



Server Administration

Module Number: 02

Module Name: Securing Files and Disks

Securing Files and Disks

AIM:

To equip students with the techniques for Securing Files and Disks from un-authorized Access.



Objectives:

The Objectives of this module are:

- Describe File Server Resource Manager.
- Explain the configure BitLocker encryption.
- Explain the configure BitLocker encryption using cypher Command.
- Describe configure BitLocker policies.
- Outline configure the EFS recovery agent.
- Manage EFS and BitLocker certificates including backup and restore.

Outcomes:

At the end of this module, you are expected to:

- Define File Server Resource Manager.
- Explain BitLocker encryption and its uses.
- Explain EFS and its uses.
- Differentiate between EFS file Encryption and BitLocker Encryption.

Contents

1. Configuring File Server Resource Manager
2. How to Securing Files
3. Encryption files with EFS
4. Configuring EFS Using the cypher Command
5. Sharing Files Protected with EFS with others
6. Configuring EFS with Group Policies
7. Configuring EFS Recovery Agent
8. Managing EFS Certificates
9. Encrypting Files with BitLocker
10. Configuring BitLocker Encryption
11. configuring BitLocker to Go
12. Configuring BitLocker Policies
13. Managing BitLocker Certificates

Configuring File Server Resource Manager

As an administrator, when you need to control and manage the amount and type of data stored on your servers, Microsoft delivers the tools to help you do just that. The File Server Resource Manager (FSRM) is a suite of tools that allows an administrator to place quotas on folders or volumes, filter file types, and create detailed storage reports. These tools allow an administrator to properly plan and implement policies on data as needed.

FSRM Features

Many of the advantages of using FSRM come from all of the included features, which allow administrators to manage the data that is stored on their file servers. Some of the advantages included with FSRM are as follows:

- **Configure File Management Tasks:** FSRM allows an administrator to apply a policy or action to data files. Some of the actions that can be performed include the ability to encrypt files or run a custom command.
- **Configure Quotas:** Quotas give an administrator the ability to limit how much disk space a user can use on a file server. Administrators have the ability to limit space to an entire volume or to specific folders.
- **File Classification Infrastructure:** Administrators can set file classifications and then manage the data more effectively by using these classifications. Classifying files, and then setting policies to those classifications, allows an administrator to set policies on those classifications. These policies include restricting file access, file encryption, and file expirations.
- **Configure File Screens:** Administrators can set file screening on a server and limit the types of files that are being stored on that server. For example, an administrator can set a file screen on a server so that any file ending in .bmp gets rejected.
- **Configure Reports:** Administrators can create reports that show them how data is classified and accessed. They also have the ability to see which users are trying to save unauthorized file extensions.

Installing the FSRM Role Service

Installing FSRM is easy when using either Server Manager or PowerShell. To install using Server Manager, you go into Add Roles And Features and choose File And Storage Services ➤ File Services ➤ File Server Resource Manager. To install FSRM using PowerShell, you use the following command:

```
Install-Windows Feature -Name FS-Resource-Manager –Include Management Tools
```

Configuring FSRM using the Windows GUI version is straightforward, but setting up FSRM using PowerShell is a bit more challenging.

The following table describes some of the PowerShell commands for FSRM.

PowerShell commands for FSRM	
Power Shell cmdlet	Description
Get-FsrmAutoQuota	Gets auto-apply quotas on a server
Get-FsrmClassification	Gets the status of the running file classification
Get-FsrmClassificationRule	Gets classification rules
Get-FsrmFileGroup	Gets file groups
Get-FsrmFileScreen	Gets file screens
Get-FsrmFileScreenException	Gets file screen exceptions
Get-FsrmQuota	Gets quotas on the server
Get-FsrmSetting	Gets the current FSRM settings
Get-FsrmStorageReport	Gets storage reports
New-FsrmAutoQuota	Creates an auto-apply quota
New-FsrmFileGroup	Creates a file group
New-FsrmFileScreen	Creates a file screen
New-FsrmQuota	Creates an FSRM quota
New-FsrmQuotaTemplate	Creates a quota template
Remove-FsrmClassificationRule	Removes classification rules
Remove-FsrmFileScreen	Removes a file screen
Remove-FsrmQuota	Removes an FSRM quota from the server
Set-FsrmFileScreen	Changes the configuration settings of a file screen
Set-FsrmQuota	Changes the configuration settings for an FSRM quota

Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk.

Decryption is the process of converting data from encrypted format back to its original format.

Encryption algorithms can be divided into three classes

- Symmetric
- Asymmetric
- Hash function

- **Symmetric Encryption** uses a single key to encrypt and decrypt data. Therefore, it is also referred to as secret-key, single-key, shared-key, and private-key encryption. To use symmetric-key algorithms, you need to initially send or provide the secret key to both the sender and the receiver.
- **An asymmetric key**, also known as public-key cryptography, uses two mathematically related keys. One key is used to encrypt the data and the second key is used to decrypt the data. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. Instead, you can make the public key known to anyone and use the other key to encrypt or decrypt the data. The public key can be sent to someone or it can be published within a digital certificate via a Certificate Authority (CA). Secure Socket Layer (SSL)/Transport Layer Security (TLS) and Pretty Good Privacy (PGP) use asymmetric keys.

- The last type of encryption is the **hash function**. Different from the symmetric and asymmetric algorithms, a hash function is meant as a one-way encryption. That means that after the data has been encrypted, it cannot be decrypted. One example of its use is to use the hash function to encrypt a password that is stored on disk. Anytime a password is entered and it needs to be verified that it is the correct password, the same hash calculation is performed on the entered password and compared to the hash value of the password stored on disk. If the two matches, the user must have typed in the password. This avoids storing the passwords in a readable format that a hacker might try to access.

Securing Files and Disks

Today, newer versions of Windows offer two file encrypting technologies:

- **Encrypting File System (EFS):** EFS protects individual files or folders.
- **BitLocker Drive Encryption:** BitLocker protects entire volumes.



Encrypting Files with EFS

Encrypting File System (EFS) can encrypt files on an NTFS volume that cannot be used unless the user has access to the keys required to decrypt the information. By default, when you encrypt a file with EFS, the file or folder turns green to show that the file is encrypted. After a file has been encrypted, you do not have to manually decrypt an encrypted file before you can use it. Instead, you work with the file or folder just like any other file that is not encrypted. When you open a file that is encrypted with EFS, the file is automatically decrypted as needed. When you save the file, it is automatically decrypted. However, if another user tries to access the same file, he cannot open it because he does not have the proper key to open the file.

EFS uses an encryption key to encrypt your data, which is stored in a digital certificate. The first time a user encrypts a file or folder, an encryption certificate and key are created and bound to the user account. The user who creates the file is the only person who can read it. As the user works, EFS encrypts the files using a key generated from the user's public key. Data encrypted with this key can be decrypted only by the user's personal encryption certificate, which is generated using a private key.

Operation of EFS

EFS works by encrypting a file with a bulk [symmetric key](#), also known as the File Encryption Key, or FEK. It uses a symmetric encryption algorithm because it takes less time to encrypt and decrypt large amounts of data than if an [asymmetric key](#) cypher is used. The symmetric encryption algorithm used will vary depending on the version and configuration of the operating system. The FEK (the symmetric key that is used to encrypt the file) is then encrypted with a [public key](#) that is associated with the user who encrypted the file, and this encrypted FEK is stored in the \$EFS alternative data stream of the encrypted file. To decrypt the file, the EFS component driver uses the private key that matches the EFS digital certificate (used to encrypt the file) to decrypt the symmetric key that is stored in the \$EFS stream. The EFS component driver then uses the symmetric key to decrypt the file. Because the encryption & decryption operations are performed at a layer below NTFS, it is transparent to the user and all their applications.

