



DATA AND SPECIFICATION SHEET

# Siveillance™ Video Core Plus

2022 R3 | DECEMBER 2022

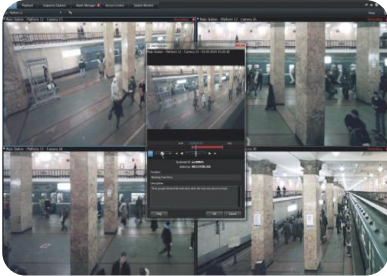
**SIEMENS**

# Contents

<b>What's New in 2022 R3</b>	<b>4</b>
Key Features	5
Product Facts	6
Feature Overview	7
Recording Server System	9
Pan-Tilt-Zoom (PTZ)	9
I/O and Events	9
Setup and Management	10
Client Access	10
Alerting and Notification	10
Logs	10
Storage & Archiving	10
Management Server and Client	10
System	10
Siveillance Video Interconnect	11
Devices	11
Rules, Time Profiles and Notifications	11
User Rights Management	12
Logging	12
Management Client Profiles	12
Siveillance Video Client Profiles	12
System Administration	12
Event Server	13
Alarm Manager	13
Authentication	13
Siveillance Video Mobile server	13
Siveillance Video Client	13
General	13
Live View	14
I/O and Events	14
PTZ	14
Playback	15
Export and Print	15

Centralized Search	15
Map Function	15
Setup and management	15
Alarm Manager	16
Siveillance Video Client - Player	16
Authentication	16
System	16
Siveillance Video Web Client	17
Siveillance Video Mobile	17
Trigger Outputs and Events	18
Audio	18
<b>Licensing Structure</b>	<b>19</b>
<b>Cybersecurity Disclaimer</b>	<b>20</b>

# Siveillance™ Video Core Plus



A powerful solution for small to medium deployments including more than 115 features and functions.

The Siveillance Video Core Plus 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 unlimited number of network video and wide variety of computer hardware equipment.

## What's New in 2022 R3

- Device search filter (Siveillance Video Management Client)
- Enhanced User Experience on Siveillance Video Client and Web Client
- Built-in search agents are available in Centralized Search
- 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](http://www.siemens.com/siveillance-video)



# Key Features

- Supports H.265
- Adding Devices on HTTPS
- Dual Live Stream and Recording per Camera
- Open/Close doors, Grant/ Deny access Mobile Client
- Siveillance Video Operates in a Windows FIPS 140-2 compliant mode
- DLNA ready
- Generic 360-dewarping
- Online Activation
- Two-step verification
- Video Client Performance improvements (Either using NVIDIA cards or Intel Quick Sync)
- Siveillance video driver framework
- Metadata support for Edge based video analytics
- The Video Driver API / SDK supports unlimited channels for integration
- Kerberos Authentication
- Two-way AAC Audio support
- Flexible device replacement licensing
- Initial setup of credentials on devices (limited to supported devices, e.g., Axis, Bosch, Hanwha and Avigilon)
- Support for ONVIF & PSIA
- Video Client with better 4K Streaming performance
- 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
- HTTP over SSL/TLS
- Cross version Management/Compatibility
- ONVIF Gateway Interface - private-to-public video, Alarm Centers, and Monitoring Stations
- Failover Management (Redundant Cluster)
- Scalable Video Quality Recording™ (SVQR)
- Hardware accelerated video decoding in the Mobile Server
- 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
- Refresh of hardware information in management client
- Adaptive Streaming
- Multi Live Streaming
- Direct Streaming
- 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<sup>(1)</sup> 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/ SIPOINT Plug-in limitations

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

## Integration

- Plug-in, Protocol, Component integration via MIP SDK
- 3<sup>rd</sup> Party Metadata integration via MIP SDK
- 3<sup>rd</sup> 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

