Peter Hicks' Blog
The personal blog of Peter Hicks

Installing TLS certificates on HP printers automatically

Installing a TLS (SSL) certificate on an HP LaserJet printer automatically isn't as difficult as you might think

I wrote an article about installing a Let's Encrypt TLS certificate on an HP LaserJet printer a while ago. Since then, I've been annoyed by having to install updated certificates manually, so I decided to look at how I could automate it.

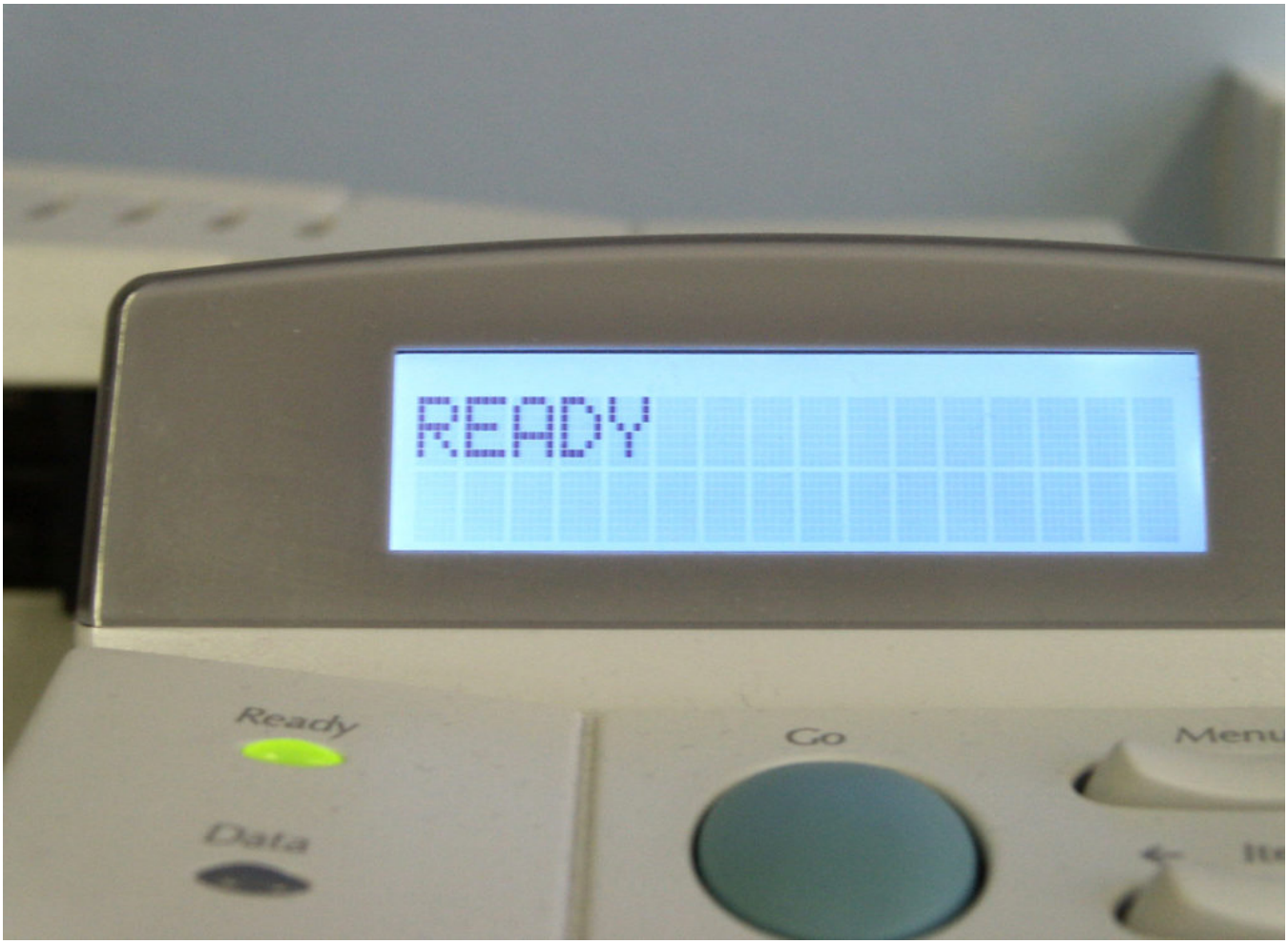

Photo by Alex Furr from FreeImages

TechRadar has a great article on securing printers, but how do you automate it? Well, with a certificate authority like Let's Encrypt for starters, but there's no mechanism for the printer to automatically update its certificate after it expires.

