameras Alarme aufzeichnen. Der Alarmindikator blinkt, bis die Zeit abläuft oder Sie den Alarm bestätigen.
Alarm Box color on Timeline/Show rule alarms in Alarm Log	Wählen Sie aus, ob der Alarm im Alarmprotokoll erscheint, und legen Sie die Farbe für den Alarm in der Zeitleiste fest.

Videoeinstellungen

Die Videoeinstellungen legen das Verhalten von PTZ-Kameras, das Erscheinungsbild der Videodekos, die Sofortwiedergabe und die Eigenschaften von Videos im Windows Client fest.



PTZ-Bewegung

Einstellung	Beschreibung
Schwenken nach links bewegt die Kamera nach links	Auswählen, um die Standardrichtungen für die Schwenkschaltflächen zu verwenden (d. h. die Schaltfläche zum Schwenken nach links schwenkt die Kamera nach links und/oder schwenkt das Bild digital nach rechts).
Schwenken nach links bewegt das Bild nach links	Auswählen, um die invertierten Richtungen für die Schwenkschaltflächen zu verwenden (d. h. die Schaltfläche zum Schwenken nach links schwenkt die Kamera nach rechts und/oder schwenkt das Bild digital nach links).
PTZ-Kamera schwenken, wenn auf den Lageplan geklickt wird	Auswählen, um PTZ-Kameras an die Stelle zu schwenken, auf die Sie auf einem Lageplan klicken.

Standard-Videodekos

Einstellung	Beschreibung
Rahmen	Auswählen, um Videoanalyse-Rahmen über dem Video im Kameraansichts-Panel anzuzeigen.
Zeit	Auswählen, um die Uhrzeit über dem Video im Kameraansichts-Panel anzuzeigen.
Datum	Auswählen, um das Datum über dem Video im Kameraansichts-Panel anzuzeigen.
Pfade	Auswählen, um Videoanalyse-Pfade über dem Video im Kameraansichts-Panel anzuzeigen.
Kameranachrichten	Auswählen, um Informationen von Kameras über dem Video im Kameraansichts-Panel anzuzeigen.
Dicke Dekos	Auswählen, um die Videoanalyse-Dekos (Rahmen und Pfade) dicker darzustellen.
Aufnahme	Auswählen, um anzuzeigen, wann der Windows Client aufzeichnet.
Videoaufbewahrung	Auswählen, um die Kapazität der Videoaufbewahrung über dem Video im Kameraansichts-Panel anzuzeigen.
Messenger-Nachrichten	Auswählen, um Nachrichten aus dem Senstar Symphony Messenger über dem Video im Kameraansichts-Panel anzuzeigen.
Sekunden	Wählen Sie aus, wie lange die Nachrichten sichtbar bleiben.
Auf aktuelle Ansichten anwenden	Klicken, um die Deko-Einstellungen auf die aktuellen Ansichten anzuwenden.

Videoqualität

Einstellung	Beschreibung
Niedrigste Auflösung	Auswählen, um Videos in der niedrigstmöglichen Auflösung anzuzeigen.
Beste Anpassung an Panelgröße	Auswählen, um Videos in der Auflösung anzuzeigen, die der Größe des Video-Panels am ehesten entspricht, einschließlich Auflösungen, die kleiner als das Video-Panel sind.
Beste Anpassung nicht kleiner als Panelgröße	Auswählen, um Videos in der Auflösung anzuzeigen, die der Größe des Video-Panels am ehesten entspricht, ohne Auflösungen, die kleiner als das Video-Panel sind.

Einstellung	Beschreibung
Höchste Auflösung	Auswählen, um Videos in der höchstmöglichen Auflösung anzuzeigen.

Sofortwiedergabe

Einstellung	Beschreibung
5 Sekunden	Auswählen, um die Sofortwiedergabe-Funktion auf 5 Sekunden einzustellen.
10 Sekunden	Auswählen, um die Sofortwiedergabe-Funktion auf 10 Sekunden einzustellen.

Videodeko-Einstellungen

Einstellung	Beschreibung
Dekos-Schriftskalierung	Definiert die Größe des Textes in Video-Panels.

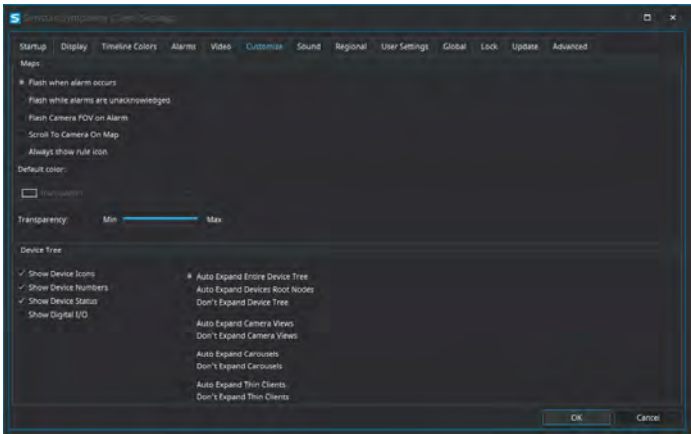
Anzeigemodus

Einstellung	Beschreibung
Tatsächliche Größe	Auswählen, damit das Video-Panel das Video in der Größe der Kamera anzeigt.
Seitenverhältnis beibehalten	Auswählen, damit das Video-Panel das Video im richtigen Seitenverhältnis anzeigt.
An Fenster anpassen	Auswählen, um das Video an das Video-Panel anzupassen.
Kameraverbindungsmodus	Wählen Sie aus, wie der Windows Client eine Verbindung zu Kameras herstellt.
Werkseinstellung	Auswählen, um den Standard-Videorenderer zu verwenden.
Renderer	Wählen Sie einen Videorenderer aus.
Farbraum	Wählen Sie den Farbraum für den Windows Client aus.

Anpassungseinstellungen

Die Einstellungen unter Anpassen bestimmen das Erscheinungsbild und Verhalten von Lageplänen und des Gerätebaums im Windows Client.

+



+

Lagepläne

Einstellung	Beschreibung
Flash when alarm occurs	Wählen Sie diese Option, damit das Alarmsymbol auf einem Lageplan blinkt, wenn ein Alarm auftritt.
Flash while alarms are unacknowledged	Wählen Sie diese Option, damit das Alarmsymbol blinkt, solange der Alarm nicht bestätigt ist.
Flash Camera FOV on Alarm	Wählen Sie diese Option, damit das Sichtfeld der Kamera auf einem Lageplan 10 Sekunden lang blinkt, wenn ein Alarm auftritt. Das Sichtfeld der Kamera blinkt weiter, wenn Sie die Option Flash while alarms are unacknowledged ausgewählt haben.
Scroll To Camera On Map	Wählen Sie diese Option, um den Lageplan auf eine Kamera zu zentrieren, wenn Sie die Kamera im Bereich Lageplan-Navigation der Oberfläche des Windows Client anklicken.
Always show rule icon	Wählen Sie diese Option, um das Regelsymbol immer auf dem Lageplan anzuzeigen.
Default color	Wählen Sie die Farbe für das Regelsymbol aus.
Transparency	Legen Sie die Transparenz für das Regelsymbol auf dem Lageplan fest.

Gerätebaum

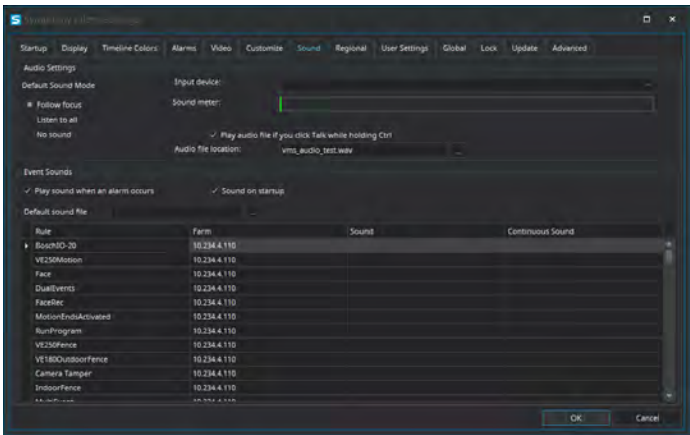
Einstellung	Beschreibung
Show Device Icons	Wählen Sie diese Option, um Gerätesymbole im Gerätebaum anzuzeigen.
Show Device Numbers	Wählen Sie diese Option, um Gerätenummern im Gerätebaum anzuzeigen.
Show Device Status	Wählen Sie diese Option, um den Status der Geräte im Gerätebaum anzuzeigen (z. B. Ein, Aus, Aktivität usw.).
Show Digital I/O	Wählen Sie diese Option, um digitale E/A-Geräte im Gerätebaum anzuzeigen.
Auto Expand Entire Device Tree	Wählen Sie diese Option, um beim Start der Oberfläche des Windows Client alle Ebenen des Gerätebaums zu erweitern.

Einstellung	Beschreibung
Auto Expand Devices Root Nodes	Wählen Sie diese Option, um beim Start der Oberfläche des Windows Client die oberste Ebene des Gerätebaums zu erweitern.
Don't Expand Device Tree	Wählen Sie diese Option, damit der Gerätebaum beim Start der Oberfläche des Windows Client eingeklappt bleibt.
Auto Expand Camera Views	Wählen Sie diese Option, um beim Start der Oberfläche des Windows Client die Kameraansichten im Gerätebaum zu erweitern.
Don't Expand Camera Views	Wählen Sie diese Option, damit die Kameraansichten beim Start der Oberfläche des Windows Client im Gerätebaum eingeklappt bleiben.
Auto Expand Carousels	Wählen Sie diese Option, um beim Start der Oberfläche des Windows Client die Sequenzen im Gerätebaum zu erweitern.
Don't Expand Carousels	Wählen Sie diese Option, damit die Sequenzen beim Start der Oberfläche des Windows Client im Gerätebaum eingeklappt bleiben.
Auto Expand Thin Clients	Wählen Sie diese Option, um beim Start der Oberfläche des Windows Client die Senstar-Thin-Client-Gruppe im Gerätebaum zu erweitern.
Don't Expand Thin Clients	Wählen Sie diese Option, damit die Senstar-Thin-Client-Gruppe beim Start der Oberfläche des Windows Client im Gerätebaum eingeklappt bleibt.

Toneinstellungen

Die Toneinstellungen legen fest, welche Geräusche der Windows Client von Kameras und Ereignissen erzeugt.

+



+

Audioeinstellungen

Einstellung	Beschreibung
Standard-Tonmodus	Legen Sie fest, wie der Windows Client Audio für Video wiedergibt oder stummschaltet. Wählen Sie Fokus folgen aus, um Audio aus dem aktiven Video-Panel wiederzugeben. Wählen Sie Allen zuhören aus, um Audio aus allen Video-Panels wiederzugeben. Wählen Sie Kein Ton aus, um alle Audiodaten stummzuschalten.
Eingabegerät	Wählen Sie das Audio-Eingabegerät aus.
Audiodatei abspielen, wenn Sie bei gedrückter Strg-Taste auf Sprechen klicken	Auswählen, um eine Audiodatei abzuspielen, wenn Sie bei gedrückter Strg-Taste auf die Schaltfläche Sprechen klicken.
Speicherort der Audiodatei	Wählen Sie die Audiodatei aus, die abgespielt werden soll, wenn Sie bei gedrückter Strg-Taste auf die Schaltfläche Sprechen klicken.

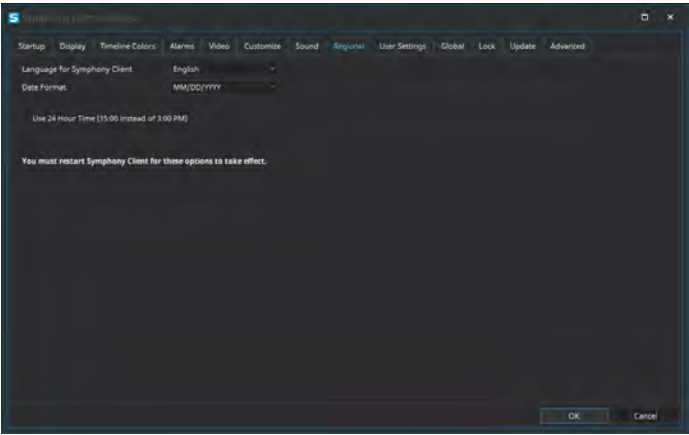
Ereignistöne

Einstellung	Beschreibung
Ton abspielen, wenn ein Alarm auftritt	Auswählen, um einen Ton abzuspielen, wenn ein Alarm auftritt. Sie können sowohl den Alarmton als auch den Dauerton für jede Regel festlegen.
Ton beim Start	Auswählen, um die Standard-Audiodatei abzuspielen, wenn die Oberfläche des Windows Client startet.
Standard-Audiodatei	Wählen Sie die Standard-Audiodatei aus.

Regionale Einstellungen

Die regionalen Einstellungen legen die Sprache und das Datums-/Zeitformat für den Windows Client fest.

+



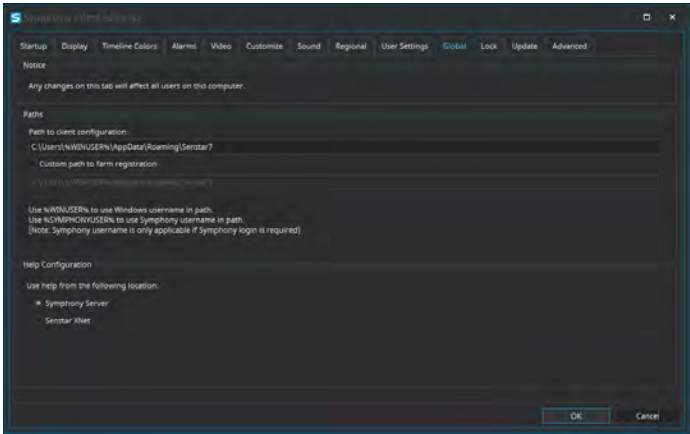
+

Einstellung	Beschreibung
Sprache für Windows Client	Wählen Sie die Sprache für die Oberfläche des Windows Client aus.
Datumsformat	Wählen Sie das Format für Datumsangaben in der Oberfläche des Windows Client aus.
24-Stunden-Format verwenden	Auswählen, um die Uhrzeit im 24-Stunden-Format in der Oberfläche des Windows Client anzuzeigen.

