Security Center System Requirements Guide 5.10

Document last updated: November 19, 2021

Genetec™

Legal notices

Document information

Document title: Security Center System Requirements Guide 5.10

Original document number: EN.500.100-V5.10.2.0(1)

Document number: EN.500.100-V5.10.2.0(1)

Document update date: November 19, 2021

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

Contents

1

Security Center System Requirements

This section includes the following topics:

Security Center 5.10 system requirements

For Security Center 5.10 system requirements, refer to the *Security Center System Requirements Guide*.

To determine which configuration is best suited for your application, contact our Sales Engineering team at salesengineering@genetec.com.

Security Center 5.10 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 5.10.

IMPORTANT: The recommended system requirements for Security Center 5.10.0.0 refer to newer generation hardware. Upgrading from Security Center 5.9 with older hardware does not impact performance when using the same feature set.

The requirements for Security Center 5.10 client workstations are as follows:

Client profile	Client characteristics
Minimum	• Intel® Core™ 2 X6800 @ 2.93 GHz • 2 GB of RAM or better • 32-bit operating system • 80 GB hard drive for OS and Security Center applications, with a minimum of 66 GB of free disk space to install the Security Center client application • 256 MB PCI-Express x16 video card • 1280 x 1024 or higher screen resolution with 96 dpi • 100 Mbps Ethernet network interface card
Recommended	• 9th Generation Intel® Core™ i7-9700 or better • 8 GB of RAM or better • 64-bit operating system • 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 • GbE network interface card • NVIDIA® GTX 1660 video card
High performance *Video intensive configuration*	• 9th Generation Intel® Core™ i9-9940X or better • 16 GB of RAM or better • 64-bit operating system • 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 • GbE network interface card • Dual NVIDIA® GeForce® RTX 2080 video card

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 5.10.

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[1]	53 / 52	36 / 34	25 / 23	6 / 8
High performance[1]	125 / 126	78 / 73	53 / 59	17 / 28

[1] 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 additional features such as visual tracking or guard tours.

NOTE: In an active operator scenario, the maximum number of decodes should not exceed 95% of these numbers.

GPU considerations

- If your Intel® processors support Intel® Quick Sync Video, then this technology can also be used provided the monitor is plugged into the motherboard. Laptops can also use Quick Sync Video.
- Two or more graphic 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.
- NVIDIA® -SLI™ bridge not supported.
- 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). The impact becomes less noticeable as the resolution of the video increases, because much more processing power is spent on decoding the video than on decrypting the video. The impact on performance becomes unnoticeable when viewing 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 5.10 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 5.10 Directory, Archiver, Access Manager, and Media Gateway.

The requirements for Security Center 5.10 servers are as follows:

Server profile	Server characteristics
Minimum[1]	• Intel® Core™ 2 Duo E6850 3.0 GHz or better • 4 GB of RAM or better • 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 • Separate storage disk from OS primary disk for Archiver storage • 32-bit operating system • 100/1000 Mbps Ethernet network interface card • Standard SVGA video card
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[1]
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[1] • Pre-event recording values set to the default value of 4 seconds[2] • Playback or Archive transfer should not exceed 100 Mbps[3]
Above 250,000 and up to 600,000 cardholders	• Intel® Xeon® E5-2620 v4 2.10 GHz or better • 32 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 • GbE network interface card • Standard SVGA video card[1]

Server profile	Server characteristics
High performance[4] *Video intensive configuration*	• **Streamvault™ rackmount appliance** 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 1000 cameras or 2000 Mbps, and 400 Mbps of video redirection. 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 • 16GB of RAM or better • 64-bit operating system • 80 GB SATA II hard driver or better for OS and Security Center applications • NVIDIA® P2000 video card

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

[2] To increase this value, you must proportionally reduce the Archiver's maximum bitrate.

[3] For cases that exceed 100 Mbps, subtract the equivalent bandwidth from the maximum archiving bandwidth.

[4] The intended throughput requires specific hardware and software configurations.

KiwiVision™ deployments

For the deployment of KiwiVision™ modules, use the KiwiVision™ Hardware Calculator.

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 5.10.

