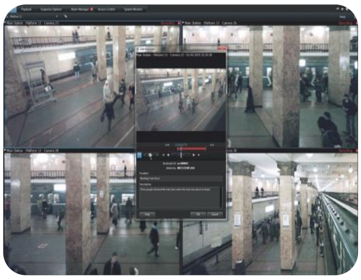
SIEMENS

Ingenuity for life

Data Sheet

Siveillance Video Advanced

For Medium To Large Solutions
2020 R3



A powerful solution for medium to large deployments including more than 140 features and functions

The Siveillance Video Advanced is designed for centrally managed multi-server deployments including large multi-site and multiple server installations requiring 24/7 surveillance, with support of multiple devices. The solution offers centralized management of all devices, servers and users, and empowers an extremely flexible rule engine driven by schedules and events:

Main features: Siveillance Video Advanced

- Hardware accelerated Video Motion Detection (VMD)
- Redundancy Option for High Availability
- Supports H.265
- Centralized Management
- Flexible Rule Engine
- Centralized Search in Smart Client
- Adaptive Streaming (Video & Web Client)
- Siveillance Video Driver Framework
- Device & Password Management
- Edge Storage
- Hardware accelerated video decoding using NVIDIA GPU
- Smart Map – offline support
- Multicast Support
- DLNA ready
- Hot & cold failover recording server
- Kerberos Authentication
- Two-step verification
- Online Activation
- Adding Devices on HTTPS
- Direct streaming method - Mobile server
- Location search using GPS Coordinates
- People, Vehicle & Location Search Filters

Siveillance Video Advanced Overview

Product Facts

Deployment type	Centrally managed, Multi-server
Number of cameras per system	Unlimited
Number of recording servers	Unlimited
Number of users	Unlimited
Video export format	AVI, MKV
Supported manufacturers	134 Plus
Supported IP devices	10,000+
Generic hardware discovery	UPnP
Audio[1]	Full Duplex,Half Duplex
Open standards	ONVIF: Profile-S/G/T/Q, PSIA
Video compression	MJPEG, MPEG-4 AVC, MPEG-4, MxPEG, H.263, H.264, H.265, H.264+,H.265+

System Components

- Siveillance Management (Client / Server)
- Siveillance Video Recording server
- Siveillance Video Event server (Events/ Alarms)
- Siveillance Video Mobile (Client/ Server)
- Siveillance Video – Video Client Player (Export/ Local Playback)
- Siveillance Video Service Channel
- Siveillance Video Log server

Key Features

- Directory service – Microsoft™ Active Directory
- Centralized Management – Monitor/Administer (local/ remote sites)
- Integrated Rule Engine – Event/Condition/Action
- Archive Video Recordings
- Integrated Alarm Management
- Intuitive Maps / Smart Maps
- HTTP over SSL/TLS
- Cross version Management/Compatibility [2]
- ONVIF Gateway Interface - private-to-public video, Alarm Centers and Monitoring Stations
- Failover Management (Redundant Cluster)
- High Availability via Microsoft™ Clustering
- Siveillance Video Monitoring Wall – Optional
- Edge Storage (Record/Playback/Syncing)
- Multi-cast streaming
- Kerberos Authentication
- Scalable Video Quality Recording™ (SVQR)
- Two-step verification
- Hardware accelerated video decoding for Video Motion Detection (Quick sync& NVIDIA)
- Hardware accelerated video decoding in the Mobile Server
- Connect DLNA supported TV screens
- Privacy Masking (permanent and liftable)
- Smart Map function (Building support)
- Encryption on communication from recording server

Distributed Operation

- Siveillance Video Interconnect – Remote Site
- Siveillance Video Federated Architecture – Remote Site

Installer

- One-click installer (Automatic device detection and retention-time configuration)
- Wizard-based interface for Plug-in

Operational Intelligence

- Metadata – Harvesting/Automation
- Built-in Video Motion Detection (VMD)
- Adjustable VMD sensitivity
- Real-time VMD analysis
- VMD exclusion zones

Video Processing

- Adjustable GOP size (MPEG4/H.264)
- Dual stream (Live/ Recording)
- Adjustable down sampling (Resolution/ FPS)
- Configurable recoding speed (Motion/Event/ Time Schedule)
- Configurable Pre/Post alarm image buffer
- Pre-buffer in Memory

Audio

- AAC Audio Communication (Full Duplex, Half Duplex)
- Audio Recording (Half Duplex)
- Unlimited audio channels
- Two-way audio in web/mobile client

Pan-Tilt-Zoom (PTZ)

- Unlimited Preset positions per camera
- Go-to preset on event
- Preset patrolling via Rules
- Combine patrolling and go-to preset on event
- Configurable Scanning/Transition speed
- Number of PTZ priority levels – 32000
- Reserve PTZ priority & rights via video client

Alarm

- Alarm Management (Reassign, Update status, Comment)
- Alarm Configuration (Description, Work instructions, Initial Owner, Time profiles, Alarm Result Codes, Alarm Category, Sound Notification, Alarm Priority Levels)
- Alarm Handling (View triggered alarms, Report, Log, Status)
- Alarm Notification (Email, Multiple notification profiles)
- Alarm Priority Levels – 32,000
- Maximum number of camera popup in alarm preview window – 15
- SNMP - TRAP support

Storage & Archiving

- Video retention time - Unlimited
- Recording capacity per device/day - Unlimited
- Online access to archives

Storage & Archiving (Contd...)

