Prepare the CAPolicy.inf File | Microsoft Learn

learn.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/prepare-the-capolicy-inf-file

robinharwood

January 11, 2023

CAPolicy.inf Syntax

In this article

The CAPolicy.inf is a configuration file that defines the extensions, constraints, and other configuration settings that are applied to a root CA certificate and all certificates issued by the root CA. The CAPolicy.inf file must be installed on a host server before the setup routine for the root CA begins. When the security restrictions on a root CA are to be modified, the root certificate must be renewed and an updated CAPolicy.inf file must be installed on the server before the renewal process begins.

The CAPolicy.inf is:

- Created and defined manually by an administrator
- Utilized during the creation of root and subordinate CA certificates
- Defined on the signing CA where you sign and issue the certificate (not the CA where the request is granted)

Once you've created your CAPolicy.inf file, you must copy it into the **%systemroot%** folder of your server before you install ADCS or renew the CA certificate.

The CAPolicy.inf makes it possible to specify and configure a wide variety of CA attributes and options. The following section describes all the options for you to create an .inf file tailored to your specific needs.

CAPolicy.inf File Structure

The following terms are used to describe the .inf file structure:

- *Section* – is an area of the file that covers a logical group of keys. Section names in .inf files are identified by appearing in brackets. Many, but not all, sections are used to configure certificate extensions.
- *Key* – is the name of an entry and appears to the left of the equal sign.
- *Value* – is the parameter and appears to the right of the equal sign.

In the following example, **[Version]** is the section, **Signature** is the key, and **"$Windows NT$"** is the value.

Example:

Text

```
[Version]
Signature="$Windows NT$"
```

Version

Identifies the file as an .inf file. Version is the only required section and must be at the beginning of your CAPolicy.inf file.

PolicyStatementExtension

Lists the policies that have been defined by the organization, and whether they're optional or mandatory. Multiple policies are separated by commas. The names have meaning in the context of a specific deployment, or in relation to custom applications that check for the presence of these policies.

For each policy defined, there must be a section that defines the settings for that particular policy. For each policy, you need to provide a user-defined object identifier (OID) and either the text you want displayed as the policy statement or a URL pointer to the policy statement. The URL can be in the form of an HTTP, FTP, or LDAP URL.

If you're going to have descriptive text in the policy statement, then the next three lines of the CAPolicy.inf would look like:

Text

```
[InternalPolicy]
OID=1.1.1.1.1.1.1
Notice="Legal policy statement text"
```

If you're going to use a URL to host the CA policy statement, then next three lines would instead look like:

Text

```
[InternalPolicy]
OID=1.1.1.1.1.1.2
URL=https://pki.wingtiptoys.com/policies/legalpolicy.asp
```

In addition, you should note:

- Multiple URL and Notice keys are supported.
- Notice and URL keys in the same policy section are supported.
- URLs with spaces or text with spaces must be surrounded by quotes. This is true for the **URL** key, regardless of the section in which it appears.

An example of multiple notices and URLs in a policy section would look like:

Text

```
[InternalPolicy]
OID=1.1.1.1.1.1.1
URL=https://pki.wingtiptoys.com/policies/legalpolicy.asp
URL=ftp://ftp.wingtiptoys.com/pki/policies/legalpolicy.asp
Notice="Legal policy statement text"
```

CRLDistributionPoint

You can specify CRL Distribution Points (CDPs) for a root CA certificate in the CAPolicy.inf. After installing the CA, you can configure the CDP URLs that the CA includes in each certificate issued. The root CA certificate shows the URLs specified in this section of the CAPolicy.inf file.

Text

```
[CRLDistributionPoint]
URL=http://pki.wingtiptoys.com/cdp/WingtipToysRootCA.crl
```

CRL Distribution Points (CDPs) support:

- HTTP
- File URLs
- LDAP URLs
- Multiple URLs

Important

CRL Distribution Points (CDPs) doesn't support HTTPS URLs.

- Quotes must surround URLs with spaces.

- If no URLs are specified – that is, if the **[CRLDistributionPoint]** section exists in the file but is empty – the CRL Distribution Point extension is omitted from the root CA certificate. This is preferable when setting up a root CA. Windows doesn't perform revocation checking on a root CA certificate, so the CDP extension is superfluous in a root CA certificate.

- CA can publish to FILE UNC, for example, to a share that represents the folder of a website where a client retrieves via HTTP.

- Only use this section if you're setting up a root CA or renewing the root CA certificate. The CA determines the subordinate CA CDP extensions.

AuthorityInformationAccess

You can specify the authority information access points in the CAPolicy.inf for the root CA certificate.

