SIEMENS

Datenblatt

Siveillance Video Advanced

Für mittlere bis große Anlagen
2019 R3

Eine leistungsstarke Lösung für mittlere bis große Anlagen mit mehr als 140 Funktionen und Merkmalen

Siveillance Video Advanced ist ausgelegt für zentral verwaltete Multi-Server-Einrichtungen, die über mehrere Standorte verteilt sein können, an denen eine Überwachung rund um die Uhr erforderlich ist. Die Lösung bietet eine zentrale Verwaltung aller Geräte, Server und Benutzer und ermöglicht eine äußerst flexible Regelmaschine, die durch Zeitpläne und Ereignisse gesteuert wird.

Haupteigenschaften: Video Advanced

- Hardwarebeschleunigte Video-Bewegungsdetektion (VMD)
- Unterstützung von H.265
- Zentrale Verwaltung
- Flexible Regel-Engine
- Edge-Speicherung
- Hardwarebeschleunigte Video-Decodierung mittels NVIDIA GPU
- Multicast-Unterstützung
- Redundanzoption für hohe Verfügbarkeit
- Hot- und Cold-Failover-Aufzeichnungsserver
- Kerberos-Authentifizierung
- Zweistufige Verifikation
- Smart Map – Offline-Unterstützung
- Unterstützung der Zutrittskontrolle über Smartphone
- DLNA Ready
- Online Aktivierung

Siveillance Video Advanced Übersicht

Produktfakten

• Anlagentyp	zentrale Verwaltung, Multi-Server
• Anzahl der Kameras pro System	unbegrenzt
• Anzahl der Aufzeichnungsserver	unbegrenzt
• Anzahl der Benutzer	unbegrenzt
• Video-Exportformat	AVI, MKV
• Unterstützte Hersteller	134 Plus
• Unterstützte IP-Geräte	5800 Plus
• Generische Hardware-Erkennung	UPnP
• Audio(1)	Vollduplex, Halbduplex
• Offene Standards	ONVIF: Profil S/G, PSIA
• Videokomprimierung	MJPEG, MPEG-4 AVC, MPEG-4, MxPEG, H.263, H.264, H.265

Systemkomponenten
- Siveillance™ Video Management (Client / Server)
- Siveillance™ Video Aufzeichnungsserver
- Siveillance™ Video Ereignisserver (Ereignisse / Alarme)
- Siveillance™ Video Mobile (Client / Server)
- Siveillance™ Video - Video-Client Player (Export / lokale Wiedergabe)
- Siveillance™ Video Service Channel
- Siveillance™ Video Log-Server

Hauptmerkmale
- Verzeichnisdienst – Microsoft™ Active Directory
- Zentrale Verwaltung – Überwachung / Verwaltung (lokale / entfernte Standorte)
- Integrierte Regel-Engine – Ereignis / Bedingung / Aktion
- Archivierung von Videoaufzeichnungen
- Integriertes Alarmmanagement
- Intuitive Pläne / Smart Maps
- HTTP über SSL / TLS
- Cross-Version-Management / Kompatibilität (2)
- ONVIF Gateway Interface – Private-to-Public Video, Alarmzentralen und Monitoring-Stationen
- Failover-Management (redundanter Cluster)
- Hohe Verfügbarkeit über Microsoft™ Clustering
- Siveillance™ VMS Monitoring Wall – optional
- Edge-Speicherung (Aufzeichnung/Wiedergabe/Synchronisation)
- Multicast Streaming
- Kerberos-Authentifizierung
- Skalierbare Videoqualität Recording™ (SVQR)
- Zweistufige Verifikation
- Hardwarebeschleunigte Video-Decodierung für Video-Bewegungsdetektion (Quick Sync)
- Hardwarebeschleunigte Video-Decodierung für Video-Bewegungsdetektion (NVIDIA)
- Anschluss DLNA-unterstützter TV-Bildschirme
- Privatzonen (permanent und aufhebbar)
- Öffnen / Schließen von Türen / Gewähren und Verweigern von Zutritt mittels der Applikation Siveillance Video MobileAccess
- Verschlüsselung bei der Kommunikation vom Aufzeichnungsserver

Verteilte Systeme
- Siveillance™ Video Interconnect – Remote Site
- Siveillance™ Video Verbundarchitektur – Remote Site

Installer
- Ein-Klick-Installer(automatische Erkennung von Geräten und Konfiguration der Speicherdauer)
- Wizard-basierte Schnittstelle für Plug-In

Operative Intelligenz
- Metadaten – Ernten / Automatisierung
- Eingebaute Video-Bewegungserkennung (VMD)
- Einstellbare VMD-Empfindlichkeit
- Echtzeit-VMD-Analyse
- VMD Ausschlusszonen

Bildverarbeitung
- Einstellbare GOP-Größe (MPEG4 / H.264)
- Dual-Stream (Live / Aufzeichnung)
- Einstellbares Downsampling (Auflösung / FPS)
- Konfigurierbare Aufzeichnungsgeschwindigkeit (Bewegung / Ereignis / Zeitplan)
- Konfigurierbarer Vor-/Nachalarmbild-Puffer
- Vorpuffer im Speicher

