How to use Data Recovery Agent (DRA) to decrypt encrypted files

Server 2012

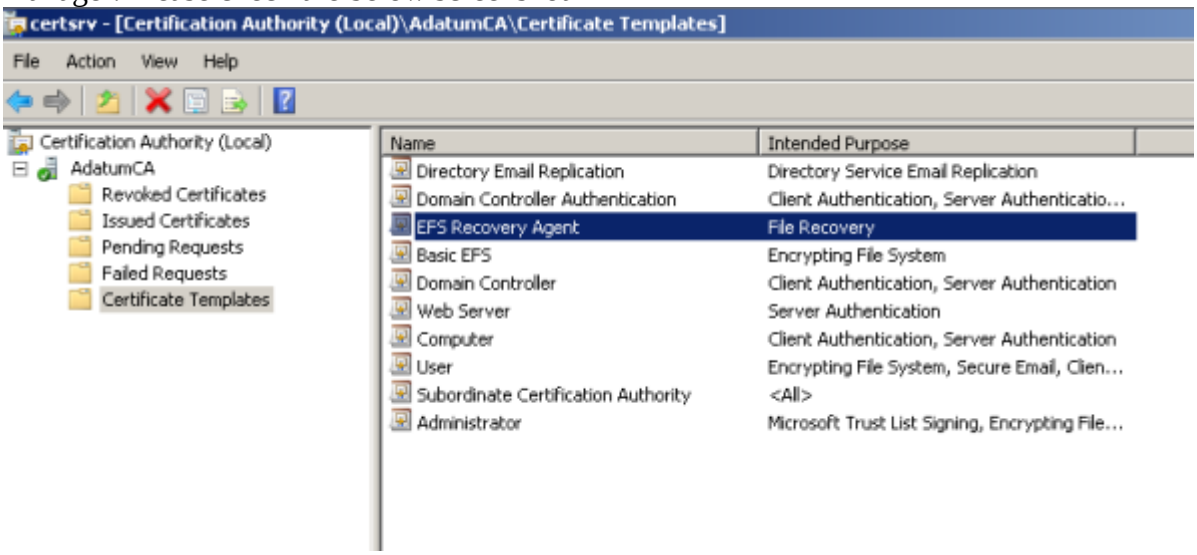
What is Data Recovery Agent (DRA) and why we need it?

Lets assume you have some confidential information stored in a file, which is encrypted by a user. As user encrypted the file using his certificate thus only he can have access to this file. Accidently user lost his certificate thus lost his private key. Now who can decrypt that file?? No one…..Yeah unless and until you have a DRA.

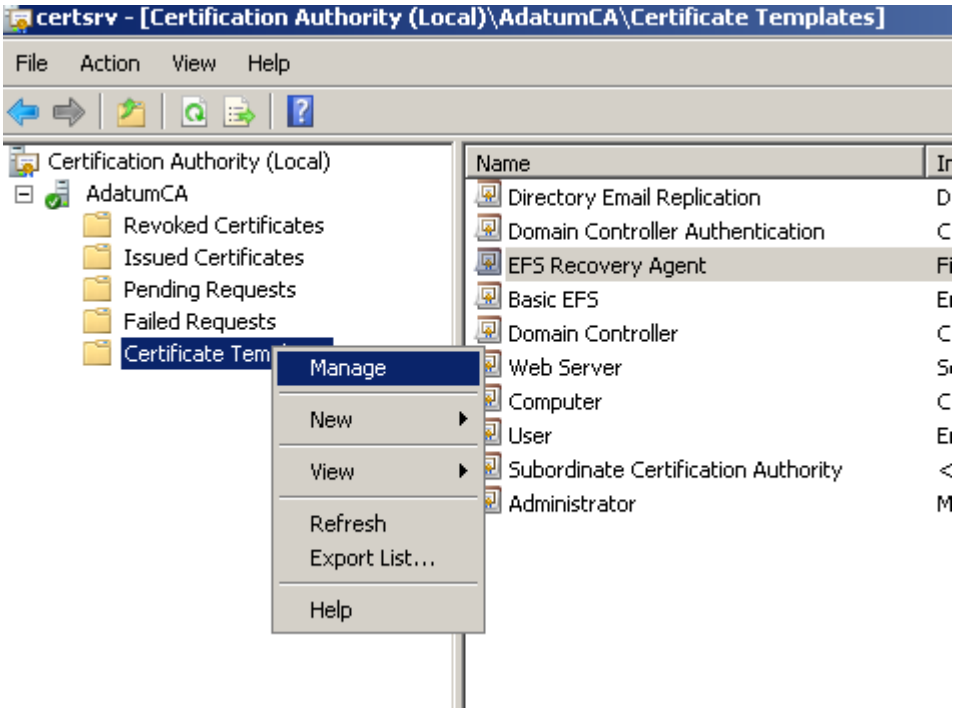
By default, the data recovery agent is defined to be the administrator account. On stand-alone workstations and workgroup machines, the administrator account is the local administrator; on domain-joined machines, the administrator account is the first domain controller's administrator account. Before using encryption for first time you must made a user DRA.

