Axxon PSIM communication details overview

Axxon PSIM 1.0.0-1.0.1 (english)

Last update 03/26/2026

Table of Contents

1 Disclaimer

This document is intended for IT teams and security professionals responsible for deploying and maintaining AxxonSoft video management systems. It determines the scope and nature of communication between *Axxon PSIM* servers and associated infrastructure. The guide outlines what data types are exchanged, the protocols and ports used, and the security measures that ensure confidentiality, integrity, and controlled access across public or private environments. It serves as a concise handout and compliance reference for integrating *Axxon PSIM* into secure enterprise or university networks.

This document summarizes the minimum requirements for network and security to deploy *Axxon PSIM* and integrate with the existing data systems, various security equipment, and auxiliary software of other developers using integrated open interfaces of the data exchange.

2 Basic hardware components of the Axxon PSIM digital video surveillance system

You can deploy the distributed video surveillance and audio monitoring system based on the *Axxon PSIM* system using the following basic hardware and software components:

1. Servers and Remote workstations based on PCs (IBM PC–based).
2. Network video hubs (WaveHub, Linux Hub, and so on).
3. Network video servers (Matrix, and so on).
4. Analog and IP video cameras.
5. Audio input devices.
6. TCP/IP communication.

3 Requirements for TCP/IP network using Axxon PSIM

On the page:

3.1 Requirements for the bandwidth of the TCP/IP network for video transmission

Network bandwidth is a limiting factor in the performance of a distributed system. The transmitted information is primarily made up of video data. For example, when you use cameras to monitor remote objects, such as ATMs, the entire information stream (video stream) is transmitted over communication channels.

To determine the required bandwidth of the TCP/IP network for transmitting video from IP devices and certain video capture cards, we recommend using the AxxonSoft Platform Calculator, available here (the **Summary stream from IP cameras (Mbit/s)** parameter). For video capture cards that are not supported by the platform calculator, use the calculation data below.

The table below shows the maximum number of remote surveillance cameras depending on the bandwidth of various communication channels. For calculation purposes, the frame rate of the video stream (the original format is PAL) is assumed to be equal to 1 FPS.

Note

In real conditions, the fluctuations of camera streams can be quite significant, depending on the scene illumination, the use of day/night mode, and how much motion there is in the frame. To accurately calculate the required network bandwidth, it is necessary to measure the stream from cameras that are already installed on the protected facility.

Communication mode	Channel bandwidth	Black and white image			Color image		
		Standard	High	Full	Standard	High	Full
Dial-Up	56 kbit/s	<1*	<1*	<1*	<1*	<1*	<1*

Communication mode	Channel bandwidth	Black and white image			Color image		
		Standard	High	Full	Standard	High	Full
ADSL, Ethernet	128 kbit/s	1	<1*	<1*	<1*	<1*	<1*
ADSL, Ethernet	256 kbit/s	2	1	1	1	1	<1*
ADSL, Ethernet	512 kbit/s	4	3	2	3	3	2
ADSL, Ethernet	1 Mbit/s	7	5	4	6	5	4
ADSL, Ethernet	1.5 Mbit/s	11	8	6	10	8	6
Ethernet	2 Mbit/s	14	11	8	13	10	8
Ethernet	10 Mbit/s	71	53	39	64	51	38
Ethernet	100 Mbit/s	711	533	388	640	512	376
Ethernet	1 Gbit/s	7282	5461	3972	6554	5243	3855

* no more than one camera, provided that maximum compression and/or additional decimation is applied.

To calculate the maximum number of remote cameras that transmit video to the network with a rate over 1 FPS, the corresponding value shown in the table must be divided by the number of frames.

Example. Live video (25 FPS—PAL) must be transmitted over a 100-megabit network. The video image is color, and the frame resolution is standard. According to the table, a 100-Mbps channel can transmit a video stream at 1 FPS and the specified color and resolution parameters from a maximum of 640 cameras. Therefore, with a video stream rate of 25 FPS, the maximum number of cameras is reduced by a factor of 25, to 640/25 = 25 cameras.

Note

In most cases, processing, transmitting, and recording audio signals requires a small amount of resources of the digital video surveillance system. When you calculate the performance of the video surveillance system, the proportion of resources allocated to audio monitoring can be neglected.

3.2 Requirements for the bandwidth of the TCP/IP network for database synchronization

If *Axxon PSIM* operates in a distributed configuration that combines several servers and/or remote administrator workstations, the *Configuration* database synchronization is performed (see Configuring database synchronization).

