



Setting Up an HTTPS Certificate for the VMAX® IP Plus™

Affected Roles: Administrator, Owner

Related Digital Watchdog VMS Apps: VMAX® Web Viewer

Complexity: Medium

Firmware Version: VMAX® IP Plus™ firmware v1.4.1.1 or newer

Last Edit: April 22, 2021

Hypertext Transfer Protocol Secure (HTTPS)

The VMAX® IP Plus™ recording unit can now be used to self-generate and implement a Hypertext Transfer Protocol Secure (HTTPS) Certificate to better protect user information and user connections. By combining the Hypertext Transfer Protocol (HTTP) and Secure Socket Layer (SSL) technology, the VMAX® unit can be set up to run device and user information through a cryptographic hash function to obscure user logins, video streams, network information, and etc. from potentially malicious actors.

This article will outline the difference between a purchased HTTPS Certificate compared to a self-generated HTTPS Certificate, how to create a self-generated certificate, and how to import a purchased certificate to set up an HTTPS connection for a VMAX® IP Plus™.

Related Material

- CCIP Encryption – [Encrypting RTSP Streams for VMAX IP Plus](#)

Supported/Affected Devices:

- VMAX® IP Plus™ Series

Cryptographic Hashing

The HTTPS function of the VMAX® IP Plus™ combines the Hypertext Transfer Protocol (HTTP) and Secure Socket Layers (SSL) to encrypt and decrypt information, such as digital signatures and authentication codes, typically between a server and a browser. By utilizing an SHA-256 (256-bit) algorithm when creating cryptographic hash, strings of data are converted into a fixed hexadecimal code of 64-character or more.

As a result, information that is run through this engine is computed quickly and can be authenticated by the sending node prior to transmitting the message.

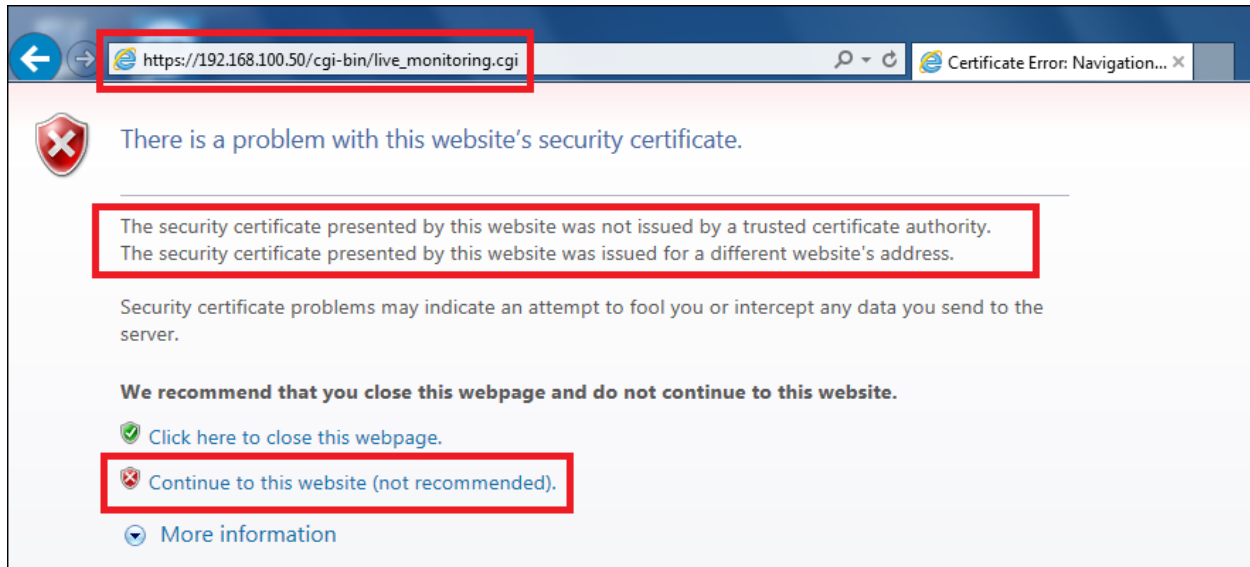
If the receiving node attempts to decode the encrypted hash, and any changes were made during the transmission by a malicious actor, the received information would differ from the original hash (encrypted code) and would not be authenticated by the system. Additionally, the malicious actor would not be able to decode the encrypted information without the encryption key data that was created when the VMAX® signed the certificate. This considerably mitigates the possibility of unwanted interception of data.

Self-Generated VS Purchased Certificates

The primary difference between a certificate that was purchased from a certificate authority and a Self-Generated Certificate that was created by the VMAX unit itself is in how a connecting web browser is likely to respond.

A certificate that was purchased from a widely recognized certificate authority of HTTPS Certificates will be accepted by most web browsers. However, a Self-Generated Certificate that was created through the device (in this case, a VMAX® unit), will be flagged by a browser and will display a warning as the certificate “was not issued by a trusted certificate authority”.

Despite the fact that a self-generated HTTPS Certificate will not be recognized as being issued by a certificate authority, the SHA 256-bit encryption of a self-generated certificate is just as secure as a purchased certificate. If you encounter this message after setting up the HTTPS connection, simply continue to the website.



Creating Self-Generated HTTPS Certificates

The VMAX® IP Plus™ recording unit is capable of self-generating an HTTPS Certificate from either directly at the recording unit itself or through the VMAX® Web Viewer using a web browser.

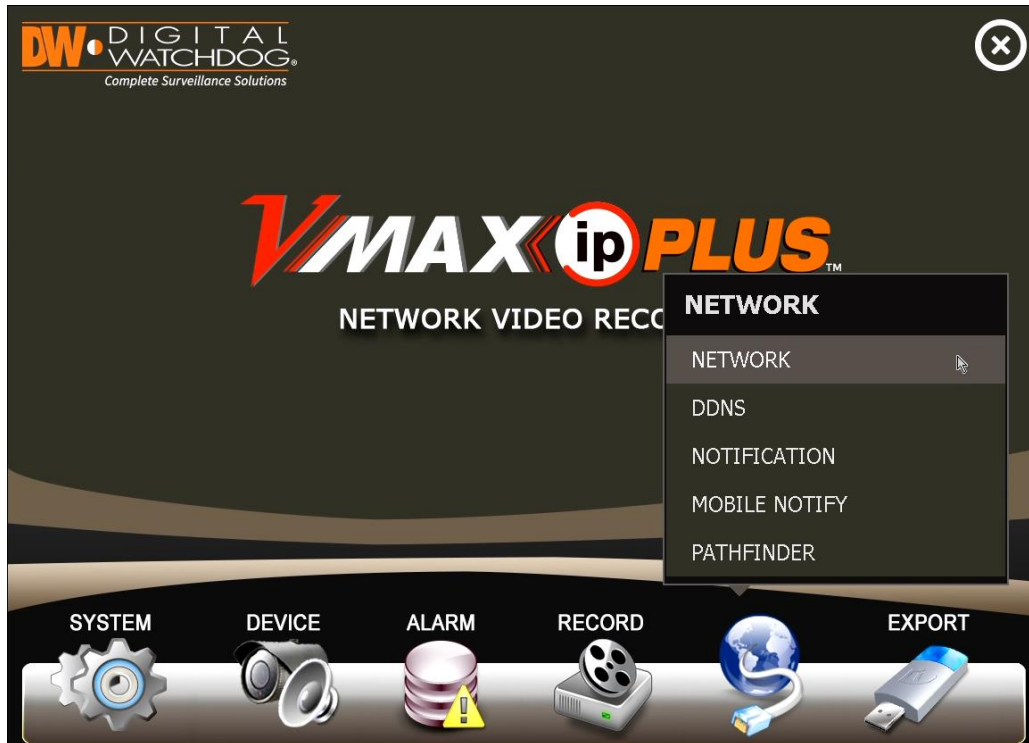
****NOTE:** The time zone of the recording unit must be set up before generating a certificate. The time setting for both the NVR and NTP server must match. Otherwise, skipping this step may impact the validity of the generated certificate and the application time may vary. Please consult your User Manual for *System Information* setup.

