How to update cURL trusted root certificates.

Phil Rigby - 2021-06-16 - Comments (0) - Server Software

With LetsEncrypt's DST Root CA X3 root certificate expiring , some customers are experiencing issues when Deskpro needs to contact external websites, such as downloading linked attachments from emails, or adding an external download link etc.

This is often due to PHP cURL, the service Deskpro uses for external websites, having outdated certificates for https requests. As it does not recognise the newer certificates, it will refuse to connect to these external websites, which can block some Deskpro services from running correctly.

This can be fixed easily by manually updating the list of trusted root certificates to include the newer **LetsEncrypt ISRG Root X1 root certificate**. We recommend using the curl.se CA Bundle, as this is regularly extracted from the Firefox browser, which is maintained by Mozilla, and is formatted in a way which cURL expects.

Linux

(Paths in this guide will assume a default Linux installation on Ubuntu 18.04 LTS, but it will be similar for other distros.)

1. Download the latest CA bundle extract from curl.se

```
wget https://curl.se/ca/cacert.pem -O /etc/ssl/certs/cacert.pem
```

2. Edit your php.ini file.

For Ubuntu 18.04, there are 2 php.ini files which need to be modified in the following locations:

`/etc/php/<version>/cli/php.ini`

`/etc/php/<version>/fpm/php.ini`

Replace the `<version>` with the version of PHP you're using, so for PHP 7.4, the path will be `/etc/php/7.4/…`

In these files, you need to either modify or add the `curl.cainfo` and `openssl.cafile` parameters with the path to the new CA bundle:

```
[curl]
 curl.cainfo = /etc/ssl/certs/cacert.pem
```

```
[openssl]
 openssl.cafile = /etc/ssl/certs/cacert.pem
```

(only add the parameter if it does not already exist in your php.ini file. Duplicate parameters can prevent PHP from running correctly)

3. Restart your php-fpm to load the new settings.

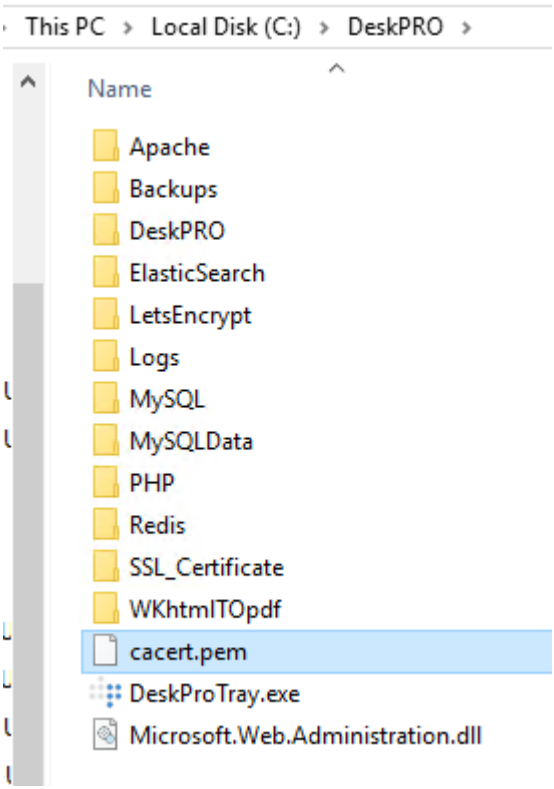
`systemctl restart php<version>-fpm`

Replace the `<version>` with the version of PHP you're using, so for PHP 7.4, the command will be `systemctl restart php7.4-fpm`

Windows

(Paths in this guide will assume the default Windows installation directory)

1. Download the latest CA bundle extract from curl.se, and place it within the Deskpro installation directory (`C:\DeskPRO\`).



2. Edit your `php.ini` file (`C:\Deskpro\PHP\php.ini`) in notepad.

3. Find the following section of your `php.ini` file:

```
[curl]
; A default value for the CURLOPT_CAINFO option. This is required to be an
; absolute path.
;curl.cainfo=

[openssl]
; The location of a Certificate Authority (CA) file on the local filesystem
; to use when verifying the identity of SSL/TLS peers. Most users should
; not specify a value for this directive as PHP will attempt to use the
; OS-managed cert stores in its absence. If specified, this value may still
; be overridden on a per-stream basis via the "cafile" SSL stream context
; option.
;openssl.cafile=
```