I've set my desktop machine to *certbot* and renew the certificate automatically. An evening's hacking around the web interface showed it's really easy to install a certificate automatically.

This is the magic command to install the certificate:

```
curl -v --insecure https://HOSTNAME/hp/device/Certificate.pfx --form
upload=@/tmp/cert.pfx --form Password=password
```

Replace *HOSTNAME* with the hostname of your printer and change */tmp/cert.pfx* as required. If you want to know how to create the PFX file, see my original post.

Has anyone else found out how to do this? If they have, they've not posted about it!

Peter Hicks / Wednesday 18 March 2020 / Printers, Security

14 thoughts on "Installing TLS certificates on HP printers automatically"

Jason Schwarz

Monday 27 July 2020 at 18:09

Works great on some devices, but I have one laserjet that might be too old for that, and they apparently use different URLs for the InkJets

---

Thomas Baeck

Tuesday 11 August 2020 at 10:07

I did try your command, but it fails for me.

I changed the hostname accordingly, the location of the certificate file and the password to the export password.

The error I receive is:
HTTP error before end of send, stop sending
<
* Closing connection 0

He Who Shall Not Be Named

Thursday 31 December 2020 at 00:05

In the interest of paying it forward for others that may run across this page. Different HP printers have different ways of getting the certificates to them. You can (as I did) simply open up the certificate interface in Safari or Chrome and enable developer tools to figure out what the right call is. It seems to change every two or three printer generations. If you have a modicum of developer / debugging expertise, you can quickly deduce what the right one is for you if the above (or below) doesn't work.

The magic incantation for some of the more modern HP printers is:

```
curl -silent --show-error --insecure "https://HOSTNAME/Security/DeviceCertificates/NewCertWithPassword/Upload?fixed_response=true" --form certificate=@"YourCert.pfx" --form password="PASSWORD"
```

Replace HOSTNAME with the printer's hostname/IP.
Replace YourCert.pfx with the path to the PFX-encoded certificate.
Replace PASSWORD with the password you used to encrypt the PFX-encoded certificate.

Colm Buckley

Saturday 16 January 2021 at 13:12

On newer Laserjet models (eg: my M479fdw) which have a more "Javascripty" web interface, the upload URL is different – but a bit of snooping in the Chrome console reveals that it's basically the same mechanism, just a different URL.

```
curl -v --insecure -u admin:ADMIN_PASSWORD --form certificate=@cert.pfx --form password=PFX_PASSWORD https://PRINTER_HOSTNAME/Security/DeviceCertificates/NewCertWithPassword/Upload
```

(that's all one line).

ADMIN_PASSWORD is the password for the 'admin' user you set in the printer's web UI.
PFX_PASSWORD is the password you set on the PFX certificate file.
PRINTER_HOSTNAME is the network name or IP address of the printer.

Hope this helps!

Peter Hicks

Saturday 16 January 2021 at 13:15

Superb, thank you very much! I may do a further post aggregating this, and another post.

Jeffrey Goh

Saturday 19 February 2022 at 03:22

Worked a charm on my ENVY Pro 6420 – I did find it better to use fullchain.pem rather than cert.pem in the PFX file so that curl doesn't even need the –insecure on subsequent uploads

---

C

Monday 22 February 2021 at 12:05

Thank you – and to people posting here as well – this is just what I'm looking for.

