Eagle Eye Application Note – AN0029

Adjusting Camera Settings Through Camera Tunnels

2023-03-03 Revision 1.0

Target Audience

This Application Note is intended for administrators of the Eagle Eye Cloud VMS that have a need to adjust camera settings which aren't available directly from the browser interface of the VMS and want to learn how this is securely accomplished using camera tunneling.

Feature Overview

There may be the occasional need to modify camera level features directly in the camera browser. In order to do this securely - either locally or remotely - a direct tunnel into the camera is required. The Eagle Eye VMS has the ability to tunnel directly into a camera's web interface to make changes to the camera that may not currently be supported by the Eagle Eye Cloud VMS directly.

Theory of Operation

Use a VPN connection via SSH Tunneling to access your Camera Web interface in a secure way. SSH (Secure Shell) is a protocol that allows you to access a remote host. SSH is a cryptographic network protocol for operating network services securely over an unsecured network and one of its most notable applications is remotely logging in via secure method.

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 and configure settings.

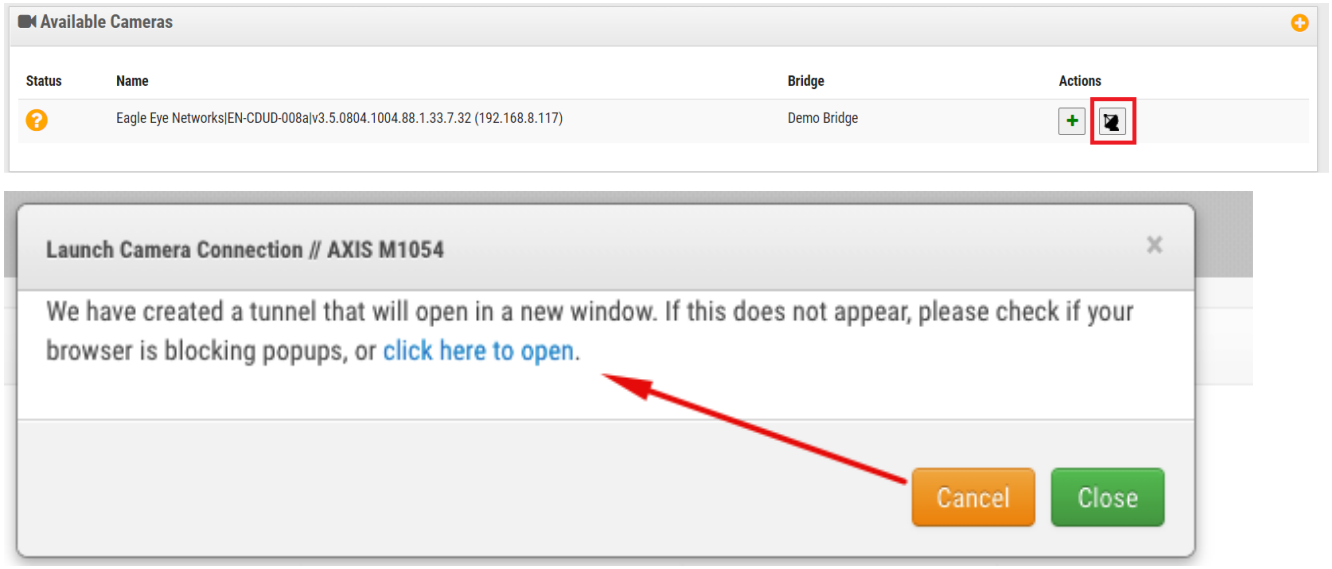
The ports required for this are as follows:

```
tcp/80      # HTTP -> SSL Redirect Only
tcp/443     # Web user interface
```

