



Security Center System Requirements

Guide 5.14

Document last updated: June 10, 2026

Legal notices

©2026 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 Cloudrunner™, AutoVu MLC™, Citywise™, Cloud Link Roadrunner™, Cloudrunner™, Cloudrunner SolarBoost™, Community Connect™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, Omnicast™, 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.

Genetec products, services, and innovations are protected by patents and other intellectual property rights in various jurisdictions, including the United States. For a detailed list of patents owned by Genetec Inc., visit www.genetec.com/patents.

All specifications are subject to change without notice.

Document information

Document title: Security Center System Requirements Guide 5.14

Original document number: EN.500.100-V5.14.1.0(1)

Document number: EN.500.100-V5.14.1.0(1)

Document update date: June 10, 2026

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

Contents

Preface

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

Chapter 1: Security Center System Requirements

Security Center 5.14 system requirements.	2
Client workstation requirements.	3
Maximum number of cameras viewed per client type.	4
Security Center 5.14 server requirements.	5
Server requirements for high-performance video.	5
Server requirements for high-performance access control.	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
Maximum number of units supported in Unit Assistant role batch operations.	14
Software requirements.	15
Additional considerations for server specifications.	17
Virtualization design guidelines for Security Center.	18

Chapter 2: AutoVu LPR System Requirements

Security Center 5.14 AutoVu ALPR server requirements.	22
---	----

Chapter 3: Genetec Mobile System Requirements

Security Center 5.14 streaming capacities for Genetec Mobile.	24
---	----

Chapter 4: Genetec Web App System Requirements

Streaming capacities for the Genetec Web App.	27
Software requirements for the Genetec Web App.	28
Browser speeds for Security Center 5.14 Genetec Web App.	29
Number of Genetec Web App user connections per Security Center 5.14 Web App Server.	30

Where to find product information	31
-----------------------------------	----

Technical support	32
-------------------	----

Security Center System Requirements

This section includes the following topics:

- ["Security Center 5.14 system requirements"](#) on page 2
- ["Client workstation requirements"](#) on page 3
- ["Maximum number of cameras viewed per client type"](#) on page 4
- ["Security Center 5.14 server requirements"](#) on page 5
- ["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
- ["Maximum number of units supported in Unit Assistant role batch operations"](#) on page 14
- ["Software requirements"](#) on page 15
- ["Additional considerations for server specifications"](#) on page 17
- ["Virtualization design guidelines for Security Center"](#) on page 18

Security Center 5.14 system requirements

For Security Center 5.14 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.

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 adhere to all applicable laws and regulations. Ensure that your deployment and use of Security Center and any such life safety component comply with your jurisdiction, environment, and industry standards. Consult professionals in life safety compliance as required.

Client workstation requirements

To ensure optimal performance, client workstations must meet or exceed the minimum, recommended, or high-performance profile for Security Center 5.14.

IMPORTANT: The recommended system requirements for Security Center 5.14 refer to newer-generation hardware. Upgrading from Security Center 5.13 with older hardware does not impact performance when using the same feature set.

The requirements for Security Center 5.14 client workstations are as follows:

Client profile	Client characteristics
Minimum	- Intel® Core™ i3-8100 3.6GHz Processor ¹ 8 GB of RAM (DDR4) 64-bit operating system (Windows 11) 128 GB SSD hard drive for OS and Security Center applications - Intel® Ethernet Connection I219-LM (GbE 1000/1000Mbps) network interface card 1920 x 1200 display resolution
Recommended	- Intel® Core™ Ultra 7 Processor 265K 32 GB RAM (DDR5) 64-bit operating system (Windows 11 Enterprise 25H2) 1 TB SSD hard drive for OS and Security Center applications - Intel® Ethernet Connection I219-LM (GbE 1000/1000Mbps) network interface card - NVIDIA® GeForce RTX 5060 Ti (16 GB) video card
High-performance <i>Video-intensive configuration</i>	- Intel® Xeon® w5-2465X Processor 3.10 GHz 64 GB RAM (DDR5) 64-bit operating system (Windows 11 Enterprise 25H2) 240 GB SATA SSD or better for OS and Security Center applications, with a minimum of 15 GB of free disk space to install a Security Center server - GbE network interface card - Dual NVIDIA® GeForce RTX 5070 Ti (16 GB) video card

¹ Supports Intel® Quick Sync Video

Maximum number of cameras viewed per client type

To ensure optimal performance, don't exceed the maximum number of cameras that can be viewed on each client workstation type in Security Center 5.14.