For the synchronization of the *Configuration* database to work correctly, the following minimum network requirements must be met:

1. The minimum speed of data transmission over the communication channel (bandwidth) is 64 kbit/s.
2. The maximum packet transmission delay is 500 milliseconds.

With worse parameter values, correct database synchronization is not guaranteed.

3.3 Requirements for the TCP/IP network quality

The following connection quality requirements are applied for the *Axxon PSIM* video subsystem to work correctly when connecting IP devices via WAN:

1. Latency:
    - For live video, no more than 10 seconds. If this value is exceeded, the connection to the IP device is terminated.
    - For face recognition, no more than 1500 milliseconds. If this value is exceeded, many faces are missed due to the skipping of a large number of frames.
    - For service and smart detectors, no more than 400 milliseconds. If this value is exceeded, the quality of object detection decreases, and smart detectors can generate events incorrectly.
2. Packet loss:
    - For live video, no more than 40%. If this value is exceeded, the connection to the camera is terminated. With a packet loss of 10% to 40%, frames are skipped (the more losses, the more skips).
    - For face recognition, service and smart detectors, no more than 25%. If this value is exceeded, faces are skipped, and the tracks of smart detectors don't correspond to objects.

4 Configuring the distributed architecture of the Axxon PSIM digital video surveillance system

4.1 General principles of designing

The digital video surveillance system generally contains:

1. Servers—hardware and software platforms used to receive and process video and audio signals from analog and IP surveillance cameras.
2. Remote administrator workstations—hardware and software platforms used for remote administration of the video surveillance system and as the specialized platforms for video gateway, remote archive server, remote web server, and so on.
3. Remote client—hardware and software platforms used as operator workstations to implement remote video surveillance and audio monitoring.

Servers, remote administrator workstations, and remote clients are integrated into the video surveillance system, fitting the system's set of functions, safety requirements, specific features of the protected facility, and so on. The video surveillance system can include several subnetworks that interact via the selected server and remote administrator workstation node. The distributed architecture of the video surveillance system provides synchronized data exchange (events, commands, setting parameters, and so on) among its components.

Servers, remote administrator workstations, and remote clients communicate with each other via LAN, WAN, VPN, and wireless networks using the TCP protocol.

> **Note**
>
> One version of *Axxon PSIM* must be installed on all components of the distributed system. This is due to the database structure of *Axxon PSIM* that can differ in different versions, so the data loss can occur.

4.2 Configuring procedure for the Axxon PSIM distributed system

To configure the distributed video surveillance system, do the following:

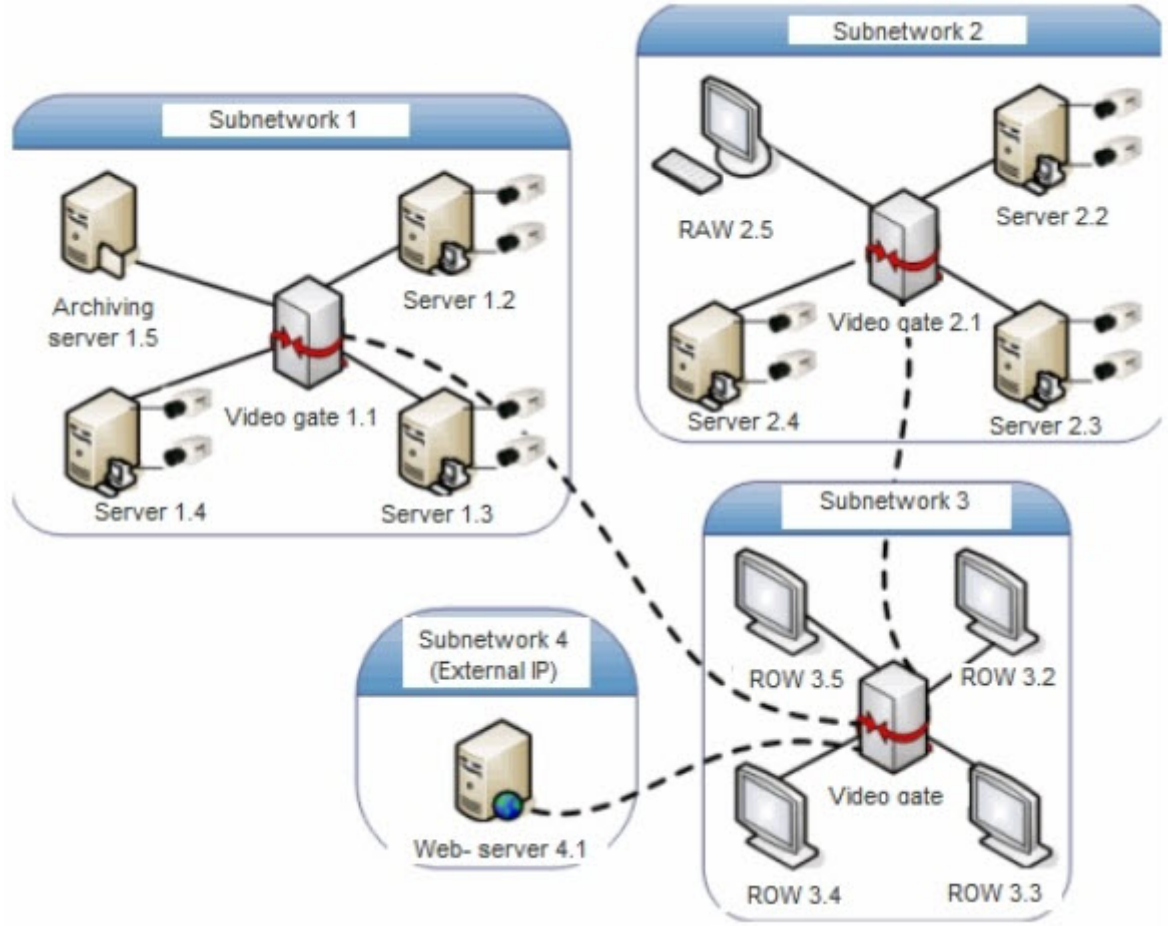
1. Create the surveillance system structure project if you didn't do it earlier.
2. Set up database synchronization for all servers and remote administrator workstations in compliance with the system structure project.
3. Register servers, remote administrator workstations, and remote clients from the same subnetwork on the administration server of this subnetwork (or at remote administrator workstation and server nodes, which optionally implement the function of administration server, if there are any subnetworks). If any selected subnetworks are present in the system, register the servers and remote administrator workstations that provide interaction of subnetworks.
4. Set up interaction of servers, remote administrator workstations, and remote clients in compliance with the system structure project.
5. Set up time synchronization in the distributed system, if necessary.
6. Specify computers in the distributed system that are used only as clients.

4.3 Example of the Axxon PSIM distributed system structure

When you create the distributed video surveillance system structure, you must take into account:

1. The number of servers, remote administrator workstations, and remote clients that must be installed on the protected facility.
2. The distances between video surveillance system components and the capacity of their communication channels. For example, servers are divided by long stretches of land; remote administrator workstations and remote clients are within the same room—the central surveillance station. Considering engineering constraints, servers will have the low-capacity channels, and remote administrator workstations and remote clients will have high-capacity channels. Then remote administrator workstations and remote clients interact with servers via the gateway only.
3. The system security requirements, for example, that prevent unauthorized administering are separated for subnetworks with servers and remote administrator workstations and subnetworks with remote clients. Subnetworks interact via the gateway only.

An example of the organization of the distributed video surveillance system is shown in the figure.



4.4 Synchronization of the database servers and remote workstations

Configuration parameters of the *Axxon PSIM* server and remote administrator workstation are stored in the distributed database. Each server and remote administrator workstation store local copies of the distributed database. Local database copies must be synchronized to provide the distributed operation of *Axxon PSIM* and data replication (synchronous alteration of local database copies).

The following synchronization mechanisms are used in *Axxon PSIM*:

1. Internal synchronization. All changes are applied to computers automatically. This mechanism is used by default and doesn't require any further configuration. Internal synchronization can be disabled, see Configuring internal synchronization.
2. DB synchronization of recipients with sources when you start *Axxon PSIM*:

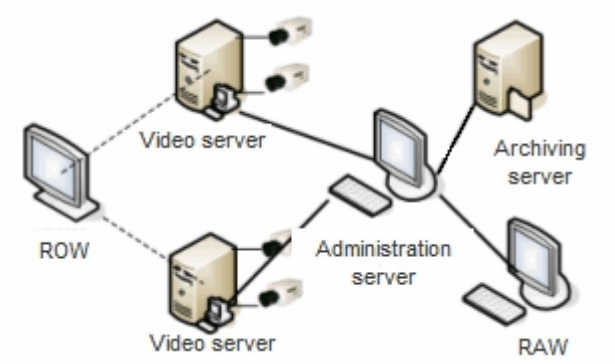
1. Configuration synchronization.
2. Configuration and protocol synchronization with changes to the sync.xml file.