Self-Generating Certificates at the Recorder

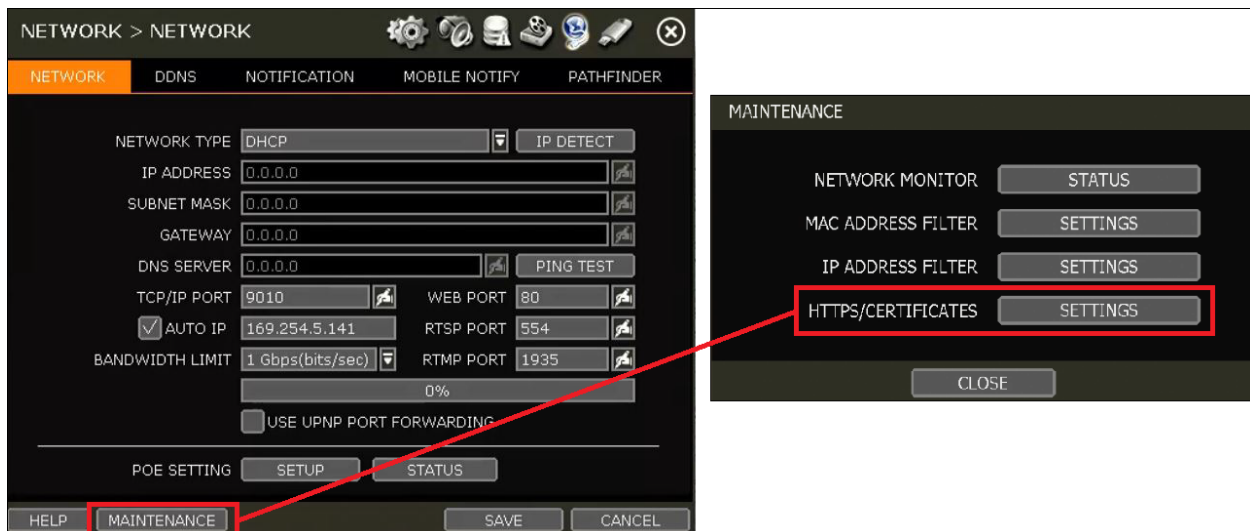
To create a self-generated HTTP Certificate directly at the VMAX® recorder:

- 1) At the recording unit, log in as the Administrator.
 - **Default ID:** admin
 - **Default PW:** <no password>
- 2) Once you have logged in as the Administrator, **right-click** with the mouse and select **Menu** from the displaying context menu.

The Setup Menu will display. Click on **Network**, then select the **Network** menu.



3) In the Network menu, click the **Maintenance** button, then select **HTTPS/Certificates**.

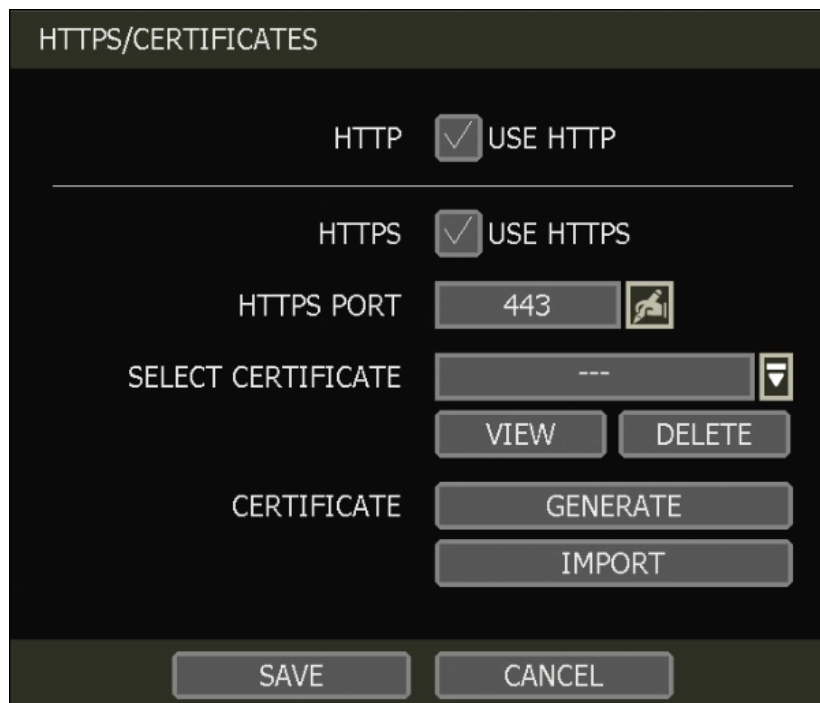


4) The **HTTPS/Certificate** menu will display.

Enable the **Use HTTPS** setting. By default, the **HTTPS Port** will be set to **Port 443**. If needed, change the *HTTPS Port* value.

To self-generate an HTTPS Certificate using the VMAX® recorder, click the **Generate** button.

****NOTE:** The *HTTPS Port* value cannot use the same port number as another device on the LAN.



The screenshot shows a configuration window titled "HTTPS/CERTIFICATES". It has a dark background with light-colored text and controls. At the top, there is a section for "HTTP" with a checked checkbox labeled "USE HTTP". Below this is a section for "HTTPS" with a checked checkbox labeled "USE HTTPS". Under the "HTTPS" section, there is a "HTTPS PORT" field with the value "443" and a small icon to its right. Below the port field is a "SELECT CERTIFICATE" field with a dropdown menu showing "---" and a small icon to its right. Below the dropdown are two buttons: "VIEW" and "DELETE". Below these are two buttons: "GENERATE" and "IMPORT". At the bottom of the window are two buttons: "SAVE" and "CANCEL".

- 5) To create a self-generated HTTPS Certificate through the VMAX®, **complete the registration form.**

The fields with an asterisk (*) are mandatory. The more information that is provided in the form, the more secure the certificate authentication will be.

Configure the following information:

- *** Certificate Name** – enter a name or label to identify the certificate by. Do not use spaces. The use of lowercase letters, uppercase letters, numbers, and special characters are permitted.

