Genetec™ Security Center.

Security Center System Requirements Guide 5.7

Genetec™

Copyright notice

Document information

Security Center System Requirements

This section includes the following topics:

Security Center 5.7 client workstation requirements

To ensure that your client workstation runs optimally, it's important to know the minimum, recommended, and high performance requirements for a Security Center 5.7 client workstation.

The requirements for Security Center 5.7 client workstations are as follows:

Client profile	Client characteristics
Minimum	- Intel® Core™ 2 X6800 @ 2.93 GHz 2 GB of RAM or better 80 GB hard drive for OS and Security Center applications 256 MB PCI-Express x16 video card 1280 x 1024 or higher screen resolution with 96 dpi 100 Mbps Ethernet network interface card
Recommended	4th Generation Intel® Core™ i7-4770 or better 8 GB of RAM or better 64-bit operating system 120 GB Solid State Drive for OS and Security Center applications - GbE network interface card - NVIDIA® QUADRO K620 2 GB video card
High performance *Video intensive configuration*	4th Generation Intel® Core™ i7-4770 or better 16 GB of RAM or better 64-bit operating system 240 GB Solid State Drive for OS and Security Center applications - GbE network interface card 1 x NVIDIA® GeForce® GTX 1060 6 GB video card

GPU considerations

- Minimum of 2 GB of video RAM recommended.
- 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.
- The decoding of H.265 HEVC video can be accelerated using an NVIDIA® GeForce® GTX 1060, GTX 1070, or GTX 1080 video card.

Maximum number of cameras viewed per client type

To ensure that your client workstation runs optimally, it is important to know the maximum number of cameras that can be viewed per client workstation type in Security Center 5.7.

The maximum number of cameras viewed per client workstation type in Security Center 5.7 are as follows:

H.264 format Resolution @ 30 fps Average bit rate/camera[1]	CIF 352 x 240 350 Kbps	VGA 640 x 480 1 100 Kbps	HD 1280 x 720 2 300 Kbps	Full HD 1920 x 1080 5 500 Kbps	Ultra HD 3840 x 2160 50 000 Kbps
Minimum	14	6	2	1	0
Recommended[2]	60	47	23	11	6
High performance[2, 3] *Video intensive configuration*	78	58	50	26	8

[1] These are estimates, and different camera manufacturer's bit rate may vary with the same resolution and frame rate. The decoding performance can also vary from one manufacturer to another.

[2] With hardware acceleration enabled.

[3] Using one video card NVIDIA® GeForce GTX 1060 with 6 GB of RAM

Performance benchmark for HEVC (H.265)

The following benchmark illustrates the average bit rate of a camera streaming at 20 fps using HEVC (H.265) video format.

The viewing workstation has a 4th Generation Intel® Core™ i7-4770 @ 3.5 GHz processor, with 16 GB RAM, an SSD hard drive, and runs Windows 8.1. The video card used is an NVIDIA® GeForce® GTX 1060 with 6 GB of RAM connected to a 4K monitor.

H.265 format Resolution @ 20 fps Average bit rate/camera	VGA 640 x 480 115 Kbps	HD 1280 x 720 445 Kbps	UXGA 1600 x 1200 730 Kbps	Full HD 1920 x 1080 3 000 Kbps
Max. number of cameras	77	51	31	24

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.

Security Center 5.7 server requirements

To ensure that your system runs optimally, it's important to know the minimum, recommended, and high performance server requirements for a Security Center 5.7 Directory, Archiver, and Access Manager.

The requirements for Security Center 5.7 servers are as follows:

Server profile	Server characteristics
Minimum	• 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 • 32-bit operating system • 100/1000 Mbps Ethernet network interface card • Standard SVGA video card[1]
Recommended	• Quad Core Intel® Xeon® E5-2620 v4 2.10 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 • GbE network interface card • Standard SVGA video card[1]
High performance[2] *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).

[1] Config Tool requires a minimum resolution of 1024 x 768. Not required for virtual servers.

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

Maximum number of cameras and readers per server type

To ensure that your system runs optimally, it's important to know the maximum number of cameras and readers per server type in Security Center 5.7.

Server type	Minimum	Recommended
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 300 Mbps[1]
Directory & Access Manager (Access control only)	100 HID Edge readers/ V2000, or 150 readers on HID V1000/Synergis™ Cloud Link 10 HID V1000/Synergis™ Cloud Link 10,000 cardholders	300 HID Edge readers/V2000, or 300 readers on HID V1000 or 1024 readers on Synergis™ Cloud Link 100 HID V1000/Synergis™ Cloud Link 250,000 cardholders
Standalone Access Manager (Access control only)	100 HID Edge readers/ V2000, or 150 readers on HID V1000/Synergis™ Cloud Link 10 HID V1000/Synergis™ Cloud Link 10,000 cardholders	700 HID Edge readers/V2000, or 500 readers on HID V1000 or 2048 readers on Synergis™ Cloud Link 100 HID V1000/Synergis™ Cloud Link 250,000 cardholders
Directory, Archiver & Access Manager (Unified)	50 cameras or 50 Mbps and 64 readers 5 HID V1000/Synergis™ Cloud Link 5,000 cardholders	100 cameras or 200 Mbps and 200 readers 40 HID V1000/Synergis™ Cloud Link 40,000 cardholders

[1] For high performance Archivers (500 cameras and up), see Security Center 5.7 server requirements on page 4.