Globale Einstellungen

Die globalen Einstellungen bestimmen den Speicherort der Konfigurationsdateien und welche Version der Senstar Symphony-Hilfe der Windows Client verwendet (entweder die mit der Installation des Server enthaltene Hilfe oder die Online-Hilfe).

+



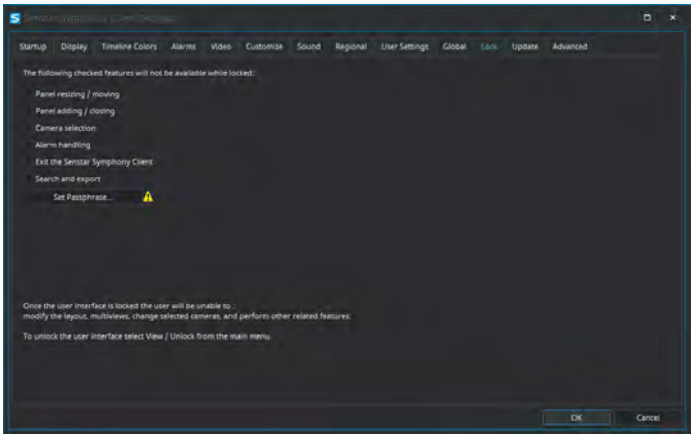
+

Einstellung	Beschreibung
Path to client configuration	Definieren Sie den Pfad zu den Konfigurationsdaten für den Windows Client.
Custom path to farm registration	Wählen Sie diese Option, um einen benutzerdefinierten Pfad für Farmregistrierungsinformationen zu definieren.
Use help from the following location	Wählen Sie aus, ob der Windows Client die mit dem Server enthaltene Hilfe oder die Hilfe aus dem Internet öffnet.

Sperreinstellungen

Die Sperreinstellungen bestimmen die Funktionalität, die Benutzern beim Sperren des Windows Client zur Verfügung steht, und ermöglichen das Festlegen der Passphrase zum Entsperren des Windows Client.

+



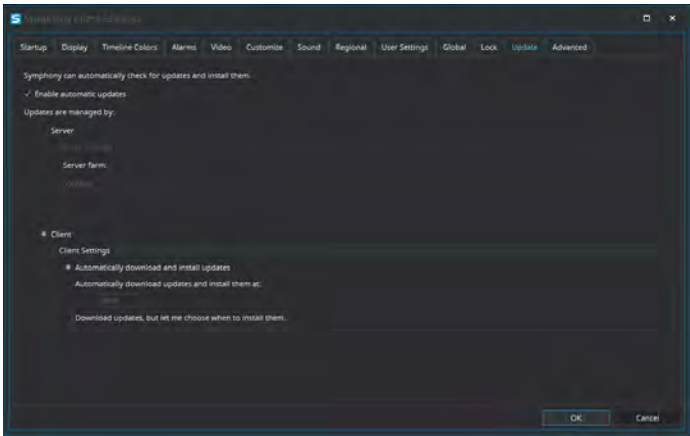
+

Einstellung	Beschreibung
Panel resizing/moving	Wählen Sie diese Option, um zu verhindern, dass Benutzer Panels (z. B. Kameraansicht, Lageplaneditor, Gerätebaum usw.) in der Oberfläche des Windows Client in der Größe ändern oder verschieben.
Panel adding/closing	Wählen Sie diese Option, um zu verhindern, dass Benutzer Panels (z. B. Kameraansicht, Lageplaneditor, Gerätebaum usw.) in der Oberfläche des Windows Client hinzufügen oder schließen.
Camera selection	Wählen Sie diese Option, um zu verhindern, dass Benutzer verschiedene Kameras auswählen.
Alarm Handling	Wählen Sie diese Option, um zu verhindern, dass Benutzer Alarme verarbeiten.
Exit the Windows Client	Wählen Sie diese Option, um zu verhindern, dass Benutzer den Windows Client schließen.
Search and export	Wählen Sie diese Option, um zu verhindern, dass Benutzer nach Video suchen und es exportieren.
Set Passphrase	Klicken Sie hier, um die Passphrase festzulegen, mit der der Windows Client entsperrt wird.

Update-Einstellungen

Die Update-Einstellungen legen fest, wie der Windows Client nach Updates sucht und diese anwendet.

+



+

Einstellung	Beschreibung
Automatische Updates aktivieren	Auswählen, um automatische Updates für den Windows Client zu aktivieren.
Updates werden verwaltet von	Wählen Sie aus, ob der Server oder der Windows Client die Updates verwaltet.

Servereinstellungen

Einstellung	Beschreibung
Serverfarm	Wenn Sie Updates über den Server verwalten, wählen Sie die Server-Farm aus, die die Updates verwaltet.

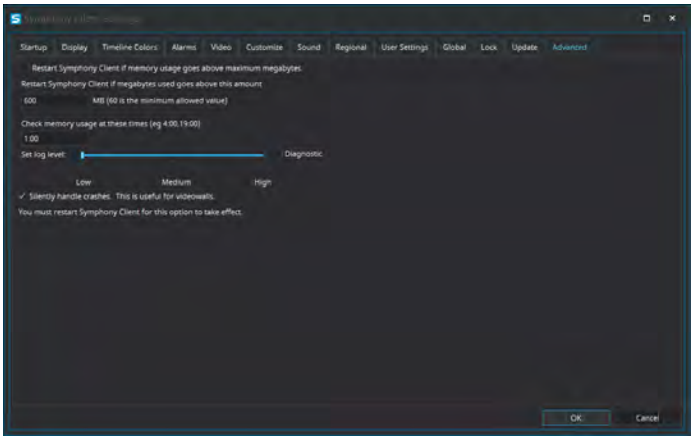
Client-Einstellungen

Einstellung	Beschreibung
Updates automatisch herunterladen und installieren	Wenn Sie Updates über den Windows Client verwalten, wählen Sie diese Option aus, um Updates herunterzuladen und zu installieren, sobald sie verfügbar sind.
Updates automatisch herunterladen und installieren um	Wenn Sie Updates über den Windows Client verwalten, wählen Sie diese Option aus, um Updates zu einer bestimmten Uhrzeit herunterzuladen und zu installieren.
Updates herunterladen, aber Zeitpunkt der Installation selbst wählen	Wenn Sie Updates über den Windows Client verwalten, wählen Sie diese Option aus, um Updates nur herunterzuladen. Wenn Sie diese Option auswählen, müssen Sie die Updates manuell installieren.

Erweiterte Einstellungen

Die erweiterten Einstellungen legen fest, wie und wann der Windows Client neu startet und wie viele Informationen in Protokolldateien aufgenommen werden.

+



+

Einstellung	Beschreibung
Restart Windows Client if memory usage goes above maximum megabytes	Wählen Sie diese Option aus, um den Windows Client automatisch neu zu starten, wenn die Speichernutzung einen bestimmten Wert erreicht.
Restart Windows Client if megabytes goes above this amount	Geben Sie die Speichernutzungsgrenze (in MB) ein, oberhalb derer der Windows Client neu startet. Diese Einstellung wird aktiv, wenn Sie die Einstellung Restart Windows Client if memory usage goes above maximum megabytes auswählen.
Check memory usage at these times	Legen Sie fest, wann der Windows Client die Speichernutzung überprüft. Dieses Feld akzeptiert kommagetrennte Werte im 24-Stunden-Format (hh:mm).
Set log level	Stellen Sie mit dem Schieberegler die Protokollebene für den Windows Client ein.
Diagnostic	Wählen Sie diese Option aus, um die Protokollebene auf Diagnose einzustellen. Diese Einstellung erzeugt die umfassendsten Protokollinformationen. Wenn Sie diese Option auswählen, überschreibt sie die mit dem Schieberegler Set log level eingestellte Protokollebene.
Silently handle crashes	Wählen Sie diese Option aus, um das CMD-Fenster auszublenden, wenn der Windows Client eine Dump-Datei erstellt.

Videowand

Die Videowand-Funktion in Senstar Symphony kann Aufnahmen von mehreren Kameras in der Serverfarm auf mehreren Monitoren anzeigen.

Jeder Windows Client kann als Videowand-Client fungieren, und Sie können alle Monitore, die an die Computer angeschlossen sind, auf denen der Windows Client ausgeführt wird, in die Videowand einbeziehen.

Client registrieren

Registrieren Sie jeden Computer, auf dem der Windows Client ausgeführt wird, den Sie in die Videowand aufnehmen möchten.

1. Klicken Sie in der Oberfläche des Windows Client auf Ansicht > Videowand.
2. Klicken Sie auf die Registerkarte Videowand-Client-Konfiguration.
3. Klicken Sie auf Aktuellen Client registrieren.
4. Klicken Sie auf Speichern.

Videowand erstellen

1. Klicken Sie in der Oberfläche des Windows Client auf View > Video Wall.
2. Klicken Sie auf der Registerkarte Video Wall Client Configuration auf Design Video Wall.
3. Klicken Sie auf New.
4. Um einen Namen für die Videowand zu definieren, führen Sie die folgenden Schritte aus:
 - a. Doppelklicken Sie auf den Standardnamen für die Videowand.
 - b. Geben Sie einen neuen Namen ein.
 - c. Drücken Sie die Eingabetaste.
5. Wählen Sie den Namen der Videowand aus und klicken Sie auf Open.
6. Ziehen Sie einen Videowand-Monitor aus dem Bereich Tool Box in das Videowand-Raster.
7. Klicken Sie auf das Monitorfeld im Videowand-Raster.
8. Geben Sie im Feld Label einen Namen für den Monitor ein und klicken Sie auf Apply.
9. Verschieben und dimensionieren Sie den Videowand-Monitor.
10. Klicken Sie auf Save.

Serverkonfiguration

Auch wenn Sie die meisten Konfigurationen für den Server in der Server-Konfigurationsoberfläche vornehmen, enthält die Oberfläche des Windows Client Funktionen zur Konfiguration einiger Einstellungen am Server.

Mit einem Server verbinden

Sie können einen Windows Client mit mehreren Server-Instanzen verbinden.

1. Klicken Sie in der Oberfläche des Windows Client auf Server Configuration > New Symphony Server Registration.
2. Führen Sie im Feld Address eine der folgenden Aufgaben aus:
 - Wählen Sie den Server aus der Liste der erkannten Server aus.
 - Geben Sie die IP-Adresse des Server ein.
 - Geben Sie den DNS-Namen des Server ein.
3. Geben Sie im Feld Name einen aussagekräftigen Namen für den Server ein. Dieser Name erscheint in der Server List in der

Oberfläche des Windows Client

.

1. Um sich beim Server anzumelden, führen Sie eine der folgenden Aufgaben aus:
 - Um Ihr Windows-Konto zur Authentifizierung beim Server zu verwenden, aktivieren Sie das Kontrollkästchen Windows Authentication.
 - Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
2. Klicken Sie auf OK.

Verbindung zu einem Server trennen

Sie können die Verbindung zu einem Server trennen, um die mit diesem Server verbundenen Kameras aus dem Windows Client zu entfernen.

1. Klicken Sie in der Oberfläche des Windows Client auf Server Configuration > Delete Symphony Server Registration.
2. Wählen Sie den Server aus, von dem Sie die Verbindung trennen möchten.
3. Klicken Sie auf Remove.

Informationen über den Server abrufen

Sie können Informationen über den Server sammeln, mit dem der Windows Client verbunden ist.

1. Klicken Sie in der Oberfläche des Windows Client auf Server Configuration > Get Info.
2. Wählen Sie in der Liste Choose Server den Server aus, zu dem Sie Informationen abrufen möchten.
3. Um zusätzliche Informationen zu erhalten, wählen Sie Verbose. Die ausführlichen Informationen umfassen:
 - Festplatteninformationen
 - Versionsinformationen des Server
 - Systeminformationen
 - Betriebszeitinformationen
 - Aufgabenlisteninformationen
 - IP-Konfigurationsinformationen
 - Lizenzinformationen
 - Netzwerkstatistiken
 - Dienstinformationen
4. Klicken Sie auf Get Info. Die Schaltfläche

Get Info

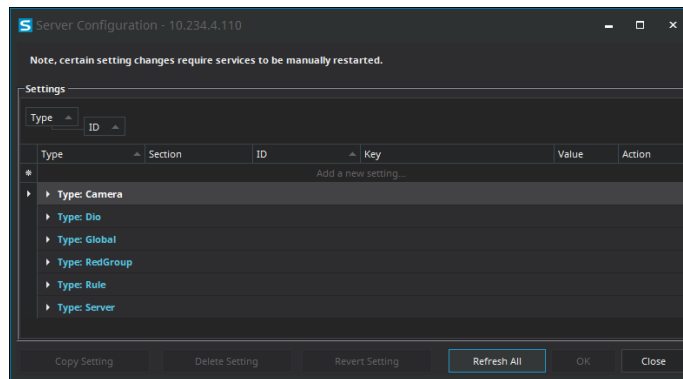
aktualisiert auch die Informationen.

Manueller Konfigurationseditor

Der Manuelle Konfigurationseditor ist eine Senstar Symphony-Komponente, mit der Sie erweiterte Einstellungen in der Senstar Symphony-Datenbank hinzufügen und bearbeiten können.

Sie können auf den Manuellen Konfigurationseditor über den Windows Client oder als eigenständige Anwendung zugreifen, wenn Sie den Server installieren.

+



+

Jede Einstellung enthält die folgenden Felder:

- Type
- Section
- ID
- Key
- Value
- Action

Wenn Sie nach Änderungen auf OK klicken, sendet der Windows Client die Änderungen an den Server, der die Änderungen der Senstar Symphony-Datenbank hinzufügt.

Einstellung hinzufügen

Sie können den Manual Configuration Editor verwenden, um eine Einstellung zur Senstar Symphony Database hinzuzufügen.

Das Hinzufügen einer Einstellung zur Senstar Symphony Database ist eine Möglichkeit, dem Server oder Windows Client erweiterte Funktionalität hinzuzufügen.

1. Klicken Sie in der Oberfläche des Windows Client auf Server Configuration > Manual Configuration Editor.
2. Klicken Sie auf Add a new setting. Der

Add a new setting

ist eine Beschriftung in einer leeren Zeile. Sie können in eine beliebige Stelle in der leeren Zeile klicken, um die Datenfelder zu aktivieren.