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 5.10 server requirements on page 5.

Server type	Maximum number of cameras or readers	
	With Minimum server profile	With Recommended server profile
Directory & Archiver (Video only)	50 cameras or 50 Mbps	100 cameras or 200 Mbps
Standalone Archiver (Video only)	75 cameras or 75 Mbps	300 cameras or 500 Mbps[1]
Standalone Redirector (Video only)	50 cameras or 50 Mbps	475 cameras or 475 Mbps[3]

Directory & 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 V1000s
	  • Up to 150 readers on Synergis™ Cloud Links
	• Readers spread across a maximum of 10 HID V1000/Synergis™ Cloud Links
	• 10,000 cardholders
		• One of the following for readers:
		  • Up to 300 HID Edge readers or 600 V2000 readers
		  • Up to 1000 readers on HID V1000
		  • Up to 1024 readers on Synergis™ Cloud Links
		• Readers spread across 100 HID V1000/Synergis™ Cloud Links
		• 250,000 cardholders

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
	  • Up to 400 readers on Synergis™ Cloud Link
	• Readers spread across 20 HID V1000/Synergis™ Cloud Links
	• 100,000 cardholders
		• One of the following for readers:
		  • Up to 700 HID Edge readers or 1400 V2000 readers
		  • Up to 2000 readers on HID V1000
		  • Up to 2048 readers on Synergis™ Cloud Link
		• Readers spread across 100 HID V1000/Synergis™ Cloud Links
		• 250,000 cardholders

Directory, Archiver & Access Manager[2] (Unified)	• Up to 50 cameras or 50 Mbps and 64 readers • Readers spread across 5 HID V1000/Synergis™ Cloud Link • 5,000 cardholders	• Up to 100 cameras or 200 Mbps and 200 readers • Readers spread across 40 HID V1000/Synergis™ Cloud Link • 40,000 cardholders

[1] For high performance Archivers (500 cameras and up), see Security Center 5.10 server requirements on page 5.

[2] If the server is configured with the minimum requirements, SQL Server must be hosted on a separate machine.

[3] For high performance Redirectors (475 cameras or 475 Mbps and up), see Security Center 5.10 server requirements.

Support for over 250,000 cardholders

To support from 250,000 to 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.

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 more information on fusion stream encryption, see the *Security Center Administrator Guide*.

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 additional 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	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.azurespeed.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, please 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 5.10.

Media Gateway agents provide video streams to the Security Center Web Client, 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 is not H.264
Web Client	Only in the following situations: • Requesting user has video watermarking enabled • Requesting user is streaming a PTZ camera and moving it (PTZ widget) • Browser does not support H.264 decoding through Media Source Extensions • Original stream is not H.264

The maximum number of camera streams supported by a dedicated Media Gateway server in Security Center 5.10 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

Performance with transcoding H.264/H.265				
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

There is a hard limit around 500 connections, the values in the table are obtained with 30 fps, if the framerate 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 640x480 (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 KiwiVision™ streams

To ensure optimal performance, do not exceed the maximum number of camera streams supported by Privacy Protector™ in Security Center 5.10.

For system requirements of all KiwiVision™ modules, please refer to the *KiwiVision™ User Guide*.

Maximum number of cameras supported in Unit Assistant Role batch operations

To ensure optimal performance, do not exceed the maximum number of cameras supported in Security Center 5.10 Unit Assistant Role (UAR) batch operations.

Some operations, like camera password change, introduces camera reconnection. It is recommended to plan these operations to occur during non-critical periods.

By default, the role runs on the server hosting the Directory and into Video Unit Control agents running on Archiver servers. It mainly uses CPU resources along with some network and disk resources.

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

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

Server Type	Recommended	High Performance
Directory & UAR	**5.9.2.0 and above** • Batch of 10,000 cameras • CPU usage increased over 80% during operation • No impact on system	**5.9.2.0 and above** • Batch of 10,000 cameras • Low CPU increase • No impact on system
	5.9.1.0 • Batch of 3000 cameras • CPU usage increased over 80% during operation • No impact on system	**5.9.1.0** • Batch of 7000 cameras • Low CPU increase • No impact on system
Archiver & UAR Agents (VideoUnitControl)	Same as maximum number of camera recommended for Archivers.	N/A

Security Center 5.10 software requirements

To ensure that your system runs optimally, it is important to know the software requirements for Security Center 5.10.

