Chapter 1 - Appendix 1 – Network configuration

In order to run ATEAS Security applications, you might need to configure certain network devices (for example, network routers, especially when the camera system is located within the local network) so that server applications will be able to operate on their specified ports. The table below shows a general overview of the network ports. The system client is always the party establishing connections. Therefore, no special settings have to be performed on the client side.

NOTE

Basic system operation requires verifying that port 8501 for the administration server and port 8502 for the camera server are open. Other ports are used for advanced functionality and integration.

1.1. Administration server

Port	Transport protocol	Application protocol	Communication
8501	TCP	ATEAS	Basic communication port
8503	TCP	ATEAS	Cloud based connection
8504	TCP	ATEAS	Receiving external events
9001 - N	TCP	WebSocket / TLS	Cloud based connection for web clients
80	TCP	HTTP	System home page, web client, automatic updates
443	TCP	HTTPS / TLS	System home page, web client, automatic updates
162	UDP	SNMP	Receiving traps for event activation

1.2. Camera server

Port	Transport protocol	Application protocol	Communication
8502	TCP	ATEAS	Basic communication port

8505	TCP	ATEAS	Custom camera events
8506	TCP	HTTP	Access to the web page of all cameras
8507	TCP	WebSocket	Unsecured web streaming
8508	TCP	WebSocket / TLS	Secured web streaming
8509	TCP	HTTP	Video streaming using DLNA
3702	UDP	SOAP	Searching Onvif devices (WS Discovery)
8080	TCP	HTTP	Body Worn System

CAUTION

If the RTP/UDP scheme is used for transmitting camera data, UDP ports are dynamically allocated and an exception for the entire camera server shall be set, not just for specific ports. This also applies for the client, provided its profile is set to LOCAL and therefore connects to multicast addresses and receives data via the UDP protocol.