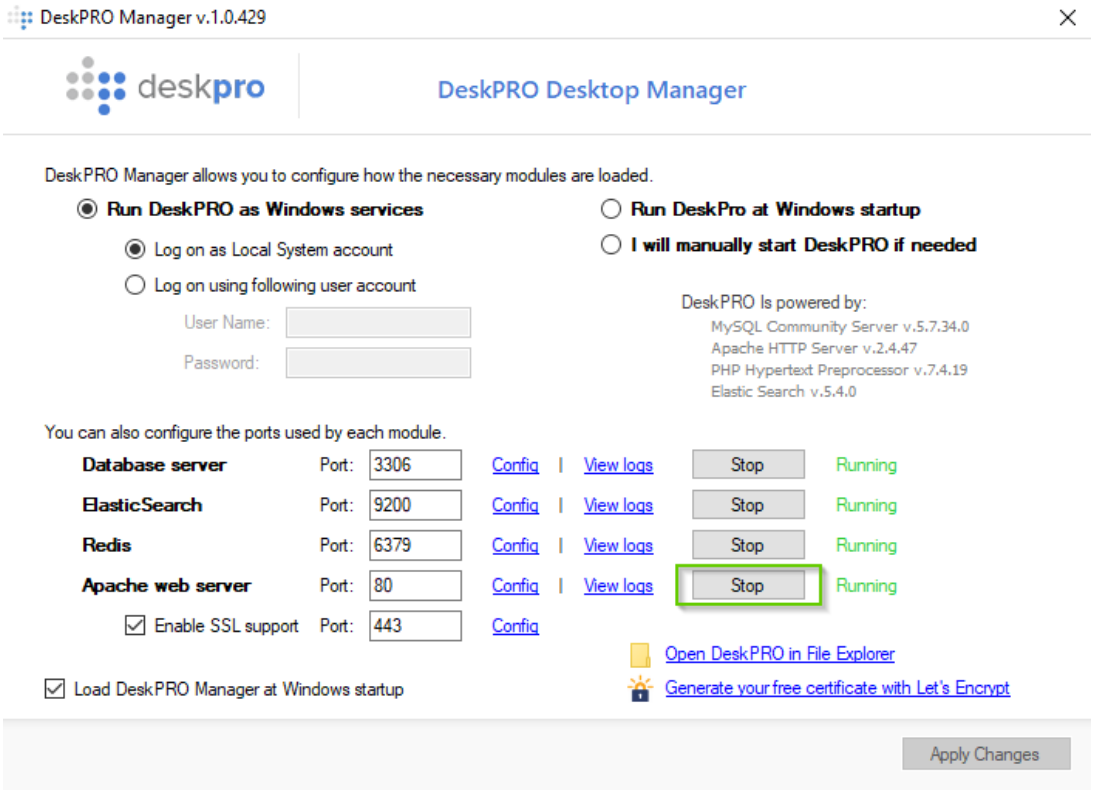
Modify both parameters to remove the semicolons (`;`) from the start of the lines, and the path to the `cacert.pem` file at the end:

```
[curl]
; A default value for the CURLOPT_CAINFO option. This is required to be an
; absolute path.
curl.cainfo=C:\DeskPRO\cacert.pem

[openssl]
; The location of a Certificate Authority (CA) file on the local filesystem
; to use when verifying the identity of SSL/TLS peers. Most users should
; not specify a value for this directive as PHP will attempt to use the
; OS-managed cert stores in its absence. If specified, this value may still
; be overridden on a per-stream basis via the "cafile" SSL stream context
; option.
openssl.cafile=C:\DeskPRO\cacert.pem
```

4. Save the file

5. Restart your web handler, by opening your DeskPRO Manager (**Start > Configure Deskpro**), then clicking the '**Stop**' button on the end of the web server line.



Wait for the service to stop completely, then click '**Start**' again to restart.

This should now update the trusted root certificates for cURL, allowing it to connect to external websites using the new **LetsEncrypt ISRG Root X1 root certificate.**

Custom Root Certificates

If you require a custom Root Certificate to use a service such as Cisco Umbrella, or you need Deskpro to trust a self-signed certificate, you can add these custom root certificates to the `cacert.pem` file.

The certificate needs to be in **Base 64** or **PEM** format, and can be appended to the bottom of the file by running `cat custom-cert.pem >> cacert.pem` in **Linux**, or copy/pasting

the certificate to the file in Notepad for **Windows.**