Renew Windows root CA certificate

https://4sysops.com/archives/renew-windows-root-ca-certificate/

A certification authority (CA) cannot issue certificates with a longer validity period than its own CA certificate. Therefore, it is crucial to renew the CA certificate in a timely manner. You can use this opportunity to set some parameters for the new certificate. You can perform this task using *certsrv.msc* and *certutil.exe*.

Contents

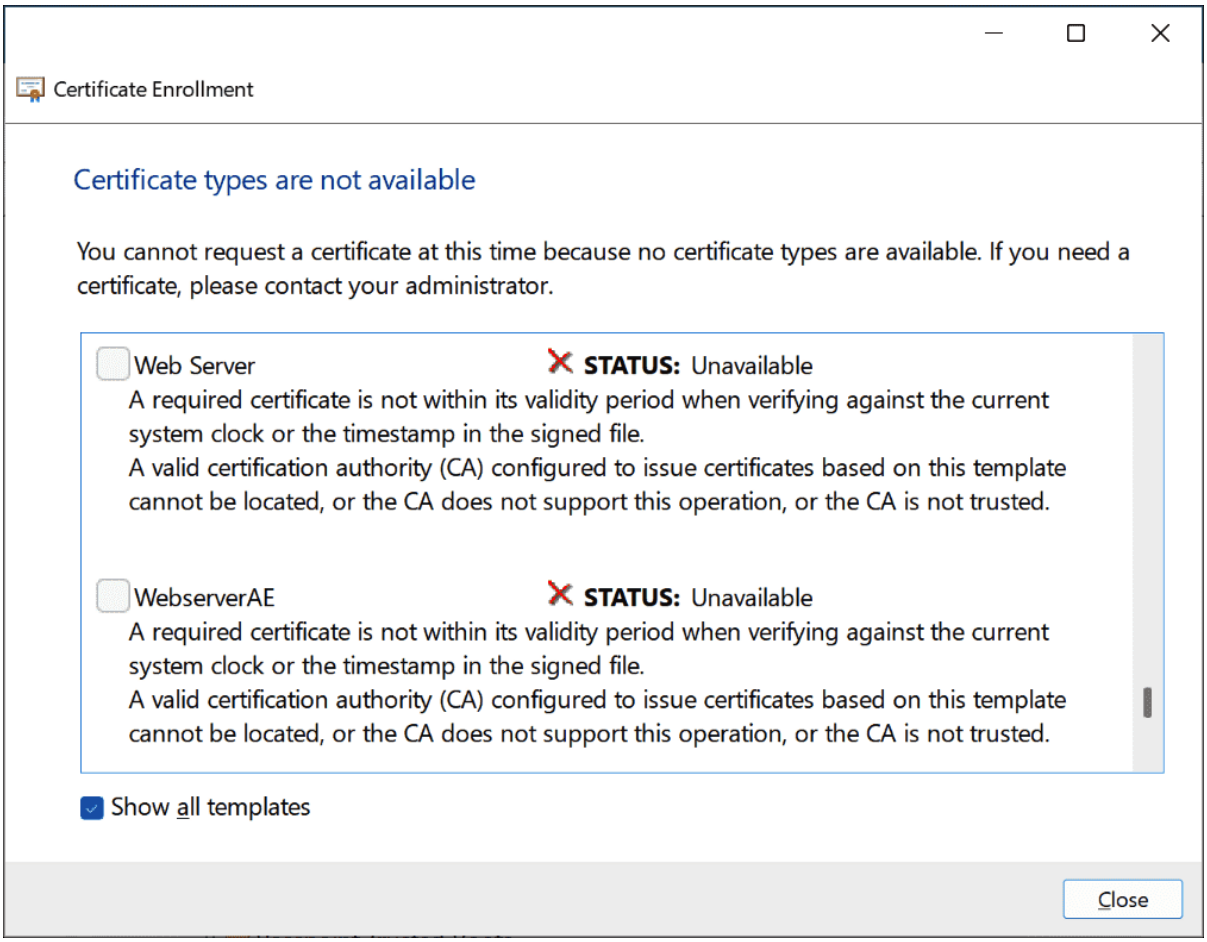
1. Issue of certificate failures
2. Show the CA certificate's expiration date
3. Options for new certificates
4. Renew CA certificate
5. Distribute the root certificate to the clients
6. Summary

If the CA certificate has expired, the certification authority will be unable to issue new certificates. This results in error messages that unfortunately do not immediately indicate the actual cause.

