

Three-tier CA Install – Windows 2008

Note: The examples given here use Contoso as the company and eng01-xxx as naming conventions, they of course will need to be changed to suit your environment.

Root CA

1. Created the **CAPolicy.inf** and placed in **C:\windows**

```
[Version]
```

```
Signature=$Windows NT$"
```

```
[certsrv_server]
```

```
Renewalkeylength=4096
```

```
RenewalvalidityPeriodUnits=20
```

```
RenewalvalidityPeriod=years
```

```
CRLPeriod=Years
```

```
CRLPeriodUnits=2
```

```
CRLOverlapPeriod=Years
```

```
CRLOverlapUnits=1
```

```
CRLDeltaPeriodUnits=0
```

```
CRLDeltaPeriod=days
```

```
DiscreteSignatureAlgorithm=1
```

2. Run the **Select Server Roles** wizard...choose **Active Directory Certificate Services**

- a. **Setup Type:** Standalone
- b. **CA Type:** Root CA
- c. **Create a new private key**
- d. RSA#Microsoft Software Key Storage Provider
- e. **Key :** 2048
- f. **Hash:** sha256
- g. **CA Name:**
 - i. Contoso Root CA
 - ii. O=Contoso Inc., C=US
- h. **Validity Period:** 20 years
- i. Changed **CertDB** and **CertLog** to **D:**
- j. **Install**

3. Create and run the post-install script (from cmd window so errors will be displayed and viewable)

```
::Declare Configuration NC
```

```
certutil -setreg CA\DSConfigDN CN=Configuration,DC=contoso,DC=com
```

```
::Define CRL Publication Intervals
```

```
certutil -setreg CA\CRLPeriodUnits 5
```

```
certutil -setreg CA\CRLPeriod "Years"  
certutil -setreg CA\CRLDeltaPeriodUnits 0  
certutil -setreg CA\CRLDeltaPeriod "Days"  
certutil -setreg CA\CRLOverlapPeriod "Years"  
certutil -setreg CA\CRLOverlapUnits 1
```

::Apply the required CDP Extension URLs

```
certutil -setreg CA\CRLPublicationURLs  
"1:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.cr\n2:http://eng01-  
issca1.contoso.com/Certdata/%%3%%8%%9.cr"
```

::Apply the required AIA Extension URLs

```
certutil -setreg CA\CACertPublicationURLs  
"1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n2:http://eng01-issca1.  
contoso.com/CertData/%%1_%%3%%4.crt"
```

::Enable all auditing events for the Contoso Corporate Root CA

```
certutil -setreg CA\AuditFilter 127
```

::Set Validity Period for Issued Certificates

```
certutil -setreg CA\ValidityPeriodUnits 10  
certutil -setreg CA\ValidityPeriod "Years"
```

:: Enable discrete signatures in subordinate CA certificates

```
Certutil -setreg CA\csp\DiscreteSignatureAlgorithm 1
```

::Restart Certificate Services

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

```
certutil -crl
```

::Copy the Root CA certificates and CRLs to the current folder

```
copy /y %windir%\system32\certsrv\certenroll\*.cr? .\
```

4. Open the **Certificate Authority** MMC, right-click **Contoso Corp Root CA** and choose **Properties**
 - a. Go to **Extensions** tab, for both **CRL** and **AIA** remove file and ldap entries
 - b. Click Include **IDP extension under CRL**, http
 - c. **Auditing** tab, check all boxes
 - d. Click **OK**
5. Copy cert and CRLs from the Root CA (from very end of step 3) to the Policy CA

Policy CA

6. Create and run script to install cert and CRLs

```
for %%c in (*.crt) do certutil -addstore -f Root "%%c"
for %%c in (*.crl) do certutil -addstore -f Root "%%c"
```
7. Created the **CAPolicy.inf** and placed in **C:\windows**

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

[certsrv_server]
renewalkeylength=2048
RenewalValidityPeriod=years
RenewalValidityPeriodUnits=10

CRLPeriod = years
CRLPeriodUnits = 26
CRLOverlapPeriod=weeks
CRLOverlapUnits=2
CRLDeltaPeriod = days
CRLDeltaPeriodUnits = 0