1. Fügen Sie die Werte zur Einstellung hinzu.
2. Klicken Sie auf OK.

Einstellung kopieren

Sie können den Manual Configuration Editor verwenden, um eine Einstellung in der Senstar Symphony Database zu kopieren.

Das Kopieren einer Einstellung ist eine schnelle Möglichkeit, der Senstar Symphony Database eine neue Einstellung hinzuzufügen, indem eine ähnliche bestehende Einstellung als Vorlage verwendet wird.

1. Klicken Sie in der Oberfläche des Windows Client auf Server Configuration > Manual Configuration Editor.
2. Wählen Sie die Einstellung aus, die Sie kopieren möchten.
3. Klicken Sie auf Copy Setting.

Die kopierte Einstellung erscheint am Ende der entsprechenden Einstellungsliste mit der Beschriftung im Feld

Key

.

Einstellung bearbeiten

Sie können den Manuellen Konfigurationseditor verwenden, um eine Einstellung in der Senstar Symphony-Datenbank zu bearbeiten.

Das Bearbeiten einer Einstellung ist eine schnelle Möglichkeit, der Senstar Symphony-Datenbank eine neue Einstellung hinzuzufügen, indem eine ähnliche bestehende Einstellung als Vorlage verwendet wird.

1. Klicken Sie in der Oberfläche des Windows Client auf Server Configuration > Manual Configuration Editor.
2. Wählen Sie die Einstellung aus, die Sie bearbeiten möchten.
3. Klicken Sie auf Edit Setting.

Einstellung zurücksetzen

Sie können den Manuellen Konfigurationseditor verwenden, um eine Einstellung auf die Werte in der Senstar Symphony-Datenbank zurückzusetzen.

Beim Zurücksetzen einer Einstellung wird die Einstellung auf die Werte in der Senstar Symphony-Datenbank zurückgesetzt, die vor dem Speichern Ihrer Änderungen vorhanden waren. Dies funktioniert nur, wenn Sie nach der Änderung noch nicht auf OK geklickt haben.

1. Klicken Sie in der Oberfläche des Windows Client auf Serverkonfiguration > Manueller Konfigurationseditor.
2. Wählen Sie die Einstellung aus, die Sie bearbeiten möchten.
3. Klicken Sie auf Einstellung zurücksetzen.

Einstellung löschen

Sie können den Manuellen Konfigurationseditor verwenden, um eine Einstellung in der Senstar Symphony-Datenbank zu löschen.

1. Klicken Sie in der Oberfläche des Windows Client auf Server Configuration > Manual Configuration Editor.
2. Wählen Sie die Einstellung aus, die Sie löschen möchten.
3. Klicken Sie auf Delete Setting.

Einstellungen aktualisieren

Sie können den Manuellen Konfigurationseditor verwenden, um die Einstellungen zu aktualisieren und Änderungen aus der Senstar Symphony-Datenbank abzurufen.

Durch das Aktualisieren der Einstellungen wird sichergestellt, dass die Einstellungen im Manuellen Konfigurationseditor mit den aktuellen Einstellungen in der Senstar Symphony-Datenbank übereinstimmen. Diese Funktion ist hilfreich, wenn mehrere Personen Änderungen an der Senstar Symphony-Datenbank vornehmen können.

1. Klicken Sie in der Oberfläche des Windows Client auf Serverkonfiguration > Manueller Konfigurationseditor.
2. Klicken Sie auf Alle aktualisieren.

Windows-Authentifizierung

Die Windows-Authentifizierung, oder Single Sign-On, verwendet Domänenidentitäten zur Authentifizierung von Benutzern.

Um die Windows-Authentifizierung zu verwenden, müssen sich der Server und der Windows Client in derselben Sicherheitsdomäne befinden, und der Benutzer muss Domänenanmeldedaten verwenden, um sich an der Oberfläche des Windows Client anzumelden.

Windows-Authentifizierung aktivieren

1. Klicken Sie in der Oberfläche des Windows Client mit der rechten Maustaste auf einen Server in der Serverliste.
2. Klicken Sie auf Edit.
3. Wählen Sie Windows Authentication aus.
4. Klicken Sie auf OK.

Berichte und Protokolle

Sie können Berichte zu den Daten des Server erstellen.

Sie können Berichte als E-Mails verteilen oder Berichte in Dateien speichern. Sie können Berichte planen, die automatisch ausgeführt werden, oder jederzeit manuell einen Bericht erstellen. Wenn Sie einen Bericht ausführen, speichert der Server den Bericht standardmäßig im Pfad \Data\Reports des Servers oder im Pfad, den Sie bei der Installation des Server festgelegt haben.

Verfügbare Berichte

Bericht	Beschreibung
Alarmbericht	Zeigt eine Liste und Informationen zu einzelnen Alarmen an
Alarmstatistik	Fasst alle Alarme für einen bestimmten Zeitraum zusammen
Bericht zur Gesichtserkennung	Zeigt Informationen zu übereinstimmenden Gesichtern an
Heat-Map-Bild	Zeigt eine grafische Darstellung von Verkehrsmustern an
Objektanzahl	Fasst die Anzahl der Objekte zusammen
Objektanzahl über eine Linie	Fasst die Objektanzahl über eine Linie zusammen
Objektstatistik	Vergleicht Verkehr und Verweildauer

Einen Bericht ausführen

Sie können jederzeit manuell einen Bericht erstellen.

1. Klicken Sie in der Oberfläche des Windows Client auf Berichte. Der Berichts-Designer öffnet sich in einem Browser.
1. Melden Sie sich am Berichts-Designer an.
2. Wählen Sie einen Bericht aus.
3. Klicken Sie auf Ausführen.

Einen Bericht bearbeiten

Sie können einen vorhandenen Bericht im Berichts-Designer ändern.

1. Klicken Sie in der Oberfläche des Windows Client auf Berichte. Der Berichts-Designer öffnet sich in einem Browser.
1. Melden Sie sich am Berichts-Designer an.
2. Führen Sie eine der folgenden Aufgaben aus:
 - Wählen Sie einen Bericht aus und klicken Sie auf Bearbeiten.
 - Doppelklicken Sie auf einen Bericht.
3. Nehmen Sie Änderungen am Bericht vor.
4. Klicken Sie auf Speichern.

Um Berichte auszuführen, muss ein Benutzer über die Berechtigungen Connect und Execute Report verfügen. Um den Heat-Map-Bildbericht auszuführen, muss der Benutzer zusätzlich über die Berechtigung Search verfügen.

Ereignisse anzeigen

Sie können Ereignisse für den Windows Client und alle Server-Instanzen anzeigen und exportieren, mit denen der Windows Client verbunden ist.

Ereignisse werden im Audit-Protokoll der Senstar Symphony-Datenbank gespeichert. Standardmäßig zeigt die Oberfläche des Windows Client die Ereignisse des aktuellen Tages an.

1. Klicken Sie in der Oberfläche des Windows Client auf Hilfe > Audit anzeigen.
2. Wählen Sie das Startdatum und die Startzeit sowie das Enddatum und die Endzeit aus.
3. Klicken Sie auf Neu laden.
4. Um die Ereignisse zu gruppieren, ziehen Sie eine Spalte
5. Um die Ereignisse als CSV-Datei zu exportieren, klicken Sie auf Exportieren.

Alarmbericht

Der Alarmbericht zeigt eine Liste und Informationen zu einzelnen Alarmen für eine bestimmte Zeit an.

1. Klicken Sie in der Oberfläche des Windows Client auf Reports. Der Report Designer

wird in einem Browser geöffnet.

1. Melden Sie sich beim Report Designer an.
2. Klicken Sie auf New Report.
3. Geben Sie einen Namen für den Bericht ein.
4. Wählen Sie in der Liste Report Type den Eintrag Alarm Report aus.
5. Um anderen Benutzern das Ausführen des Berichts zu erlauben, wählen Sie Allow other users to run this report.
6. Klicken Sie auf OK.
7. Führen Sie im Abschnitt Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.
 - b. Wählen Sie eine oder mehrere Kameras aus. Sie können nach Kameras anhand des Kameranamens suchen.
 - c. Klicken Sie auf OK.
8. Führen Sie im Abschnitt Date Range die folgenden Aufgaben aus, um die im Bericht enthaltenen Daten zu bestimmen:
 - a. Definieren Sie im Abschnitt Start including data from den Beginn der Daten.
 - b. Definieren Sie im Abschnitt Stop including data after das Ende der Daten.
 - c. Um Daten aus einem bestimmten Zeitbereich an jedem Tag zu verwenden, wählen Sie Use custom time range for data collection und geben Sie den Zeitbereich an.
9. Führen Sie im Abschnitt Schedule die folgenden Aufgaben aus, um den Bericht automatisch auszuführen:
 - a. Wählen Sie Schedule Enabled.
 - b. Legen Sie im Abschnitt Recurrence fest, wann der Bericht ausgeführt wird.
 - c. Legen Sie im Abschnitt Schedule start fest, wann der Bericht automatisch ausgeführt wird.
 - d. Legen Sie im Abschnitt Schedule finish fest, wann der Bericht aufhört, automatisch ausgeführt zu werden.
10. Führen Sie im Abschnitt Distribution die folgenden Aufgaben aus, um zu bestimmen, wie der Server Berichte verteilt:
 - a. Um den Bericht als E-Mail-Anhang zu versenden, wählen Sie Send report in email, geben Sie die E-Mail-Adressen der Empfänger an und wählen Sie die Dateiformate für die Berichte aus.
 - b. Um den Bericht als Datei zu speichern, wählen Sie Save report to file, geben Sie den Pfad an, definieren Sie den Dateinamen und wählen Sie die Dateiformate aus.
11. Führen Sie im Abschnitt Table Layout die folgenden Aufgaben aus, um das Erscheinungsbild der Tabelle im Bericht zu bestimmen:
 - a. Wählen Sie in der Liste Columns die Informationen aus, die in den Spalten des Berichts

erscheinen sollen.

- b. Wählen Sie im Abschnitt Grouping aus, wie die Informationen im Bericht gruppiert werden.
- c. Wählen Sie im Abschnitt Sorting aus, wie die Informationen sortiert werden.

12. Klicken Sie auf Save.

Alarmstatistikbericht

Der Alarmstatistikbericht fasst Alarmer für eine bestimmte Zeit zusammen.

1. Klicken Sie in der Oberfläche des Windows Client auf Reports. Der

Report Designer

wird in einem Browser geöffnet.

1. Melden Sie sich beim Report Designer an.
2. Klicken Sie auf New Report.
3. Geben Sie einen Namen für den Bericht ein.
4. Wählen Sie in der Liste Report Type den Eintrag Alarm Statistics aus.
5. Um anderen Benutzern das Ausführen des Berichts zu erlauben, wählen Sie Allow other users to run this report.
6. Klicken Sie auf OK.
7. Führen Sie im Abschnitt Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.
 - b. Wählen Sie eine oder mehrere Kameras aus. Sie können nach Kameras anhand des Kameranamens suchen.
 - c. Klicken Sie auf OK.
8. Führen Sie im Abschnitt Date Range die folgenden Aufgaben aus, um die im Bericht enthaltenen Daten zu bestimmen:
 - a. Definieren Sie im Abschnitt Start including data from den Beginn der Daten.
 - b. Definieren Sie im Abschnitt Stop including data after das Ende der Daten.
 - c. Um Daten aus einem bestimmten Zeitbereich an jedem Tag zu verwenden, wählen Sie Use custom time range for data collection und geben Sie den Zeitbereich an.
9. Führen Sie im Abschnitt Schedule die folgenden Aufgaben aus, um den Bericht automatisch auszuführen:
 - a. Wählen Sie Schedule Enabled.
 - b. Legen Sie im Abschnitt Recurrence fest, wann der Bericht ausgeführt wird.
 - c. Legen Sie im Abschnitt Schedule start fest, wann der Bericht automatisch ausgeführt wird.
 - d. Legen Sie im Abschnitt Schedule finish fest, wann der Bericht aufhört, automatisch ausgeführt zu werden.
10. Führen Sie im Abschnitt Distribution die folgenden Aufgaben aus, um zu bestimmen, wie der Server

Berichte verteilt:

- a. Um den Bericht als E-Mail-Anhang zu versenden, wählen Sie Send report in email, geben Sie die E-Mail-Adressen der Empfänger an und wählen Sie die Dateiformate für die Berichte aus.
 - b. Um den Bericht als Datei zu speichern, wählen Sie Save report to file, geben Sie den Pfad an, definieren Sie den Dateinamen und wählen Sie die Dateiformate aus.
11. Führen Sie im Abschnitt Graph die folgenden Aufgaben aus, um das Erscheinungsbild des Diagramms im Bericht zu bestimmen:
- a. Wählen Sie in der Liste Default Graph den anzuzeigenden Alarmtyp aus.
 - b. Wählen Sie in der Liste Graph Type aus, ob das Diagramm ein Linien- oder Balkendiagramm ist.
 - c. Wählen Sie in der Liste Graph Size die Größe des Diagramms aus.
12. Führen Sie im Abschnitt Table Layout die folgenden Aufgaben aus, um das Erscheinungsbild der Tabelle im Bericht zu bestimmen:
- a. Wählen Sie in der Liste Columns die Informationen aus, die in den Spalten des Berichts erscheinen sollen.
 - b. Wählen Sie im Abschnitt Grouping aus, wie die Informationen im Bericht gruppiert werden.
 - c. Wählen Sie im Abschnitt Sorting aus, wie die Informationen sortiert werden.
13. Klicken Sie auf Save.

Gesichtserkennungsbericht

Der Gesichtserkennungsbericht zeigt Informationen über Gesichter für eine bestimmte Zeit an.

Damit der Gesichtserkennungsbericht verfügbar ist, muss die Videoanalyse Gesichtserkennung installiert sein.

Beim Erstellen dieses Berichts müssen Sie unterschiedliche Kameras als Eingangs- und Ausgangskameras auswählen.

1. Klicken Sie in der Oberfläche des Windows Client auf Reports. Der

Report Designer

wird in einem Browser geöffnet.