- Configurable Storage & Retention Period (Per device, Per Group)
- Storage Overview (Used Space vs Available Space)
- Trigger Event on premature deletion of video due to insufficient physical storage
- Archiving schedules (Min - Hourly, Max - Practically Unlimited)
- Archive recordings
- Archive to network drives (NAS, iSCSI, SAN)
- Support for live video play without recording storage

Integration [(3)]

- Plug-in, Protocol, Component integration via MIP SDK
- 3rd Party Metadata integration via MIP SDK
- 3rd Party Event and action rule engine integration via MIP SDK
- Siemens Security Product integration
  - SiPass Integrated™ via MIP SDK
  - Siveillance Control & Control Pro – via MIP SDK
  - Desigo CC – via MIP SDK

Viewing Clients

- Hardware accelerated video decoding on Client using multiple NVIDIA cards
- Maximum number of clients - Unlimited
- Customizable IP range & port with NAT support
- User Authorization (Local Windows Accounts, Microsoft Active Directory, VMS Application Accounts)
- Assign ad-hoc content to Monitor-Wall (Alarms, Images, Bookmarks, Maps, Carrousels)
- Customizable dashboard tiles with drilldown possibilities
- E-mail, Alarm, Notification)
- Real-time system health monitor
- Simplified Export Panel

I/O & Events

- Soft I/O (Motion, Tamper, Temperature)
- Hardwire I/O (Push button, Sensor)
- Event Triggers (Audio detection, Input trigger, System Notification, Communication failure)
- Event Action (Notification: Email, Play audio clip, Matrix Control, Device Configuration)
- Multiple notification profiles

Management

- Configuration wizards for aided system setup
- Device Management (Device Grouping, Device Model Detection, Replacement Wizard)
- Seamless virtual hardware movement between recording servers

Management (Contd..)

- Centralized Management (Recording server management, User Management)
- Centralized management of Siveillance Video Client application – Max 3 Video Client profiles
- Day length time profile
- On-the-fly configuration changes
- Run servers as Windows Services
- Scheduled start/stop of devices
- Built-in backup-restore support
- Offline license activation
- Dual Authorization for login
- User access permission per client
- Smart Map – offline support
- Web Client Alarm list
- Simple installation
- Inheritance of user rights

Reports & Logs

- System log
- Audit log
- Rule log
- Configuration report

Siveillance Video Monitoring Wall

- Siveillance Video Monitor Wall - Add-on (Optional)
- Number of Siveillance Video Monitor Wall – Unlimited
- Number of concurrent video streams – Unlimited
- Maximum number of video streams per display -100
- Presets for display layouts and camera content
- Enable Rule-based control (Layout/Content)

Siveillance Video ACM

- Doors - Up to 5000
- Events - Up to 600 events per second
- Connect multiple Access Control systems
- Access points grouping
- Extended logs and audit trail
- Dynamic syncing of configuration from sub-system to Siveillance Video

Siveillance Video SiPass integrated / SIPORT Plug-in limitations

- Doors - Up to 1000
- Cardholder - Up to 200,000 / SIPORT – 10,000
- Events - Up to 45 events per second / SIPORT - N/A

Languages* (Management Interface)

- Chinese (Simplified), Chinese (Traditional), Danish, English, French, German, Italian, Japanese, Korean, Turkish
- Portuguese (Brazilian), Russian, Spanish and Swedish.

What’s New - 2020 R3

- Siveillance Video Operates in a Windows FIPS 140-2 compliant mode
- Generic 360-dewarping
- Video Client Performance improvements (*Either using NVIDIA cards or Intel Quick Sync)*
- The Video Driver API / SDK supports unlimited channels for integration
- Initial setup of credentials on devices (limited to supported devices, e.g., Axis, BOSCH, Hanwha and Avigilon)
- Multi-category Search
- Adaptive streaming for Siveillance Video Mobile
- Video Client with better 4K Streaming performance
- Web Client and Mobile Client now supports all Video CODEC (MJPEG, H.264 & H.265) via Direct Streaming capability

Note:

1. Supports ability to decode compressed audio stream and render the audio on a client.
   Full-duplex - Data transmission that can be transmitted in both directions at the same time.
   Half-duplex - Data transmission in just one direction at a time.
2. The central site must be Siveillance Video 2020
3. Siveillance Video provides possibility to seamlessly integrate 3rd party management station via MIP SDK – supports three types of integration: basic protocol integration, component-based integration via .NET library and plug-in integration to embed plug-ins directly into Siveillance Video.

*For a complete feature and supported languages overview please refer to the **Siveillance Video Comparison Guide.**
www.siemens.com/siveillance-video

Issued by

Siemens Schweiz AG
Smart Infrastructure Division
International Headquarters
Theilerstrasse 1 a
CH-6300 Zug, Switzerland
Tel. +41 41 724 24 24

Cybersecurity Disclaimer “BT communication”

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens’ portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html

Siemens’ portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under http://www.siemens.com/cert/en/cert-security-advisories.htm