



# **Security Center System Requirements**

## **Guide 5.12**

Document last updated: January 31, 2025

# Legal notices

---

©2025 Genetec Inc. All rights reserved.

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Cloud Link Roadrunner™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Cloudlink™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, Streamvault Edge™, Synergis™, Valcri™, their respective logos, as well as the Mobius Strip Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

Patent pending. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Genetec Citigraf™, Genetec Clearance™, and other Genetec™ products are the subject of pending patent applications, and may be the subject of issued patents, in the United States and in other jurisdictions worldwide.

All specifications are subject to change without notice.

## Document information

Document title: Security Center System Requirements Guide 5.12

Original document number: EN.500.100-V5.12.2.0(2)

Document number: EN.500.100-V5.12.2.0(2)

Document update date: January 31, 2025

You can send your comments, corrections, and suggestions about this guide to [documentation@genetec.com](mailto:documentation@genetec.com).

# Contents

---

## Preface

Legal notices . . . . .	ii
-------------------------	----

## Chapter 1: Security Center System Requirements

Security Center system requirements . . . . .	2
Security Center 5.12 client workstation requirements . . . . .	3
Maximum number of cameras viewed per client type . . . . .	4
Security Center 5.12 server requirements . . . . .	6
Maximum number of cameras and readers per server type . . . . .	8
Adapted server requirements for Cloud Storage . . . . .	10
Network requirements for Cloud Storage . . . . .	11
Maximum number of Media Gateway camera streams . . . . .	12
System requirements for KiwiVision in Security Center 5.12 . . . . .	14
GPU support on the KiwiVision Analyzer role . . . . .	14
Maximum number of units supported in Unit Assistant role batch operations . . . . .	16
Security Center 5.12 software requirements . . . . .	18
Additional considerations for server specifications in Security Center 5.12 . . . . .	20
Virtualization design guidelines for Security Center . . . . .	21

## Chapter 2: AutoVu LPR System Requirements

Security Center 5.12 AutoVu ALPR server requirements . . . . .	24
----------------------------------------------------------------	----

## Chapter 3: Genetec Mobile System Requirements

Security Center 5.12 streaming capacities for Genetec Mobile . . . . .	26
------------------------------------------------------------------------	----

## Chapter 4: Security Center Web Client System Requirements

Security Center 5.12 streaming capacities for Web Client . . . . .	29
Software requirements for Security Center 5.12 Web Client . . . . .	31
Browser speeds for Security Center 5.12 Web Client . . . . .	32
Number of Web Client user connections per Security Center 5.12 Web Client Server . . . . .	33

## Chapter 5: Genetec Web App System Requirements

Streaming capacities for the Genetec Web App . . . . .	35
Software requirements for the Genetec Web App . . . . .	37
Browser speeds for Security Center 5.12 Genetec Web App . . . . .	38
Number of Genetec Web App user connections per Security Center 5.12 Web App Server . . . . .	39

Where to find product information . . . . .	40
---------------------------------------------	----

Technical support . . . . .	41
-----------------------------	----

# Security Center System Requirements

This section includes the following topics:

- ["Security Center system requirements"](#) on page 2
- ["Security Center 5.12 client workstation requirements"](#) on page 3
- ["Maximum number of cameras viewed per client type"](#) on page 4
- ["Security Center 5.12 server requirements"](#) on page 6
- ["Maximum number of cameras and readers per server type"](#) on page 8
- ["Network requirements for Cloud Storage "](#) on page 11
- ["Maximum number of Media Gateway camera streams"](#) on page 12
- ["System requirements for KiwiVision in Security Center 5.12"](#) on page 14
- ["Maximum number of units supported in Unit Assistant role batch operations"](#) on page 16
- ["Security Center 5.12 software requirements"](#) on page 18
- ["Additional considerations for server specifications in Security Center 5.12"](#) on page 20
- ["Virtualization design guidelines for Security Center"](#) on page 21

## Security Center system requirements

---

For Security Center to perform as expected, the following hardware and software components are required.

To determine which configuration is best suited for your application, contact our Sales Engineering team at [salesengineering@genetec.com](mailto:salesengineering@genetec.com).

**IMPORTANT:** Security Center is not a life safety platform. If you intend to integrate any life safety component with your Security Center instance, you must follow all applicable laws and regulations, including any industry-specific codes. Ensure that your deployment and use of Security Center and any such life safety component complies with the rules and standards applicable in your jurisdiction, environment, and industry. Consult professionals in life safety compliance as required.

## Security Center 5.12 client workstation requirements

To ensure optimal performance for your needs, client workstations must meet or exceed the minimum, recommended, or high-performance profile for Security Center 5.12.

**IMPORTANT:** The recommended system requirements for Security Center 5.12 refer to newer generation hardware. Upgrading from Security Center 5.11 with older hardware doesn't impact performance when using the same feature set.

The requirements for Security Center 5.12 client workstations are as follows:

Client profile	Client characteristics
<b>Minimum</b>	<ul style="list-style-type: none"> <li>Intel® Core™ 2 X6800 @ 2.93 GHz</li> <li>2 GB of RAM or better</li> <li>32-bit operating system</li> <li>80 GB hard drive for OS and Security Center applications, with a minimum of 6 GB of free disk space to install the Security Center client application</li> <li>256 MB PCI-Express x16 video card</li> <li>1280 x 1024 or higher screen resolution with 96 dpi</li> <li>100 Mbps Ethernet network interface card</li> </ul>
<b>Recommended</b>	<ul style="list-style-type: none"> <li>9<sup>th</sup> Generation Intel® Core™ i7-9700 or better</li> <li>8 GB of RAM or better</li> <li>64-bit operating system</li> <li>120 GB Solid-State Drive for OS and Security Center applications, with a minimum of 6 GB of free disk space to install the Security Center client application</li> <li>GbE network interface card</li> <li>NVIDIA® GTX 1660 video card or newer equivalent</li> </ul>
<b>High-performance</b> <i>Video intensive configuration</i>	<ul style="list-style-type: none"> <li>9<sup>th</sup> Generation Intel® Core™ i9-9940X or better</li> <li>16 GB of RAM or better</li> <li>64-bit operating system</li> <li>240 GB Solid-State Drive for OS and Security Center applications, with a minimum of 6 GB of free disk space to install the Security Center client application</li> <li>GbE network interface card</li> <li>Dual NVIDIA® GeForce® RTX 2080 video card</li> </ul>

## Maximum number of cameras viewed per client type

To ensure optimal performance, do not exceed the maximum number of cameras that can be viewed on each client workstation type in Security Center 5.12.

The maximum number of camera streams supported by each client workstation profile is as follows:

Decoding benchmark H.264 / HEVC (H.265)				
Resolution @ 30fps	VGA 640 x 480	HD 1280 x 720	Full HD 1920 x 1080	Ultra HD 3840 x 2160
Average bit rate per camera H.264/H.265	1 Mbps	2.3 Mbps	5.5 Mbps	20 Mbps
Minimum	6 / 0	2 / 0	1 / 0	0 / 0
Recommended <sup>1</sup>	53 / 52	36 / 34	25 / 23	6 / 8
High-performance <sup>1</sup>	125 / 126	78 / 73	53 / 59	17 / 28

<sup>1</sup> Maximum number of streams at full capacity (85% CPU and GPU utilization) in a static environment (video wall). Reducing the number of streams is required based on the use of other features such as visual tracking or guard tours.

**NOTE:** In an active operator scenario, the maximum number of decodings should not exceed 95% of these numbers. The numbers in the previous table are obtained under the following conditions:

- Full HD (1080p) monitors are used for all tests.
- Two monitors are used when more than 64 tiles are required.
- Low-motion video scenes are used on all cameras.
- The rendered frame rate could be reduced to a minimum of 10 fps.

