DATA AND SPECIFICATION SHEET

Siveillance™ Video Advanced

2022 R3 | DECMEBER 2022
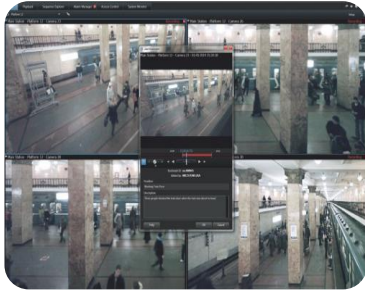
SIEMENS

Contents

Siveillance™ Video Advanced

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:

What's New in 2022 R3

- Device search filter (Siveillance Video Management Client)
- Enhanced User Experience on Siveillance Video Client and Web Client
- SSO (Single Sign On) support in Siveillance Video Web & Mobile
- Biometry support in Siveillance Video Mobile :
  Users can now use biometrics or device credentials to verify their identity to access
  Siveillance Video Mobile. Available for both Android and iOS users.
- Mobile device management support in Siveillance Video Mobile :
  Through MDM, organizations can manage and secure devices, apps, and data from a unified console.
- Siveillance Video Incident Manager purchasable as an add-on license

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 2022

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 refers to the **Siveillance Video Comparison**

Guide. www.siemens.com/siveillance-video

Key Features

- Hardware accelerated Video Motion Detection (VMD)
- Location search using GPS Coordinates
- Redundancy Option for High Availability
- People, Vehicle & Location Search Filters
- Supports H.265
- Siveillance Video Operates in a Windows FIPS 140-2 compliant mode
- Flexible Rule Engine
- Generic 360-dewarping
- Centralized Search in Smart Client
- Adaptive Streaming (Video & Web Client)
- Video Client Performance improvements (Either using NVIDIA cards or Intel Quick Sync)
- Siveillance Video Driver Framework
- Device & Password Management
- The Video Driver API / SDK supports unlimited channels for integration
- Hardware accelerated video decoding using Quick Sync & NVIDIA GPU
- Smart Map – offline support
- Initial setup of credentials on devices (limited to supported devices, e.g., Axis, Bosch, Hanwha and Avigilon)
- Multicast Support
- Multi-category Search
- DLNA ready
- Adaptive streaming for Siveillance Video Mobile
- Hot & cold failover recording server
- Kerberos Authentication
- Video Client with better 4K Streaming performance
- Two-step verification
- Online Activation
- Adding Devices on HTTPS
- Web Client and Mobile Client now supports all Video CODEC (MJPEG, H.264 & H.265) via Direct Streaming capability
- Direct streaming method - Mobile server
- Directory service – Microsoft™ Active Directory
- Centralized Management – Monitor/Administer (local/ remote sites)
- Archive Video Recordings
- Integrated Alarm Management
- Intuitive Maps / Smart Maps
- HTTP over SSL/TLS
- Cross version Management/Compatibility
- 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)
- Scalable Video Quality Recording™ (SVQR)
- Privacy Masking (permanent and can be removed manually)
- Encryption on communication from recording server
- PTZ Specific Camera icon
- Bookmark (Create, Edit, and delete)
- New Export tab in Video Client
- Expanded bookmarks for Mobile Client
- Support for extended Identify Providers
- Siveillance Video API-Gateway
- Push Notification for Mobile Client (this function requires a valid SSA/SUR)

Product Facts

Siveillance Video

- 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 and Siveillance Video Format
- Supported manufacturers   Above 170
- Supported IP devices   12,000+
- Generic hardware discovery   UPnP
- Audio   Full Duplex, Half Duplex
- Open standards   ONVIF: Profile-S/G/T/Q, PSIA
- Video compression   MJPEG, MPEG-4 AVC, MPEG-4, MxPEG, H.264, H.265, H.264+,H.265+

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 3500
- Cardholder - Up to 200,000 / SIPORT – 10,000
- Events - Up to 45 events per second / SIPORT - N/A

Integration

- 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

Languages* (Management Interface)

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

Feature Overview

- **Unlimited Scalability**
  Siveillance Video Advanced supports an unlimited number of   users, cameras, servers, and sites, and allows seamless expansion of any installation.
- **Centralized Management**
  A Management Client connected to the management server enables full remote system configuration of all recording servers, failover servers, devices, rules, schedules, and user rights.
- **Siveillance Video Interconnect**
  A unique system concept that enables individual Siveillance Video Advanced systems to be connected with a central Siveillance Video Pro system for central surveillance operation across geographically dispersed sites.
- **Siveillance Video Federated Architecture**
  System concept that enables individual Siveillance Video Advanced systems to be connected with a central Siveillance Video Pro system in a hierarchical architecture for infinite scalability and central management.
- **Bookmarking**
  Allows users to mark video sections of particular interest and add descriptive notes for later analysis or sharing with other users.
- **Metadata Support**
  Supports reception, storage, and export of metadata, including metadata from camera-resided video analytics and location data in video push from Siveillance Video Mobile
- **Secure multi-stage storage**
  Unique data storage solution that combines superior performance and scalability with video data grooming for cost efficient, long-term video storage, with option to encrypt and digitally sign stored video and audio.
- **64- bit recording servers**
  Allow more cameras to be run on a single recording server
- **High availability- failover recording servers**
  A redundancy option for recording servers to ensure maximum system uptime while minimizing video interruption in the event of system problems. Operate in two failover modes: Cold stand-by and Hot stand-by
- **High performance recording server**
  Building on a native 64-bit windows implementation and a highly optimized database technology with RAM-based pre-buffering, the recording server supports minimum 3.1 Gbit/s recording rate
- **Virtual environment**
  Support for VMware and Hyper-V virtualization solutions (to exclude hardware acceleration which in not supported in a virtual environment)
  installations using a standardized ONVIF compliant video-out interface
- **Versatile rule system:**
  Facilitates the automation of different aspects of the system, including camera control, system behavior and external devices, based on events or time schedules
- **System Monitor**
  Customizable real-time system monitoring dashboard and report function for proactive maintenance of the VMS installation
- **Alarm Manager**
  Single-point alarm function that provides a consolidated and clear overview of security and system-related alarms.
- **Intuitive Map Function**
  Multi-layered and interactive maps display the location of every camera and offer control of the entire surveillance system. Siveillance Video Monitoring wall has a seamless drag-and-drop function for instant display of any cameras in a map
- **Siveillance Video Monitoring wall - optional**
  Flexible and hardware independent Monitoring wall option that seamlessly integrates with the Management Client and Siveillance Video Client.
- **Multicast Support**
  Optimizes network load in systems with several users by sending one video stream per camera to multiple Siveillance Video Clients.
- **High Efficiency Video Coding**
  H.265 enables better video quality with same bandwidth or same video quality with less bandwidth compared to h.264 video codec

