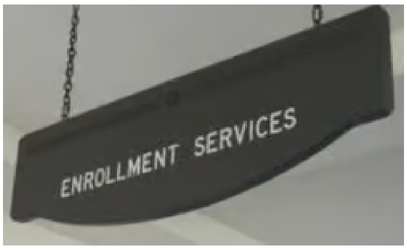
Windows Server 2012 R2 Two-Tier PKI CA Pt. 3

derekseaman.com/2014/01/windows-server-2012-r2-two-tier-pki-ca-pt-3.html

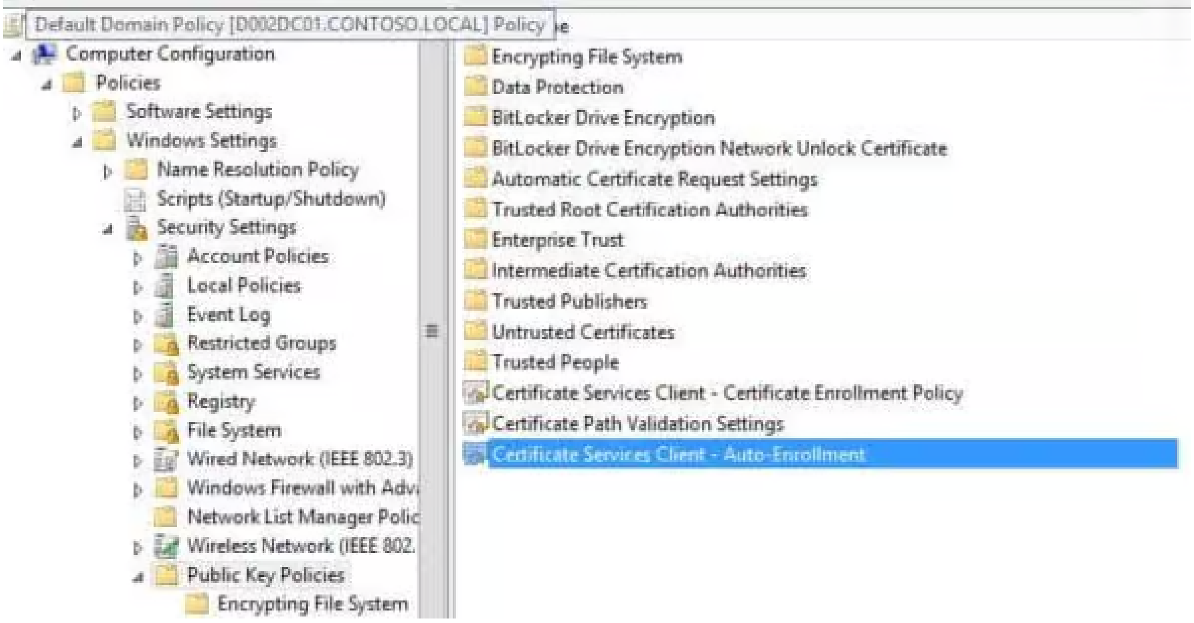
Derek Seaman January 10, 2014



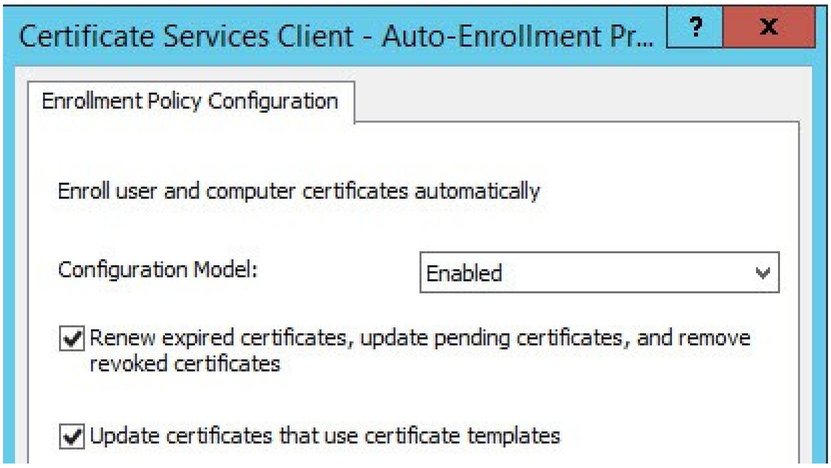
Now that we have our Windows Server 2012 R2 certificate authority configured in Part 1, and our subordinate setup in Part 2, now we should setup autoenrollment and secure the subordinate's web certificate services with SSL. Autoenrollment is where domain joined Windows computers are automatically issued a computer certificate. Services such as IIS and Microsoft SCCM can take advantage of these certificates. Finally, I'll show you how to configure certificate delegation so authorized administrators in your organization can submit certificate requests for certain templates. This is a short series, at just three installments. But this should point you in the right direction for thinking about how to deploy your two-tier Certificate Authority on Windows Server 2012 r2.

Autoenrollment Configuration