### GPU considerations

- NVIDIA<sup>®</sup> card with CUDA compute capability 5.0 or higher is recommended.
- NVIDIA<sup>®</sup> -SLI™ bridge not supported.
- If your Intel<sup>®</sup> processors support Intel<sup>®</sup> Quick Sync Video, this technology can also be used provided the monitor is plugged into the motherboard. Laptops can also use Quick Sync Video.
- Two or more graphics cards can be used to support different monitors individually. To have the video decoding done on the card, at least one monitor must be connected to each card.
- Activating hardware acceleration can generate a slight video decoding delay.

### Encryption impact on workstation performance

Video encryption can increase the CPU usage by up to 40% when viewing low-resolution video (CIF). As the resolution of the video increases, the impact is less noticeable because it takes more processing power to decode video than to decrypt video. The impact on performance becomes negligible for HD and Ultra-HD video.

## Watermark impact on workstation performance

Video watermarks are rendered by the client workstation. This extra load reduces the maximum number of live and playback video streams that can be displayed simultaneously. On average, the maximum number of tiles that can be displayed when hardware acceleration is enabled is reduced by 10%. This reduction reaches 30% on machines without hardware acceleration. The performance impact increases with the video resolution.



## Security Center 5.12 server requirements

To ensure optimal performance for your needs, servers must meet or exceed the minimum, recommended, or high-performance profile for a Security Center 5.12 Directory, Archiver, Access Manager, and Media Gateway.

The requirements for Security Center 5.12 servers are as follows:

Server profile	Server characteristics
<b>Minimum<sup>1</sup></b>	<ul style="list-style-type: none"> <li>Intel® Core™ 2 Duo E6850 3.0 GHz or better</li> <li>4 GB of RAM or better</li> <li>80 GB hard drive for OS and Security Center applications, with a minimum of 15 GB of free disk space to install a Security Center server</li> <li>Separate storage disk from OS primary disk for Archiver storage</li> <li>32-bit operating system</li> <li>100/1000 Mbps Ethernet network interface card</li> <li>Standard SVGA video card</li> </ul>
<b>Recommended (Up to 300 Mbps)</b>	<ul style="list-style-type: none"> <li>Intel® Xeon® Silver 4210 2.2 GHz or better</li> <li>16 GB of RAM or better</li> <li>64-bit operating system</li> <li>80 GB SATA II hard drive or better for OS, Security Center applications, and Archiver database storage (when using a local Archiver database), with a minimum of 15 GB of free disk space to install a Security Center server</li> <li>GbE network interface card</li> <li>Standard SVGA video card</li> </ul>
<b>Above 300 Mbps and up to 500 Mbps</b>	<ul style="list-style-type: none"> <li>Intel® Xeon® Silver 4210 2.2 GHz or better</li> <li>16 GB of RAM or better</li> <li>64-bit operating system</li> <li>80 GB SATA II hard drive or better for OS and Security Center applications, with a minimum of 15 GB of free disk space to install a Security Center server</li> <li>Dedicated video disks of at least 12 drives in RAID 5 or 6</li> <li>GbE network interface card</li> <li>Standard SVGA video card</li> <li>Pre-event recording values set to the default value of 4 seconds<sup>2</sup></li> <li>Playback or Archive transfer should not exceed 100 Mbps<sup>3</sup></li> </ul>
<b>Above 250,000 and up to 600,000 cardholders</b>	<ul style="list-style-type: none"> <li>Intel® Xeon® E5-2620 v4 2.10 GHz or better</li> <li>32 GB of RAM or better</li> <li>64-bit operating system</li> <li>80 GB SATA II hard drive or better for OS and Security Center applications, with a minimum of 15 GB of free disk space to install a Security Center server</li> <li>GbE network interface card</li> <li>Standard SVGA video card</li> </ul>

Server profile	Server characteristics
<b>High-performance<sup>4</sup></b> <i>Video intensive configuration</i>	<ul style="list-style-type: none"> <li>• <b>Streamvault™ rackmount appliance</b></li> </ul> <p>The Streamvault 2000, 4000, and 7000 Series offer high performance for video-intensive archiving. Starting from 500 cameras or 500 Mbps, and 150 Mbps of video redirection, up to 1,000 cameras or 2,000 Mbps, and 400 Mbps of video redirection.</p> <p>To find the right Streamvault model for your project, contact Genetec™ Sales at <a href="mailto:sales@genetec.com">sales@genetec.com</a>, or call 1-866-684-8006 (option #2).</p>
<b>Media transcoding applications</b>	<ul style="list-style-type: none"> <li>• Intel® Core™ i7-9700K, Intel® Xeon® E-2186G, or better</li> <li>• CPU with support for Intel® Quick Sync™ Video</li> <li>• 16 GB of RAM or better</li> <li>• 64-bit operating system</li> <li>• 80 GB SATA II hard driver or better for OS and Security Center applications</li> <li>• NVIDIA® RTX A2000 video card</li> </ul>

<sup>1</sup> For the minimum server profile, the *Maximum server memory* of SQL Server must be limited to 512 MB.

<sup>2</sup> To increase this value, you must proportionally reduce the Archiver's maximum bit rate.

<sup>3</sup> When playback exceeds 100 Mbps, subtract the equivalent bandwidth from the maximum archiving bandwidth.

<sup>4</sup> The intended throughput requires specific hardware and software configurations.

## Maximum number of cameras and readers per server type

To ensure optimal performance, do not exceed the maximum number of cameras and readers supported by each server type and server profile in Security Center 5.12.

The maximum changes depending on the server profile you are using with your server type. The specifications for the *Minimum* and *Recommended* server profiles are listed in [Security Center 5.12 server requirements](#) on page 6.

Server type	Maximum number of cameras or readers	
	With Minimum server profile	With Recommended server profile
<b>Directory &amp; Archiver</b> (Video only)	50 cameras or 50 Mbps	100 cameras or 200 Mbps
<b>Standalone Archiver</b> (Video only)	75 cameras or 75 Mbps	300 cameras or 500 Mbps <sup>1</sup>
<b>Standalone Redirector</b> (Video only)	50 cameras or 50 Mbps	475 cameras or 475 Mbps <sup>2</sup>
<b>Directory &amp; Access Manager</b> (Access control only)	<ul style="list-style-type: none"> <li>One of the following for readers:               <ul style="list-style-type: none"> <li>Up to 100 HID Edge readers or 200 V2000 readers</li> <li>Up to 150 readers on HID V1000 units</li> <li>Up to 150 readers on Axis Powered by Genetec units</li> <li>Up to 150 readers on Synergis™ Cloud Link units</li> <li>Up to 400 readers on Cloud Link Roadrunner™ units</li> </ul> </li> <li>Readers spread across 10 HID V1000/Synergis Cloud Link or 100 Axis Powered by Genetec/Cloud Link Roadrunner units</li> <li>10,000 cardholders</li> </ul>	<ul style="list-style-type: none"> <li>One of the following for readers:               <ul style="list-style-type: none"> <li>Up to 300 HID Edge readers or 600 V2000 readers</li> <li>Up to 1,000 readers on HID V1000 units</li> <li>Up to 1,024 readers on Axis Powered by Genetec units</li> <li>Up to 1,024 readers on Synergis Cloud Link units</li> <li>Up to 4,000 readers on Cloud Link Roadrunner units</li> </ul> </li> <li>Readers spread across 100 HID V1000/Synergis Cloud Link or 1,000 Axis Powered by Genetec/Cloud Link Roadrunner units</li> <li>250,000 cardholders</li> </ul>

