# 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-

certsry - [Certification Authority (Local)\AdatumCA\Certificate Templates]					
File Action View Help					
♦ 2 × 2 ≥ 2					
Certification Authority (Local) AdatumCA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates	Name  Directory Email Replication  Domain Controller Authentication  EFS Recovery Agent  Basic EFS  Domain Controller  Web Server  Computer  User  Subordinate Certification Authority  Adeinistration	Intended Purpose Directory Service Email Replication Client Authentication, Server Authenticatio File Recovery Encrypting File System Client Authentication, Server Authentication Server Authentication Client Authentication, Server Authentication Encrypting File System, Secure Email, Clien <all></all>			
		neroone mae aac aginny, and yyeing me			

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-

🙀 certsrv - [Certification Authority (Local)\AdatumCA\Certificate Templates]				
File Action View Help				
🗢 🔿 🙍 🧟 🔹				
Certification Authority (Local)          AdatumCA         Revoked Certificates         Issued Certificates         Pending Requests         Failed Requests         Certificate Tem         Manage         New         View         Refresh         Export List         Help	Name         Image: Directory Email Replication         Domain Controller Authentication         EFS Recovery Agent         Basic EFS         Domain Controller         Web Server         Computer         User         Subordinate Certification Authority         Administrator	Ir D C Fi C S C C E C M		

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: Supers       6         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			

Properties of New Template			
Issuance Requirements   Superseded Templates   Extensions   Security   General Request Handling   Subject Name			
Purpose:   Encryption  Delete revoked or expired certificates (do not archive)  Include symmetric algorithms allowed by the subject  Archive subject's encryption private key			
Minimum key size: 2048			
Do the following when the subject is enrolled and when the private key associated with this certificate is used: © Enroll subject without requiring any user input			
<ul> <li>Prompt the user during enrollment</li> <li>Prompt the user during enrollment and require user input when the private key is used</li> </ul>			
To choose which cryptographic service providersCSPsCSPs			
OK Cancel Apply Help			

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

General Request Han	dling Subject Name		
ssuance Requirements   Superseded	Templates Extensions Securit		
Group or user names:			
& Authenticated Users			
👗 Administrator 🦯			
🚨 Domain Admins (ADATUM\Domain Admins)			
🍇 Enterprise Admins (ADATUM\Ente	erprise Admins)		
	Add Remove		
Permissions for Administrator	Allow Deny		
Full Control			
Read			
Write			
Enroll			
Autoenroll			
For special permissions or advanced se	ttings, click Advanced		
Advanced.			
Learn about access control and permissions			
Learn about access control and permiss			

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.



and installed on this computer.	
STATUS: Succeeded	Details
	Finish
	and installed on this computer.

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

🗐 Group Policy Management Editor				
File Action View Help				
🗐 Default Domain Policy [SYD-DC1.Adatum.com] Policy 📃 🔺 Issued To 🔺				
🕞 👰 Computer Configuration				
🖃 🧮 Policies				
🕀 🦳 Software Settings				
🖃 🧮 Windows Settings				
📄 Scripts (Startup/Shutdown)				
🖃 🚋 Security Settings				
🕀 📑 Account Policies				
🕀 📑 Local Policies				
🕀 📑 Event Log				
🕀 📑 Restricted Groups				
🕀 📑 System Services				
🕀 🔂 Registry				
🗉 📴 File System				
🕀 🧊 Wired Network (IEEE 802.3) Policies				
🕀 📫 Windows Firewall with Advanced Security				
🧮 Network List Manager Policies				
🕀 🌆 Wireless Network (IEEE 802.11) Policies				
🖂 🧮 Public Key Policies				
Encrypting File Sy	Add Data Recovery Agent			
Automatic Certific	Create Data Recovery Agent			
Trusted Root Cert				
Enterprise Trust	New •			
	All Tasks			
	View			
Untrusted Certific				
Irusted People	Refresh			
🛨 🔛 Sortware Restriction H	Export List			
ID Security Policies on	Properties			
	rioperdes			
🖂 🏢 Policy-Dased Q03	Help			

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