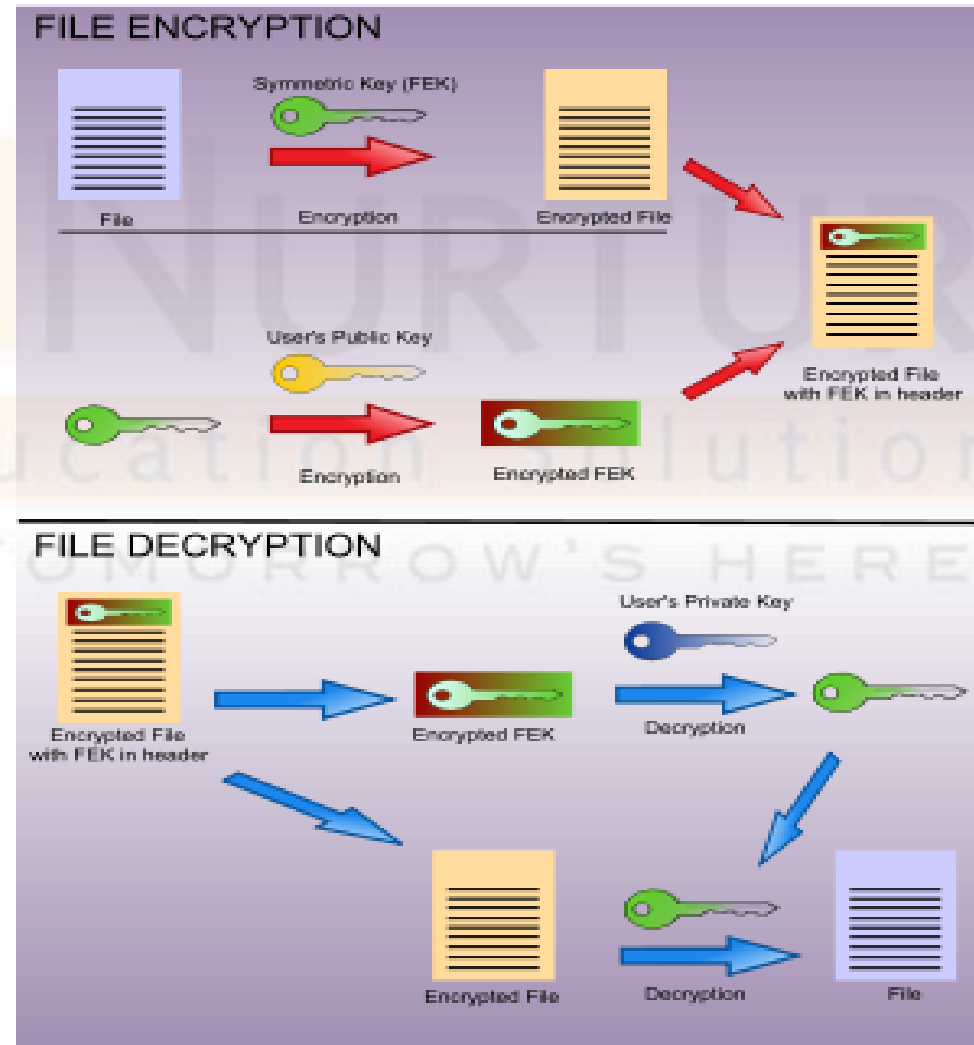
Folders whose contents are to be encrypted by the file system are marked with an encryption attribute. The EFS component driver treats this encryption attribute in a way that is analogous to the inheritance of file permissions in NTFS: if a folder is marked for encryption, then by default all files and subfolders that are created under the folder are also encrypted. When encrypted files are moved within an NTFS volume, the files remain encrypted. However, there are a number of occasions in which the file could be decrypted without the user explicitly asking Windows to do so.

Operation of EFS

Files and folders are decrypted before being copied to a volume formatted with another file system, like [FAT32](#). Finally, when encrypted files are copied over the network using the SMB/CIFS protocol, the files are decrypted before they are sent over the network.

Securing Files and Disks

Operation of Encrypting File System



Configuring Of Efs

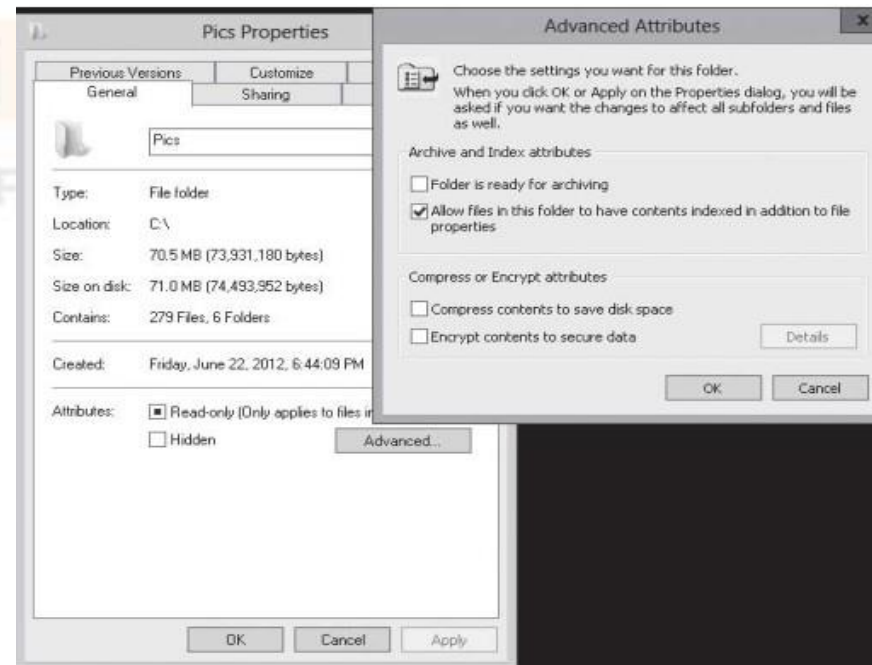
To encrypt or decrypt a folder or file, enable or disable the encryption attribute just as you set any other attribute, such as read-only, compressed, or hidden. If you encrypt a folder, all files and subfolders created in the encrypted folder are automatically encrypted. Microsoft recommends that you encrypt at the folder level. You can also encrypt or decrypt a file or folder using the cypher command.

Encrypt A Folder Or File Using Efs

To encrypt a folder or file, perform the following steps:

1. Right-click the folder or file you want to encrypt, and then click **Properties**. The **Properties** dialogue box opens.
2. Click the **General** tab, and then click **Advanced**. The **Advanced Attributes** dialogue box appears.

Displaying the Advanced Attributes
dialogue box



Encrypt A Folder Or File Using Efs (Cont...)

3. Select the **Encrypt contents to secure data** checkbox.
4. Click OK to close the **Advanced Attributes** dialogue box.
5. Click OK to close the **Properties** dialogue box.
6. If you encrypt a file in an unencrypted folder, it gives you a warning. If you want to encrypt only the file, select **Encrypt the file only** and click OK. If you want to encrypt the folder and all content in the folder, select the **Encrypt the file and its parent folder (recommended)** option. Click OK.



Encrypting a file in an unencrypted folder

Encrypt A Folder Or File Using Efs (Cont...)

7. If you encrypt a folder, it asks you to confirm the changes. If you want to encrypt only the folder, select Apply changes to this folder only. If you want to apply to all folders, select Apply changes to this folder, subfolders and files. Click OK to close the Confirm Attribute Changes dialog box.



Confirming attribute changes

Decrypt A Folder Or File

To decrypt a folder or file, perform the following steps:

1. Right-click the folder or file you want to decrypt, and then click **Properties**. The **Properties** **dialogue** box opens.
2. Click the **General** **tab**, and then click **Advanced**. The **Advanced Attributes** dialogue box opens.
3. Clear the **Encrypt contents to secure data** checkbox.
4. Click OK to close the **Advanced Attributes** dialogue box.
5. Click OK to close the **Properties** dialogue box.
6. When it asks you to confirm the changes. If you want to decrypt only the folders, select **Apply changes to this folder** only. If you want to apply to all folders, select **Apply changes to this folder, subfolders and files**. Click OK.

Points to be followed while working with EFS:

- You can encrypt or compress NTFS files only when using EFS; you can't do both. If the user marks a file or folder for encryption, that file or folder is uncompressed.
- If you encrypt a file, it is automatically decrypted if you copy or move the file to a volume that is not an NTFS volume.
- Moving unencrypted files into an encrypted folder automatically causes those files to be encrypted in the new folder.
- Moving an encrypted file from an EFS-encrypted folder does not automatically decrypt files. Instead, you must explicitly decrypt the file.

Points to be followed while working with EFS: (Cont...)

- Files marked with the System attribute or that are in the root directory cannot be encrypted.
- Remember that an encrypted folder or file does not protect against the deletion of the file, listing the files or directories. To prevent deletion or listing of files, use NTFS permissions.
- Although you can use EFS on remote systems, data that is transmitted over the network is not encrypted. If encryption is needed over the network, use SSL/TLS (Secure Sockets Layer/Transport Layer Security) or IPsec.

Using The Cypher Command

The cypher command is useful when it comes to EFS. Cypher is a command-line utility that allows you to change and/or configure EFS. When it comes to using the cypher command, you should be aware of a few things:

- Administrators can decrypt files by running cypher.exe in the Command Prompt Window (advanced users).
- Administrators can use a cypher to modify an EFS-encrypted file.
- Administrators can use a cypher to import EFS certificates and keys.
- Administrators can also use a cypher to back up EFS certificates and keys.

