Certificate Services – Migrate from SHA1 to SH (SHA256)

KB ID 0001243 ***Dtd*** 10/10/16

Problem

It's time to start planning! Microsoft will stop their browsers displaying the 'lock' icon for services that are secured with a certificate that uses SHA1. This is going to happen in February 2017 so now's the time to start thinking about testing your PKI environment, and making sure all your applications support SHA2.

Note: This includes code that has been signed using SHA1 as well!

Solution

Below I'm just using an 'offline root CA' server, if you have multi tiered PKI deployments, then start at the root CA, fix that, then reissue your Sub CA certificates to your intermediate servers, fix them, then repeat the process for any issuing CA servers. Obviously if you only have a two tier PKI environment you will only need to do the root and Sub CA servers.

For your SubCA's see PART TWO of this article.

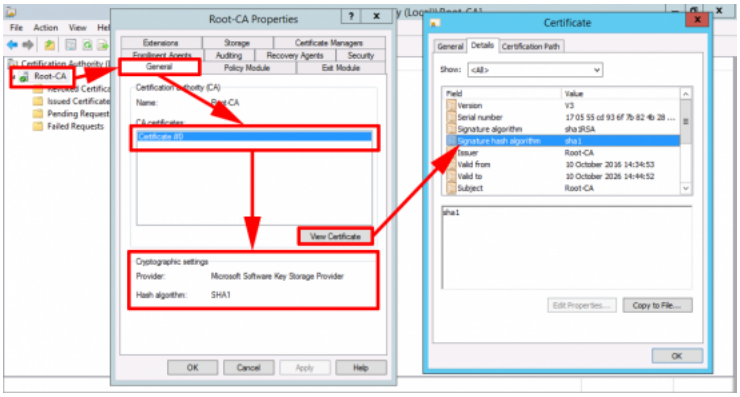
Upgrade Your Microsoft PKI Environment to SHA2 (SHA256)

What about certificates that have already been issued?

We are **NOT** going to revoke any CA certificates that have already been issued so existing certificates will remain unaffected.

Here we can see my CA server is using SHA1

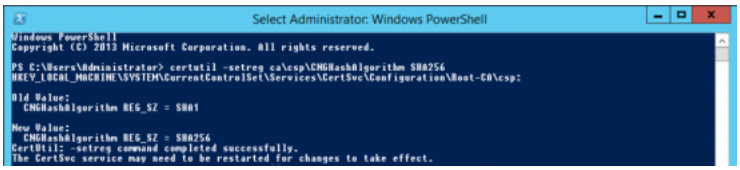
Note: If your server says the provider is ***Microsoft Strong Cryptographic Provider*** and not ***Microsoft Software Key Storage Provider*** then skip down a bit.



You may have multiple Certificates (that is not unusual).

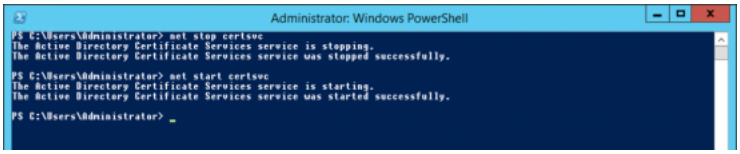
Open a PowerShell Window (run as administrator), issue the following command;