   Note

   DB tables that aren't synchronized during synchronization are in the sync.xml file. We highly recommend not changing this file.

3. Only protocol synchronization.

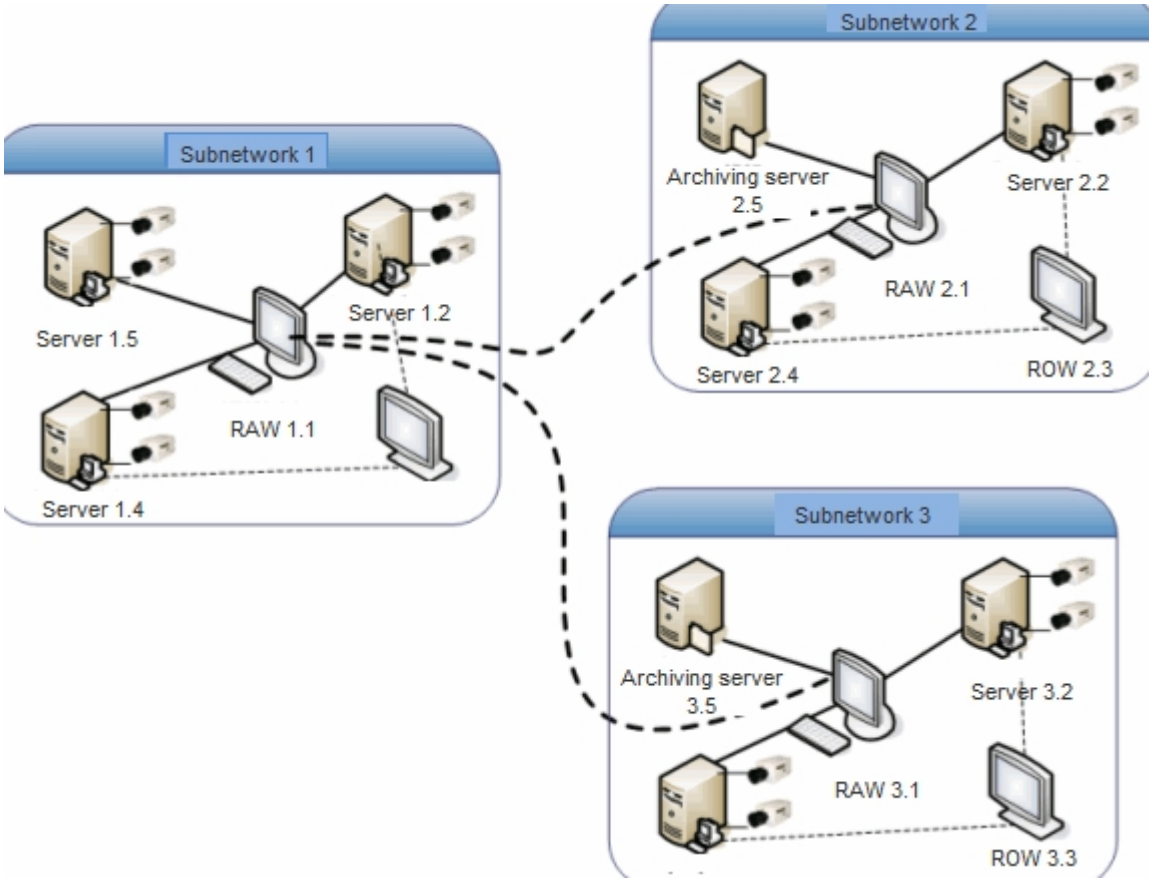
In the simplest case, database synchronization is performed for all servers and remote administrator workstations with the database of the administration server.



Note

The remote client has no database; therefore, the database of the administration server must not be synchronized with it.

If any selected subnetworks are present in the system, the server and databases of the remote administrator workstation must be synchronized with the server or remote administrator workstation database node (see, for example, the figure below).



