HP Printer Set up for Secure HTTPS Printing for Banner

ITS has worked out a way to print securely via HTTPS from a Banner DB server to a remote HP printer. No other printer brands have been tested yet. If possible, please use only HP printers.

Disclaimer: This works on some newer HP printers, but we can’t verify that this is the only way to make it work or that there are unnecessary steps in the procedure. If you have tips that can save others time, please let us know and we'll update the document. There are a few knobs to tweak.

Make sure that your campus firewall is open to the printer from 168.25.50.0/24 and 168.25.55.0/24 (the Banner hosted networks) for ports 443 (HTTPS or SSL), 515 (lpd), and 9100 (HP raw printing).

Make sure the firmware is reasonably new. We don't have an exact cutoff for working vs. nonworking firmware but anything within the last two years is probably fine. Feel free to send us more as you find them. Firmware that we know work are:

HP M804:
Firmware Bundle Version

: 3.2.5

Firmware Revision: 2302908_435012

Firmware Date Code

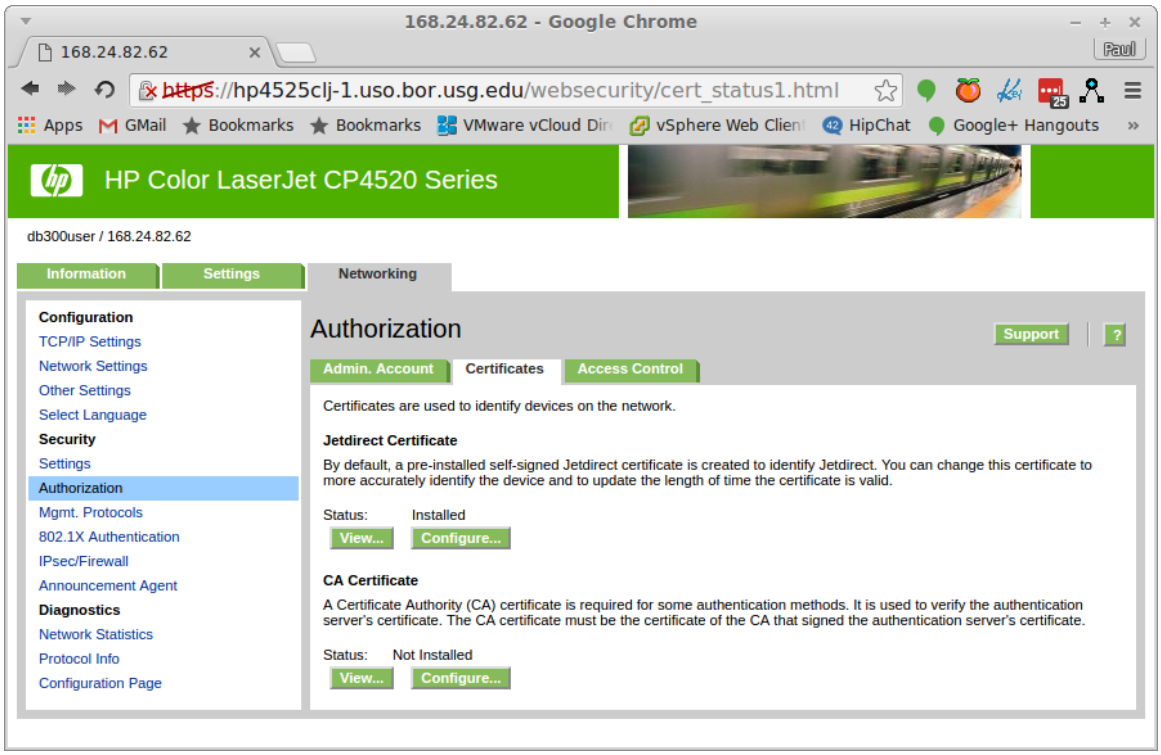
: 20140529

HP Color LaserJet CP4025:
20150731 07.220.2 (from the diagnostics page)