Securing Files and Disks

The cypher .exe command displays or alters the encryption of folders and files on NTFS volumes. If you use the cypher command without parameters, cypher displays the encryption state of the current folder and any files it contains. The syntax of the cypher command includes the following:

cypher /options [pathname [...]]

- /C: Displays information on the encrypted file.
- /D: Decrypts the specified files or directories.
- /E: Encrypts the specified files or directories. Directories are marked so that files added afterwards will be encrypted. The encrypted file can become decrypted when it is modified if the parent directory is not encrypted. It is recommended that you encrypt the file and the parent directory.
- /H: Displays files with the hidden or system attributes. These files are omitted by default.
- /K: Creates a new certificate and key for use with EFS. If this option is chosen, all the other options are ignored.

Securing Files and Disks

- /N: This option works only with /U. This prevents keys from being updated. It is used to find the encrypted files on the local drives.
- /R: Generates an EFS recovery key and certificate, and then writes them to a .PFX file (containing certificate and private key) and a .CER file (containing only the certificate).
- /S: Performs the specified operation on the given directory and all files and subdirectories in it.
- /U: Tries to touch all the encrypted files on local drives. This updates the user's file encryption key or recovery keys to the current ones if they are changed. This option does not work with other options except /N.
- /W: Removes data from available unused disk space on the entire volume. If this option is chosen, all other options are ignored. The directory specified can be anywhere in a local volume. If it is a mount point or points to a directory in another volume, the data on that volume is removed.
- /X: Backs up the EFS certificate and keys to the specified filename that follows the /X: If EFS file is provided, the current user's certificate(s) used to encrypt the file is backed up. Otherwise, the user's current EFS certificate and keys are backed up.

Securing Files and Disks

- /ADDUSER: Adds a user to the specified encrypted file(s).
- /REKEY: Updates the specified encrypted file(s) to use the configured EFS current key.
- /REMOVEUSER /certhash: <Hash>: Removes a user from the specified file(s). CERTHASH must be the SHA1 hash of the certificate to remove.

For example, To use cypher to encrypt a subfolder named c:\Data\Reports, and then execute the following command:

```
cypher /e c:\Data\Reports
```

To decrypt the folder, execute the following command:

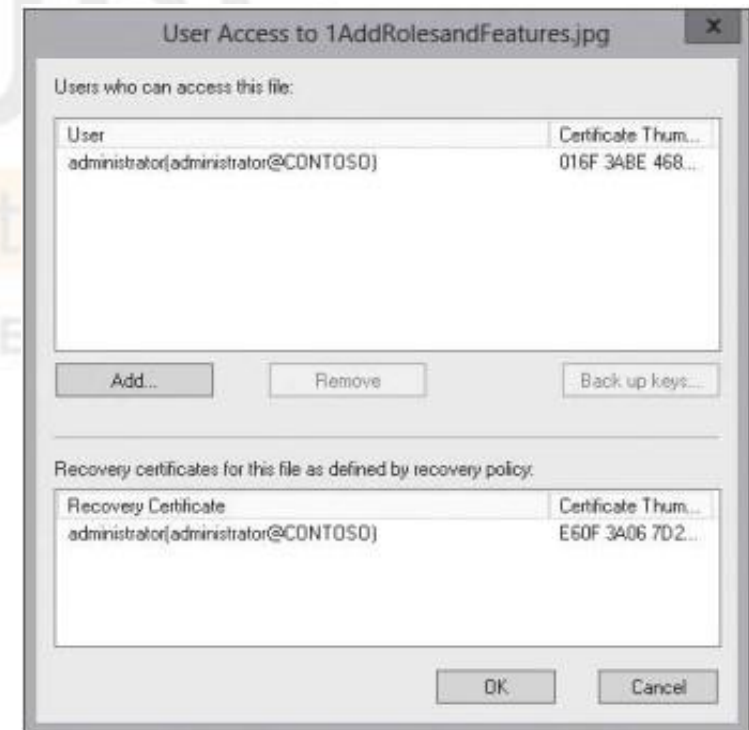
```
cypher /d c:\Data\Reports
```

Sharing Files Protected With Efs With Others

When EFS was originally created, an EFS file could be accessed by only the one person who encrypted the file. In later versions of NTFS, if you need to share an EFS-protected file with other users, you add an encryption certificate to the file.

To share a file protected with EFS with others, perform the following steps:

1. Right-click the encrypted file and select **Properties**.
2. On the **General** tab, click **Advanced**. The **Advanced Attributes** dialogue box opens.
3. Click **Details**. The **User Access** dialog box opens



User Access dialogue box

Securing Files and Disks

4. Click the **Add** button. The **Encrypting File System** dialog box opens.



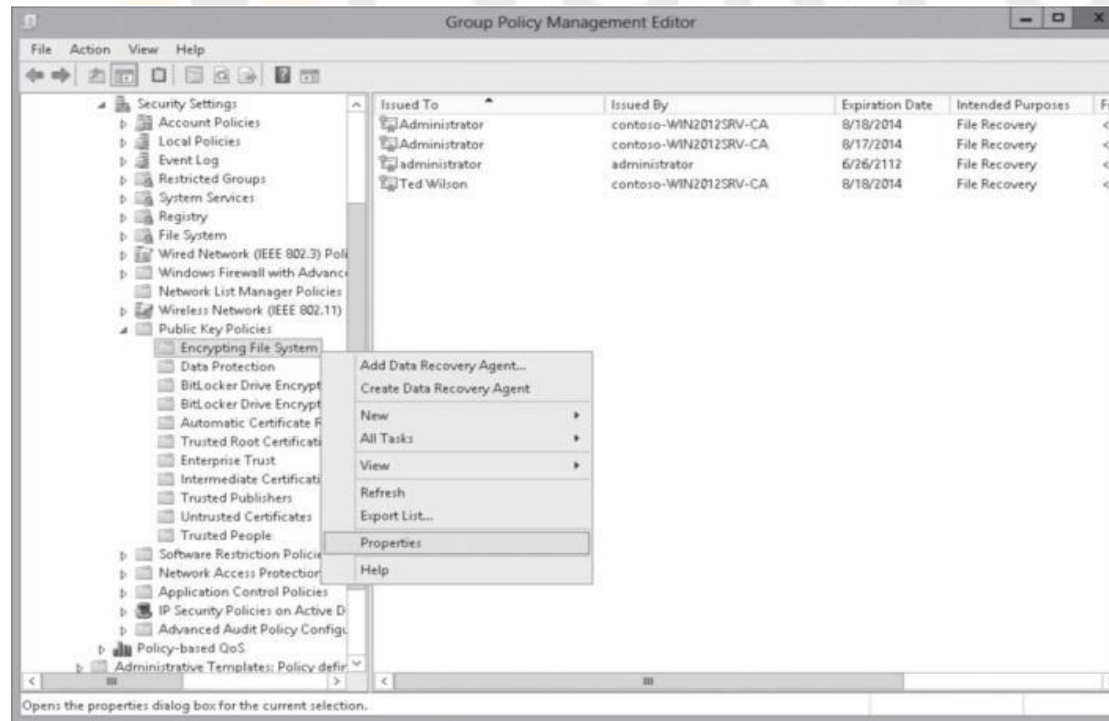
Encrypting File System dialog box

5. Select the user you want to grant access to and click **OK** to close the **Encrypting File System** dialog box.
6. Click **OK** to close the **User Access** dialogue box.
7. Click **OK** to close the **Advanced Attributes** dialogue box.
8. Click **OK** to close the **Properties** dialogue box.

Configuring Efs With Group Policies

To help you manage the use of EFS, you can use group policies to meet your organisation's security needs.