1. Open your domain level GPO (Default Domain Policy in my case) and navigate to **Public Key Policies** as shown in the figure below. Double click on the highlighted policy.


Default Domain Policy [D002DC01.CONTOSO.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3)
Windows Firewall with Adv
Network List Manager Polic
Wireless Network (IEEE 802.
Public Key Policies
Encrypting File System
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certificate
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment

2. Enable the policy and check the two options below.



Certificate Services Client - Auto-Enrollment Pr...

Enrollment Policy Configuration

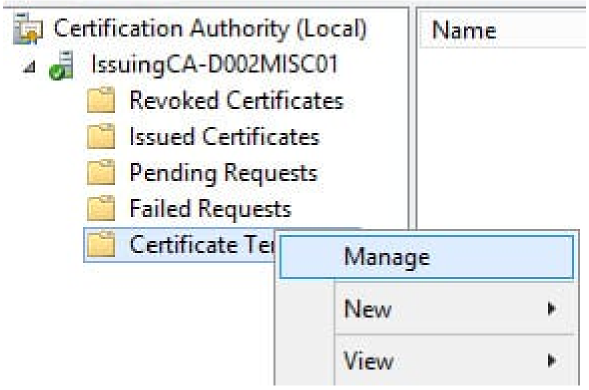
Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

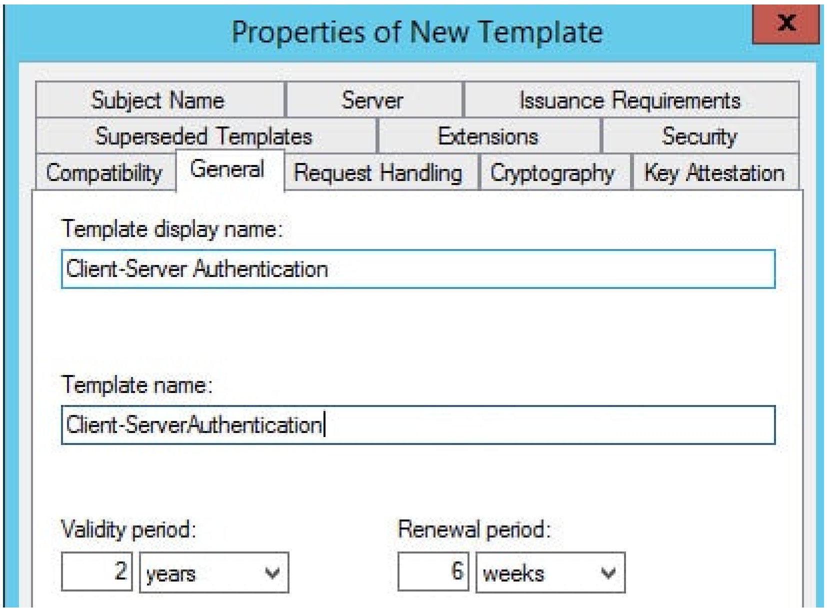
☑ Update certificates that use certificate templates

3. On your subordinate CA, open the CA snap-in and manage the Certificate Templates as shown below.



4. Scroll down and locate **Workstation Authentication.** Right click and **Duplicate** the template.

5. Click on the **General** tab and enter a template name (any name). I'll use **Client-Server Authentication**. I also changed the validity period to 2 years.