Server type	Maximum number of cameras or readers	
	With Minimum server profile	With Recommended server profile
<b>Standalone Access Manager</b> (Access control only)	<ul style="list-style-type: none"> <li>One of the following for readers:               <ul style="list-style-type: none"> <li>Up to 400 HID Edge readers or 800 V2000 readers</li> <li>Up to 400 readers on HID V1000 units</li> <li>Up to 400 readers on Axis Powered by Genetec units</li> <li>Up to 400 readers on Synergis Cloud Link units</li> <li>Up to 800 readers on Cloud Link Roadrunner units</li> </ul> </li> <li>Readers spread across 20 HID V1000/Synergis Cloud Link or 200 Axis Powered by Genetec/Cloud Link Roadrunner units</li> <li>100,000 cardholders</li> </ul>	<ul style="list-style-type: none"> <li>One of the following for readers:               <ul style="list-style-type: none"> <li>Up to 700 HID Edge readers or 1400 V2000 readers</li> <li>Up to 2,000 readers on HID V1000 units</li> <li>Up to 2,048 readers on Axis Powered by Genetec units</li> <li>Up to 2,048 readers on Synergis Cloud Link units</li> <li>Up to 4,000 readers on Cloud Link Roadrunner units</li> </ul> </li> <li>Readers spread across 100 HID V1000/Synergis Cloud Link or 1,000 Axis Powered by Genetec/Cloud Link Roadrunner units</li> <li>250,000 cardholders</li> </ul>
<b>Directory, Archiver &amp; Access Manager<sup>3</sup></b> (Unified)	<ul style="list-style-type: none"> <li>Maximum of 50 cameras or 50 Mbps and 64 readers</li> <li>Readers spread across 5 HID V1000/Synergis Cloud Link units</li> <li>5,000 cardholders</li> </ul>	<ul style="list-style-type: none"> <li>Maximum of 100 cameras or 200 Mbps and 200 readers</li> <li>Readers spread across 40 HID V1000/Synergis Cloud Link units</li> <li>40,000 cardholders</li> </ul>

<sup>1</sup> For high-performance Archivers (500 cameras and up), see [Security Center 5.12 server requirements](#) on page 6.

<sup>2</sup> For high-performance Redirectors (475 cameras or 475 Mbps and up), see [Security Center 5.12 server requirements](#) on page 6.

<sup>3</sup> If the server is configured with the minimum requirements, SQL Server must be hosted on a separate machine.

## Support for over 250,000 cardholders

To support 250,000–600,000 cardholders in your system, the Directory and Access Manager roles must both be standalone. As a minimum requirement, each server hosting these roles must meet the specifications of the [Above 250,000 and up to 600,000 cardholders](#) server profile.

## Fusion Stream Encryption impact on Archiver performance

The first encryption certificate enabled on the Archiver reduces the capacity of the Archiver by 30%. Each additional encryption certificate applied to all cameras further reduces the Archiver capacity by 4%.

For example, on an Archiver that supports 300 cameras without encryption:

Number of certificates enabled	Number of supported cameras
0 encryption certificates (no encryption)	300 cameras
1 encryption certificate	210 cameras

Number of certificates enabled	Number of supported cameras
5 encryption certificates	178 cameras
10 encryption certificates	145 cameras
20 encryption certificates	96 cameras

**BEST PRACTICE:** Do not exceed 20 encryption certificates per Archiver.

For information, see [What is fusion stream encryption?](#) on the TechDoc Hub.

## Adapted server requirements for Cloud Storage

Your Security Center system must comply with the minimum performance requirements to support the video encryption required by Cloud Storage.

All video archives are encrypted before they are uploaded to the cloud. Because encryption requires more system resources, the server specifications must be adjusted as shown:

Server specifications	Directory and Archiver	Standalone Archiver
Minimum	20 cameras or 40 Mbps	50 cameras or 65 Mbps
Recommended	30 cameras or 65 Mbps	100 cameras or 200 Mbps
High-performance	N/A	See high-performance server profile.

## Network requirements for Cloud Storage

To ensure that Cloud Storage is constantly available, and accommodates network outages and variations in video recording throughput, your network must meet minimum internet uplink throughput requirements.

Item	Requirement
Connection type	Internet
Uplink throughput to the cloud	At least 30% higher than video recording throughput
Network availability	Minimum 99.9% guaranteed (SLA) by the internet service provider
Network latency	Less than 150 milliseconds with one Azure data center: <a href="http://www.azure-speed.com/Azure/Latency">http://www.azure-speed.com/Azure/Latency</a>

Your network must provide a guaranteed uplink that is 30% greater than the video throughput recorded by all *Archiver* roles configured on the system.

### Example

- If your system has one Archiver that records 100 Mbps of video, your network must provide a guaranteed uplink to the cloud of at least 130 Mbps.
- If your system has two Archivers that record 100 Mbps of video each, your network must provide a guaranteed uplink of at least 260 Mbps.

Cloud Storage uploads video archives using HTTPS as fast as the uplink allows. If you need more than 1 Gbps of throughput per system, contact Genetec Inc.

## Maximum number of Media Gateway camera streams

To ensure optimal performance, do not exceed the maximum number of camera streams supported by a Media Gateway in Security Center 5.12.

Media Gateway agents provide video streams to the Genetec™ Web App, Genetec™ Mobile app, and external RTSP connections. In some cases, video transcoding might be required. Video stream transcoding is determined by the requesting application as follows:

Requesting application	Transcoded?
External RTSP connections	Never
Genetec Mobile	Only when all the following conditions are met: <ul style="list-style-type: none"> <li>Media Gateway <b>Allow transcoding</b> setting is enabled for the Mobile Server role</li> <li>Mobile role allows the use of MJPEG streams</li> <li>Original stream is not H.264</li> </ul>
Genetec™ Web App	Only in the following situations: <ul style="list-style-type: none"> <li>Requesting user has video watermarking enabled</li> <li>Requesting user is streaming a PTZ camera and moving it (PTZ widget)</li> <li>Browser does not support H.264 decoding through Media Source Extensions</li> <li>Original stream is not H.264</li> </ul>
Security Center Web Client	Only in the following situations: <ul style="list-style-type: none"> <li>Requesting user has video watermarking enabled</li> <li>Requesting user is streaming a PTZ camera and moving it (PTZ widget)</li> <li>Browser does not support H.264 decoding through Media Source Extensions</li> <li>Original stream is not H.264</li> </ul>

The maximum number of camera streams supported by a dedicated Media Gateway server in Security Center 5.12 is as follows:

Performance without transcoding				
H.264				
Resolution @30fps	VGA 640 x 480	HD 1280 x 720	Full HD 1920 x 1080	Ultra HD 3840 x 2160
Average bit rate per camera	1 Mbps	2.3 Mbps	5.5 Mbps	20 Mbps
Recommended	200 streams / ~220 Mbps	170 streams / ~350 Mbps	100 streams / ~600 Mbps	35 streams / ~0.85 Gbps
High-performance	340 streams / ~370 Mbps	300 streams / ~600 Mbps	175 streams / ~1 Gbps	60 streams / ~1.2 Gbps

Performance with transcoding H.264/H.265				
Input Resolution @30fps	VGA 640 x 480	HD 1280 x 720	Full HD 1920 x 1080	Ultra HD 3840 x 2160
Average bit rate per camera	1 Mbps	2.3 Mbps	5.5 Mbps	20 Mbps
Recommended	45 streams, 50 Mbps / 39 streams, 43 Mbps	30 streams, 60 Mbps / 15 streams, 30 Mbps	16 streams, 100 Mbps / 6 streams, 12 Mbps	6 streams, 120 Mbps / 1 streams, 20 Mbps
Media transcoding applications server	55 streams, 60 Mbps / 65 streams, 70 Mbps	50 streams, 100 Mbps / 50 streams, 100 Mbps	26 streams, 160 Mbps / 26 streams, 160 Mbps	7 streams, 140 Mbps / 8 streams, 160 Mbps

**NOTE:** Bitrate is for input streams only. Output resolution is VGA.

## Considerations

- Video watermarking requires extra processing of transcoded video frames. If watermarking is applied to all streams, the maximum number of Media Gateway camera streams is reduced by 30%.
- There is a hard limit of around 500 connections.
- The values in the table are obtained with 30 fps.
- If the frame rate is reduced and the throughput remains under the maximum values in the table, then the number of connections can be increased linearly.
- When transcoding, output is resized to resolutions of 640 x 480 (VGA) or less, maintaining the aspect ratio.

