Using a self signed certificate

There is nothing that will stop you from using a self signed certificate with Smartcrypt. The most important part with certificates is the trust chain. By definition, a self signed certificate is only trusted by the machine that generates the certificate.

Certificates trust can be deployed through group policy, or it can be done on individual machines.

> To do the following on Windows, you will need to have administrative rights on the machine. Also, proceeding is at your own risk. Adding certificates to be trusted should only be done for certificates you know the source and the producer of the certificate.

Generating a self-signed certificate for the Smartcrypt Manager

The simplest method is to use PowerShell 4.0. This comes as part of Server 2012R2. If you are using something older, you will need to use another method.

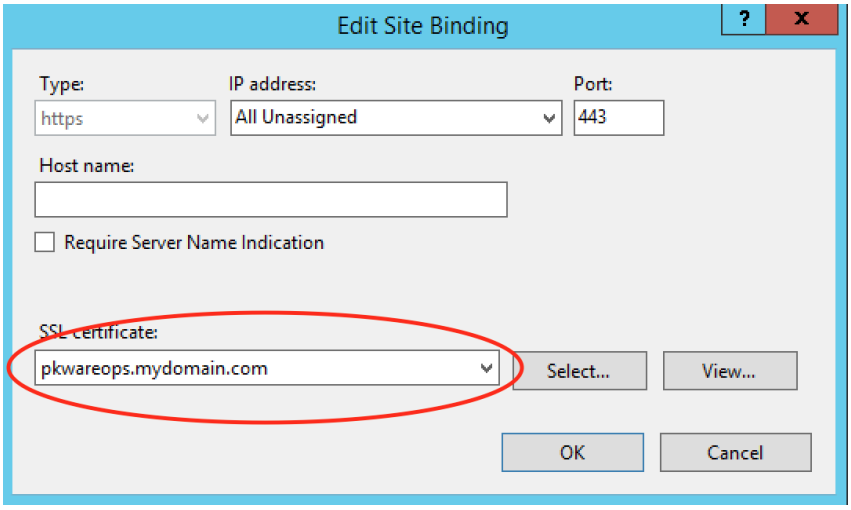
Step 1:

Example

```
New-SelfSignedCertificate -DnsName pkwareops.mydomain.com -CertStoreLocation cert:\LocalMachine\My
```

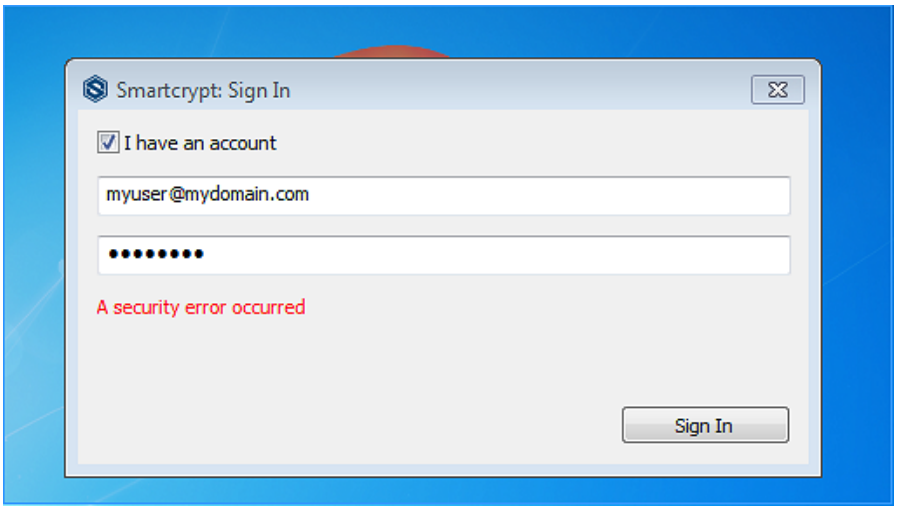
Step 2:

Edit the https bindings of your site and select the newly created certificate. *(Note, you will need to visit this site from client devices you wish run the Smartcrypt Application and choose to trust this certificate)*

