

How do I update root certificates in Apache/PHP/cURL environment

Following is the instruction for dealing with the new ISIS' SSL certificate authority (effective 4/21/2006), Geo Trust, in a UNIX or Windows environment using Apache/PHP/cURL. The instruction can generally apply to any new SSL certificate authority.

UNIX

If your web application is getting an error with ISIS login, try the following:

1. Your PHP was probably compiled with cURL, i.e, `--with-curl=/usr/local/curl-7.12.0`. Our cURL is installed in `/usr/local/curl-7.12.0`, but yours can be any arbitrary path. Find out what is it.
2. Your cURL came with the default CA bundle file, which contains root certificates for all the well known certificate authorities at the time cURL was installed. Our file is `/usr/local/curl-7.12.0/share/curl/curl-ca-bundle.crt`, which is the default location for the default compilation of cURL. If you compiled cURL with a custom location for this file, find out what is it and that's the one you will update.
3. Looked for the new ISIS certificate authority from Geo Trust in `/usr/local/curl-7.12.0/share/curl/curl-ca-bundle.crt`. Basically all the following 3 lines should be in `curl-ca-bundle.crt`:

```
Equifax Secure Global eBusiness CA-1
```

```
Validity Period: Mon Jun 21, 1999 to Sun Jun 21, 2020 (GMT)
```

```
Certificate Fingerprint (MD5): 8F:5D:77:06:27:C4:98:3C:5B:93:78:E7:D7:7D:9B:CC
```

If any of these lines are not in `curl-ca-bundle.crt`, you need to update your `curl-ca-bundle.crt`.

- 4a. If you don't have any local certificates in `curl-ca-bundle.crt`, you can replace the entire `curl-ca-bundle.crt`. Save the old `curl-ca-bundle.crt` and get `cacert.pem` from

<http://curl.haxx.se/docs/caextract.html>. Replace `curl-ca-bundle.crt` with `cacert.pem`.

- 4b. If you have some local certificates in `curl-ca-bundle.crt`, get `cacert.pem` from

<http://curl.haxx.se/docs/caextract.html> and extract "Equifax Secure Global eBusiness CA"

certificate from cacert.pem by extracting the lines between and including:

```
Equifax Secure Global eBusiness CA
```

and

```
END CERTIFICATE
```

Make a copy of the current curl-ca-bundle.crt and then append this piece of new certificate data to curl-ca-bundle.crt.

5. Restart your Apache server (the PHP module in Apache reads curl-ca-bundle.crt at startup).

6. Test login to ISIS.

Windows

cURL in Apache/PHP on Windows doesn't read a CA Bundle at startup and must be set by the application. On Windows adjust your CA Bundle file as above for UNIX. If you don't have one already [read this](#).

Revision #8

Created 2006-04-28 08:44:02 UTC by Chieu, Orachat

Updated 2007-08-31 09:00:53 UTC by Hunt, Carl