**CAUTION:** Do not host Media Gateway on the same server as an Archiver. The Media Gateway role can use significant processing power. High CPU usage on the Archiver server can result in *Archiving queue full* situations that might lead to data loss.



# System requirements for KiwiVision in Security Center 5.12

To ensure that your KiwiVision™ system performs as expected, the following hardware and software components are required.

Due to typically high-performance requirements, using virtual machines isn't recommended.

## Security video analytics and People Counter modules

Before activating KiwiVision™ Security video analytics, make sure that your system can handle the additional load. Running video analytics with insufficient resources can negatively impact performance or can cause system failure. Your system should meet the following requirements:

- The KiwiVision plugin must be installed on a server and on client workstations that run a 64-bit operating system, and meet the recommended hardware and software specifications. See [Security Center 5.12 server requirements](#) on page 6 and [Security Center 5.12 software requirements](#) on page 18 for more information.

**NOTE:** A 32-bit operating system is sufficient for client workstations that only run Security Desk.

- Every server running a KiwiVision Manager, KiwiVision Analyzer, or Config Tool with which you want to configure analytics requires an AVX compatible processor.

**NOTE:** An AVX compatible processor isn't required for workstations that only run Security Desk.

## Privacy Protector module

**NOTE:** Do not host Privacy Protector™ on the same server as an Archiver. The Privacy Protector role can use significant processing power. When CPU usage on the Archiver server is high, *Archiving queue full* situations can occur and data can be lost.

For the best performance, use NVIDIA® Quadro® video cards. Alternatively, you can also use an Intel® CPU (Quick Sync chip set) that supports Intel® Quick Sync Video.

## Requirement calculators

- **For all KiwiVision modules:** Use the [KiwiVision™ Hardware Calculator](#) to help you calculate the number of machines required for your KiwiVision deployment. The calculator accounts your intended number of cameras and types of analytics.
- **For KiwiVision:** Use the [KiwiVision™ Camera Requirements Calculator](#) to help you with the following:
  - To determine how many cameras you need to cover the area you want to monitor, calculate the maximum distance from which cameras can detect objects.
  - To meet the camera requirements for your KiwiVision deployment, verify whether your existing camera setup needs to be modified.

## GPU support on the KiwiVision Analyzer role

This section lists GPU support considerations for the KiwiVision™ Analyzer role in Security Center 5.12.

Note the following considerations:

- Running people-counting analytics on a GPU helps reduce CPU usage.
- GPU support is only available for the Tailgating detection and People counting scenarios.
- GPU support is enabled on KiwiVision Analyzer roles by default, but a warning is displayed until the GPU Pack is installed.
- A video card (Maxwell, Pascal, Volta, Turing, or Ampere) with one of the following CUDA compute capabilities is required: 5.0, 5.2, 5.3, 6.0, 6.2, 7.0, 7.2, 7.5, 8.0, 8.6.
- The latest official graphics card driver from Nvidia must be installed.

- A minimum of 4 GB of video memory is required.
- On each server hosting a KiwiVision Analyzer role that you want to support GPU, you must install the KiwiVision Analyzer GPU Pack that corresponds to your version of the KiwiVision video analytics plugin.
- In the properties of each KiwiVision Analyzer role that you want to support GPU, you must enable GPU support.

## Maximum number of units supported in Unit Assistant role batch operations

To ensure optimal performance, do not exceed the maximum number of video and access control units supported in Security Center 5.12 Unit Assistant role (UAR) batch operations.

Some operations, like password change and certificate updates for a camera or an access control unit, require the unit to be reconnected. Be sure to schedule these operations during non-critical periods.

**IMPORTANT:** Monitor the server CPU usage if normal usage is already high to ensure that UAR operation does not introduce undesirable impacts.

The maximum number of units supported by each server type in Security Center 5.9.1.0 and later is as follows:

Server Type	Recommended		High-performance	
Directory & UAR	<b>5.11 and 5.12</b> (Passwords and certificates)		<b>5.11 and 5.12</b> (Passwords and certificates)	
	<b>Passwords</b>	<b>Certificates</b>	<b>Passwords</b>	<b>Certificates</b>
	<ul style="list-style-type: none"> <li>Batch of 10,000 units</li> <li>CPU usage increased over 80% during operation</li> <li>No impact on system</li> </ul>	Not tested. The numbers are expected to be similar to those of high-performance servers.	<ul style="list-style-type: none"> <li>Batch of 10,000 units</li> <li>Low CPU increase</li> <li>No impact on system</li> </ul>	<b>Video:</b> <ul style="list-style-type: none"> <li>Batch of 1,000 units</li> <li>Low CPU increase</li> <li>No impact on system</li> </ul> <b>Access control:</b> <ul style="list-style-type: none"> <li>Batch of 100 units</li> <li>Low CPU increase</li> <li>No impact on system</li> </ul>
	<b>5.9.2.0 to 5.10.4.0</b> (Video and access control passwords)		<b>5.9.2.0 to 5.10.4.0</b> (Video and access control passwords)	
	<ul style="list-style-type: none"> <li>Batch of 3,000 units</li> <li>CPU usage increased over 80% during operation</li> <li>No impact on system</li> </ul>		<ul style="list-style-type: none"> <li>Batch of 7,000 units</li> <li>Low CPU increase</li> <li>No impact on system</li> </ul>	
	<b>5.9.1.0</b> (Video passwords only)		<b>5.9.1.0</b> (Video passwords only)	

Server Type	Recommended	High-performance
	<ul style="list-style-type: none"> <li>• Batch of 1,000 units</li> <li>• CPU usage increased over 80% during operation</li> <li>• No impact on system</li> </ul>	<ul style="list-style-type: none"> <li>• Batch of 1,000 units</li> <li>• Low CPU increase</li> <li>• No impact on system</li> </ul>
<b>Archiver &amp; UAR Agents</b>	Same as maximum number of units recommended for Archivers	Same as maximum number of units recommended for Archivers

## Security Center 5.12 software requirements

To ensure that your system runs optimally, it is important to know the software requirements for Security Center 5.12.

**NOTE:** If you plan on running antivirus software on any machine running Security Center, you must also configure the required exceptions. For more information, see [Best practices for configuring antivirus software for Security Center](#).