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

Decoding benchmark						
Resolution @ 30fps	Full HD – 1920 x 1080			Ultra HD – 3840 x 2160		
	H.264	HEVC (H.265)	AV1	H.264	HEVC (H.265)	AV1
Average bit rate per camera (Mbps)	4.8	3.2	3.1	19	13.4	12.7
Minimum	5	6	3	1	1	0
Recommended ¹	64	64	56	19	18	16
High-performance ¹	104	102	100	36	36	30

¹ This refers to the maximum number of streams at full capacity (85% CPU and GPU use) in a static environment (video wall). Reducing the number of streams is required based on an active operator scenario and the use of other features such as visual tracking and guard tours. For information about optimizing tile display when you're using a video wall, see [Optimizing multiple tile display](#).

NOTE: The decoding benchmark numbers are obtained using two 4K UHD monitors for all tests.

GPU considerations

- If your Intel® processors support Intel® Quick Sync Video, you can use this technology if the monitor is connected to the motherboard. Laptops can also use Quick Sync Video.
- Security Center supports NVIDIA graphics cards.
- You can use two or more graphics cards to support different monitors individually. To ensure that video decoding is performed on a specific cards, 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. 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 5.14 server requirements

To ensure optimal performance, servers must meet or exceed the minimum, recommended, or high-performance profile for Security Center 5.14 Directory, Archiver, Access Manager, and Media Gateway roles.

- To configure a dedicated high-performance server for archiving, see [Server requirements for high-performance video](#) on page 5.
- To configure a dedicated high-performance server for access control, see [Server requirements for high-performance access control](#) on page 6.
- If you plan to configure a virtual environment for Security Center, see [Virtualization design guidelines for Security Center](#) on page 18.

The requirements for Security Center 5.14 servers are as follows:

Server profile	Server characteristics
Minimum¹	• Intel® Core™ i5-8500 CPU 3.0 GHz or better • 8 GB of RAM or better • 64-bit operating system • 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 • 100/1000 Mbps Ethernet network interface card • Standard SVGA video card
Recommended	• Intel® Xeon® E-2434 3.4 GHz or better • 16 GB of RAM or better • 64-bit operating system • 240 GB SATA SSD or better for OS and Security Center applications, with a minimum of 15 GB of free disk space to install a Security Center server • GbE network interface card • Standard SVGA video card
High-performance²	• 2 Intel® Xeon® Silver 4416+ 2.0 GHz (40 cores total) • 64 GB of RAM or better • 64-bit operating system • 240 GB SATA SSD or better for OS and Security Center applications, with a minimum of 15 GB of free disk space to install a Security Center server • 10 GbE network interface card • Standard SVGA video card

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

² The intended throughput requires specific hardware and software configurations.

Server requirements for high-performance video

If you need a dedicated high-performance server for your video recording requirements, use one of these server profiles for your Security Center 5.14 Archiver role.

The requirements for Security Center 5.14 archiving servers are as follows:

NOTE: All specifications assume 5 Mbps streams. Smaller bit rates reduce performance.