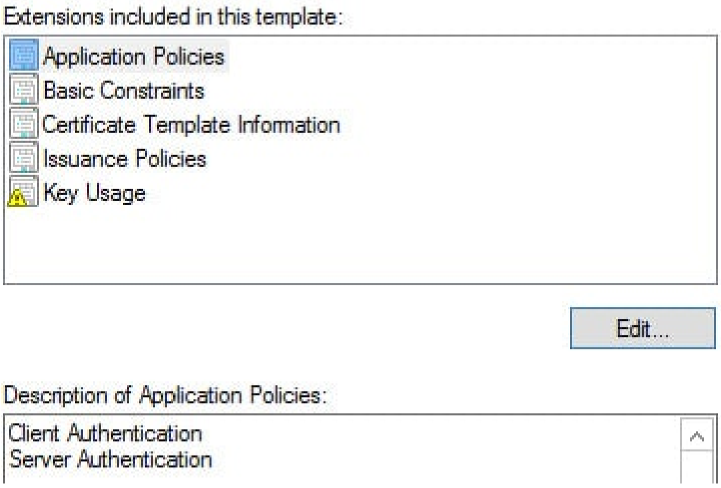
Template display name: Client-Server Authentication

Template name: Client-ServerAuthentication

Validity period: 2 years

Renewal period: 6 weeks

6. Click on the **Extensions** tab. Highlight **Application Policies** and click **Edit**. Add **Server Authentication**.



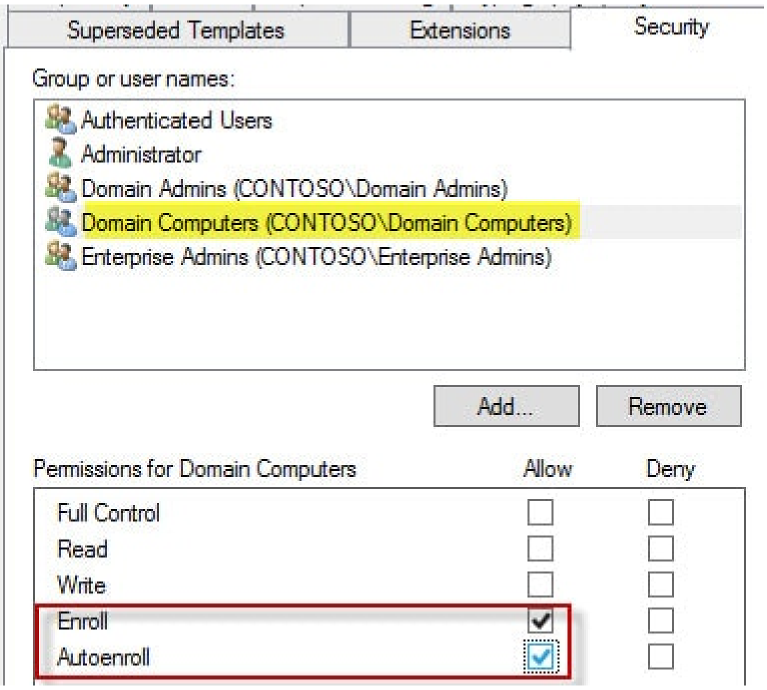
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Client Authentication
Server Authentication

7. Click on the **Security** tab and modify the **Domain Computers** group to enable Autoenroll. Close out the template and template window.

