Knowledge Base

HOW TO: Back Up the Recovery Agent Encrypting File System Private Key in Windows 2000

PSS ID Number: 241201

Article Last Modified on 11/21/2003

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Datacenter Server

This article was previously published under Q241201

IN THIS TASK

SUMMARY

You can use the Encrypting File System (EFS) to encrypt data files to prevent unauthorized access. EFS uses a dynamically generated encryption key to encrypt the file. This File Encryption Key (FEK) is encrypted with the your EFS public key and added to the file. You must have the EFS private key to decrypt the FEK. After you decrypt the FEK, you can use the FEK to decrypt the file.

In EFS, you can use a Recovery Agent decrypted encrypted files in the event that your EFS private key is lost. Every time a file is encrypted, the FEK is also encrypted with this Recovery Agent's EFS public key. This encrypted FEK is attached to the file with the copy that is encrypted with your EFS public key. If you use the Recovery Agent's private key, you can decrypt the FEK, and then decrypt the file.

In Windows 2000, the local administrator is the default Recovery Agent. If the computer is joined to a Windows 2000 domain, the domain administrator is the default Recovery Agent. This article describes how to back up the EFS Recovery Agent's private key so that encrypted data can be recovered in the event that the copy that is located on the computer is lost.

WARNING: After you export the private key to a disk, store the disk in a secure place. If someone gains access to your EFS private key, he or she can gain access to your encrypted data.

back to the top

Export Your Private Key from the Recovery Agent

1. Log on to your computer using the local Administrator account. **NOTE**: You must use the built-in Administrator account, not just an account with Administrator privileges.
2. Click **Start**, click **Run**, type `secpol.msc`, and then click **OK**.
3. Expand **Public Key Policies**.
4. Click the **Encrypted Data Recovery Agents** category.
5. In the right pane, right-click the certificate that is issued to the administrator that has the intended purpose of file recovery, point to **All tasks**, and then click **Export**.
6. Click **Next**.
7. Make sure **Yes, export the private key** is selected, and then click **Next**.
8. To remove the private key associated with the Administrator account, click to select the **Delete the private key if the export is successful** check box.
9. Click **Next**.
10. Type and confirm a password to secure the exported key, and then click **Next**.
11. After you are prompted to save the certificate and the private key to a file, type an appropriate file name, and then click **Next**.

    Microsoft recommends that you back up the file to a disk or removable media device, and then store the backup in a location where you can confirm the physical security of the backup.
12. When the **Completing the Certificate Export Wizard** page is displayed, verify the settings that you selected, and then click **Finish**.
13. Click **OK**.
14. You must restart the computer to complete the removal of the private key.

back to the top

Export the Domain Recovery Agent's Private Key

1. Locate the first domain controller that was promoted into the domain.
2. Log on to the domain controller by using the Domain Administrator account.

   NOTE: You must use the built-in Administrator account, not just an account that has Administrator privileges.
3. Click **Start**, click **Run**, type `dompol.msc`, and then click **OK**.
4. Expand **Public Key Policies**.

5. Click the **Encrypted Data Recovery Agents** category.
6. In the right pane, right-click the certificate that is issued to the administrator that has an intended purpose of file recovery, point to **All tasks**, and then click **Export**.
7. Click **Next**.
8. Make sure that **Yes, export the private key** is selected, and then click **Next**.

   If this option is unavailable, you are not logged on to the first domain controller in the domain, the private key has been deleted, or you are not logged on as the built-in domain administrator. If the Recovery Agent private key cannot be located on any domain controller, encrypted files in the domain cannot be recovered.
9. To remove the private key associated with the Administrator account, click to select the **Delete the private key if the export is successful** check box.
10. Click **Next**.
11. Type and confirm a password to secure the exported key, and then click **Next**.
12. After you are prompted to save the certificate and the private key to a file, type an appropriate file name, and then click **Next**.

    Microsoft recommends that you back up the file to a disk or removable media device, and then store the backup in a location where you can confirm the physical security of the backup.
13. Confirm the settings on the **Completing the Certificate Export Wizard**, and then click **Finish**.
14. Click **OK**.
15. Restart the domain controller to complete the removal of the private key.

Troubleshooting

If your computer is a member of a Windows domain, the domain administrator can designate certain users as EFS recovery agents, who can recover data even if a specific user's private key is lost.

If your computer is not participating in a Windows domain, (for example, a stand-alone computer, or a computer in a Microsoft Windows NT 4.0-based domain structure), the local Administrator account is the designated EFS recovery agent. Because of this, you can recover your encrypted data only if you previously backed up the local administrator's private key.

back to the top

REFERENCES

For additional information, click the article numbers below to view the articles in the Microsoft Knowledge Base:

223316 Best Practices for Encrypting File System

230520 How to Encrypt Data Using EFS in Windows 2000

242296 How to Restore an EFS Private Key for Encrypted Data Recovery

To download the "Encrypting File System for Windows 2000" white paper, please visit the following Microsoft Web site:

http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp

back to the top

Keywords: kbEFS kbenv kbhowto kbHOWTOmaster w2000efs KB241201
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000DataServ kbwin2000DataServSearch kbwin2000Pro kbwin2000ProSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinDataServSearch

Send feedback to Microsoft