Issue of certificate failures

In this case, attempting to issue certificates through *certmgr.msc* or *certlm.msc* may lead to the certificate templates dialog box displaying an empty window. When you activate the *Show all templates* option, the following message appears:

A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file. A valid certification authority (CA) configured to issue certificates based on this template cannot be located, or the CA does not support this operation, or the CA is not trusted.

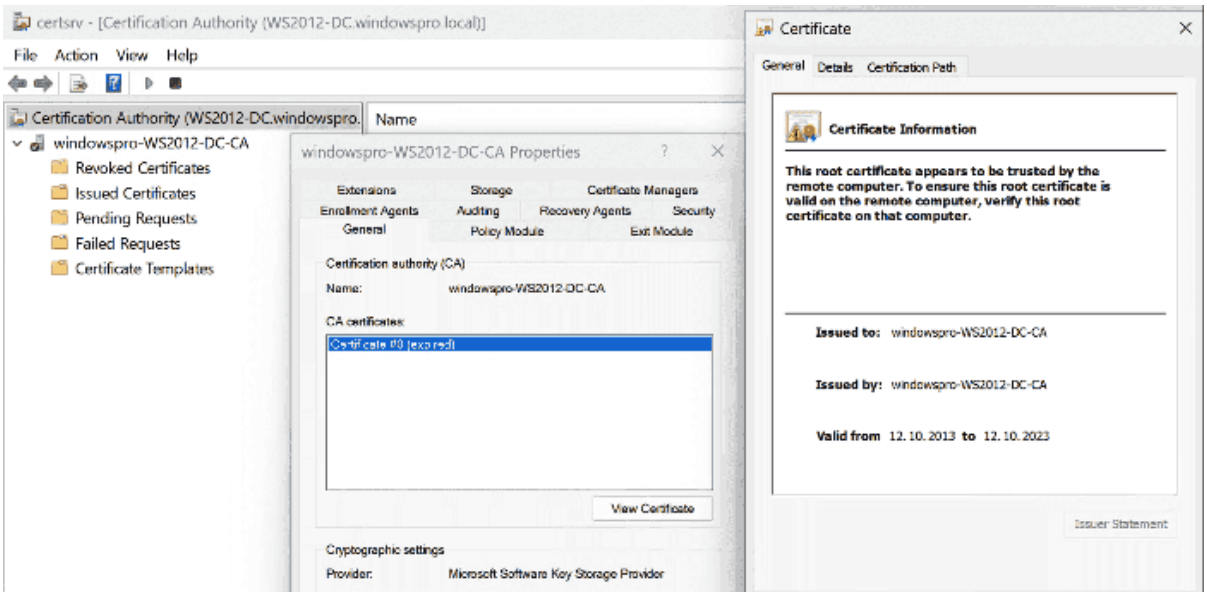


Error message in the Certificate Enrollment Wizard after the CA certificate has expired

If you use the *Get-Certificate* cmdlet to request a certificate, you will get error code 0x800b0101.