1. Melden Sie sich beim Report Designer an.
2. Klicken Sie auf New Report.
3. Geben Sie einen Namen für den Bericht ein.
4. Wählen Sie in der Liste Report Type den Eintrag Face Recognition aus.
5. Um anderen Benutzern das Ausführen des Berichts zu erlauben, wählen Sie Allow other users to run this report.
6. Klicken Sie auf OK.
7. Führen Sie im Abschnitt Entrance Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.
 - b. Wählen Sie eine oder mehrere Kameras aus. Sie können nach Kameras anhand des

Kameranamens suchen.

- c. Klicken Sie auf OK.
8. Führen Sie im Abschnitt Exit Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.
 - b. Wählen Sie eine oder mehrere Kameras aus. Sie können nach Kameras anhand des Kameranamens suchen.
 - c. Klicken Sie auf OK.
9. Führen Sie im Abschnitt Face Recognition die folgenden Aufgaben aus:
 - a. Um Gesichter auszuschließen, die zuerst von einer Ausgangskamera und dann von einer Eingangskamera erfasst werden, wählen Sie Remove exit-to-entrance matches.
 - b. Wählen Sie im Feld Minimum confidence for report aus, wie zuverlässig die Gesichtserkennungs-Videoanalyse sein muss, damit sie das Gesicht meldet.
 - c. Wählen Sie im Feld Reporting block size die Zeit (in Sekunden) aus, aus der die Gesichtserkennungs-Videoanalyse die beste Gesichtsübereinstimmung wählt.
 - d. Legen Sie im Feld Number of blocks to check after current fest, wie viele Zeitblöcke die Gesichtserkennungs-Videoanalyse nach einer Gesichtsübereinstimmung durchsucht.
 - e. Legen Sie im Feld Timeout for first match in block die Zeit fest, vor der die Gesichtserkennungs-Videoanalyse ein Gesicht erkennen muss, das die Szene betritt, damit das Gesicht für eine Übereinstimmung infrage kommt.
 - f. Wählen Sie in der Liste Hours to run report die Zeiten aus, zu denen die Gesichtserkennungs-Videoanalyse Daten für den Bericht generiert.
10. Führen Sie im Abschnitt Date Range die folgenden Aufgaben aus, um die im Bericht enthaltenen Daten zu bestimmen:
 - a. Definieren Sie im Abschnitt Start including data from den Beginn der Daten.
 - b. Definieren Sie im Abschnitt Stop including data after das Ende der Daten.
 - c. Um Daten aus einem bestimmten Zeitbereich an jedem Tag zu verwenden, wählen Sie Use custom time range for data collection und geben Sie den Zeitbereich an.
11. Führen Sie im Abschnitt Schedule die folgenden Aufgaben aus, um den Bericht automatisch auszuführen:
 - a. Wählen Sie Schedule Enabled.
 - b. Legen Sie im Abschnitt Recurrence fest, wann der Bericht ausgeführt wird.
 - c. Legen Sie im Abschnitt Schedule start fest, wann der Bericht automatisch ausgeführt wird.
 - d. Legen Sie im Abschnitt Schedule finish fest, wann der Bericht aufhört, automatisch ausgeführt zu werden.
12. Führen Sie im Abschnitt Distribution die folgenden Aufgaben aus, um zu bestimmen, wie der Server Berichte verteilt:
 - a. Um den Bericht als E-Mail-Anhang zu versenden, wählen Sie Send report in email, geben Sie die E-Mail-Adressen der Empfänger an und wählen Sie die Dateiformate für die Berichte aus.

- b. Um den Bericht als Datei zu speichern, wählen Sie Save report to file, geben Sie den Pfad an, definieren Sie den Dateinamen und wählen Sie die Dateiformate aus.
- 13. Führen Sie im Abschnitt Table Layout die folgenden Aufgaben aus, um das Erscheinungsbild der Tabelle im Bericht zu bestimmen:
 - a. Wählen Sie in der Liste Columns die Informationen aus, die in den Spalten des Berichts erscheinen sollen.
 - b. Wählen Sie im Abschnitt Grouping aus, wie die Informationen im Bericht gruppiert werden.
 - c. Wählen Sie im Abschnitt Sorting aus, wie die Informationen sortiert werden.
- 14. Klicken Sie auf Save.

Heat-Map-Bildbericht

Der Heat-Map-Bildbericht zeigt eine grafische Darstellung der Verkehrsmuster für eine bestimmte Zeit an.

- 1. Klicken Sie in der Oberfläche des Windows Client auf Reports. Der Report Designer wird in einem Browser geöffnet.
 - 1. Melden Sie sich beim Report Designer an.
 - 2. Klicken Sie auf New Report.
 - 3. Geben Sie einen Namen für den Bericht ein.
 - 4. Wählen Sie in der Liste Report Type den Eintrag Heat Map Image aus.
 - 5. Um anderen Benutzern das Ausführen des Berichts zu erlauben, wählen Sie Allow other users to run this report.
 - 6. Klicken Sie auf OK.
 - 7. Führen Sie im Abschnitt Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.
 - b. Wählen Sie eine oder mehrere Kameras aus. Sie können nach Kameras anhand des Kameranamens suchen.
 - c. Klicken Sie auf OK.
 - 8. Führen Sie im Abschnitt Zone Selection die folgenden Aufgaben aus, um zu bestimmen, welche Zonen in der Kameraansicht Daten für den Bericht generieren:
 - a. Klicken Sie auf Add Zone.
 - b. Verschieben Sie die Zone oder ändern Sie ihre Form.
 - c. Um die Zone umzubenennen, klicken Sie auf Rename Zone, geben Sie einen neuen Namen ein und klicken Sie auf OK.
 - d. Wiederholen Sie den Vorgang, um eine weitere Zone hinzuzufügen.
 - 9. Führen Sie im Abschnitt Sensitivity die folgenden Aufgaben aus, um festzulegen, wie empfindlich die Heat Map auf Ereignisse reagiert:

- a. Um die Anzahl der Schnittpunkte festzulegen, die auftreten müssen, bevor die Heat Map mit dem Erfassen von Schnittpunkten für eine Zone beginnt, wählen Sie Minimum intersections und geben Sie den Wert ein.
 - b. Um die Anzahl der Schnittpunkte festzulegen, die auftreten müssen, bevor die Heat Map die Aktualisierung des Werts für eine Zone stoppt, wählen Sie Maximum Intersections und geben Sie einen Wert ein.
 - c. Um festzulegen, wie lange ein Objekt stationär bleiben muss, bevor die Heat Map mit dem Erfassen von verweilenden Objekten für eine Zone beginnt, wählen Sie Minimum Dwell Time und legen Sie die Zeit fest.
 - d. Um festzulegen, wie lange ein Objekt stationär bleibt, bevor die Heat Map die Aktualisierung des Werts für eine Zone stoppt, wählen Sie Maximum Dwell Time und legen Sie die Zeit fest.
 - e. Um festzulegen, wie lange ein Objekt stationär sein muss, bevor es als verweilend betrachtet wird, wählen Sie Dwell Threshold und legen Sie die Zeit fest.
10. Führen Sie im Abschnitt Date Range die folgenden Aufgaben aus, um die im Bericht enthaltenen Daten zu bestimmen:
- a. Definieren Sie im Abschnitt Start including data from den Beginn der Daten.
 - b. Definieren Sie im Abschnitt Stop including data after das Ende der Daten.
 - c. Um Daten aus einem bestimmten Zeitbereich an jedem Tag zu verwenden, wählen Sie Use custom time range for data collection und geben Sie den Zeitbereich an.
11. Führen Sie im Abschnitt Schedule die folgenden Aufgaben aus, um den Bericht automatisch auszuführen:
- a. Wählen Sie Schedule Enabled.
 - b. Legen Sie im Abschnitt Recurrence fest, wann der Bericht ausgeführt wird.
 - c. Legen Sie im Abschnitt Schedule start fest, wann der Bericht automatisch ausgeführt wird.
 - d. Legen Sie im Abschnitt Schedule finish fest, wann der Bericht aufhört, automatisch ausgeführt zu werden.
12. Führen Sie im Abschnitt Distribution die folgenden Aufgaben aus, um zu bestimmen, wie der Server Berichte verteilt:
- a. Um den Bericht als E-Mail-Anhang zu versenden, wählen Sie Send report in email, geben Sie die E-Mail-Adressen der Empfänger an und wählen Sie die Dateiformate für die Berichte aus.
 - b. Um den Bericht als Datei zu speichern, wählen Sie Save report to file, geben Sie den Pfad an, definieren Sie den Dateinamen und wählen Sie die Dateiformate aus.
13. Führen Sie im Abschnitt Table Layout die folgenden Aufgaben aus, um das Erscheinungsbild der Tabelle im Bericht zu bestimmen:
- a. Wählen Sie in der Liste Columns die Informationen aus, die in den Spalten des Berichts erscheinen sollen.
 - b. Wählen Sie im Abschnitt Grouping aus, wie die Informationen im Bericht gruppiert werden.
 - c. Wählen Sie im Abschnitt Sorting aus, wie die Informationen sortiert werden.
14. Klicken Sie auf Save.

Bericht für automatische Kennzeichenerkennung

Der LPR-Bericht zeigt Informationen über Kennzeichen für eine bestimmte Zeit an.

1. Klicken Sie in der Oberfläche des Windows Client auf Reports. Der Report Designer wird in einem Browser geöffnet.
1. Melden Sie sich beim Report Designer an.
2. Klicken Sie auf New Report.
3. Geben Sie einen Namen für den Bericht ein.
4. Wählen Sie in der Liste Report Type den Eintrag LPR Report aus.
5. Um anderen Benutzern das Ausführen des Berichts zu erlauben, wählen Sie Allow other users to run this report.
6. Klicken Sie auf OK.
7. Führen Sie im Abschnitt Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.
 - b. Wählen Sie eine oder mehrere Kameras aus. Sie können nach Kameras anhand des Kameranamens suchen.
 - c. Klicken Sie auf OK.
8. Wählen Sie im Abschnitt Filter die Kennzeichenlisten aus, über die berichtet werden soll.
9. Führen Sie im Abschnitt Date Range die folgenden Aufgaben aus, um die im Bericht enthaltenen Daten zu bestimmen:
 - a. Definieren Sie im Abschnitt Start including data from den Beginn der Daten.
 - b. Definieren Sie im Abschnitt Stop including data after das Ende der Daten.
 - c. Um Daten aus einem bestimmten Zeitbereich an jedem Tag zu verwenden, wählen Sie Use custom time range for data collection und geben Sie den Zeitbereich an.
10. Führen Sie im Abschnitt Schedule die folgenden Aufgaben aus, um den Bericht automatisch auszuführen:
 - a. Wählen Sie Schedule Enabled.
 - b. Legen Sie im Abschnitt Recurrence fest, wann der Bericht ausgeführt wird.
 - c. Legen Sie im Abschnitt Schedule start fest, wann der Bericht automatisch ausgeführt wird.
 - d. Legen Sie im Abschnitt Schedule finish fest, wann der Bericht aufhört, automatisch ausgeführt zu werden.
11. Führen Sie im Abschnitt Distribution die folgenden Aufgaben aus, um zu bestimmen, wie der Server Berichte verteilt:
 - a. Um den Bericht als E-Mail-Anhang zu versenden, wählen Sie Send report in email, geben Sie die E-Mail-Adressen der Empfänger an und wählen Sie die Dateiformate für die Berichte aus.
 - b. Um den Bericht als Datei zu speichern, wählen Sie Save report to file, geben Sie den Pfad an,

definieren Sie den Dateinamen und wählen Sie die Dateiformate aus.

12. Führen Sie im Abschnitt Table Layout die folgenden Aufgaben aus, um das Erscheinungsbild der Tabelle im Bericht zu bestimmen:
 - a. Wählen Sie in der Liste Columns die Informationen aus, die in den Spalten des Berichts erscheinen sollen.
 - b. Wählen Sie im Abschnitt Grouping aus, wie die Informationen im Bericht gruppiert werden.
 - c. Wählen Sie im Abschnitt Sorting aus, wie die Informationen sortiert werden.
13. Klicken Sie auf Save.

Objektzählungsbericht

Der Objektzählungsbericht zeigt Informationen über Objekte für eine bestimmte Zeit an.

1. Klicken Sie in der Oberfläche des Windows Client auf Reports. Der Report Designer wird in einem Browser geöffnet.
 1. Melden Sie sich beim Report Designer an.
 2. Klicken Sie auf New Report.
 3. Geben Sie einen Namen für den Bericht ein.
 4. Wählen Sie in der Liste Report Type den Eintrag Object Counts aus.
 5. Um anderen Benutzern das Ausführen des Berichts zu erlauben, wählen Sie Allow other users to run this report.
 6. Klicken Sie auf OK.
 7. Führen Sie im Abschnitt Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.
 - b. Wählen Sie eine oder mehrere Kameras aus. Sie können nach Kameras anhand des Kameranamens suchen.
 - c. Klicken Sie auf OK.
 8. Führen Sie im Abschnitt Date Range die folgenden Aufgaben aus, um die im Bericht enthaltenen Daten zu bestimmen:
 - a. Definieren Sie im Abschnitt Start including data from den Beginn der Daten.
 - b. Definieren Sie im Abschnitt Stop including data after das Ende der Daten.
 - c. Um Daten aus einem bestimmten Zeitbereich an jedem Tag zu verwenden, wählen Sie Use custom time range for data collection und geben Sie den Zeitbereich an.
 9. Führen Sie im Abschnitt Schedule die folgenden Aufgaben aus, um zu bestimmen, wann der Bericht ausgeführt wird und welche Informationen er enthält:
 - a. Wählen Sie aus, ob der Bericht manuell oder nach einem Zeitplan ausgeführt werden soll.
 - b. Wenn Sie das Ausführen des Berichts nach einem Zeitplan auswählen, legen Sie den Zeitplan fest.