DiscreteSignatureAlgorithm=1
```
8. Run the **Select Server Roles** wizard...choose **Active Directory Certificate Services**
 - a. **Setup Type:** Standalone
 - b. **CA Type:** Subordinate CA
 - c. **Create a new private key**
 - d. RSA#Microsoft Software Key Storage Provider
 - e. **Key :** 2048
 - f. **Hash:** sha256
 - g. **CA Name**
 - i. Contoso Corp Policy CA
 - ii. O=Contoso Inc., C=US
 - h. Save a certificate request to file and manually send it later (saved on C:\)
 - i. Changed **CertDB** and **CertLog** to **D:**
 - j. **Install**
9. Copy the cert request from **C:** to the **root CA**
 - a. Open the **Certificate Authority** MMC
 - b. Right-click the **Contoso Corp Root CA**, choose **All Tasks>Submit a new request...**
 - c. **Import** the Policy CA cert request and go to **Pending Requests**
 - d. Right-click the request in the right pane and choose **All Tasks > Issue**
 - e. Go to **Issued Certificates**, double-click the newly issued cert and go to the **Details** tab, select **Copy to File...**
 - f. Choose **Cryptographic Message (.P7B)**, check the box (**Include all certs...**)
 - g. Choose a location, export and copy it to the Policy CA
10. On the Policy CA, open the **Certificate Authority** MMC, right-click **Contoso Policy CA**, choose **All Tasks>Start Service**
11. When prompted to install cert, select **Yes**, and browse to the cert copied in step 9g, and the service will start

12. Create and run post-install script

```
::Declare Configuration NC
certutil -setreg CA\DSConfigDN CN=Configuration,DC=contoso,DC=com

::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 26
certutil -setreg CA\CRLPeriod "Weeks"
certutil -setreg CA\CRLOverlapUnits 2
certutil -setreg CA\CRLOverlapPeriod "Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\CRLDeltaPeriod "Days"

::Apply the required CDP Extension URLs
certutil -setreg CA\CRLPublicationURLs
"1:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.cr\n2:http://eng01-issca1.
contoso.com/Certdata/%%3%%8%%9.cr"

::Apply the required AIA Extension URLs
certutil -setreg CA\CACertPublicationURLs
"1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n2:http://eng01-issca1.
contoso.com/CertData/%%1_%%3%%4.crt"

::Enable all auditing events for the Contoso Corporate Policy CA
certutil -setreg CA\AuditFilter 127

::Set Validity Period for Issued Certificates
certutil -setreg CA\ValidityPeriodUnits 5
certutil -setreg CA\ValidityPeriod "Years"

::Enable discrete signatures in subordinate CA certificates
Certutil -setreg CA\csp\DiscreteSignatureAlgorithm 1

::Restart Certificate Services
net stop certsvc & net start certsvc

certutil -crl

copy /y %windir%\system32\certsrv\certenroll\*.cr? . \
```

13. Open the **Certificate Authority** mmc, right-click **Contoso Corp Policy CA** and choose **Properties**

- a. Go to **Extensions** tab, for both **CRL** and **AIA** remove file and ldap entries
- b. Click Include **IDP extension under CRL**, http
- c. **Auditing** tab, check all boxes
- d. Click **OK**

14. Copy Root and Policy certs and CRLs (from the steps 3 and 12) to the Issuing CA

Issuing CA

15. Install the **Internet Information Services** role
 - a. In **Server Manager**, choose **Add Roles, Web Server (IIS), Add Required Features**
 - b. Under **Role Services, Web Services > Security >** choose **Digest Authentication, Install**
16. Create and run script to install cert and CRLs (open CMD window as administrator)

```
for %%c in ("rootca_Contoso Corp Root CA*.crt") do certutil -addstore -f Root "%%c"
for %%c in ("Contoso Corp Root CA*.crl") do certutil -addstore -f Root "%%c"
for %%c in ("intca1_Contoso Corp Policy CA*.crt") do certutil -addstore -f CA "%%c"
for %%c in ("Contoso Corp Policy CA*.crl") do certutil -addstore -f CA "%%c"
```
17. Create and run script to add Root and Policy CA certs to AD (open CMD window as administrator)