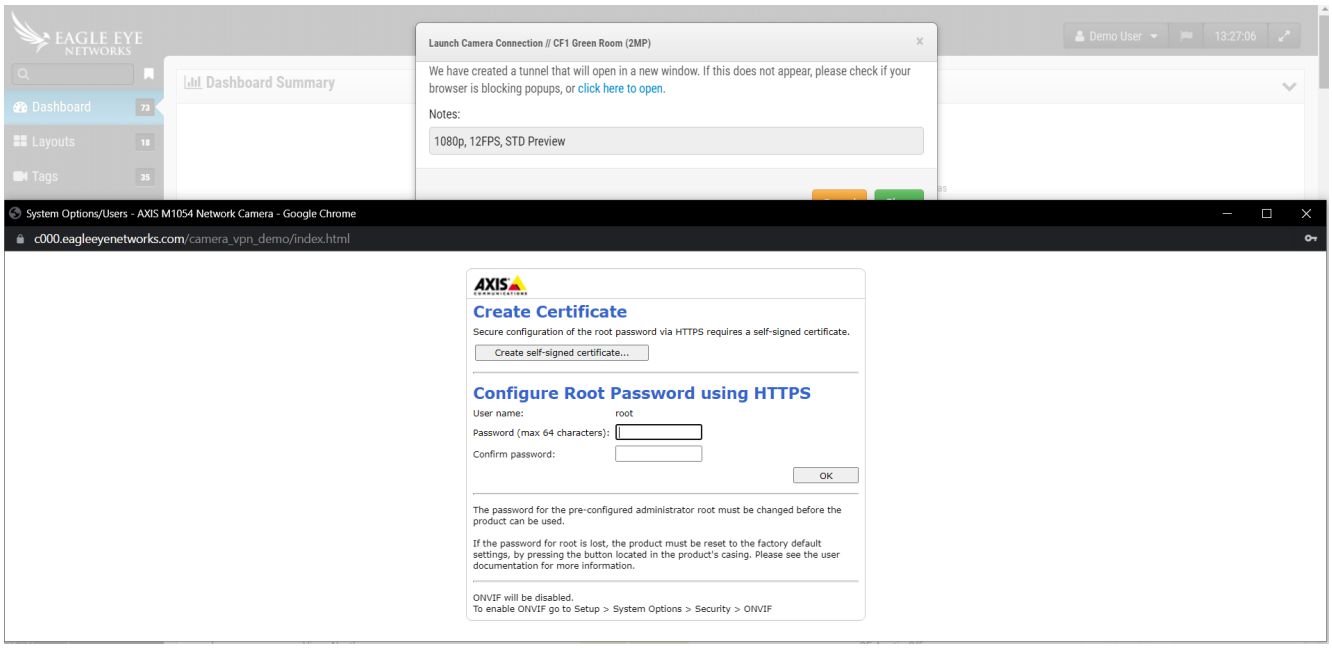
tcp/50000-60000 # Secure video transfer
The IPs are generally the same as for the bridge; Tunneling a Camera will require tcp/50000-60000 to be allowed or opened on the local Firewall as outbound traffic. A random port within the 50000 to 60000 range will be opened upon initiation of the Camera Tunnel.

Functionality

The Bridge/CMVR will do auto-discovery for all the cameras connected to the CAMLAN port as this port serves as a DHCP server for the devices connected to it.
To open a VPN tunnel to the camera and to login to the Camera Web Interface, click on the Satellite icon under “Actions” and enter the associated credentials as shown below:

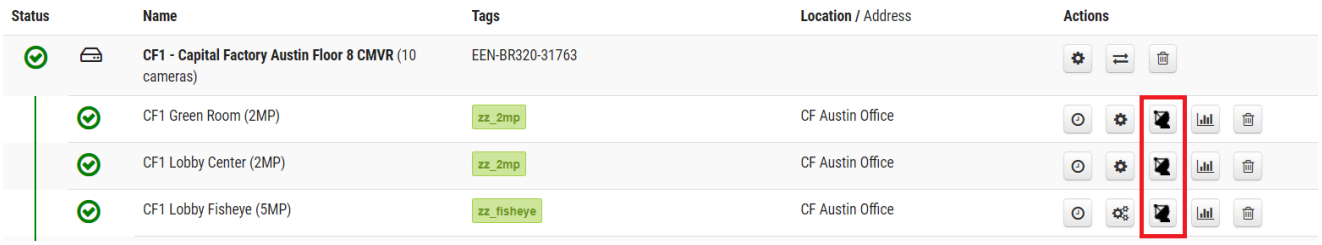


Clicking on the Satellite icon will pop-up the Launch Camera Connection window.