- **Hardware Accelerated Video Motion Detection**
  Video motion detection decoding takes advantages of processing power in Graphical Processing Units to significantly reduce the CPU load and improve performance of recording servers. It requires CPU with support for Intel Quick Sync Video or NVIDIA card with compute architecture 3.x (Kepler) or newer.
- **Hardware Accelerated Video Decoding**
  Hardware accelerated video decoding on the Video Client using multiple NVIDIA cards
- **Operational Intelligence**
  o   Metadata – Harvesting/Automation
  o   Built-in Video Motion Detection (VMD)
  o   Adjustable VMD sensitivity
  o   Real-time VMD analysis
  o   VMD exclusion zones
- **Two-Step Verification**
  Prevents non-authorized people from accessing the system and protects against "man in the middle" attacks
- **Centralized Search**
  Easy to use search tool that aggregates different data types registered in the Siveillance Video as entries and allows users to find everything they look for in one place. Search categories that include People, Vehicle & Location Search Filters providing improved geographical awareness
- **Adaptive Streaming**
  Adaptive streaming technologies enable the optimum streaming video viewing experience for a diverse range monitoring device. Deliver video to the user in the most efficient way possible with less hardware needed. Adaptive Streaming can be enabled in Video client, Web client and Mobile client.
- **Alarm Notification for Video Client**
  Even when the Video Client is minimized, or the operator is working on another screen, alarm notifications will appear – to help keep focus on what's important.
  Click on the notification to gain instant access to the Alarm Manager – for related video, bookmarking, and further investigation. Administrators can choose what alarm levels trigger this notification, and as before, can define what these level mean. Feature is community-enabled for MIP SDK.
- **Centralized Search - LPR**
  Integrating Siveillance LPR results into the Centralized Search agent
  Make use of camera application metadata for license plate recognition. Axis Optimizer plugin now including Centralized Search plugin. another step further in bringing all the searchable elements in the Centralized Search tab.
- **Multi-Live Streaming**
  Define multiple streams for live viewing with different properties according to available bandwidth
- **Automatic Camera Discovery**
  Enables fast discovery of more than 4,500 IP cameras, IP video encoder's models from more than 100 different manufacturers.
- **Multiple Language Support**
  Lets most operators use the system in their native language with support for 31 different languages, while the Management Client is available in 14 languages.
- **Fast Evidence Export**
  Deliver authentic evidence to public authorities by exporting video to various formats, including video from multiple cameras in encrypted Siveillance Video format with dedicated player application included.
- **Audit Logs**
  Enables extensive logging of all user system access, configuration changes and operator actions.
- **Flexible User and Rights Management**
  Strict privileges on management of users' access to functions and camera actions. Modular user management with support for basic user accounts to global user management with single sign-on Microsoft® Active Directory accounts.
- **Dual Authorization**
  Additional level of system security when operating in high-security areas, where users are granted system access only when a second user has confirmed the login with a successful authorization of the second user.
- **Liftable Privacy Masking**
  Privacy well protected both on live and recorded video using permanent and liftable privacy masking
- **Privacy Masking**
  Allows users to define privacy masks to hide areas in the camera view that must not be visible or recorded.

- **Smart Maps**
  Quickly navigate to the correct geographical overview to identify and preview relevant cameras in a user interface similar to Google or Bing maps using smart maps
  o Building support in Smart Map allows to Navigate with ease between cameras on different floors
  o Alarms on Smart Maps
  o Alarms, Input devices and Microphones
    - The ability to hear audio directly in the map view
    - Icons like doorbells and sensors for an improved overview in map
  o Device Clustering
    - Automatically groups near-by map items into clusters for a better visual overview when zooming out
- **Web Client Alarm list**
  List of alarms in the systems so users can quickly get and overview and act if needed
- **User access permission**
  System administrators controlling systems with multiple users can control access permission per client for each of the three Siveillance Video clients, resulting in safer security access
- **Simple installation**
  Selecting "Single Computer" set up during the initial installation the system automatically performs certain configurations for an easier installation experience
- **Open Network Bridge (earlier ONVIF Bridge)**
  Includes the ability to do forward playback with different speeds and backward playback for an improved investigation experience
- **DLNA Support**
  Connect Siveillance Video to any DLNA supported TV and display video captured from cameras without a computer or a client.
- **One-Click Installer**
  Configure Siveillance Video faster and easier during installation, with automatic device detection and retention-time configuration.
- **Wizard-based interface for Plug-in**
- **Siveillance Video Mobile Access Control Support.**
  Open / close / grant/ deny access and control perimeter via Siveillance Video Mobile app.
- **Online License Activation**
  Activate Siveillance Video Camera License via internet
- **64-bit Client Player**
  Take full advantage of the modern CPU's benefits to process more information at once.
- **Siveillance LPR Integration via MIP SDK**
  External applications can create and manage match lists fully through the MIP-SDK Configuration API.
- **Trusted Root Certificate via CA**
  Use trusted certificates between the Siveillance Management Server and Siveillance Recording
- **More Secured, Stronger data protection and Enhanced Encryption**
  Siveillance Video now includes
  o The latest Microsoft CNG encryption modules
  o Password protected configuration
  o Server Configurator Utility now available for the Mobile Server
- Siveillance Video now Operates in a compliant mode that is approved by U.S. Federal information processing standards (FIPS 140-2)

Integration options

- The Siveillance Video Integration Platform Software Development Kit (MIP SDK) 2020 enables seamless integration of video analytics algorithms and other third-party applications in Siveillance Video Client and Management Client.
- Compatible with Siveillance Video Access Control Module and integrates with alarms, gates, building management systems, using hardware input/output (I/O) and various types of events.
- Generic event integration enables easy and fast integration of third-party applications and systems via a simple message-based socket
  communication interface.
- System configuration API enables external applications to make changes to the system's configuration.
- Siveillance Video Driver Framework within MIP SDK allows IoT devices manufacturers to develop their own drivers and provide faster device compatibility and deeper integration with other devices connected via Siveillance Video application.