- c. Geben Sie die Zeit an, ab der Daten für den Bericht erfasst werden sollen. Sie können eine relative Zeit basierend auf dem Bericht festlegen oder bestimmte Zeiten auswählen.
 - d. Wählen Sie aus, wie die Daten gruppiert werden sollen.
- 10. Führen Sie im Abschnitt Distribution die folgenden Aufgaben aus, um zu bestimmen, wie der Server Berichte verteilt:
 - a. Um den Bericht als E-Mail-Anhang zu versenden, wählen Sie Send report in email, geben Sie die E-Mail-Adressen der Empfänger an und wählen Sie die Dateiformate für die Berichte aus.
 - b. Um den Bericht als Datei zu speichern, geben Sie den Pfad an, definieren Sie den Dateinamen und wählen Sie die Dateiformate aus.
- 11. Führen Sie im Abschnitt Graph die folgenden Aufgaben aus, um das Erscheinungsbild des Diagramms im Bericht zu bestimmen:
 - a. Wählen Sie in der Liste Default Graph den anzuzeigenden Alarmtyp aus.
 - b. Wählen Sie in der Liste Graph Type aus, ob das Diagramm ein Linien- oder Balkendiagramm ist.
 - c. Wählen Sie in der Liste Graph Size die Größe des Diagramms aus.
- 12. Führen Sie im Abschnitt Table Layout die folgenden Aufgaben aus, um das Erscheinungsbild der Tabelle im Bericht zu bestimmen:
 - a. Wählen Sie in der Liste Columns die Informationen aus, die in den Spalten des Berichts erscheinen sollen.
 - b. Wählen Sie im Abschnitt Grouping aus, wie die Informationen im Bericht gruppiert werden.
 - c. Wählen Sie im Abschnitt Sorting aus, wie die Informationen sortiert werden.
- 13. Klicken Sie auf Save.

Bericht für Objektzählung über eine Linie

Der Bericht für Objektzählung über eine Linie zeigt Informationen über Objekte, die eine Linie überqueren, für eine bestimmte Zeit an.

1. Klicken Sie in der Oberfläche des Windows Client auf Reports. Der Report Designer wird in einem Browser geöffnet.
1. Melden Sie sich beim Report Designer an.
2. Klicken Sie auf New Report.
3. Geben Sie einen Namen für den Bericht ein.
4. Wählen Sie in der Liste Report Type den Eintrag Object Counts Across a Line aus.
5. Um anderen Benutzern das Ausführen des Berichts zu erlauben, wählen Sie Allow other users to run this report.
6. Klicken Sie auf OK.
7. Führen Sie im Abschnitt Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.

- b. Wählen Sie eine oder mehrere Kameras aus. Sie können nach Kameras anhand des Kameranamens suchen.
 - c. Klicken Sie auf OK.
- 8. Wählen Sie im Abschnitt Line die Linie aus, über die Objekte gezählt werden sollen.
- 9. Führen Sie im Abschnitt Date Range die folgenden Aufgaben aus, um die im Bericht enthaltenen Daten zu bestimmen:
 - a. Definieren Sie im Abschnitt Start including data from den Beginn der Daten.
 - b. Definieren Sie im Abschnitt Stop including data after das Ende der Daten.
 - c. Um Daten aus einem bestimmten Zeitbereich an jedem Tag zu verwenden, wählen Sie Use custom time range for data collection und geben Sie den Zeitbereich an.
- 10. Führen Sie im Abschnitt Schedule die folgenden Aufgaben aus, um zu bestimmen, wann der Bericht ausgeführt wird und welche Informationen er enthält:
 - a. Wählen Sie aus, ob der Bericht manuell oder nach einem Zeitplan ausgeführt werden soll.
 - b. Wenn Sie das Ausführen des Berichts nach einem Zeitplan auswählen, legen Sie den Zeitplan fest.
 - c. Geben Sie die Zeit an, ab der Daten für den Bericht erfasst werden sollen. Sie können eine relative Zeit basierend auf dem Bericht festlegen oder bestimmte Zeiten auswählen.
 - d. Wählen Sie aus, wie die Daten gruppiert werden sollen.
- 11. Führen Sie im Abschnitt Distribution die folgenden Aufgaben aus, um zu bestimmen, wie der Server Berichte verteilt:
 - a. Um den Bericht als E-Mail-Anhang zu versenden, wählen Sie Send report in email, geben Sie die E-Mail-Adressen der Empfänger an und wählen Sie die Dateiformate für die Berichte aus.
 - b. Um den Bericht als Datei zu speichern, geben Sie den Pfad an, definieren Sie den Dateinamen und wählen Sie die Dateiformate aus.
- 12. Führen Sie im Abschnitt Graph die folgenden Aufgaben aus, um das Erscheinungsbild des Diagramms im Bericht zu bestimmen:
 - a. Wählen Sie in der Liste Default Graph den anzuzeigenden Alarmtyp aus.
 - b. Wählen Sie in der Liste Graph Type aus, ob das Diagramm ein Linien- oder Balkendiagramm ist.
 - c. Wählen Sie in der Liste Graph Size die Größe des Diagramms aus.
- 13. Führen Sie im Abschnitt Table Layout die folgenden Aufgaben aus, um das Erscheinungsbild der Tabelle im Bericht zu bestimmen:
 - a. Wählen Sie in der Liste Columns die Informationen aus, die in den Spalten des Berichts erscheinen sollen.
 - b. Wählen Sie im Abschnitt Grouping aus, wie die Informationen im Bericht gruppiert werden.
 - c. Wählen Sie im Abschnitt Sorting aus, wie die Informationen sortiert werden.
- 14. Klicken Sie auf Save.

Bericht für Personenzählung mit Überkopf-Kameras

Der Bericht zur Personenzählung von oben zeigt Informationen über die Anzahl der von einer Deckenkamera gezählten Personen an.

1. Klicken Sie in der Oberfläche des Windows Client auf Reports. Der Report Designer wird in einem Browser geöffnet.
1. Melden Sie sich beim Report Designer an.
2. Klicken Sie auf New Report.
3. Geben Sie einen Namen für den Bericht ein.
4. Wählen Sie in der Liste Report Type den Eintrag Overhead People Count aus.
5. Um anderen Benutzern das Ausführen des Berichts zu erlauben, wählen Sie Allow other users to run this report.
6. Klicken Sie auf OK.
7. Führen Sie im Abschnitt Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.
 - b. Wählen Sie eine oder mehrere Kameras aus. Sie können Kameras nach Kameranamen suchen.
 - c. Klicken Sie auf OK.
8. Wählen Sie im Abschnitt Line die Linie aus, über die Personen gezählt werden sollen.
9. Führen Sie im Abschnitt Date Range die folgenden Aufgaben aus, um die im Bericht enthaltenen Daten festzulegen:
 - a. Definieren Sie im Abschnitt Start including data from den Beginn der Daten.
 - b. Definieren Sie im Abschnitt Stop including data after das Ende der Daten.
 - c. Um Daten aus einem bestimmten Zeitbereich an jedem Tag zu verwenden, wählen Sie Use custom time range for data collection und geben Sie den Zeitbereich an.
10. Führen Sie im Abschnitt Schedule die folgenden Aufgaben aus, um festzulegen, wann der Bericht ausgeführt wird und welche Informationen er enthält:
 - a. Wählen Sie aus, ob der Bericht manuell oder nach einem Zeitplan ausgeführt werden soll.
 - b. Wenn Sie auswählen, dass der Bericht nach einem Zeitplan ausgeführt werden soll, legen Sie den Zeitplan fest.
 - c. Geben Sie die Zeit an, ab der Daten für den Bericht erfasst werden sollen. Sie können eine relative Zeit basierend auf dem Bericht festlegen oder bestimmte Zeiten auswählen.
 - d. Wählen Sie aus, wie die Daten gruppiert werden sollen.
11. Führen Sie im Abschnitt Distribution die folgenden Aufgaben aus, um festzulegen, wie der Server Berichte verteilt:
 - a. Um den Bericht als Anhang per E-Mail zu senden, wählen Sie Send report in email, geben Sie die E-Mail-Adressen der Empfänger an und wählen Sie die Dateiformate für die Berichte aus.

- b. Um den Bericht als Datei zu speichern, geben Sie den Pfad an, definieren Sie den Dateinamen und wählen Sie die Dateiformate aus.
12. Führen Sie im Abschnitt Graph die folgenden Aufgaben aus, um das Erscheinungsbild des Diagramms im Bericht festzulegen:
 - a. Wählen Sie in der Liste Default Graph den anzuzeigenden Alarmtyp aus.
 - b. Wählen Sie in der Liste Graph Type aus, ob das Diagramm ein Linien- oder Balkendiagramm ist.
 - c. Wählen Sie in der Liste Graph Size die Größe des Diagramms aus.
13. Führen Sie im Abschnitt Table Layout die folgenden Aufgaben aus, um das Erscheinungsbild der Tabelle im Bericht festzulegen:
 - a. Wählen Sie in der Liste Columns die Informationen aus, die in den Spalten des Berichts angezeigt werden.
 - b. Wählen Sie im Abschnitt Grouping aus, wie die Informationen im Bericht gruppiert werden.
 - c. Wählen Sie im Abschnitt Sorting aus, wie die Informationen im Bericht sortiert werden.
14. Klicken Sie auf Save.

Objektstatistikbericht

Der Objektstatistikbericht zeigt Informationen über Objektverkehr und Verweildauer für eine bestimmte Zeit an.

1. Klicken Sie in der Oberfläche des Windows Client auf Reports. Der Report Designer wird in einem Browser geöffnet.
 1. Melden Sie sich beim Report Designer an.
 2. Klicken Sie auf New Report.
 3. Geben Sie einen Namen für den Bericht ein.
 4. Wählen Sie in der Liste Report Type den Eintrag Object Statistics aus.
 5. Um anderen Benutzern das Ausführen des Berichts zu erlauben, wählen Sie Allow other users to run this report.
 6. Klicken Sie auf OK.
 7. Führen Sie im Abschnitt Cameras die folgenden Aufgaben aus, um die Kameras hinzuzufügen, die Informationen für den Bericht liefern:
 - a. Klicken Sie auf Add Cameras.
 - b. Wählen Sie eine oder mehrere Kameras aus. Sie können nach Kameras anhand des Kameranamens suchen.
 - c. Klicken Sie auf OK.
 8. Führen Sie im Abschnitt Date Range die folgenden Aufgaben aus, um die im Bericht enthaltenen Daten zu bestimmen:
 - a. Definieren Sie im Abschnitt Start including data from den Beginn der Daten.
 - b. Definieren Sie im Abschnitt Stop including data after das Ende der Daten.

- c. Um Daten aus einem bestimmten Zeitbereich an jedem Tag zu verwenden, wählen Sie Use custom time range for data collection und geben Sie den Zeitbereich an.
9. Führen Sie im Abschnitt Schedule die folgenden Aufgaben aus, um zu bestimmen, wann der Bericht ausgeführt wird und welche Informationen er enthält:
 - a. Wählen Sie aus, ob der Bericht manuell oder nach einem Zeitplan ausgeführt werden soll.
 - b. Wenn Sie das Ausführen des Berichts nach einem Zeitplan auswählen, legen Sie den Zeitplan fest.
 - c. Geben Sie die Zeit an, ab der Daten für den Bericht erfasst werden sollen. Sie können eine relative Zeit basierend auf dem Bericht festlegen oder bestimmte Zeiten auswählen.
 - d. Wählen Sie aus, wie die Daten gruppiert werden sollen.
10. Führen Sie im Abschnitt Distribution die folgenden Aufgaben aus, um zu bestimmen, wie der Server Berichte verteilt:
 - a. Um den Bericht als E-Mail-Anhang zu versenden, wählen Sie Send report in email, geben Sie die E-Mail-Adressen der Empfänger an und wählen Sie die Dateiformate für die Berichte aus.
 - b. Um den Bericht als Datei zu speichern, geben Sie den Pfad an, definieren Sie den Dateinamen und wählen Sie die Dateiformate aus.
11. Führen Sie im Abschnitt Graph die folgenden Aufgaben aus, um das Erscheinungsbild des Diagramms im Bericht zu bestimmen:
 - a. Wählen Sie in der Liste Default Graph den anzuzeigenden Alarmtyp aus.
 - b. Wählen Sie in der Liste Graph Type aus, ob das Diagramm ein Linien- oder Balkendiagramm ist.
 - c. Wählen Sie in der Liste Graph Size die Größe des Diagramms aus.
12. Führen Sie im Abschnitt Table Layout die folgenden Aufgaben aus, um das Erscheinungsbild der Tabelle im Bericht zu bestimmen:
 - a. Wählen Sie in der Liste Columns die Informationen aus, die in den Spalten des Berichts erscheinen sollen.
 - b. Wählen Sie im Abschnitt Grouping aus, wie die Informationen im Bericht gruppiert werden.
 - c. Wählen Sie im Abschnitt Sorting aus, wie die Informationen sortiert werden.
13. Klicken Sie auf Save.

Anhang

Referenzinformationen für den Windows Client.

In diesem Abschnitt

- Open-Befehl
- Protokolldateien anzeigen
- Single Sign-On deaktivieren
- Timeout des SSL-Zertifikats konfigurieren

Open-Befehl

Sie können den Windows Client mit einem Befehl in der Befehlszeile öffnen. Darüber hinaus können Sie dem Befehl Argumente hinzufügen, die bestimmte Kameras und im Falle von PTZ-Kameras bestimmte Kamera-Voreinstellungen öffnen.

In der benutzerdefinierten Anwendungsentwicklung können Sie diesen Befehl mit einem Steuerelement verknüpfen, um den Windows Client aus einer anderen Anwendung heraus zu öffnen.

`ae.exe ai://server/camera/preset`

Wobei:

- server die Adresse des Servers ist
- camera die ID der Kamera ist
- preset die Voreinstellung für die PTZ-Kamera ist

Protokolldateien anzeigen

Sie können Protokolldateien für den Windows Client und alle Server-Instanzen, mit denen der Windows Client verbunden ist, anzeigen, durchsuchen und herunterladen.

1. Klicken Sie in der Oberfläche des Windows Client auf Hilfe > Detaillierte Protokolle anzeigen.
2. Wählen Sie im Feld Datum das Datum aus, für das Sie Protokolldateien anzeigen möchten.
3. Wählen Sie einen Server oder den Client aus.
4. Wählen Sie die anzuzeigende Protokolldatei aus.
5. Um die sichtbare Protokolldatei zu kopieren, klicken Sie auf In Zwischenablage kopieren.
6. Um Protokolldateien herunterzuladen, führen Sie die folgenden Schritte aus:
 - a. Klicken Sie auf Herunterladen.
 - b. Wählen Sie das Start- und Enddatum aus oder wählen Sie Alle Protokolle vom Server heruntergeladen aus.
 - c. Klicken Sie auf Herunterladen.
7. Um die sichtbare Protokolldatei zu durchsuchen, führen Sie die folgenden Schritte aus:
 - a. Geben Sie den Suchtext in das Textfeld ein.
 - b. Klicken Sie auf Weitersuchen.