Show the CA certificate's expiration date

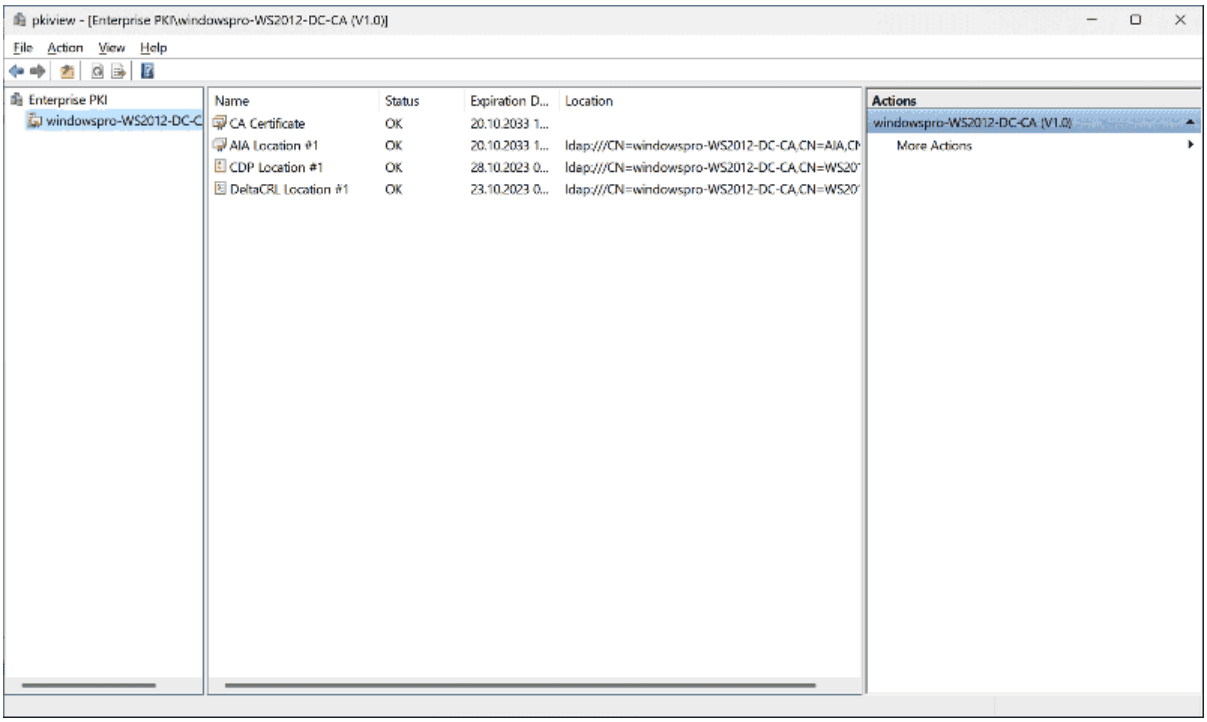
To check the expiration date of the current CA certificate, launch the *Certificate Authority* MMC snap-in (*certsrv.msc*). From there, open the properties in the context menu of the CA, and under the *General* tab, you'll find a list of all the issued CA certificates.



Show a CA certificates properties in certsrv.msc_

The overview also displays their index and may mark a certificate as *expired*. Additionally, you can open the details of a certificate from here to verify its expiry date.

The basic data of the CA certificate can also be found in *pkiview.msc*.



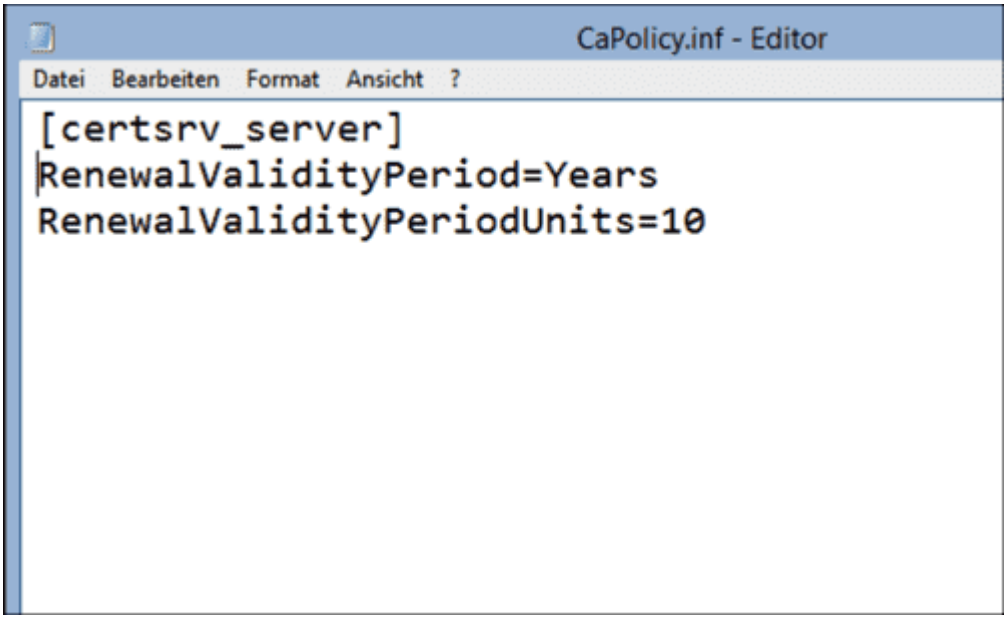
The MMC snap in pkiview.msc displays the certificates expiration date and its general health status