```
for %%c in ("rootca_Contoso Corp Root CA*.crt") do certutil -dspublish -f "%%c" RootCA
for %%c in ("intca1_Contoso Corp Policy CA*.crt") do certutil -dspublish -f "%%c" SubCA
for %%c in ("Contoso Corp Root CA*.crl") do certutil -dspublish -f "%%c"
for %%c in ("Contoso Corp Policy CA*.crl") do certutil -dspublish -f "%%c"
gpupdate /force
```
18. Run the **Select Server Roles** wizard...choose **Active Directory Certificate Services**
 - a. Choose **Certificate Authority** and **CA Web Enrollment**
 - b. **Setup Type:** Enterprise
 - c. **CA Type:** Subordinate CA
 - d. **Setup Private Key:** Create a new private key
 - e. **Crypto:** RSA#Microsoft SW Key Storage Provider, 2048 Length, hash: sha1
 - f. **Common name:** Contoso Corp Issuing CA
 - g. **DN:** O=Contoso Inc.,C=US
 - h. **Save a certificate request to file** and manually send it later (saved on C:\)
 - i. Changed **CertDB** and **CertLog** to **D:\CertLog** and **E:\CertDB**
 - j. **Install**
19. Copy the cert request from **C:** to the Policy CA
 - a. Open the **Certificate Authority** MMC
 - b. Right-click the **Contoso Policy CA**, choose **All Tasks>Submit a new request...**
 - c. **Import** the Policy CA cert request and go to **Pending Requests**
 - d. Right-click the request in the right pane and choose **All Tasks > Issue**
 - e. Go to **Issued Certificates**, double-click the newly issued cert and go to the **Details** tab, select **Copy to File...**
 - f. Choose **Cryptographic Message (.P7B)**, check the box (**Include all certs...**)
 - g. Choose a location, export and copy it to the Policy CA
20. On the Issuing CA, open the **Certificate Authority** MMC, right-click **Contoso Issuing CA**, choose **All Tasks>Start Service**
21. When prompted to install cert, select **Yes**, and browse to the cert copied in step 9.g, and the service will start
22. Copy root and policy certs and CRLs to **D:\Certs**
23. In **IIS**, under **Sites**, right-click **Default Web Site**, choose **Add Virtual Directory**
 - a. **Alias:** CertData
 - b. **Path:** D:\Certs
24. *Create and run post-install script*

```
::Declare Configuration NC
certutil -setreg CA\DSConfigDN CN=Configuration,DC=contoso,DC=com
```

```
::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 3
certutil -setreg CA\CRLPeriod "Days"
certutil -setreg CA\CRLOverlapUnits 4
certutil -setreg CA\CRLOverlapPeriod "Hours"
certutil -setreg CA\CRLDeltaPeriodUnits 12
certutil -setreg CA\CRLDeltaPeriod "Hours"
```

```
::Enable all auditing events for the Contoso Corporate Issuing CA
certutil -setreg CA\AuditFilter 127
```

```
:: Enable discrete signatures in issued certificates
Certutil -setreg CA\csp\DiscreteSignatureAlgorithm 1
```

```
::Set Maximum Validity Period for Issued Certificates
certutil -setreg CA\ValidityPeriodUnits 2
certutil -setreg CA\ValidityPeriod "Years"
```

```
::Restart Certificate Services
net stop certsvc & net start certsvc
```

```
certutil -crl
```

25. Open the **Certificate Authority** MMC, right-click **Contoso Corp Issuing CA** and choose **Properties**
 - a. Go to **Extensions** tab, for both **CRL** and **AIA** remove file entries
 - b. Click **Include IDP extension under CRL**, http
 - c. **Auditing** tab, ensure all boxes are
 - d. Click **OK**
26. Login to Root, Policy and Issuing CAs and up auditing in **gpedit.msc**, **Computer Settings**, **Windows Settings**, **Security Settings**, **Local Policies**, **Audit Policy**, enable **Success & Failure** for all
27. Run command to have auditing events show up in event viewer