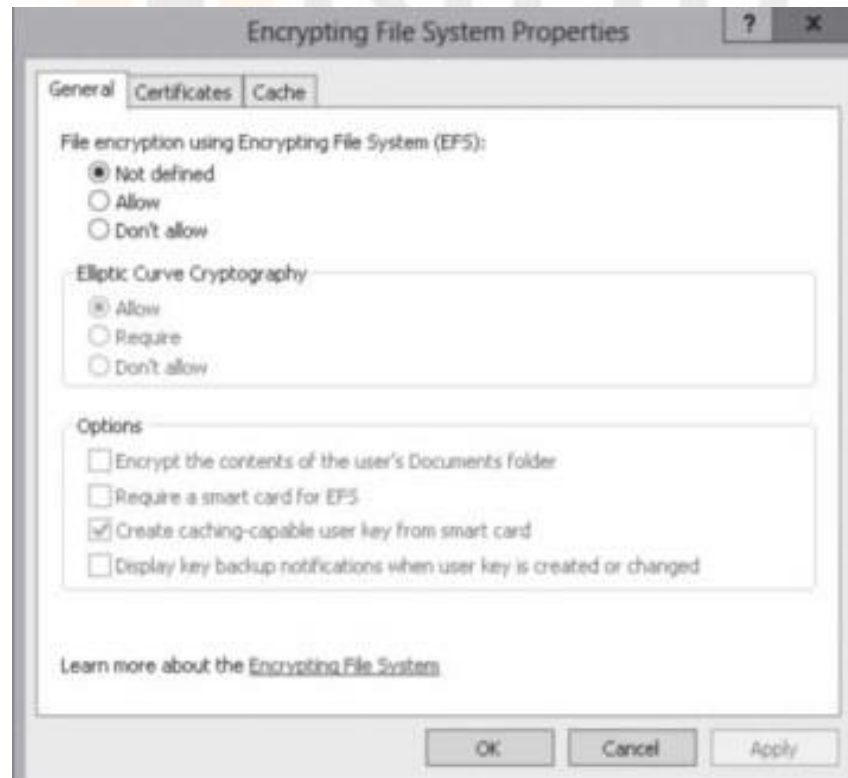
To establish an EFS policy, right-click Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Encrypting File System and select Properties.



Encrypting File
System properties

Securing Files and Disks

Under the General tab, you can choose to allow or disallow the use of EFS. If you do not configure any policy settings for EFS, it is allowed. If you choose to use EFS, you can automatically encrypt a user's Documents folder, require a smart card for use with EFS, or notify users to make backup copies of their encryption keys. In addition, you can require strong encryption, and you can use Elliptic Curve Cryptography (ECC) encryption.



Encrypting File System
Properties General tab

Securing Files and Disks

By clicking the Certificates tab, you can specify the key size for the certificates and allow EFS to generate self-signed certificates when a CA is not available.



Encrypting File System Properties Certificates tab

What is the EFS recovery agent?

The EFS Recovery Agent is a user with permission to decrypt data, encrypted by another user, if the latter lost the encryption certificate keys or if the user's account was deleted, but the encrypted data is needed. As a rule, the Recovery Agent is the Administrator, but it can also be a different user. There can be multiple Recovery Agents. In order to assign Recovery Agent permissions to a user, first Recovery Agent certificates need to be created using the command "cypher /R: filename", where "filename" is the path and name of the created certificates without the extension. After this, the user will be asked to enter a password to protect the private key and to confirm it (the password is not displayed in the console on entry). Then two files are created with the specified name: *.cer and *.pfx. These contain the public and private certificate keys, respectively. Now the certificate must be added to the user's personal storage, specified by the Recovery Agent importing the file *.pfx.

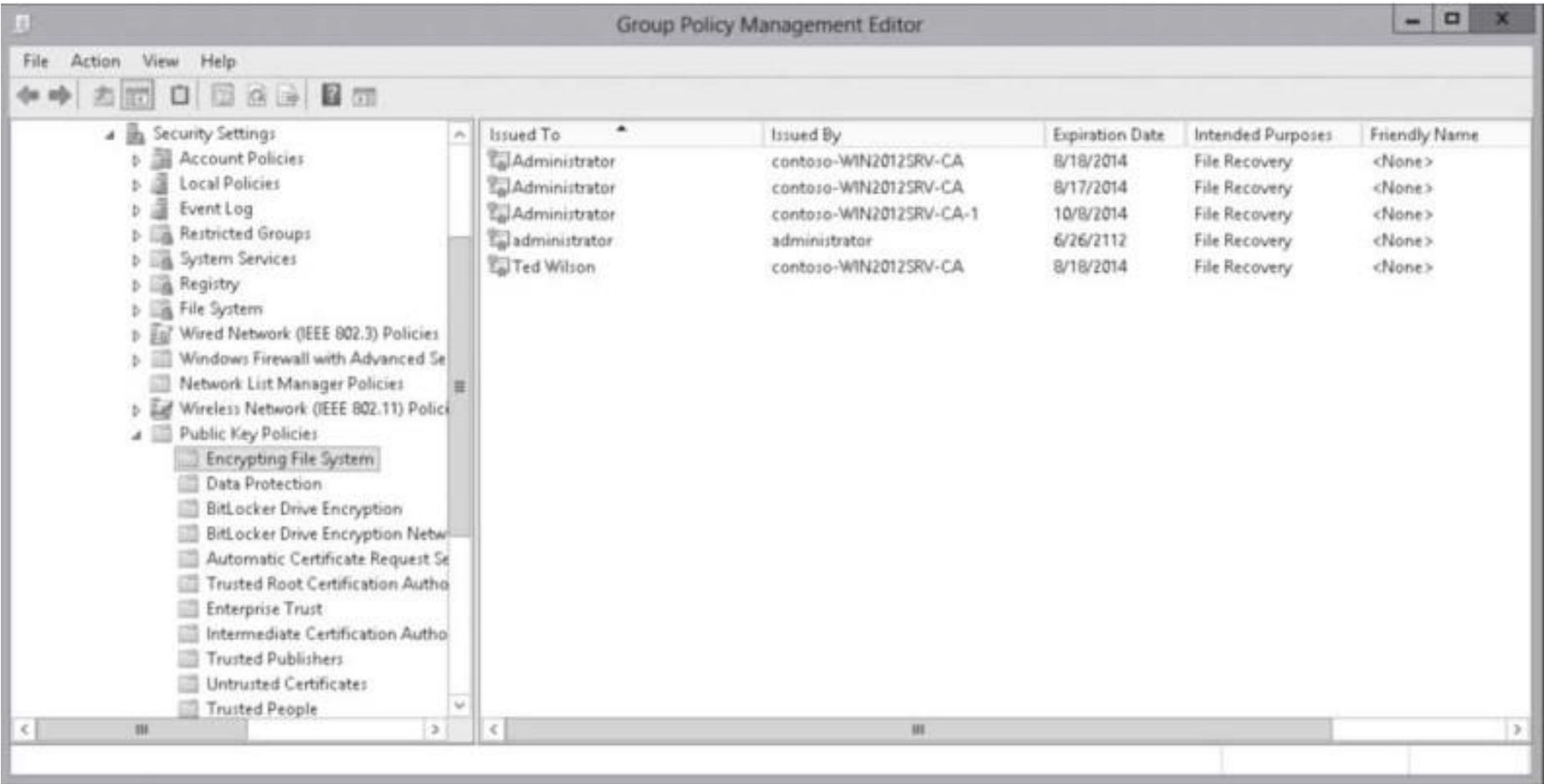
Configuring The EFS Recovery Agent

If for some reason, a person leaves the company or a person loses the original key, and the encrypted files cannot be read, you can set up a **Data Recovery Agent (DRA)** that can recover EFS-encrypted files for a domain. To define DRAs, you can use Active Directory group policies to configure one or more user accounts as DRAs for your entire organisation. However, to accomplish this, you need to have an enterprise CA.

Add recovery agents for EFS

1. Log in as the DRA account.
2. Open the Group Policy Management console.
3. Expand Forest, Domains, and then the name of your domain.
4. Right-click the Default Domain Policy and click Edit.
5. Expand Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\.
6. Right-click Encrypting File System, and select Create Data Recovery Agent.
7. Click Encrypting File System and notice the certificates that are displayed.
8. Close the Group Policy Editor.
9. Close Group Policy Management console.