The requirements for Security Center 5.12 software are as follows:

Category	Supported software
<b>Operating systems</b>	<ul style="list-style-type: none"> <li>• Microsoft Windows 10 Pro version 1607 and later<sup>1</sup></li> <li>• Microsoft Windows 10 Enterprise LTSB version 1607 and later<sup>1</sup></li> <li>• Microsoft Windows 11 Pro/Enterprise<sup>3,4</sup></li> <li>• Microsoft Windows Server 2016<sup>2,3</sup></li> <li>• Microsoft Windows Server 2019<sup>2,3</sup></li> <li>• Microsoft Windows Server 2022<sup>2,3,6</sup></li> </ul>
<b>Database Engines<sup>5</sup></b>	<ul style="list-style-type: none"> <li>• SQL Server 2014 Express/Standard/Enterprise</li> <li>• SQL Server 2016 Express/Standard/Enterprise<sup>3</sup></li> <li>• SQL Server 2017 Express/Standard/Enterprise<sup>3</sup></li> <li>• SQL Server 2019 Express/Standard/Enterprise<sup>3</sup></li> <li>• SQL Server 2022 Express/Standard/Enterprise<sup>3</sup></li> </ul>
<b>Browsers for Security Center Server Admin</b>	<ul style="list-style-type: none"> <li>• Microsoft Edge</li> <li>• Chrome</li> <li>• Firefox</li> <li>• Safari</li> </ul>
<b>Browsers for Synergis™ Appliance Portal</b>	<ul style="list-style-type: none"> <li>• Microsoft Edge</li> <li>• Chrome</li> </ul>
<b>Browsers for Security Center Web Client<sup>7</sup></b>	<ul style="list-style-type: none"> <li>• Microsoft Edge</li> <li>• Chrome</li> <li>• Firefox</li> <li>• Safari (desktop version)</li> </ul>
<b>Browsers for the Genetec™ Web App<sup>7</sup></b>	<ul style="list-style-type: none"> <li>• Microsoft Edge</li> <li>• Chrome</li> <li>• Firefox</li> <li>• Safari (desktop version)</li> </ul>

Category	Supported software
<b>Browser for AutoVu™ ALPR AutoVu Cloudrunner™ integration<sup>7</sup></b>	<ul style="list-style-type: none"> <li>• Microsoft Edge</li> </ul>
<b>Virtualization (Server)</b>	<ul style="list-style-type: none"> <li>• VMware ESXi 7.x</li> <li>• VMware ESXi 8.x</li> <li>• Microsoft Hyper-V with Windows Server 2016/2019/2022</li> </ul>

<sup>1</sup> Both 32-bit and 64-bit versions are supported.

<sup>2</sup> Only Standard, Enterprise, and Datacenter Editions are supported.

<sup>3</sup> Only 64-bit versions are supported.

<sup>4</sup> Microsoft Windows 11 Pro/Enterprise requires at least 4 GB of RAM for installation.

<sup>5</sup> For the minimum server profile, the *Maximum server memory* of SQL Server must be limited to 512 MB.

<sup>6</sup> Microsoft Windows Server 2022 is incompatible with the minimum server profile.

<sup>7</sup> We recommend that you keep your browser up to date.

## Additional considerations for server specifications in Security Center 5.12

---

To ensure your system runs optimally, there are additional things to consider for server specifications in Security Center 5.12.

Note the following additional considerations for server specifications in Security Center 5.12.

- When video streaming is not in multicast from the camera, the maximum throughput calculation must include camera streams being redirected by the Archiver.
- Software motion detection can reduce the maximum capacity by as much as 50%. When enabling motion detection, use hardware motion detection to ensure maximum capacity.
- Systems above 300 cameras, 1000 readers, or 300 HID Edge readers, must isolate the Directory on a dedicated server.
- A more powerful server than the recommended specification does not necessarily increase the maximum capacity.
- A virtual machine with the same specifications as its physical counterpart has 20% less capacity.
- A dedicated Network Interface Card (NIC) should be assigned per instance of the Archiver role or Access Manager role when using virtualization.
- VMware ESXi must be installed on a clean computer; that is, no operating system is installed on the computer.
- The Genetec™ Server service cannot be installed on the same machine as the domain controller.

# Virtualization design guidelines for Security Center

When designing a virtual environment for Security Center, follow these best practices to ensure that the system is properly dimensioned for your needs.

**IMPORTANT:** Contact your Systems Engineer if your system does not follow the virtualization design guidelines.

Virtual machines have a small decrease in performance when compared to real hardware. The performance loss due to virtualization is typically under 20% of the overall machine performance, but can vary depending on the selected hardware and the hypervisor configuration. The following recommendations are based on internal testing and field experience to minimize the performance impact.

For more information about virtualization, refer to [Archiver Redundancy Performance in Security Center](#).

## Provisioning

- **Virtual Machine (VM):** Do not exceed six total VMs per host and a maximum of four video-intensive VMs per host (video-intensive VMs run Archiver, Auxiliary Archiver, Media Gateway, or Privacy Protector roles).  
Make sure that Security Center is installed on a dedicated host.
- **CPU:** Although hyperthreaded virtual cores can be used in a VM deployment, only the physical cores should be considered in the design when computing capacity.
- **Memory:** Assign at least 16 GB of RAM to each VM and keep 16 GB of RAM unallocated for the hypervisor. The total amount of memory allocated to the VMs and the hypervisor should not exceed the total amount of physical memory available from the host.
- **Storage:** Storage configurations depend on the hardware vendor's best practices and the system environment.

For the operating system:

- Install Microsoft Windows and Microsoft SQL databases on a dedicated, high-performance drive, usually on an SSD or a Storage Area Network (SAN) with SSD or hybrid storage.
- Do not use the OS drive for archived video.
- Make the OS partition at least 120 GB.

For archived video, configure Archiver video disks inside one of the following:

- A data store (VMDK or VHD)
- Raw Device Mapping (RDM) for fiber channel
- In-Guest iSCSI

**NOTE:** Other configurations might result in degraded performance.

- **Network:**
  - Send video traffic on a different VLAN from storage traffic.
  - Preferred configuration is at least one 40 GbE or 10 GbE network card for shared traffic (management, video, and storage) with a Virtual Switch. Otherwise, dedicate a 1 GbE network card per VM for video traffic.

**NOTE:** Alternate network configurations might result in multicast traffic being sent to all hosted VMs simultaneously. Depending on the host or its configuration, this might impact the overall performance.

## Security Center

- **Archiver:** When provisioning multiple archiving VMs on a host, do not exceed the following data transmission rates:
  - 300 Mbps for incoming and outgoing video on each VM.
  - 1200 Mbps for incoming video and outgoing playback on each host.



- **Directory:** Use static MAC addresses when installing a Directory on a VM. Changing this value invalidates the system license.

# AutoVu LPR System Requirements

This section includes the following topics:

- ["Security Center 5.12 AutoVu ALPR server requirements"](#) on page 24

## Security Center 5.12 AutoVu ALPR server requirements

To ensure that your system runs optimally, it is important to know the minimum, recommended, and high-performance requirements for a Security Center 5.12 AutoVu™ ALPR server.