- **Driver API / SDK**
  Increased cap on driver API / SDK - The cap on supported channels has skyrocketed to 512, giving professionals more freedom of choice. This is a vast improvement from the 16-channel limit for ONVIF and the 64-channel limit for the Universal Driver. Partners building their own integrations with the Driver API/SDK, can now enjoy complete freedom, going from a 1-channel limit to support for an unlimited number of channels.
- **Device Firmware Upgrade**
  Device Firmware Upgrade - system administrators with supported device brands* can complete updates from a single user interface, saving time and energy. Bulk updates for devices in Video Advanced and Video Pro are also possible.
- **360-degree Dewarping - Expanded**
  Extended 360-degree dewarping device support - Adjust each camera's field of view (FOV) to optimize the dewarping algorithm and allow Video to support dewarping in even more 360-degree cameras
- AI Bridge simplifies the integration and deployment of AI and intelligent video analytics applications and ensures access to video and the return of events and metadata. The first version of the AI Bridge is developed and aimed specifically at the NVIDIA EGX Enterprise Platform

Recording Server System

- Simultaneous digital multi-channel MJPEG, MPEG4, MPEG-4 ASP, MxPEG, H.264 and H.265 video recording of IP cameras and IP video encoders without any software limitations on number of cameras per server.
- Edge Storage with flexible retrieval enables video retrieval from camera storage based on time schedules, events, or manual requests. This enables users to effectively retrieve video recordings across low-bandwidth connections.
- Two-way audio allows users to transmit and record audio from connected microphones and audio from the operator's microphone to attached speakers.
- Generic framework for receiving and storing metadata from compatible devices and clients.
- Route traffic between multiple connected cameras and multiple clients requesting live view, playback, and export.
- Multicast one video stream to all Siveillance Video Clients. The infrastructure must support IGMP to reach remote networks.
- Multi-live streaming gives the possibility to define multiple streams for live viewing with different properties. It optimizes Siveillance Video Client viewing performance according to the available bandwidth and view layouts, which is ideal for deployments with remote viewing Number of streams supported is set by the camera driver
- A dedicated recording stream enables optimization stream properties (resolutions, encodings, and frame rate) for video storage and forensic usage
- Secure high-speed recording database holding JPEG images or MPEG4, MPEG-4 ASP, MxPEG or H.264/ H.265 streams.
- Flexible control of recording characteristics for MPEG4/H.264/H.265 streams, making it possible to toggle between recording key frames only or the full stream
- Record more than 30 frames per second per camera, limited only by hardware.
- To facilitate post-deployment system performance optimization and seamless system expansion, camera can be moved between two recording servers in runtime.
- Encrypted communication between Recording Server and services retrieving streaming data
- Digital signing of the recording server's video database can be used to verify that recorded video has not been modified or tampered with while stored or after export
- Video decoding takes advantage of processing power in Graphical Processing Units. This includes the GPU part of the Intel CPU (requires CPU with support for Intel Quick Sync Video) and in the GPU of additional external NVIDIA cards
- Functional recording server even if a recording storage area is unavailable. Continued recording of video from devices with available recording storage and live video on devices without available recording storage
- Support for shutdown of recording server if recording storage becomes unavailable, to enable fail over to take over
- Recording quality depends entirely on camera and video encoder capabilities with no software limitations.
- Possibility to import pre-event images recorded locally in camera or video encoder.
- Built-in, real-time, camera-independent motion detection with the ability to generate motion metadata for Smart Search.
- The recording server runs as a Windows service under local system account or optional local Windows user or Microsoft Active Directory account with run-as-a-service privileges.
- Port forwarding enables clients to access the recording servers from outside a network address translation (NAT) firewall.
- Secure HTTPS camera connection on devices supporting HTTPS.

High availability

- Siveillance Video Advanced offers two levels of redundancy on the recording servers: Cold and hot stand-by failover
- Both mechanisms offer fully automatic and user transparent failover in the event of hardware or system failure, with automatic synchronization at system recovery
- Cold stand-by failover is a cost-efficient redundancy solution where one, or a group of, failover recording servers can act as backup to one or multiple recording servers
- Hot Stand-by failover is a high-security redundancy solution providing minimal interruption in recording and live streams, where a dedicated failover recording server is preconfigured for a recording server

Pan-Tilt-Zoom (PTZ)

- "Pass-through" control of manual PTZ operation from clients with user priority.
- 32,000 PTZ priority levels for control of rights between different operators and automatic patrolling schemes.
- Execute rule-based go-to preset position on events and patrolling.
- Pause PTZ patrolling on event and resume patrolling after manual session timeout.
- System feedback to operators failing to gain access to a PTZ camera when is used by another user or when engaged in an automated patrolling scheme with higher priority
- The advanced PTZ control also allows an operator to reserve the control of a PTZ camera, which prevents other users or automated patrolling schemes (with higher priority) to take over the control.
- Configurable Scanning/Transition speed
- Unlimited Preset positions per camera

I/O and Events

- Support for devices with one or more input and output ports.
- Powerful rule processing engine for execution of start and stop actions triggered by events or time profiles.
- Handle pre-event recordings that significantly reduces the wear and tear of disc systems by keeping the pre-buffered video in memory instead of writing it to a disk using Pre-buffer in Memory.

Setup and Management

- Download and install the recording server from a web page on the management server. The recording server is completely managed via the Management Client and configuration changes are applied instantly while recording is in operation.
- Local recording server configuration data is available during periods where the management server is inaccessible.
- Recording server manager is available in the local console notification area (icon tray) for status messages, start/stop of the service and change of network settings.

Client Access

- Facilitate client access
- Clients are authenticated and authorized at the management server and use a session-limited access token to access the recording server.

Alerting and Notification

- The system acts as a simple network management protocol (SNMP) agent that can generate an SNMP trap as a result of a rule activation.

Logs

- Logging of system, audit, and rule entries to the management server with local caching during offline scenarios.

Management Server and Client

System

- Management server for initial user authentication, system configuration and logging.
- Management Client compatible with Siveillance Video Core, Core plus, Advanced and Pro 2019 R1 and newer
- Management Client for central administration of system components such as recording servers, devices, security, rules, and logging.
- All configuration and logs from the entire system are stored in a centralized Microsoft SQL database and accessible by the management server only.
- Failover solution for the management server provides a resilient system solution based on Windows Server Clustering, ensuring high system availability.
- Management server manager is available in the local console notification area (icon tray) for status messages and to start/stop the service.
- The management server runs as a Windows service under local system account or optional local Windows user or Microsoft active directory account with run-as-a-service privileges.
- To activate your licenses, the system offers offline activation.
- Support for both IPv4 and IPv6 addressing.