Audio
- AAC-Audiokommunikation (Vollduplex, Halbduplex)
- Audioaufzeichnung (Halbduplex)
- Unbegrenzte Anzahl Audiokanäle
- Zweiwege-Audio im web/mobile client

Pan-Tilt-Zoom (PTZ)
- Unbegrenzte Anzahl Positionen pro Kamera
- Go-to preset on event (Position anfahren bei Ereignis)
- Voreingestellte Patrouillen über Regeln
- Kombination von Patrouille und Go-to-Preset auf Event
- Konfigurierbare Scan-/Übergangsgeschwindigkeit
- Anzahl der PTZ-Prioritätsstufen – 32000
- Reservierung von PTZ-Priorität und Rechten über Video-Client

Alarme
- Alarmverwaltung (Neuzuordnung, Status, Kommentar)
- Alarmkonfiguration (Beschreibung, Arbeitsanweisungen, ursprüngliche Eigentümer, Zeitprofile, Alarmergebniscodes, Alarmprioritätsstufen)
- Alarmbehandlung (Ansicht ausgelöste Alarme, Report, Log, Status)
- Alarmmeldung (E-Mail, Mehrfachbenachrichtigungsprofile)
- Alarmprioritätsstufen – 32.000
- Maximale Anzahl der Kamera-Popups im Vorschaufenster – 15
- SNMP TRAP-Unterstützung

Speicherung und Langzeitarchivierung
- Speicherdauer für Videos – unbegrenzt
- Aufnahmekapazität pro Gerät/Tag – unbegrenzt
- Online-Zugriff auf Archive
- Konfigurierbare Speicherdauer (pro Gerät, pro Gruppe)
- Speicherübersicht (Platzbedarf)
- Meldung bei vorzeitiger Löschung von Videos aufgrund von nicht ausreichendem Speicherplatz
- Archivierungspläne (min. – stündlich, max. – praktisch unbegrenzt)
- Archivierung von Aufzeichnungen
- Archivierung auf Netzlaufwerk (NAS, iSCSI, SAN)
- Unterstützung der Live-Videodarstellung ohne Aufzeichnung

Integrationen (3)
- Integration von Plugins, Protokollen, Komponenten über MIP SDK
- Integration der Metadaten von Fremdfirmen über MIP SDK
- Integration der Ereignis- und Aktionsregel-Engines von Fremdfirmen über MIP SDK
- Integration von Siemens-Security-Produkten
  - SiPass integrated™ über MIP SDK
  - Siveillance™ Vantage über MIP SDK
  - Siveillance™ Site IQ Analytics(4)
  - Desigo CC – über MIP SDK

Video Clients
- Hardwarebeschleunigte Video-Decodierung mit mehreren NVIDIA-Karten
- Maximale Anzahl an Kunden – unbegrenzt
- Anpassbarer IP-Bereich und -Port mit NAT-Unterstützung
- Benutzerberechtigung (lokale Windows-Konten, Microsoft™ Active Directory, VMS-Anwendungskonten)
- Zuweisen von Ad-hoc-Inhalten zu Monitor-Wall (Alarme, Bilder, Lesezeichen, Pläne, Kamerasequenzen)
- Anpassbares Dashboard mit Drilldown-Möglichkeit E-Mail, Alarm, Benachrichtigung)
- Echtzeit-Systemmonitor
- Einfache Handhabung beim Export

www.siemens.com/siveillance-vms

Siveillance Video Advanced Übersicht

I/O und Ereignisse
- Soft I/O (Bewegung, Sabotage, Temperatur)
- Hardwire I/O (Taster, Sensor)
- Ereignis-Trigger (Audio-Erkennung, Eingabe-Trigger, System-Benachrichtigung, Kommunikationsausfall)
- Ereignisaktion (Benachrichtigung: E-Mail, Abspielen von Audioclips, Matrixsteuerung, Gerätekonfiguration)

Verwaltung
- Mehrere Benachrichtigungsprofile
- Konfigurationsassistenten für unterstützte Systemeinrichtung
- Geräteverwaltung (Gerätegruppierung, Gerätemodellerkennung, Geräteaustauschassistent)
- Nahtloses virtuelles Verschieben von Hardware zwischen den Aufzeichnungsservern
- Zentrale Verwaltung (Aufzeichnungsserver-, Benutzerverwaltung)
- Zentrale Verwaltung der Siveillance VMS-Video-Clientanwendung – max. 3 Video-Client-Profile
- Anpassung der Zeitprofile an Tageslänge
- "On-the-fly"-Konfigurationsänderungen
- Betrieb der Server als Windows-Dienste
- Start / Stopp von Geräten nach Zeitplan
- Integrierte Unterstützung für Sicherung und Wiederherstellung
- Offline-Lizenzaktivierung
- 4-Augen-Prinzip für Anmeldung
- Benutzerzugriffsberechtigung pro Client
- Smart Map – Offline-Unterstützung
- Web-Client-Alarmliste
- Einfache Installation