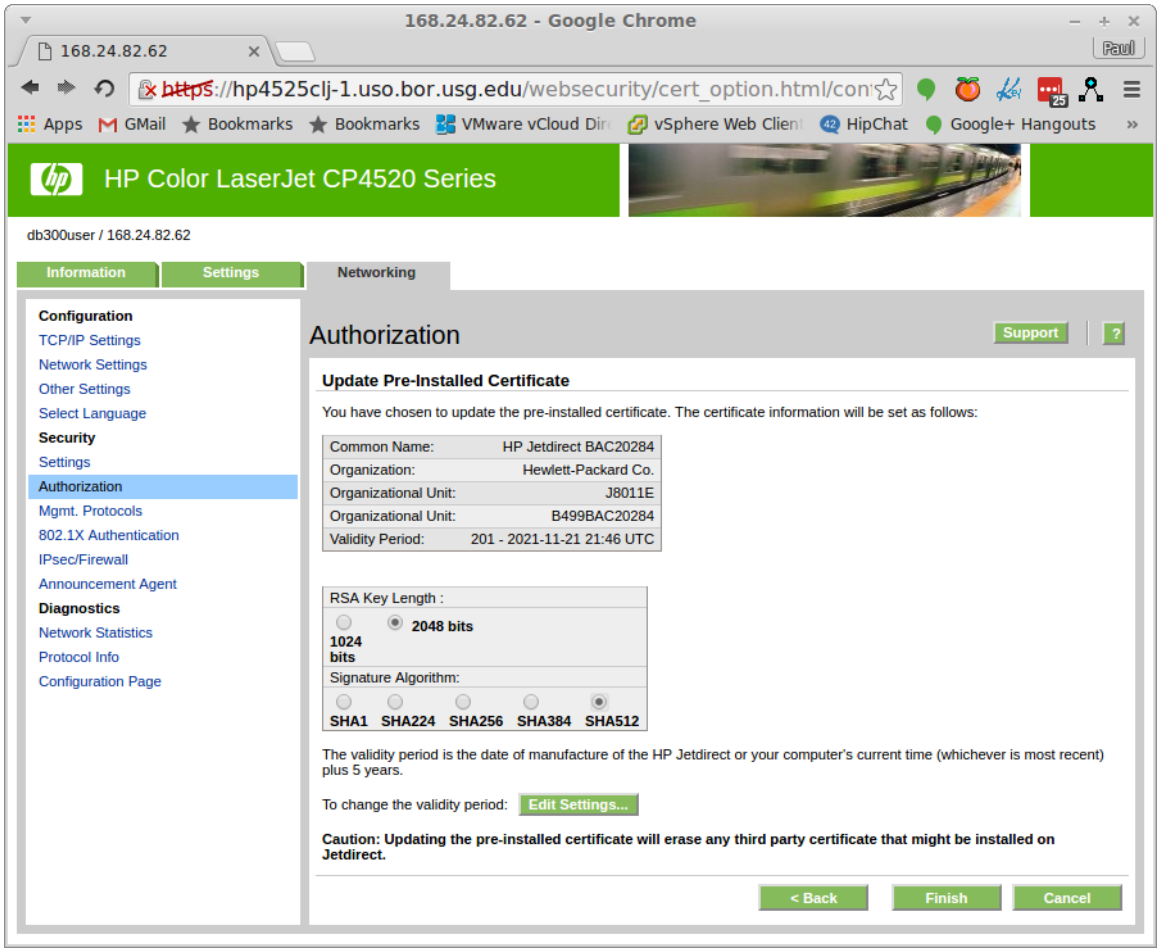
Some firmware installation guidelines are included at the bottom of this document for those who haven't done it in a while.

Two SSL certificates in the HP printer will need to be updated. (As stated above, perhaps both don't need to be updated. When we got it working, we'd already updated both. It's easy so we keep doing it.)