Server profile	Server characteristics
Recommended (Up to 300 Mbps)	- Intel® Xeon® Silver 4210 2.2 GHz or better 16 GB of RAM or better 64-bit operating system 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 - GbE network interface card - Standard SVGA video card
Above 300 Mbps and up to 500 Mbps	- Intel® Xeon® Silver 4210 2.2 GHz or better 16 GB of RAM or better 64-bit operating system 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 - Dedicated video disks of at least 12 drives in RAID 5 or 6 - GbE network interface card - Standard SVGA video card - Pre-event recording values set to the default value of 4 seconds¹ - Playback or Archive transfer should not exceed 100 Mbps²
High-performance ³ <i>Video intensive configuration</i>	Streamvault™ rackmount appliance The Streamvault 2000, 4000, and 7000 Series offer high performance for video-intensive archiving, starting from 900 Mbps of total throughput, up to 4,135 Mbps of total throughput. To find the right Streamvault model for your project, contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).
Media transcoding applications	- Intel® Core™ i7-9700K, Intel® Xeon® E-2186G, or better - CPU with support for Intel® Quick Sync™ Video 16 GB of RAM or better 64-bit operating system 80 GB SATA II hard driver or better for OS and Security Center applications - NVIDIA® RTX A2000 video card

¹ All specifications with a RAID controller were derived with one RAID rebuild. Not having a RAID rebuild increases the maximum recording capability.

² Exceeding recommended playback volume reduces the recording capability.

³ The intended throughput requires specific hardware and software configurations.

Server requirements for high-performance access control

If you need a dedicated high-performance server for your access control requirements, use one of these server profiles for your Security Center 5.14 Access Manager role.

The requirements for Security Center 5.14 access control servers are as follows:

Cardholders	Server characteristics
Up to 250,000 cardholders	• Intel® Xeon® E-2434 3.4 GHz • 16 GB of RAM or better • 64-bit operating system • SSD for OS and Security Center applications, with a minimum of 15 GB of free disk space to install a Security Center server • 1 GbE network interface card
Up to 600,000 cardholders	• Intel® Xeon® E-2436 2.9 GHz • 32 GB of RAM or better • 64-bit operating system • SSD for OS and Security Center applications, with a minimum of 15 GB of free disk space to install a Security Center server • 1 GbE network interface card

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 5.14.

The maximum number of supported cameras changes depending on the server profile you're using with your server type. The specifications for the *Minimum* and *Recommended* server profiles are listed in [Security Center 5.14 server requirements](#) on page 5.

Server type	Maximum number of cameras or readers	
	With Minimum server profile	With Recommended server profile
Directory and Archiver (Video only)	50 cameras or 50 Mbps	100 cameras or 200 Mbps
Standalone Redirector (Video only)	50 cameras or 50 Mbps	475 cameras or 475 Mbps
Directory and Access Manager (Access control only)	- One of the following for readers: - Up to 100 HID Edge readers or 200 V2000 readers - Up to 150 readers on HID V1000 units - Up to 150 readers on Axis Powered by Genetec units - Up to 150 readers on Synergis™ Cloud Link units - Up to 400 readers on Cloud Link Roadrunner™ units - Readers spread across 10 HID V1000/Synergis Cloud Link or 100 Axis Powered by Genetec/Cloud Link Roadrunner units 10,000 cardholders	- One of the following for readers: - Up to 300 HID Edge readers or 600 V2000 readers - Up to 1,000 readers on HID V1000 units - Up to 1,024 readers on Axis Powered by Genetec units - Up to 1,024 readers on Synergis Cloud Link units - Up to 4,000 readers on Cloud Link Roadrunner units - Readers spread across 100 HID V1000/Synergis Cloud Link or 1,000 Axis Powered by Genetec/Cloud Link Roadrunner units 250,000 cardholders

Server type	Maximum number of cameras or readers	
	With Minimum server profile	With Recommended server profile
Standalone Access Manager (Access control only)	- One of the following for readers: - Up to 400 HID Edge readers or 800 V2000 readers - Up to 400 readers on HID V1000 units - Up to 400 readers on Axis Powered by Genetec units - Up to 400 readers on Synergis Cloud Link units - Up to 800 readers on Cloud Link Roadrunner units - Readers spread across 20 HID V1000/Synergis Cloud Link or 200 Axis Powered by Genetec/Cloud Link Roadrunner units 100,000 cardholders	- One of the following for readers: - Up to 700 HID Edge readers or 1,400 V2000 readers - Up to 2,000 readers on HID V1000 units - Up to 2,048 readers on Axis Powered by Genetec units - Up to 2,048 readers on Synergis Cloud Link units - Up to 4,000 readers on Cloud Link Roadrunner units - Readers spread across 100 HID V1000/Synergis Cloud Link or 1,000 Axis Powered by Genetec/Cloud Link Roadrunner units 250,000 cardholders
Directory, Archiver, and Access Manager¹ (Unified)	50 cameras or 50 Mbps 64 readers spread across 5 HID V1000/Synergis Cloud Link units. 5,000 cardholders	100 cameras or 200 Mbps 200 readers spread across 40 HID V1000/Synergis Cloud Link units. 40,000 cardholders