## Language (Management Interface)

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

# Feature Overview

- **Scalable multi-server and multi-site solution**  
Siveillance Video CorePlus supports unlimited number of IP devices, unlimited number of recording servers.
- **Centralized Management**  
Siveillance Video CorePlus can be used as a remote site in Interconnect architecture.
- **Alarm Manager**  
Single-point alarm function that provides a consolidated and clear overview of security and system-related alarms.
- **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.
- **64-bit Recording Servers**  
Allow more cameras to be run on a single recording server.
- **Customizable Management User Interface** Adaptable management user interface makes it possible to toggle the availability of functions on and off in the Management Client
- **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.
- **ONVIF T and Q Profiles**
- The generic ONVIF driver will now cover features for ONVIF profiles T and Q in addition to the existing Profile G and S
- **Hardware Accelerated Video Motion Detection Video**  
Motion detection (VMD) decoding is moved from the CPU to the GPU part of the Intel® Quick Sync Video. CPU to significantly reduce the CPU load and improve performance of the recording servers.
- **Operational Intelligence**
  - Metadata – Harvesting/Automation
  - Built-in Video Motion Detection (VMD)
  - Adjustable VMD sensitivity
  - Real-time VMD analysis
  - 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.
- **Intuitive Map Function**  
Multi-layered and interactive maps display the location of every camera and offer control of the entire surveillance system. It also has seamless drag-and-drop integration with Siveillance Video Monitoring wall.
- **Multiple Language Support**  
Let's 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 accesses, 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.
- **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.
- **Web Client Alarm List**  
List of alarms in the systems so users can quickly get and overview and act if needed
- **Network Configuration**  
Camera user handling and network settings configuration done directly in the VMS – for your existing ONVIF-compliant devices. Simplify the way you work and quickly change network settings – without the need to access each individual device.

- **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 MIPS SDK.
- **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
- **Liftable Privacy Masking**  
Privacy well protected both on live and recorded video using permanent and liftable privacy masking
- **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 Video 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 Server for heightened security on server communication
- **Device Password Management**  
Built-in password generator complies with the requirements of supported device manufacturers
- **More Secured, Stronger data protection and Enhanced Encryption**  
Siveillance Video now includes
  - The latest Microsoft CNG encryption modules
  - Password protected configuration
  - 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)
- **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**  
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



## Integration Options

- The Siveillance Video Integration Platform Software Development Kit (MIP SDK) 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.

## 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.
- 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.
- 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.
- Recording quality depends entirely on camera and video encoder capabilities with no software limitations.
- 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.
- Support for both IPv4 and IPv6 addressing
- Secure HTTPS camera connection on devices supporting HTTPS.
- Remote Connect Services enable you to securely connect remote cameras across different types of private and public networks.

## Pan-Tilt-Zoom (PTZ)

- "Pass-through" control of manual PTZ operation from clients with user priority.
- 3 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.
- Unlimited Preset positions per camera
- Configure PTZ preset positions via Video client
- Go-to preset on event
- Configurable Scanning/Transition speed
- Reserve PTZ priority & rights via video client

## 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.

## 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 rule activation.

## Logs

- Logging of system, audit, and rule entries to the management server with local caching during offline scenarios.
- Site details (name, address, administrators, and additional information) defined in the federated system is available in the site navigation.

## 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 of recordings
- Archive to network drives (NAS, iSCSI, SAN)
- Support for live video play without recording storage
- Storage overview gives instant indication of used vs. available storage in total and for individual cameras.
- Manage maximum recording time for manual recordings.

## Management Server and Client

### System

- Management server for user authentication login, system configuration and logging.
- Management Client for central administration of the system such as recording servers, devices, security, rules and logging.
- Management Client compatible with Siveillance Video Core, Core plus, Advanced and Pro 2019 R1 and newer
- All configuration and logs from the entire system are stored in a centralized Microsoft SQL database and accessible by the management server only.
- 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 register and validate your licenses, the system offers easy-to-use offline activation.
- Support for both IPv4 and IPv6 addressing.
- Configuration wizards for aided system setup
- Device Management (Device Grouping, Device Model Detection, Replacement Wizard)
- Seamless virtual hardware movement between recording servers
- Day length time profile

## Siveillance Video Interconnect

- Siveillance Video Core Plus can be used as a remote site
- 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 for where motion detection is to be disabled to avoid unwanted detection.