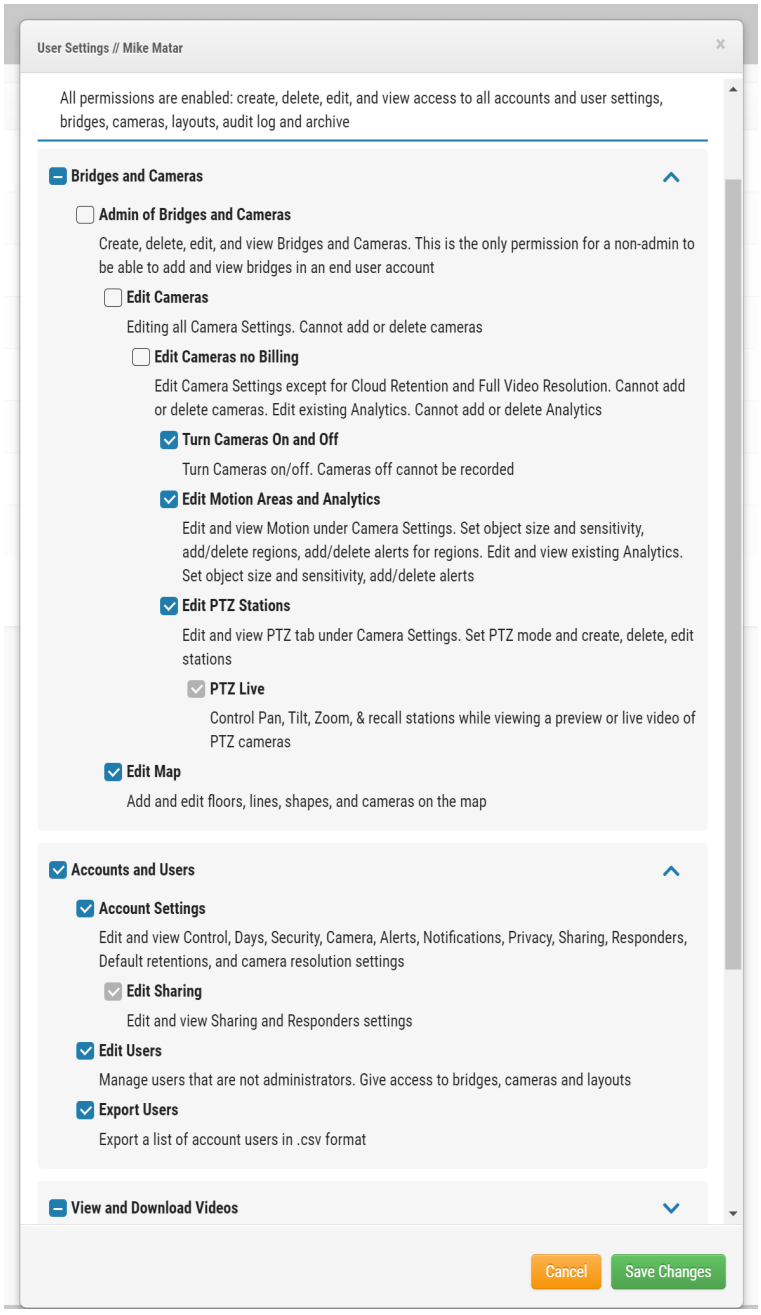
Example image of a camera manufacturer's camera configuration page.

Note that even after the camera has been added to the Bridge, the satellite icon will always be shown next to the Settings icon in the device tree and as can be seen below:



Administrators, as well as Operators with permissions enabled for “Admin of Bridges and Cameras”, “Edit Cameras” and “Edit Cameras No Billing” are all able to tunnel into a camera.

To Disable the Satellite Icon on the Operator Page, go to the Users tab and Change User Settings. Under the Permission tab, make sure permissions are unselected as below:



This results in the disappearance of Satellite Icon on the Dashboard under Actions. This effectively disables accessing the Camera Web Interface page:

Application

Tunneling into the camera allows Administrators to remotely access a Camera Web Interface securely without the need of be on-site to perform advanced configuration on the camera web-page :

- Create an Onvif User
- Assign Cameras an IP address
- Check Camera Logs
- Adjust Camera Parameters and settings

Tunneling into Cameras is possible for linked Cameras to a Bridge/CMVR and even for auto-discovered Cameras within the VMS

Click on the satellite icon of the first camera to see a tunnel setup to the camera. Close the window after you see it and close the dialog box.