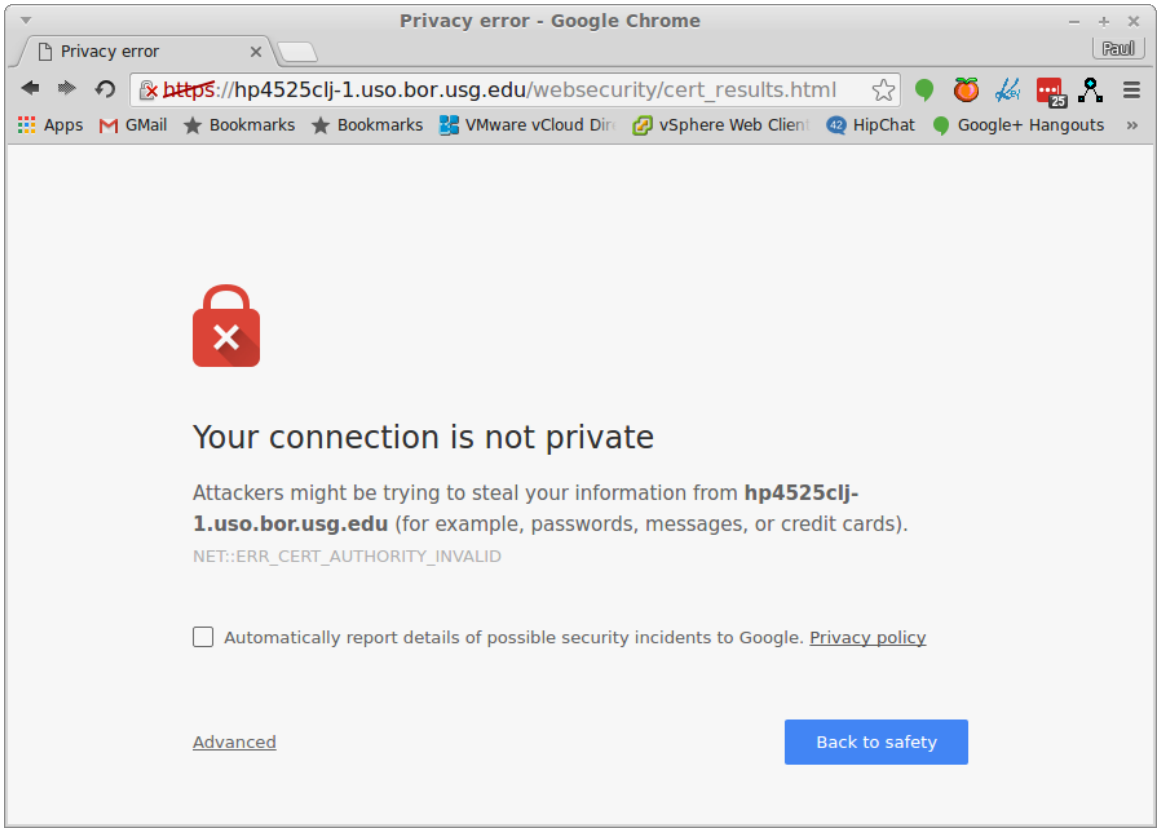
Choose the **Networking** tab at the top, then **Authorization** item on the left, then **Certificates** in the sub-window. Under Jetdirect Certificate, select the **Configure** button.