Lets follow the steps..

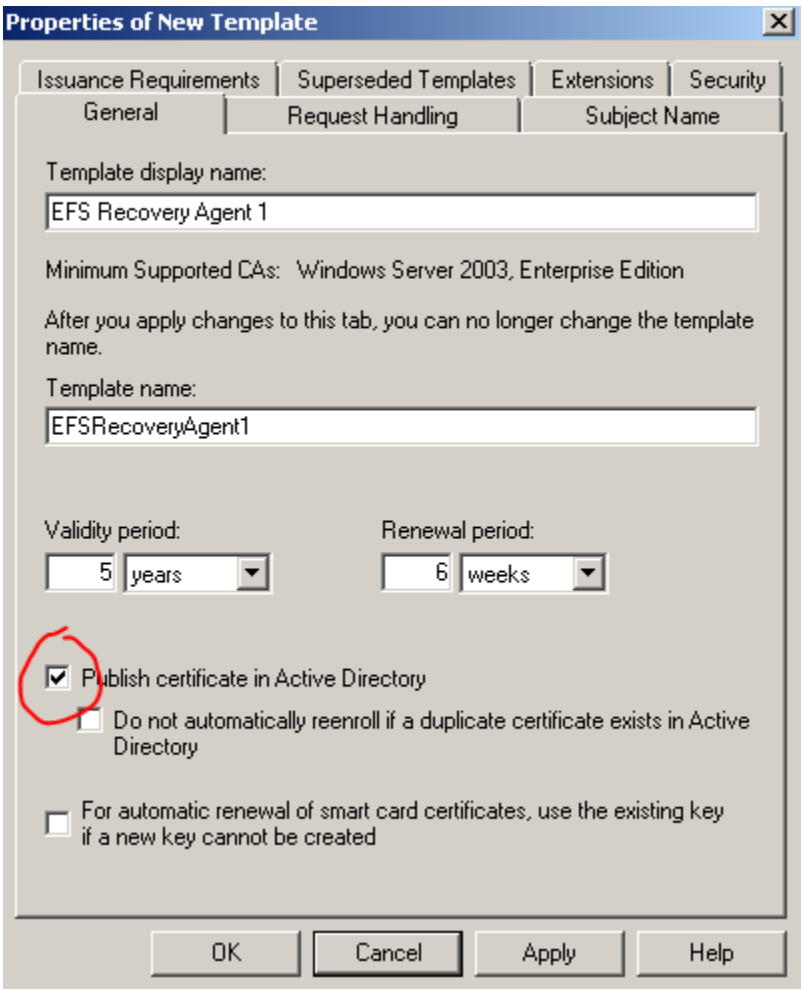
1. By default administrator is defined to be DRA, thus administrator needs to enroll for an EFS recovery Agent certificate. you can find the EFS recovery Agent certificate into certificate manager. Please check the below screenshot-

