# Eagle Eye Application Note - AN062

# Essential Firewall Configuration Guide for Securing Eagle Eye Cloud VMS

2024-03-06 Revision 1.0

## Target Audience

This Application Note is designed to cover firewall configuration when installing an Eagle Eye Cloud VMS system and is intended for intermediate to advanced technical administrators and installers. It is intended for any size/class of user who maintains a firewall IP allowlist, e.g, while setting up the network to connect IP cameras to the Eagle Eye Bridge.

## Introduction

The Eagle Eye Cloud VMS and its bridge hardware is specifically designed to be highly secure, and uses only outbound TCP and UDP connections to talk to the cloud. This document provides the required IPv4 and port information required for restricted outbound connections on a local firewall.

## Overview

Eagle Eye Networks may add or remove IP spaces from time to time in order to optimize performance of the Cloud VMS. For users that maintain advanced firewall configurations with a specified allowlist, new IP additions must be updated in order to maintain surveillance system functionality. This document provides a source to ensure that firewall configurations are always kept up to date.

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 however, this is not generally a problem). UPnP is NOT required (the bridge won't use it if enabled).

For further information on the ONVIF camera discovery protocol used, see this article on Web Service-Discovery. Web Service Discovery is an OASIS industry standard and generally works without much effort on most internal networks. You should not need to further adjust your firewall unless there are additional firewall layers between your bridge and cameras.

# Outbound Ports for Eagle Eye Bridge/CMVR

The following TCP and UDP ports are used by the Eagle Eye Bridge/CMVR. 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 test video transfer to the cloud |
| 8082/udp | # Used to transfer video metadata to the cloud |
| 50000-60000/tcp | # Used for remote troubleshooting and maintenance (secured via SSL) |

Ports 80 and 443 are utilized for firmware management. If these ports are filtered or blocked it can cause failed updates for our systems.

Ports 8081 and 8082 are utilized for the preview stream. If this port is filtered or blocked it will impact the preview stream's stability and quality.

Eagle Eye utilizes standard ports for our troubleshooting tools (e.g. Ncat and Fping). These may show as being utilized on your network; please note they are used only for system maintenance.

# Outbound IPs for Eagle Eye Bridge/CMVR

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

| | | |
|---|---|---|
| 167.248.134.0/23 | 209.94.248.0/26 | 195.81.164.160/27 |
| 167.94.38.0/23 | 61.120.148.0/25 | 89.202.213.96/28 |
| 167.94.228.0/23 | 210.248.158.0/24 | 62.50.13.192/27 |
| 208.81.96.0/22 | 218.102.54.64/26 | 199.45.160.0/22 |
| 216.245.88.0/21 | 223.197.211.0/25 | |
| 192.40.4.0/23 | 199.204.51.0/25 | |

**Note:** Ensure that your Firewall has our DNS sites allowed as well. Those sites are as follows:
*.eagleeyenetworks.com
*.plumv.com
*.eencloud.com

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

Independent of the Eagle Eye Bridge/CMVR, the Eagle Eye Web Interface 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 as follows:

| | |
|---|---|
| tcp/80 | # HTTP->SSL Redirect Only |
| tcp/443 | # Web user interface |
| tcp/50000-60000 | # Secure video transfer |

**Note:** The IPs are generally the same as for the Bridge/CMVR.

## Outbound Ports for Eagle Eye Camera Direct

Camera Direct (the direct-to-cloud solution that eliminates the need for a Bridge/CMVR) uses the following TCP ports. All connections are outbound-only, meaning that connections are outbound and never accept 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 discover video termination endpoints in the cloud |
| 8181/TCP | # Used to transfer video to the cloud |

## Subnets for Eagle Eye Camera Direct

Camera Direct utilizes the following subnets. Apart from these, the IP addresses which are used by “Outbound IPs for Eagle Eye Bridge/CMVR” also need to be allowed.

dispatch1v1.eagleeyenetworks.com (167.248.134.73)
dispatch2v1.cameramanager.com (167.248.135.100)
dispatch2v1.eagleeyenetworks.com (167.248.135.100)
192.40.4.124
192.40.5.26

**Note:** Eagle Eye utilizes the 2.centos.pool.ntp.org server for NTP — usually through port 223, as is the standard.