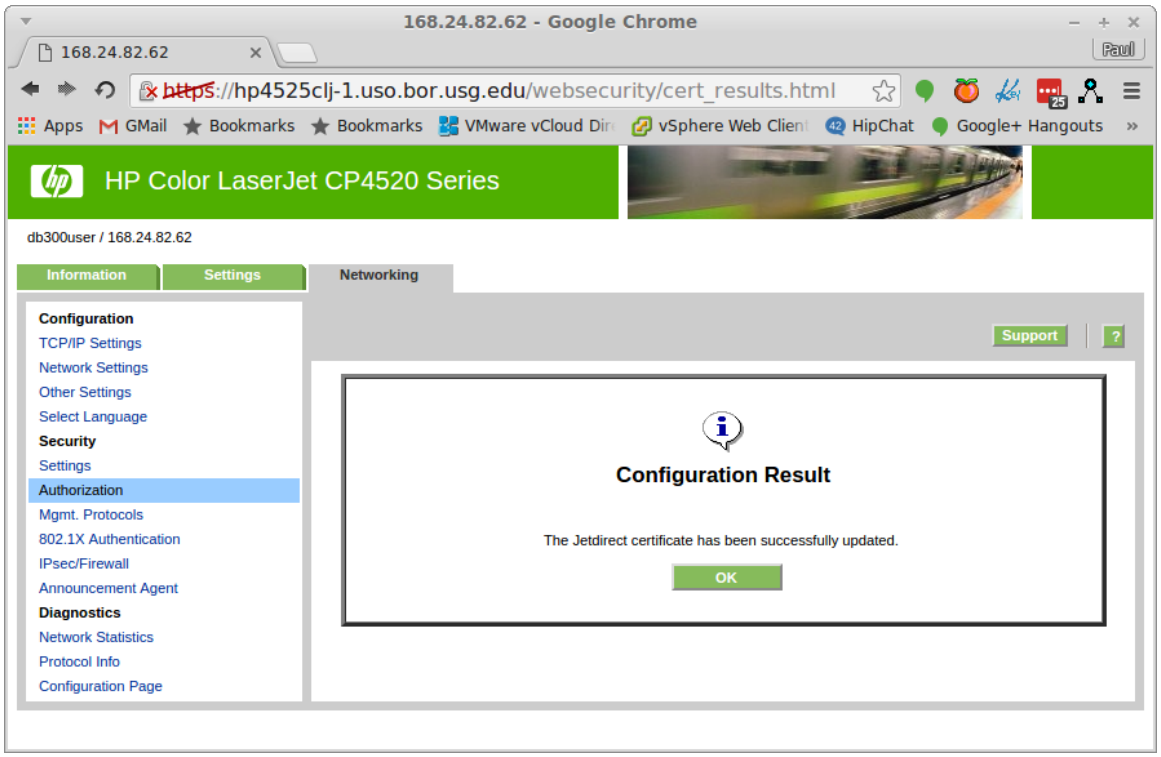


Create a new self-signed cert with SHA256 or higher, 2048 bits or higher:

