Managing Key Archival and Recovery

1 out of 1 rated this helpful - Rate this topic

Applies To: Windows Server 2008 R2

When users lose their private keys, any information that was persistently encrypted with the corresponding public key is no longer accessible. Using key archival and recovery helps protect encrypted data from permanent loss if, for example, an operating system needs to be reinstalled, the user account to which the encryption key was originally issued is no longer available, or the key is otherwise no longer accessible. To help protect private keys, Microsoft enterprise certification authorities (CAs) can archive a user's keys in its database when certificates are issued. These keys are encrypted and stored by the CA.

This private key archive makes it possible for the key to be recovered at a later time. The key recovery process requires an administrator to retrieve the encrypted certificate and private key and then a key recovery agent to decrypt them. When a correctly signed key recovery request is received, the user's certificate and private key are provided to the requester. The requester would then use the key as appropriate or securely transfer the key to the user for continued use. As long as the private key is not compromised, the certificate does not have to be replaced or renewed with a different key.

Key archival and recovery are not enabled by default. This is because many organizations would consider the storage of the private key in multiple locations to be a security vulnerability. Requiring organizations to make explicit decisions about which certificates are covered by key archival and recovery and who can recover archived keys helps ensure that key archival and recovery are used to enhance security rather than detract from security.

You must be a CA administrator to complete this procedure. For more information, see Implement Role-Based Administration.

To configure your environment for key archival of Encrypting File System (EFS) certificates

1. Create a key recovery agent account or designate an existing user to serve as the key recovery agent.
2. Configure the key recovery agent certificate template and enroll the key recovery agent for a key recovery agent certificate. For information, see Identify a Key Recovery Agent.
3. Register the new key recovery agent with the CA. For information, see Enable Key Archival for a CA.
4. Configure a certificate template, such as Basic EFS, for key archival, and enroll users for the new certificate. If users already have EFS certificates, ensure that the new certificate will supersede the certificate that does not include key archival. For information, see Configure a Certificate Template for Key Archival.
5. Enroll users for encryption certificates based on the new certificate template.

Users are not protected by key archival until they have enrolled for a certificate that has key recovery enabled. If they have identical certificates that were issued before key recovery was enabled, data encrypted with these certificates is not covered by key archival.

Identify a Key Recovery Agent

2 out of 2 rated this helpful - Rate this topic

Updated: June 30, 2011

Applies To: Windows Server 2008 R2

A key recovery agent is a person who is authorized to recover a certificate on behalf of an end user. Because the role of key recovery agents can involve sensitive data, only highly trusted individuals should be assigned to this role.

To identify a key recovery agent, you must configure the Key Recovery Agent certificate template to allow the person assigned to this role to enroll for a key recovery agent certificate.

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure. For more information, see Implement Role-Based Administration.

To configure the Key Recovery Agent certificate template

1. Open the Certificate Templates snap-in.
2. In the console tree, right-click the **Key Recovery Agent** certificate template.
3. Click **Duplicate Template**.
4. In the **Duplicate Template** dialog box, click **Windows Server 2003 Enterprise** unless all of your certification authorities (CAs) and client computers are running Windows Server 2008 R2, Windows Server 2008, Windows 7, or Windows Vista.

   Note

   Version 2 certificate templates are customizable certificate templates that are supported with Windows Server 2008 Enterprise–based CAs or Windows Server 2003 Enterprise Edition–based CAs. Version 2 certificate templates enable advanced CA features such as key archival and recovery and certificate autoenrollment. For more information, see Certificate Templates Overview (http://technet.microsoft.com/en-us/library/cc730826.aspx).

5. In **Template**, type a new template display name, and then modify any other optional properties as needed.
6. On the **Security** tab, click **Add**, type the name of the users you want to issue the key recovery agent certificates to, and then click **OK**.
7. Under **Group or user names**, select the user names that you just added. Under **Permissions**, select the **Read** and **Enroll** check boxes, and then click **OK**.

   Note

   To enhance security and control of the key recovery process, you should not use autoenrollment for key recovery agent certificates.

Before the new key recovery agent can enroll for a certificate based on the new certificate template that you created, the template must first be added to the CA. For information about how to complete this procedure, see Add a Certificate Template to a Certification Authority (http://go.microsoft.com/fwlink/?LinkId=147110).

If the certificate was configured with Read and Enroll permissions, the new key recovery agent must use the Certificates snap-in and the Certificate Import Wizard to obtain a key recovery certificate. If the certificate template was configured with Autoenroll permissions, the certificate will be issued automatically the next time the user logs on to the network.

Note

By default, the **CA certificate manager approval** check box is selected on the **Issuance Requirements** tab. Unless you clear this check box, a CA manager must approve the certificate request before a key recovery agent certificate is issued.

The next procedure, Enable Key Archival for a CA, cannot be completed until the key recovery agent has obtained this certificate.