The requirements for a Security Center 5.12 server hosting the ALPR Manager role are as follows:<sup>1</sup>

Server profile	Server characteristics
<b>Minimum<sup>2</sup></b>	<ul style="list-style-type: none"> <li>Intel® Core™ i5-3550 equivalent processor or better</li> <li>8 GB of RAM (minimum 4 GB dedicated to SQL Server)</li> <li>Separated storage disk from OS primary disk</li> <li>50 AutoVu camera units (fixed or mobile)<sup>4</sup></li> <li>SQL Server Express database server containing up to 6,000,000 ALPR Events (Reads and Hits combined)</li> <li>Maximum of 5 simultaneous user connections</li> </ul>
<b>AutoVu Recommended</b>	<ul style="list-style-type: none"> <li>Intel® Core™ i7-3820 equivalent processor or better</li> <li>16 GB of RAM (minimum 6 GB dedicated to SQL Server)</li> <li>Dedicated RAID5 storage with 4 enterprise grade disks or better</li> <li>100 AutoVu camera units (fixed or mobile)<sup>4</sup></li> <li>SQL Server Standard database server containing up to 25,000,000 ALPR Events (Reads and Hits combined)</li> <li>Maximum of 20 simultaneous user connections</li> </ul>
<b>AutoVu High performance</b>	<ul style="list-style-type: none"> <li>Intel® Xeon® E5-2620 v4 equivalent processor or better</li> <li>32 GB of RAM (minimum 8 GB dedicated to SQL Server)</li> <li>Dedicated RAID5 storage with at least 8 high-performance enterprise grade disks or better</li> <li>Up to 300 AutoVu camera units (fixed or mobile)<sup>3,4</sup></li> <li>SQL Server Standard database server containing up to 80,000,000 ALPR Events (Reads and Hits combined)</li> <li>Maximum of 80 simultaneous user connections</li> </ul>

<sup>1</sup> These requirements are for installation on a single server. For higher performance, you can distribute the load on several servers.

<sup>2</sup> For the minimum server profile, the *Maximum server memory* of SQL Server must be limited to 512 MB.

<sup>3</sup> Must be distributed between three ALPR Managers with a maximum of 100 AutoVu units per LPR Manager. The total number of AutoVu units on all ALPR Managers connected to the same Archiver cannot exceed 100 AutoVu units.

<sup>4</sup> A mobile AutoVu system can include up to 4 SharpZ3 camera units and up to 2 wheel imaging cameras.

# Genetec Mobile System Requirements

This section includes the following topics:

- ["Security Center 5.12 streaming capacities for Genetec Mobile"](#) on page 26

## Security Center 5.12 streaming capacities for Genetec Mobile

The number of video streams and amount of traffic that Security Center 5.12 can deliver vary depending on the camera stream settings, the Mobile Server role settings, and the performance of the server that hosts the Media Gateway and Mobile Server roles.

The Media Gateway role is used by Genetec™ Mobile, Security Center Web Client, and Genetec™ Web App to get transcoded video from Security Center. The Media Gateway role supports the Real Time Streaming Protocol (RTSP), which external applications can use to request raw video streams from Security Center.

The stream settings are configured in Config Tool. For more information, see the following topics:

- [Configuring Mobile Server roles](#)

You can configure different video settings for wireless network (WiFi) and cellular connections. Mobile Server always uses the wireless network connection when it is available. To configure these settings in Config Tool, open the *System* task and click the **Roles** view. Select **Mobile Server** > **Properties** > **Video** and click the **Video settings** icon (⚙️).

- [Configuring video streams of cameras](#)

The Mobile Server sends the video stream that most closely matches the stream requested by the Genetec™ Mobile app. This minimizes the transcoding work done by the Media Gateway.

The maximum number of streams supported for the Genetec Mobile app depends on what the Media Gateway supports. The stream format and video quality settings of the cameras also affect the supported number of streams. For more information, see [Maximum number of Media Gateway camera streams](#) on page 12.

The following sets of test results show the impact on the streaming capacity of transcoding to MJPEG. The results show the maximum number of video MJPEG streams, without diminished performance, for each server type and various streaming scenarios. In each scenario, the server hosts the Mobile Server and the Media Gateway roles, and the CPU usage is maintained between 75% and 80%.

### MJPEG streaming capacities on a recommended server

The following tests were conducted on a server with an Intel Xeon E5-1620 v3 Quad-Core Processor at 3.50 GHz with 16 GB RAM, running Windows 10 64-bit Enterprise Edition.

Source streams (H.264) @ 15 fps	Requested streams (MJPEG)	Max number of streams	Outbound network traffic	Outbound network traffic per stream
320 x 240 (0.2 Mbps)	320 x 240	75	63.0 Mbps	0.84 Mbps
640 x 480 (0.5 Mbps)	640 x 480	60	60.0 Mbps	1.00 Mbps
1280 x 720 (1.0 Mbps)	1280 x 720	40	45.8 Mbps	1.15 Mbps
640 x 480 (0.5 Mbps)	320 x 240	50	52.6 Mbps	1.05 Mbps
1280 x 720 (1.0 Mbps)	320 x 240	40	40.4 Mbps	1.01 Mbps
1280 x 720 (1.0 Mbps)	640 x 480	40	40.6 Mbps	1.02 Mbps
1920 x 1080 (3.0 Mbps)	320 x 240	20	22.0 Mbps	1.10 Mbps

## MJPEG streaming capacities on a high-performance server

The following tests were conducted on a server with two Intel Xeon Silver 4110 processors at 2.1 GHz with 32 GB RAM, running Windows Server 2016 64-bit Standard Edition. These specifications conform to the [high-performance server requirements](#).

Source streams (H.264) @ 15 fps	Requested streams (MJPEG)	Max number of streams	Outbound network traffic	Outbound network traffic per stream
320 x 240 (0.2 Mbps)	320 x 240	160	158.0 Mbps	0.98 Mbps
640 x 480 (0.5 Mbps)	640 x 480	110	139.0 Mbps	1.26 Mbps
1280 x 720 (1.0 Mbps)	1280 x 720	70	145.0 Mbps	2.07 Mbps
640 x 480 (0.5 Mbps)	320 x 240	90	161.4 Mbps	1.79 Mbps
1280 x 720 (1.0 Mbps)	320 x 240	80	60.0 Mbps	0.75 Mbps
1280 x 720 (1.0 Mbps)	640 x 480	80	70.0 Mbps	0.87 Mbps
1920 x 1080 (3.0 Mbps)	320 x 240	40	18.0 Mbps	0.45 Mbps

# Security Center Web Client System Requirements

This section includes the following topics:

- ["Security Center 5.12 streaming capacities for Web Client"](#) on page 29
- ["Software requirements for Security Center 5.12 Web Client"](#) on page 31
- ["Browser speeds for Security Center 5.12 Web Client"](#) on page 32
- ["Number of Web Client user connections per Security Center 5.12 Web Client Server"](#) on page 33

## Security Center 5.12 streaming capacities for Web Client

The number of video streams and amount of traffic that Security Center 5.12 can deliver vary depending on the camera stream settings, the Media Gateway role settings, the dimensions of the requested video, and the performance of the server that hosts the Media Gateway and Web Client Server roles.

The Media Gateway role is used by Genetec™ Mobile, Security Center Web Client, and Genetec™ Web App to get transcoded video from Security Center. The Media Gateway role supports the Real Time Streaming Protocol (RTSP), which external applications can use to request raw video streams from Security Center.

The stream settings are configured in Config Tool. For more information, see the following topics:

- [Configuring Media Gateway roles](#)
- [Configuring video streams of cameras](#)

The Web Client Server sends the video stream that best fit the size of the video tile in the Web Client requesting the video.

The following tests were conducted on a server with an Intel Xeon E5-2620 v4 Quad-Core Processor at 2.10 GHz with 16 GB RAM, running Windows 10 64 bit, the Web Client Server role, and the Media Gateway role.

### NOTE:

- In our tests, the Security Center Web Client streams MJPEG at 8 fps.
- The calculation for the transcoded outbound network traffic bit rate includes an additional 15% overhead, but also depends greatly on the content of the video (the encoder targets 80% quality factor). For example, if the table indicates a transcoded outbound network traffic bit rate of 65 Mbps, the calculation is as follows:

New bit rate (325 Kbps) x 180 streams = 58500 Kbps or 57 Mbps + 15% overhead = approximately 65 Mbps

- To save system resources, you can cap the transcoded resolution. For more information, see [Limiting Media Gateway connections](#).