- *** Validity (Days)** – set the amount of time (in days) that the certificate will be valid. By default, the *Validity* will be set to 365 days, but can be increased or decreased as needed.
- *** Country** – enter the abbreviation of the location. For example, “United States” would be “US”.
- **State or Province** – enter the abbreviation of the State or Province of the location. For example, “California” would be “CA”.
- **Locality** – enter the name of the city of the location.
- **Organization** – enter a company name.
- **Organization unit** – enter a company department.
- *** Common Name** – by default, the IP Address of the recording unit will be used. If a DNS server will be used when connecting, you can enter the common identifier here. For example, the domain of “digital-watchdog.com” can be used when connecting through HTTPS if it was registered on the DNS server and is specified in the HTTPS Certification form during self-generation.
- **RSA** – this represents the level of security for the public-key cryptography algorithm. By default, the RSA is set to 4096-bit encryption and cannot be changed.
- **SHA** – this represents the level of security for the Secure Hash Algorithm (SHA) that is used for hashing data and certificate files. By default, the SHA is set to 256-bit encryption and cannot be changed.
- **Alternative Hostname 1** – enter the alternate domain or host for this certificate. For example, “.digital-watchdog.local” can be used if the domain has been registered on a DNS server.
- **Alternative Hostname 2** – enter an alternate domain or host for this certificate.
- *** Alternative IP** – by default, the *Alternative IP* is set to the IP Address of the NVR. You can enter the Public IP Address of the network here to use an HTTPS connection when connecting over WAN.

HTTPS/CERTIFICATES

CERTIFICATE NAME *

VPPlus

VALIDITY(DAYS) *

365

COUNTRY *

US

STATE OR PROVINCE

CA

LOCALITY

Cerritos

ORGANIZATION

Digital Watchdog

ORGANIZATION UNIT

Support

COMMON NAME *

192.168.100.50

RSA

4096

SHA

256

ALTERNATIVE HOSTNAME 1

digital-watchdog.c...

ALTERNATIVE HOSTNAME 2

ALTERNATIVE IP *

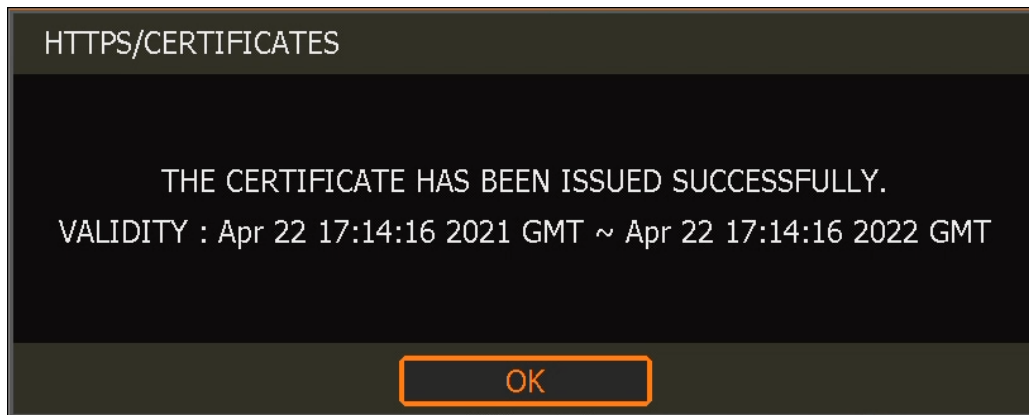
47.180.64.226

GENERATE

CLOSE

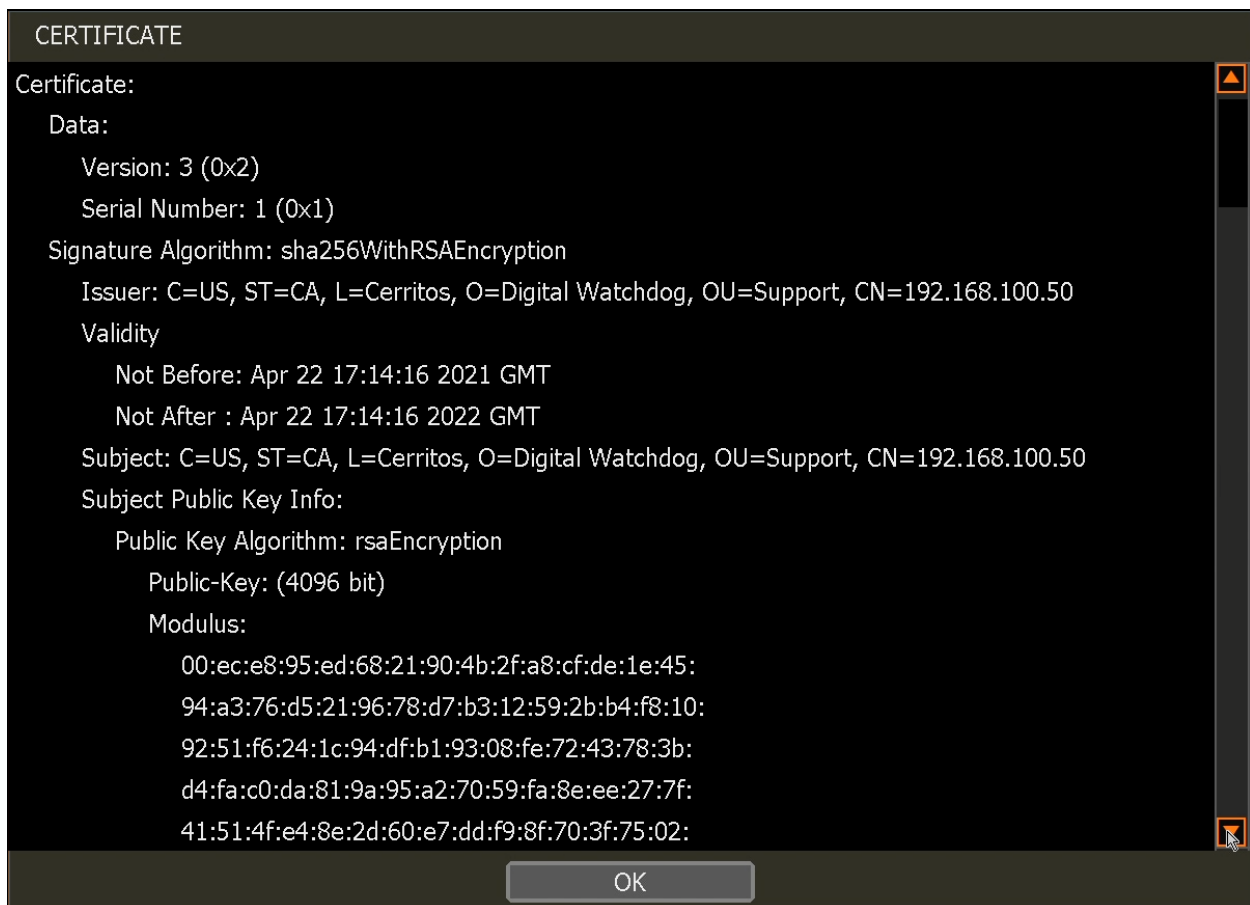
6) Once the registration form has been completed, click the **Generate** button. A confirmation message will display.

Click the **OK** button to close the confirmation message.



- 7) After generating the HTTPS Certificate, click on the **Select Certificate** box and **select the HTTPS Certificate**.