---

kaczmar2

Thursday 25 November 2021 at 18:34

Thank you very much. This works perfectly for me on a HP LaserJet Pro MFP M426dfw, with the URL: https://HOSTNAME/hp/device/Certificate.pfx

One note. I needed to add credentials in order to complete the request; otherwise, I was receiving 401 (Unauthorized): `curl -v --insecure -u admin:HP_WEB_PORTAL_ADMIN_PASSWD https://HOSTNAME/hp/device/Certificate.pfx`

J

Saturday 13 August 2022 at 18:58

be careful copying the commands here as a hyphen is turned into an em dash and the curl command will fail. Make sure all "-" are literal hyphens

Peter Hicks

Friday 19 August 2022 at 14:15

That's a good point. I'll see if I can edit those comments.

Mariusz

Saturday 13 May 2023 at 21:30

Hi i just try to Upload the pfx cert on my envy 4520. I have tried on web UI but then i get error code 0XB92E35D0. Than i have found your solution and try it with curl but comes the same error on printer display after upload. Here the answer from printer

C:\curl\bin>curl -v –insecure -u admin:password –form certificate=@cert.pfx –form password=password https://192.168.178.60/Security/DeviceCertificates/NewCertWithPassword/Upload
* Trying 192.168.178.60:443...
* Connected to 192.168.178.60 (192.168.178.60) port 443 (#0)
* ALPN: offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):

```
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / AES256-GCM-SHA384
* ALPN: server did not agree on a protocol. Uses default.
* Server certificate:
* subject: CN=HP23A06A; L=Vancouver; ST=Washington; C=US; O=HP;
OU=HP-IPG
* start date: Jun 2 09:20:56 2020 GMT
* expire date: May 31 09:20:56 2030 GMT
* issuer: CN=HP23A06A; L=Vancouver; ST=Washington; C=US; O=HP; OU=HP-
IPG
* SSL certificate verify result: self-signed certificate (18), continuing anyway.
* using HTTP/1.x
* Server auth using Basic with user 'admin'
> POST /Security/DeviceCertificates/NewCertWithPassword/Upload HTTP/1.1
> Host: 192.168.178.60
> Authorization: Basic YWRtaW46VGVsaTA3MSEh
> User-Agent: curl/8.0.1
> Accept: */*
> Content-Length: 5705
> Content-Type: multipart/form-data; boundary=————————
c96492a1322c6340
>
* We are completely uploaded and fine
```

Mariusz

Saturday 13 May 2023 at 21:33

HTTP/1.1 500 Internal Server Error
< Server: HP HTTP Server; HP ENVY 4520 series – K9T09B; Serial Number: TH85H5K0QN0660; Built:Tue Jun 02, 2020 09:20:56AM {CFP1FN2023BR}
< Content-Length: 0
< Cache-Control: must-revalidate, max-age=0
< Pragma: no-cache
<
* Connection #0 to host 192.168.178.60 left intact

Chris Nesbitt-Smith

Friday 3 November 2023 at 16:43

Have a HP LaserJet color flow MFP M575 | HP FutureSmart 4 | 4.12.0.1

For anyone else struggling (or just me in a few months when it breaks and I loose my config)

Needed to disable CSRF protection 🙁
https://HOSTNAME/hp/device/GeneralSecurity/Index

I could be less lazy and hunt the page for the CSRF token and then submit, but I don't have the energy for that right now

then:

curl https://YOURHOSTNAME/hp/device/SignIn/Index -v \
-c ./cookies.txt \
–form agentIdSelect=hp_EmbeddedPin_v1 \
–form PinDropDown=AdminItem \
–form PasswordTextBox=YOURPASSWORD \
–form signInOk=Sign+In \

```
–insecure && \
curl -v -b ./cookies.txt –insecure \
–form .Import_FileName_handle=@certificate.pfx \
–form Finish=Finish \
–form CSRFToken= \
–form Hide=Hide \
–form password=CERTPASSWORD \
https://YOURHOSTNAME/websecurity/cert_import.htm/config
```

Chris Nesbitt-Smith

Friday 3 November 2023 at 17:13

or for a collected package: https://github.com/chrisns/infra/blob/main/devices-tls/hp-m575m.cns.me.yaml

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Peter Hicks' Blog / Proudly powered by WordPress