Siveillance Video Interconnect

- Siveillance Video Advanced is compatible with Siveillance Video Interconnect and works as a remote site

Siveillance Video Federated Architecture

- System concept that enables individual Siveillance Video Advanced systems to be interconnected with a central Siveillance Video system as a remote site.
- Resilient architecture that allows individual systems to function autonomously in the event of network problems. Site details (name, address, administrators, and additional information) defined in the federated system is made available to the federating parent system.

Storage & Archiving

- 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 recordings
- Archive to network drives (NAS, iSCSI, SAN)
- Support for live video play without recording storage
- Definition of one or more storage containers with individual archiving schemes and retention times. Recording capacity is limited only by disk space.
- Each storage container is defined as live database and one optional archive, where the video data is moved from the live database to secondary disk systems or network drives. The archived data is still online and available for clients.

Devices

- Hardware wizard to add devices automatically using Universal Plug and Play (UPnP) discovery, via IP network range scanning, or using manual devices detection. All methods support automatic or manual model detection.
- Search and add devices directly on HTTPS
- Wizard for swift replacement of malfunctioning devices with preserved configuration settings and recordings.
- Enable and disable devices, which is very useful if they are not used or are down for maintenance.
- Adjust settings such as brightness, color level, compression, maximum bit rate, resolution and rotation per camera or camera group.
- Select and configure video format, frames per second (FPS), resolution and quality for the video streams used per camera.

- Select and configure one, or more, video streams per camera to be used for live viewing. Each stream can be in different video format, FPS, resolution, and quality.
- Adjustable group of pictures (GOP) length for MPEG4 and H.264/ H.265 encoded video.
- Optional preview window for immediate verification of video settings per camera or for a group of cameras
- Assign camera shortcut number for easy operation by clients.
- Define multiple PTZ preset positions on the server.
- Import PTZ preset positions from cameras.
- PTZ scanning on supported devices.
  Define multiple PTZ patrolling schemes with adjustable wait time between shifts and customizable transitions with disabling of motion detection to avoid false alarms.
- Run multiple patrolling schedules per camera per day. For example, run different schedules for day/night/weekend.
- Privacy mask consistently hides certain areas in the camera view in live and playback video and in exported material.
- Configure device events like motion detection with pre- and post-buffers, or input signal behavior options.
- Fine-tune motion detection sensitivity per camera manually or automatically.
- Apply one or multiple exclusion zones where motion detection is to be disabled to avoid unwanted detection.
- Ability to allocate individual devices to different storage containers.
- Move a device or a group of devices between two storage containers.
- Storage overview gives instant indication of used vs. available storage in total and for individual cameras.
  Manage maximum recording time for manual recording.
- Trigger events:
  The Siveillance Video Advanced system and connected devices support a wide set of events that can be used to trigger actions using the rule system. Events are grouped in the following categories:
  o Hardware: events that relate to physical hardware devices connected to the system.
  o Devices: events that relates to certain functions and states of devices available to the Siveillance Video system via the connected hardware devices.
  o External Events: events that relate to VMS integrations.
- Recording server: events that relate to failover, archiving and database functions.
  Analytics: events from integrated applications and systems.
- For further details on available trigger events, please refer to the Siveillance Video Administrator's Manual.
- Stop actions: The rule engine may also trigger stop actions in the VMS system, connected devices or integrated systems upon the completion of a rule.
  For a complete list of available stop actions, please refer to the Siveillance Video
  Administrator's Manual.
- Siveillance Video Monitoring wall start and stop actions; Set Siveillance Video Monitoring wall to preset layout, set Siveillance Video Monitoring wall monitor layout and camera content.
- Multi-recipient customizable email notification with image and/or AVI attachment of incidents.
- Management client contains a field showing the firmware version of each device
- Option "Update Hardware" updates the information about the firmware and features available for a specific device
- Device search filter enables searches for devices in the recording server tree. Searches can be made on device name and IP address. All disabled devices are by default not shown in the device tree, but they can be displayed by ticking the checkbox in the search bar

User Rights Management

- Common and central management of all user rights across all user and programmatic (MIP SDK) interfaces
- Overall system security definition makes it possible to globally allow or deny permission to devices and functions (such as manage, read, edit and delete).
- Device-specific security definition makes it possible to allow or deny permission to individual devices and functions (such as manage, read, edit and delete).
- Supports inherited user rights and the ability to assign partial management rights
- Inputs and outputs: visibility, administrate, status, activation
- PTZ: manual control, activate PTZ presets, PTZ priority, manage PTZ presets and patrolling, lock/unlock PTZ presets, reserve, and release PTZ session
- Remote recordings: retrieve remote recordings
- Siveillance Video Monitoring Wall: visibility, administrate, control, playback

- Alarms: visibility of alarms and ability to manage alarms
- MIP: Plug-in permissions
- General application permissions: Management Client, Siveillance Video Client, Siveillance Video Web Client and Siveillance Video Mobile
- Scripting disable/enable option
- Device firmware upgrade of single devices
- Device firmware upgrade of multiple devices in bulk4
- Initial setup of credentials on devices without factory default credentials increases the level of security in the customer's system.
- User handling: Add/change VMS user account that communicates with the device. List and delete existing device's users.
- Network configuration: enabling change of IP address, subnet mask, and default gateway for a device.

Rules, Time Profiles and Notifications

- Powerful Microsoft Outlook®-style rule system supports an unlimited number of rules.
- Rule actions are triggered by event, time interval or a combination of event and time. Rules can be optionally stopped by an event or after a certain time.
- Time profiles with recurring time selection and expire condition support an unlimited number of time profiles.
- Dynamic day-length time profile follows daylight changes over the year for a given location defined by a GPS position, including daylight savings time.
  - Alarms: visibility of alarms and ability to manage alarms
  - Application: manager Siveillance Video Client/ Siveillance Video Web Client/ Siveillance Video Mobile, live/ playback/setup, status API and service registration API
  - Siveillance Video: Plug-in permissions

Logging

- Logs of system, audit and rule entries are consolidated from all Recording Servers at regular intervals.
- Each log file has adjustable size and time limitations to avoid overloading the database.

