Knowledge Base

The Local Administrator Is Not Always the Default Encrypting File System Recovery Agent

PSS ID Number: 255026

Article Last Modified on 11/18/2003

The information in this article applies to:

- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Professional SP1

This article was previously published under Q255026

SUMMARY

This article discusses how the local administrator is not always the default Encrypting File System (EFS) recovery agent.

MORE INFORMATION

The EFS tool provides built-in data recovery by enforcing a recovery policy requirement. The requirement is: a recovery policy must be in place before users can encrypt files. The recovery policy provides for a person to be designated as the recovery agent. If the recovery policy is not inherited from a site, domain, or organizational unit policy, the local policy is in effect.

A default local recovery policy is automatically created when an administrator account logs on to the computer for the first time. When this process occurs, that administrator becomes the default recovery agent. In some situations, the first administrator to log on to Windows 2000 is not the local administrator account.

Scenario 1: The Network Identification Wizard

When Windows 2000 Professional completes Setup and restarts, the Network Identification Wizard prompts the user to either select an automatic logon account or a username and password for logon purposes. When a username is specified, that account is created, placed in the Local Administrators group, and then logged on to the computer. Because the newly created account is the first administrator to log on to the computer, the EFS service generates a self-signed certificate issued to that user and places it in the Encrypted Data Recovery Policy (EDRP).

Scenario 2: Joining a Domain During Setup

During the setup of Windows 2000 Server or Windows 2000 Advanced Server, the option to join a domain or workgroup is provided. If the server is joined to a domain, any user account that is a member of the Domain Administrators global group is an administrator on that server. If one of these Domain Administrator accounts is logged on, that account becomes the recovery agent in the local EDRP.

This behavior is acceptable in environments where a domain-level recovery policy is defined because the domain recovery policy supercedes any local policy on members of the domain. However, if a recovery policy is not specified at the site, domain, or organizational unit level (it has been deleted), the local policy is in effect.

NOTE: If a recovery policy is initialized at the site, domain or organizational unit level, but it contains no recovery certificates, EFS is disabled on computers that apply that policy as their highest priority (the policy is not overridden by one that has a higher priority).

Keywords: kbEFS kbinfo w2000efs KB255026
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbWin2000AdvServSP1 kbwin2000Pro kbwin2000ProSearch kbWin2000ProSP1 kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbwin2000ServSP1 kbWinAdvServSearch