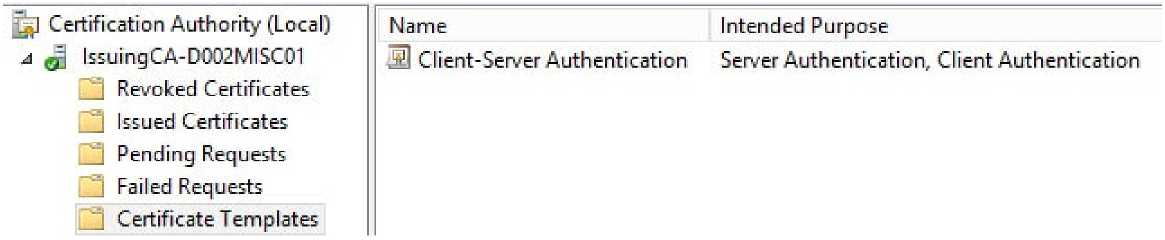


Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (CONTOSO\Domain Admins)
- Domain Computers (CONTOSO\Domain Computers)
- Enterprise Admins (CONTOSO\Enterprise Admins)

Permissions for Domain Computers	Allow	Deny
Full Control	□	□
Read	□	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

8. Back in the issuing CA console right click on **Certificate Templates**, select **New**, then **Certificate Template to Issue**. Select the template name you just created. Wait a few minutes for the settings to simmer a bit. If you want you could also publish the **Domain Controller** template. This will enable the DCs to offer LDAPS services. If the template you just created is not listed, you can simply wait a bit or restart the CA services and that should kick it in the pants.

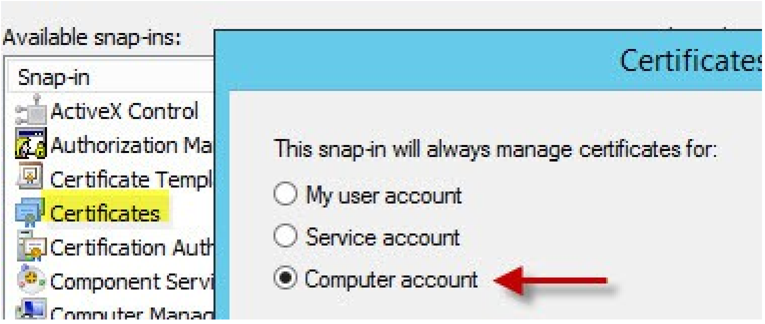


Name	Intended Purpose
Client-Server Authentication	Server Authentication, Client Authentication

Autoenrollment Validation

1. Open an elevated command prompt or Powershell and type **gpupdate /force**. Wait a couple of minutes, as certificate enrollment is not always instant.

2. Open a blank MMC console and add the **Certificates** snap-in. Manage the **Computer account**.



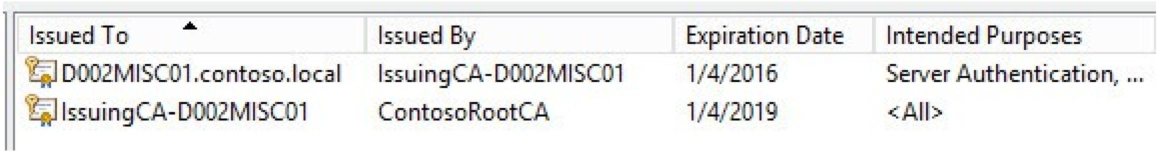
This snap-in will always manage certificates for:

○ My user account

○ Service account

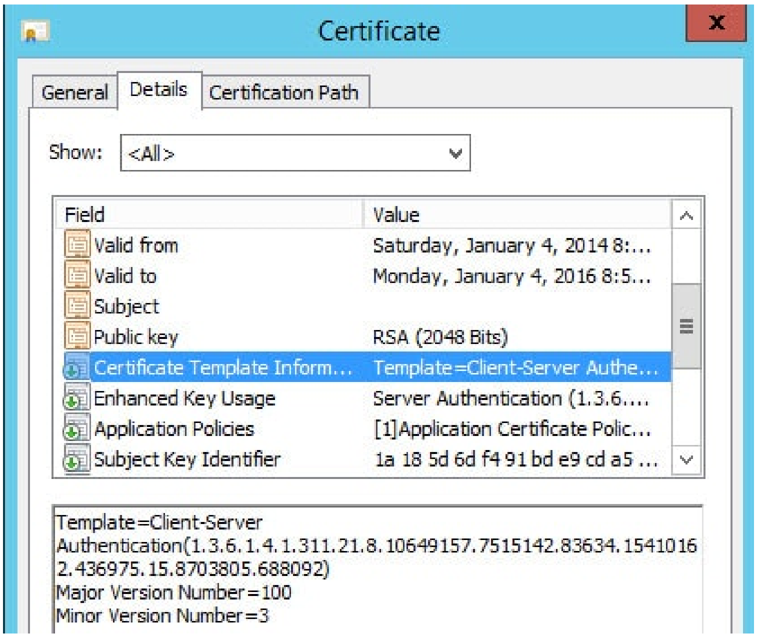
● Computer account

3. On your subordinate CA you should now see two certificates. In my case the top certificate was the one issued by the autoenrollment policy.



Issued To	Issued By	Expiration Date	Intended Purposes
D002MISC01.contoso.local	IssuingCA-D002MISC01	1/4/2016	Server Authentication, ...
IssuingCA-D002MISC01	ContosoRootCA	1/4/2019	<All>

4. You can verify the certificate was issued from the proper template by opening the properties then on the **Details** tab look for the **Certificate Template Information** property. It will clearly state the template name used to create the certificate.



Show: <All>

Field	Value
Valid from	Saturday, January 4, 2014 8:...
Valid to	Monday, January 4, 2016 8:5...
Subject	
Public key	RSA (2048 Bits)
Certificate Template Inform...	Template=Client-Server Authe...
Enhanced Key Usage	Server Authentication (1.3.6....
Application Policies	[1]Application Certificate Polic...
Subject Key Identifier	1a 18 5d 6d f4 91 bd e9 cd a5 ...

```
Template=Client-Server
Authentication(1.3.6.1.4.1.311.21.8.10649157.7515142.83634.1541016
2.436975.15.8703805.688092)
Major Version Number=100
Minor Version Number=3
```

5. As the GPO refreshes on other computers in the domain, they should also be issued a certificate as well. Autoenrollment can run into snags, so I have seen cases where everything has been configured properly but for some reason a certificate is not issued.

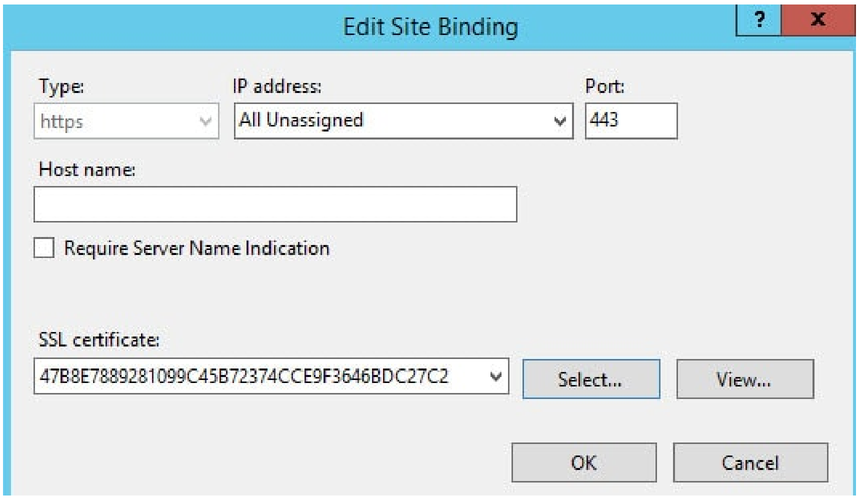
Configure CA Web Services for SSL

1. After the autoenrollment certificate has been validated on the subordinate CA, open the IIS Manager on your subordinate CA.