Siveillance Video Client Profiles

- Centralized management of Siveillance Video Client application options enables optimization of Siveillance Video Client for different user categories and skill levels.
- Define up to three different Siveillance Video Client profiles.
- Ability to enforce or recommend optional Siveillance Video Client application options for a user or group of users, using maximum three different Siveillance Video Client profiles.
- Define general Siveillance Video Client application options, including visibility of time, visibility of (camera) live indicators, default image quality, default frame rate, keyboard and joystick setup, startup mode and de-interlacing filters.
- Access to live mode and availability of individual control panels and overlay buttons.
- Access to playback mode and availability of individual control panels, overlay buttons and settings for specific functions, such as default export path.
- Access to Centralized Search, Alarm Manager, System Monitor.
- Roles control user and administrator access to:
  - General: Siveillance Video Client profiles, dual authorization rights, system log-in time profile.
  - Cameras: visibility, administrate, live view (within time profile), playback (within time profile), search sequences, export, smart
    search, AUX commands, manual recording, bookmark functions, Evidence Lock functions.
  - Microphones and speakers: visibility, administrate, listen to live audio (within time profile), playback audio (within time profile), search sequences, export, manual recording, bookmark functions, Evidence Lock functions, speak to speakers.
  - Inputs and outputs: visibility, administrate, status, activation.
  - Remote recordings: retrieve remote recordings
  - Siveillance Video Monitoring wall: visibility, administrate, control.
    External events: visibility, administrate, trigger.
    View groups privileges.
  - Servers: Siveillance Video management server access and authentication details

Authentication

- System log-in uses Microsoft Active Directory, local Windows, or basic user account.
- Use current Windows log on for authentication.
- Dual authorization offers an optional additional level of system security, where Management Client users are granted access to the system only
  when a second user or supervisor has confirmed the log-in with a successful authorization of the second user.
- Access to setup mode and the availability of individual control panes and setup functions.
- Definition of available view layouts.
- Password change for Basic user – Force password change on next login.
- Use organization's own Identity and Access Management system (Open ID Connect based) to authorize and authenticate users. It enables support for SSO

System Administration

- Built-in backup and restore support for manual system backup of all configuration data, including:
  system configuration data, maps, alarm settings and definitions and client views.
- System Monitor function gives actual and historic performance and usage reports of server performance, storage availability, network usage and camera performance.
- Configuration Reporting enables complete or partial documentation of system configuration. Custom and site-specific free-text information,
  integrator's notes and logo can be added to printer-friendly reports.
- Kerberos Authentication ensures faster and mutual authentication using open and more secure standards than the existing NTLM authentication.
- Change single and multiple-device passwords directly within Siveillance Video for an easier and more secure user experience
- Customizable alarm categories enable logical grouping of alarms dependent on their type and nature
- Customizable alarm statuses enable alignment of the alarm handling workflow with existing workflows and security systems
- Alarm handling result code enables tracking of the outcome of the alarms
- Automatic allocation to alarm owner with escalation and alarm forwarding possibilities
- Time profiles for definition of active alarms
- Possibility to associate one or more cameras to an alarm (maximum 15 cameras can be displayed simultaneously in the alarm preview window)
- A set of alarm handling reports gives valuable in-formation about alarm inflow and alarm handling performance
- Extensive logging of alarms
- Microsoft Clustering support for the event server enables secure and redundant alarm handling

License Administration

- Expanded license information for multi-site installations where both the total used licenses for the common SLC is presented and the license use in the specific system.
- License overview that presents the license use of all the individual sites running on the same SLC.

Event Server

Alarm Manager

- Single-point alarm management of all internal system alarms and external security alarms.
- Alarm descriptions and work instructions make alarms actionable for operators.
- An alarm location map can be linked to each alarm providing instant situational awareness to the operator dealing with the alarm.
- Customizable alarm priorities allow operators to focus on the most critical alarms.
- Customizable alarm categories enable logical grouping of alarms dependent on their type and nature.
- Customizable alarm statuses enable alignment of the alarm handling workflow with existing workflows and security systems.
- Alarm handling result code enables tracking of the outcome of the alarms.
- Automatic allocation to alarm owner with escalation and alarm forwarding possibilities

- Time profiles for definition of active alarms.
- Possibility to associate one or more cameras to an alarm (maximum 15 cameras can be displayed simultaneously in the alarm preview window).
- A set of alarm handling reports gives valuable information about alarm inflow and alarm handling performance.
- Extensive logging of alarms.
- Microsoft Clustering support for the event server enables secure and redundant alarm handling.

Siveillance Video Mobile server

- The Siveillance Video Mobile server runs as a dedicated service, allowing it to be installed either on the same server as other system components or on dedicated hardware in more demanding installations.
- The Siveillance Video Mobile servers can transcode video so streams are robust and can adapt to changing connection bandwidth. The server also optimizes the use of available bandwidth to get the best possible stream quality.
- Adjustable transcoding logic enables capping of video resolution and frame rate for video streams provided to Siveillance Video Web Clients and Siveillance Video Mobile clients.
- Option to bypass the transcoding logic and send direct streams to Siveillance Video Mobile and Web Clients. With no transcoding happening in the Mobile Server, live video is streamed directly to Siveillance Video Mobile and Web Client.
- Installing the Siveillance Video Mobile server plugin in the Management Client will give access to Siveillance Video Mobile server management in order to change settings, read out miscellaneous status information, configure codecs used for exports as well as manage ongoing and completed exports.
- Siveillance Video Mobile servers can be installed in parallel, offering redundancy and/or allowing more simultaneous users.
- Siveillance Video Mobile servers can be configured through the tray controller to easily adjust or update settings.
- Use either a default-generated certificate for HTTPS encrypting the connection to the Siveillance Video Mobile server or provide your own custom certificate.
- Video Push configuration is done from the server, so users can download and use Siveillance Video Mobile without having to do any configuration.
- Siveillance Video Mobile server supports creating server-side export through Siveillance Video Web Client and Siveillance Video Mobile.
- Siveillance Video Web Client, including optional browser plug-ins, is included with the Siveillance Video Mobile server. No additional setup is needed.
- Hardware accelerated video decoding in the Mobile Server

Siveillance Video Client

General

- Dedicated task-oriented tabs for Centralized Search, Alarm Manager and System Monitor, in addition to the traditional Live and Playback tabs.
- Application theme support with choice of dark or light themes.
- True multi window support where secondary windows have full functionality and can be operated in independent mode or synchronized mode where they follow the control of the main window.
- Shortcuts to select a specific window, or specific camera in a window.
- Camera search function promptly finds cameras, types of cameras and views in the system with the ability to create temporary views to display all or a subset of cameras matching the search criteria.
- Display metadata bounding boxes from supported devices in live views and playback.
- Significant reduction in network traffic and central storage costs. with Scalable Video Quality Recording™ (SVQR) technology enabling instant access to low quality recorded video, with the possibility to later retrieve high quality video from the edge when or if needed.
- Export video in three simple steps (Select cameras, set start time, and end time, Click Export) using Simplified export panel.
- Generic 360 dewarping allows users to cover a wide area with a single device with 360 cameras, but at the same time get a 'normal' view of a fisheye image.

