



SYSTEM REQUIREMENTS

# Siveillance™ Video

2022 R1 | April 2022

**SIEMENS**

# Copyright

Copyright © 2022. Siemens Switzerland Ltd. All rights reserved.

The information contained in this publication is company-proprietary to Siemens Switzerland Ltd. This publication and related software are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Reverse engineering / copying of any Siemens Switzerland Ltd hardware, software, documentation, or training material is strictly prohibited.

This publication and related software remain the exclusive property of Siemens Switzerland Ltd. No part of this publication or related software may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission from Siemens Switzerland Ltd.

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.

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

Name	Description
CPU	Intel® Core™ i3-1005G1 3.40 GHz
RAM	8 GB
Network	1 Gigabit Ethernet
Hard Disk Space	256GB SSD for OS/VMS storage (Add additional storage depending on the number of days you want to save data)
Graphics	Onboard GFX, AGP, or PCI-Express, minimum 1024 x 768, 16-bit color
Operating	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 Enterprise LTSC (Long-Term Servicing Branch) 2016 (version 1607 or later)
	Microsoft® Windows® 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core
	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
	Microsoft SQL Server® 2019 (Only supported on Microsoft® Windows® 10 or greater and Microsoft® Windows® Server 2016 or greater)

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

Software	Microsoft® .NET 4.7.2 Framework, Microsoft® .NET 6 Runtime
	DirectX 11 or newer
Hardware	Hardware acceleration with Intel® Quick Sync requires an Intel® CPU 4th generation or newer. Decoding with NVIDIA graphics card is supported with GPU capability version 6.x (Pascal) or newer.

## Software Requirements for Computer running Mobile Server

Name	Description
CPU	Intel® Core™ i3-1005G1 3.40 GHz
RAM	8 GB
Network	1 Gigabit Ethernet
Hard Disk Space	256GB SSD for OS/VMS storage (Add additional storage depending on the number of days you want to save data)
Graphics Adapter	Onboard GFX, AGP, or PCI-Express, minimum 1024 x 768, 16-bit color
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 Enterprise LTSB (Long-Term Servicing Branch)2016 (version 1607 or later)
	Microsoft® Windows® 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core
	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

---

## Software Requirements for Computer running Mobile Server

Name	Description
Software	Microsoft® .NET 4.7.2 Framework, Microsoft® .NET Core 3.1.13 Framework
	DirectX 11 or newer

---

## System Requirements for running 32 cameras (1080P, @25 FPS, 2.5 Mbit/s) on Siveillance Video Core

Name	Description
CPU	Intel® Core™ Core i5-10300H 4.5 GHz max
RAM	16 GB
Network	2 x 1 Gigabit Ethernet
Graphics Adapter	Intel® UHD Graphics (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 number of days you want to save data)

---

## System Requirements for running 120 cameras (1080P, @25 FPS, 2.5 Mbit/s) on Siveillance Video Core Plus, Advanced & Pro

Name	Description
CPU	Intel® Core™ i7-10850H 5.1 GHz max
RAM	32 GB
Network	2 x 1 Gigabit Ethernet
Graphics Adapter	Intel® UHD Graphics (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 number of days you want to save data)



## System Requirements for running 700 cameras (1080P, @25 FPS, 2.5 Mbit/s) on Siveillance Video Core Plus, Advanced & Pro

Name	Description
CPU	Intel® Xeon® E3-1535M V6 4.2 GHz max
RAM	64 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 number of days you want to save data)

## Computer running Siveillance Video Client, Video Client Player and Video Wall

Name	Description
Operating	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 Enterprise LTSB (Long-Term Servicing Branch)2016 (version 1607 or later)
	Microsoft® Windows® 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core
	Microsoft® Windows® 11 Pro
	Microsoft® Windows® 11 Enterprise
	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	
Software	Microsoft® .NET 4.7.2 Framework
	DirectX 11 or newer

## Computer running Siveillance Video Client, Video Client Player and Video Wall

Name	Description
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.
	Hardware acceleration with NVIDIA Graphics card requires 64-bit Microsoft® Windows® version

## Computer running Siveillance Video Web Client

Name	Description
Browser	Microsoft Edge Chromium 87
	Safari® 15
	Google Chrome™ 87
	Mozilla® Firefox® 83

## Device running Siveillance Video Mobile

Name	Description
Operating	Android 9.0 or higher
	iOS 13.0 or higher
Network	2G/3G
	(4G or WiFi)*

\*Required for using Direct Streaming

# 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