HikCentral V1.1
Port List

System Ports

The following ports are used for the regular transmission of the signaling and data in HikCentral V 1.1. You may need to forward these ports on routers for WAN access or allow them for firewalls according to your software deployment or network structure.

Server	Destination	Port No.	Internal External	Source[1]	Function and Description	Solution if Conflicted
VSM (Video Surveillance Management Server)	NGINX	80 (TCP)	External	Web Client, Control Client	Used for Web Client & Control Client access in HTTP protocol	Modify it in Service Manager.[2]
		443 (TCP)	External		Used for Web Client & Control Client access in HTTPS protocol	
	VSM	14200 (TCP)	External	VSM (Remote Site)	Used for Remote Site registration to Central System.	Modify it in Service Manager.
		15300 (TCP and UDP)	External	3rd Party System	Used for receiving generic event.	Modify it in Service Manager.
		9999 (TCP)	Internal	NGINX	HTTP ISAPI communication port	Modified automatically.
		9998 (TCP)	Internal	NGINX	HTTP WebSocket port	Modified automatically.
		9443 (TCP)	Internal	NGINX	HTTPS port from NGINX port 443.	Modified automatically.
		8443 (TCP)	Internal	NGINX	WebSocket SSL port from NGINX port 443.	Modified automatically.
		8087 to 8096 (TCP)	Internal	3rd Party Device	Alarm listening port for 3rd party device. 1. Doesn't support arming mode. Port 8087 to 8097 should be available on the PC installed with VAG. 2. Doesn't support 3rd party device of arming mode. Alarms cannot be received if VSM is in internal network and device is in external. 3. Allow it on firewall.	Make sure the port is available.
	3rd Party	8765	Internal	VSM	Communication between	Modified

	Device Access Gateway	(TCP)			VSM and 3rd party device access gateway.	automatically.
	Streaming Gateway	554 (TCP)	External	Control Client	Getting stream for live view	Modify it in Service Manager.
		10000 (TCP)	External	Control Client	Getting stream for playback	Modify it in Service Manager.
		6001 (UDP)	Internal	VSM	The port of the network management agent	Modified automatically.
		6678 (TCP)	Internal	VSM	Configuration port	Modified automatically.
	Smart Wall Management Service	6666 (TCP)	Internal	NGINX	Used for responding to Control Client's request.	Modified automatically.
		6667 (TCP)	Internal	VSM	Used for communication with VSM.	Modified automatically.
		6668 (TCP)	Internal	NGINX	Used for sending real-time message to Control Client.	Modified automatically.
	Keyboard Proxy Service	8910 (TCP)	External	Network Keyboard	Used for network keyboard to access the Keyboard Proxy Service.	Modify it in Service Manager.
		8911 (TCP)	Internal	VSM	Used for communication with VSM.	Modified automatically
	NTP (Network Time Protocol) Service	123 (UDP)	External	Servers & Device	NTP server for time synchronization.	Modify port number of another system that occupies 123.
	PostgreSQL	5432 (TCP)	Internal	VSM	Database port.	Modify it manually (Installation will stop when conflict detected).
	Service Manager Service	7208 (TCP)	Internal	Service Manager	Communication port between Service Manager interface process and service process.	Modified automatically.
Streaming Server	Streaming Server	554 (TCP)	External	Control Client	Getting stream for live view	Modify it in Service Manager.
		10000 (TCP)	External	Control Client	Getting stream for playback	Modify it in Service Manager.
		6001 (UDP)	External	VSM	The port of network management agent	Modify it in Service Manager.

	Service Manager Service	7208 (TCP)	Internal	Service Manager	Communication port between Service Manager interface process and service process.	Modified automatically.