¹ 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 provided in [Server requirements for high-performance access control](#) on page 6.

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
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	Not applicable	See Server requirements for high-performance video on page 5.

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: http://www.azure.speed.com/Azure/Latency

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, don't exceed the maximum number of camera streams supported by a Media Gateway in Security Center 5.14.

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: - Media Gateway Allow transcoding setting is enabled for the Mobile Server role - Mobile role allows the use of MJPEG streams - Original stream isn't H.264
Genetec™ Web App	Only in the following situations: - Requesting user has video watermarking enabled - Requesting user is streaming a PTZ camera and moving it (PTZ widget) - Browser doesn't support H.264 decoding through Media Source Extensions - Original stream isn't H.264

The maximum number of camera streams supported by a dedicated Media Gateway server in Security Center 5.14 is as follows:

Performance without transcoding						
Resolution @ 30 FPS	Full HD – 1920 x 1080			Ultra HD – 3840 x 2160		
	H264	HEVC (H.265)	AV1	H264	HEVC (H.265)	AV1
Average bit rate per camera	4.76 Mbps	3.21 Mbps	3.06 Mbps	19 Mbps	13.35 Mbps	12.74 Mbps
Recommended	127 streams	153 streams	151 streams	50 streams	72 streams	66 streams
High-performance	170 streams	198 streams	184 streams	110 streams	129 streams	123 streams

NOTE: Bit rate 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's 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, the 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.

Maximum number of units supported in Unit Assistant role batch operations

To ensure optimal performance, don't exceed the maximum number of video and access control units supported in Security Center 5.14 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 doesn't introduce undesirable impacts.

The maximum number of units supported by each server type in Security Center 5.14 is as follows:

Server type	Recommended High-performance			
Directory & UAR	Passwords	Certificates	Passwords	Certificates
	- Batch of 10,000 units - CPU usage increased over 80% during operation - No impact on system	Not tested. The numbers are expected to be similar to those of high-performance servers.	- Batch of 10,000 units - Low CPU usage increase - No impact on system	Video: - Batch of 1,000 units - Low CPU usage increase - No impact on system Access control: - Batch of 100 units - Low CPU usage increase - No impact on system
Archiver and UAR Agents	Same as maximum number of units recommended for Archivers		Same as maximum number of units recommended for Archivers	

Software requirements

To ensure that your system runs optimally, it is important to know the software requirements for Security Center 5.14.

NOTE: If you plan on running antivirus software on any machine using 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 5.14 software are as follows:

Category	Supported software
Operating systems	- Microsoft Windows 11 Pro/Enterprise^{2,3} - Microsoft Windows Server 2019^{1,2} - Microsoft Windows Server 2022^{1,2,5} - Microsoft Windows Server 2025^{1,2,5}
Database Engines ^{2,4}	- SQL Server 2017 Express/Standard/Enterprise - SQL Server 2019 Express/Standard/Enterprise - SQL Server 2022 Express/Standard/Enterprise - SQL Server 2025 Express/Standard/Enterprise
Browsers for Security Center Server Admin	- Microsoft Edge - Chrome - Firefox - Safari
Browsers for Synergis™ Appliance Portal	- Microsoft Edge - Chrome
Browsers for the Genetec™ Web App ⁶	- Microsoft Edge - Chrome - Firefox - Safari (desktop version)
Browser for Genetec Cloudrunner™ integration ⁶	Microsoft Edge
Virtualization (Server)	- VMware ESXi 7.x - VMware ESXi 8.x - Microsoft Hyper-V with Windows Server 2016/2019/2022/2025

¹ Only Standard, Enterprise, and Datacenter Editions are supported.