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
```

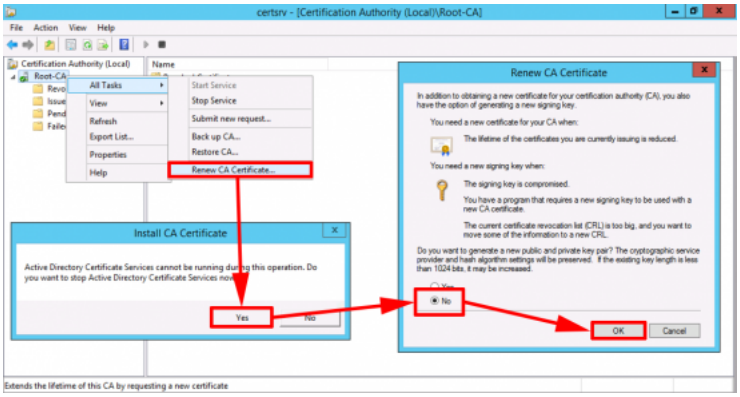


Restart Certificate Services.

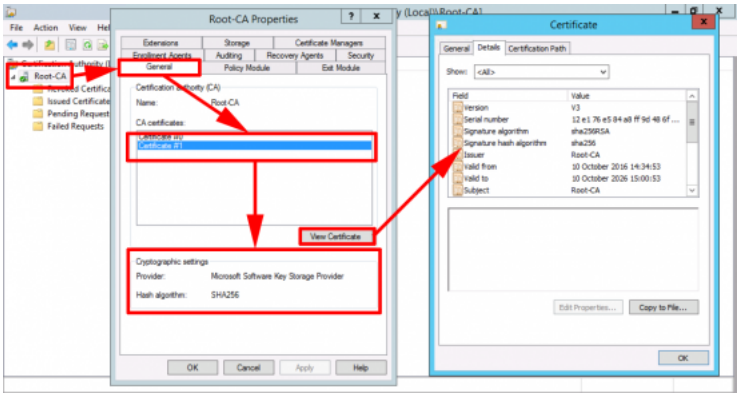
```
net stop certsvc
net start certsvc
```



Now you need to generate a new CA certificate.

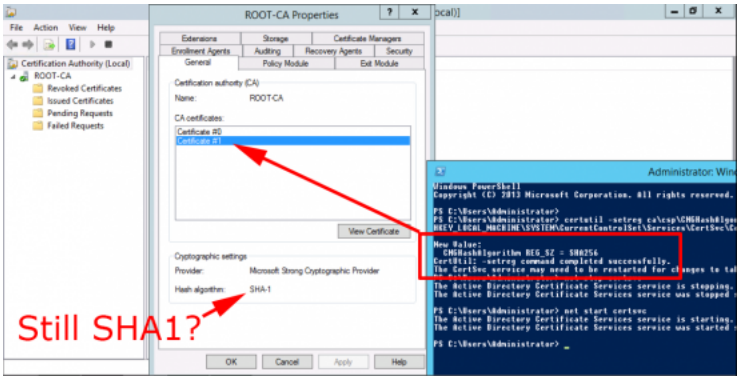


Now you can see your new cert is using SHA256.

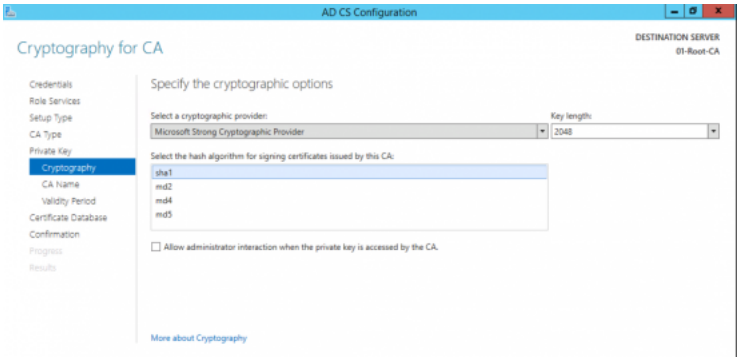


Mine Won't Change From SHA1?

That's because your cryptographic provider does not support higher than SHA1, for example 'The command to change to SHA256 was successful, but the new certificate still says SHA1. If you look the Provider is set to '***Microsoft Strong Cryptography Provider***'.

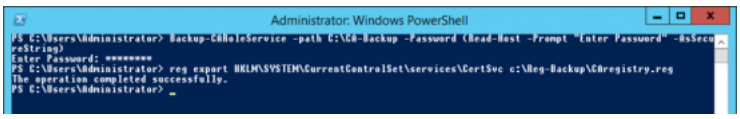


As you can see the strongest hash algorithm that supports is SHA1 that's why it refuses to change.



How Do I Change the CA Cryptographic Provider?

Make a backup of the CA Settings and the CA registry Settings.