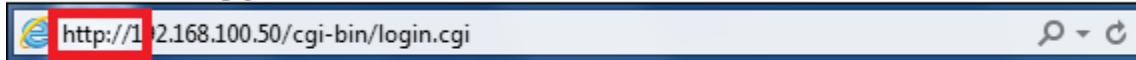
After selecting the certificate, click the **View** button to view the certificate and the encryption.



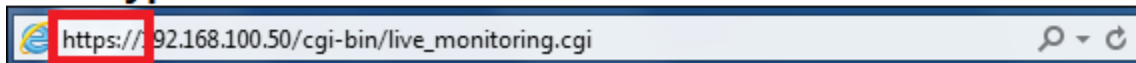
- 8) When you are finished, click the **Save** button to apply the HTTPS Certificate to the VMAX® unit.

The VMAX® IP Plus™ can now be securely connected with using an HTTPS connection. When connecting using a web browser, be sure to enter “https://” before entering the IP address or URL of the recording unit to use the secure HTTPS connection.

Non-Encrypted HTTP Connection



Encrypted HTTPS Connection



Self-Generating Certificates with Web Viewer

To create a self-generated HTTP Certificate using the VMAX® Web Viewer:

- 1) Open a **web browser** and connect with the VMAX® IP Plus™ **Web Viewer**.

Log in as the Administrator of the VMAX® unit.

- **Default User ID:** admin
- **Default User PW:** <no password>



- 2) Once you have logged in as the Administrator, click the **Setup** button to access the settings.

From the *Setup* menus, click on the **Network** tab, then select **Certificate Generation**.

The screenshot shows the Digital Watchdog VMAX Web Viewer interface. The browser address bar displays `http://192.168.100.50/cgi-bin/setup.cgi`. The top navigation bar includes tabs for **LIVE MONITORING**, **PLAY**, and **SETUP** (highlighted with a red box). To the right of the tabs are links for **QSG**, **Manual**, **FAQ**, and **Support**, along with a user profile for **admin** and a **Logout** button. On the left sidebar, the **NETWORK** menu item is highlighted with a red box, and its sub-menu **CERTIFICATE GENERATION** is also highlighted with a red box. A red arrow points from this sub-menu to the main content area. The main content area is titled **CERTIFICATE GENERATION** and contains a form with the following fields: **CERTIFICATE NAME** (text input), **VALIDITY (DAYS)** (text input with value 365), **COUNTRY** (text input with value US), **STATE OR PROVINCE** (text input), **LOCALITY** (text input), **ORGANIZATION** (text input), **ORGANIZATION UNIT** (text input), **COMMON NAME** (text input with value 192.168.100.50), **RSA** (text input with value 4096), **SHA** (text input with value 256), **ALTERNATIVE HOSTNAME 1** (text input), **ALTERNATIVE HOSTNAME 2** (text input), and **ALTERNATIVE IP** (text input with value 192.168.100.50). At the bottom of the form is a **GENERATE** button.

- 3) The *Certificate Generation* menu will display.

To create a self-generated HTTPS Certificate through the VMAX® Web Viewer, **complete the registration form**.

The fields with an asterisk (*) are mandatory. The more information that is provided in the form, the more secure the certificate authentication will be.

Configure the following information:

- *** Certificate Name** – enter a name or label to identify the certificate by. Do not use spaces. The use of lowercase letters, uppercase letters, numbers, and special characters are permitted.
- *** Validity (Days)** – set the amount of time (in days) that the certificate will be valid. By default, the *Validity* will be set to 365 days, but can be increased or decreased as needed.

- *** Country** – enter the abbreviation of the location. For example, “United States” would be “US”.
- **State or Province** – enter the abbreviation of the State or Province of the location. For example, “California” would be “CA”.
- **Locality** – enter the name of the city of the location.
- **Organization** – enter a company name.
- **Organization unit** – enter a company department.
- *** Common Name** – by default, the IP Address of the recording unit will be used. If a DNS server will be used when connecting, you can enter the common identifier here. For example, the domain of “*digital-watchdog.com” can be used when connecting through HTTPS if it was registered on the DNS server and is specified in the HTTPS Certification form during self-generation.
- **RSA** – this represents the level of security for the public-key cryptography algorithm. By default, the *RSA* is set to 4096-bit encryption and cannot be changed.
- **SHA** – this represents the level of security for the Secure Hash Algorithm (SHA) that is used for hashing data and certificate files. By default, the *SHA* is set to 256-bit encryption and cannot be changed.
- **Alternative Hostname 1** – enter the alternate domain or host for this certificate. For example, “.digital-watchdog.local” can be used if the domain has been registered on a DNS server.
- **Alternative Hostname 2** – enter an alternate domain or host for this certificate.
- *** Alternative IP** – by default, the *Alternative IP* is set to the IP Address of the NVR. You can enter the Public IP Address of the network here to use an HTTPS connection when connecting over WAN.

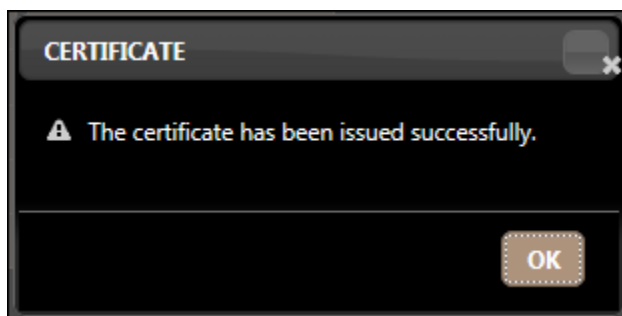
The screenshot shows the Digital Watchdog Setup web interface. The browser address bar displays `http://192.168.100.50/cgi-bin/setup.cgi`. The interface has a top navigation bar with tabs for **LIVE MONITORING**, **PLAY**, and **SETUP** (which is active). To the right of the tabs are links for **QSG**, **Manual**, **FAQ**, and **Support**, along with a user profile for **admin** and a **Logout** button. A left sidebar contains a menu with categories: **SYSTEM** (expanded), **DEVICE**, **EVENT**, **RECORD**, **NETWORK**, and **LOG**. Under **SYSTEM**, there are sub-items: **SYSTEM STATUS**, **INFORMATION**, **USER**, **DISPLAY**, **HDD**, **UPGRADE**, and **CONFIGURATION**. The main content area is titled **CERTIFICATE GENERATION** and contains a form with the following fields:

CERTIFICATE NAME	VPPlus
VALIDITY (DAYS)	365
COUNTRY	US
STATE OR PROVINCE	CA
LOCALITY	Cerritos
ORGANIZATION	Digital Watchdog
ORGANIZATION UNIT	Support
COMMON NAME	192.168.100.50
RSA	4096
SHA	256
ALTERNATIVE HOSTNAME 1	digital-watchdog.local
ALTERNATIVE HOSTNAME 2	
ALTERNATIVE IP	47.180.64.226

At the bottom of the form is a **GENERATE** button.

- 4) Once the registration form has been completed, click the **Generate** button. A confirmation message will display.