Securing Files and Disks



Viewing the Encrypting File System certificates

Managing EFS Certificates

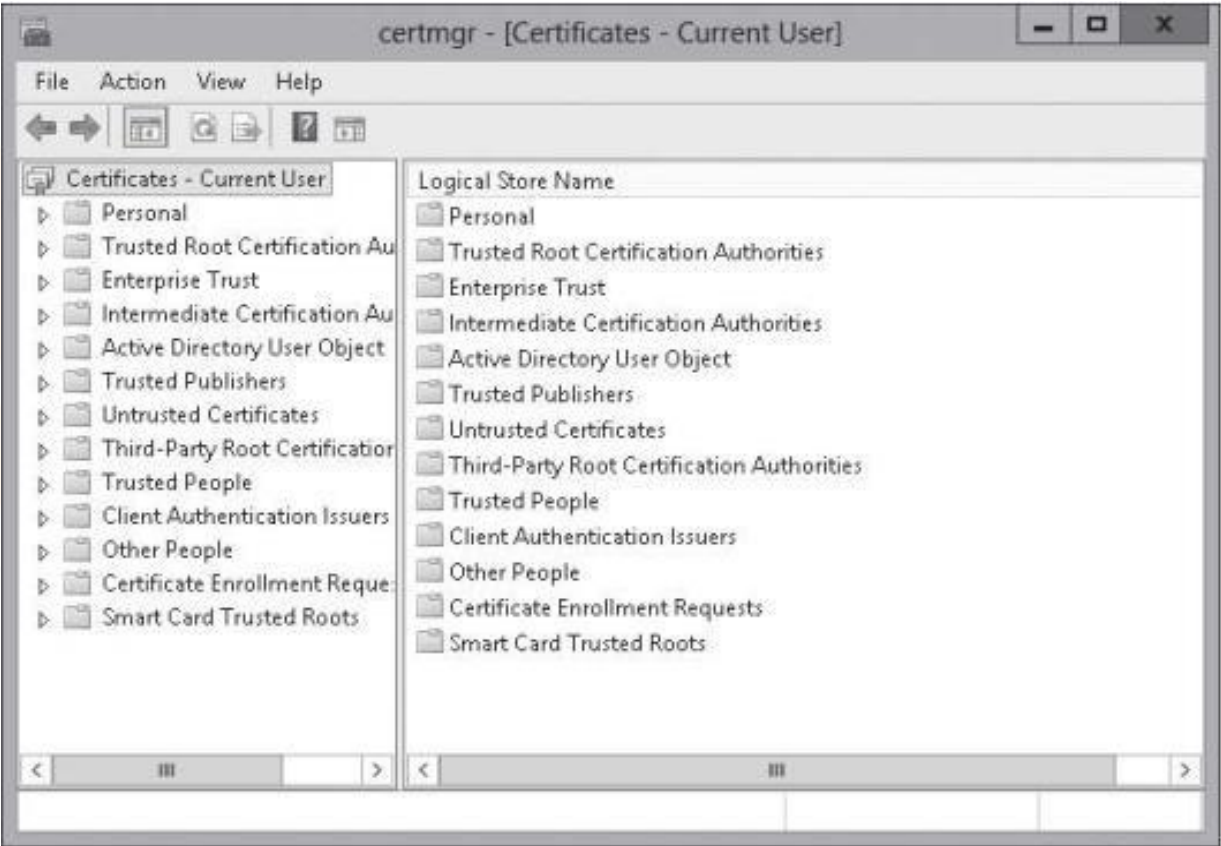
The first time you encrypt a folder or file, an encryption certificate is automatically created. If your certificate and key are lost or damaged and you don't have a backup, you won't be able to use the files that you have encrypted. Therefore, you should back up your encryption certificate.

Back Up An EFS Certificate

To back up your EFS certificate, perform the following steps:

1. Open a command prompt.
2. Execute the certmgr.msc command. If you are prompted for an administrator password or confirmation, type the password or provide confirmation. The certmgr console opens.
3. In the left pane, double-click Personal, and then click Certificates.
4. In the main pane, right-click the certificate that lists Encrypting File System under Intended Purposes. Select All Tasks, and then click Export. If there is more than one EFS certificate, you should back up all of them one by one.

Securing Files and Disks



Opening the certmgr console



Exporting a certificate

Securing Files and Disks

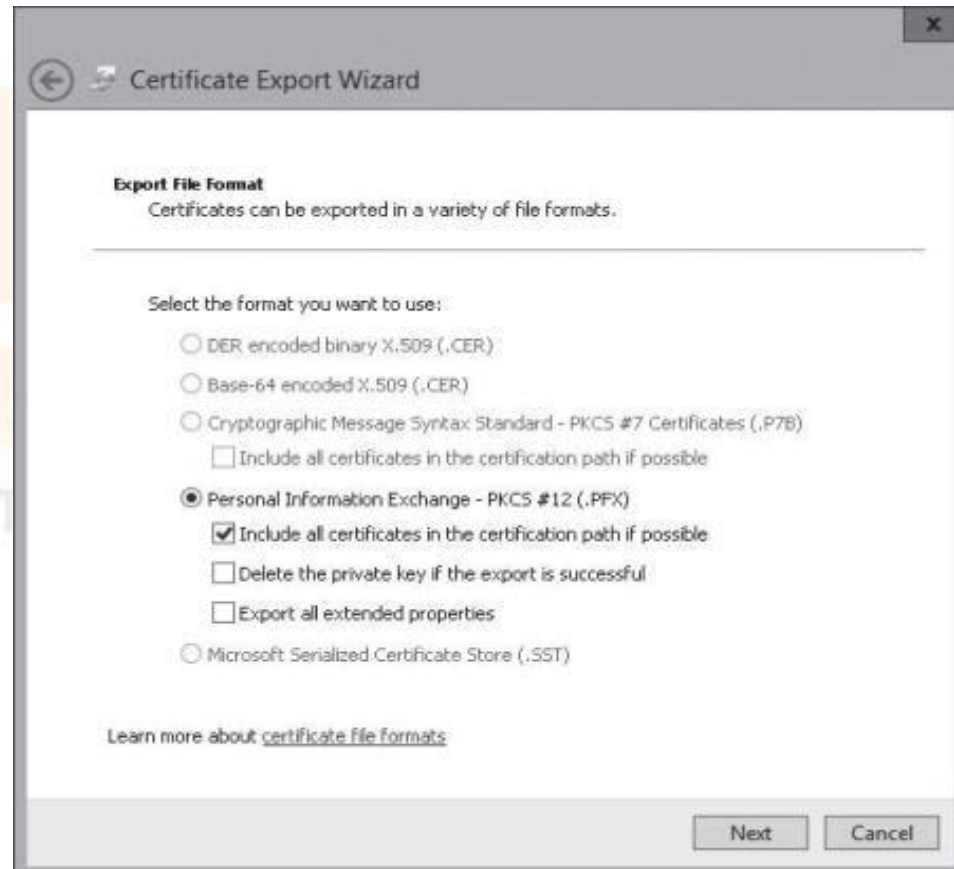
5. When the Certificate Export Wizard starts, click Next.
6. On the Export Private Key page, click Yes, export the private key, and then click Next.



Exporting the private key on the Export Private Key page

Securing Files and Disks

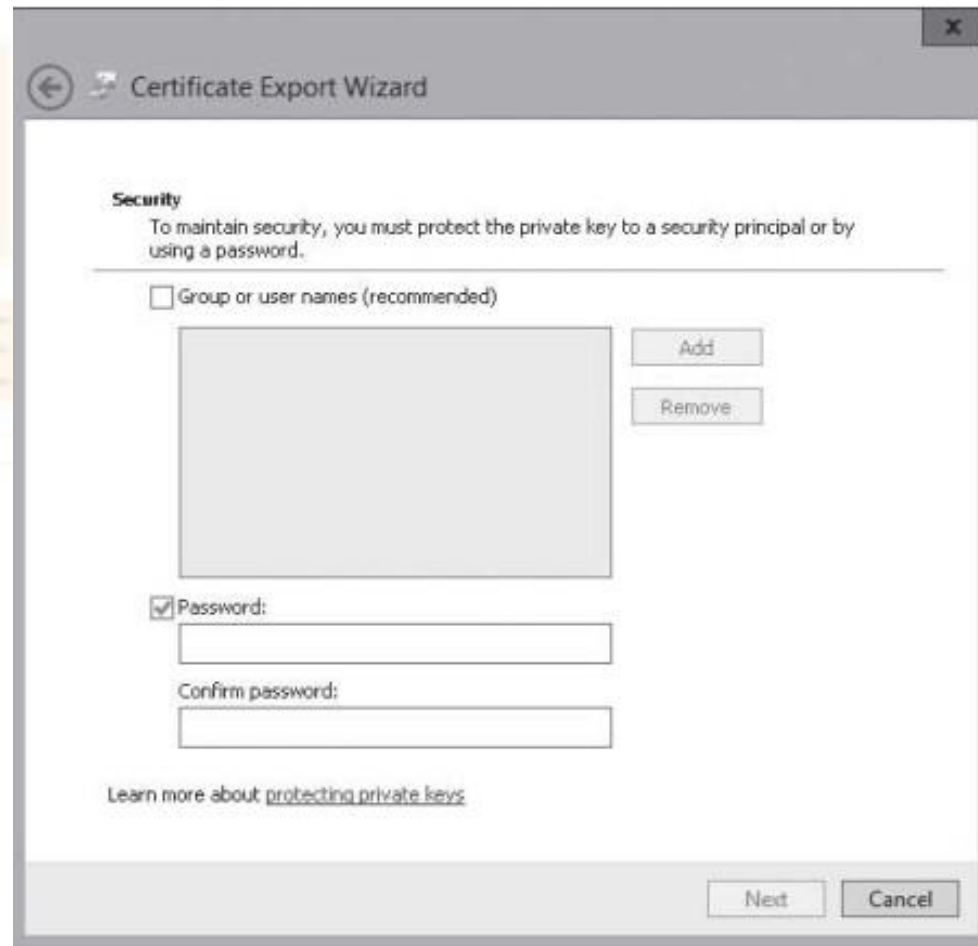
7. On the Export File Format page, click Personal Information Exchange—PKCS #12 (.PFX), and then click Next.