Options for new certificates

If it's necessary to issue a new CA certificate, you don't have to do it with the default values. Instead, you can preconfigure several parameters. To do so, create a file named *CaPolicy.inf* and enter the following lines, for example, to extend the certificate's validity to 10 years:

```
[certsrv_server]
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=10
```

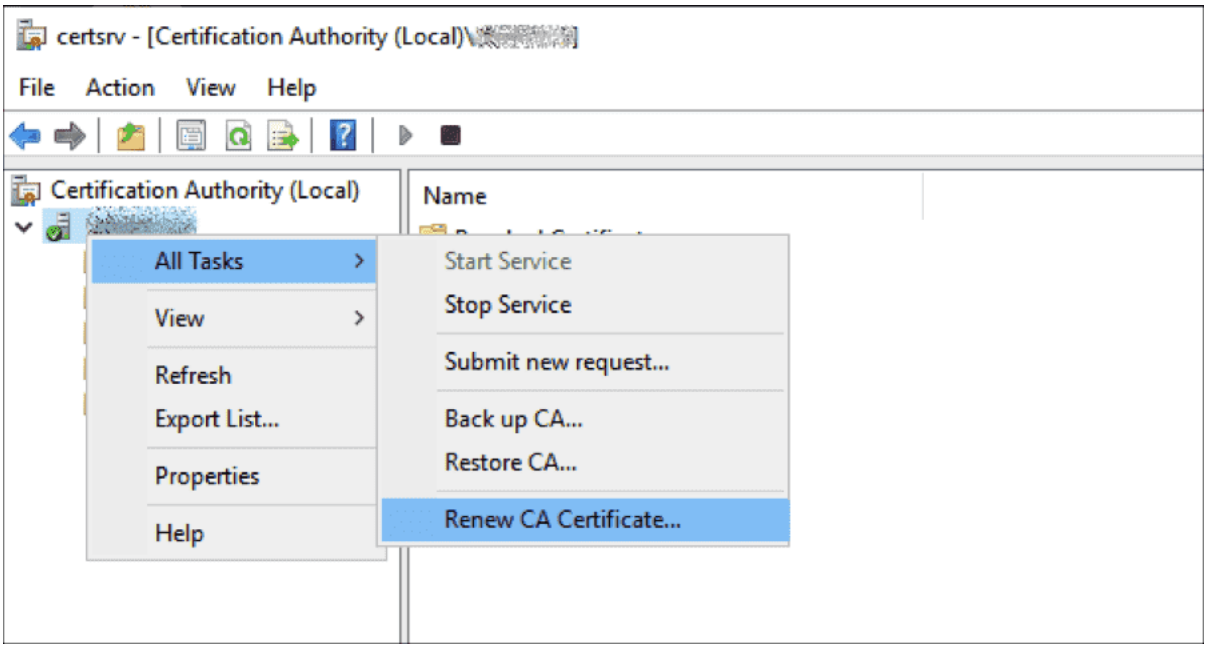
The configuration supports several other parameters. You can find an overview of all the supported entries in Microsoft's documentation. Copy the file to the Windows directory (%SystemRoot%) on the CA server.



Entries in CaPolicy.inf to set the validity of a new CA certificate to 10 years

Renew CA certificate

For this task, open the context menu of the Certification Authority in *certsrv.msc*, and select the *Renew CA Certificate* option under *All Tasks*.



Renew CA certificate via the MMC snap in Certification Authority

This action launches a wizard, which first announces that certificate services need to be temporarily stopped. The next dialog box allows the user to choose whether to retain the signing keys or generate new ones.