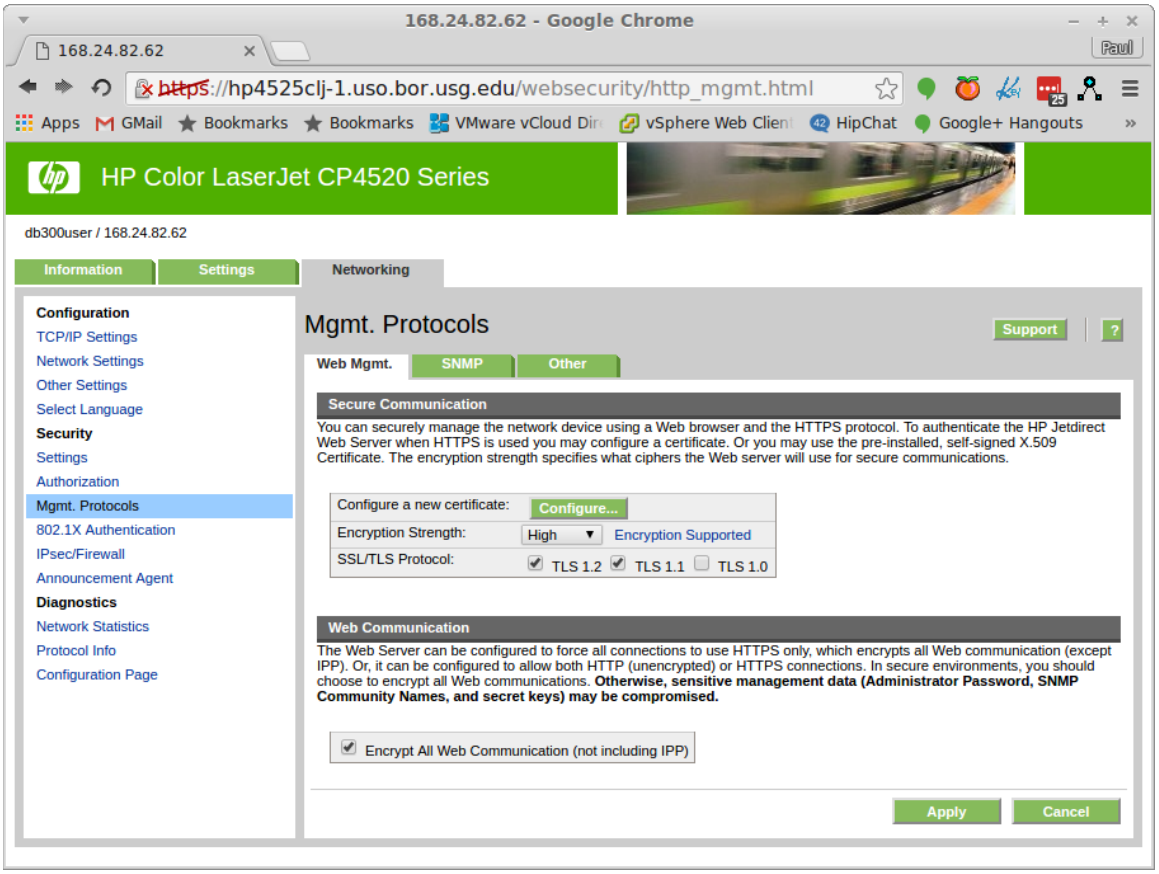


When it does this, you'll lose connection and then reconnect. Your browser will make you approve the new cert.