### Security Center cameras configured to H.264 (320 x 240) 15 fps @ 250 Kbps

Requested dimensions	Max number of streams	Outbound network traffic	Outbound network traffic per stream
MJPEG (320 x 240)	180	65 Mbps	0.36 Mbps <sup>1</sup>
H.264 (320 x 240)	150	42 Mbps	0.28 Mbps

### Security Center cameras configured to H.264 (640 x 480) 15 fps @ 500 Kbps

Requested dimensions	Max number of streams	Outbound network traffic	Outbound network traffic per stream
MJPEG (320 x 240)	80	40 Mbps	0.5 Mbps <sup>1</sup>
MJPEG (640 x 480)	110	125 Mbps	1.14 Mbps <sup>1</sup>
H.264 (640 x 480)	150	90 Mbps	0.6 Mbps



**Security Center cameras configured to H.264 (1280 x 720) 15 fps @ 2.5 Mbps**

Requested dimensions	Max number of streams	Outbound network traffic	Outbound network traffic per stream
MJPEG (320 x 180)	45	30 Mbps	0.67 Mbps <sup>1</sup>
MJPEG (640 x 360)	40	60 Mbps	1.5 Mbps <sup>1</sup>
MJPEG (1280 x 720)	55	190 Mbps	3.45 Mbps <sup>1</sup>
H.264 (1280 x 720)	135	120 Mbps	0.89 Mbps

**Security Center cameras configured to H.264 (1920 x 1080) 15 fps @ 2.5 Mbps**

Requested dimensions	Max number of streams	Outbound network traffic	Outbound network traffic per stream
MJPEG (320 x 180)	23	12 Mbps	0.52 Mbps <sup>1</sup>
MJPEG (640 x 360)	20	28 Mbps	1.4 Mbps <sup>1</sup>
MJPEG (1280 x 720)	16	65 Mbps	4.1 Mbps <sup>1</sup>
MJPEG (1920 x 1080)	16	140 Mbps	8.75 Mbps <sup>1</sup>
H.264 (1920 x 1080)	60	260 Mbps	4.33 Mbps

<sup>1</sup> The Web Client Server automatically transcodes the video stream when required, which can result in a different bit rate than the original stream.

## Software requirements for Security Center 5.12 Web Client

Before using Web Client, familiarize yourself with the operating systems and browsers that are supported with Web Client.

The software requirements for Security Center 5.12 Web Client are the following:

Operating system	Supported Browsers
Microsoft Windows 10 Professional and Enterprise (32-bit or 64-bit)	<ul style="list-style-type: none"> <li>• Microsoft Edge for Windows 10</li> <li>• Google Chrome latest version</li> <li>• Mozilla Firefox latest version</li> </ul>
Microsoft Windows Server 2016 Standard Edition and R2 (32-bit or 64-bit)	<ul style="list-style-type: none"> <li>• Microsoft Edge for Windows 10</li> <li>• Google Chrome latest version</li> <li>• Mozilla Firefox latest version</li> </ul>
Microsoft Windows Server 2017 Standard Edition and R2 (32-bit or 64-bit)	
Microsoft Windows Server 2019 Standard Edition and R2 (32-bit or 64-bit)	
Microsoft Windows Server 2022 Standard Edition and R2 (32-bit or 64-bit)	
Mac OS X 10.9.1	Apple Safari (desktop version)

**NOTE:** If you are not seeing high-quality (H.264) video in your Firefox browser, make sure that H.264/avc3 on the media source extension is enabled.

**NOTE:** Apple Safari for iOS and Google Chrome for Android devices are not supported by Security Center 5.12 Web Client. To access Security Center videos and data from your smartphone, you should use Genetec™ Mobile.

## Browser speeds for Security Center 5.12 Web Client

How quickly video loads and PTZ cameras respond depends on many factors, including the decoding latency of your web browser. In addition, not all browsers support high-quality H.264 video. To ensure that your videos load in Web Client as quickly as possible, choose a browser that supports H.264 and that has the lowest latency.

Browser latency is the average amount of time that it takes a browser to decode and display a video frame.

The latency of a browser is just one of the factors that affects how close to real-time a live video plays; how quickly video loads in a tile when you play, rewind, fast forward and play in slow motion; and how responsive PTZ cameras are to commands. Other factors that affect the speed at which video loads include the processing power of your computer and the Security Center servers, and the latency of the network between you, the Security Center system, and the cameras.

Typically, most browsers decode MJPEG streams within 300 ms. However, only some browsers can decode H.264 streams, and the latency of these browsers varies.

The following table compares the time that it takes some common browsers to load H.264 video in a single tile of the Web Client *Monitoring* task.

Browser that supports H.264	Browser latency for H.264 stream
Google Chrome	300 ms
Mozilla Firefox	300 ms to 800 ms
<b>NOTE:</b> If you are not seeing high-quality (H.264) video in your Firefox browser, make sure that H.264/avc3 on the media source extension is enabled.	

Some browsers cannot decode H.264 video. If Web Client detects that your browser does not support H.264 streams, it displays the video anyway, but as a lower quality MJPEG stream. So, if you need to display high-quality video in Web Client, choose a web browser that supports H.264.

**NOTE:** Web Client always switches from H.264 to MJPEG in the following cases:

- When controlling a PTZ camera
- When playing video in slow motion, rewind, and fast forward.

## Number of Web Client user connections per Security Center 5.12 Web Client Server

For the best possible experience in Security Center Web Client 5.12, plan for the maximum number of simultaneous user connections and approximate amount of traffic.

### How many users can a Web Client Server serve?

As more streams are requested simultaneously, more load is placed on the server. If the server becomes overloaded, users can experience slow Web Client pages.

To plan how many Web Client Servers you need, determine the maximum expected amount of traffic during peak hours. The amount of traffic depends on the number of users that log on at the same time and the camera quality settings. Then choose the server hardware that best manages that load.

The following table shows examples of how many users can view a single video stream in Web Client at the same time. The results are based on tests performed in our lab on a server that meets the recommended hardware configuration.

User activity	Number of concurrent user connections	Camera video quality setting
Monitoring one live MJPEG (640 x 480) video	60	H.264 (640 x 480), 15 fps @ 500 Kbps
Monitoring one live H.264 (640 x 480) video	100	
Generating reports and managing cardholders only.	100	No cameras in system. Access control only.

### What is a user connection?

A user connection is any user account that logs on to Web Client. Even if 50 users log on using the same user account, there are 50 user connections.

### How can I increase the number of concurrent user connections?

To add more users to your system, you can do any of the following:

- Deploy high-performance server hardware.
- Reduce the video quality of cameras.
- Add more Web Client Servers.

# Genetec Web App System Requirements

This section includes the following topics:

- ["Streaming capacities for the Genetec Web App"](#) on page 35
- ["Software requirements for the Genetec Web App"](#) on page 37
- ["Browser speeds for Security Center 5.12 Genetec Web App"](#) on page 38
- ["Number of Genetec Web App user connections per Security Center 5.12 Web App Server"](#) on page 39

## Streaming capacities for the Genetec Web App

The number of video streams and amount of traffic that Security Center 5.12 can deliver vary depending on several factors. For example, the camera stream settings, the Media Gateway role settings, the video resolution, and the performance of the server that hosts the Web App Server role.

The Media Gateway role is used by Genetec™ Mobile, Security Center Web Client, and Genetec™ Web App to get transcoded video from Security Center. The Media Gateway role supports the Real Time Streaming Protocol (RTSP), which external applications can use to request raw video streams from Security Center.