For example, to set up database synchronization for the servers of the distributed system shown in the figure, you must:

1. Synchronize the 1.2, 1.4, 1.5 server databases with the 1.1 remote administrator workstation database.
2. Synchronize the 2.2, 2.4 server databases and the 2.5 archiving server with the 2.1 remote administrator workstation database.
3. Synchronize the 3.2, 3.4 server databases and the 3.5 archiving server with the 3.1 remote administrator workstation database.
4. Synchronize the 3.1 and 2.1 remote administrator workstation databases with the 1.1 remote administrator workstation database.

4.5 Registration of servers and workstations on the Axxon PSIM administration server

Administration of servers and remote administrator workstations is performed from one selected workstation—the administration server. We recommend having one administration server for each dedicated subnetwork of the video surveillance system (for example, for security reasons).

All servers, remote administrator workstations, and remote clients must be registered on the administration server.

4.6 Configuring the interaction of Axxon PSIM distributed system components

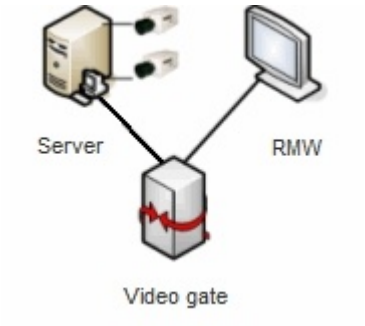
To provide the operation of the distributed system, you must configure the interaction between servers, remote administrator workstations, and remote clients. The interaction between servers, remote administrator workstations, and remote clients means database replication (for servers and remote administrator workstations only) and event exchange. During configuration, you must specify for each server, remote administrator workstation, and remote client the lists of interacting and non-interacting servers, remote administrator workstations, and remote clients.

You can configure the interaction of surveillance system components from the administration server or, if there are dedicated subnetworks, from the server or remote administrator workstation node.

Let's consider the setup of the server and remote client connection via videogate as an example. A diagram of the interaction of relevant components is shown in the figure.

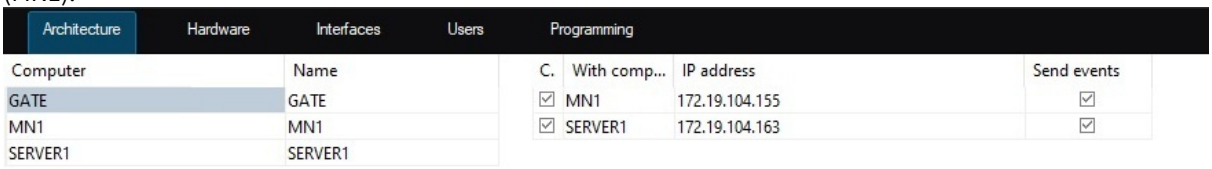
Note

Videogate is used in large distributed video surveillance systems for routing video signals between servers and clients located in different subnetworks.

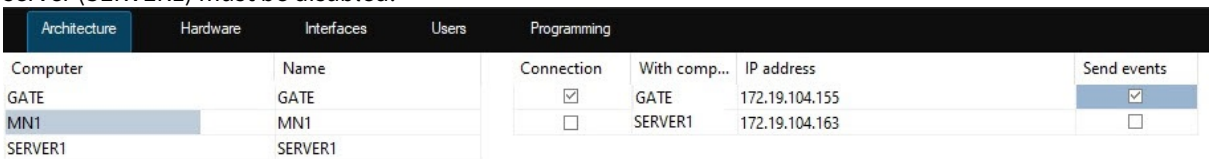


According to the diagram shown in the figure above, interaction must be disabled between the server and remote client. As a result, the **Architecture** tab displays the following configuration parameters:

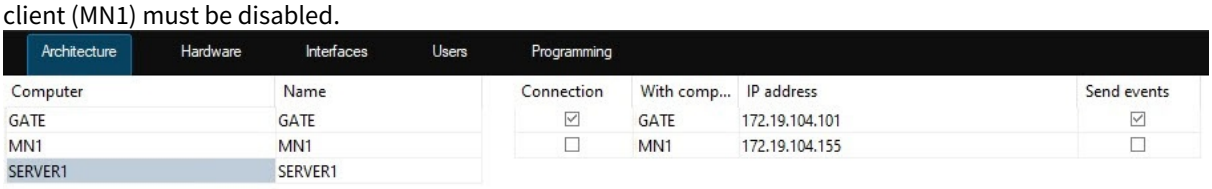
1. For the videogate (GATE), interaction must be set with the server (SERVER1) and with the remote client (MN1).



