



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies

ⓘ We're no longer updating this content regularly. Check the [Microsoft Product Lifecycle](#) for information about how this product, service, technology, or API is supported.

[Return to main site](#)



Basic CRL checking with certutil

Article • 11/30/2006

I want to start this blog with a very basic topic: CRL checking.

In the past we have documented a lot about CRL checking but I am still seeing that people have difficulties to verify if a certificate is valid or not. We have two whitepapers about CRL troubleshooting:

- [Troubleshooting Certificate Status and Revocation](#) which is the initial version of the whitepaper (don't know why this document is still

out there)

- [Certificate Revocation and Status Checking](#) which is the updated version of the initial whitepaper

Certutil.exe is the command-line tool to verify certificates and CRLs. To get reliable verification results, you must use certutil.exe because the Certificate MMC Snap-In does not verify the CRL of certificates. A certificate might be wrongly shown in the MMC snap-in as valid but once you verify it with certutil.exe you will see that the certificate is actually invalid.

Remember, that certutil.exe operates in the security context of the current session context. This is important if you need to verify the validity of computer certificates. What if your current user session has the right proxy settings but the machine context does not? In Windows Server 2003 and Windows XP, the proxy configuration of the machine context can be configured with proxycfg.exe. In Windows Vista and Windows Server Codename Longhorn, use netsh winhttp show proxy to verify the proxy settings of the machine context.

If you have a certificate and want to verify its validity, perform the following command:

```
certutil -f -urlfetch -verify [FilenameOfCertificate]
```

For example, use

```
certutil -f -urlfetch -verify mycertificatefile.cer
```

The command output will tell you if the certificate is verifiable and is valid. Any dwErrorStatus unequal 0 is a real error. For more information on the status see CERT_TRUST_STATUS (<https://msdn2.microsoft.com/en-us/library/aa377590.aspx>) on MSDN.

If you have a HTTP or LDAP URL and want to look at the CRL, use the following command:

```
certutil -URL [URL]
```

For example, use

```
certutil -URL
```

<https://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl> 

The URL can be a HTTP or LDAP URL. The nice thing with the `-URL` verb is that it shows a user interface where also the retrieval timeout can be set. Thus, it might be, that a CRL can be retrieved with an extended retrieval timeout while `certutil -verify` fails because it uses the default timeout. To also extend the retrieval timeout for the `-verify` verb, use the `-t` option like this:

```
certutil -t 30 -f -urlfetch -verify [FilenameOfCertificate]
```

Sometimes, you not only want to look at the CRL but also want to download the CRL as a file. In this case, use the `-split` option like this:

```
certutil -split -URL
```

<https://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl> 

or

```
certutil -split -URL
```

```
ldap://myLDAPserver/CN=MyCA,CN=CRL,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

The `-split` option creates a file named `"BlobX_X_X.*"` in your current working directory. If multiple CRLs are downloaded several `Blob*.*` files are created. As a global option, `-split` can also be used with other `certutil` verbs, for example:

```
certutil -f -split -urlfetch -verify [FilenameOfCertificate]
```

If the certificate is part of a multi-tier CA topology or delta CRLs are used, you will see a `Blob*.*` file for each CRL in the chain.

Once a CRL was downloaded, it is cached locally. To examine the URLs of CRLs that are in the local cache, perform the following command:




```
certutil -urlcache CRL
```

Comments

- **Anonymous**
January 01, 2003
You are enrolled. The device resets and shortly afterward you see the checked "V" icon, indicating you
- **Anonymous**
January 01, 2003
The link to 2nd whitepaper is broken. Correct link is <http://technet.microsoft.com/en-us/library/bb457027.aspx>
- **Anonymous**
November 25, 2013
Nice post.
- **Anonymous**
December 07, 2013
#Certificate MMC Snap-In does not verify the CRL of certificates#
stupid shitcoders...Even after all these years
- **Anonymous**
December 19, 2014
I the command prompt.
"certsrv.msv /e"
Wil show you the CRL list in the MMC Snapin
- **Anonymous**
December 19, 2014
I the command prompt.
"certsrv.msv /e"
Wil show you the CRL list in the MMC Snapin

- **Anonymous**
December 19, 2014
I the command prompt.
"certsrv.msv /e"
Wil show you the CRL list in the MMC Snapin
- **Anonymous**
December 19, 2014
Editet:
"certsrv.msc /e"
- **Anonymous**
June 07, 2016
is there a way for certutil to exclude CRL checking on machines
which do not have access to the internet?

 English (United States)  Your Privacy Choices  Theme 

[Manage cookies](#) [Previous Versions](#) [Blog](#)  [Contribute](#) [Privacy](#)  [Terms of Use](#) [Trademarks](#) 

© Microsoft 2024