1: The port that the source uses for initiating a communication is random

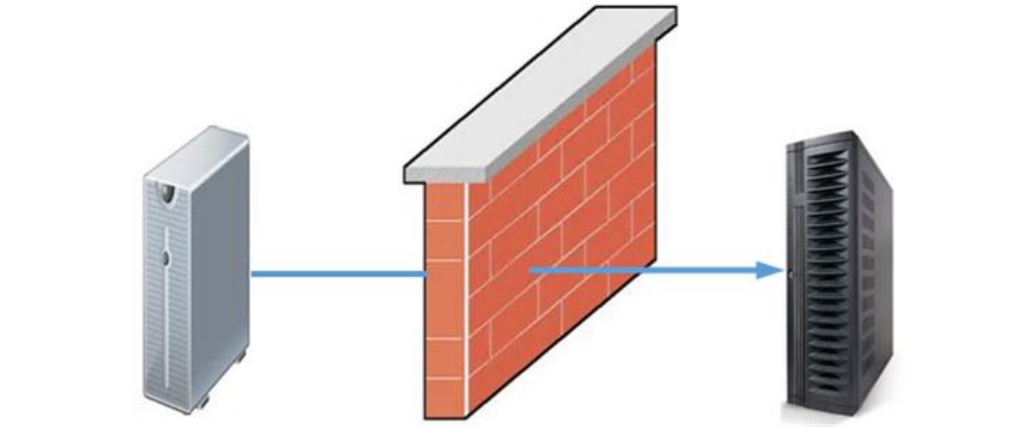
2. The VSM server's port 80 and 443 CANNOT be modified to the followings: 1, 7, 9, 11, 13, 15, 17, 19, 20, 21, 22, 23, 25, 37, 42, 43, 53, 77, 79, 87, 95, 101, 102, 103, 104, 109, 110, 111, 113, 115, 117, 119, 123, 135, 139, 143, 179, 389, 465, 512, 513, 514, 515, 526, 530, 531, 532, 540, 556, 563, 587, 601, 636, 993, 995, 2049, 3659, 4045, 6000, 6665, 6666, 6667, 6668, and 6669.

Device usually uses 80, 8000, and 554 ports for communication. Allow/forward theses ports on device if need. Please consult our local support for detailed ports of device.

Device Port	Source	Description
80	Web Client	Direct streaming from device to Web Client
8000	VSM, Control Client	Adding device; Direct streaming from device to Control Client
554	Streaming Server	Streaming from device to Streaming Server

Allowing Port on Firewall

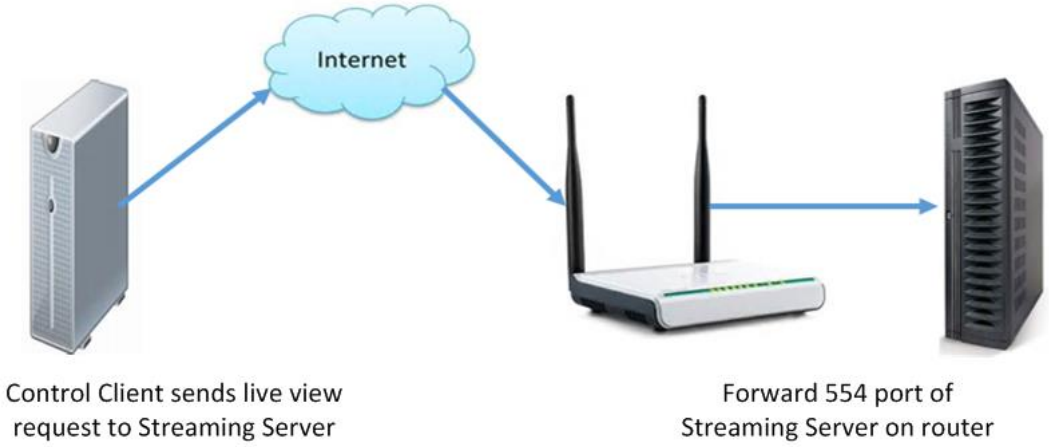
If the service and source are deployed on separate server, corresponding service port should be allowed on firewall as inbound rule, for example:

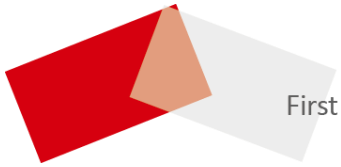


If ports cannot be allowed on firewall, you can also allow the service/process on firewall to ensure the communication. Please choose the firewall strategy according to the actual situation.

Forwarding Port on Router

If the service and source are deployed in different LANs, corresponding service port should be forwarded on router.





First Choice for Security Professionals