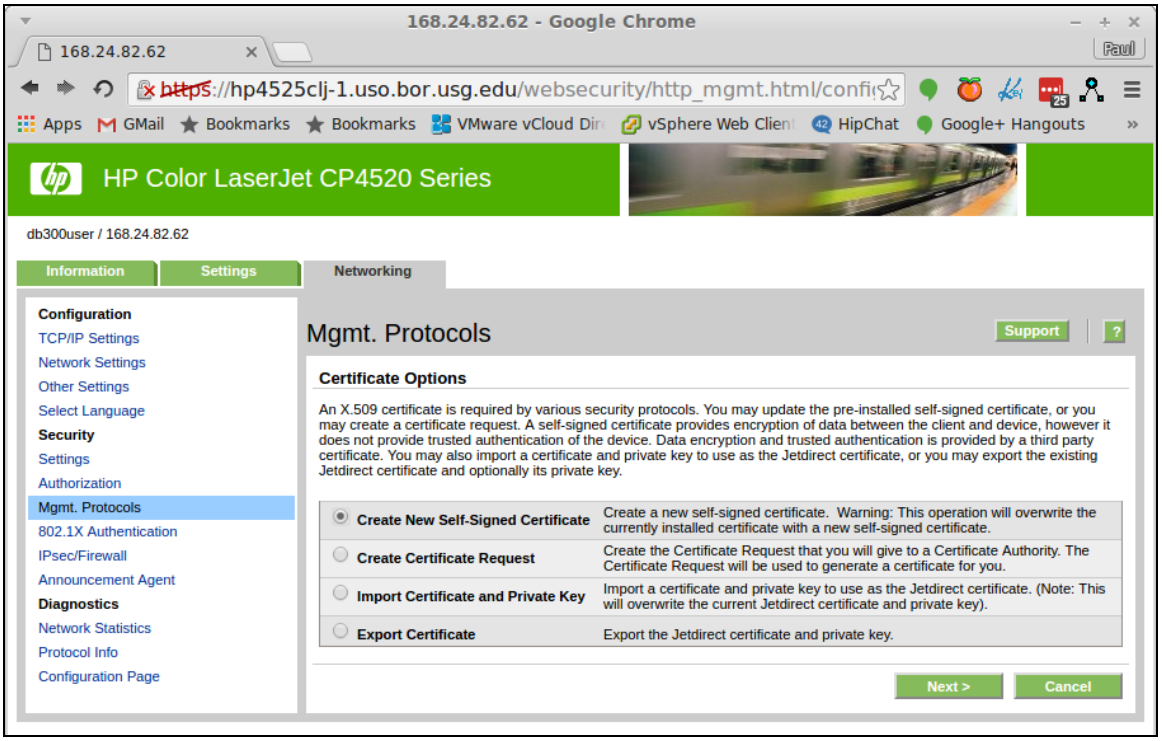




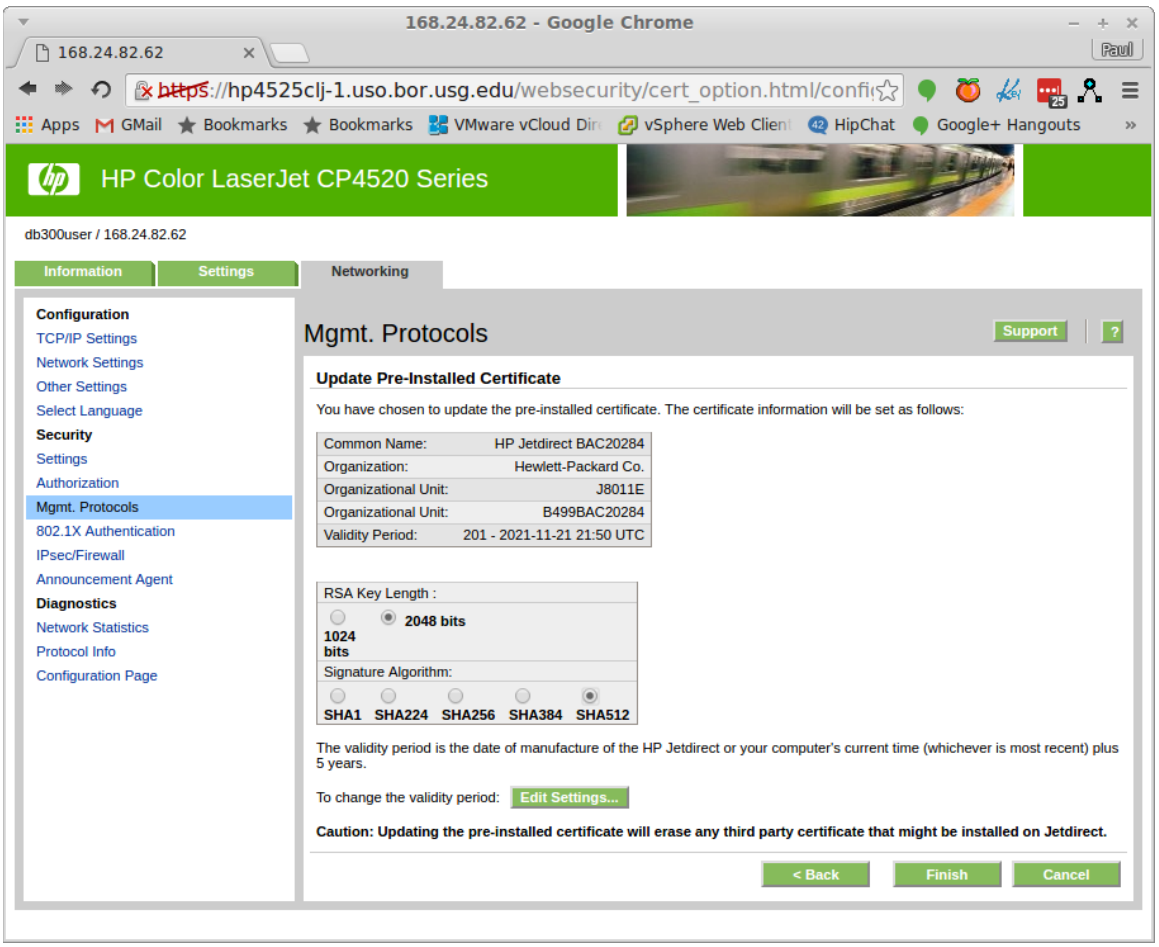
Go to the **Mgmt. Protocols** menu item. Adjust Encryption Strength to High and uncheck TLS 1.0 and SSL 3.0 (which doesn't use TLS). TLS 1.1 is the lowest one you should have. We tried using only TLS 1.2 but the print server side doesn't seem to be able to do that yet, so TLS 1.1 it is! You can also check the “Encrypt all web communication” box if you’d like, which would make it more secure but probably make HTTP:// web access stop working. Select the Apply button to save the changes.