2. For the remote client (MN1), interaction must be set with the videogate (GATE), and interaction with the server (SERVER1) must be disabled.



3. For the server (SERVER1), interaction must be set with the videogate (GATE), and interaction with the remote client (MN1) must be disabled.



In *Axxon PSIM*, the **Computer** object corresponding to the remote client (MN1) isn't displayed on the **Hardware** tab of the **System settings** dialog window.

However, if you set the **Send events** checkbox (the **Connection** checkbox is clear), the **Computer** object corresponding to the remote client (MN1) is displayed on the **Hardware** tab on the server (SERVER1), but it is marked with the icon, and the object name is highlighted in grey color. It means that administration of the given object is forbidden.

4.7 Assigning role to a computer in Axxon PSIM

If large distributed systems contain more than 30 computers and it is certain that a computer is used as the client only, we recommend specifying it on the settings panel of the corresponding **Computer** object. This allows you to optimize the software operation.

Note

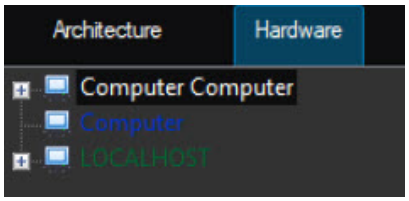
There is no need to use this setting in the smaller distributed systems.

Attention!

If you use the computer as the server/remote administrator's workstation, but it is set to be used as the client only, the distributed system doesn't operate correctly.

The role of the computer in the distributed system is displayed in the object tree in the following way:

- The current server that operates locally is highlighted in **green**.
- Clients are highlighted in **blue**.
- Other remote servers in the system are highlighted in **black**.



4.8 Features of the Axxon PSIM distributed system operation using NAT

If the distributed system is built on the basis of a network in which servers and/or clients are behind NAT, then we recommend using VPN technology for such system operation. However, this isn't a requirement: you can configure the distributed architecture in the usual way as described in Configuring the interaction of distributed system components. In this case, make sure to specify the server's external IP address for the client-to-server connection and don't specify the client IP address.

When you configure NAT, you must open the ports used by running *Axxon PSIM* modules, see The list of TCP ports used in *Axxon PSIM*. Moreover, you must open the ports that are used by MS SQL Server for database synchronization.

Note

By default, MS SQL Server uses the 1433 TCP port and the 1434 UDP port.

If the ONVIF IP camera is behind NAT, then proper operation of this camera isn't guaranteed. This limitation is due to the special features of the ONVIF protocol.

5 List of TCP ports used in Axxon PSIM

On the page:

The list of TCP ports used in *Axxon PSIM* is given in the table. You can change the ports using the ChangePort registry key.

MS SQL Server also uses the TCP port 1433 and the UDP port 1434 (by default) for database synchronization.

Note

MS SQL can use dynamic ports to synchronize databases.
To specify which ports are used, go to the **Start** → **Microsoft SQL Server Express 2014** → **Configuration Tools** → **SQL Server Configuration Manager** → **SQL Server Network Configuration** → **Protocol for SQLEXPRESS** → **TCP/IP** → **IP Addresses** menu and check which type and number of ports are specified in the **IPAll** parameter.
Configure the use of fixed ports according to the manual on the http://technet.microsoft.com/en-gb/library/ms177440.aspx Microsoft website if the use of dynamic ports is unacceptable.

Ports 8085 and 8087 are used to connect clients to the Web Server 2.0 module.

Note

This data is necessary for setting up the security system and firewall on the server. The **Corresponding module to which connection is made** parameter is set for client-server modules.

Axxon PSIM base

Module name	Name of the corresponding object in Axxon PSIM	Connection port	Corresponding module to which connection is made
AnalogChart.run	Charts	22358 Remote	PSIM.exe
ARCHPANEL.RUN	Backup archive panel	22118 Remote	PSIM.exe

AUDIO.RUN	Microphone Audio card Sound notification	21008 Remote	PSIM.exe
AUDIO.RUN	Microphone	20903 Remote	VIDEO.RUN
AUDIO.RUN	Microphone	20904 Remote	VIDEO.RUN
AUDIO.RUN	Backup audio archive	20911 Local	-
AUDIO.RUN	Audio playback card	20910 and 24008 Local	-
BacNetInt.run	BacNet	22350 Remote	PSIM.exe
CAM_TITLE.RUN	Captioner	21077 Remote	PSIM.exe
CloudAuth.run	CLOUD_AUTH	22442 Remote	PSIM.exe
CONFCHEKUTIL.RUN	Configuration check	22220 Remote	PSIM.exe
DIALOG.RUN	Operator query panel	21058 Remote	PSIM.exe
display_manager.run	Display Manager	22323 Remote	PSIM.exe
DRS.RUN	Data replication service	22175 Remote	PSIM.exe
EVENT_COUNTER.RUN	Event counter	22153 Remote	PSIM.exe
EVENT_VIEWER.RUN	Event viewer	21055 Remote	PSIM.exe
FIXMLServer.run	ISD integration server	22389 Remote	PSIM.exe