```
Backup-CARoleService -path C:\CA-Backup -Password (Read-Host -Prompt "Enter Password" -AsSecureString)
TYPE IN A PASSWORD
reg export HKLM\SYSTEM\CurrentControlSet\services\CertSvc c:\Reg-Backup\CAregistry.reg
```

Note: You might want to create the Reg-Backup folder first and grant some rights to it.

Now we need to delete the certificates this CA uses (don't panic we've backed them up!) But first we need to find the certificate's hashes to delete. Open an administrative command prompt, stop certificate services, and then

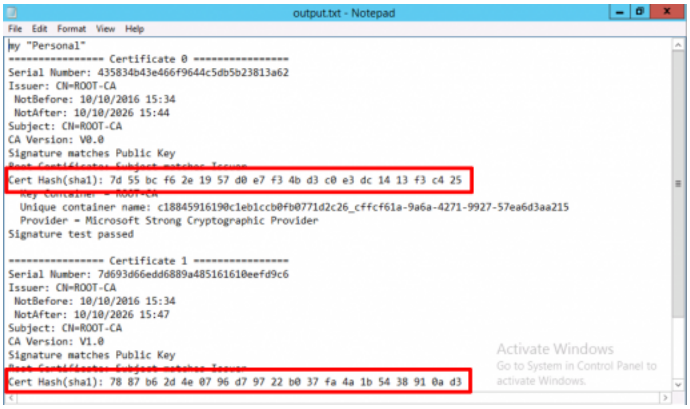
issue the following command;

Note: ROOT-CA is the name of **YOUR** CA.

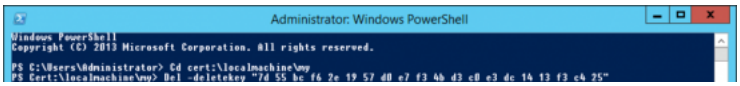
```
Stop-service certsvc

Certutil -store my ROOT-CA >output.txt
```

Open ***output.tx***t then take a note of the hashes for the certificate(s)



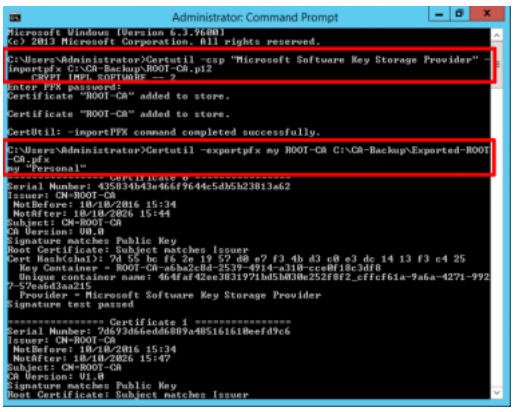
Then Open an Administrative PowerShell window and delete them;




```
cd cert:\localmachine\my
Del -deletekey <Certificate HASH>
```

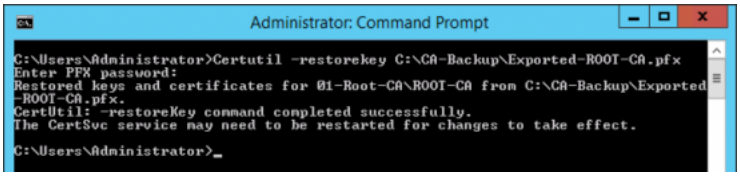
Now we need to import the p12 file we backed up earlier, then export that as a PFX file. Change ROOT-CA to the name of YOUR CA and the path to your backup folder and certificate as approriate.

```
Certutil -csp "Microsoft Software Key Storage Provider" -importpfx C:\CA-Backup\ROOT-CA.p12
Certutil -exportpfx my ROOT-CA C:\CA-Backup\Exported-ROOT-CA.pfx
ENTER AND CONFIRM A PASSWORD
```

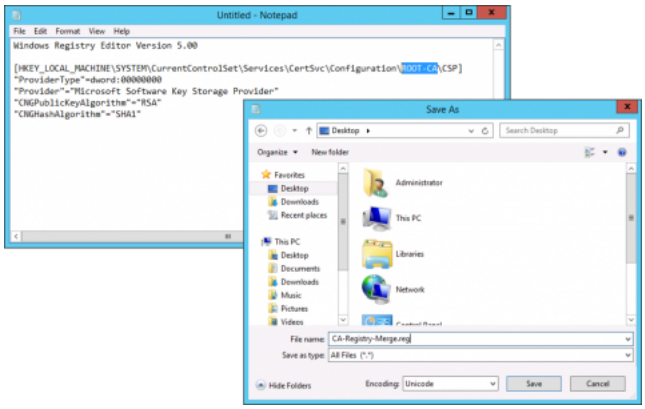


Then restore the key from your PFX file.