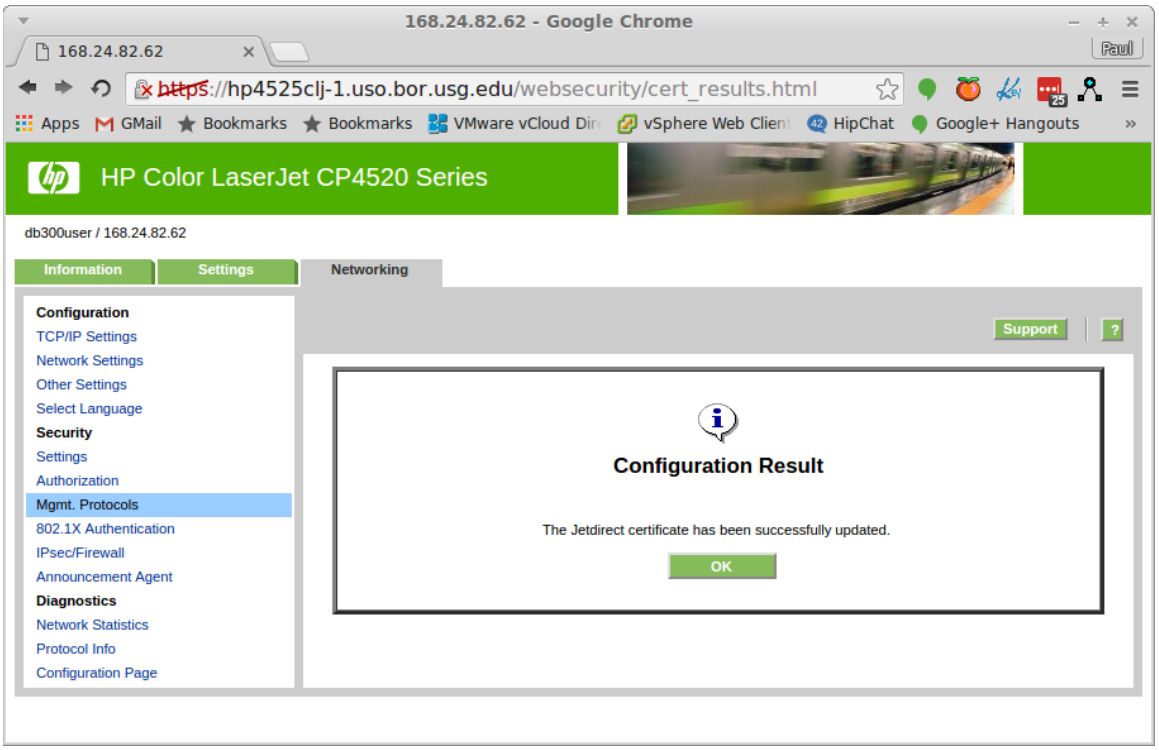
Now, create another (different place) self-signed cert for the management traffic. This is the point where we are not sure if BOTH of these certs are needed. Feel free to experiment and let us know.



Go as high as you can on the SHA version/bits - hopefully SHA256 or better, 2048 bits or better.