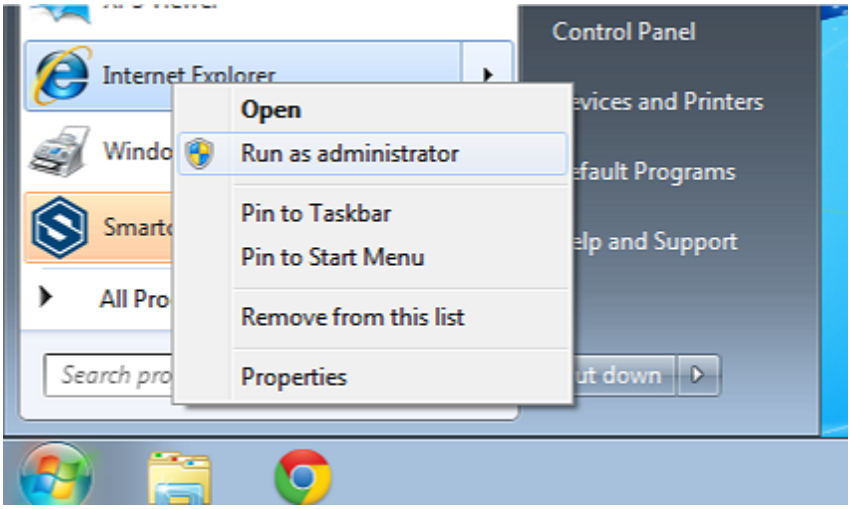


How to determine if your certificate used for the Smartcrypt Manager is trusted on a machine

The Smartcrypt client will display an error if the certificate is not trusted

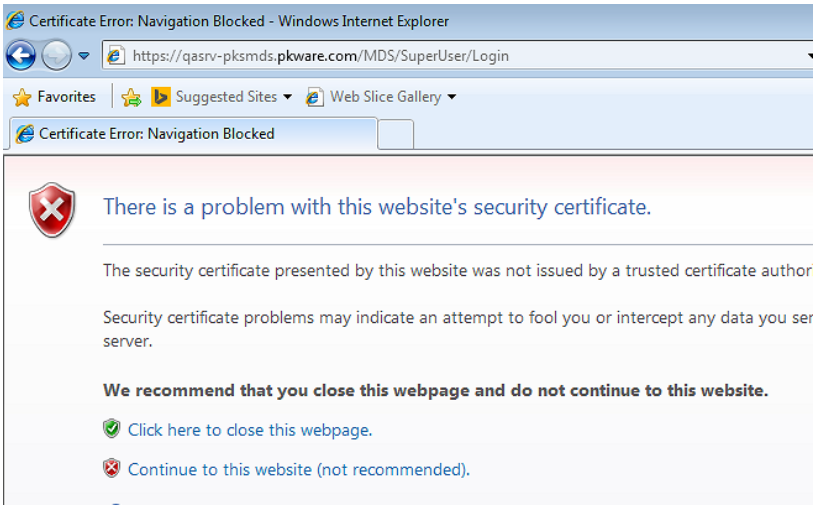


You can also verify this by browsing the Smartcrypt Manager in Internet Explorer. As a shortcut, open Internet Explorer as an Administrator so we can export the certificate



Now that Internet Explorer is open, browse to the Smartcrypt Manager login page. This will be different per installation, but it will ender with /superuser/login