Selecting the Personal Information Exchange on the Export File Format page

Securing Files and Disks

8. On the Security page, select the Password checkbox, and type in the password in the Password and Confirm password text boxes. Click Next.



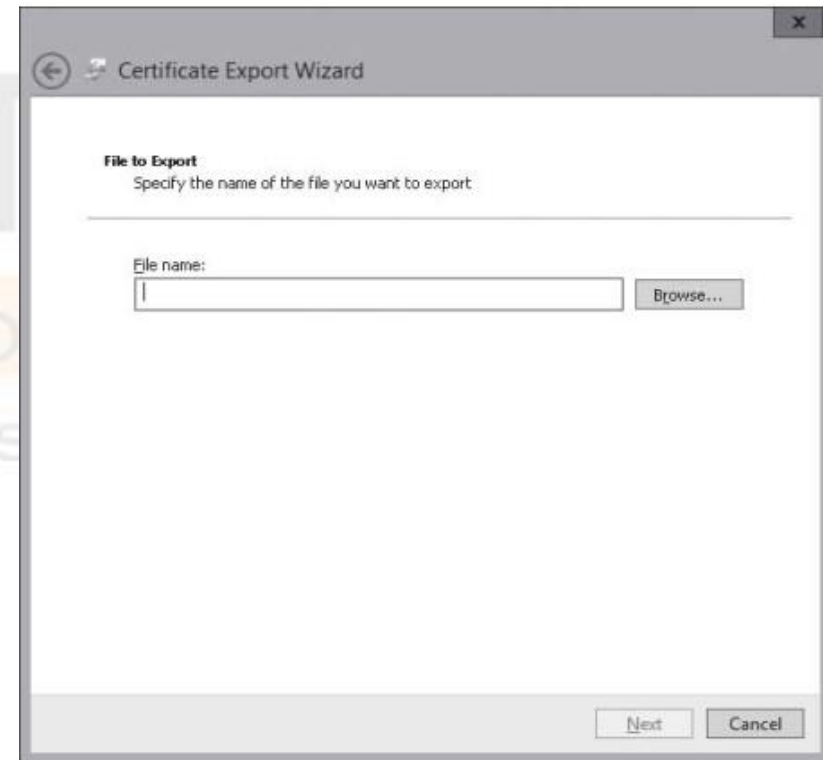
The image shows a screenshot of the 'Certificate Export Wizard' window, specifically the 'Security' page. The window has a title bar with a back arrow, a forward arrow, and the text 'Certificate Export Wizard'. The 'Security' section contains the following elements:

- A heading 'Security' followed by the text: 'To maintain security, you must protect the private key to a security principal or by using a password.'
- A checkbox labeled 'Group or user names (recommended)' which is currently unchecked.
- A large empty rectangular box for listing group or user names.
- Two buttons, 'Add' and 'Remove', positioned to the right of the box.
- A checkbox labeled 'Password:' which is checked.
- Two text input fields: one for 'Password:' and one for 'Confirm password:'.
- A link at the bottom: 'Learn more about [protecting private keys](#)'.
- At the bottom right, there are 'Next' and 'Cancel' buttons.

Selecting Password on the Security page

Securing Files and Disks

9. On the File to Export page, type a name for the file and the location (include the whole path) or click Browse, navigate to a location, type a filename, and then click Next.
10. Click Next, and then click Finish.
11. When the export is successful, click OK.



Specifying the filename (and its location) to export

Restore An EFS Certificate

To restore your EFS certificate, perform the following steps:

1. Open a command prompt.
2. Execute the certmgr.msc command. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the left pane, double-click Personal, and then click Certificates.
4. Right-click Certificates, select All Tasks, and then select Import.
5. When the Certificate Import Wizard starts, click Next.
6. On the File to Import page, specify the path and name of the certificate, and click the Next.
7. If it asks for a password, provide the password and click Next.
8. On the Certificate Store page, click Next.
9. On the Completing the Certificate Import Wizard page, click Finish.
10. When the import is successful, click OK.

How Can One Loose Access To EFS- Encrypted Data?

The system is not booting due to a component having been replaced or failed or due to operating system failure. For example, the motherboard is out of order the boot sector is damaged, system files are corrupted, some “half-baked” updates or a different unstable piece of software was installed. In this case, the hard drive can be connected to a different computer and the data can be read off it, but if it is EFS encrypted, this would not work.

The user profile was deleted. In this case, the files (and the user keys) may still be on the disk, but the system cannot see them, even if the user is recreated with the same name, a different ID will be assigned to the account, which is used in the encryption process. In this situation, access to the data encrypted using EFS will also be lost.

How Can One Lose Access To EFS- Encrypted Data? (Cont...)

- **The user is migrated to a different domain** (is authenticated through a different server). If the user encryption keys were stored on the server at the times of the migration (usually this is the case), then an unprofessional migration can result in the loss of access to the EFS encrypted data.
- **System reinstallation.** In this case, access to EFS-encrypted data would naturally be lost. If a backup copy of the entire system disk is made at the time, or at least of the user profile (“Documents and Settings”), then access could be restored with the use of special software, but only if the keys are not damaged.
- **The system administrator at the company or the user has reset the user password.** In this case, access to EFS-encrypted data would also be lost.

Advantages Of EFS

- EFS technology makes it so that files encrypted by one user cannot be opened by another user if the latter does not possess appropriate permissions. After encryption is activated, the file remains encrypted in any storage location on the disk, regardless of where it is moved. Encryption is can be used on any files, including executables.
- The user with permission to decrypt a file is able to work with the file like with any other, without experiencing any restrictions or difficulties. Meanwhile, other users receive a restricted access notification when they attempt to access the EFS encrypted file.
- This approach is definitely very convenient. The user gets the opportunity to reliably and quickly (using standard means) limit access to confidential information for other household members or colleagues who also use the computer.

Disadvantages Of EFS

- This chain of encryption, according to EFS developers, should reliably protect data, but in practice, The protection can be ultimately reduced to the good old login-password combination.
- If the password is lost or reset, it becomes impossible to gain access to the EFS-encrypted files on the drive. In fact, access can be lost irreversibly.
- If the operating system fails or is reinstalled, it becomes impossible to gain access to the EFS-encrypted files on the drive. In fact, access can be lost irreversibly.
- Regular users do not fully understand how EFS works and often pay for it when they lose their data. Microsoft has issued EFS documentation that explains how it works and the main issues that may be encountered when encrypting, but these are difficult for regular users to understand, and few read the documentation before starting to work.

Encrypting Files With Bitlocker

Unlike EFS, BitLocker allows you to encrypt the entire volume. Therefore, if a drive or laptop is stolen, the data is still encrypted even if the thief installs it in another system for which he is an administrator.

BitLocker Drive Encryption (BDE) is the feature in Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 that can use a computer's **Trusted Platform Module (TPM)**, which is a microchip that is built into a computer. It is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft. BitLocker Drive Encryption can use a TPM to validate the integrity of a computer's boot manager and boot files at start-up and to guarantee that a computer's hard disk has not been tampered with while the operating system was offline. BitLocker Drive Encryption also stores measurements of core operating system files in the TPM.

The system requirements of BitLocker are:

- Because BitLocker stores its own encryption and decryption key in a hardware device that is separate from your hard disk, you must have one of the following:
 - A computer with TPM. If your computer was manufactured with TPM version 1.2 or higher, BitLocker stores its key in the TPM.
 - A removable USB memory device, such as a USB flash drive. If your computer doesn't have TPM version 1.2 or higher, BitLocker stores its key on the flash drive.
- Have at least two partitions: a system partition (contains the files needed to start your computer and must be at least 350 MB for computers running Windows 8) and an operating system partition (contains Windows). The operating system partition is encrypted, and the system partition remains unencrypted so that your computer can start. If your computer doesn't have two partitions, BitLocker creates them for you. Both partitions must be formatted with the NTFS file system.
- Your computer must have a BIOS that is compatible with TPM and supports USB devices during computer start-up. If this is not the case, you need to update the BIOS before using BitLocker.

Securing Files and Disks

BitLocker has **five operational modes** for OS drives, which define the steps involved in the system boot process. These modes, in a descending order from the most to least secure, are as follows:

- **TPM + startup PIN + startup key:** The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a personal identification number (PIN) and insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.
- **TPM + startup key:** The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.
- **TPM + startup PIN:** The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a PIN before the system can unlock the BitLocker volume and complete the system boot sequence.

