

# Firewall Configuration for Secure Networks

The Eagle Eye VMS and its bridge hardware is specifically designed to be highly secure and only uses outbound TCP and UDP connections to talk to the cloud. If you restrict outbound connections on your local firewall, here is the IPv4 and port information you will need.

## Outbound Ports for the Eagle Eye Bridge

The following TCP and UDP ports are used by the Eagle Eye Bridge. All connections are outbound-only, meaning that the bridge connects outbound and never accepts inbound connections (so you do NOT need to set up e.g. NAT rules as a general rule).

80/tcp # Used to discover video termination endpoints in the cloud

443/tcp # Used to transfer video to the cloud (TLS 1.2+)

773/tcp # Used to transfer video to the cloud (TLS 1.2+)

8081/tcp # Used to transfer video to the cloud

8082/udp # Used to transfer video metadata to the cloud

50000-60000/tcp # Used occasionally to provide remote troubleshooting and maintenance (Secured via SSL)

- ⚠ There can be no proxies or similar application-layer filtration devices between the Eagle Eye Bridge and the Internet, and multicast must be enabled so the bridge can detect cameras (if the bridge and cameras are on the same subnet, generally this isn't a problem). UPNP is NOT required (the bridge won't use it if enabled).
- 

- ① For further information on the ONVIF camera discovery protocol we use, see [this article on WS-Discovery](#). Web Service Discovery is an OASIS industry standard and generally works without much effort on most internal networks. You should not need to adjust your firewall to get it to work unless there is additional firewalling between your bridge and cameras

## Outbound IPs for the Eagle Eye Bridge

Should you need to restrict the Eagle Eye Bridge to a specific set of IP addresses, the following is the list of Eagle Eye IP addresses you should allow in CIDR format:

### Eagle Eye Cloud VMS

192.40.4.0/23  
209.94.248.0/26  
208.81.96.0/22  
61.120.148.0/25  
210.248.158.0/24  
218.102.54.0/24  
199.204.51.0/25  
84.16.229.32/27  
84.16.229.160/27  
95.168.179.0/27  
95.168.182.32/27  
95.168.185.64/26  
130.250.6.128/27  
37.58.51.0/25  
216.245.88.0/21

### Eagle Eye Camera Manager

62.50.13.192/27  
89.202.212.160/28  
195.81.42.160/27  
195.81.164.160/27  
212.23.62.240/28  
89.202.213.96/28

## Outbound Ports for the Eagle Eye Web and Mobile Applications

Independent of the bridge, the Eagle Eye Web and Mobile Applications for PCs, tablets, and phones also need to connect to the cloud to retrieve video, set settings, and so on. The ports required for this are:

tcp/80 # HTTP->SSL Redirect Only

tcp/443 # Web user interface

tcp/50000-60000 # Secure video transfer

The IPs are generally the same as for the bridge.

<https://support.een.com/portal/en/kb/articles/firewall-configuration-for-secure-networks>