Single Sign-On deaktivieren

Sie können die Single Sign-On-Option beim Wechseln von Benutzern und Registrieren neuer Farmen im Windows Client deaktivieren.

Wenn Sie Single Sign-On deaktivieren, ist das Kontrollkästchen Windows-Authentifizierung beim Benutzerwechsel oder bei der Registrierung einer neuen Server-Farm deaktiviert.

1. Öffnen Sie die Datei acc.ini unter %appdata%\Senstar8.
2. Fügen Sie im Abschnitt **[Main]** den folgenden Text hinzu:

```
DisableWindowsAuthentication=True
```

1. Speichern und schließen Sie die Datei acc.ini.

Timeout für SSL-Zertifikat konfigurieren

Sie können festlegen, wie lange der Windows Client auf ein gültiges Zertifikat wartet, bevor er auf eine Nicht-SSL-Verbindung zurückgreift.

Der Standard-Timeout für das SSL-Zertifikat beträgt 15000 Millisekunden.

1. Öffnen Sie die Datei acc.ini unter %appdata%\Senstar8.
2. Fügen Sie der Datei acc.ini den folgenden Text hinzu:

```
[Connectivity]  
ReceiveTimeoutInMilliseconds=timeout
```

Wobei timeout angibt, wie lange der Windows Client auf ein gültiges SSL-Zertifikat wartet.

1. Speichern und schließen Sie die Datei acc.ini.

Web Client

Der Web Client bietet Funktionen zur Kameraüberwachung, Videoverwaltung, Berichtserstellung und Alarmkonfiguration.

Der Web Client bildet den Windows Client so weit wie möglich nach. Die meisten Kernfunktionen des Windows Client stehen auch im Web Client zur Verfügung. Zusätzlich enthält der Web Client den Report Designer.

Jeder Server besitzt einen eigenen Web Client. Informationen zur Konfiguration des verwendeten Symphony-Servers finden Sie unter **General Settings: Web Client (EN)**.

Am Web Client anmelden

Sie können den Web Client in einem Webbrowser öffnen.

Über die Oberfläche des Web Client erreichen Sie zusätzlich die Konfigurationsoberfläche des Server.

1. Rufen Sie im Browser die IP-Adresse Ihres Server auf.
2. Wählen Sie in der Sprachliste Ihre Sprache aus.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
4. Klicken Sie auf die Schaltfläche Web Client.

Überwachung

Auf der Registerkarte **Überwachung** können Sie Live-Video und aufgezeichnete Aufnahmen ansehen sowie Alarmer einsehen.

Aufbau der Oberfläche

Die Oberfläche der Registerkarte **Überwachung** ist in folgende Bereiche unterteilt:

Datum

Über die Datumsauswahl oben links wählen Sie das Datum, dessen Aufzeichnungen in den Kameraansichten angezeigt werden sollen.

Kameras

Im Gerätebaum unter **Geräte** werden Kameras und Geräteordner aufgelistet. Klicken Sie auf eine Kamera, um sie in der aktiven Kachel anzuzeigen. Über das Feld **Suche...** lässt sich der Baum filtern; mit dem Symbol **Filter zurücksetzen** (🔄) heben Sie den Filter wieder auf.

Alarmer

Im Bereich **Alarmer** unten links werden zuletzt ausgelöste Alarmer mit den Spalten **Zeit**, **Kamera** und **Regel** aufgeführt.

Kachelraster

In der oberen Werkzeugleiste wählen Sie über die Schaltflächen **1**, **4**, **9** oder **16** die Anzahl der gleichzeitig angezeigten Kameraansichten.

Obere Werkzeugleiste

Rechts in der Kopfzeile finden Sie die Schaltfläche **Konfiguration** (Wechsel zur Konfigurationsoberfläche), **Über Symphony-Client** (Versions- und Hilfeinformationen), die

Sprachauswahl und **Abmelden**.

Verwandte Aufgaben

- Eine Kamera anzeigen

Eine Kamera anzeigen

Sie können eine Kamera im Web Client öffnen, um Live-Video oder Aufzeichnungen anzusehen.

1. Wählen Sie auf der Registerkarte **Überwachung** im Bereich **Kameras** eine Kamera aus dem Gerätebaum aus.
2. Verwenden Sie die Zeitleiste oberhalb des Videobildes, um zwischen Live-Wiedergabe und aufgezeichnetem Material zu wechseln.

Zeitleiste und Wiedergabesteuerung

Über der Kameraansicht wird eine Zeitleiste mit den Aufzeichnungen des gewählten Tages angezeigt. Klicken Sie auf eine Position in der Zeitleiste, um zu diesem Zeitpunkt zu springen.

Über die Wiedergabesteuerung navigieren Sie durch die Aufzeichnung:

- **Wiedergabe / Pause**
- **1 Bild zurück / 1 Bild vor**
- **1 Sek. zurück / 1 Sek. vorgehen**
- **10 Sek. zurück / 10 Sek. vorgehen**
- **Letzter Alarm / Nächster Alarm**
- **Letzte Aktivität / Nächste Aktivität**
- **Zum Live-Bild wechseln**

Bildausschnitt

In der Titelleiste der Kameraansicht stehen die Schaltflächen **Einzoomen** und **Auszoomen** zur Verfügung, um den dargestellten Bildausschnitt zu vergrößern oder zu verkleinern.

Kamerasteuerung

Bei Kameras mit entsprechender Hardwareunterstützung lassen sich folgende Bildparameter direkt im Web Client anpassen:

- **Iris+ / Iris-**
- **Helligkeit+ / Helligkeit-**
- **Fokus+ / Fokus-**
- **Kontrast+ / Kontrast-**

Berichte

Auf der Registerkarte **Berichte** verwalten und führen Sie Berichte des Web Client aus.

Liste der Berichte

Die Berichtsliste enthält folgende Spalten:

Name

Bezeichnung des Berichts.

Typ

Berichtstyp (zum Beispiel **Alarmbericht**).

Freigegeben

Zeigt an, ob andere Benutzer den Bericht ausführen dürfen.

Serientyp

Zeigt an, ob für den Bericht eine wiederkehrende Ausführung konfiguriert ist.

Zuletzt ausgeführt

Zeitpunkt der letzten Ausführung.

Erstellt

Zeitpunkt der Erstellung.

Aktionen

Wählen Sie einen Bericht in der Liste aus, um folgende Aktionen zu aktivieren:

- **Ausführen** – Bericht ausführen.
- **Bearbeiten** – Einstellungen des Berichts ändern.
- **Kopieren** – Bericht als Vorlage für einen neuen Bericht duplizieren.
- **Löschen** – Bericht entfernen.

Über die Schaltfläche **Bericht erstellen** oben rechts legen Sie einen neuen Bericht an. Siehe [Bericht erstellen](#).

Bericht erstellen

Sie können im Web Client einen neuen Bericht anlegen.

1. Öffnen Sie die Registerkarte **Berichte**.
2. Klicken Sie auf **Bericht erstellen**.
3. Geben Sie unter **Bezeichnung** einen Namen für den Bericht ein.
4. Wählen Sie unter **Bericht Typ** den gewünschten Berichtstyp:
 - **Alarmbericht**
 - **Alarmstatistik**
 - **Gesichtserkennungsbericht**
 - **Heat Map Darstellung**
 - **LPR-Bericht**
 - **Objektstatistik**
 - **Objektzählung**

- **Objektzählung mit virtueller Linie**
- **Personenzählung mit Überkopf-Kameras**
- **Retention Time Report**

5. Aktivieren Sie unter **Freigabe** das Kontrollkästchen **Andere Benutzer können diesen Bericht ausführen**, wenn andere Benutzer den Bericht ausführen dürfen sollen.
6. Klicken Sie auf **OK**.

Player

Der Player ist eine Anwendung zum Abspielen von Videodateien, die im Windows Client erzeugt wurden.

Der Player ist eine schlanke Lösung zum Anzeigen von Videos und Suchergebnissen aus dem Server. Standardmäßig wird der Player zusammen mit dem Windows Client und dem Server installiert; Sie können ihn aber auch als eigenständige Anwendung installieren.

Player installieren

Sie können den Player als eigenständige Anwendung installieren.

1. Laden Sie das Installationsprogramm herunter und führen Sie es aus.
2. Wählen Sie die Sprache aus und klicken Sie auf **OK**.
3. Lesen Sie die Lizenzbedingungen, wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
4. Wählen Sie den Installationsort aus.
5. Wählen Sie aus, ob das Remote Support Tool installiert werden soll.
6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Installieren**.
8. Klicken Sie auf **Schließen**.

Wasserzeichenprüfung aktivieren

Sie können die Wasserzeichenprüfung für den Player aktivieren, um zu verhindern, dass der Player manipuliertes Video abspielt.

1. Öffnen Sie die Datei acc.ini unter %appdata%\Senstar8.
2. Fügen Sie die folgenden Werte hinzu:

```
[VideoRecvCTRL]
UseWatermarking=True
```

1. Speichern und schließen Sie die Datei acc.ini.

Eine Videodatei abspielen

Sie können Video aus einer Datei oder von einer URL abspielen.

Videodateien können Sie aus Kameraansichtspanels oder Suchergebnissen im Windows Client exportieren.

Eine Video-URL können Sie erzeugen, indem Sie Suchergebnisse als E-Mail-Link exportieren. Um Video von einer URL abzuspielen, muss sich der Computer mit dem Player im selben Netzwerk wie der Server befinden.

1. Führen Sie im Player eine der folgenden Aufgaben aus:

- Um Video aus einer Datei abzuspielen, klicken Sie auf **File > Play From File**, navigieren Sie zur Datei und klicken Sie auf **Open**.
 - Um Video von einer URL abzuspielen, klicken Sie auf **File > Play From URL**, geben Sie die URL ein und klicken Sie auf **OK**.
2. Um Dekorationen anzuzeigen, klicken Sie auf **Decorations** und aktivieren oder deaktivieren Sie die Dekorationen.
 3. Um zu zoomen, klicken Sie auf **Zoom** und dann auf **Zoom In** oder **Zoom Out**.
 4. Um die Wiedergabegeschwindigkeit festzulegen, ziehen Sie den Regler **Speed** auf die gewünschte Geschwindigkeit.
 5. Verwenden Sie die folgenden Bedienelemente, um im Video zu navigieren:

Option	Beschreibung
Play/Pause	Video abspielen oder anhalten.
< snippet	Rückwärts zur letzten Aktivität im Video springen.
< frame	Ein Einzelbild zurückgehen.
frame >	Ein Einzelbild vorgehen.
snippet >	Vorwärts zur nächsten Aktivität im Video springen.
Schieberegler	Ziehen Sie den Schieberegler, um zur entsprechenden Position im Video zu navigieren.

Anhang

In diesem Abschnitt

- Versionshinweise
- Netzwerk-Ports
- Glossar
- Rechtliche Hinweise
 - Senstar Symphony Hinweise zu Drittanbietern

Versionshinweise

Release 8.12.1 (August 2026)

Fehlerbehebungen

Zusammenfassung	Beschreibung
NetSendHist-Problem	Ein Problem wurde behoben, durch das die CPU- und RAM-Auslastung auf einem Symphony-Server in bestimmten Umgebungen 100 % erreichen konnte.

Release 8.12.0 (Juli 2026)

Neue Funktionen

Zusammenfassung	Beschreibung
Geschütztes Videomaterial	Sicherheitspersonal und Administratoren können Aufnahmen einer Kamera oder Kameragruppe für einen definierten Zeitraum als geschützt markieren, damit sie nicht von der Aufbewahrungs-Engine gelöscht werden – mit berechtigungsbasiertem Schützen/Freigeben, Audit-Protokollierung und einer Verwaltungsansicht des geschützten Videomaterials.
OnGuard-Integration	Senstar Symphony bietet jetzt eine vollständige, ereignisgesteuerte Integration mit OnGuard 8.3/8.4.
SNMP-v3-Unterstützung	SNMP v3 mit Authentifizierungs- und Verschlüsselungsoptionen für erhöhte Cybersicherheit wurde ergänzt, zusätzlich zur bestehenden Unterstützung von SNMP v1/v2.
Video-Display-Engine-Umschalter in Startup	In Startup wurde ein Umschalter ergänzt, mit dem Benutzer zur neuen GPU-gestützten Display Engine wechseln können, mit dem Hinweis, dass Audioausgabe noch nicht unterstützt wird.
Externe Metadaten-Injektion	Die API bietet eine einfache Möglichkeit, Metadaten wie Paketdaten oder beliebige andere Daten für die erweiterte Suche in jede Kamera einzuspeisen.
Speicherwarnung für geschütztes Videomaterial	Administratoren können Warn- und Alarmschwellen konfigurieren, die ein Anmeldebanner auslösen, wenn geschütztes Video einen festgelegten Prozentsatz des Speicherplatzes überschreitet.
Audit-Bericht über Kameraverbindungen	Neuer Bericht über Verbindungs- und Trennungssitzungen von Benutzern und Kameras mit aggregierten Summen pro Stunde, Tag, Woche oder Monat sowie CSV-Export.
Blinkende Panelrahmen in der Advanced Alarm Console	Der Rahmen des Videopanel blinkt, wenn in der Advanced Alarm Console ein unbestätigter Alarm auftritt – sowohl in der Einzel- als auch in der Quad-Ansicht.

Zusammenfassung	Beschreibung
MP4-Export	Bediener können aufgezeichnetes Video im MP4-Format auf die lokale Festplatte exportieren.
Neuer Alarm für Kamera-/Server-Failover und Failback	Der Alarm kann verwendet werden, um Aktionen in der Rule Engine auszulösen.
Klartextmodus für die TCP-Aktion	Die TCP-Aktion kann Klartextnachrichten mit Unterstützung für Escape-Zeichen senden, statt des standardmäßigen XML-Formats.
Bearbeitbare Berechtigungen für SEM-verbundene Farmen	Berechtigungen, die nicht von Senstar Enterprise Manager (SEM) verwaltet werden, können jetzt über die Serverkonfiguration geändert werden, wenn eine Farm mit SEM verbunden ist.
Türstatusanzeigen auf Karten	Karten zeigen für integrierte Türen eine permanente Offen/Geschlossen-Anzeige statt eines kurzen Aufblinkens.
Option zum Deaktivieren des Failovers	Administratoren können das Failover über alle Gruppen hinweg für eine festgelegte Dauer vorübergehend deaktivieren und anschließend wieder aktivieren.