² Only 64-bit versions are supported.

³ Microsoft Windows 11 Pro/Enterprise requires at least 4 GB of RAM for installation.

⁴ For the minimum server profile, the *Maximum server memory* of SQL Server must be limited to 512 MB.

⁵ Microsoft Windows Server 2022 and 2025 are incompatible with the minimum server profile.

⁶ We recommend that you keep your browser up to date.

Additional considerations for server specifications

To ensure that your system runs optimally, there are additional things to consider for server specifications in Security Center 5.14.

Note the following considerations for server specifications in Security Center 5.14:

- When video streaming isn't 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 with more than 300 cameras, 1,000 readers, or 300 HID Edge readers must isolate the Directory on a dedicated server.
- A more powerful server than the recommended specification doesn't 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 can't 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 the system is correctly dimensioned for your needs.

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

Virtualization performance

Virtual machines have a slight decrease in performance compared to physical hardware.

IMPORTANT: The performance loss due to virtualization is typically under 20% of the overall machine performance, but it can vary depending on the selected hardware and hypervisor configuration. See [Security Center 5.14 server requirements](#) on page 5 for recommended specifications to ensure optimal performance.

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

Virtualization decisions must also account for modular infrastructure, where multiple server modules are hosted inside a chassis and share network interfaces, power supplies, and cooling systems. Resource contention or a failure in one component can affect multiple servers in that environment.

The image below shows a Dell PowerEdge Modular Infrastructure as an example of a *server chassis* with seven *server modules*.



The following recommendations are based on internal testing and field experience to minimize performance impact. Most recommendations focus on how virtual machines (VMs) are distributed across server modules. We only mention the *server chassis* when a guideline is written explicitly for the module infrastructure.

Provisioning

- **Virtual Machine (VM):**

- Do not exceed six total VMs per server module, with a maximum of four video-intensive VMs per server module.
Video-intensive VMs run the Archiver, Auxiliary Archiver, or Media Gateway role.
- You must install Security Center on a dedicated server module. Do not share any server module running Genetec™ VMs with non-Genetec VMs.
- Monitor VM performance for signs of CPU scheduling delays.
If your platform reports CPU wait time (or *CPU Ready*), ensure it remains at or below 50 ms (or 5%) to avoid performance degradation. For more information on VM performance metrics, see [CPU ready and its role in VM performance](#).
- **Virtual CPU (vCPU):**
 - When assigning vCPUs, ensure you assign only complete logical cores from the same physical CPU. Never split hyperthreaded vCPUs between multiple VMs by assigning vCPU core 0 to one VM and vCPU core 1 to another.
 - If you want to run fault-tolerant VMs, you must understand the hardware limits of this setup. Fault-tolerant VMs typically do not support transferring more than four vCPUs, even if you assign more to the VM. For example, if you assign 8 vCPUs to a fault-tolerant VM, only 4 will be transferred during a failure. For information about fault-tolerant configuration, see your VM manuals.
 - If you are not running fault-tolerant VMs, we recommend assigning 8 or more vCPUs per VM.
- **Memory:**
 - Assign at least 16 GB of RAM to each VM.
 - Keep 16 GB of RAM unallocated for the hypervisor.
 - The total amount of memory allocated to the VMs and the hypervisor must not exceed the total amount of physical memory available from the server module.
- **Storage:** Storage configurations depend on the hardware vendor's best practices and the system environment.
For operating systems:
 - Install Microsoft Windows and Microsoft SQL databases on a dedicated, high-performance drive, typically an SSD or a Storage Area Network (SAN) with SSD or hybrid storage.
 - Do not use the operating system (OS) drive for archived video.
 - Make the OS partition at least 120 GB.
 For archived video: Configure Archiver video disks using one of the following methods:
 - A data store (VMDK, VHD, or SMB Shares)
 - Raw Device Mapping (RDM) for Fiber Channel
 - In-Guest iSCSI**NOTE:** Other configurations might result in degraded performance.
- **Network:**
 - If you create virtual network adapters, do not rely on the link speed reported by Windows. Measure actual bandwidth to determine performance.
 - Send video traffic on a different VLAN or subnet than storage traffic.
 - Preferred connectivity for Genetec VMs is 10 GbE or greater.
 - Where only 1 GbE connectivity is available, assign one dedicated 1 GbE connection per VM for video traffic.**NOTE:** Alternate network configurations might send multicast traffic to all hosted VMs simultaneously. Depending on the server module or its configuration, this might affect overall performance.
- **High availability (Security Center failover):**