(Continued) BitLocker has five operational modes

- **Startup key only:** The BitLocker configuration process stores a startup key on a USB flash drive, which the administrator must insert each time the system boots. This mode does not require the server to have a TPM chip, but it must have a system BIOS that supports access to the USB flash drive before the operating system loads.
- **TPM only:** The system stores the BitLocker volume encryption key on the TPM chip and accesses it automatically when the chip has determined that the boot environment is unmodified. This unlocks the protected volume, and the computer continues to boot. No administrative interaction is required during the system boot sequence.

Configuring Bitlocker Encryption

Before you can use BitLocker on a server running Windows Server 2012, you must first install BitLocker using Server Manager. You can then determine whether you have TPM and turn on BitLocker.

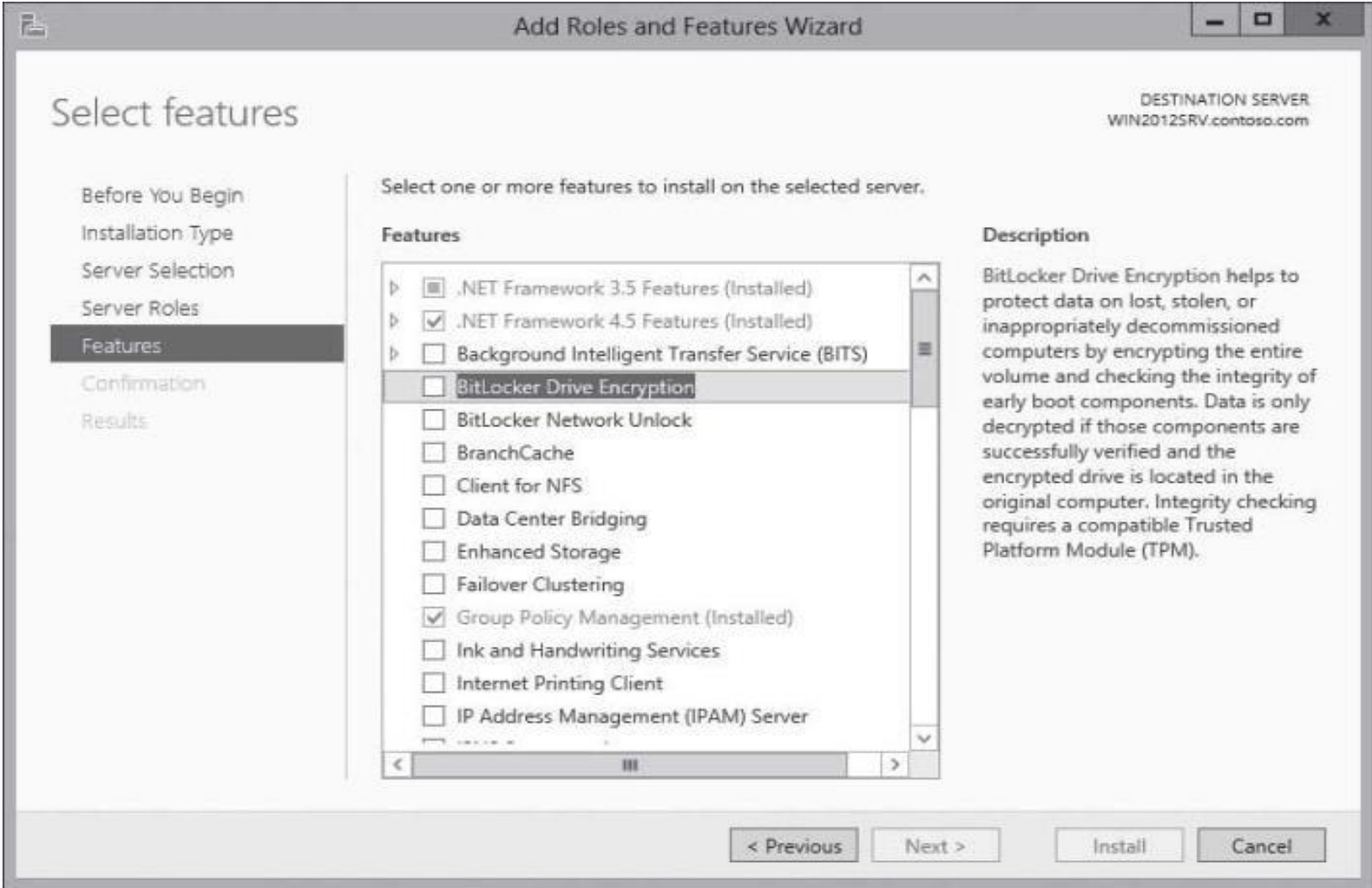


Install Bitlocker

To install BitLocker on a computer running Windows Server 2012, perform the following steps:

1. Click the Server Manager button on the task bar to open Server Manager.
2. At the top of Server Manager, select Manage and click Add Roles and Features. The Add Roles and Feature Wizard opens.
3. On the Before you begin page, click Next.
4. Select Role-based or feature-based installation and then click Next.
5. Click Select a server from the server pool, click the name of the server to install BitLocker to, and then click Next.
6. On the Select server roles page, click Next.
7. On the Select features page, select BitLocker Drive Encryption.

Securing Files and Disks



Using the Select Features page

Securing Files and Disks

8. When the Add Roles and Features Wizard dialog box appears, click Add Features.



Opening the Add Roles
and Features Wizard

Securing Files and Disks

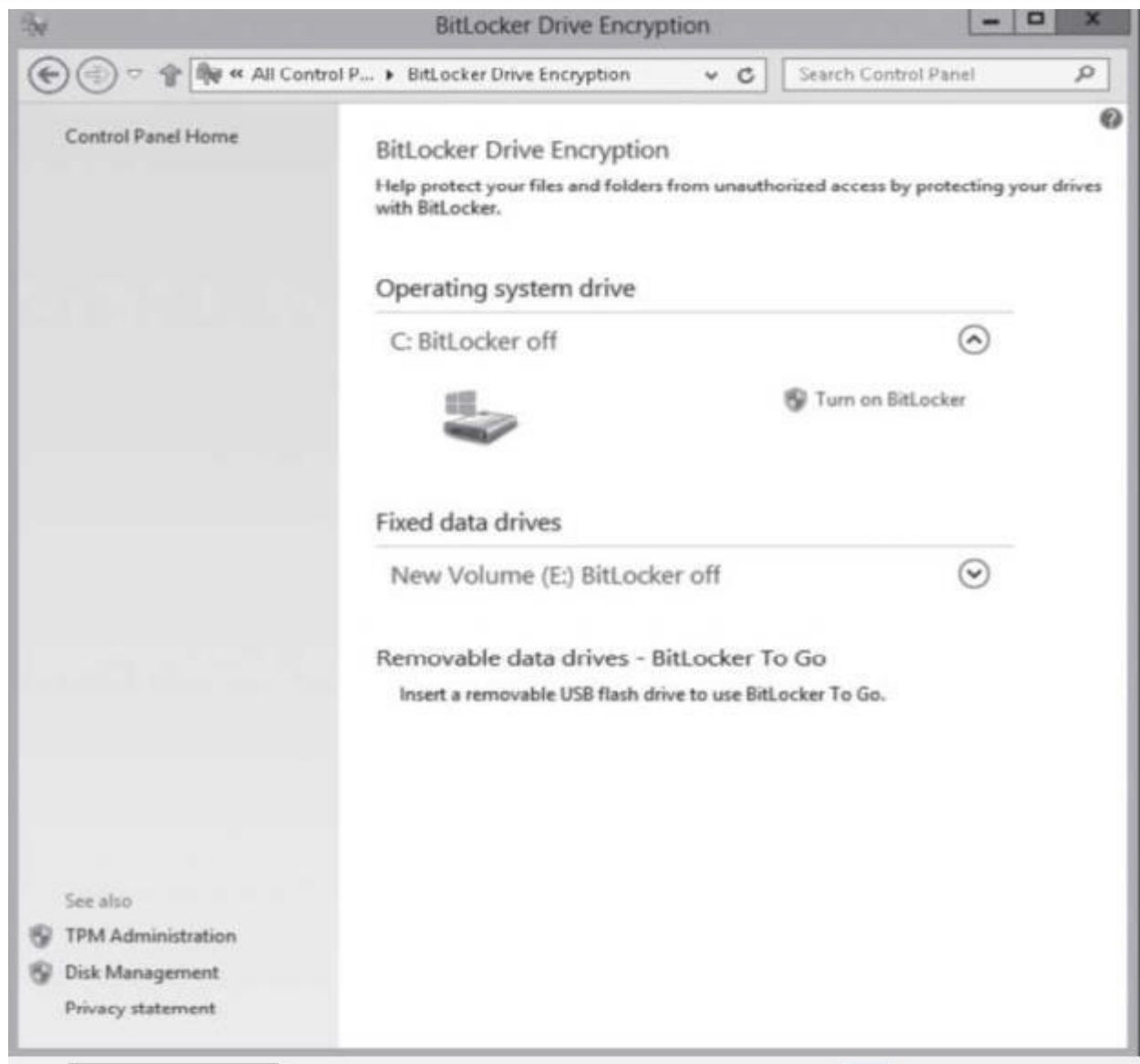
9. On the Select Features page, click Next.
10. On the Confirm installation selections page, click Install.
11. When BitLocker is installed, click Close.
12. Reboot Windows.

