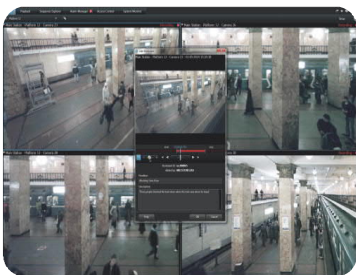# SIEMENS
Ingenuity for life

Siveillance Video Core

For small solutions
2020 R1

A powerful solution for small to medium deployments including more than 110 features and functions

The Siveillance Video Core is designed for small to mid-sized installations that need robust single-server surveillance software with the full functionality of advanced management, flexible scheduling, fast searching and analysis. The system supports up to 48 cameras simultaneously with a wide variety of network video and computer hardware equipment.

Main features: Siveillance Video Core

- Supports H.265
- Dual Live Stream and Recording per Camera
- DLNA ready
- Online Activation
- Two-step verification
- Siveillance video driver framework
- Metadata support for Edge based video analytics
- Support for ONVIF & PSIA
- Siveillance Site IQ PSE Analytics (Included)
- Flexible device replacement licensing
- Two-way AAC Audio support
- Kerberos Authentication

www.siemens.com/siveillance-video

Siveillance Video Core Overview

Product Facts
- Deployment type   Single-server
- Number of cameras per system   48
- Number of recording servers   1
- Number of users   Unlimited
- Video export format   AVI, MKV
- Supported manufacturers   134 Plus
- Supported IP devices   8000 Plus
- Generic hardware discovery   UPnP
- Audio[1]   Full Duplex, Half Duplex
- Open standards   ONVIF : Profile-S/G,PSIA
- Video compression   MJPEG, MPEG-4 AVC, MPEG-4, MxPEG, H.263, H.264, H.265

System Components
- Siveillance Video 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 Recordingssmart
- Integrated Alarm Management
- Intuitive Maps
- HTTP over SSL/TLS
- Cross version Management/Compatibility [2]
- ONVIF Gateway Interface - private-to-public video, Alarm Centers and Monitoring Stations
- Kerberos Authentication
- Scalable Video Quality Recording™ (SVQR)
- Two-step verification
- Hardware accelerated video decoding for Video Motion Detection (Quick sync)
- Hardware accelerated video decoding in the Mobile Server
- Connect DLNA supported TV screens
- Privacy Masking (permanent and liftable)
- Encryption on communication from recording server

Distributed Operation
- Siveillance Video Interconnect– 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
- Configure PTZ preset positions via Video client
- 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 – 1
- 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

Storage & Archiving
- Video retention time - Unlimited
- Recording capacity per device/day - Unlimited
- Online access to archives
- 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 of 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 and Control Pro – via MIP SDK
  - Desigo CC – via MIP SDK

Viewing Clients
- 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
- Centralized Management (Recording server management, User Management)
- 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
- Web Client Alarm list
- Simple installation
- Inheritance of user rights

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

Siveillance Video Access

- 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 Plug-in limitations

- Doors - Up to 1000
- Cardholder - Up to 6000
- Events - Up to 45 events per second

Languages* (Management Interface)

- Chinese [Simplified], Chinese [Traditional], Danish, English, French, German, Italian, Japanese, Korean, Portuguese [Brazilian], Russian, Spanish, Swedish, Turkish

Reports & Logs

What's New - 2020 R1

- o Network configuration for ONVIF cameras
- o ONVIF Profile T and Q support
- o Alarm notification for video client

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

Cyber security disclaimer

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 Smart Infrastructure, 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 http://www.siemens.com/industrialsecurity

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 https://www.siemens.com/cert/en/cert-security-advisories.htm

www.siemens.com/siveillance-video