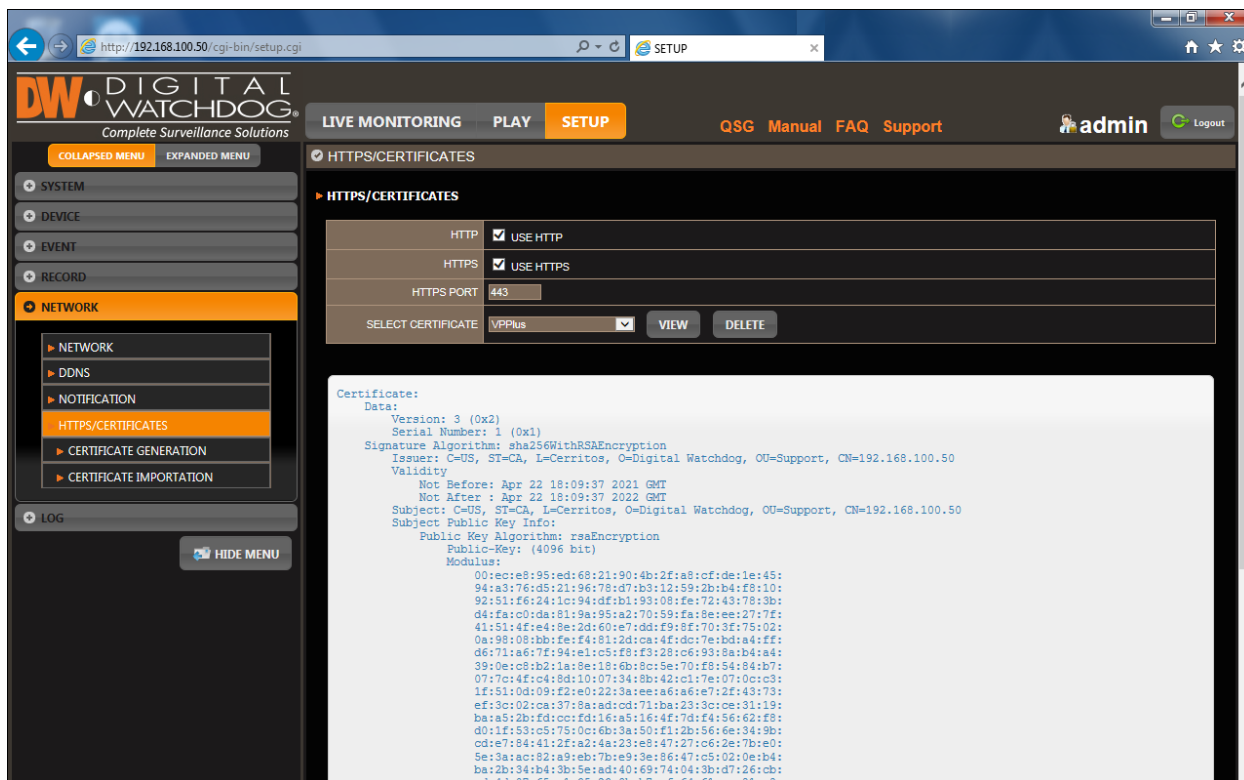
Click the **OK** button to close the message.



- 5) After generating the HTTPS Certificate, click on the **HTTPS/Certificates** tab.

Click on the **Select Certificate** box and **select the HTTPS Certificate**.

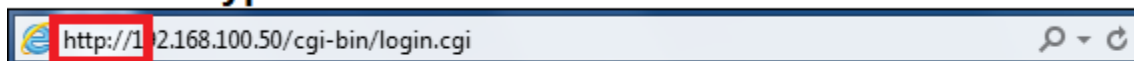
Click the **View** button to view the certificate and the encryption.



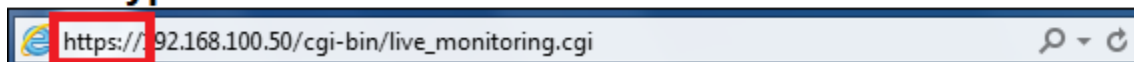
- 6) When you are finished, click the **Save** button to apply the HTTPS Certificate to the VMAX® unit.

The VMAX® IP Plus™ can now be securely connected with using an HTTPS connection. When connecting using a web browser, be sure to enter “**https://**” before entering the IP address or URL of the recording unit to use the secure HTTPS connection.

Non-Encrypted HTTP Connection



Encrypted HTTPS Connection



Purchased HTTPS Certificates

Another way that an HTTPS Certificate can be obtained is by purchasing the material from a recognized seller. Purchased certificates that were imported to

a VMAX® IP Plus™ will automatically be recognized by a web browser when connecting through HTTPS.

The certificate file can be imported either directly at the recording unit itself or through the VMAX® Web Viewer.

****NOTE:** Importing an HTTPS Certificate directly at the VMAX® unit requires the use of a FAT32 USB stick. Any external storage device that is not formatted to FAT32 format will not be recognized by the standalone unit.

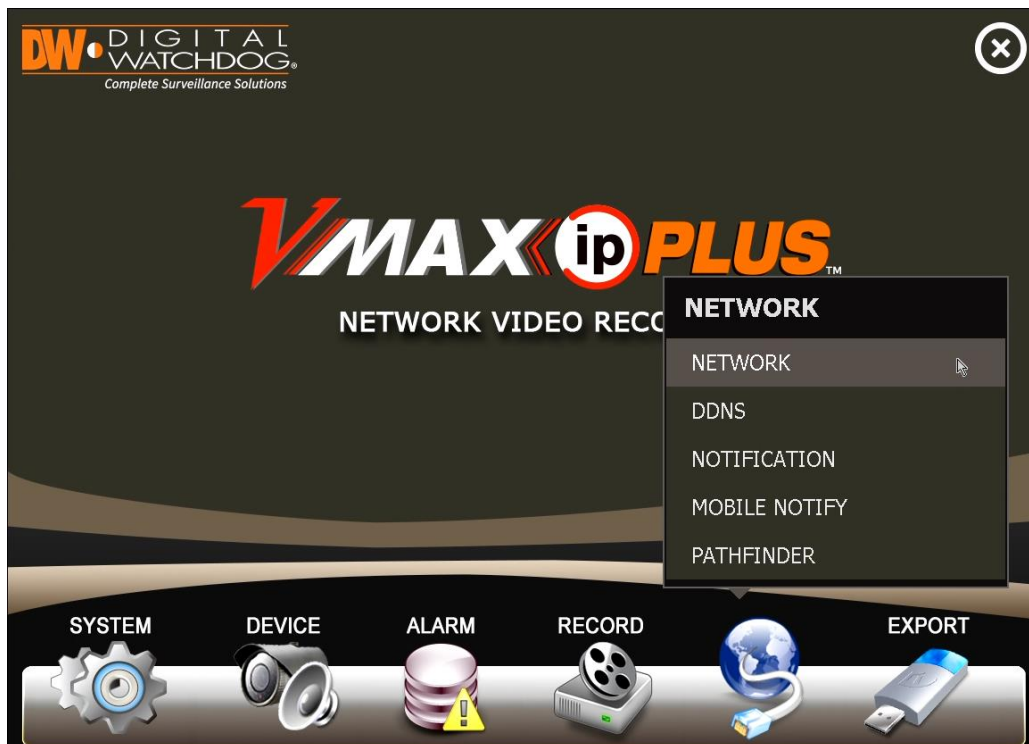
****NOTE:** All files that will imported directly at the recording unit must be placed in the root directory of the USB stick. If a file is stored in a folder, the VMAX® unit will not be able to access the file.