FIXMLServer.run	ISD integration server	20985 Remote	FIRSERVER.RUN
http_server.run	HTTP-server	22360 Remote	PSIM.exe
IIDK_TEST.EXE	IIDK interface	20900 Remote	VIDEO.RUN
IIDK_TEST.EXE	IIDK interface	21030 Remote	PSIM.exe
IIDK_TEST.EXE	IIDK interface	21111 Remote	PSIM.exe
INC_MANAGER.RUN	Incident manager	22401 Remote	PSIM.exe
INC_MANAGER.RUN	Incident manager	22440 Remote	System
INC_SERVER.RUN	Incident server	22432 Remote	PSIM.exe
INC_SERVER.RUN	Incident server	22439 Local	INC_MANAGER.RUN
IntegrationHTTPClient.run	VideoGuard integration client	22390 Remote	PSIM.exe
JAVA.EXE	Web-server 2.0	22212 Remote	PSIM.exe
KEYB.RUN	Keyboard	21005 Remote	PSIM.exe
LDAPIMPORT.RUN	LDAP service	22252 Remote	PSIM.exe
LIVEPLAYER.RUN	Live sound switch	22199 Remote	PSIM.exe

Manitou.run	Manitou software	22302 Remote	PSIM.exe
MAP.RUN	Map	21051 Remote	PSIM.exe
MapServer	Map server	22414 Remote	PSIM.exe
MC_CLIENT.RUN	Intercom Control Monitor	22179 Remote	PSIM.exe
MESSAGE.RUN	Alarm Message Window	21056 Remote	PSIM.exe
MMS.RUN	Mail Message Service	21031 Remote	PSIM.exe
monitor_an.run	NGP monitor	22395 Remote	PSIM.exe
OnvifServer.run	ONVIF-Server (NGP manager), ONVIF-Server	22250 Remote	PSIM.exe
OPCIE.RUN	HTML Interface	22141 Remote	PSIM.exe
OPERATORPROTOCOL.RUN	Operator protocol	22215 Remote	PSIM.exe
PLAYER.RUN	Audio player	20910 Remote	AUDIO.RUN
PLAYER.RUN	Audio player	21060 Remote	PSIM.exe
PSIM_HOST.EXE	Computer	21111 Remote	PSIM.exe
SipPanel.run	SIP panel	22331 Remote	PSIM.exe

SMS.RUN	Short Message Service	21035 Remote	PSIM.exe
StateStat.run	State statistics	22222 Remote	PSIM.exe
STREAMINGSERVER.RUN	RTSP Server (NGP manager), RTSP Server	22228 Remote	PSIM.exe
StreamTerminal.run	SIP terminal	22332 Remote	PSIM.exe
StreamTerminal.run	SIP terminal	22537 Local	-
Telegram.run	Telegram bot	22368 Remote	PSIM.exe
TELEMETRY.RUN	Telemetry Controller	21010 Remote	PSIM.exe
TELEMETRY_PANEL.RUN	Telemetry control panel	22101 Remote	PSIM.exe
TITLEVIEWER.RUN	Search by captions	20978 Remote	CAM_TITLE.run
TITLEVIEWER.RUN	Search by captions	22112 Remote	PSIM.exe
Video_ngp.run	NGP manager	22420 Remote	PSIM.exe
Video_ngp.run	NGP manager	20500 Local	-
Video_ngp.run	NGP manager	20109 Local	-
VideoPSIMClient.run	VideoPSIMClient	22451 Remote	PSIM.exe
VIDEO.RUN	CAM_TITLE.run, Detector_Ext.run	20900 Local	-