Reporte und Protokolle
- Systemprotokoll
- Audit-Log
- Regelprotokoll
- Konfigurationsreport

Siveillance Video Monitor Wall
- Siveillance™ Video Monitor Wall – Zusatzprodukt (optional)
- Anzahl der Siveillance™ VMS Monitor Walls – unbegrenzt
- Anzahl gleichzeitig angesehener Videoströme – unbegrenzt
- Maximale Anzahl Videoströme pro Bildschirm – 100
- Voreinstellungen für Display-Layouts und Kamerainhalte
- Aktivierung einer regelbasierten Steuerung (Layout/Inhalte)

Siveillance ™ Video Access
- Türen – bis zu 5000
- Ereignisse – bis zu 600 Ereignisse pro Sekunde
- Anbindung mehrerer Zutrittskontrollsysteme
- Gruppierung von Zutrittspunkten
- Erweiterte Protokolle und Audit Trail
- Dynamische Synchronisation der Konfiguration vom Subsystem zu SiVMS

Siveillance™ Video SiPass integrated – Einschränkungen für Plugins
- Türen – bis zu 1000
- Personen – bis zu 6000
- Ereignisse – bis zu 45 Ereignisse pro Sekunde

Sprachen * (Management Interface)
- Chinesisch (traditionell), Dänisch, Englisch, Französisch, Deutsch, Italienisch, Japanisch, Koreanisch, Portugiesisch (Brasilianisch), Russisch, Spanisch, Schwedisch, Türkisch

Was ist Neu bei- 2019 R3

- Zentrale Suche in Smart Client
- Siveillance Video Driver Framework
- Adaptive Streaming
- Device Password Management

(1) Möglichkeit der Dekodierung komprimierter Audio-Streams und Audiowiedergabe auf einem Client.
Vollduplex – Datenübertragung in beide Richtungen gleichzeitig
Halbduplex – Datenübertragung jeweils nur in einer Richtung

(2) Der zentrale Standort muss Siveillance™ Video Pro 2019 sein.

(3) Siveillance Video bietet die Möglichkeit, Verwaltungsstationen von Drittanbietern nahtlos über das MIP SDK zu integrieren. Dabei werden drei Integrationsarten unterstützt: Grundlegende Protokollintegration, komponentenbasierte Integration über die .NET-Bibliothek und Plug-In-Integration zum Einbetten von Plug-Ins in Siveillance Video.

***** Eine Beschreibung aller Funktionalitäten sowie eine Übersicht der unterstützten Sprachen finden Sie im **Siveillance Video Comparison Guide**.
www.siemens.com/siveillance-VMS

Haftungsausschluss Cyber Security

Siemens offeriert ein Portfolio von Produkten, Lösungen, Systemen und Dienstleistungen mit Sicherheitsfunktionen, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Im Geschäftsfeld der Gebäudetechnik umfasst dies Systeme für Gebäudeautomation und -leittechnik, Brandschutz, Sicherheitsmanagement und physische Sicherheitssysteme.
Um Anlagen, Systeme, Maschinen und Netzwerke vor Online-Bedrohungen zu schützen, ist es erforderlich, ein ganzheitliches, dem neuesten Stand der Technik entsprechendes Sicherheitskonzept zu implementieren und stets auf dem aktuellen
Stand zu halten. Das Portfolio von Siemens bildet nur einen Bestandteil eines solchen Konzeptes. Sie sind dafür verantwortlich, unbefugten Zugang zu Ihren Anlagen, Systemen, Maschinen und Netzwerken zu verhindern. Diese sollten nur mit einem Netzwerk oder dem Internet verbunden werden, wenn und soweit die Verbindung erforderlich ist und angemessene Sicherheitsvorkehrungen (z. B. Firewalls bzw. Netzwerksegmentierung) vorhanden sind. Darüber hinaus sind die Sicherheitsempfehlungen von Siemens zu beachten. Für nähere Informationen kontaktieren Sie bitte Ihren Ansprechpartner bei Siemens oder besuchen Sie unsere Webseite http://www.siemens.com/industrialsecurity.
Zur Verbesserung der Sicherheit wird das Portfolio von Siemens kontinuierlich weiterentwickelt. Siemens empfiehlt dringend, Updates zu verwenden, sobald diese zur Verfügung stehen, und stets die neusten Versionen zu verwenden. Werden Versionen verwendet, die nicht mehr unterstützt werden, oder werden neueste Updates nicht verwendet, kann sich Ihr Risiko bezüglich Online- Bedrohungen erhöhen. Siemens empfiehlt dringend, Sicherheitsempfehlungen zu den neuesten Sicherheitsgefährdungen, Patches und damit verbundenen Massnahmen zu befolgen, die unter anderem unter https://www.siemens.com/cert/de/cert-security-advisories.htm veröffentlicht werden.

Technische Daten und Verfügbarkeit können ohne Vorankündigung geändert werden.

Siemens Switzerland Ltd
Smart Infrastructure
Global Headquarters
Theilerstrasse 1 a
6300 Zug,
Schweiz.
Phone : +41 41 724 24 24