Windows SSL Certificate Cleaner

Dr Gadgit

21 Jul 2015 CPOL

Displays Windows SSL certifiacte in a tree-view and allows you to delete some certificates

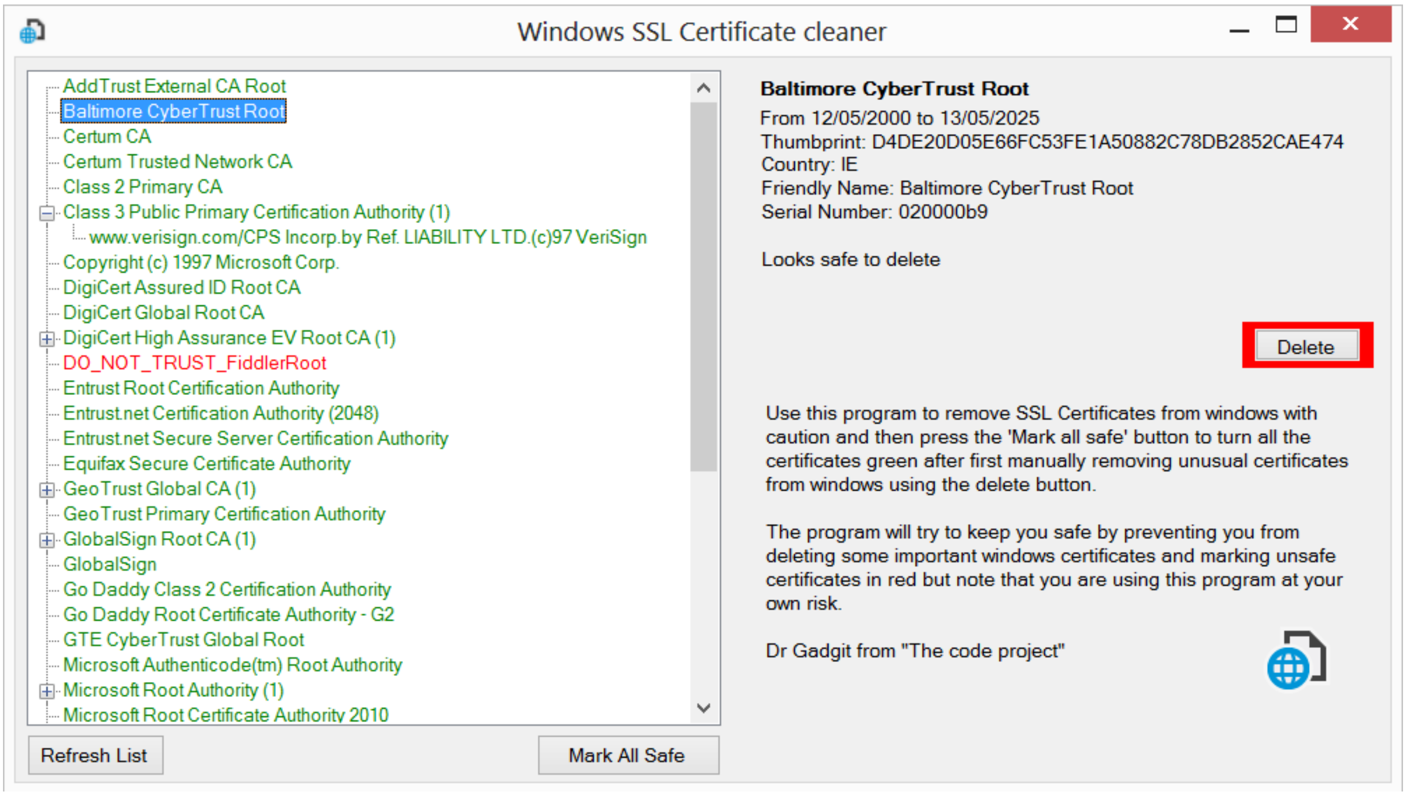
Download Windows app - 33 KB

Download CertCheck - 428.4 KB

Introduction

The Windows management console and security snap-in makes it hard to see just what is going on in Windows as more and more central authority root SSL certificates are added to your machine so this program hopes to simplify matters by presenting the certificates in a tree view and uses colour coded warnings to help make cleaning out suspect certificates easier.

This little Windows application was built using Visual Studio 2010 and you can download all the source code for the full project by clicking the '*CertChecker*' link at the top of the screen or just click the '*Windows App*' link to download the program ready to run as a Windows .EXE file.