Verbesserungen

Zusammenfassung	Beschreibung
Metadaten-Aufbewahrung für geschütztes Videomaterial	Die Metadatenbereinigung berücksichtigt jetzt geschütztes Videomaterial korrekt und verhindert, dass Metadaten länger als nötig aufbewahrt werden.
Serverangabe im Banner für geschütztes Videomaterial	Das Speicherwarnbanner für geschütztes Videomaterial gibt in Multi-Server-Umgebungen jetzt an, für welchen Server es gilt.
Geschwindigkeitsgrenzen für synchronisierte Wiedergabe	Neue acc.ini-Option zum Festlegen der minimalen und maximalen Wiedergabegeschwindigkeit bei aktivierter synchronisierter Wiedergabe.
Umgang der neuen Video Display Engine mit Lücken im Edge-Speicher	Die Display Engine überspringt jetzt Lücken in Aufnahmen von Edge-Speicherkameras, statt für die gesamte Dauer der Lücke einen Verbindungsfehler anzuzeigen.
Höher aufgelöster Stream bei Maximierung/Vollbild	Panels wechseln jetzt zum höher aufgelösten Stream, wenn ein Panel maximiert oder in den Vollbildmodus geschaltet wird.
Konsistente Reihenfolge injizierter Metadaten-Dekorationen	Injizierte Metadaten-Dekorationen werden jetzt in einer konsistenten Reihenfolge angezeigt.
API-Zugriff auf Aktionen	Neue REST-API, gesichert durch einen API-Schlüssel, zum Auslösen vorhandener Aktionssätze und einzelner Aktionen aus externen Systemen.
Verbesserungen am Aufbewahrungsbericht	Der Bericht „Resource Recording Log“ zeigt jetzt, wer ihn erstellt hat, den vollständigen IP-/DNS-Namen der Kamera und klarere Integritätsberechnungen.
Zeitleisten werden nach Failover aktualisiert	Zeitleisten werden jetzt nach einem Failover oder Failback eines Servers aktualisiert, damit Bediener aktuelle Signaldaten sehen.
Korrekte Kamera-Serverzeit auf Zeitleisten	Zeitleisten verwenden jetzt die Zeit des Servers, der der jeweiligen Kamera zugeordnet ist, statt der Zeit der aktuell ausgewählten Farm.
Zeitleistenfarbe wird korrekt geladen	Zeitleisten zeigen nicht mehr kurzzeitig eine falsche Platzhalterfarbe an, bevor die tatsächlichen Aktivitätsdaten geladen sind.
Zuverlässige Einstellungsaktualisierungen	Ein seltenes Timing-Problem wurde behoben, durch das der Einstellungs-Poller eine Aktualisierung verpassen konnte.
Zuverlässigkeit geplanter HeatMap-Berichte	Geplante HeatMap-Berichte schlagen nicht mehr fehl, wenn einem Empfindlichkeitselement Attribute fehlen.
Hostnamen-Unterstützung der Gallagher-Integration	Das Serverfeld der Gallagher-Integration akzeptiert jetzt neben IP-Adressen auch Hostnamen und FQDNs.

Zusammenfassung	Beschreibung
OnGuard-Option zur erneuten Authentifizierung	Bestimmte OnGuard-Verbindungsfehler zeigen jetzt einen Nicht-Fehler-Zustand mit einer manuellen Option zur erneuten Authentifizierung im Knoten „Authentication Status“ an.
Schnellerer Start der AMAG-Integration	Die AMAG-Integration verwendet während der Initialisierung jetzt eine einzelne Verbindung, was die Startzeit bei Farmen mit vielen Geräten verkürzt.
LDAPS-Unterstützung	Unterstützung für sicheres LDAP (LDAPS) für Umgebungen, die verschlüsselte Verzeichnisverbindungen erfordern.
Validierung des CSV-Kameraimports	Der CSV-Kameraimport prüft jetzt vor dem Hinzufügen von Geräten, ob alle Pflichtfelder vorhanden sind.
Konfigurierbares Timeout beim Beenden von Diensten	Das Timeout, nach dem ein Dienst beim Herunterfahren zwangsweise beendet wird, ist jetzt konfigurierbar, mit einem höheren Standardwert von 10 Sekunden.
Geringere Datenbanklast durch Webdienst-Anfragen	Reduzierte SQL-Server-Last durch häufige Thin-Client-Kameraanfragen und Sitzungsverlängerungen auf großen Farmen.
License Plate Log über Mitternacht hinweg	Das License Plate Log aktualisiert sich jetzt ohne Interaktion weiter und zeigt die letzten 24 Stunden über Mitternacht hinweg korrekt an.
Details zu Fiber-Cut-Alarmen auf Karten	Die Karte des Senstar Symphony Clients zeigt jetzt Details zu „Fiber Cut“-Alarmen an, einschließlich Zonen-Polylinie und Meterangabe, analog zu Zoneneindringungsalarmen.
Neue Kartensymbole für aktivierte/deaktivierte DIO	Administratoren können beim Konfigurieren von DIO-Geräten auf einer Karte neue grüne (aktiviert) und rote (deaktiviert) Symbole auswählen.
Sicherere Fehlermeldungen	Fehlermeldungen im Configuration Manager und in der Webanwendung geben keine Stacktraces oder andere sensible Konfigurationsdetails mehr preis.
Verschlüsselte Bericht-URLs	Vom Configuration Manager erzeugte Bericht-URLs werden jetzt über HTTPS statt über unverschlüsseltes HTTP bereitgestellt.
Schnellere Regelbearbeitung in der Webkonfiguration	Verbesserte Performance beim Hinzufügen oder Bearbeiten von Regeln in der Webkonfigurationsoberfläche, insbesondere bei Farmen mit vielen Regeln.
Korrekte Meldungen beim Wiederherstellen von Online-Backups	Beim Wiederherstellen eines Online-Backups wird jetzt die tatsächliche von Xnet zurückgegebene Meldung angezeigt statt eines generischen Fehlers.
Größere Symbole in der Client-Titelleiste	Die Symbole in der Titelleiste des Senstar Symphony Clients wurden vergrößert, passend zum übrigen Standardumfang.
Optimierte Performance der OPC-Berichte (Overhead People Counting)	Schnellere Verarbeitung von OPC-Berichten durch vorberechnete Pfad- und Linienüberquerungsdaten.
Genauere KI-Objektzählung	Der Overhead-Algorithmus der KI-Objekterkennung und -verfolgung wurde verfeinert, um die Genauigkeit von Fahrzeugzählberichten und Zähllinien zu verbessern.

Fehlerbehebungen

Zusammenfassung	Beschreibung
Stabilität der synchronisierten Wiedergabe	Mehrere Probleme behoben, durch die synchronisierte Wiedergabepanels asynchron werden, bei Pause einfrieren oder während normaler Wiedergabe, beim Überspringen von Lücken und bei Neustarts kurz ein schwarzes Panel anzeigen konnten.
Wiedergabegeschwindigkeit und Scrubbing	Mehrere Probleme behoben: Der Geschwindigkeitsregler konnte sich unerwartet zurücksetzen, Scrubbing und Rückwärtswiedergabe von hochauflösendem oder H.265-Video liefen nicht flüssig, und ein Panel konnte nach dem Leeren und einem Client-Neustart zur alten Display Engine zurückwechseln.

Zusammenfassung	Beschreibung
Edge-Speicher-Downloads und Lücken in der Zeitleiste	Mehrere Probleme bei Edge-Speicher-Videodownloads und der Anzeige von Zeitleistenlücken behoben, darunter falsche Download-Startzeiten, inkonsistente Lückenmeldung zwischen Display Engine und Signalen, falsch eingefärbte Zeitleistenabschnitte und die fehlende Möglichkeit, Video direkt von einer Edge-Kamera abzuspielen.
Dekorations- und Overlay-Korrekturen der neuen Video Display Engine (VDE)	Mehrere Probleme mit Dekorationen und Bedienelementen der neuen VDE behoben, darunter fehlende oder falsch angewendete Wasserzeichen-, Zeitstempel- und Metadaten-Dekorationen, überlappende Dekorationen in Multi-View-Layouts sowie falsch dargestellte VDE-Steuersymbole und Transparenz.
Stabilität von Video Display Engine und Client	Zahlreiche Abstürze, Einfrieren, Hänger sowie Speicher- und CPU-Probleme behoben, die die VDE, Historical Video und den Senstar Symphony Client im normalen Betrieb, beim Panelwechsel und im Dauerbetrieb beeinträchtigten.
Zuverlässige Anzeige und Aktualisierung von Zeitleisten	Mehrere Probleme behoben, bei denen Panel- oder konsolidierte Zeitleisten nicht geladen wurden, falsch angezeigt wurden oder nicht mehr mit den Ereignisdaten übereinstimmten, einschließlich eines Sommerzeit-Problems an Sonntagen.
Alarmanzeige und Berechtigungen	Mehrere Probleme bei der Alarmverarbeitung behoben, darunter Alarmmarkierungen und Protokolleinträge, die Regel- oder Kartenberechtigungen nicht berücksichtigten, unzuverlässige Alarmnavigation und Vorereignis-Puffersignale, die bei IO-ausgelösten Alarmen nicht in Echtzeit gezeichnet wurden.
Weitergabe des Gerätemodells	Probleme bei der Weitergabe des Gerätemodells (ChangeMethod) behoben, darunter neu hinzugefügte Kameras, die erst nach einem Dienstneustart erschienen, und eine in seltenen Fällen nicht funktionierende Polling-basierte Weitergabe.
Kamerastatus und ONVIF-Erkennung	Falscher Offline-Kamerastatus im Gerätebaum und in der Zeitleiste behoben sowie ONVIF-Erkennungsprobleme, die bestimmte Kameramodelle falsch bezeichneten oder nicht erkannten.
Kartenkorrekturen	Mehrere Kartenprobleme behoben, darunter nicht gelöschte hervorgehobene Linien, falsche Standardstile beim Ziehen von Ausgangsknoten, nicht unterscheidbare Regelschaltflächen, fehlende Textkonturen und Karten, die nicht korrekt auf Klicks oder Ziehbewegungen reagierten.
Tracking-Links	Tracking-Links (Karten und Browser) korrigiert, die sich nicht zu einem Kamerapanel hinzufügen ließen oder die Auswahl im Gerätebaum nicht mehr aktualisierten.
Zuverlässigkeit der OnGuard-Integration	Mehrere Zuverlässigkeitsprobleme der OnGuard-Integration behoben, darunter Knoten, die nicht als offline erkannt wurden, Aux-Eingänge, die keine Statusänderungen erhielten, und Keep-Alive-Heartbeat-Fehler, von denen sich die Integration nicht erholte.
Wiederherstellung der AMAG-Integration	Behoben: Die AMAG-Integration erholte sich nicht, nachdem ihr Kommunikationskanal in einen Fehlerzustand geraten war.
Berichtskorrekturen	Mehrere Berichtsprobleme behoben, darunter geplante Berichte eines gelöschten Benutzers, die nicht versendet wurden, inkonsistentes Layout zwischen exportierten PDF- und E-Mail-Berichten, ungültige Zusatzzeilen im Recording Detailed Log und nicht ausblendbare Spalten im Aufbewahrungsbericht.
Serverzuverlässigkeit	Einen SQL-Deadlock behoben, der das Failback eines Senstar Symphony Servers verhindern konnte, sowie Mobile-Bridge-Multicast-Nachrichten, die mit einem nicht standardmäßigen internen Basisport nicht funktionierten.
Gerätebaum und Client-Einstellungen	Mehrere Probleme behoben, bei denen der Gerätebaum nicht aktualisiert oder korrekt geladen wurde – etwa nach Berechtigungsänderungen, verweigertem Ordnerzugriff und Serverentfernung – ohne dass ein Client-Neustart erforderlich ist.
RpcBridge.dll-Fehler beim Öffnen von Aira-Dateien	Fehlermeldung „RpcBridge.dll wurde nicht gefunden“ beim Öffnen einer heruntergeladenen .aira-Datei nach Installation des Player behoben.

Zusammenfassung	Beschreibung
Kamera kopieren/einfügen in der aktuellen VDE	Behoben: Die Option „Kamera kopieren/einfügen“ funktionierte für Kameras in der aktuellen VDE nicht.
Interner Serverfehler beim MP4-Export	Einen internen Serverfehler behoben, der den MP4-Export fehlschlagen ließ.
Umgehung der Digitalzoom-Berechtigung	Behoben: Ein Benutzer ohne die Berechtigung „Zoom über Clients steuern“ konnte weiterhin das Digitalzoom-Feld verwenden.
Gleichzeitige Metadaten-Injektionen	Ein Problem behoben, das mehrere exakt gleichzeitige Metadaten-Injektionen verhinderte.
PTZ-Preset-Berechtigung	Behoben: Benutzer mit ausschließlich der PTZ-Preset-Berechtigung konnten keine Presets verwenden, wenn die PTZ-Steuerung verweigert war.
Mobile-Bridge-Kamera-ID	Behoben: Aus dem Verlauf abgerufene Mobile-Bridge-Alarme lieferten eine leere Kamera-ID.
Kennzeichenerkennung über I/O-Eingang	Behoben: Unter „Integrationen“ konfigurierte digitale Eingänge lösten keine Kennzeichenlesungen aus.
Header der HTTP-Request-Aktion	Ein Problem behoben, das das Hinzufügen von Headern zur HTTP-Request-Aktion verhinderte.
Kompatibilität von Client-/Serverversionen	Falschen Kamerastatus und fehlerhafte Zeitleistenaktualisierungen behoben, wenn ein älterer Windows Client mit einem neueren Server verbunden wurde.
Audiowiedergabe mit gedrückter Strg-Taste	Behoben: Die Wiedergabe von Audiodateien funktionierte nicht, während die Strg-Taste gedrückt war.
Gebietsschema-abhängige Wiedergabegeschwindigkeit	Ein Parsing-Problem behoben, das auf nicht-englischen Windows-Gebietsschemata die Videowiedergabegeschwindigkeit auf 0 setzen konnte.
Nicht übersetzte Optionsfelder in „Gesichter suchen“	Nicht übersetzte Beschriftungen von Optionsfeldern im Fenster „Gesichter suchen“ behoben.
Unterstützung für Axis-Tastatur und -Jogdial	Unterstützung für die Axis-Tastatur T8312 und das Jogdial T8313 (sowie die neueren TU9002/TU9003) korrigiert.
Datumsangabe im Paneltitel	Behoben: Der Paneltitel zeigte „Gestern“ an, wenn der Tag vor dem gestrigen ausgewählt war.