VIDEO.RUN	Video Capture Device	21050 Remote	PSIM.exe
VIDEO.RUN	Video stream archiver	20901 Local	-
VIDEO.RUN	Video stream gate	20902 Local	-
VMDADB.RUN	VMDA metadata storage	22219 Remote	PSIM.exe
VMS.RUN	Voice Message Service	21032 Remote	PSIM.exe
VNS.RUN	Voice notification service	21004 Remote	PSIM.exe
WEBSERVER.RUN	Web-server	21034 Remote	PSIM.exe
WINDOW.RUN	External window	21053 Remote	PSIM.exe
YITUClient.run	YITU Client	22452 Remote	PSIM.exe

Monitoring PSIM

Module name	**Name of the corresponding object in Axxon PSIM**	**Connection port**	**Corresponding module to which connection is made**
forward.run	Data gateway	22327	PSIM.exe
CentralNetServer.exe	CSC	7755	VIDEOSRV.EXE
VIDEOSRV.EXE	IIDK interface	21030	PSIM.exe
VIDEOSRV.EXE	VideoServer	20900	VIDEO.RUN
VIDEOSRV_C.RUN	Agent of Control	22001	-

VIDEOSRV_E.RUN	Search in archive	22003	PSIM.exe
VIDEOSRV_M.RUN	Monitoring	22222	PSIM.exe
VIDEOSRV_R.RUN	Monitoring reports	22223	PSIM.exe
VIDEOSRV_S.RUN	Server of Control	22002	-
VIDEOSRV.EXE	Server of Control	7777	VIDEOSRV.EXE
STATEUPS.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
BATDISCH.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
POWEROFF.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
POWERON.EXE (UPS operation)	-	8888	VIDEOSRV.EXE

Note

If *CSC (Central Server of Control)* is in use, then between the *CSC* communication server and the *Server of Control*, the 20 and 21 TCP ports are used to provide FTP operation.

DetectorPack PSIM

Module name	Name of the corresponding object in Axxon PSIM	Connection port	Corresponding module to which connection is made
Detector_Ext.run	Fire detection	20993 Local	-
Detector_Ext.run	Fire detection	22221 Remote	PSIM.exe

ACFA PSIM subsystem

Module name	Name of the corresponding object in Axxon PSIM	Connection port	Corresponding module to which connection is made
axacfa.run	AxACFA	22428 Remote	PSIM.exe
axacfa.run	Honeywell	22428 Remote	PSIM.exe
Esser.run	Esser	22396 Remote	PSIM.exe
glx2.run	Galaxy Dimension Panel	22300 Remote	PSIM.exe
suprema_cr.run	Suprema BioMini	22319 Remote	PSIM.exe
suprema_2.run	Suprema Biometrical ACS v2	22328 Remote	PSIM.exe
suprema_realscan.run	Suprema Realscan	22333 Remote	PSIM.exe
DataBridge.run	Data Bridge	22293 Remote	PSIM.exe
DataBridge.run	Data Bridge	2555 Remote	AppHost.exe

vanderbilt_spc.run	Vanderbilt SPC	22333 Remote	PSIM.exe

6 Additional information about ports used in Axxon PSIM

Ports used in *Axxon PSIM*:

CCTV: Hikvision and Milesight	Web server port—80, RSTP server port—554
Galaxy Dimension Panel	When you use a network connection: 1. The command socket (from glx2.run to the panel)—port 10005, strictly fixed. 2. The event socket (from the panel to glx2.run)—a configurable port, 10002 by default. The listening address (the local address on which the communication from the panel is expected) is also configured in the hardware tree. **Note!** Each module opens a separate channel for event listening, and these channels must not intersect. For example, if there are 10 Galaxy panels in the system, there must be 10 different ports for listening
Esser	Esser module—port 22396. communication with Esser SEI module is via RS (physical connection)
Vanderbilt SPC	The *PSIM* server is listening to communication between the Vanderbilt device and the *PSIM* server on a configurable port, but by default it is 52000. The Vanderbilt server module works on 22382 (server → client). The Vanderbilt client works on 22403 (client → server)
Suprema Biometrical ACS v2	suprema_2.run uses port 22328. Ports that communicate with devices are configured in the Suprema devices and in the settings of an object in *Axxon PSIM*. Therefore, it's sufficient to select a pool of ports based on the number of devices, reserve it in advance, and configure it accordingly. Outgoing communication ports are dynamically selected, and you cannot set them forcibly. This is a feature of the SDK. The easiest way is to allow all outgoing communication to the suprema_2.run application in the firewall settings. Otherwise, significant modifications are required to implement communication from devices to the module, rather than from the module to devices