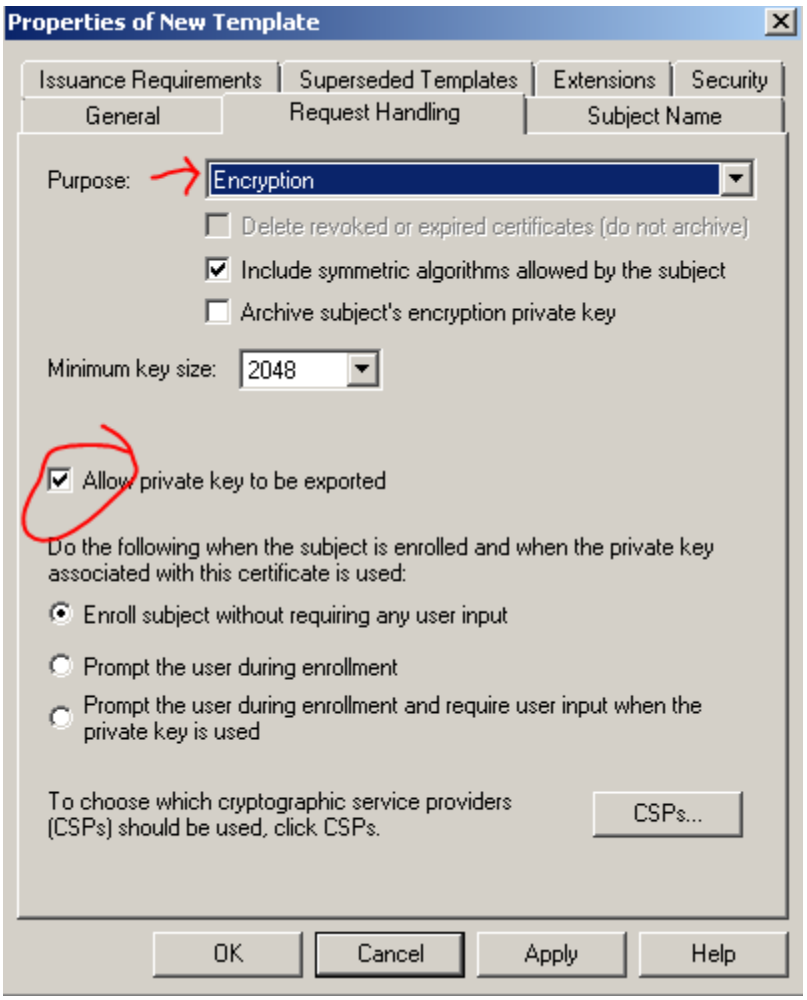


this certificate is default certificate and known as Type 1 certificate. You can't customize its properties. Although for our purpose we can use this but lets create a Type 2 certificate which we can customize. Check screenshot-