Glossar

Aktionssatz

Eine geordnete Folge von Aktionen, die der Server ausführt, wenn eine [Regel](#) auslöst. Typische Aktionen sind Video aufzeichnen, einen Alarm auslösen, eine E-Mail senden, einen digitalen Ausgang schalten und einen Integrationsendpunkt aufrufen. Siehe [Aktionssätze](#).

Alarm

Ein [Ereignis](#) mit hoher Priorität, das eine Reaktion des Bedieners erfordert. Ein Alarm entsteht, wenn eine [Regel](#) auslöst, deren Aktionssatz die Aktion „Alarm erstellen“ enthält. Alarme durchlaufen einen Lebenszyklus: ausgelöst, angezeigt, bestätigt, gelöst, archiviert. Siehe [Alarme verwalten](#).

(Video-)Analyse

Software, die den Videostream einer Kamera analysiert, um zu erkennen oder zu klassifizieren, was in der Szene geschieht. Beispiele: Bewegungserkennung, Personen- und Fahrzeugverfolgung im Außenbereich, Gesichtserkennung. Analysen erzeugen [Ereignisse](#), auf die Regeln reagieren können. Siehe [Videoanalysen](#).

Karussell

Eine Ansichtspanel-Konfiguration, die automatisch eine Gruppe von Kameras durchläuft und jede für eine konfigurierte Dauer anzeigt. Nützlich, wenn ein Bediener mehr Kameras überwachen muss, als auf den Bildschirm passen. Siehe [Karussells](#).

Windows Client

Die Windows-Anwendung, mit der Bediener Video ansehen, auf Alarmer reagieren und Berichte erstellen. Wird auf dem Server-Host und auf Arbeitsstationen installiert. Siehe [Windows Client](#).

Gerät

Jede im Server konfigurierte Hardware: Kameras, Zutrittskontrollleser, digitale Ein-/Ausgabe-Hardware, Eindringensensoren, Videowall-Endpunkte. Der [Gerätebaum](#) organisiert sie für die Bediener.

Gerätebaum

Die hierarchische Geräteliste im Windows Client. Administratoren steuern ihre Struktur über Gerätegruppen.

Ereignis

Ein einzelnes, mit Zeitstempel versehenes Vorkommnis im System: Bewegung hat begonnen, ein Gesicht wurde erkannt, eine Tür wurde geöffnet, ein digitaler Eingang wurde aktiv. Ereignisse sind das Rohmaterial, das [Regeln](#) verarbeiten. Siehe [Ereignisse](#).

Serverfarm

Zwei oder mehr Server-Instanzen, die eine gemeinsame Konfiguration nutzen und als ein einziges System auftreten. Kameras, Regeln, Benutzer und Sicherheitsprofile werden einmal definiert und gelten für die gesamte Farm. Siehe [Einstellungen](#).

Sichtfeld (FoV)

Der Bereich einer Szene, den eine Kamera mit ihrem Objektiv und ihrer Montage tatsächlich erfassen kann. Wird als Form auf Lageplänen angezeigt, um Abdeckung und Lücken darzustellen. Siehe [Sichtfeld anzeigen](#).

Integration

Eine direkte Verbindung zwischen dem Server und einem Drittsystem (Zutrittskontrolle, Perimetersensoren, Spezialhardware). Die Integration bildet die Ereignisse des Drittsystems auf Senstar Symphony-Ereignisse ab, auf die Regeln reagieren können. Siehe [Integrationshardware hinzufügen](#).

Verarbeitungsmaske

Eine Form (oder mehrere Formen) im Kamerabild, die einer Videoanalyse mitteilt, welche Pixel ignoriert werden sollen. Dient dazu, Bereiche auszuschließen, in denen die Analyse Störungen erzeugen würde (bewegtes Laub, vorbeifahrender Verkehr, Zeiteinblendungen).

Aufbewahrung

Das maximale Alter aufgezeichneten Videos, bevor der Server es löscht. Wird pro Kamera, pro Server oder pro Farm festgelegt, wobei die Einstellung pro Kamera Vorrang hat. Siehe [Videospeicher für eine Kamera konfigurieren](#).

Regel

Die Automatisierungseinheit in Senstar Symphony. Eine Regel besteht aus einem [Ereignis](#) (Auslöser), einem [Aktionssatz](#) (was zu tun ist), einem [Zeitplan](#) (wann sie aktiv ist) und einem Schweregrad. Siehe [Regeln](#).

Zeitplan

Ein wiederkehrendes Zeitfenster, in dem eine [Regel](#) aktiv ist. Zeitpläne sind über mehrere Regeln hinweg wiederverwendbar. Siehe [Zeitpläne](#).

Sicherheitsprofil

Ein wiederverwendbares Berechtigungspaket. Profile werden [Gruppen](#) zugeordnet; Benutzer erben sie über ihre Gruppenmitgliedschaft. Siehe [Sicherheitsprofile](#).

Server

Der zentrale Dienst einer Senstar Symphony-Installation. Zeichnet Video von Kameras auf, führt die [Regel-Engine](#) aus, speichert Ereignisse und Alarmer und setzt Berechtigungen durch. Siehe [Server](#).

Standort

Eine logische Gruppierung von Kameras und Geräten, die einen physischen Ort darstellt (ein Gebäude, ein Gelände, einen Perimeterabschnitt). Wird für Berechtigungen, Berichte und die Kartenorganisation verwendet.

Zustand

Der konkrete melde- oder betriebsrelevante Zustand eines Sensors oder Geräts, etwa Alarm, Maskierung, Überwachung oder Normal (gesichert).

Vorlage

Eine gespeicherte Sammlung von Kamera-Konfigurationseinstellungen, die auf andere Kameras angewendet werden kann, um wiederholte Einrichtung zu vermeiden. Siehe [Vorlagen](#).

Benutzergruppe

Ein Container für Benutzer. Sicherheitsprofile werden Gruppen zugeordnet; Benutzer erben Berechtigungen aus den Gruppen, denen sie angehören. Ein Benutzer kann mehreren Gruppen angehören; die Berechtigungen ergeben sich aus der Vereinigungsmenge. Siehe [Gruppen](#).

Ansichtspanel

Ein rechteckiger Bereich im Arbeitsbereich des Windows Client, der eine Inhaltsquelle anzeigt — Live-Video, aufgezeichnetes Video, eine Karte, einen Browser, ein Karussell oder eine Alarmansicht. Siehe [Ansichtspanels](#).

Web Client

Ein browserbasierter Client, der ähnliche Funktionen wie der Windows Client bietet, ohne dass Software installiert werden muss. Siehe [Web Client](#).

Netzwerk-Ports

Die Software des Server verwendet standardmäßig die folgenden Netzwerk-Ports.

Netzwerkkonfiguration für Einzelserver

Port	Protokoll	Beschreibung
80	TCP	HTTP-Webserver, der für die Serverkonfiguration auf HTTPS auf Port 443 weiterleitet
443	TCP	Sicherer HTTPS-Webserver für die Serverkonfiguration
8433	TCP	Senstar Symphony Mobile Bridge (Listening-Port für mobile Geräte)
8434	TCP	Senstar Symphony Mobile Bridge (Listening-Port für Ereignisse)
8488	TCP	Senstar Symphony Mobile Bridge (Listening-Port für Video-Proxy)
50000	TCP	HTTP-Webserver für den Web-Client
50001	TCP	Webdienst (Steuerungs- und Benachrichtigungsport)
50010	TCP	RTSP für Live- und historisches Video
50014	TCP	Sicherer HTTPS-Webserver für den Web-Client (sofern konfiguriert)

Netzwerkkonfiguration für Serverfarmen

Port	Protokoll	Beschreibung
80	TCP	HTTP-Webserver, der für die Serverkonfiguration auf HTTPS auf Port 443 weiterleitet
443	TCP	Sicherer HTTPS-Webserver für die Serverkonfiguration
1433	TCP	Ausgehende Regel für SQL-Server in der SQL-Server-Firewall
1434	UDP	Port für SQL-Kommunikation
5045	UDP	Port für Zustandsüberprüfungen
8433	TCP	Senstar Symphony Mobile Bridge (Listening-Port für mobile Geräte)
8488	TCP	Senstar Symphony Mobile Bridge (Listening-Port für Video-Proxy)
50000	TCP	HTTP-Webserver für den Web-Client
50001	TCP	Webdienst (Steuerungs- und Benachrichtigungsport)
50004	TCP	Port für Server-Subdienste
50010	TCP	RTSP für Live- und historisches Video
50014	TCP	Sicherer HTTPS-Webserver für den Web Client (sofern konfiguriert)

Zusätzliche Netzwerkkonfiguration

Port	Protokoll	Beschreibung
5041	TCP	Zutrittskontrolle
50002	TCP	SSO-Authentifizierungsanfragen
50005	TCP	Videowand
50015	TCP	SSO-Authentifizierungsanfragen und Kryptografie

Rechtliche Informationen

Copyright © 2026 Senstar Corporation und/oder ihre Lizenzgeber. Alle Rechte vorbehalten.

Dieses Material dient ausschließlich zu Informationszwecken. Senstar gibt keinerlei ausdrückliche, stillschweigende oder gesetzliche Garantien hinsichtlich der in diesem Dokument enthaltenen Informationen.

Die Einhaltung aller geltenden Urheberrechtsgesetze liegt in der Verantwortung des Benutzers. Ohne Einschränkung der urheberrechtlichen Rechte darf kein Teil dieses Dokuments ohne ausdrückliche schriftliche Genehmigung der Senstar Corporation in irgendeiner Form oder mit irgendwelchen Mitteln (elektronisch, mechanisch, durch Fotokopie, Aufzeichnung oder anderweitig) oder zu irgendeinem Zweck reproduziert, in einem Datenspeichersystem gespeichert oder eingebracht oder übertragen werden.

Senstar kann Patente, Patentanmeldungen, Marken, Urheberrechte oder andere geistige Eigentumsrechte besitzen, die den Gegenstand dieses Dokuments betreffen. Sofern nicht ausdrücklich in einer schriftlichen Lizenzvereinbarung von Senstar gewährt, verleiht die Bereitstellung dieses Dokuments keinerlei Lizenzen für diese Patente, Marken, Urheberrechte oder anderes geistiges Eigentum.

Senstar und das Senstar-Logo sind eingetragene Marken der Senstar Corporation.

Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

Senstar Symphony Drittanbieter-Hinweise

Komponente	Hinweis
ARH Carmen ANPR/LPR	Copyright © 1993-2015. Alle Rechte vorbehalten. EULA
Boost Software	Copyright © 1998-2005 Beman Dawes, David Abrahams. Copyright © 2004-2007 Rene Rivera. Boost ist unter der Boost Software License lizenziert.
Crypto++	Copyright © 1995-2013 Wei Dai. Alle Rechte vorbehalten. Crypto++ ist unter der Boost Software License lizenziert.
CxImage	Copyright © 2001-2008 Davide Pizzolato. CxImage ist unter dieser Lizenz lizenziert.
Cybertec Patroni	Copyright © 2000–2021 CYBERTEC PostgreSQL International GmbH.
Dapper	Dapper ist unter der Apache License 2.0 lizenziert.

Komponente	Hinweis
DevExpress WinForms	Copyright © 1998-2021 Developer Express Inc. EULA
DirectShow.NET Library	Copyright © 1991, 1999 Free Software Foundation, Inc. Die DirectShow.NET Library ist unter der GNU Lesser General Public License (LGPL) Version 2.1 lizenziert.
excellibrary	Die excellibrary ist unter der GNU Lesser General Public License (LGPL) lizenziert.
FFmpeg	Copyright © 2007 Free Software Foundation, Inc. FFmpeg ist unter der GNU Lesser General Public License (LGPL) Version 2.1 oder höher lizenziert.
gson	Copyright © 2008 Google Inc. google/gson ist unter der Apache License 2.0 lizenziert.
Intel Integrated Performance Primitives	Copyright © Intel Corporation. EULA
Jayrock	Copyright © Atif Aziz. Alle Rechte vorbehalten. Jayrock ist unter der GNU Lesser General Public License (LGPL) lizenziert.
Joda-Time	Copyright © 2002-2018 Joda.org. Alle Rechte vorbehalten. Joda-Time ist unter der Apache License 2.0 lizenziert.
libcurl	Copyright © 1996-2018, Daniel Stenberg. Alle Rechte vorbehalten. libcurl ist unter dieser Lizenz lizenziert.
libjpeg	Copyright © 1991-2018 Thomas G. Lane, Guido Vollbeding.
Live555	Copyright © Live Networks, Inc. Alle Rechte vorbehalten. Live555 ist unter der GNU Lesser General Public License (LGPL) lizenziert.
Microsoft .NET Library	Copyright © 2021 Microsoft EULA
OpenH264	Copyright © 2013, Cisco Systems. OpenH264 ist unter dieser Lizenz lizenziert.
OpenCV	Copyright © 2018 OpenCV team. OpenCV ist unter dieser Lizenz lizenziert.
OpenSSL	Copyright © 1998-2018 The OpenSSL Project. Alle Rechte vorbehalten. OpenSSL ist unter dieser Lizenz lizenziert.
PaddlePaddle/Paddle	Copyright © 2016 PaddlePaddle Authors. Alle Rechte vorbehalten. PaddlePaddle/Paddle ist unter der Apache License 2.0 lizenziert.
PostgreSQL	Copyright © 1996-2021 The PostgreSQL Global Development Group. PostgreSQL ist unter The PostgreSQL Licence lizenziert.

Komponente	Hinweis
RapidXML	Copyright © 2006, 2007 Marcin Kalicinski. RapidXML ist unter der Boost Software License lizenziert.