How to Use the CAPolicy.inf File for Installation

If you want to deploy a root or subordinate CA, and you want to predefine some values for use during installation and define some additional parameters, you can use the CAPolicy.inf file to complete these steps. The CAPolicy.inf file is a plaintext file that contains various settings that are used when installing the AD CS role, or when renewing the CA certificate. The CAPolicy.inf file is not required to install AD CS, but without it, the default settings will be applied, and in many cases, the default settings are insufficient. You can use the CAPolicy.inf file to configure CAs in more complicated deployments.

Each CAPolicy.inf file is divided into sections, and has a simple structure, which can be described as follows:

- A *section* is an area in the .inf file that contains a logical group of keys. A section always appears in brackets in the .inf file.

- A *key* is the parameter that is to the left of the equal (=) sign.

- A *value* is the parameter that is to the right of the equal (=) sign.

For example, if you want to specify an Authority Information Access point in the CAPolicy.inf file, you will use following syntax:

[AuthorityInformationAccess]

URL=http://pki.adatum.com/CertData/adatumCA.crt

In this example, AuthorityInformationAccess is a section, URL is the key, and **http://pki.adatum.com/CertData/adatumCA.crt** is the value.

You can also specify some CA server settings in the CAPolicy.inf file. One example of the section that specifies these settings is:

```
[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
```

Note: All parameters from the previous examples are optional.

You can also use the CAPolicy.inf file when installing AD CS to define the following:

- Certification practice statement: Describes the practices that the CA uses to issue certificates. This includes the types of certificates issued, information for issuing, renewing, and recovering certificates, and

other details about the CA's configuration.

- Object identifier (OID): Identifies a specific object or attribute.

- CRL publication intervals: Defines the interval between publications for the base CRL.

CA renewal settings: Defines renewal settings as follows:

- o Key size: Defines the length of the key pair used during the root CA renewal.

- o Certificate validity period: Defines the validity period for a root CA certificate.

- o CDP and AIA paths: Provides the path used for root CA installations and renewals.

Once you have created your CAPolicy.inf file, you must copy it into the %systemroot% folder of your server (for example, C:\Windows) before you install the AD CS role, or before you renew the CA certificate.

Note: The CAPolicy.inf file is processed for both the root and subordinate CA installations and renewals.