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" in *Security Center Best Practices - Enterprise*.

The requirements for Security Center 5.10 software are as follows:

Category	Supported software
Operating systems[5]	• Microsoft® Windows 8.1 Pro/Enterprise[1] • Microsoft® Windows 10 Pro version 1607 and later[1] • Microsoft® Windows 10 Enterprise LTSB version 1607 and later[1] • Microsoft® Windows 11 Pro/Enterprise[3] • Microsoft® Windows Server 2012[2,3] • Microsoft® Windows Server 2012 R2[2,3] • Microsoft® Windows Server 2016[2,3] • Microsoft® Windows Server 2019[2,3] • Microsoft® Windows Server 2022[2,3,6]
Database Engines[4]	• SQL Server 2012 Express/Standard/Enterprise • SQL Server 2014 Express/Standard/Enterprise • SQL Server 2016 Express/Standard/Enterprise[3] • SQL Server 2017 Express/Standard/Enterprise[3] • SQL Server 2019 Express/Standard/Enterprise[3]
Browsers for Security Center Server Admin	• Internet Explorer 11 • Microsoft Edge 25 or later • Chrome 46 or later • Firefox 42 or later • Safari 9 or later
Browsers for Synergis™ Appliance Portal	• Microsoft Edge 80 or later • Chrome 80 or later
Browsers for Security Center Web Client	• Internet Explorer 11 or later • Microsoft Edge for Windows 10 • Chrome • Firefox • Safari (desktop version)

Category	Supported software
Virtualization (Server)	• VMware ESXi 5.x • VMware ESXi 6.x • VMware ESXi 7.x • Microsoft® Hyper-V with Windows Server 2012/2012 R2/2016/2019
Clustering	• Microsoft® Windows Server 2012/2012 R2/2016/2019 • NEC ExpressCluster X R3 WAN/LAN Editions for Windows v.3.0.0.1

[1] Both 32-bit and 64-bit versions are supported.

[2] Only Standard, Enterprise, and Datacenter Editions are supported.

[3] Only 64-bit versions are supported.

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

[5] Microsoft® Windows 7 Pro/Enterprise/Ultimate SP1 and Microsoft® Windows Server 2008 R2 SP1 are no longer supported because they are no longer supported by Microsoft.

[6]Microsoft® Windows Server 2022 is incompatible with the minimum server profile.

Additional considerations for server specifications in Security Center 5.10

To ensure your system runs optimally, there are additional things to consider for server specifications in Security Center 5.10.

Note the following additional considerations for server specifications in Security Center 5.10.

- 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 or doors must isolate the Directory on a dedicated server.
- A more powerful server than the recommended specification will not necessarily increase the maximum capacity.
- A virtual machine with the exact 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, and will help minimize the performance impact.

For more information about virtualization, refer to Archiver Redundancy Performance in Security Center.

Provisioning

- **Virtual Machine (VM):** Do not exceed 6 total VMs per host and a maximum of 4 video-intensive VMs per host (Video-intensive VMs run Archiver, Auxiliary Archiver, Media Gateway, or Privacy Protector roles).

  Make sure Security Center is installed on a dedicated host.
- **CPU:** Do not assign more vCPUs to your VMs than the number of physical cores on the host machine. Hyperthreaded virtual cores should not be provisioned.
- **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 1GbE 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 will invalidate the system license.

2

AutoVu™ LPR System Requirements

This section includes the following topics:

Security Center 5.10 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 5.10 AutoVu™ ALPR server.

The requirements for a Security Center 5.10 server hosting the ALPR Manager role are as follows:[1]

Server profile	Server characteristics
Minimum[2]	• 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™ units (Sharp or Genetec Patroller™ combined) • 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™ units (Sharp or Genetec Patroller™ combined) • 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™ units (Sharp or Genetec Patroller™ combined)[3] • 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 Manager or Archiver roles on the machine.