Live View

- View live video from 1-100 cameras per computer monitor/view.
- Multiple computers monitor support provides a main window and any number of either floating windows or full screen views.
- Live view digital zoom allows a full view of recordings while the operator can digitally zoom in to see details.
- Supports 41 different view layouts optimized for 4:3 and 16:9 display settings in both landscape and portrait.
- Independent playback capability allows for instant playback of recorded video for one or more cameras, while in live mode.
- Centralized storage of shared and private camera views enables coherent access to views across the system.
- Possibility to instantly re-arrange cameras in views for optimized monitoring of incidents, with single click restore of original view.
- Instant camera placement in live view allows for instant replacement of cameras in a view, where new cameras can be placed in a particular view and positioned through a simple drag-and drop operation.
- Update on "motion only" optimizes CPU use by allowing motion detection to control whether or not the image should be decoded and displayed.
- Global hotspot function allows users to work in detail with any camera selected from any view.
- Import static or active HTML maps for fast navigation to cameras and to provide a good overview of premises
- Hide HTML page toolbar in HTML page views.
- Activate matrix via graphical maps of premises using JavaScript or integrate with centralized access control systems.
- The operator can assign outputs, PTZ presets and views as actions to joystick buttons and as keyboard shortcuts.
- Two-way audio support enables Siveillance Video Client to record and play live audio from camera-connected microphones and outgoing audio from the operator's microphone to one or multiple camera speakers.
- Adaptive de-interlacing option secures high video quality, based on the actual video content received. Siveillance Video Client can optionally apply a filter to areas of the image where jagged edges would otherwise show up.
- Operators may start/stop manual recording on individual cameras, where the recording status is propagated to all Siveillance Video Client users active in the system.
- Support for live video play without recording storage

PTZ

- Control PTZ cameras by using
  - PTZ preset positions
  - PTZ point-and-click control
  - Overlay buttons
  - PTZ zoom to a defined rectangle
  - Video overlaid PTZ control
  - Virtual joystick function
  - Joystick
- Take manual control of a PTZ camera that is running a patrolling scheme. After a timeout with no activity the camera reverts to its scheduled patrolling scheme.
- Fisheye camera (Grandeye™/IPIX™) support for 1x2 or 2x2 "Quad View" for viewing all 360° at once 360° ImmerVision Enables® Panomorph lens technology.

I/O and Events

- Overlay buttons provide intuitive control of cameras, camera-integrated devices, and other integrated systems directly from the camera view.
- Manually trigger output port relay operation, for example when controlling gates.
- Manually trigger events by activating a server-defined event from a list.

Bookmarking

- Manually define quick or detailed bookmarks with the bookmark function.
- Create bookmarks based on rules
- Bookmarks are shown in timeline with instant preview

- Listing and previewing of bookmarks in recording search
- Bookmark reports enable effortless incident documentation
- Direct video export of a bookmark reduces the time needed to prepare forensic video material

Playback

- Playback video from 1-100 cameras per computer monitor/view
- Advanced video navigation includes fast/slow playback, jump to date/time, single step, and video motion search
- Integrated video timeline with time navigation and playback controls, including an integrated function to select a time interval for export or video retrieval from Edge Storage devices and interconnected systems
- Overview of recorded sequences and bookmarks
- Independent playback capability allows the independent playback of recorded video from one or more cameras
- Instant camera placement in playback view allows users to instantly replace cameras in a view, where a new camera can be placed in a particular view and position with a simple drag-and drop operation
- Digital zoom allows the operator to see magnified details in the recorded video

Export and Print

- The snapshot function enables operators to produce instant visual documentation of a camera by saving the camera image to a file or send it directly to a printer.
- The storyboarding function makes it possible to include video sequences from different or overlapping time intervals form different cameras in the one and the same export.
- Export in Siveillance Video format; including the standalone Siveillance Video Client – Player application for instant and easy viewing by authorities.
- Export preview with looped playback.
- Disable re-export option to prevent undesirable distribution of sensitive evidence material.
- Create evidence material in media player format (AVI files), MKV format, or still image format (JPEG images).
- Bulk camera export in multiple formats to multiple destinations, including direct export to optical media, results in more efficient video exports and more secure handling of evidence material.
- Export comment function enables users to add general and/or camera-specific comments to a video export when exporting to Siveillance Video format.
- In media player format, comments can be added as pre/post slides.
- Print incident reports including image, surveillance details and free-text user comments.
- Bookmarks are shown in timeline with instant preview
- Listing and previewing of bookmarks in recording search.
- Direct video export of a bookmark reduces the time needed to prepare forensic video material.

Centralized Search

- In this search tool, users can filter for motion, alarms, events, bookmarks, and other types of data – all in one place. This means far more rapid and efficient video investigations.
- This platform smoothly embeds partner integrations with powerful analytic capabilities via dedicated filtering options. Through specific plug-ins and devices, search criteria such as line-crossing and object-in-field will be enabled directly in the Search tab, saving time, and increasing efficiency.
- Multi-category Search allows users to combine and search across multiple Search categories to quickly find what is needed. The Search categories include people, vehicle, and location as well as any Search agents developed and integrated into Siveillance Video by third-party technology partners like Bosch, Hanwha and Axis.
- Rank Search results by relevance - Operators can rank Search results by relevance, with the most relevant results listed at the top. This new function helps users find results that best match their search parameters and quickly find what they are looking for.