The stream settings are configured in Config Tool. For more information, see the following topics:

- [Configuring Media Gateway roles](#)
- [Configuring video streams of cameras](#)

The Web App Server sends the video stream that best fits the size of the video tile in the Genetec™ Web App requesting the video.

### Security Center cameras configured to H.264 (320 x 240) 15 FPS @ 250 Kbps

Requested dimensions	Max number of streams	Outbound network traffic	Outbound network traffic per stream
MJPEG (320 x 240)	180	65 Mbps	0.36 Mbps <sup>1</sup>
H.264 (320 x 240)	150	42 Mbps	0.28 Mbps

### Security Center cameras configured to H.264 (640 x 480) 15 FPS @ 500 Kbps

Requested dimensions	Max number of streams	Outbound network traffic	Outbound network traffic per stream
MJPEG (320 x 240)	80	40 Mbps	0.5 Mbps <sup>1</sup>
MJPEG (640 x 480)	110	125 Mbps	1.14 Mbps <sup>1</sup>
H.264 (640 x 480)	150	90 Mbps	0.6 Mbps

### Security Center cameras configured to H.264 (1280 x 720) 15 FPS @ 2.5 Mbps

Requested dimensions	Max number of streams	Outbound network traffic	Outbound network traffic per stream
MJPEG (320 x 180)	45	30 Mbps	0.67 Mbps <sup>1</sup>
MJPEG (640 x 360)	40	60 Mbps	1.5 Mbps <sup>1</sup>
MJPEG (1280 x 720)	55	190 Mbps	3.45 Mbps <sup>1</sup>
H.264 (1280 x 720)	135	120 Mbps	0.89 Mbps

**Security Center cameras configured to H.264 (1920 x 1080) 15 FPS @ 2.5 Mbps**

Requested dimensions	Max number of streams	Outbound network traffic	Outbound network traffic per stream
MJPEG (320 x 180)	23	12 Mbps	0.52 Mbps <sup>1</sup>
MJPEG (640 x 360)	20	28 Mbps	1.4 Mbps <sup>1</sup>
MJPEG (1280 x 720)	16	65 Mbps	4.1 Mbps <sup>1</sup>
MJPEG (1920 x 1080)	16	140 Mbps	8.75 Mbps <sup>1</sup>
H.264 (1920 x 1080)	60	260 Mbps	4.33 Mbps

<sup>1</sup> The Web App Server automatically transcodes the video stream when required, which can result in a different bit rate than the original stream.

## Software requirements for the Genetec Web App

Before using the Genetec™ Web App, familiarize yourself with the operating systems and browsers that are supported.

The Genetec Web App has the following software requirements:

Operating system	Supported browsers
Microsoft Windows 10 Professional and Enterprise (32-bit or 64-bit)	<ul style="list-style-type: none"> <li>• Microsoft Edge latest version</li> <li>• Google Chrome latest version</li> <li>• Mozilla Firefox latest version</li> </ul>
Microsoft Windows 11 Professional and Enterprise (32-bit or 64-bit)	
Microsoft Windows Server 2016 Standard Edition and R2 (32-bit or 64-bit)	<ul style="list-style-type: none"> <li>• Microsoft Edge latest version</li> <li>• Google Chrome latest version</li> <li>• Mozilla Firefox latest version</li> </ul>
Microsoft Windows Server 2017 Standard Edition and R2 (32-bit or 64-bit)	
Microsoft Windows Server 2019 Standard Edition and R2 (32-bit or 64-bit)	
Microsoft Windows Server 2022 Standard Edition and R2 (32-bit or 64-bit)	
Mac OS	Apple Safari latest version

**NOTE:** If you are not seeing high-quality (H.264) video in your Firefox browser, make sure that H.264/avc3 on the media source extension is enabled.

**NOTE:** Apple Safari for iOS and Google Chrome for Android devices are not fully supported by the Genetec Web App. To access Security Center videos and data from your smartphone, use Genetec™ Mobile.



## Browser speeds for Security Center 5.12 Genetec Web App

The decoding latency of your web browser determines how quickly video loads and PTZ cameras respond to commands. To ensure that your videos load in the Genetec™ Web App as quickly as possible, choose a browser that supports H.264 and that has the lowest latency.

Latency is the amount of delay on a network or internet connection. It can affect the average time that it takes for a browser to decode and display video

Several factors affect video playback, video control in tiles, and responsiveness to PTZ commands::

- Browser latency
- Processing power of your workstation and servers
- Network latency between your workstations, Security Center system, and cameras

The following table compares how long it takes some common browsers to load H.264 video in a single tile of the Genetec Web App *Tiles* task.

Browser that supports H.264	Browser latency for H.264 stream
Google Chrome	300 ms
Mozilla Firefox	300 ms to 800 ms
<b>NOTE:</b> If you are not seeing high-quality (H.264) video in your Firefox browser, make sure that H.264/avc3 on the media source extension is enabled.	

If the Genetec Web App detects that your browser does not support H.264 streams, it displays the video as a lower quality MJPEG stream. If you need to display high-quality video, choose a web browser that supports H.264.

# Number of Genetec Web App user connections per Security Center 5.12 Web App Server

To plan an effective deployment with the Genetec™ Web App, it helps to know the number of users and the network traffic.

## How many users can a Web App Server serve?

As more streams are requested simultaneously, more load is placed on the server. If the server is overloaded, Genetec Web App pages become slow.

To plan how many web servers you need, choose the server hardware that best manages the load created by the following factors:

- The maximum number of users that log on at the same time.
- The maximum amount of traffic that is expected during peak hours.

The following table shows how many users can concurrently view a single video stream in the Genetec Web App based on the recommended hardware configuration.

User activity	Number of concurrent user connections	Camera video quality setting
Monitoring one live MJPEG (640 x 480) video	60	H.264 (640 x 480), 15 fps @ 500 Kbps
Monitoring one live H.264 (640 x 480) video	100	
Generating reports and managing cardholders only	100	No cameras in the system.

## What is a user connection?

A user connection is any user account that logs on to the Genetec Web App. Even if 50 users log on using the same user account, that is 50 user connections.

## How can I increase the number of concurrent user connections?

To add more users to your system, you can do any of the following:

- Deploy high-performance server hardware.
- Reduce the video quality of cameras.
- Add more web servers.

# Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the [TechDoc Hub](#).

Can't find what you are looking for? Contact [documentation@genetec.com](mailto:documentation@genetec.com).

- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explains how the product works and provide instructions on how to use the product features. To access the help, click **Help**, press F1, or tap the ? (question mark) in the different client applications.

# Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

To access the TechDoc Hub, log on to [Genetec Portal](#) and click [TechDoc Hub](#). Can't find what you're looking for? Contact [documentation@genetec.com](mailto:documentation@genetec.com).

- **Genetec Technical Assistance Center (GTAC):** Contacting GTAC is described in the [Genetec Advantage Description](#).

## Technical training

In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to <http://www.genetec.com/support/training/training-calendar>.

## Licensing

- For license activations or resets, contact GTAC at <https://portal.genetec.com/support>.
- For issues with license content or part numbers, or concerns about an order, contact Genetec Customer Service at [customerservice@genetec.com](mailto:customerservice@genetec.com), or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, contact Genetec Sales at [sales@genetec.com](mailto:sales@genetec.com), or call 1-866-684-8006 (option #2).

## Hardware product issues and defects

Contact GTAC at <https://portal.genetec.com/support> to address any issue regarding Genetec appliances or any hardware purchased through Genetec Inc.