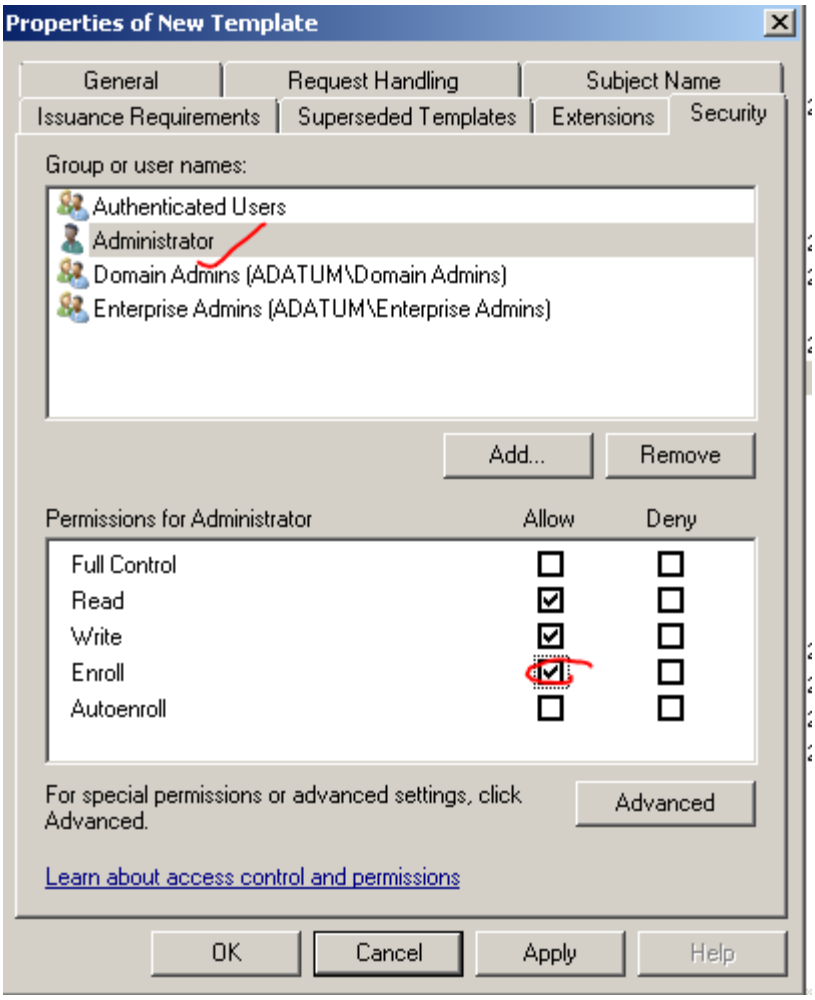


2. Inside certificate manger you'll find default EFS Recovery Agent certificate, rght click on it and create a duplicate certificate. Then you can customize the certificate like below-

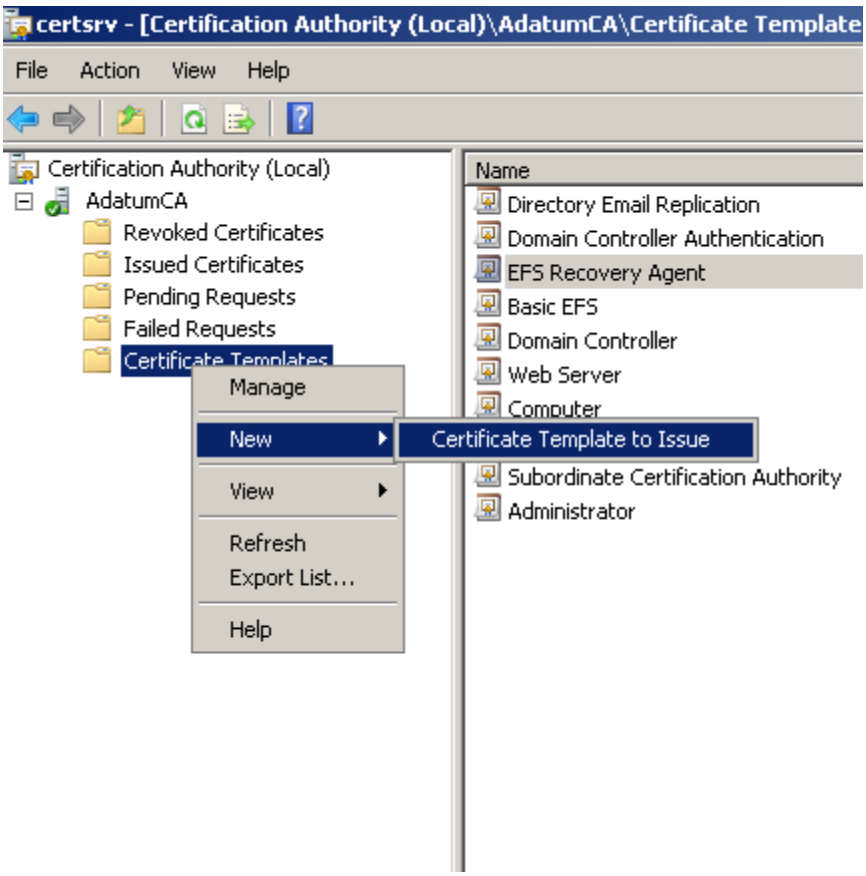

Properties of New Template
Issuance Requirements
Superseded Templates
Extensions
Security
General
Request Handling
Subject Name
Template display name:
EFS Recovery Agent 1
Minimum Supported CAs: Windows Server 2003, Enterprise Edition
After you apply changes to this tab, you can no longer change the template name.
Template name:
EFSRecoveryAgent1
Validity period:
5
years
Renewal period:
6
weeks
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created
OK
Cancel
Apply
Help



Make sure Private key is marked as exportable. Also make sure administrator can enroll for this certificate.