Importing Certificates at the Recorder

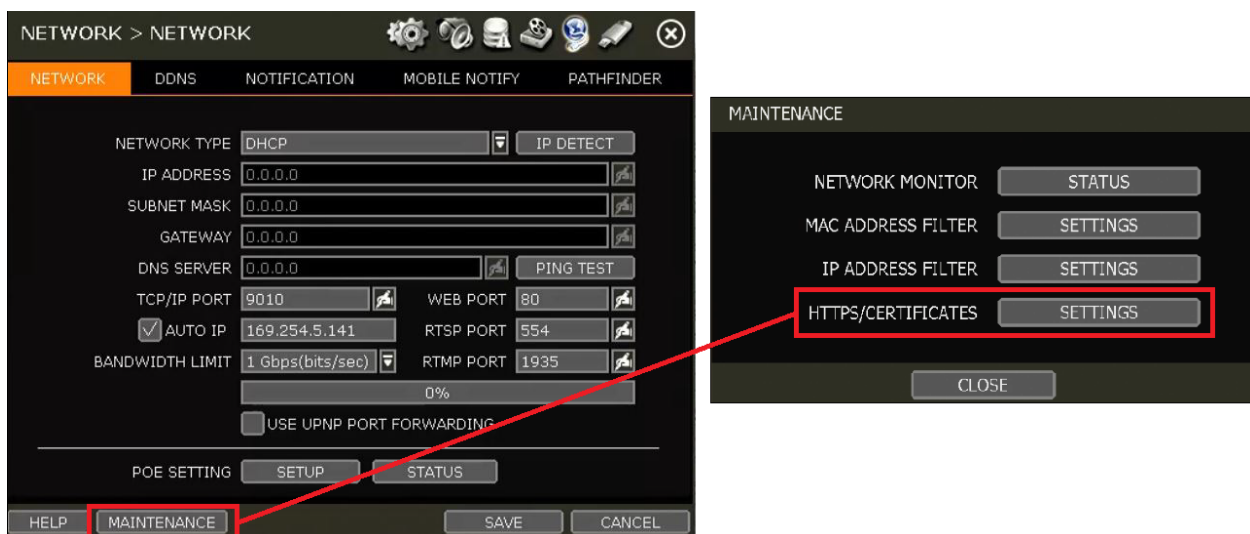
To import a purchased HTTP Certificate directly at the VMAX® recorder:

- 1) At the recording unit, log in as the Administrator.
 - **Default ID:** admin
 - **Default PW:** <no password>
- 2) Once you have logged in as the Administrator, **right-click** with the mouse and select **Menu** from the displaying context menu.

The *Setup Menu* will display. Click on **Network**, then select the **Network** menu.



- 3) In the *Network* menu, click the **Maintenance** button, then select **HTTPS/Certificates**.

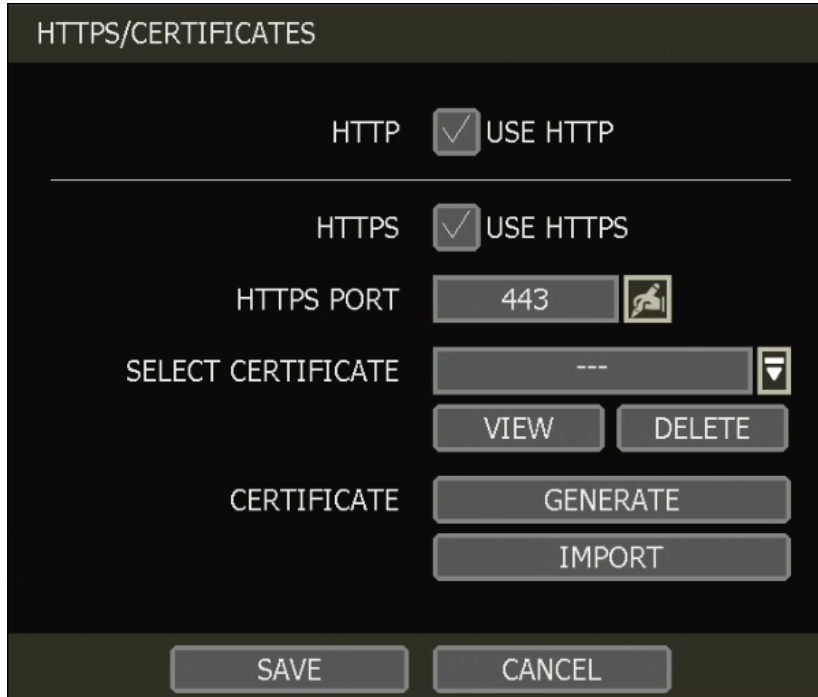


- 4) The *HTTPS/Certificate* menu will display.

Enable the **Use HTTPS** setting. By default, the **HTTPS Port** will be set to **Port 443**. If needed, change the *HTTPS Port* value.

To self-generate an HTTPS Certificate using the VMAX® recorder, click the **Import** button.


****NOTE:** The *HTTPS Port* value cannot use the same port number as another device on the LAN.




HTTPS/CERTIFICATES

HTTP ☒ USE HTTP

HTTPS ☒ USE HTTPS

HTTPS PORT 443 

SELECT CERTIFICATE --- 

VIEW DELETE

CERTIFICATE GENERATE

IMPORT

SAVE CANCEL


- 5) **Connect the FAT32 format USB stick** containing the HTTPS Certificate to the VMAX® unit. Enter the **Certificate** name, then click the **Scan** button.


Once the certificate file has been detected, select the **Type** of certificate file that will be imported, then click the **Import** button. A confirmation message will display.

Click the **OK** button to close the message.


****NOTE:** If the NVR does not detect the USB stick, make sure that the USB is using FAT32 format. Additionally, make sure that the file is not in a folder and is placed in the root directory of the USB stick.


HTTPS/CERTIFICATES - IMPORT

CERTIFICATE NAME 


IMPORT FROM 


TYPE ☐ PKCS#12 (pfx)

CERTIFICATE (.pfx) 


PASSWORD 

TYPE ☐ CRT + PRIVATE KEY

CERTIFICATE (.crt) 

PRIVATE KEY (.key) 

TYPE ☒ PEM (Privacy Enhanced Mail)

CERTIFICATE (.pem) 