- Do not assign VMs hosted on the same physical server as primary and secondary (failover) servers of the same Security Center role.
- Use dedicated resources on the server chassis for Genetec™ VMs to avoid resource contention. When setting up failover, use a second server chassis to house the failover server modules for Security Center roles. This way, you avoid complete system outages caused by server chassis failures.

VM operations

- **System snapshots:** Capture system snapshots during scheduled maintenance periods. These operations freeze input/output (I/O) for the duration of the process and can lead to issues such as disconnections and packet loss.
- **Live migration:** For the same reason, we do not recommend dynamic load balancing. A live VM migration freezes I/O and can cause similar disconnections and packet loss.

Security Center

- **Archiver:** When provisioning multiple archiving VMs on a server module, don't exceed the following data transmission rates:
 - 300 Mbps for incoming and outgoing video on each VM.
 - 1,200 Mbps for incoming video and outgoing playback on each server module.
- **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 5.14 AutoVu ALPR server requirements"](#) on page 22

Security Center 5.14 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 5.14 AutoVu™ ALPR server.

The requirements for a Security Center 5.14 server hosting the ALPR Manager role are as follows:¹

Server profile	Server characteristics
Minimum²	- Intel® Core™ i5-3550 equivalent processor or better 8 GB of RAM (minimum 4 GB dedicated to SQL Server) - Separated storage disk from OS primary disk 50 AutoVu camera units (fixed or mobile)⁴ - SQL Server Express database server containing up to 6,000,000 ALPR Events (Reads and Hits combined) - Maximum of 5 simultaneous user connections
AutoVu Recommended	- Intel® Core™ i7-3820 equivalent processor or better 16 GB of RAM (minimum 6 GB dedicated to SQL Server) - Dedicated RAID5 storage with 4 enterprise grade disks or better 100 AutoVu camera units (fixed or mobile)⁴ - SQL Server Standard database server containing up to 25,000,000 ALPR Events (Reads and Hits combined) - Maximum of 20 simultaneous user connections
AutoVu High performance	- Intel® Xeon® E5-2620 v4 equivalent processor or better 32 GB of RAM (minimum 8 GB dedicated to SQL Server) - Dedicated RAID5 storage with at least 8 high-performance enterprise grade disks or better - Up to 300 AutoVu camera units (fixed or mobile)^{3,4} - SQL Server Standard database server containing up to 80,000,000 ALPR Events (Reads and Hits combined) - Maximum of 80 simultaneous user connections

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

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

³ 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.

⁴ 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 5.14 streaming capacities for Genetec Mobile"](#) on page 24

Security Center 5.14 streaming capacities for Genetec Mobile

The number of video streams and amount of traffic that Security Center 5.14 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 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 the Config Tool. For more information, see the following topics:

- [Configuring Mobile Server roles](#)

You can configure different video settings for wireless network (Wi-Fi) and cellular connections. Mobile Server always uses the wireless network connection when it's 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 *Recommended* server profile requirements, as detailed in [Security Center 5.14 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	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 *High-performance* server profile requirements, as detailed in [Security Center 5.14 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

Genetec Web App System Requirements

This section includes the following topics:

- ["Streaming capacities for the Genetec Web App"](#) on page 27
- ["Software requirements for the Genetec Web App"](#) on page 28
- ["Browser speeds for Security Center 5.14 Genetec Web App"](#) on page 29
- ["Number of Genetec Web App user connections per Security Center 5.14 Web App Server"](#) on page 30

Streaming capacities for the Genetec Web App

The number of video streams and amount of traffic that Security Center 5.14 can deliver vary depending on several factors. These factors include, 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 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.

