



Siveillance™ Video

System Requirements

2020 R1



Software Requirements for Computers running Siveillance Video Core, Core Plus, Advanced & Pro

Operating System

- Microsoft® Windows® 8.1 Pro (64 bit)
- Microsoft® Windows® 8.1 Enterprise (64 bit)
- Microsoft® Windows® 10 Pro (64 bit)
- Microsoft® Windows® 10 Enterprise (64 bit)
- Microsoft® Windows® 10 IoT LTSB 2016 or later (64 bit)
- Microsoft® Windows® 10 IoT Enterprise version 1803 or later (64 bit)
- Microsoft® Windows® Server 2012 (64 bit): Standard and Datacenter
- Microsoft® Windows® Server 2012 R2 (64 bit): Standard and Datacenter
- Microsoft® Windows® Server 2016 (64 bit): Essentials, Standard and Datacenter
- Microsoft® Windows® Server 2019 (64 bit): Essentials, Standard and Datacenter

To run clustering/failover management servers, you need a Microsoft® Windows® Server 2012/2012 R2 Standard or Datacenter edition, Microsoft® Windows® Server 2016 Standard or Datacenter edition, or a Microsoft® Windows® Server 2019 Standard or Datacenter edition

File System

For the Recording Storage Location, NTFS file system is recommended

SQL Versions

- Microsoft SQL Server® 2012 SP1
- Microsoft SQL Server® 2014
- Microsoft SQL Server® 2016
- Microsoft SQL Server® 2017

Software

Microsoft® .NET 4.7 Framework
DirectX 11 or newer

Hardware acceleration

- Hardware acceleration with Intel® Quick Sync requires an Intel® CPU 4th generation or newer, supporting Intel Quick Sync and Intel® GPU enabled in BIOS.
- Decoding with NVIDIA graphics card is supported with GPU capability version 6.x (Pascal) or newer.



System Requirements for running 32 cameras (720P, @25 FPS, 2 Mbit/s) on Siveillance Video Core

CPU	Intel® Core™ i3-6100 3.7 GHz
RAM	8 GB
Network	2 x 1 Gigabit Ethernet
Graphics Adapter	Intel® HD Graphics 530 (If Hardware Acceleration is required add graphics card fitting the requirements)
Hard Disk Space	128GB SSD for OS/VMS storage (Add additional storage depending on the amount of days you want to save data)



System Requirements for running 120 cameras (720P, @25 FPS, 2 Mbit/s) on Siveillance Video Core Plus, Advanced & Pro

CPU	Intel® Core™ i3-6100 3.7 GHz
RAM	16 GB
Network	2 x 1 Gigabit Ethernet
Graphics Adapter	Intel® HD Graphics 530 (If Hardware Acceleration is required add graphics card fitting the requirements)
Hard Disk Space	256GB SSD for OS/VMS storage (Add additional storage depending on the ammount of days you want to save data)



System Requirements for running 700 cameras (720P, @25 FPS, 2 Mbit/s) on Siveillance Video Core Plus, Advanced & Pro

CPU	Intel® Xeon® E3-1515M V5 2.8 GHz
RAM	32 GB
Network	10 Gigabit Ethernet
Graphics Adapter	Intel® Iris™ Pro Graphics P580 (If Hardware Acceleration is required add graphics card fitting the requirements)
Hard Disk Space	2 x 256 GB SSD RAID 1 for OS/VMS storage (Add additional storage depending on the amount of days you want to save data)



Software Requirements for Computers running Siveillance Video Client, Video Client-Player and Monitor Wall

Operating System

- Microsoft® Windows® 8.1 Pro
- Microsoft® Windows® 8.1 Enterprise
- Microsoft® Windows® 10 Pro
- Microsoft® Windows® 10 Enterprise
- Microsoft® Windows® 10 IoT LTSB 2016 or later (64 bit)
- Microsoft® Windows® 10 IoT Enterprise version 1803 or later (64 bit)
- Microsoft® Windows® Server 2012: Standard and Datacenter
- Microsoft® Windows® Server 2012 R2: Standard and Datacenter
- Microsoft® Windows® Server 2016: Standard and Datacenter
- Microsoft® Windows® Server 2019: Standard and Datacenter

Software

Microsoft® .NET 4.7 Framework,
DirectX 11.0 or newer

Hardware acceleration

- Hardware acceleration with Intel® Quick Sync requires an Intel® CPU supporting Intel Quick Sync and Intel® GPU enabled in BIOS.
- Decoding with NVIDIA graphics card is supported with GPU capability version 6.x (Pascal) or newer.
- Hardware acceleration with NVIDIA Graphics card requires 64-bit Microsoft® Windows® version.



Computer running Siveillance Video Web Client

CPU	Intel® Core™2 Duo, 2.0 Ghz Intel® Core™ i3-5010U, 2.1 Ghz
RAM	2 GB
Network	Ethernet 100 Mbit / WiFi 2Mbit
Graphics Adapter	Onboard GFX, AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16-bit color
Hard Disk Space	Minimum 500 MB free
Operating System	Any capable of running the below browsers
Software	Browser: <ul style="list-style-type: none">• Microsoft Edge 42• Safari® 11.0.1• Google Chrome™ 64• Mozilla® Firefox® 58



Siveillance Video Mobile Client

RAM	2GB*
Operating System	Android 6.0 or higher
	iOS 11.0 or higher
Network	2G/3G data connection. 4G or Wi-Fi*.

*Required for using Direct Streaming



Downloads and documentation

The Siveillance Video 2020 R1 software, release notes, administrator manual and the Siveillance Video 2020 R1 video Client user manual are all available for download from below urls.

Localization & System

Requirements

<http://intranet.siemens.com/siveillance-video>

Product availability

<https://support.industry.siemens.com/cs/products?mfn=ps&pnid=24899&lc=en-WW>



Support & Contacts

Technical Support

Siveillance Technical Support: siveillance.support.industry@siemens.com

Intranet: [Siveillance Video Intranet](#)

Internet: [Siveillance Video Internet](#)

EMEA: +49 89 9221 8000

APAC: +91 44 6156 4325

Americas: +1 800 877 7545

Cyber security disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of 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 <http://www.siemens.com/industrialsecurity>

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

© 2020 Copyright Siemens Switzerland Ltd

Technical specifications and availability subject to change without notice.