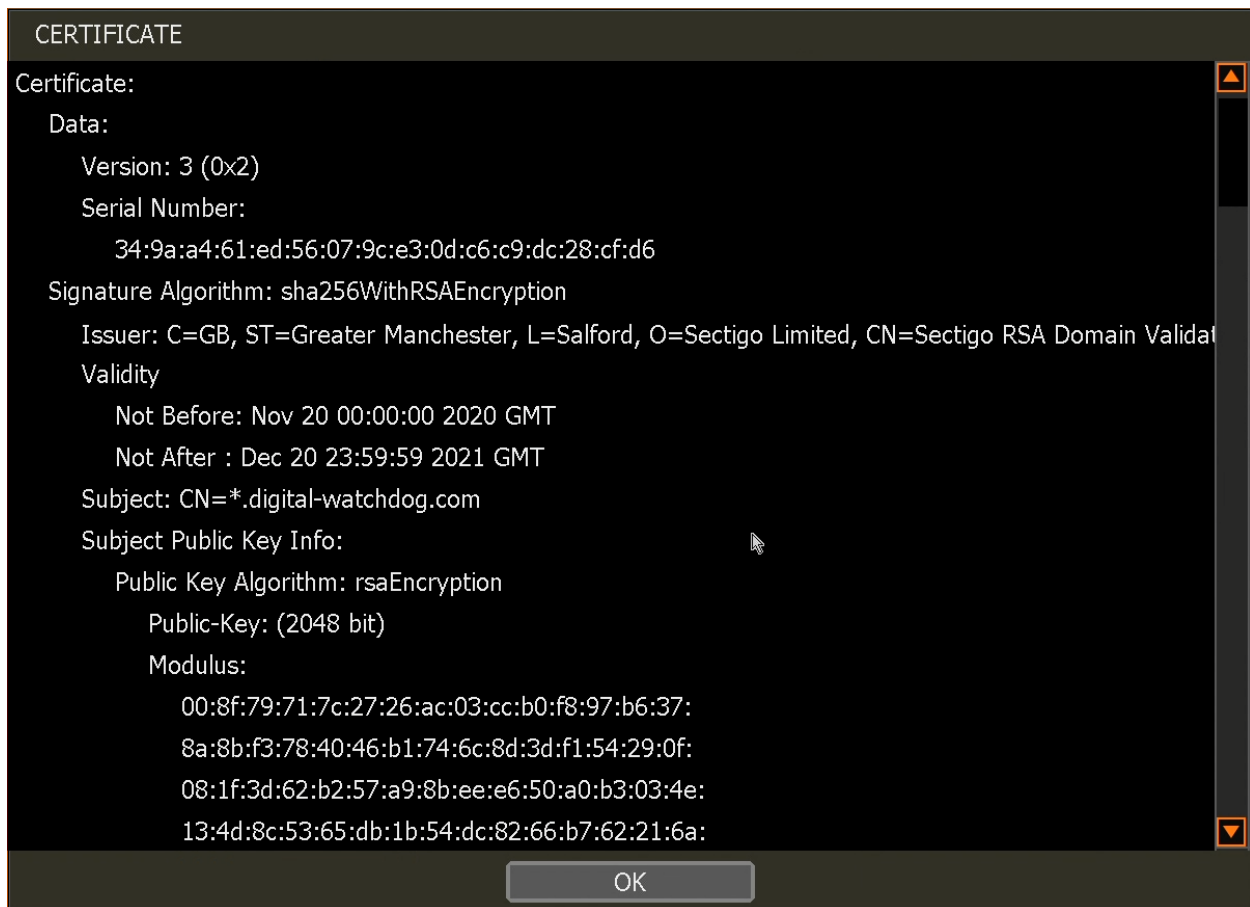
CERTIFICATE

THE CERTIFICATE WAS SUCCESSFULLY IMPORTED.
CERTIFICATE NAME: cert

6) Next, click the **Close** button to close the *Import* menu.

After importing the HTTPS Certificate, click on the **Select Certificate** box and **select the HTTPS Certificate**.

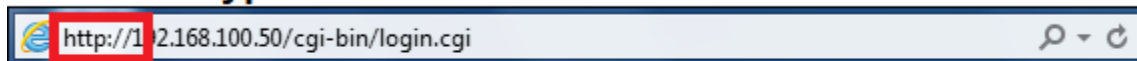
After selecting the certificate, click the **View** button to view the certificate and the encryption.



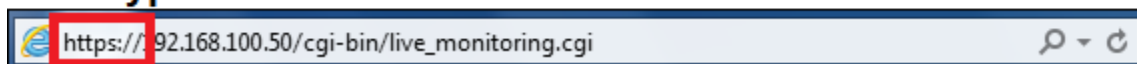
- 7) When you are finished, click the **Save** button to apply the HTTPS Certificate to the VMAX® unit.

The VMAX® IP Plus™ can now be securely connected with using an HTTPS connection. When connecting using a web browser, be sure to enter “**https://**” before entering the IP address or URL of the recording unit to use the secure HTTPS connection.

Non-Encrypted HTTP Connection



Encrypted HTTPS Connection



Importing Certificates with Web Viewer

To import an HTTP Certificate using the VMAX® Web Viewer:

1) Open a **web browser** and connect with the VMAX® IP Plus™ **Web Viewer**.

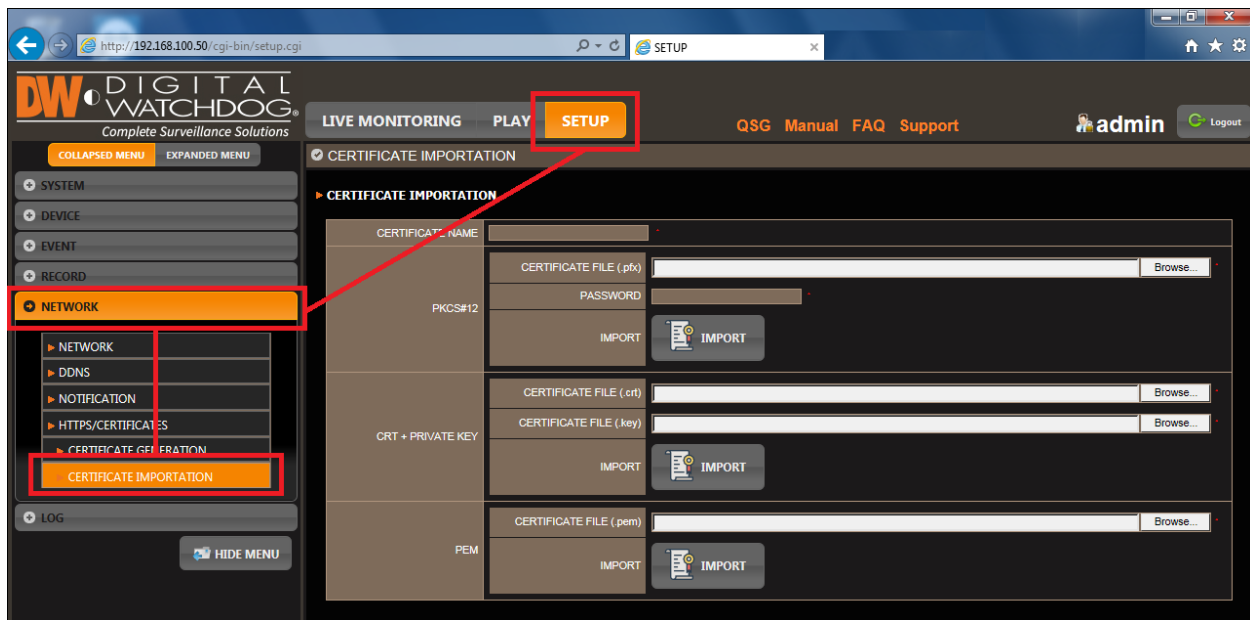
Log in as the Administrator of the VMAX® unit.

- **Default User ID:** admin
- **Default User PW:** <no password>



2) Once you have logged in as the Administrator, click the **Setup** button to access the settings.