Text

```
[AuthorityInformationAccess]
URL=http://pki.wingtiptoys.com/Public/myCA.crt
```

Some more notes on the authority information access section:

- Multiple URLs are supported.
- HTTP, FTP, LDAP and FILE URLs are supported. HTTPS URLs aren't supported.
- This section is only used if you're setting up a root CA, or renewing the root CA certificate. Subordinate CA AIA extensions are determined by the CA who issued the subordinate CA's certificate.
- URLs with spaces must be surrounded by quotes.
- If no URLs are specified – that is, if the **[AuthorityInformationAccess]** section exists in the file but is empty – the Authority Information Access extension is omitted from the root CA certificate. Again, this would be the preferred setting when there's no authority higher than a root CA that would need to be referenced by a link to its certificate.

certsrv_Server

The `[certsrv_server]` section of the CAPolicy.inf is optional. The `[certsrv_server]` is used to specify renewal key length, the renewal validity period, and the certificate revocation list (CRL) validity period for a CA that is being renewed or installed. None of the keys in this section are required. Many of these settings have default values that are sufficient for most needs and can be omitted from the CAPolicy.inf file. Alternatively, many of these settings can be changed after the CA has been installed.

An example would look like:

Text

```
[certsrv_server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
CRLPeriod=Days
CRLPeriodUnits=2
CRLDeltaPeriod=Hours
CRLDeltaPeriodUnits=4
ClockSkewMinutes=20
LoadDefaultTemplates=True
AlternateSignatureAlgorithm=0
ForceUTF8=0
EnableKeyCounting=0
```

RenewalKeyLength sets the key size for renewal only. This is only used when a new key pair is generated during CA certificate renewal. The key size for the initial CA certificate is set when the CA is installed.

When renewing a CA certificate with a new key pair, the key length can be either increased or decreased. For example, if you have set a root CA key size of 4096 bytes or higher, and then discover that you have Java apps or network devices that can only support key sizes of 2048 bytes. Whether you increase or decrease the size, you must reissue all the certificates issued by that CA.

RenewalValidityPeriod and **RenewalValidityPeriodUnits** establish the lifetime of the new root CA certificate when renewing the old root CA certificate. It only applies to a root CA. The certificate lifetime of a subordinate CA is determined by its superior. RenewalValidityPeriod can have the following values: Hours, Days, Weeks, Months, and Years.

CRLPeriod and **CRLPeriodUnits** establish the validity period for the base CRL. **CRLPeriod** can have the following values: Hours, Days, Weeks, Months, and Years.

CRLDeltaPeriod and **CRLDeltaPeriodUnits** establish the validity period of the delta CRL. **CRLDeltaPeriod** can have the following values: Hours, Days, Weeks, Months, and Years.

Each of these settings can be configured after the CA has been installed:

CLI

```
Certutil -setreg CACRLPeriod Weeks
Certutil -setreg CACRLPeriodUnits 1
Certutil -setreg CACRLDeltaPeriod Days
Certutil -setreg CACRLDeltaPeriodUnits 1
```

Remember to restart Active Directory Certificate Services for any changes to take effect.

LoadDefaultTemplates only applies during the install of an Enterprise CA. This setting, either True or False (or 1 or 0), dictates if the CA is configured with any of the default templates.

In a default installation of the CA, a subset of the default certificate templates is added to the Certificate Templates folder in the Certification Authority snap-in. This means that as soon as the AD CS service starts after the role has been installed a user or computer with sufficient permissions can immediately enroll for a certificate.

You may not want to issue any certificates immediately after a CA has been installed, so you can use the LoadDefaultTemplates setting to prevent the default templates from being added to the Enterprise CA. If there are no templates configured on the CA, then it can issue no certificates.

AlternateSignatureAlgorithm configures the CA to support the PKCS#1 V2.1 signature format for both the CA certificate and certificate requests. When set to 1 on a root CA the CA certificate will include the PKCS#1 V2.1 signature format. When set on a subordinate CA, the subordinate CA will create a certificate request that includes the PKCS#1 V2.1 signature format.

ForceUTF8 changes the default encoding of relative distinguished names (RDNs) in Subject and Issuer distinguished names to UTF-8. Only those RDNs that support UTF-8, such as those that are defined as Directory String types by an RFC, are affected. For example, the RDN for Domain Component (DC) supports encoding as either IA5 or UTF-8, while the Country RDN (C) only supports encoding as a Printable String. The ForceUTF8 directive will therefore affect a DC RDN but won't affect a C RDN.

EnableKeyCounting configures the CA to increment a counter every time the CA's signing key is used. Don't enable this setting unless you have a Hardware Security Module (HSM) and associated cryptographic service provider (CSP) that supports key counting. Key counting isn't support by either the Microsoft Strong CSP or the Microsoft Software Key Storage Provider (KSP) support.

Create the CAPolicy.inf file

Before you install AD CS, you configure the CAPolicy.inf file with specific settings for your deployment.