- AddTrust External CA Root
- Baltimore CyberTrust Root
- Certum CA
- Certum Trusted Network CA
- Class 2 Primary CA
- Class 3 Public Primary Certification Authority (1)
  - www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
- Copyright (c) 1997 Microsoft Corp.
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert High Assurance EV Root CA (1)
- DO_NOT_TRUST_FiddlerRoot
- Entrust Root Certification Authority
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- Equifax Secure Certificate Authority
- GeoTrust Global CA (1)
- GeoTrust Primary Certification Authority
- GlobalSign Root CA (1)
- GlobalSign
- Go Daddy Class 2 Certification Authority
- Go Daddy Root Certificate Authority - G2
- GTE CyberTrust Global Root
- Microsoft Authenticode(tm) Root Authority
- Microsoft Root Authority (1)
- Microsoft Root Certificate Authority 2010

Baltimore CyberTrust Root
From 12/05/2000 to 13/05/2025
Thumbprint: D4DE20D05E66FC53FE1A50882C78DB2852CAE474
Country: IE
Friendly Name: Baltimore CyberTrust Root
Serial Number: 020000b9

Looks safe to delete

Use this program to remove SSL Certificates from windows with caution and then press the 'Mark all safe' button to turn all the certificates green after first manually removing unusual certificates from windows using the delete button.

The program will try to keep you safe by preventing you from deleting some important windows certificates and marking unsafe certificates in red but note that you are using this program at your own risk.

Dr Gadgit from "The code project"

Background

I decided to write this program because I know that my ISP is hijacking DNS requests made to outside servers and redirecting them back to IP-Address owned by my ISP since this allows ISPs to lower upstream costs and improves performance but this means that any SSL traffic also gets diverted to the ISP's servers so I suspect that they are somehow using Man-in-the-middle (MITM) to achieve this and that would involve using a none to trust worthy CA certificate on my machine.

My first step was to clean out the Windows certificate store and this resulted in myself writing this program because the tools used by Windows are not very helpful and have hardly changed over the past twenty years.

Using the Code

I added a form to the project as can be seen in the image at the top of this screen that uses a class '`CertStore`' to retrieve a collection of machine/user certificates with a tree structure using '`CertItem`' so that CA Certificates contain a collection of child certificates that are better known as intermediate certificates that are authorized by the CAs.

Add the files *CertStore.cs* and *Helper.cs* to your own project if you want a list of Windows certificates in your project using the code below.

```
using System;
using System.Collections.Generic;
using CertCheck;

Dictionary<string, CertItem> Certificates =CertStore.LoadCertificates();
foreach (CertItem I in Certificates.Values)
    {
        //Do your thing here or call I.Delete(); to delete the CA certificate and any children
    }   //See I.ErrorMessage for any warnings about the certificate
```

Reading Windows certificates in .NET is easy using a `X509Certificate2` and `X509Store` from the '`System.Security.Cryptography.X509Certificates`' namespace as shown in the code snippet below:

```
using System;
using System.Collections.Generic;
using System.Security;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;

Dictionary<string,CertItem> DicCA=new Dictionary<string, CertItem>
(StringComparer.OrdinalIgnoreCase);
Dictionary<string, CertItem> DicCASorted = new Dictionary<string, CertItem>();
X509Store store = new X509Store(StoreName.Root, StoreLocation.CurrentUser);
store.Open(OpenFlags.ReadOnly);
foreach (X509Certificate2 Cert in store.Certificates)
     {//Load up the CA Certificates for this user
       CertItem I = new CertItem(Cert,store, "CAUser",true);
       DicCA.Add(I.Name  + I.Thumbprint , I);
     }
//you could use I.Delete() to delete the certificate but the app must run with admin rights to
do this
```

The store location here is '`CurrentUser`' but you might also like to use '`LocalMachine`' to get the rest of the certificates and also change the `StoreName` to access personal certificates or other stores.

Windows certificates also contain thumb prints and you should not delete any certificates using the thumb prints shown below as it might stop your machine from working and the frontend I have put on this program prevents you from making this mistakes but you can find out more detail about these certificates here.

Do not delete certificates with these thumb prints.

```
00c1008b3c3c8811d13ef663ecdf40            4a19d2388c82591ca55d735f155ddca3,

03c78f37db9228df3cbb1aad82fa6710,         79ad16a14aa0a5ad4c7358f407132e65,

03c78f37db9228df3cbb1aad82fa6710
```

If you have Windows updates turned on, then Microsoft will often add new certificates to your certificate store automatically without warning and some of the certificate encryption keys Microsoft uses are hardcoded into Windows, but I see it as the fox is guarding the chicken house and keep my updates turned off.

How Safe is SSL?

When Alice wants to talk to Bob, she sets up a SSL Connection and Bob sends her back a very expensive key with 256 teeth and she then builds a lock for the key and puts her cheap session key into a steel box and locks it with the padlock she built around Bob's key and she then sends it back to Bob who has the master key for the expensive padlock.

Bob opens the box using his master key and once the handshake is over, they send love letters to each other but they don't use Bob's lock, they use Alice's cheap lock and key!

This guy says it better than me Youtube HTTPS.

License

About the Author

Dr Gadgit

United Kingdom

Old dog that is tired of learning new tricks when the new dish they are cooking never tastes quite so good as the old one.

Comments and Discussions

1 message has been posted for this article Visit **https://www.codeproject.com/Tips/1010900/Windows-SSL-Certificate-Cleaner** to post and view comments on this article, or click **here** to get a print view with messages.