**Sectigo Certificate Revocation List Configuration:**

**Introduction:**

**The Issue:**  Sectigo Certificate Revocation List publication is out on the internet and the environment does not allow outbound internet access. Thus causing the Sectigo Certificate Chain to be unable to resolve the revocation list so it will start searching for ways to resolve the list thus slowing the connection down.

**Resolution:**  Make some configuration changes so the servers can find the published certificate revocation lists so it can validate the certificate.

**Technical Requirements:**

Have the following urls resolve properly:

<http://equifax.crl.sectigo.com/EquifaxGlobalRootCA.crl>

<http://equifax.crt.sectigo.com/EquifaxGlobalRootCA.crt>

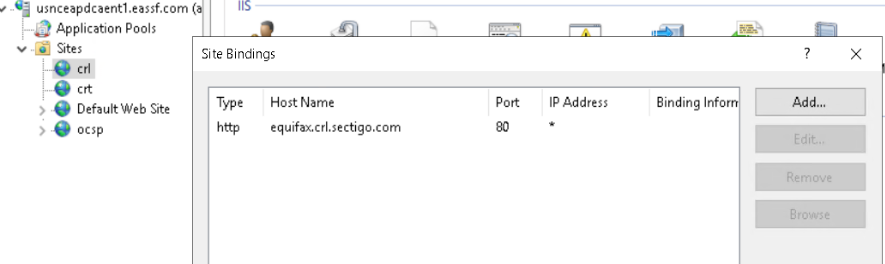
**Configure** **Work Around:**

Configure an IIS server with internet and configure hosts file with the following:

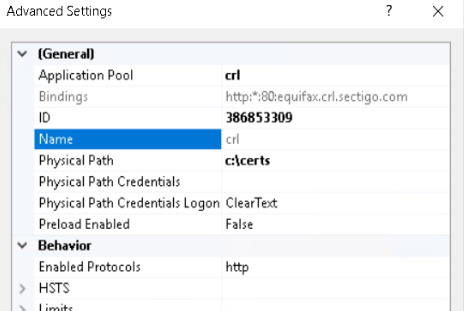
10.12.14.133 equifax.crl.sectigo.com

10.12.14.133 equifax.crt.sectigo.com

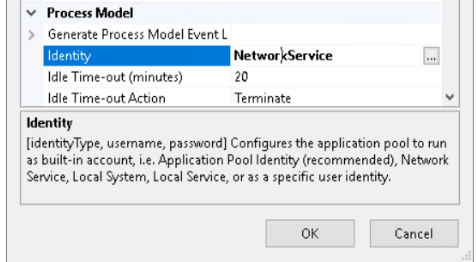
On IIS Host Create 2 new websites. CRT and CRL with the sectigo urls on port 80.



Both website’s physical path along with all other eassf.com revocation list point into c:\certs

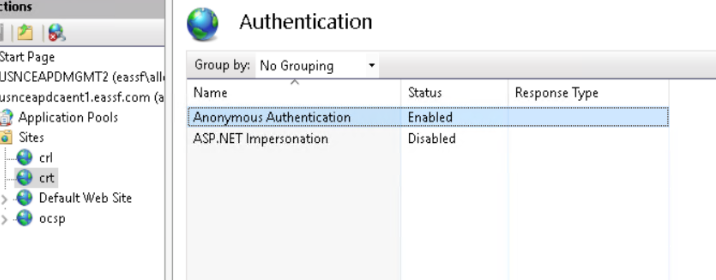


For both these websites, under application pool→ advanced settings→ Under Identity I selected “Network Service”

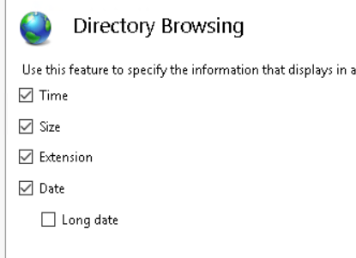


**Make things Visible:**

In IIS Manager go to Authentication. Enable Anonymous access



In IIS Manager go to Directory Browsing. Enable it



**Delegate permissions**

Next you need to go to File Manager and set both file and share permissions

You need to make sure of the following

Anonymous - read Domain Admins - Full

Domain users - read Administrators - Full

Network service - modify Certificate Publishers Full

**Get CRL and CRT files:**

Download the .crt and .crl. Use the NPS server to download these 2 files and copy to c:\certs of usnceapdcaent1.

**Publish:**

Rdp to usnceapdcaent1 and publish the .crt. And crl with the following commands:

certutil -dspublish -f c:\certs\EquifaxGlobalRootCA.crt rootca

certutil -dspublish -f c:\certs\EquifaxGlobalRootCA.crt ntauthca

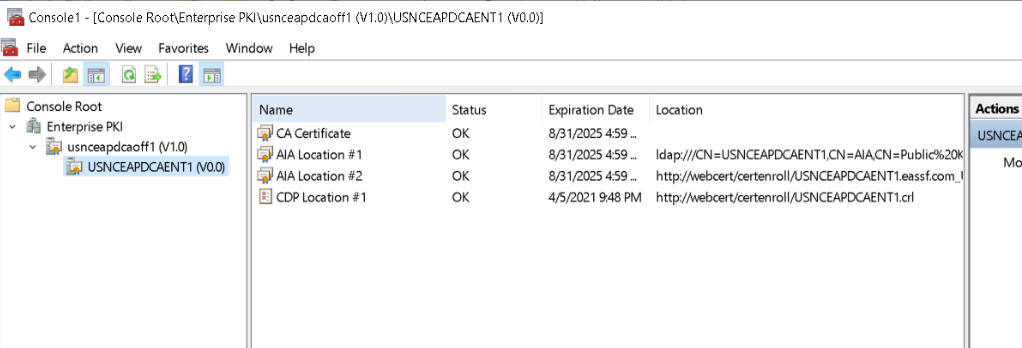
certutil -dspublish -f c:\certs\EquifaxGlobalRootCA.crl root-ca

**Validate and Verify:**

Also validate the certificate to make sure everything is reachable

Certutil -f -urlfetch -vetrify EquifaxGlobalRootCA.crt or the equifax ssl certificate

On Mgmt2. Start-->Run-->mmc.exe add/remove snapin → Enterprise PKI. Verify that all is clear and there are no errors like the picture below



Next Check each Active Directory Containers. Highlight Enterprise PKI→ Action--Manage Active Directory Containers. Go through each one and the only container that should have errors is the CDP container and that’s because of expired crls. You can delete the expired CRLs.

**Automation:**

Sectigo publishes a new CRL every week. So to make things easier there are 2 azure automation jobs that run daily..

Create a script to automatically download to and publish to new location