3

Genetec™ Mobile System Requirements

This section includes the following topics:

Security Center 5.10 streaming capacities for Genetec™ Mobile 5.0

The number of video streams and amount of traffic that Security Center 5.10 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 Web Client 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 followings topics in the *Security Center Administrator Guide*:

- "Configuring Mobile Server roles"

  You can configure different video settings for WiFi and cellular connections. Mobile Server always uses the WiFi connection when it is available. You can find these settings in Config Tool under **Mobile Server** > **Properties** > **Video** > **Video settings**.
- "Configuring video streams of cameras"

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

NOTE: Genetec™ Mobile does not support H.264. The Media Gateway converts all H.264 streams to MJPEG before sending them to the mobile device. If the requested video resolution is lower than the source video resolution, the Media Gateway requires more CPU to downscale the image, which reduces the number of streams that the server can handle.

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

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

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

4

Security Center Web Client System Requirements

This section includes the following topics:

Security Center 5.10 streaming capacities for Web Client

The number of video streams and amount of traffic that Security Center 5.10 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 Server roles.

The Media Gateway role is used by Genetec™ Mobile and Web Client 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 followings topics in the *Security Center Administrator Guide*:

- "Configuring the Media Gateway role"
- "Configuring video streams of cameras"

  The Web 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 Server role, and the Media Gateway role.

NOTE:

- In our tests, the 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 on limiting Media Gateway connections, see the *Security Center Administrator Guide*.

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[1]
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[1]
MJPEG (640 x 480)	110	125 Mbps	1.14 Mbps[1]
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[1]
MJPEG (640 x 360)	40	60 Mbps	1.5 Mbps[1]
MJPEG (1280 x 720)	55	190 Mbps	3.45 Mbps[1]
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[1]
MJPEG (640 x 360)	20	28 Mbps	1.4 Mbps[1]
MJPEG (1280 x 720)	16	65 Mbps	4.1 Mbps[1]
MJPEG (1920 x 1080)	16	140 Mbps	8.75 Mbps[1]
H.264 (1920 x 1080)	60	260 Mbps	4.33 Mbps

[1] The Web 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 5.10 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 5.10 Web Client are the following:

Operating system	Supported Browsers
Microsoft® Windows 10 Professional and Enterprise (32-bit or 64-bit) Microsoft® Windows 8.1 Professional and Enterprise (32-bit or 64-bit)	• Microsoft Internet Explorer 11 or higher • Microsoft Edge for Windows 10 • Google Chrome latest version • Mozilla Firefox latest version
Microsoft® Windows Server® 2012 Standard Edition and R2 (32-bit or 64-bit) Microsoft® Windows Server® 2016 Standard Edition and R2 (32-bit or 64-bit) 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 Internet Explorer 11 or higher • Google Chrome latest version • Mozilla Firefox latest version
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 5.10 Web Client. To access Security Center videos and data from your smartphone, you should use Genetec™ Mobile.

Browser speeds for Security Center 5.10 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. So 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 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 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 **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.	300 to 800 ms
Microsoft Edge	3 seconds
Microsoft Internet Explorer 11 on Windows 10	3.3 seconds

Some browsers, like Microsoft Internet Explorer 11 on Windows 7, 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 user connections per Security Center 5.10 Web Server

When planning for Security Center Web Client 5.10, consider how many different users will connect to the same Web Client URL at the same time. Knowing how many users and approximately how much traffic they will generate will help you plan a deployment that ensures your users have the best possible experience in Web Client.

How many users can a Web Server serve?

As additional streams are requested simultaneously, more load is placed on the server. If the server becomes overloaded, users will notice that the Web Client pages are slow.

When planning how many Web Servers you need, figure out the maximum number of users that will log on at one time and the maximum amount of traffic expected during peak hours. Then choose the server hardware that will best manage that load.

The following table will give you an idea 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 exact 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. 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.
- **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.
- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: Genetec™ Assurance Description and Genetec™ Advantage Description.

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log on or sign up at https://gtapforum.genetec.com.
- **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, please contact GTAC at https://portal.genetec.com/support.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at https://portal.genetec.com/support to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.