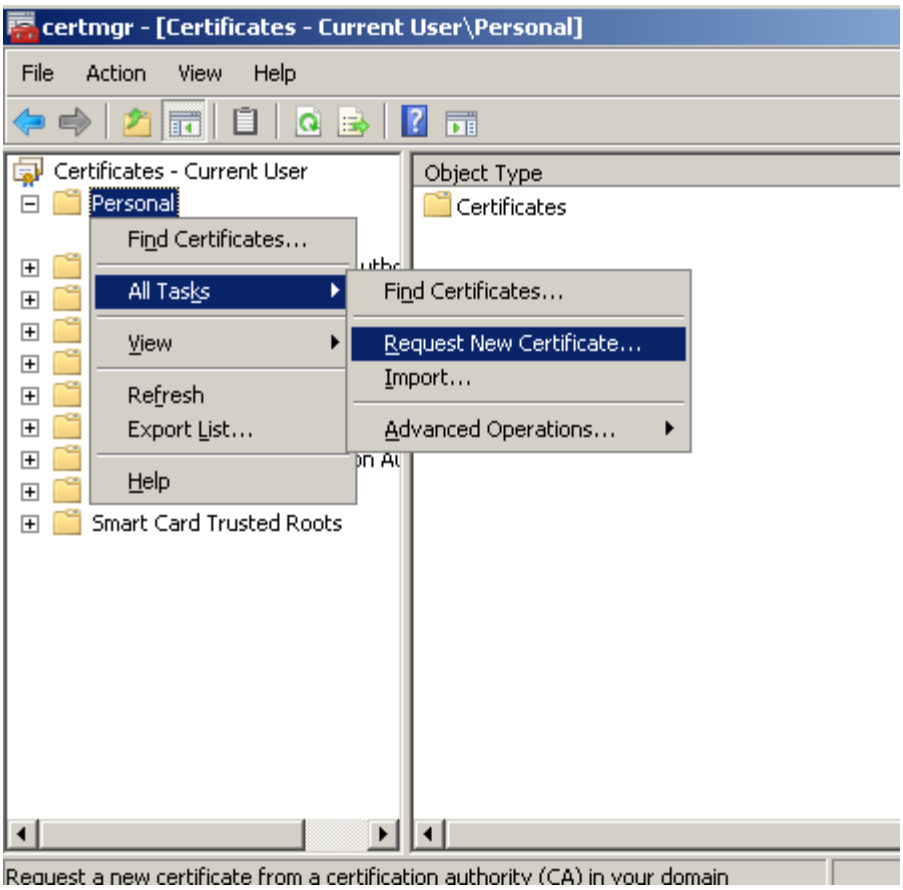


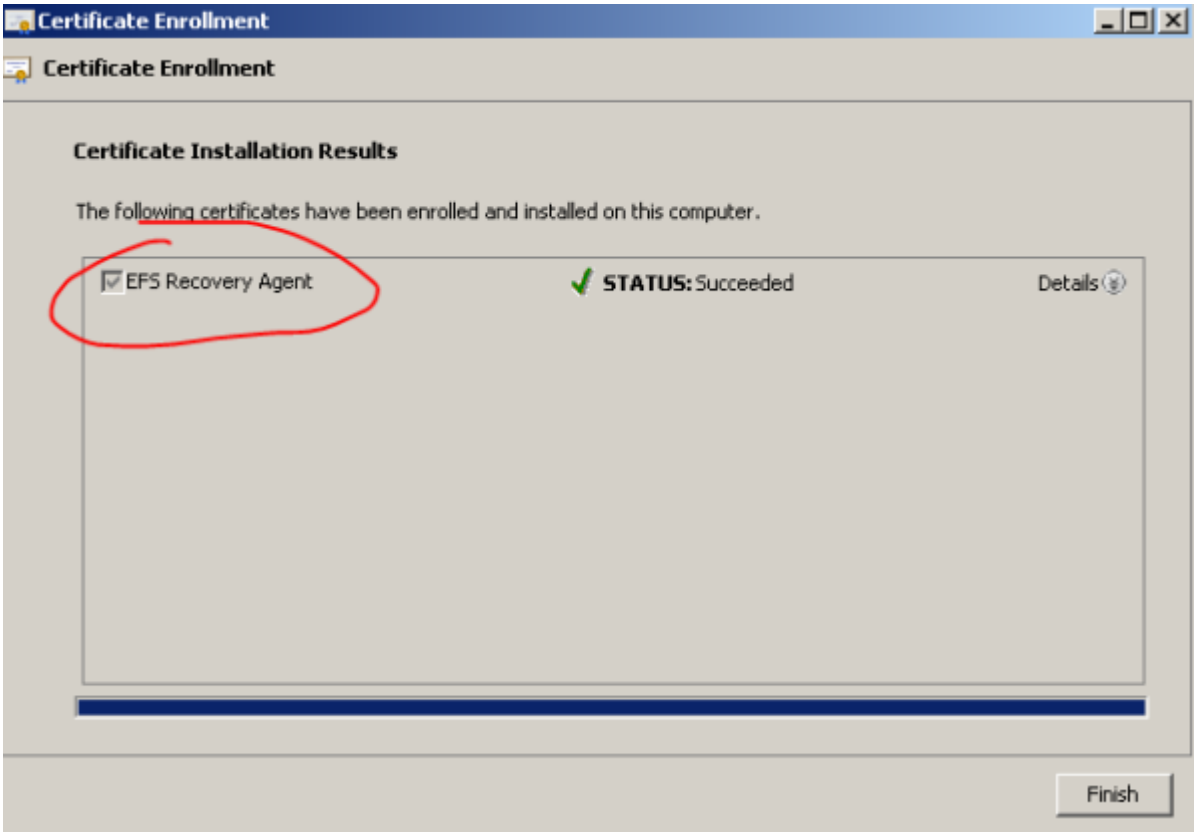
3. Now once done click OK and close the certificate template console, come back to certificate management and bring the newly created template-



