AVERTX CONNECT NETWORK REQUIREMENTS

INTRODUCTION

AvertX Connect is a secure and powerful Web-enabled platform that reduces maintenance costs and streamlines the management of video surveillance systems. Customers using AvertX Connect can manage users, access live and recorded video, and export video incidents to cloud servers without fear of exposing their security system to potential threats. Our service ensures the security and integrity of your data by implementing technologies designed to prevent a wide range of hacking and data loss scenarios.

This document has been created to work as a guide to ensure your installation goes smoothly.

ENSURING REMOTE ACCESS THROUGH AVERTX CONNECT

AvertX Connect utilizes a video relay system that does not require port forwarding, thereby reducing maintenance and complexity. While no additional network configuration should be required, some specific ports cannot be blocked for outgoing traffic.

In order to ensure the successful commissioning of your AvertX Connect enabled recorder, the following ports must not be blocked:

Incoming

- None required

Outgoing (these ports do not need to be forwarded, but cannot be blocked)

- TCP port 443 (used for AvertX Connect relay)

Content Filtering

In some cases, menus and interfaces will load properly and all setup elements are accessible, but Live and Search video never appear. This problem likely stems from content filtering (also known as ‘media inspection’ on some devices). When a firewall or proxy is configured to filter content, the system will attempt to wait until the entire file has been received before examining it, as identified by the 'end of file' marker contained in the video stream data. However, when streaming video from a recorder, the data does not have an 'end of file' marker, so the system holds the video indefinitely while waiting for the marker.

AvertX recommends that you review your content filtering options and refer to the allowlist section for details on URLs to exclude from the filter.

ALLOWLIST REQUIREMENTS

Network Allowlist Requirements

If the network is preventing the recorder from communicating with AvertX Connect, it will prevent the service from making the necessary connection required for authenticating the recorder. This will require a Network Administrator to whitelist the hosts that the recorder will reach out to in order to make a connection to AvertX Connect.

Note We recommend adding the domains as documented below to your network allowlist instead of the IP address the domains resolve to. If your network filter uses reverse DNS, it is recommended to add your recorder to an exclusion range that is not filtered as our IP range will resolve to amazonaws.com.

Note Communication with the relay service u5fgb.com uses a payload of message/http. This is an embedded HTTP response message from the recorder to the client software. If your network filter is blocking traffic to u5fgb.com you must allow “Content-Type” of “message/http” in your network filter.

Ports TCP 80 and TCP 443 are utilized by default for each address unless otherwise specified. On highly secure networks, TCP port 443 can be used exclusively for communication [HTTPS/TLS].

The following locations are required for LAN Smart Forwarding (LSF) and communication with relay service:

***.*.u5fgb.com (for recorders located in the United States)**

lsf-avx.u5fgb.com

Note Adding *.*.u5fgb.com will allow communication to new relay services as they become available.

connect.avertx.com (for communication with API services and AvertX Connect login portal)

- TCP 443 only

Required for software updates, video clip export and thumbnail images (TCP 443 for all):

avx-prod-devmon.s3.us-west-2.amazonaws.com

avx-prod-files.s3.amazonaws.com

avx-prod-media.s3.us-west-2.amazonaws.com

The following locations are optional:

stun.u5fgb.com (for peer to peer connections to improve performance)

- UDP 3478

***.avertx.com (for support of future enhancements)**

- TCP 443 only

assist.dvrsupportcenter.com (for temporary Remote Assist Session initiated by Technical Support)

- TCP 443 only

1.cctv.pool.ntp.org (for support of NTP (Network Time Server)

- UDP 123 only

Note Cisco Iron Port devices may need a “Cisco Data Security” policy setup to allow POST traffic through. This will resolve issues with live video showing black when using relay.

Email Allowlist Requirements

When using an email service that filters emails based on a allowlist, it is possible that communication from AvertX Connect will be blocked. Configuring your email server allowlist to accept incoming emails from AvertX Connect servers will prevent missed communication from AvertX Connect.

The following server is required:

***@connect.avertx.com**

BANDWIDTH RECOMMENDATIONS

AvertX recommends an NVR site upload bandwidth speed of 5 Mbps for an optimal experience when remotely viewing video over the WAN (Internet). This will result in a positive user experience when reviewing video from one 4MP high definition stream, or up to 9 standard definition streams. In instances where less than 5 Mbps is available remote users should plan to utilize standard definition streams for retrieving video over the WAN.

While the AvertX Connect platform is highly configurable to meet exact bandwidth usage requirements the following table may be referenced as a typical use case:

Average bandwidth usage based on D1/4MP, 4,000Kbps, 15 IPS, 30 GOP IP Cameras		
Channel Count	Live & Search SD Playback	Live & Search HD playback
Single channel	800 Kbps	4 Mbps
4 channel grid	3 Mbps	16 Mbps
9 channel grid	7 Mbps	36 Mbps
16 channel grid	13 Mbps	64 Mbps

Note The AvertX Connect platform dynamically chooses HD or SD streams for viewing based on the client display configuration selected by the user. For example, a 4CH view will deliver SD video by default while a single channel view will automatically deliver the HD stream. Stream selection may also be manually controlled using the stream selection control at the top of the applicable display screen.