j0mbie
J 10 months ago

Posted 10 months ago Edited 10 months ago Last Activity 3 months ago

How to upload your own SSL certificate to a UniFi Protect NVR (2021-05-07)

Tags

UniFi

UniFi Protect

UniFi Video

I went through a great deal of trouble getting an SSL certificate on a new NVR, so I thought I would share to save anyone else the headaches. I tried a lot of different things, so hopefully I'm including all the correct necessary steps.

The first thing to note is that the old "keystore" method is now outdated. Ubiquiti made the process a lot easier by just putting the necessary files in one location. Just replace the files as needed. The files are located at the following location:

```
/data/unifi-core/config/unifi-core.crt
/data/unifi-core/config/unifi-core.key
```

You'll be replacing these two files with your certificate and your private key, respectively. To be able to do so (via a Windows machine), you'll want to download three free utilities: PuTTY, WinSCP, and Notepad++

First, enable SSH access on your NVR. This can be done with a full administrative account, via the web GUI of your NVR, under the settings. It will ask you to make a password for access -- you won't be able to see this password later (though you can change it), so record the password in your password manager of choice, or by other secure means.

Next, open up PuTTY and put in the IP address of your NVR. Give the session a name and click Save. This will allow you to easily import to WinSCP later. Go ahead and click Open afterwards, and make sure SSH is working correctly. You won't need PuTTY much more after this, except to issue a reboot. (You can use the PuTTY connection to make a Certificate Signing Request (CSR) if you want, but it's usually easier to just use an online utility, or even better if your SSL certificate issuer will do it for you.)

Now, create a Certificate Signing Request (CSR) if your SSL issuer doesn't do this for you, which should generate a private key as well. I like https://csrgenerator.com/ for this, but in all honesty, you should generate it yourself with OpenSSL. Make sure the size is RSA 2048. Save the resulting key file as "unifi-core.key" on your computer, and upload or copy/paste the CSR into your SSL issuer's site wherever they ask for it.

Once you go through all the necessary hoops required by your SSL certificate issuer, download your certificate (and CA bundle if they give you one). They may give you two certificates, one in plaintext and one in PEM format. We are looking for the plaintext version. You can verify it's the proper format by opening the file in Notepad++. If the top

contains something along the lines of "-----BEGIN CERTIFICATE-----", then you have the right file. Save/rename that file as "unifi-core.crt" in Notepad++.

Optionally, you may have to combine your certificate and your CA bundle files. Try without doing this first, and if you get a problem at the end, come back to this step. If you DO have to combine these files, it's pretty easy. Open your CA bundle files in Notepad++, copy all the text, and paste it underneath the "-----END CERTIFICATE-----" line on your regular certificate. Make sure there are no extra lines between each certificate in the resulting file, and no extra lines at the beginning or end of the file. There are lots of guides on the internet on how to combine certificates and CA bundles on the internet, so I won't go into full detail here.

Now, what really got me is that my key did not have the right encoding type. Open both your certificate and your key in Notepad++, and check what encoding type it is under the Encoding menu. If it isn't "UTF-8", you'll have to change it, and re-save the file. In my case, I was provided with a key that was "UTF-8-BOM", and the NVR wasn't having any of that.

Once you have your proper unifi-core.crt and unifi-core.key files, it's time to fire up WinSCP. Once you open it, you can import your PuTTY saved session to your NVR. After that, go ahead and connect to the NVR in WinSCP, then navigate to "/data/unifi-core/config/" on the right-hand side. Upload your unifi-core.crt and unifi-core.key files, overwriting the existing files on the NVR.

Back in PuTTY, issue the "reboot" command. Just type it in there and hit enter. Your NVR will reboot itself.

Now, if you've done everything right, once your NVR comes back up, you should have a valid certificate. Close all your browser windows, or just open a new incognito/private window, and browse to your NVR by the hostname you made for your certificate (not by IP address). If you don't get a warning, you should be good to go. If you get a warning that the Certificate Authority isn't trusted, you'll have to go back to that optional step, combine your certificate and CA bundle, and try again.

However, the problem a lot of people had was, they still had an invalid certificate. If they inspected the certificate in their browser, it would show the hostname as "unifi.local". This means that the NVR didn't like something about the certificate or key file, and proceeded to delete them and re-create the defaults. You'll have to do some troubleshooting at this step. Re-upload the certificate and key files via WinSCP. Then, go ahead and PuTTY back into your NVR, and use the following command to get to the right directory: cd /data/unifi-core/config/

Once there, we are going to check your certificate and your key files. Make the PuTTY window large (or fullscreen) so you can properly see the output of these commands. Then, use the following to check your certificate:

```
openssl x509 -in unifi-core.crt -text -noout
```

This will give you a lot of output that you will have to parse through. Make sure the Signature Algorithm is "sha256WithRSAEncryption", make sure the Validity has a proper Not Before and Not After (and that the current date falls between the two), make sure the Public-Key is "2048 bit", make sure everything looks good in the Issuer section, and make

sure the Subject has your proper hostname as the "CN=".

Next we will verify your key with the following command:

```
openssl rsa -in unifi-core.key -check
```

The main thing we are looking for here, is the "RSA key ok" at the very top. In my case, this gave me an error instead, which is what made me stumble upon the fact that my key file was encoded wrong.

If both of those look good, it's possible your key and your cert don't match for some reason. Go ahead and check this with an online utility that you trust, such as https://www.sslshopper.com/certificate-key-matcher.html (make sure not to use something shady). If these don't match, you might have to re-issue your certificate, and/or contact your SSL issuer's support.

Once you have everything sorted out, remember that you have to reboot your NVR whenever you make these kind of changes. Go ahead and issue the "reboot" command via PuTTY to do so, and make sure to check again using a clean browser session (or new incognito/private session). Chrome for example will cache the old certificate for some time, so the best way to be sure you're pulling the updated certificate is to close it completely and re-open.