Prerequisite: You must be a member of the Administrators group.

1. On the computer where you're planning to install AD CS, open Windows PowerShell, type **notepad.exe** and press ENTER.

2. Enter the following text:

   Text

   ```
   [Version]
   Signature="$Windows NT$"
   [PolicyStatementExtension]
   Policies=InternalPolicy
   [InternalPolicy]
   OID=1.2.3.4.1455.67.89.5
   Notice="Legal Policy Statement"
   URL=https://pki.corp.contoso.com/pki/cps.txt
   [Certsrv_Server]
   RenewalKeyLength=2048
   RenewalValidityPeriod=Years
   RenewalValidityPeriodUnits=5
   CRLPeriod=weeks
   CRLPeriodUnits=1
   LoadDefaultTemplates=0
   AlternateSignatureAlgorithm=1
   [CRLDistributionPoint]
   [AuthorityInformationAccess]
   ```

3. Select **File**, and then select **Save As**.

4. Navigate to the *%systemroot%* folder.

5. Ensure the following options are set:

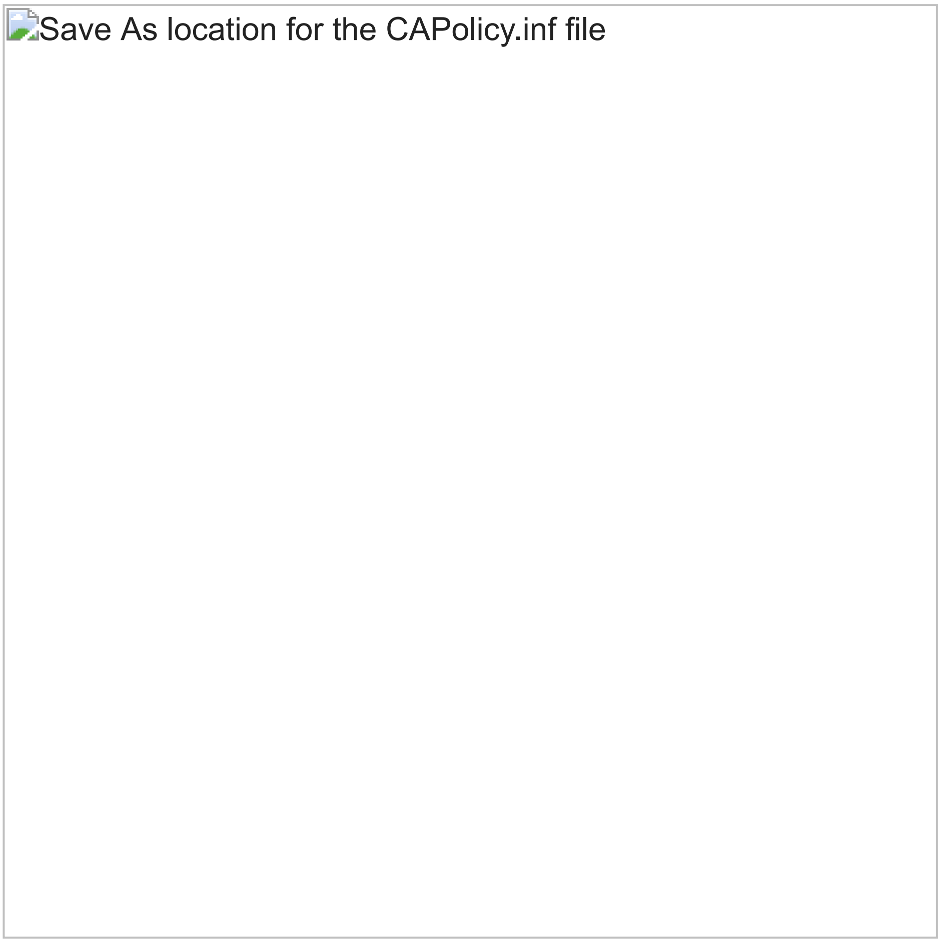
   - **File name** is set to **CAPolicy.inf**

   - **Save as type** is set to **All Files**

   - **Encoding** is **ANSI**

6. Select **Save**.

7. When you're prompted to overwrite the file, select **Yes**.



Save As location for the CAPolicy.inf file

Caution

Be sure to save the CAPolicy.inf with the inf extension. If you do not specifically type **.inf** at the end of the file name and select the options as described, the file will be saved as a text file and will not be used during CA installation.

8. Close Notepad.

Important

In the CAPolicy.inf, you can see there is a line specifying the URL `https://pki.corp.contoso.com/pki/cps.txt`. The Internal Policy section of the CAPolicy.inf is just shown as an example of how you would specify the location of a certificate practice statement (CPS). In this guide, you are not instructed to create the certificate practice statement (CPS).

Additional resources