You'll get disconnected and have to re-approve the self-signed cert, then should see a success screen:



It should be ready for a test print from the BOR Banner server. Submit a ticket with the IP number and name of the printer queue and we can attempt to set it up.

If you have access to a Linux/UNIX machine with nmap installed, check that you do not have TLS 1.0 or SSL 3 turned on with a command like this (can take 30-60 seconds):

nmap --script ssl-enum-ciphers -p 443 168.18.x.y

Starting Nmap 5.51 (http://nmap.org) at 2016-12-02 14:27 EST

Nmap scan report for 168.18.x.y

Host is up (0.027s latency).

PORT   STATE SERVICE

443/tcp open https

| ssl-enum-ciphers:

| TLSv1.0

| Ciphers (3)

| TLS_RSA_WITH_3DES_EDE_CBC_SHA

| TLS_RSA_WITH_AES_128_CBC_SHA

| TLS_RSA_WITH_AES_256_CBC_SHA

| Compressors (1)

| uncompressed

| TLSv1.1

| Ciphers (3)

| TLS_RSA_WITH_3DES_EDE_CBC_SHA

| TLS_RSA_WITH_AES_128_CBC_SHA

| TLS_RSA_WITH_AES_256_CBC_SHA

| Compressors (1)

| uncompressed

| TLSv1.2

| Ciphers (7)

| TLS_RSA_WITH_3DES_EDE_CBC_SHA

| TLS_RSA_WITH_AES_128_CBC_SHA

| TLS_RSA_WITH_AES_128_CBC_SHA256

| TLS_RSA_WITH_AES_128_GCM_SHA256

```
|       TLS_RSA_WITH_AES_256_CBC_SHA
|       TLS_RSA_WITH_AES_256_CBC_SHA256
|       TLS_RSA_WITH_AES_256_GCM_SHA384
|     Compressors (1)
|_      uncompressed

Nmap done: 1 IP address (1 host up) scanned in 60.60 seconds
```

That one has versions of TLS that are too old. This one is better:

```
nmap --script ssl-enum-ciphers -p 443 168.24.x.y

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-02 14:30 EST
Nmap scan report for hpmxxxx.uso.bor.usg.edu (168.24.x.y)
Host is up (0.0010s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.1
|     Ciphers (3)
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA
|       TLS_RSA_WITH_AES_128_CBC_SHA
|       TLS_RSA_WITH_AES_256_CBC_SHA
|     Compressors (1)
|       uncompressed
|   TLSv1.2
|     Ciphers (7)
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA
|       TLS_RSA_WITH_AES_128_CBC_SHA
|       TLS_RSA_WITH_AES_128_CBC_SHA256
|       TLS_RSA_WITH_AES_128_GCM_SHA256
```

| TLS_RSA_WITH_AES_256_CBC_SHA

| TLS_RSA_WITH_AES_256_CBC_SHA256

| TLS_RSA_WITH_AES_256_GCM_SHA384

| Compressors (1)

|_ uncompressed

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds

We can scan from the banner database server as long as port 443 is open, if you don't have a handy way to do it locally.

Good luck and feel free to ask us questions!

-The GABEST sysadmins

Notes for firmware updates:

Here are some rough notes on how we've been updating firmware. The most modern ones can have a file uploaded through the web GUI, but somewhat older ones need FTP.

1. http://support.hp.com/us-en/drivers
2. Enter model number e.g. "laserjet m806" "color laserjet cp4025"
3. Click your specific model if you even know
4. "Select your product's operating system"
5. Try some version of Windows!
6. There will be a firmware section, download the biggest thing they've got! Sometimes it is a bundle of stuff, sometimes just a zipped rfu (Remote Firmware Update) file
7. Unzip it and figure out which is the rfu file you want
8. FTP printername.yourschool.edu, hit ENTER twice rather than giving creds
9. Bin
10. Hash
11. Put blahblah.rfu
12. Quit
13. Ping printername.uso.bor.usg.edu|perl -n -e 'print " " x rand(5), $_'
14. Watch it stop answering and then start again after a few minutes