```
Certutil -restorekey C:\CA-Backup\Exported-ROOT-CA.pfx
```



Now you need to import a couple of Registry files, in the examples below replace ROOT-CA with the name of your CA



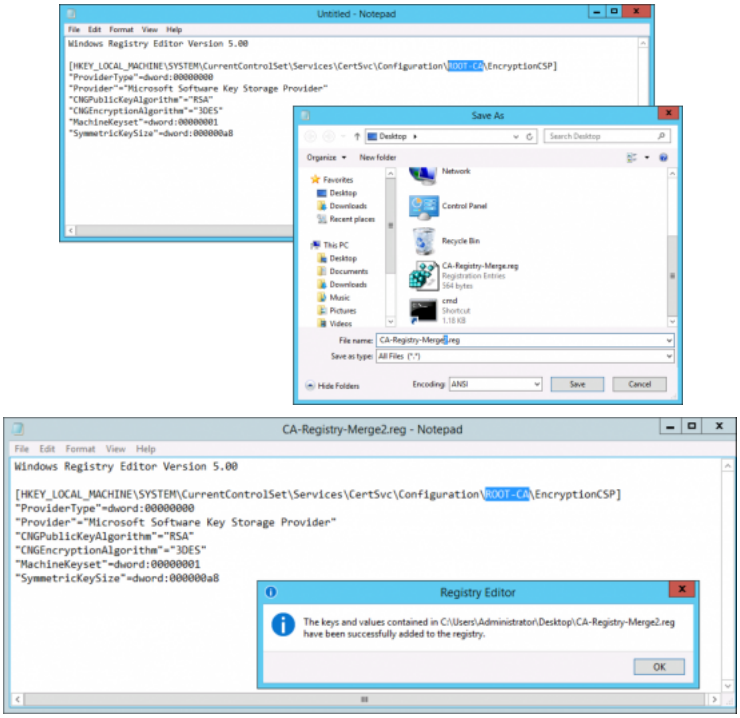
Save the file as CA-Registry-Merge.reg (set the save as file type to All Files)


```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ROOT-CA\CSP]
"ProviderType"=dword:00000000
"Provider"="Microsoft Software Key Storage Provider"
"CNGPublicKeyAlgorithm"="RSA"
"CNGHashAlgorithm"="SHA1"
```

Merge the file into the registry.

Repeat the process with the following regisry file save this one as CA-Registry-Merge2.reg



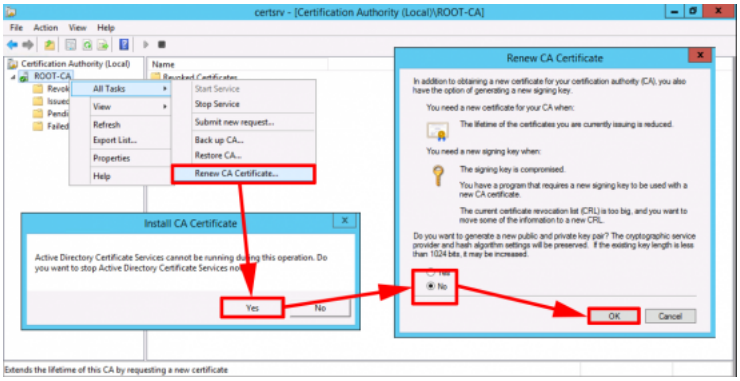

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ROOT-CA\EncryptionCSP]
"ProviderType"=dword:00000000
"Provider"="Microsoft Software Key Storage Provider"
"CNGPublicKeyAlgorithm"="RSA"
"CNGEncryptionAlgorithm"="3DES"
"MachineKeyset"=dword:00000001
"SymmetricKeySize"=dword:000000a8
```