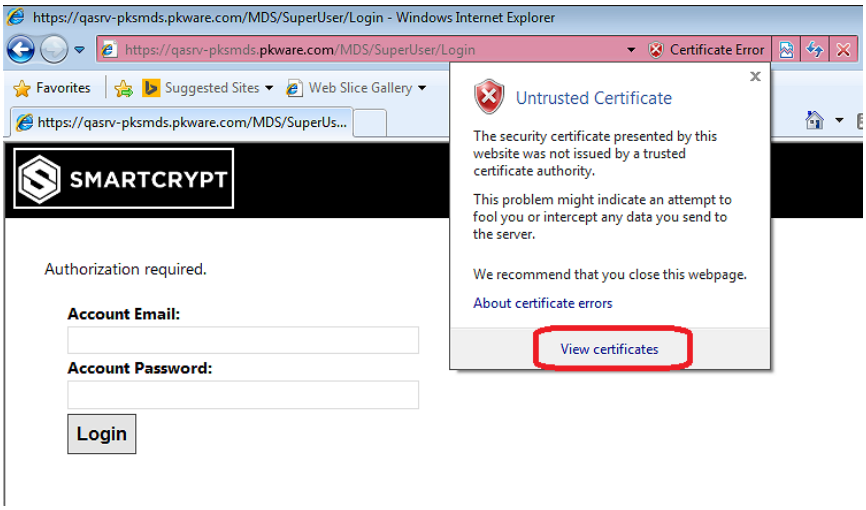
```
https://pkwareops.mydomain.com/mds/superuser/login
```



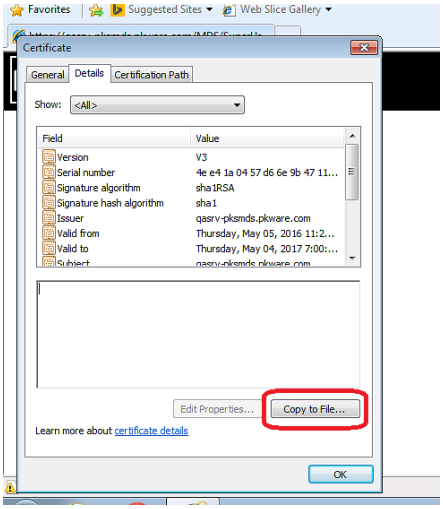
If you see the warning "There is a problem with this website's security certificate," the self signed certificate is not trusted.

How do I get a self signed certificate from Internet Explorer?

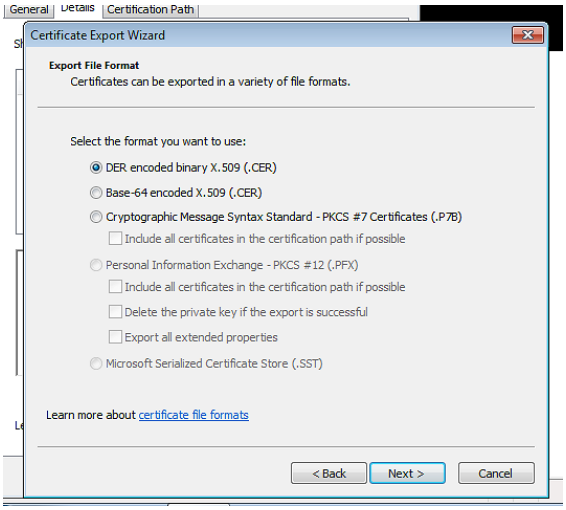
After opening Internet Explorer as an Administrator, you can export the the certificate being served by the Smartcrypt Manager. Click the red x that says "Certificate Error" and select "View Certificates"



In the certificate window that opens, look at the Details tab to export the certificate by clicking the button that say "Copy to file"

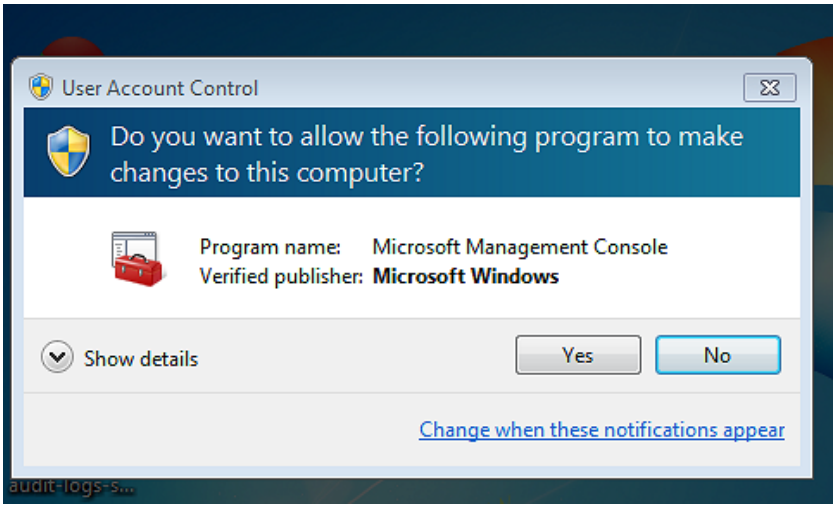


The certificate export wizard will open. The .der format is fine for exporting. Then select a location to save the certificate to.