Map Function

- Built-in map function in Siveillance Video Client provides intuitive overview of the system and offers integrated access to all system components.
- Map images can be in standard graphic file formats including JPG, GIF, PNG and TIF.
- Any number of layered maps such as city, street, building and room.
- Instant camera preview on "mouse over" and one-click shows all cameras on map.

- One click functions to open floating window with all cameras (maximum 25 cameras) on the map.
- Depiction of camera view zones on map with clickable PTZ zones for instant PTZ control.
- Easy drag-and-drop and point-and-click definition of cameras, servers, microphones, speakers, I/O devices, hot-zones for map hierarchies, camera view-zones and PTZ camera presets position view zones.
- Integrated control of speakers, microphones, and events and output I/O control, including doors, gates, and light and access control systems.
- Real-time status monitoring indication from all system components including cameras, I/O devices, and system servers.
- Graphical visualization of the system status through color coding.
- Hierarchical propagation of status indications to higher ordered maps.

Alarm Manager

- Dedicated dock-able tab for the Alarm Manager.
- Alarm list with extensive filtering capabilities and an alarm preview in both live and playback mode.
- Extensive alarm sort and filtering functions allow operators to focus on most critical alarms.
- Instant preview of primary and related cameras helps reduce the number of false alarms.
- Tight integration with the map function allows operators to indicate and acknowledge active alarms via the map.
- Alarm descriptions and work instructions make alarms actionable for operators.
- Alarm escalation and alarm forwarding possibilities allow operators with appropriate skills to handle different alarms.
- Alarm reports enable incident documentation.
- Alarm location map presents the alarm operator with a map showing the alarm area when an alarm is selected.
- Optional sound notifications for different alarm priorities for notification of new incoming alarm.
- Alarm disabling option enables users to suppress alarms from a given device in a certain time period
- Instant access to both live and recorded video from the cameras that are related to the alarm.
- Alarm handling reports give valuable information about alarm inflow and alarm handling performance.
- Alarm Notification (Email, Multiple notification profiles)
- Alarm Priority Levels – 32,000
- Maximum number of camera popup in alarm preview window – 15
- SNMP - TRAP support
- Alarm notifications to a single or a groups of Siveillance Video Mobile Client users using Push Notifications

System Monitor

- Dedicated dockable tab with system performance and use information.
- System Monitor function gives actual and historic performance and use reports of storage availability, network use, and server and camera performance.
  To empower system administrators to pro-actively maintain their video surveillance installation, Siveillance Video 2021 includes an extension of the System Monitoring function. The new customizable dashboard gives the system administrators a real-time at-the-glance overview of system status and allows them to do instant drilldown for first level root-cause analysis. The extended System Monitor also includes:
  o Warning/alarm thresholds per object type and individual objects
  o Predictive video retention warning
  o E-mail, alarm, and Customer
  o Dashboard notification

Authentication

- System log-in uses Microsoft Active Directory, local Windows, or a basic user account.
- Different levels of status indications available (alarm, warning, and errors).
- System performance data for cameras and servers including camera resolution, FPS, network use and disk space.
- Ability to suppress status indications (such as error and warning) for a given device.
- Possibility to edit device names in a map, and assign map-specific names and references to devices in a map
- Map editing subject to user rights.

Setup and Management

- Download and install Siveillance Video Client from a web page on the management server.
- Notification about new updates at log-in
- Application options allow users to adapt the layout and personalize the application to their preferences.

System

- Support for IPv4 and IPv6 addressing
- 64-bit Windows® operating system support enables better performance when viewing and operating many cameras.
- Support for multicast streams with automatic switch to unicast if the network becomes unreliable.

Siveillance Video Client - Player

- Playback recorded or archived video and audio evidence, including edited storyboard exports.
- Same user-friendly interface and basic functionality as Siveillance Video Client.
- Instant one-click playback for easy viewing of exported video evidence.
- Advanced second-level investigation tools make it easy to refine exported video and re-export the most essential evidence.
- Metadata bounding boxes included in exports are displayed time synchronized in Siveillance Video Client – Player.
- The project tool allows users to merge video exports or archives from two different locations or Siveillance Video systems together into one new export.
- View up to 100 cameras time-synched during playback
- Camera search function promptly finds cameras, type of cameras and camera views in the system.
- Scrollable activity timeline with magnifying feature
- Instant search on recordings based on date/time and activity/alarm (video motion detection).
- Evidence can be generated as a printed report, a JPEG image, an AV or MKVI film or in Siveillance Video format.
- Export audio recordings in WAV, MKV or AVI format.
- Exported video can be digitally zoomed to view an area of interest and minimize export footprint size.
- Re-export evidence containing Siveillance Video format and Siveillance Video Client - Player for instant, easy viewing by authorities.
- Encryption and password protection of exported video material with a choice of the following strong encryption algorithms: 256-bit AES.

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

Siveillance Video Web Client

- Two-way audio in web client
- Broadcast audio to multiple camera-connected speakers at once through Web Client
- Access Siveillance Video views through the browser and avoid advanced setup.
- Remote users can listen to, playback and export audio recordings remotely from anywhere through an Internet connection
- Shared views can be managed centrally via the server with administrator/user rights and user groups.
- Camera search function promptly finds cameras, types of cameras and camera views in the system.

- Easy video playback including fast/slow playback, single frame step, and jump to date/time with frame preview while adjusting time.
- Option for client-side video decoding via browser-plugins.
- Control PTZ cameras remotely, including preset positions.
- Dynamic bandwidth optimization when streaming from server to client gives better use of bandwidth.
- Create AVI files or save JPEG images.
- Export on the server to avoid moving large video files back and forth. Only download needed files or save them for downloading when on a faster connection.
- Preview exports on the server without downloading them.
- Trigger outputs and events with live view of related camera.
- System login using Siveillance Video username and password.
- System login using Microsoft Active Directory user
- Secure connection through HTTPS.
- No installation needed on client computer.
- Secure video evidence handling with a digital signature of re-exported video material enables users to verify that the video has not been modified or tampered with when viewing the export in Siveillance Video Client – Player.
- View, modify or add general and/or camera-specific comments for a given video export.
- De-interlacing of video from analog cameras.
- IPIX technology for PTZ in 360° recorded images.
- 360° ImmerVision Enables panomorph lens technology.
- Use organization's own Identity and Access Management system (Open ID Connect based) to authorize and authenticate users. It enables support for SSO.