Performance without transcoding						
Resolution @ 30 FPS	Full HD – 1920 x 1080			Ultra HD – 3840 x 2160		
	H264	HEVC (H.265)	AV1	H264	HEVC (H.265)	AV1
Average bit rate per camera	4.76 Mbps	3.21 Mbps	3.06 Mbps	19 Mbps	13.35 Mbps	12.74 Mbps
Recommended	127 streams	153 streams	151 streams	50 streams	72 streams	66 streams
High-performance	170 streams	198 streams	184 streams	110 streams	129 streams	123 streams

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 11 Professional and Enterprise	• Microsoft Edge latest version • Google Chrome latest version¹ • Mozilla Firefox latest version²
Microsoft Windows Server 2019 Standard Edition	• Microsoft Edge latest version • Google Chrome latest version¹ • Mozilla Firefox latest version²
Microsoft Windows Server 2022 Standard Edition	
Microsoft Windows Server 2025 Standard Edition	
Mac OS	Apple Safari latest version ¹

¹ The Genetec Web App doesn't fully support Apple Safari for iOS and Google Chrome for Android devices. To access Security Center videos and data from your mobile device, use Genetec™ Mobile.

² If you aren't seeing high-quality (H.264) video in your Firefox browser, make sure that H.264/avc3 on the media source extension is enabled.

Browser speeds for Security Center 5.14 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
NOTE: If you aren't 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 doesn't 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 5.14 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.

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 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 are needed, choose the server type 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 resources required by each connected user, based on their typical activity

User activity like generating reports, managing cardholders, and acknowledging alarms requires fewer server resources. However, some user activity is more resource-intensive, such as monitoring video streams and receiving ALPR license plate reads. Therefore, server performance depends on how resource-intensive the average activity is for each client connection.

The following table shows the suggested number of Web App client connections each server type supports.

NOTE: Video bandwidth is more critical than the number of users when choosing the number and type of servers you require for your system. The video bandwidth you need depends on the number of cameras you have and the video quality configured for each camera.

Server type	Maximum Web App client connections
Recommended	300
High-performance	400

How can I increase the number of concurrent user connections?

To add more users to your system or to increase performance for existing users, you can:

- 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.

- **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

The Genetec™ Technical Assistance Center (GTAC) provides technical support to customers worldwide. As a Genetec customer, you have access to TechDoc Hub, where you can find documentation and answers to product questions.

- **Genetec TechDoc Hub:** TechDoc Hub includes articles, manuals, and videos that help answer questions and resolve technical issues. Before contacting GTAC or opening a support case, search TechDoc Hub for potential fixes, workarounds, or known issues.

To access TechDoc Hub, sign in to the [Genetec Portal](#) and click [Go to TechDoc Hub](#). If you can't find what you're looking for, contact documentation@genetec.com.

- **Genetec Technical Assistance Center (GTAC):** Information about contacting GTAC is available in the [Genetec Advantage Description](#).

Technical training

In a professional classroom environment or from your own office, qualified trainers guide you through system design, installation, operation, and troubleshooting. Technical training is available for all products and for customers with varying levels of technical experience, and it can be customized to meet specific needs and objectives. For more information, see the [Genetec training certification courses directory](#).

Licensing

- For license activation or reset requests, contact GTAC at <https://www.genetec.com/portal/support>.
- For issues with license content, part numbers, or orders, contact Genetec Customer Service at customerservice@genetec.com or call 1-866-684-8006 (option 3).
- For demo licenses or pricing questions, contact Genetec Sales at sales@genetec.com or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Contact the Genetec Technical Assistance Center (GTAC) at <https://www.genetec.com/portal/support> to report or resolve issues with Genetec appliances or hardware purchased through Genetec Inc.