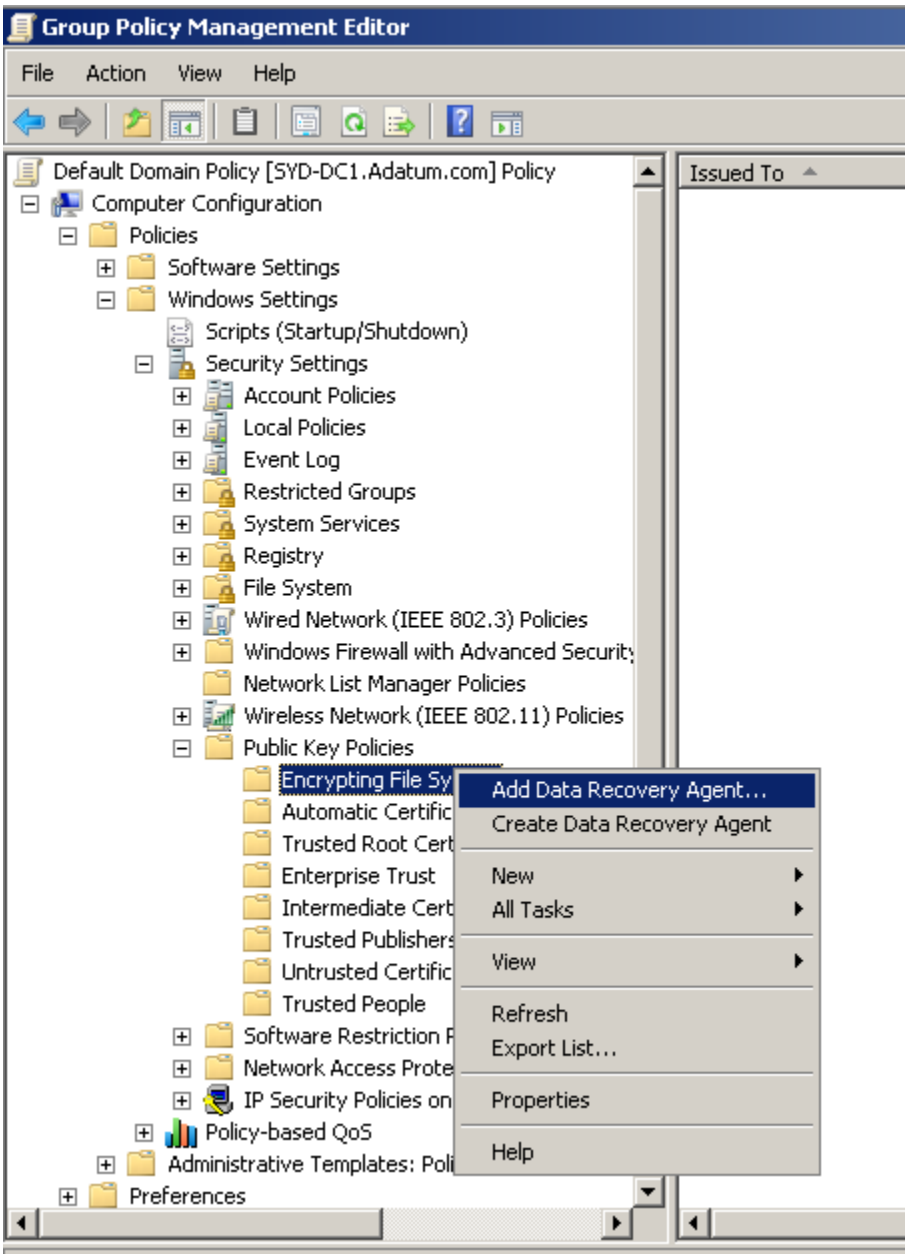
4. Choose the created Type 2 certificate and your certificate is ready for enrollment.

5. Now enroll the administrator for the certificate from the certmgr.msc.

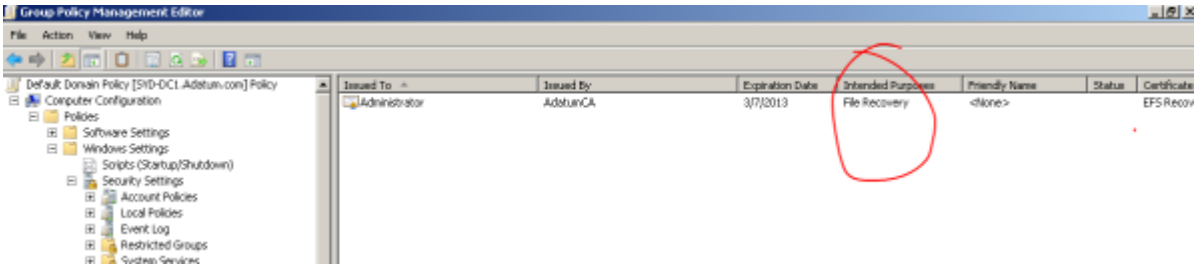

certmgr - [Certificates - Current User\Personal]
File
Action
View
Help
Certificates - Current User
Personal
Find Certificates...
All Tasks
View
Refresh
Export List...
Help
Find Certificates...
Request New Certificate...
Import...
Advanced Operations...
Smart Card Trusted Roots
Object Type
Certificates
Request a new certificate from a certification authority (CA) in your domain



6. Now open group policy management console and edit the policy and add the administrator to DRA.



7. Add the administrator from the directory search and then you'll be presented published certificate of administrator to install.



8. Run Gpupdate /force.

9. Now export the certificate private keys and import it onto client, while logged on using administrator credentials.

10. Now you would be able to decrypt the every encrypted file