VK2 IP Cameras: Applying SSL Certificates and HTTPS for Security

VISTA KNOWLEDGE BASE

INTRODUCTION

Default web browser (and NVR recorder) access to VK2 cameras uses the HTTP protocol via port 80 sending clear text login IDs and passwords passing over the network. To increase security, and confidence for those users web browsing to any IP camera direct, you can enable HTTPS to encrypte the login and also upload an SSL Security Certificate to the camera.

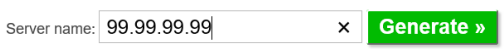
Note: setting an IP camera to use HTTPS may prevent it from streaming and recording video to your NVR\VMS if the recorder does not support HTTPS itself! At present, Vista NVR recorders do not support HTTPS.

OBTAINING A CERTIFICATE AND CONVERTING TO .PEM

There are many SSL Certificate types (covering these is outside the scope of this document), but you need to initially determine which of below you are to use on the IP camera;

1. **Self-signed SSL Certificate** - generally available for free by simply Googling "*generate free SSL certificate*". Usually a single Certificate protecting a single IP device\camera via the fully qualified domain name that you use to access the camera – for example *mycamera.mydomain.com*. Considered "less trustworthy" due to the fact that anyone can create and use one!

Note: when registering a self-signed SSL Certificate, enter the hostname or IP address (below examples) that you intend to use in your web browsers address bar when accessing the camera! The SSL Certificate will be encrypted to this server name and only valid when using this same name in your browser!



2. **Trusted SSL Certificate** – purchased from a company such as GlobalSign etc. After passing satisfactory security auditing of your company's details, a certificate is issued. Can purchase anything from a single host certificate (*mycamera.mydomain.com*) to one that protects all devices under your domain name (*mydomain.com*). Trusted Certificates are the most trustworthy for Internet users. An end-user's IT department may be able to advise if an SSL Certificate of theirs can be utilised.

Note: VK2 cameras only accept single-file *.pem* Certificate files! Do not attempt to upload a two-part Certificate via *.cert* or *.key* files – the camera will be rendered inoperative requiring factory defaulting! Convert to *.pem*!

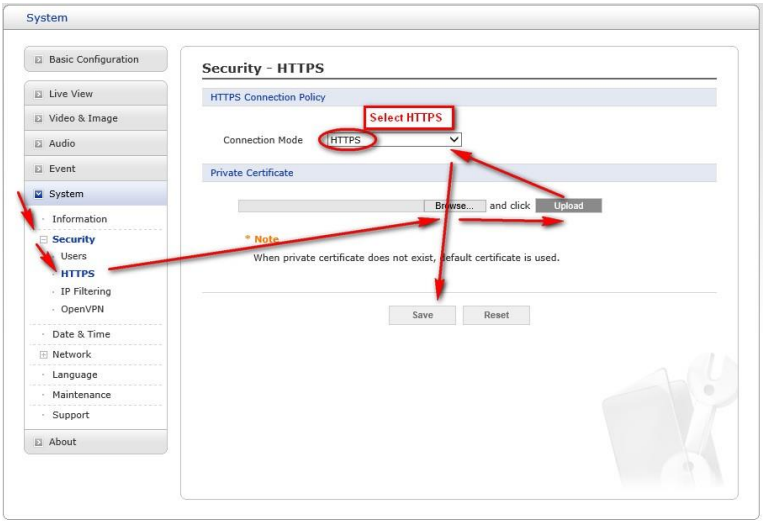
CONVERT CERTIFICATE FILES TO .PEM

Once you have the two ***.cert*** and ***.key*** files that make up a normal Certificate, you will need to convert them to a single ***.pem*** file. To do this, simply use any of the free conversion websites that can be found via a Google search for "***convert .cert to .pem***".

Once you have downloaded the .pem file, then continue to the next section to upload to the camera etc.

CONFIGURE IP CAMERA & UPLOAD SSL CERTIFICATE

1. Using a laptop or PC on an IP network with access to the IP camera, open a web browser and enter the IP address to connect to the camera;
2. Click the Setup icon and login using the admin ID and password rellevant for your camera
3. Refer to the example below and click menu **System** >> **Security** >> **HTTPS**
4. Click [Browse] and select the single ***.pem*** file that you converted earlier for you SSL Certificate
5. Click [Upload]



6. Next, select the [Connection Mode] drop-down box and select HTTPS only.
7. Click [Save]

From now on, connectivity to the IP camera can only be carried out via HTTPS.

Close your browser, and reconnect specifying https: in the browser, ie ***https://myipcamera.mydomain.com***

If your SSL Certificate is self-signed, you may first receive a security prompt warning the site is "not trusted". Simply click to "Accept the risk and connect anyway".

This ends the procedure