2. In the left pane select **Default Web Site**. In the right pane select **Bindings**.

3. Click on **https** then click **Edit**.

4. Select the SSL certificate that was created from the client-server template. You can view the certificate in the GUI if you aren't sure which one to pick.



Edit Site Binding

Type: https

IP address: All Unassigned

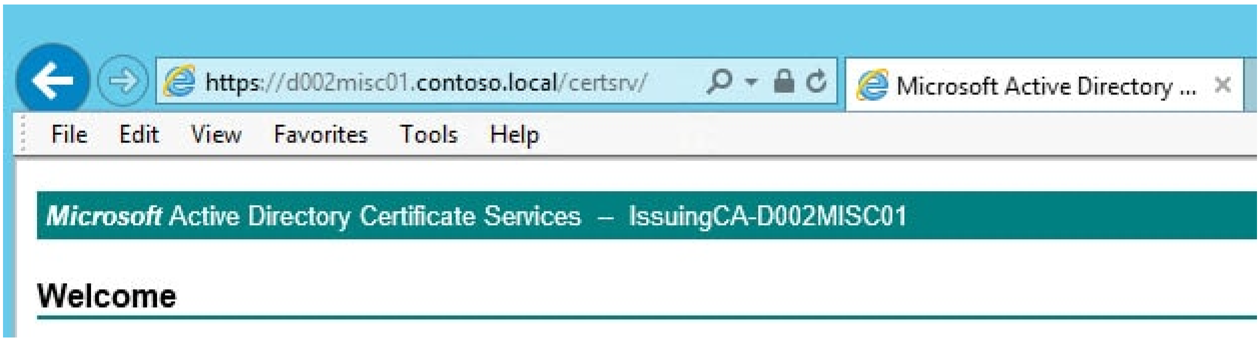
Port: 443

Host name:

□ Require Server Name Indication

SSL certificate: 47B8E7889281099C45B72374CCE9F3646BDC27C2

5. Open IE and navigate to the FQDN of your subordinate CA and to the certsrv site (e.g. https://D002Misc01.contoso.local/certsrv). You will likely be prompted for credentials, then presented with the standard ADCS home page. You should not have any SSL errors or warnings.



https://d002misc01.contoso.local/certsrv/

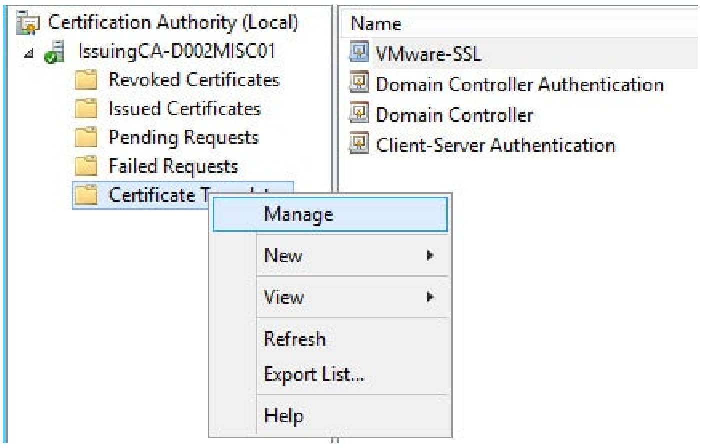
Microsoft Active Directory ...