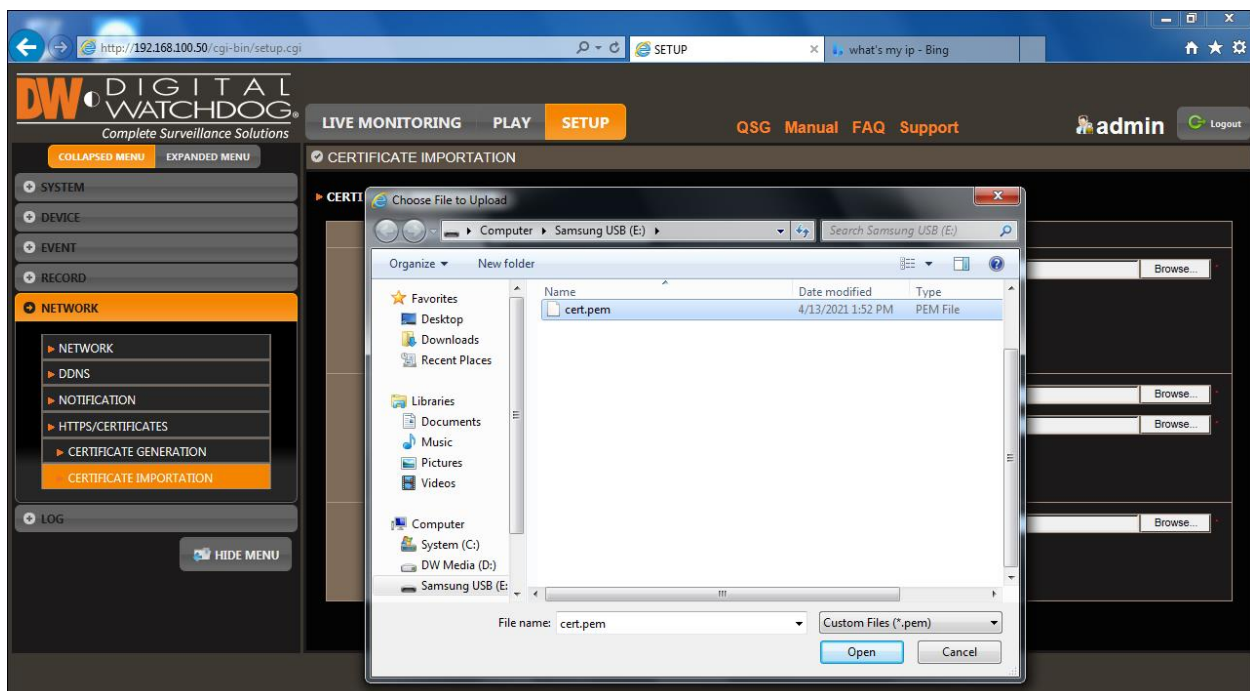
From the *Setup* menus, click on the **Network** tab, then select **Certificate Importation**.



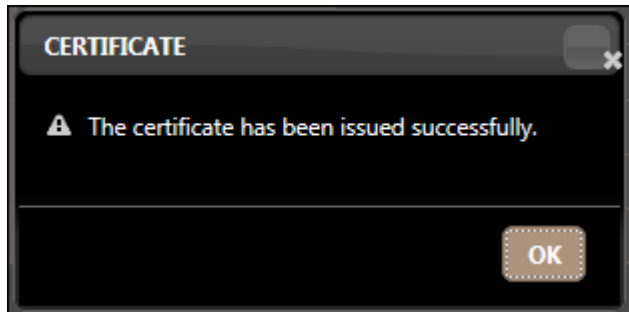
3) The *Certificate Importation* menu will display.

Click in the **Certificate Name** box and enter the name of the certificate.

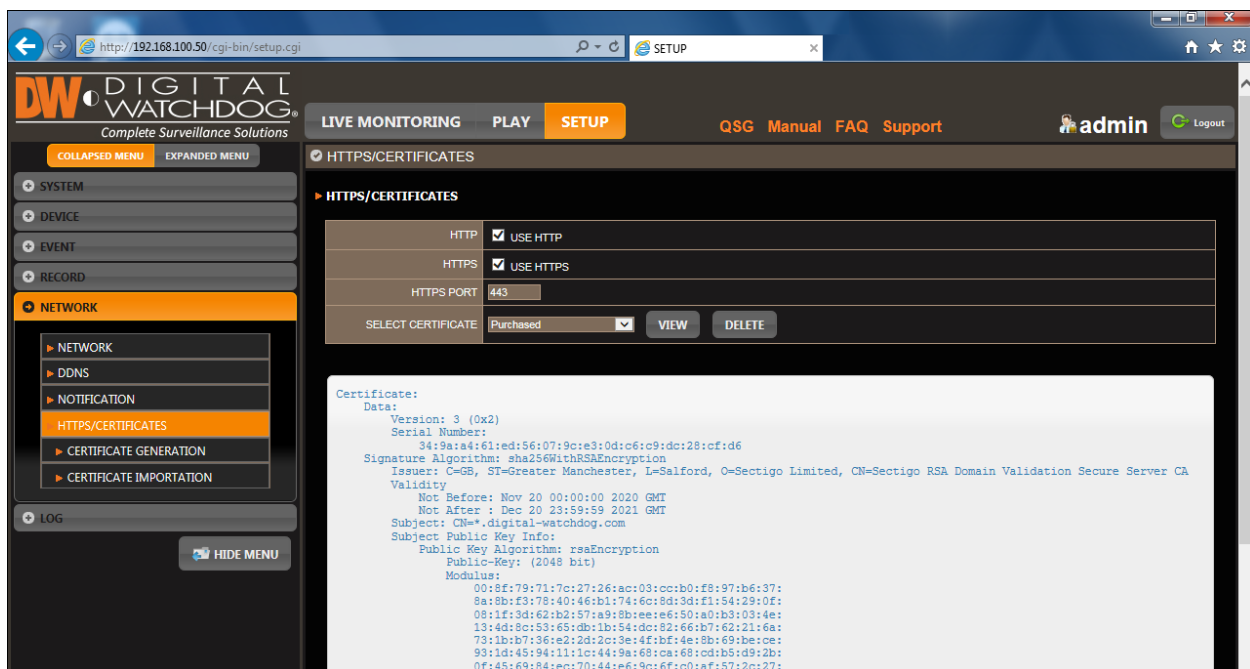
Next, click the **Browse** button and **select the certificate file** that needs to be imported.



- 4) Once the certificate file has been selected, click the **Import** button. A confirmation message will display.



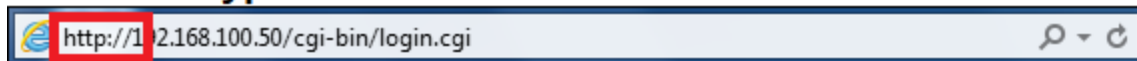
- 5) After importing the HTTPS Certificate, click on the **HTTPS/Certificates** tab. Click on the **Select Certificate** box and **select the HTTPS Certificate**. Click the **View** button to view the certificate and the encryption.



- 6) When you are finished, click the **Save** button to apply the HTTPS Certificate to the VMAX® unit.

The VMAX® IP Plus™ can now be securely connected with using an HTTPS connection. When connecting using a web browser, be sure to enter “**https://**” before entering the IP address or URL of the recording unit to use the secure HTTPS connection.

Non-Encrypted HTTP Connection



Encrypted HTTPS Connection