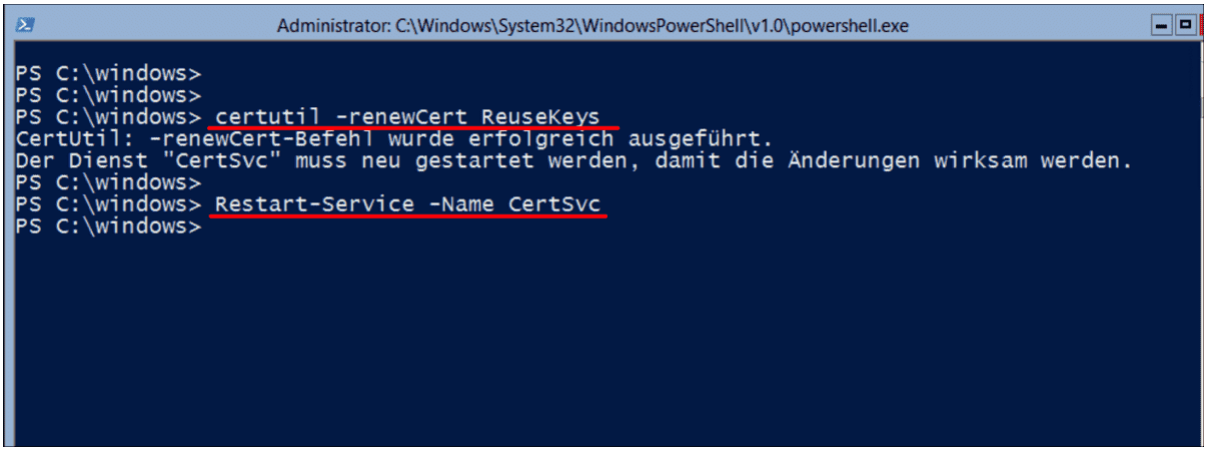
Microsoft names compromised existing keys, specific software requirements, or an overly long certificate revocation list (CRL) as possible reasons for generating new keys.

With new keys, the certification authority also creates a new CSR that only contains the serial numbers of certificates revoked since the issuance of the new CA certificate. Microsoft's documentation explains how this affects the naming of the CRL.

Retaining the keys simplifies the process because it keeps all previously issued certificates chained up to the new CA certificate. For an in-depth discussion of the pros and cons of new signing keys, refer to this blog post by Vadims Podāns.

As an alternative to the *certsrv.msc* GUI, you can use the *certutil.exe* utility to renew the CA certificate while retaining the existing public and private keys:

```
certutil -renewCert ReuseKeys
```



Renew the CA certificate with certutil.exe while reusing the previous keys

If you omit the *ReuseKeys* switch, the utility also creates new keys. With the following entry in the abovementioned CaPolicy.inf, you can set the key length, in this example to 2048 bits:

```
RenewalKeyLength=2048
```

Distribute the root certificate to the clients

After renewing the root CA certificate, you must deploy it to the clients to make them trust all certificates issued by the certification authority. Windows PCs store this certificate under cert:\LocalMachine\Root or under a user's trusted root certificates.

If you are running an enterprise CA, the root certificate is automatically distributed within the domain. Clients receive it during the refresh of Group Policies. If you want to speed up this process, you can force a refresh using gpupdate /force.

In the case of a standalone CA, you have to export the certificate and publish it in Active Directory using the following command:

```
certutil -f -dspublish <RootCACertificate-File> RootCA
```

This method ensures that the root certificate is propagated to all machines in the domain. Alternatively, you can distribute the root certificate via Group Policy, especially if you want to provide it only to specific OUs.

To determine the type of CA you are dealing with, you can use the following method:

```
certutil -getreg ca\\catype
```

Summary

The expiration of a CA certificate significantly impairs a certification authority. Therefore, it is crucial to take timely action to renew the certificate. Typically, you wouldn't do this at the last moment because the remaining validity period of the CA certificate determines the maximum validity of the certificates it issues.

You can use tools such as *certsrv.msc* or *certutil.exe* to renew the CA certificate. During the renewal process, you must decide whether you want to generate new keys as well. Maintaining the existing keys simplifies the task, but certain circumstances, such as a long CRL or a potential key compromise, may necessitate generating a new key pair.

Before renewing the CA certificate, you can configure various options, including its validity period, using the *CAPolicy.inf* file.

Subscribe to 4sysops newsletter!

After successfully issuing a new certificate for a root CA, you need to distribute it to clients. This process is automatic for an enterprise CA, but for a standalone CA, you can use *certutil.exe* or a Group Policy Object to achieve this.