Microsoft Active Directory Certificate Services – IssuingCA-D002MISC01

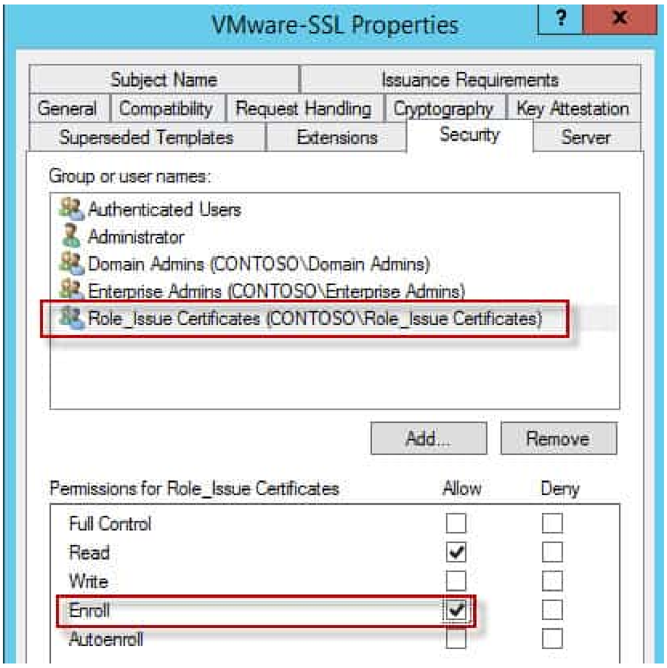
Welcome

Template Delegation

1. On your subordinate CA and open the Certificate Template manager as shown below.



2. Locate the certificate template which you want to delegate. In my case I have a VMware-SSL template that I want to delegate to the group we created earlier in this series. Open the properties for the certificate template and select the **Security** tab. Add the **Role_Issue Certificates** group (or whatever your group is called) and give it the **Enroll** permission.



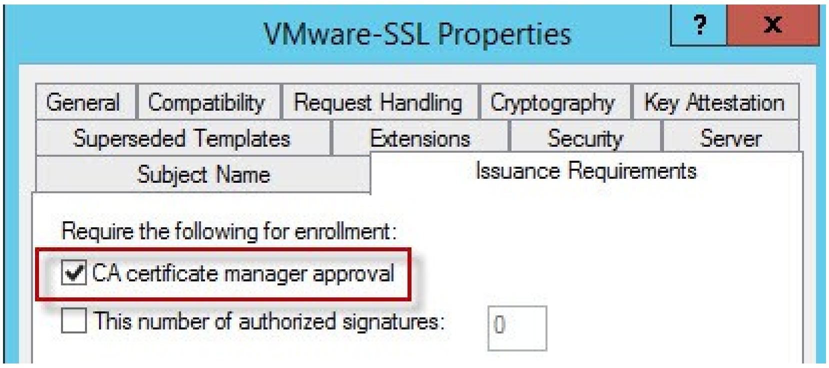
Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (CONTOSO\Domain Admins)
- Enterprise Admins (CONTOSO\Enterprise Admins)
- Role_Issue Certificates (CONTOSO\Role_Issue Certificates)

Permissions for Role_Issue Certificates

	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

3. Optionally you configure the CA to allow requests to be submitted, but require a CA administrator to approve the certificates before they can be issued. If you want to do this, open the **Issuance Requirements** tab and check to the **CA certificate manager approval** box. This would defeat the purpose of autoenrollment certificates, such as those for computers, so generally this would be for certificates that users are requesting.



VMware-SSL Properties

Require the following for enrollment:

☑ CA certificate manager approval

□ This number of authorized signatures: 0

What’s Next?

If you want to issue SSL certificates for your VMware infrastructure, then you can check out my post here for the template requirements. Although that article is for vSphere 5.5, the template will also work for vSphere 4.x and 5.x. Now you have a fully functional, for lab/home usage, offline root and online subordinate CA. As I stated in Part 1, this guide just shows you the general technical steps for a two-tier Certificate Authority. There’s a lot of processes and procedures that an organization needs to flesh out and document before deploying PKI in the environment. There could be legal or other consequences if you just throw this on a production network and then down the road experience security issues which can be traced back to a poorly implemented CA.