```
auditpol /set /subcategory:"other system events" /success:enable /failure:enable
```
28. Add Templates for use by opening the **Certificate Authority** MMC, under **Contoso Corp Issuing CA**, right-click **Certificate Templates>New>Certificate Template to Issue**
 - a. Add **Computer**, **Domain Controller**, **User**, **Web Server**, etc.
29. Create a Self-Signed cert to enable SSL on the Certificate Server website, thus allowing other Templates to be available
 - a. Open the **IIS Manager** MMC, highlight **ENG01-ISSCA1**, double-click **Server Certificates** in the **Features** pane, from **Actions**, choose **Create Self-Signed Certificate**
 - b. Go to **Default Web Site**, choose **Bindings**, highlight **https**, **Edit... SSL Cert:** newly created self-signed
30. Create a cert request to for a valid CA SSL on the Certificate Server website
 - a. Go to **IIS Manager > ENG01-ISSCA1 > Server Certificates > Create Certificate Request...**
 - i. Fill-in the fields:
 1. **CN**=eng01-issca1. contoso.com
 2. **O**=Contoso Inc
 3. **OU**=IT Operations
 4. Etc.

- ii. MS RSA SChannel... 1024 **Bit length**
 - iii. Choose location and name the request
 - iv. **Finish**
31. Login into <https://eng01-issca1.contoso.com/CertSrv>, choose **Request a Cert > Or, submit an advanced certificate request > Create and submit to this CA > Submit a certificate request by using a base-64...**
 32. Paste the contents of 30c, choose **Web Server** from **Certificate Template** and **Submit**.
 33. Login into <https://eng01-issca1.contoso.com/CertSrv>, choose **Download a CA Cert > Download CA certificate** and choose a location.
 34. Go to **IIS Manager > ENG01-ISSCA1 > Server Certificates > Complete Certificate Request...**, choose the cert from above, add a **Friendly name** for use
 35. Go to **Default Web Site**, choose **Bindings**, highlight **https**, **Edit... SSL Cert:** newly create CA generated cert
 36. Highlight **CertSrv, SSL Settings**, double-click and choose **Require SSL** and **Require 128-bit SSL**

Summary

At this point, both the root and policy CAs should be offline until needed in the future. Using virtual machines for these roles are a perfect way to mothball these systems, as they don't use physical resources and almost no disk space.

Below is a list of tasks and maintenance items once the issuing CA is online.

Tasks and Maintenance

Renewing the Issuing CA Certificate

1. Open **Certificate Authority MMC**
2. Select the **Contoso Issuing CA** in the right hand pane, right-click and choose **All Tasks > Renew CA certificate**
3. Save the request to a file
4. Boot and copy the request Policy CA
5. Open **Certificate Authority MMC**
6. Select the **Contoso Policy CA** in the right hand pane, right-click and choose **All Tasks > Submit new request...**
 - a. **Import** the Policy CA cert request and go to **Pending Requests**
 - b. Right-click the request in the right pane and choose **All Tasks > Issue**
 - c. Go to **Issued Certificates**, double-click the newly issued cert and go to the **Details** tab, select **Copy to File...**
 - d. Choose **Cryptographic Message (.P7B)**, check the box **(Include all certs...)**
 - e. Choose a location, export and copy it to the Issuing CA
7. On the Issuing CA, open the **Certificate Authority MMC**, right-click **Contosa Issuing CA**, choose **All Tasks>Start Service**
8. When prompted to install cert, select **Yes**, and browse to the cert copied in step e, and the service will start

Changing the CRL Publication Interval

1. Open **Certificate Authority MMC**
2. Drill down to **Revoked Certificates**, right-click and choose **Properties**

Manually Publishing a New CRL

1. Open **Certificate Authority MMC**
2. Drill down to **Revoked Certificates**, right-click and choose **All Tasks > Publish**

Creating a New Template

1. Open **Certificate Authority MMC**
2. Drill down to **Certificate Templates**, right-click and choose **Manage**
3. In the **Certificates Templates Console**, right-click a template similar to the one to be created and choose **Duplicate Template**
4. Make changes as required, it is ready of use. To add, see Adding a Template for Issuing below.

Adding a Template for Issuing

1. Open **Certificate Authority MMC**
2. Drill down to **Certificate Templates**, right-click and choose **New > Certificate Template to Issue**, choose **Template(s)** and click **OK** (types are here: [http://technet.microsoft.com/en-us/library/cc730826\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc730826(WS.10).aspx))

Obtaining a User Certificate

1. Browse to: <https://eng01-issca1.contoso.com/certsrv> and choose **Request a certificate**
2. Click **User Certificate** and **Submit**, answer **Yes**, to allow the website to submit a request for you
3. Click **Install the certificate** to complete the request
4. Open an **MMC**, press **Ctrl + M** and add **Certificates, My User Account** to see if the certificate has been installed successfully (under **Certificates, Personal, Certificates**) and to examine the properties (double-click the certificate)

Obtaining a Web Server Certificates

1. Create a web certificate request from the destination server
2. Login into <https://eng01-issca1.contoso.com/CertSrv>, choose **Request a Cert > Or, submit an advanced certificate request > Create and submit to this CA > Submit a certificate request by using a base-64...**
3. Paste the contents of step 1 above, choose **Web Server** from **Certificate Template** and **Submit**.
4. Login into <https://eng01-issca1.contoso.com/CertSrv>, choose **Download a CA Cert > Download CA certificate**, choose a download location and import/install as per the web server documentation

Certificate Authority Backup

1. Open **Certificate Authority MMC**
2. Right-click the **Contoso Corp Issuing CA** and choose **All Tasks > Back up CA...**
3. Check the first two boxes and choose a location (*must be an empty folder*), enter a **Password** and **Finish**

Enable GPO Auto-enrollment for Computers

1. Open the **GPMC**, right-click the OU to enable, choose **Edit...**
2. Go to **Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Automatic Certificate Request Settings**, right-click choose **New > Automatic Certificate Request...**
3. Choose **Computer > Finish**
4. Double-click **Autoenrollment Settings** under **Public Key Policies** and select **Enable** and both check boxes.
5. Computers in the OU will start getting certificates after a reboot or two

Monitoring Health and Install

1. Run the **Enterprise PKI** tool to see if any certificate paths are broken or if certificates will be expiring soon
2. Open a CMD window to run certutil commands
 - a. `certutil -dcinfo` retrieves certificates from Domain Controllers with information on the Issuer, Dates, Template, etc.
 - b. `certutil -getreg CA` retrieves information on the Enterprise CA, CRLPeriods, URLs, settings, etc.