Siveillance Video Mobile

- One & Two-way audio in Mobile client
- Audio support on video push enables users to push live video from the device's camera directly into Siveillance Video for stronger documentation of incidents.
- Supports any mobile device running Android or iOS.
- Add login credentials for multiple servers in the Siveillance Video Mobile to easily switch between sites or different connection addresses.
- Views are inherited from the connected Siveillance Video system. The user is restricted up to 2 views from the Siveillance Video client system.
- A view with all cameras is automatically generated, allowing Siveillance Video Mobile to be used when no views are set up. It also provides a quick way of searching through cameras.
- Camera search function promptly finds cameras, types of cameras and camera views in the system.
- Timeline Search and Preview - The new recording timeline in Video Mobile is enhanced with an enlarged preview image when users scroll the timeline. This makes it easier to see the recorded footage and locate a relevant video sequence.
- Cameras can be viewed in full screen to take better advantage of the device's screen. It is also possible to search through cameras in a view while in full screen by swiping left or right.
- Digital pinch-to-zoom enables users to zoom in on a part of the image for closer review and conduct detailed investigation of video when using megapixel or high-definition cameras.
- Playback recordings from the database and select a specific time or recorded sequence to start playback, step through recordings and select a playback speed.
- View recordings from the database while keeping an eye on what is currently happening. The client displays a live picture-in-picture frame of the same camera when in playback mode. The picture-in-picture can be moved by dragging and double tapping will return to live view.
- Option to include location metadata in Video Push
- Control PTZ cameras with Siveillance Video Mobile either manually or by selecting predefined presets for quick navigation.
- Video Push allows users to use their mobile devices' cameras as cameras in your Siveillance Video. Easy to use and requires no setup in the mobile device.
- Connect securely to the Siveillance Video Mobile server using HTTPS encryption.
- Receive alarm notifications using Push Notifications, notifications include access to video, alarm information and instructions
- Investigation function to access investigations done in the Web client

- System log-in using Siveillance Video username and password. Possible to change basic user password via a link from the login dialogue box.
- System log-in using Microsoft Active Directory user
- Support of biometric authentication for log-in for Android and iOS devices
- MDM (Mobile Device Management) support for Android and iOS devices
- Use organization's own Identity and Access Management system (Open ID Connect based) to authorize and authenticate users. It enables support for SSO

Siveillance Video Monitoring Wall (Optional)

- Hardware independent, it runs on standard servers and displays. No special Monitoring wall hardware or network configurations required.
- Flexible and scalable, it supports multiple Siveillance Video combination of monitors at any location.
- Share important information with control room personnel using manual text messages or pre-defined messages that are displayed on certain events and incidents
- Black screen monitoring is a new capability that allows operators to focus on critical activities. In Monitor Wall the cameras can automatically be removed from the Monitor Wall when an incident has been cleared. This means that the control room operators only are presented with the relevant video feeds.
- In addition to live video the Monitor Wall supports playback of video, where any authorized operator seamlessly can control playback of video from his/her Video Client. This enables collaboration in assessment of incidents and investigations.
- To enable flexible and efficient collaboration in control rooms the Monitor Wall supports a wide set of different content. This means that operators instantly can share alarms, still images, bookmarks, maps, carrousels, etc. with peers, and coordinate effort and responses

Management

- Management of Siveillance Video Monitoring wall is fully integrated with the Management Client.
- Intuitive Siveillance Video Monitoring wall builder enables easy definition of any number of Siveillance Video Monitoring wall, including the size and position of individual monitors.
- Siveillance Video Monitoring wall presets provide powerful control of the layout (camera grid) and camera content
- All user actions are subject to the assignment of user rights.

Control

- Dynamic user control of Siveillance Video Monitoring wall layout and content through manual drag-and-drop of cameras and views into Siveillance Video Monitoring wall via Siveillance Video Client.
- Automatic event-driven control of Siveillance Video Monitoring wall layout and content based on rules, such as motion detection, I/O, integrated third-party applications, time, or video analytics events.
- Layout control enables instant insertion of a camera in a specific monitor and position, changes of Siveillance Video Monitoring wall monitor layout, setting of all
- Trigger outputs and events:
  Use your mobile device to trigger outputs connected to the Siveillance Video, or trigger user-defined events to have greater control while on the go.
  Connect securely to the Siveillance Video Mobile server using HTTPS encryption.
- Export on the server to avoid moving large video files back and forth. Only download needed files or save them for downloading when on a faster connection.

View

- Individual Siveillance Video Client users can view Siveillance Video Monitoring wall views as a part of the available view selection, which enables Siveillance Video Monitoring wall to be used as an operator collaboration tool.

Audio

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

Licensing Structure

Server Base License

- A Siveillance Video Advanced server base license is mandatory for installing the product
- The base server license permits the following deployments within the legal entity purchasing the base server license:
  - Unlimited number of Management Servers
  - Unlimited number of Recording Servers
  - Unlimited number of Siveillance Video Clients, Siveillance Video Web Clients and Siveillance Video Mobile applications

Hardware Device License

- To connect cameras, audio devices video encoders and other devices to Siveillance Video Advanced, one license per physical hardware devices required. In total, for all copies of the product installed under this license, the product may only be used with hardware devices as you have purchased hardware device licenses for (For encoders, please refer the Supported Hardware webpage for license requirements)
- An unlimited number of hardware device licenses can be purchased. To extend an installation with additional hardware device licenses, the base server license number (SLC) is required when ordering
- New license enforcement logic enables simplified licensing handling:
- Off-line systems require initial activation and re-activation at extensions 15% (min 10/max 100) cameras may be replaces per year without re-activation (e.g., if the customer is licensed with 500 cameras then 15% of 500 which is 75 cameras can be replaced without re-activation and if the cameras are 2000 then maximum of 100 (as 15% of 2000 is 300 which is greater than 100) cameras can be replaced without re-activation.)

Siveillance Video Monitoring Wall Application License

- Siveillance Video Monitoring Wall is an add-on product to Siveillance Video Advanced and is subject to separate licensing
- The Siveillance Video Monitoring Wall application license permits connection of unlimited numbers of Siveillance Video Monitoring Walls (including physical displays) and camera feeds

Siveillance Video Incident Manager Application License

- Siveillance Video Incident Manager is an add-on product to Siveillance Video Advanced and is subject to separate licensing

Note to Value Added Partners:

Certain links in this document may not work for you because they direct to Siemens internal information. Please get in touch with your local Siemens partner for relevant information.

Cybersecurity 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 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

Issued by

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