## Devices

- Hardware wizard to add devices; automatically using Universal Plug and Play (UPnP) discovery, via IP network range scanning, or using manual device 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 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.
- 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

## Rules, Time Profiles and Notifications

- Rule actions are triggered by event, time interval or a combination of event and time. Rules can be optionally stopped by event or after a certain time.
- Time profiles with reoccurring 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.
- Rule-based bookmark creation.
- **Trigger events:**  
The Siveillance Video 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:  
**Hardware:** events that relate to physical hardware devices connected to the system.  
**Devices:** events that relate to certain functions and states of devices available to the Siveillance Video system via the connected hardware devices.  
**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.  
**Start actions:** The triggering events may initiate a wide set of actions in the VMS, connected devices or integrated systems.  
For a complete list of available actions, please refer to the Siveillance Video Administrator's Manual.  
**Stop actions:** The rule engine may also trigger stop actions in the VMS, 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
- Multi-recipient customizable email notification with image and/or AVI attachment of incidents.

## User Rights Management

- Supports inherited user rights and the ability to assign partial management rights
  - 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).
- Roles control user and administrator access to:
- General:** Management Client and Siveillance Video Client profiles, dual authorization rights, system log-in time profile.
- Cameras:** Visibility, administrate, liveview (within time profile), playback (within time profile), search sequences, export, smart search, AUX commands, manual recording.
- Inputs and outputs:** visibility, administrate, status, activation.
- External events:** visibility, administrate, trigger
- View groups privileges.
- 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 and clients.
- Each log file has adjustable size and Time Limitations

## Management Client Profiles

- Centralized management of Management Client application options enables optimization of the Management Client for different user categories and skill levels.
- Ability to tailor the availability of main/sub functions in the Management Client for different user roles.

## 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.
- Ability to enforce or recommend optional
- Siveillance Video Client application options for a user or group of users, using an unlimited number of Siveillance Video Client profiles.
- Define general Siveillance Video Client application options, including (listing not exhaustive): 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 the availability of individual control panes and overlay buttons.
- Access to playback mode and the availability of individual control panes, overlay buttons and settings for specific functions, such as default export path.
- Access to setup mode and the availability of individual control panes and setup functions.
- Access to Centralized Search, Alarm Manager, System Monitor.
- Access to setup mode and the availability of individual control panes and setup functions.
- Definition of available view layouts.

## System Administration

- Built-in backup and restore support for manual system backup of all configuration data, including (listing not exhaustive): system configuration data, maps, alarm settings and definitions and client views.
- 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 the 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
- 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.

### Authentication

- System log-in uses Microsoft Active Directory, local Windows or basic user account.
- Use current Windows logon 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.
- Password change for Basic user – Force password change on next login.

### 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 server can transcode video 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 Web Clients.
- 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 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
- The Siveillance Video Mobile server can serve video directly to the Web client/Mobile clients via the direct streaming feature. No transcoding to MJPEG required which significantly reduces the load on the Mobile server

## Siveillance Video Client

### General

- Dedicated task-oriented tabs for the 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.

## 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.
- 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.
- Search Matrix function shows live video from multiple cameras in any view layout with customizable rotation paths, remotely controlled by computers sending matrix remote commands.
- 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.
- 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.
- Update on "motion only" optimizes CPU use by allowing motion detection to control whether the image should be decoded and displayed.
- Global hotspot function allows users to work in detail with any camera selected from any view.
- Local hotspot function allows users to work in detail with a camera selected from the same view.
- Carousel function allows a specific view item to rotate between pre-defined cameras that are not necessarily present in the view at the same time. Operators can select default or custom display times for each camera, and they are able to manually switch to the next or previous camera in the carousel list
- 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.
- 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 drivers.

## I/O and Events

- Manually trigger output port relay operation, for example when controlling gates.
- Manually trigger events by activating a server- defined event from a list.

## 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
- 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.

## 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, Evidence Lock or video retrieval from Edge Storage devices and interconnected systems.
- Toggle between simple and advanced timeline mode.
- Overview of recorded sequences
- 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.
- Support for live video play without recording storage

## 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 sending it directly to a printer.
- Create evidence material in media player format (AVI files), MKV format, or still image format (JPEG images).
- Disable re-export option to prevent undesirable distribution of sensitive evidence material.
- 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.
- In media player format comments can be added as pre/post slides.
- Print incident reports including image, surveillance details and free-text user comments.

