So

Back

Ask a related question

Posted 3 years ago Last Activity 3 years ago

Trusted SSL Certificate Install

0 4 2k

HI All

Anyone have an step by step instructions for installing a trusted SSL in 3.9.8? I have the UVC-2TB NVR

Thanks

Responses (4)

M

mitchellve

3 years ago

Hi,

there is a guide => https://community.ui.com/questions/6f6648de-4f03-4ed0-ba49-5665b22e08e3

Regards,

Mitchell

0

J

jfoster17

Sign up Log in

button in their GUI, why does UBNT have so many different ways to install something so important. The UniFi video, UniFi WiFi, NVR, Airmax OS, and Aircontrol have different ways to install certificates.

1

A

ablamire99

3 years ago

must admit it does seem a very complicated process for a very trivial task. Spoken to support and their response was its not officially supported because "you can skip the warning and proceed" which is very unhelpful.

So

0

wharrgarbl

3 years ago

After rendering my install inoperable a few times and re-building/restoring, this is what ultimately worked for me.

This is on a Debian installation with a LetsEncrypt SSL Cert (that I generated from inside a Plesk control panel where I host my web site and exported - If you can swing a paid certificate to avoid having to do this process every 3 months for a LetsEncrypt cert I would reccommend it). The NVR is just running Debian so should work exactly the same way.

There are many ways and places to get the certificate. Biggest thing is you make sure you specify the DNS name (with the full fqdn of your server) when you create your CSR request it so you don't get warnings in Chrome.

I exported the entire certificate chain as a PEM file (just a plain text file with the base64 encoded certificate request, the private key, the actual certificate, and the CA's certificate listed in the file in that order). I'm assuming it will work with just the certificate and private key saved as separate PEM (or any extension as long as it's the plain text base64 encoded data) files if you are using a globally trusted certificate authority. Save your certificate or the full certificate chain PEM file as ufv-server.cert.pem

Save just your private key as ufv-server.key.pem (if you have a full chain PEM, edit the PEM file in a text editor, create a ufv-server.key.pem file with just the private key section)

Copy these two files to /tmp on the server (Use something like WinSCP, or just create them in SSH and paste the content into them)

From here you need to convert the certificate and key files to encoded der files and make Unifi recognize and use them.

From inside an SSH connection as root or SU to root, change to the tmp dir:

```
cd /tmp
```

then issue these commands.

```
service unifi-video stop
openssl x509 -outform der -in ufv-server.cert.pem -out ufv-server.cert.der
openssl pkcs8 -topk8 -inform PEM -outform DER -in ufv-server.key.pem -out ufv-server.key.der -nocrypt
mkdir -p /usr/lib/unifi-video/data/certificates
```

So

Edit the /usr/lib/unifi-video/data/system.properties file:

```
nano /usr/lib/unifi-video/data/system.properties
```

and add this line:

ufv.custom.certs.enable=true

Ctrl-X to save then exit.

Then

```
service unifi-video start
```

That should be it. The service should start and the URL will work with your certificate and without warnings.

If it breaks, there is probably something wonky with the certificate files. Just do this to have unifi re-generate the self-signed certs to revert to the way it was:

```
service unifi-video stop
rm -rf /usr/lib/unifi-video/data/keystore /usr/lib/unifi-video/data/ufv-truststore /usr/lib/unifi-video/conf/
rm -rf /usr/lib/unifi-video/data/certificates
service unifi-video start
```

Sure, the default self-signed certificate is secure enough to protect data, but having to click through the certificate warning every single time I access it, and not being able to save passwords because the browser does not like the certificate is beyond annoying. There is absolutely no reason why they cannot put this functionality in the web interface. Just need text boxes to paste in your certificate, key, and if needed CA data, validate with some openssl commands that you are using legitimate data, and execute the commands on the back end to convert the data, move some things around, update the config file, and restart the service. Maybe even add a utility to generate the CSR, and a button to undo and revert to self-signed. Heck, maybe even add the option to automatically generate a certificate from LetsEncrypt using certutil commands on the back end and keep it updated.

BTW... If you have the SDN controller running on the same box, just a few more steps and you can use the same cert to secure it.

So

Save just the certificate as UNIFI.CRT or use the PEM file name if you are using just the cert and not the chain) and do this (might be able to exclude the "-CAfile ufv-server.cert.pem" command if you have a globally trusted cert but I did not try it)

```
openssl pkcs12 -export -in UNIFI.CRT -inkey ufv-server.key.pem -out unifi.p12 -name unifi -CAfile ufv-server.

mv /var/lib/unifi/keystore /var/lib/unifi/keystore.backup

keytool -importkeystore -deststorepass aircontrolenterprise -destkeypass aircontrolenterprise -destkeystore /
```

1

Page 1