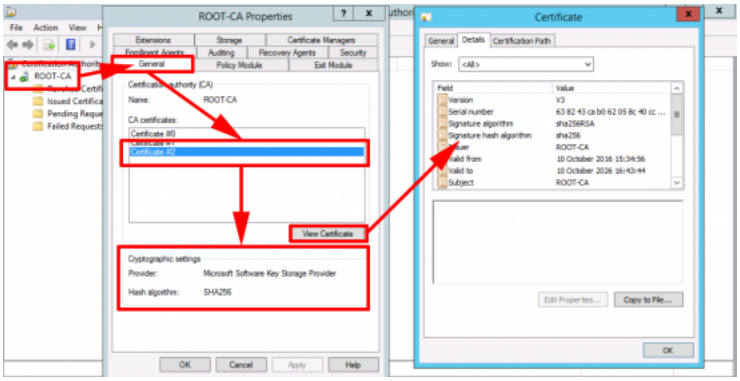
Now change the hashing algorithm to SHA256, open an administrative command prompt and issue the following two commands;

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
net start certsvc
```

Renew the CA Cert.



You can now see the new cert is using SHA256.



Related Articles, References, Credits, or External Links

NA

Author: PeteLong

Share This Post On

18 Comments

Cesar Olivares

15/02/2017

Great article! Especially the part where your CA does not change SHA1, if you allow me, I will post it on my blog in Spanish referring to your article

Post a Reply

Juergen

30/03/2017

As far as I know this only works on Server 2012 (changing the cryptographic provider). Any workaroud for Server 2008 R2.
Thanks, Juergen

Post a Reply

PeteLong

03/04/2017

I've not tried with 2008/2008R2 but that's getting a bit long in the teeth now, mainstream support for this stopped in 2015, why should Microsoft even bother trying to make this work?

Post a Reply

Edmund

29/07/2017

Hey Pete,

Great Article. I'm about to go through this process on my environments. Any recommendation on testing this on a possible offline or dev environment? How would I go about re-creating my existing MS CA into a "dev" stack environment where I can test this?

Another idea i had was to run 2 local 2 tier CA's in paralell (my existing prod CA) and my new CA. Does that work? I could not find any readings on google...(doesn't seem like people have done that)? I'm simply trying to make this upgrade process less risky...

Post a Reply

PeteLong

02/08/2017

I just span up a test model in VMware before I did is 'Live'. If you CA's are physical P2V them int a sandbox environment and perform the upgrade on the replicas to test. If they are already virtual, either clone them or get a free trial of Veeam and use that to replicate the environment.

Pete

Post a Reply

Chev

24/10/2017

what will happen to existing certificates issued by the server after the upgrade to SHA1 to SHA2?

Post a Reply

PeteLong

24/10/2017

They work till they expire ☺ unless something that uses them drops support for SHA1 of course!

P

Post a Reply

JohnV

15/12/2017

Read two other articles and still had issues, multiple checkpoint removals later I found your article and I am up and running on SHA2 certs.

Post a Reply

PeteLong

19/12/2017

Good new glad you are fixed ☺

P

Post a Reply

bala

16/01/2018

Do we need to renew the Root CA is it mandatory? will it cause any issues with the existing certs?

Post a Reply

PeteLong

16/01/2018

I would say yes, you previous Root CA cert still stands, so certificates already issued will not be affected.

P

Post a Reply

Ewald Bracko

18/01/2018

A really well done Step-by-Step article!
I had no issued while following the whole explanation including the “change cryptography provider” part.
Keep up your good work!

Best Regards

Ewald

Post a Reply

PeteLong

18/01/2018

Thanks for the feedback!

Post a Reply

Sultan

12/03/2018

Hello and thank you for this article. I tried without success to apply this to my sbs 2011 stardard server.
Do you think that it's possible to change the "Microsoft Strong Cryptography Provider" to an anather provider SHA-2 compatible ?

Post a Reply

PeteLong

13/03/2018

To be honest it's not something I've done, but I'll publish the question in case someone wants to answer.

Post a Reply

Ray

20/03/2018

Great stuff! Just ran this on my CA when we moved our servers from 2008 R2 to 2016 CU8. Worked perfectly, well written.

Post a Reply

PeteLong

21/03/2018

Thanks for the feedback!
P

Post a Reply

Coert

02/05/2018

Very nice! Thank you.

Post a Reply

Submit a Comment

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Submit Comment

Cop