## Centralized Search

- 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
- Search categories are video sequences, bookmarks, motion, alarms, events, people, vehicle, location and LPR (Note: - People, Vehicle and Location Limited to certain camera models that can perform video analytics and export ONVIF compliant metadata)

## 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 function 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.
- 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.

## Alarm Manager

- Dedicated dockable 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 in 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 Management (Reassign, Update status, Comment)
- Alarm Handling (View triggered alarms, Report, Log, Status)
- Alarm Notification (Email, Multiple notification profiles)
- Alarm Priority Levels – 32,000
- Alarm notifications to a single or a groups of Siveillance Video Mobile Client users using Push Notifications
- Maximum number of camera popup in alarm preview window – 15

## Siveillance Video Client - Player

- Play back recorded or archived video evidence
- Same user-friendly interface and most functions as Siveillance Video Client.  
Offers a simplified user interface with the possibility option to toggle between “Simple” and “Advanced” modes.
- 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, types 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 AVI or MKV film or in Siveillance Video 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.
- View, modify or add general and/or camera- specific comments for a given video export.

## Authentication

- System log-in uses Microsoft Active Directory, local Windows, or a basic user account.
- Use current Windows logon for authentication.
- Auto-log-in and auto-restore views.
- Use organization's own Identity and Access Management system (Open ID Connect based) to authorize and authenticate users. It enables support for SSO

## System

- Support for IPv4 and IPv6 addressing
- 64-bit Windows® operating system support enables better performance when viewing and operating many cameras.

## Siveillance Video Web Client

- Two-way audio in web client
- Broadcast audio to multiple camera-connected speakers at once through Web Client
- Remote users can listen to, playback and export audio recordings remotely from anywhere through an Internet connection
- Access Siveillance Video views through the browser and avoid advanced setup.
- 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.
- 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 log-in using Siveillance Video username and password.
- System log-in using Microsoft Active Directory user.
- Secure connection through HTTPS.
- Direct streaming supported, meaning that the Web client can receive H.264 directly from the recording server without transcoding, which is more efficient and provides a smoother experience
- Adaptive streaming enables a lower resolution stream from the recording server to the Video Client, Video Wall, Mobile Client, or Web client when a high resolution is not required, i.e., when displaying video where the view items do not require high resolution streams
- 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.
- Direct streaming supported meaning that the Mobile client can receive H.264 and H.265 directly from the recording server without transcoding in the Mobile Server, which is more efficient and provides a smoother experience
- Adaptive streaming enables a lower resolution stream from the recording server to the Video Client, Video Wall, Mobile Client, or Web client when a high resolution is not required, i.e., when displaying video where the view items do not require high resolution streams
- Supports any mobile device running Android or iOS.
- Add log-in credentials for multiple servers in Siveillance Video Mobile to easily switch between sites or different connection addresses.
- Views are inherited from the connected Siveillance Video system. The client automatically obtains the user's private and shared views from the system to be used as camera lists in Siveillance Video Mobile.
- 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.
- 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.
- Play back recordings from the database and select a specific time or recorded sequence to start playback, step through recordings and select a playback speed.
- 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.
- 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.
- 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 the Siveillance Video. Easy to use and requires no setup in the mobile device.
- Option to include location metadata in Video Push.
- 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

## Trigger Outputs and Events

- Mobile devices can trigger outputs connected to the Siveillance Video, or 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.

## 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 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 Management Server
  - Unlimited Recording Server
  - Unlimited number of Siveillance Video Clients, Siveillance Video Web Clients, and Siveillance Video Mobile applications

## Hardware Device License

- To connect cameras, video encoders and other devices to Siveillance Video, 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.)

## Licensing of Siveillance Video Interconnect

- Siveillance Video Core Plus can be used as a remote site

## Siveillance Video Incident Manager Application License

- Siveillance Video Incident Manager is an add-on product to Siveillance Video Core Plus 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