Hopefully this helps someone else out, as the previous instructions were a bit all over the place. (And a lot of the folders they reference on the NVR simply don't exist anymore.) I don't know how long this guide will stay valid for, but this worked for me on 2021-05-07. Good luck!

Responses (10)

Sort by Newest Oldest Page 1

E **Eaglehawk**
10 months ago

Thank you for posting your steps. This has been one of the things holding me back from making my UDM Pro go into "production". Right now my hack involves using a Synology to redirect the https requests to the Unifi back end.

1

B **brendanbiggs**
10 months ago

WOW!! what an incredible write up. Followed your steps and checks but using a wildcard cert from Let's Encrypt. Worked perfectly!! I understand I'll have to redo these steps ever 60 to 90 days but I'm a home user so no big deal or if I get lazy then I'll buy a certificate. I'm using a Unifi Cloud Key Gen 2 + running Unifi OS 2.1.7, Network 6.2.23 and Protect 1.18.1

using a UniFi Cloud Key Gen2+ running UniFi OS 2.1.7, Network 6.2.26 and Protect 1.18.1 and all work beautifully. I have the G4 Doorbell and 2 G3 Flex and everything works

awesome also checked and the protect app is still working too. I had this working with HA Proxy on my router/firewall but the video would always buffer out whether it was saved or live view. I had to either save the video and play it locally or log in using the private IP address and deal with the cert error but NOT any more. Thank you!!

1

brossow

10 months ago

> *@brendanbiggs wrote:*
> *WOW!! what an incredible write up. Followed your steps and checks but using a wildcard cert from Le t's Encrypt. Worked perfectly!! I understand I'll have to redo these steps ever 60 to 90 days but I'm a ho me user so no big deal or if I get lazy then I'll buy a certificate.*

Wish UI would support Let's Encrypt (or anything else) right out of the box via the GUI. Doesn't seem unreasonable. Synology (an example I'm familiar with) does and even handles automatic renewals with Let's Encrypt.

3

S scioara

10 months ago

> *@brendanbiggs wrote:*
> *I understand I'll have to redo these steps ever 60 to 90 days but I'm a home user so no big deal or if I g et lazy then I'll buy a certificate.*

Use the same method used to re-ad your SSH keys to the device after an update, and you don't need to manually do it every time:

https://github.com/boostchicken/udm-utilities/tree/master/on-boot-script

0

J joseph.stefanelli

7 months ago

@j0mbie

Can you PM me? I have some questions regarding this

0

C cgrvadmin

4 months ago

I always use the command line tools to do my heavy lifting. This ensures there are no encoding issues with the files. So here is what I did:

encoding issues with the files. So here is what I did:

Issue the following at the UNVR's command prompt

```
- openssl req -new -newkey rsa:2048 -nodes -keyout unifi-core.key -out unifi-core.csr
- cat unifi-core.csr
```

Copy and paste the output of the cat command in to the website that is issuing your certificate. In my case I opted for a "low assurance" certificate from www.ssls.com and paid for 5 years to receive the maximum possible discount. Now wait for the certificate to be issued. (In my case, it came as part of the email, so I just copied it and issued the following … vim unifi-core.crt … i for insert … Paste … ESC to exit insert mode … Type a colon : followed by 'wq' to write the file and quit).

Once you receive your newly minted certificate file, upload it (and the CA bundle if one was provided) to your UNVR via

- Fugu for Mac

- WinSCP for Windows

Now back in Terminal or PuTTY, rename your certificate file

```
- mv {nameofyourcrtfile}.crt unifi-core.crt
```

If you uploaded a CA bundle we need to combine them

```
- cat unifi-core.crt ca-bundle.crt > unifi-core.crt
```

Copy the files into the correct location

```
- cp unifi-core.crt /data/unifi-core/config/
- cp unifi-core.key /data/unifi-core/config/
- reboot
```

I hope this information helps someone. Thank you to the original author as I used your very informative article as a stepping off point.

1

---

jamesdorton

4 months ago

Using the steps from j0mbie, inconjunction with the steps from cgrvadmin, I was able to generate a certificate request using openssl on my UDMPro, sign it with my Active Directory Certificate Authority server, and upload the signed request to the UDMPro. Upon reboot, I see the UDMPro hasn't regenerated the certificates, which was a good sign that I had done something right. The message I'm getting now is NET::ERR_CERT_COMMON_NAME_INVALID. Which I don't understand because the Common Name I used on the cert is the same as the name of the UDMPro. Thoughts?

0

G Gokou900

4 months ago

> *@jamesdorton wrote:*
> *Using the steps from j0mbie, inconjunction with the steps from cgrvadmin, I was able to generate a certificate request using openssl on my UDMPro, sign it with my Active Directory Certificate Authority server, and upload the signed request to the UDMPro. Upon reboot, I see the UDMPro hasn't regenerated the certificates, which was a good sign that I had done something right. The message I'm getting now is NET::ERR_CERT_COMMON_NAME_INVALID. Which I don't understand because the Common Name I used on the cert is the same as the name of the UDMPro. Thoughts?*

Are you sure you used the correct common name? You should use the DNS name you use to access the UDM as the common name.

0

P pharvey

3 months ago

At the end, you don't have to reboot, you can issue a command to restart the service.

```
systemctl restart unifi-core
```

0

P pharvey

3 months ago

@jamesdorton I know I'm late to the party, but if you haven't already figured it out, make sure to also add a dns entry under the alternative name part. I also add the IP address so that I don't get a cert error if I access the box that way as well.

0

Page 1

Your Response

Write your response here ...

Comment

UI.com