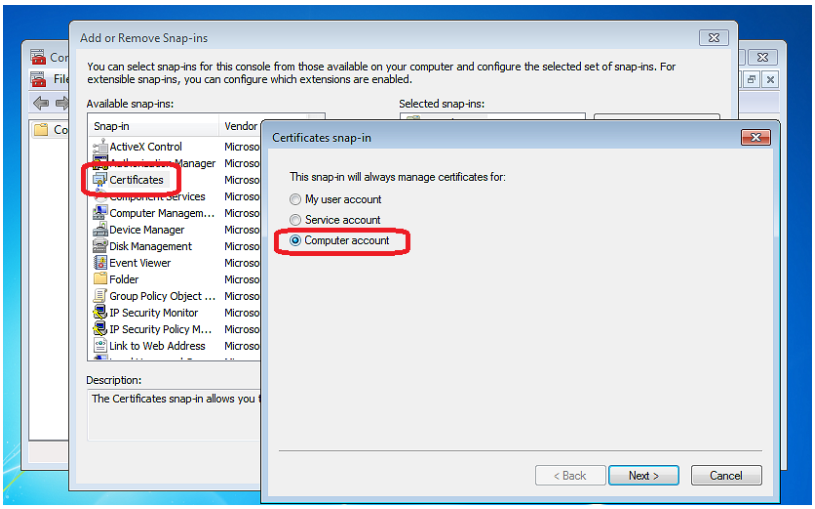


I have the certificate, how do I force my machine to trust it?

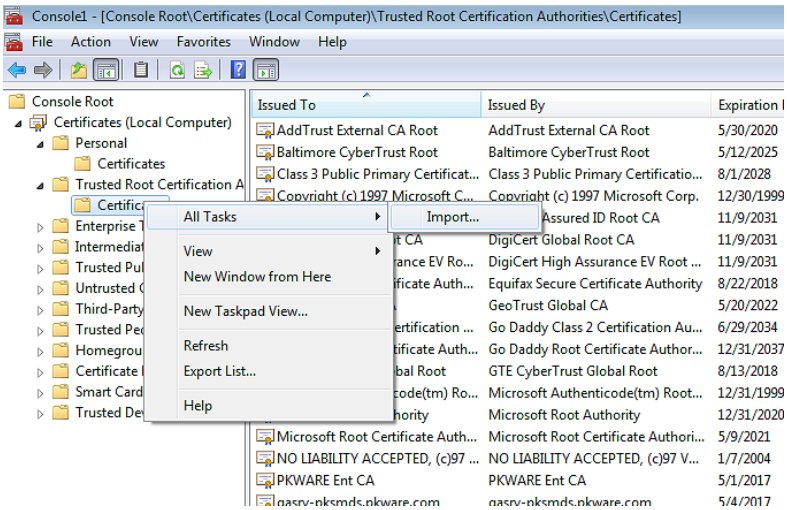
Open the tool Microsoft Management Console (MMC)



From the file menu option, select Add/remove Snap-in. In the list of Snap-ins, select Certificates. When prompted for what to manage, select computer account



In the list of Certificate groups, find "Trusted Root Certificate Authorities" and expand the option. The certificates option should display. Right click and select Import



Browse to the .der file that was exported and select the certificate to complete the process. You should see a new row in the Trusted Root Certificate Authorities list. To confirm the certificate is trusted close Internet Explorer. Relaunch and browse to the Smartcrypt Manager login page. Internet Explorer should not alert you to any trust issues.