KEY FEATURES

Siveillance™ Video

2022 R3 | DECEMBER 2022

SIEMENS

Copyright

Due to continued product development, the information in this publication and related software may change without notice. Please report any errors to Siemens Switzerland Ltd in writing. Siemens Switzerland Ltd does not warrant that this publication or related software is error-free.

Any references to companies or persons are for purposes of illustration only and are not intended to refer to actual individuals or organizations.

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.

Key Features

Management Client device search filter

It is now possible to search for devices in the recording server tree. Searches can be made on device name and IP address. In addition, 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.

Video Client transmits telemetric data

Smart Client now transmits telemetric data to the Systems with the purpose of optimizing the product. Data collected includes data on feature usage, errors / exceptions, and system configuration. All data is sent encrypted and pseudonymized. Telemetry can be turned off from the Management Client

Updated visual elements and changes

Easily change single and multiple-device passwords directly within Siveillance Video system for an easier and more secure user experience. Device password management is easier than ever with a built-in password generator complying with the requirements from each of the individual supported device manufacturers.

Changed behavior of Independent playback in the Video Client has been modified

To make it more usable, when using independent playback to quickly check up on something witnessed in a particular video feed. Now when entering Independent Playback from Live mode, the video will skip back 10 seconds and automatically start playing. If Independent playback is entered from playback mode, while the video is playing forward the video will similarly skip back 10 seconds, while if the video is playing backwards the video will skip forward 10 seconds. If the video is stopped Independent playback mode will be entered, but no skip will take place.

Left pane views/ devices navigation and search in Web Client

To bring the Web Client look and feel closer to the Smart client, we have renewed the Live page navigation in the Web Client to have the left pane with all views, all camera view and all cameras tree below. The left pane can be expanded and collapsed and there is also the ability to search in both the views and the devices trees. Once the user has selected what he or she were searching for, up to 7 such search items can be kept in the recent search suggestions, so that the user can more easily find frequently used views/camera feeds.

Toast notifications for alarms raised in Web Client

When an alarm or other event is raised, now the user is prompted to go to the alarms page with a toast notification within the Web Client. Similar events are grouped in the same toast message, to preserve screen real estate. Clicking on the toast message will bring the user to the Alarms tab in the Web Client, so they can see the alarm details and respond to it.

Ease of use

The login procedure splits into two. The server screen is now separated from the user log in screen. Users can add servers separately and then choose to enter their credentials. The new screens are user – centered and the following buttons and settings.

o Log out

o Change password

o Disconnect from server

o Go to the app settings.

For Android users: Time picker – the time picker has a new and simplified interface. For more information, see Using the playback timeline

Using biometrics or device credentials to secure the app in Siveillance Video Mobile Client

You can now use biometrics or your device credentials to verify your identity before you open the app. Quick authentication based on your fingerprint, face ID, or device credentials facilitates access to the Mobile client and improves the security of the app.

Mobile device management (MDM)

Mobile client now supports mobile device management (MDM). With MDM, you can manage and secure devices, apps, and data from a unified console.

H.265 Support in Open Network Bridge

The Siveillance Video Open Network Bridge enables frictionless communication between Siveillance Video and other IP video surveillance products. Easily share video streams between different VMS systems and applications, access and retrieve H.264 and H.265 video streams simultaneously. Explore new opportunities and win business.

API Gateway support

The API Gateway is installed on-premises and is intended to serve as a front-end and common entry point for RESTful API services on all the current VMS server components (management server, event server, recording servers, log server, etc). The API Gateway acts as broker, routing requests and responses between external clients and the various downstream Siveillance Video services.

The RESTful API is implemented in part by each specific VMS server component, and the API Gateway can simply pass-through these requests and responses, while for other requests, the API Gateway will convert requests and responses as appropriate.

External IDP Users

An external IDP is an external application and service in which you can store and manage user identity information and provide user authentication services to other systems. You can associate an external IDP with the Siveillance Video.

The external IDP provides a set of claims to automatically create a name for the user in Siveillance Video, and in it an algorithm is used to pick a name from the external IDP that is unique in the VMS database.

Users can now log into their Web Client with their preferred identity provider service. This option is however only available for secure, encrypted connections. If the Mobile server does not have an encryption certificate setup, the button for third party IDP will not appear on the Web Client login page.

You can log in to the Mobile app using an external IDP. The alternative login method allows you to bypass the required user credentials of a basic user or a Windows user and continue to be authorized to access the app.

Video Client – New Export workflow

On the Exports tab, you can choose which formats to use for the export, and for each format, you can change the Export settings:

- Format settings
- Media player format settings
- Still images settings-

Incident Manager

Siveillance Video Incident Manager is a Siemens add-on supported from 2022 R2 onwards that enables organizations to document incidents and combine them with sequence evidence (video and, potentially, audio) from their Siveillance Video.

Users of Siveillance Video Incident Manager can save all the incident information in incident projects. From the incident projects, they can track the status and activities of each incident. In this way, the users can manage incidents effectively and easily share strong incident evidence, both internally with colleagues and externally with authorities.

The operators of Siveillance Video Client start, save, and manage incident projects and add various information to the incident projects. This includes free text, incident properties that the administrators have defined, and sequences from the Siveillance Video. For full traceability, the Siveillance Video logs when administrators define and edit incident properties and when operators create and update the incident projects.

Note: There are over 150 features and functions that are available within the Siveillance Video Pro, over 138 for the Siveillance Video Advanced & over 100 for the Siveillance Video Core plus and Core. For a complete overview of features please see the Siveillance Video Comparison Guide.

Downloads & Documentation

The Siveillance Video software, release notes, sales documents and technical manuals are all available for download from below URLs.

Documents & Manuals	Siveillance Video Intranet
Software Installer	SIOS Portal

Support & Contacts

Technical Support	mySupport: Service Request Intranet: Siveillance Video Intranet Internet: Siveillance Video Internet EMEA: +49 89 9221 8000 APAC: +91 44 6156 4325 America: +1 800 877 7545
Training	Internal Siemens: Siemens My Learning External: Contact your local Siemens representative

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