Encryption impact on Archiver performance

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

Example: On an Archiver that supports 300 cameras without encrytion:

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

Number of certificates enabled	Number of supported 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.*

Privacy protection impact on performance

CAUTION: Ensure that the Privacy Protector role is <u>not</u> on the same server as the Archiver because it can affect the CPU performance and the archives. When the CPU usage is high on the Archiver server, *Archiving queue full* situations can occur and data can be lost.

BEST PRACTICE: Use an Intel® CPU that supports Intel® Quick Sync Video (such as Intel® Xeon® Processor E3 v5 Family).

Security Center 5.7 AutoVu™ LPR server requirements

To ensure that your system runs optimally, it's important to know the minimum, recommended, and high performance requirements for a Security Center 5.7 AutoVu™ LPR server.

The requirements for Security Center 5.7 AutoVu™ LPR servers are as follows:[1]

Server profile	Server characteristics
Minimum[2]	• Intel® Quad Core™ i5-3550 processor equivalent or better (6000 CPU Mark or better) • 12 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 Express database server containing up to 6 000 000 LPR Events (Reads and Hits combined) • Maximum of 5 simultaneous user connections
Recommended	• Intel® Quad Core™ i7-3820 processor equivalent or better (8000 CPU Mark 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 Standard database server containing up to 25 000 000 LPR Events (Reads and Hits combined) • Maximum of 20 simultaneous user connections
High performance	• Intel® Xeon Quad Core™ processor equivalent or better than E5-1620 v4 (10 000 CPU Mark 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 250 AutoVu™ units (Sharp or Genetec Patroller™ combined) • SQL Standard database server containing up to 80 000 000 LPR 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] SV-32 v2 equivalent machine.

Security Center 5.7 software requirements

To ensure that your system runs optimally, it is important to know the software requirements for Security Center 5.7.

The requirements for Security Center 5.7 software are as follows:

Category	Supported software
Operating systems	• Microsoft® Windows 7 Pro/Enterprise/Ultimate SP1[1] • Microsoft® Windows 8.1 Pro/Enterprise[1] • Microsoft® Windows 10 version 1511 and later[1] • Microsoft® Windows 10 Enterprise LTSB • Microsoft® Windows Server 2008 R2 SP1[2,3] • Microsoft® Windows Server 2012[2,3] • Microsoft® Windows Server 2012 R2[2,3] • Microsoft® Windows Server 2016[2,3]
Database Engines	• SQL Server 2008 R2 Express/Standard/Enterprise • SQL Server 2012 Express/Standard/Enterprise • SQL Server 2014 Express/Standard/Enterprise • SQL Server 2016 Express/Standard/Enterprise[3]
Browsers for Security Center Server Admin	• Internet Explorer 9, 10, and 11 • Chrome 46 (or later) • Firefox 42 (or later) • Safari 9 (or later) • Microsoft® Edge 25 (or later)
Browsers for Synergis™ Appliance Portal	• Internet Explorer 9, 10, or Google Chrome
Browsers for Web Client 5.7	• Internet Explorer 11 or higher • Edge for Windows 10 • Chrome • Firefox • Safari (desktop version)

Category	Supported software
Virtualization (Server)	• VMware ESXi 5.x • VMware ESXi 6.x • Microsoft® Hyper-V with Windows Server 2012/2012 R2/2016 and SQL Server 2016
Clustering	• Microsoft® Windows Server 2008/2008 R2/2012/2012 R2 • NEC ExpressCluster X R3 WAN/LAN Editions for Windows v.3.0.0.1

[1] Both 64 and 86 bit versions are supported.

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

[3] Only 64 bit versions are supported.

Additional considerations for server specifications in Security Center 5.7

To ensure your system runs optimally, there are additional things to consider for server specifications in Security Center 5.7.

Note the following additional considerations for server specifications in Security Center 5.7.

- When video streaming is not in multicast from the camera, the maximum throughput calculation must include camera streams being redirected by the Archiver.

- Software-based motion detection can reduce the maximum capacity by as much as 50%. When enabling motion detection, use unit-based 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 high end 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 when using virtualization.

- VMware ESXi must be installed on a clean computer; that is, no operating system is installed on the computer.

- Genetec™ Server cannot be installed on the same machine as the domain controller.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ Technical Information Site:** The latest documentation is available on the Technical Information Site. To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. 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 explain how the product works and provide instructions on how to use the product features. Genetec Patroller™ and the Sharp Portal also include context-sensitive help for each screen. 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 the Genetec™ Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec™ Technical Information Site:** 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 the Technical Information Site for potential fixes, workarounds, or known issues.

  To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. 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: EN_GLM_ASSURANCE and EN_GLM_ADVANTAGE.

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 in 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://gtap.genetec.com.

- 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://gtap.genetec.com to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.