DETERMINE WHETHER YOU HAVE TPM

To find out whether your computer has Trusted Platform Module (TPM) security hardware, perform the following steps:

1. Open the Control Panel.
2. Click System and Security and click BitLocker Drive Encryption. The BitLocker Drive Encryption window opens.
3. In the left pane, click TPM Administration. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

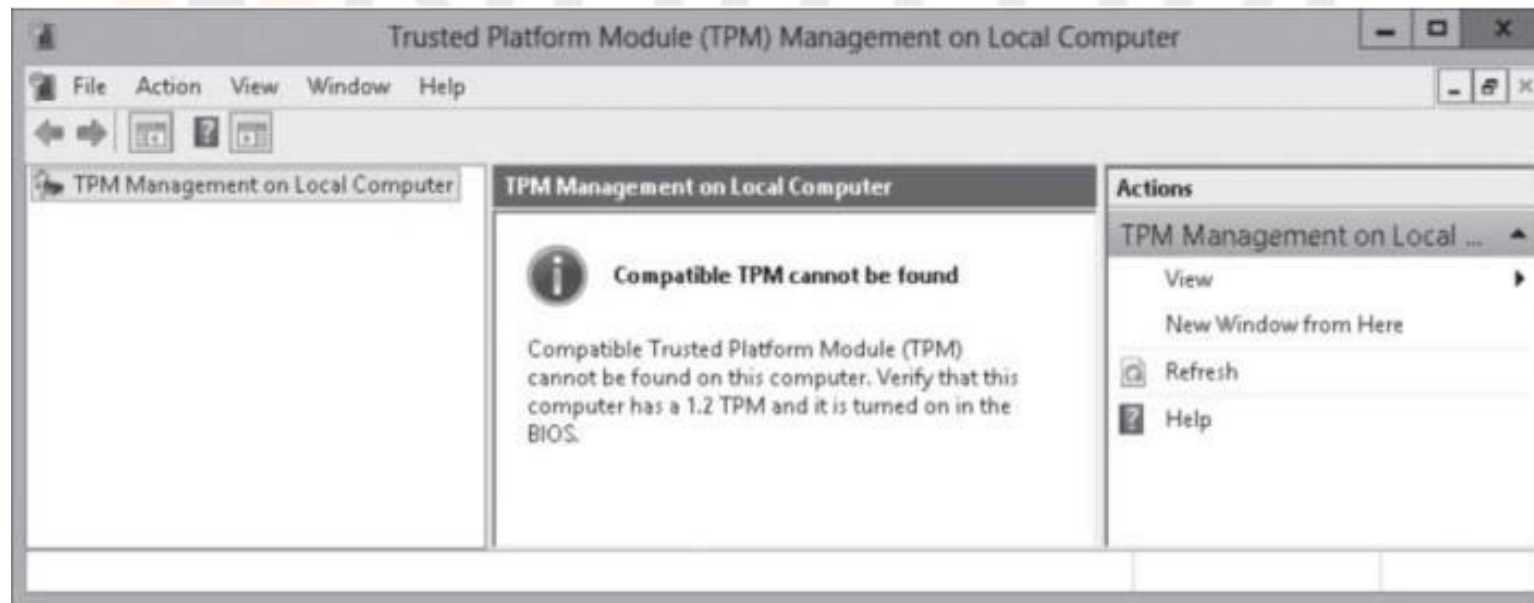
Securing Files and Disks



Displaying the BitLocker Drive Encryption window

Securing Files and Disks

The TPM Management on Local Computer snap-in tells you whether your computer has the TPM security hardware. If your computer doesn't have it, you'll need a removable USB memory device to turn on BitLocker and store the BitLocker start-up key that you need whenever you start your computer.



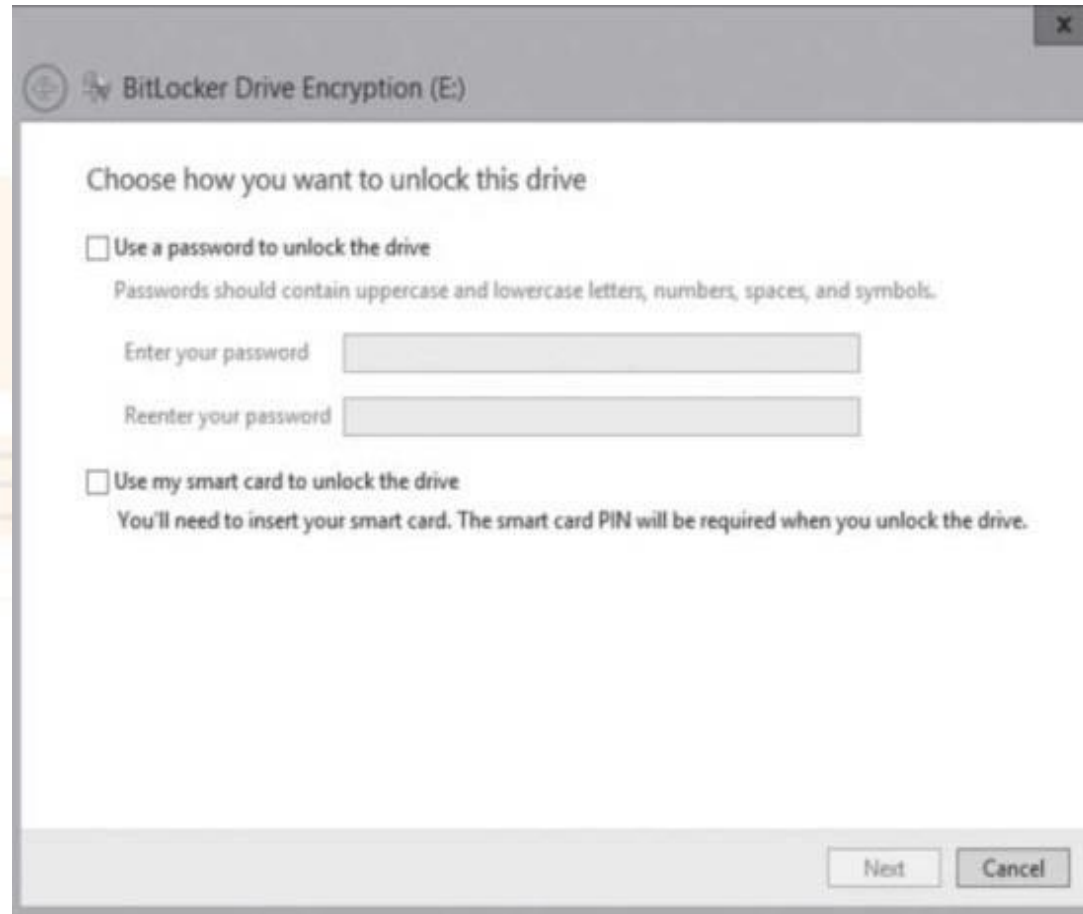
Showing that the system does not have Compatible Trusted Platform Module (TPM)

TURN ON Bit LOCKER

To turn on BitLocker on a computer running Windows Server 2012, perform the following steps:

1. Click the Start button, and then click the Control Panel.
2. Click System and Security and click BitLocker Drive Encryption. The BitLocker Drive Encryption window opens.
3. Click Turn on BitLocker for the volume that you want to encrypt. A BitLocker Drive Encryption (X:) window opens.
4. On the Choose how you want to unlock this drive page, select the Use a password to unlock the drive. Type a password in the Enter your password and Reenter your password text boxes, and then click Next.

Securing Files and Disks



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

☐ Use a password to unlock the drive
Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password

Reenter your password

☐ Use my smart card to unlock the drive
You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

Next Cancel

Using the Choose how you want to unlock this drive page

5. On the How do you want to back up your recovery key? click Save to a file option.

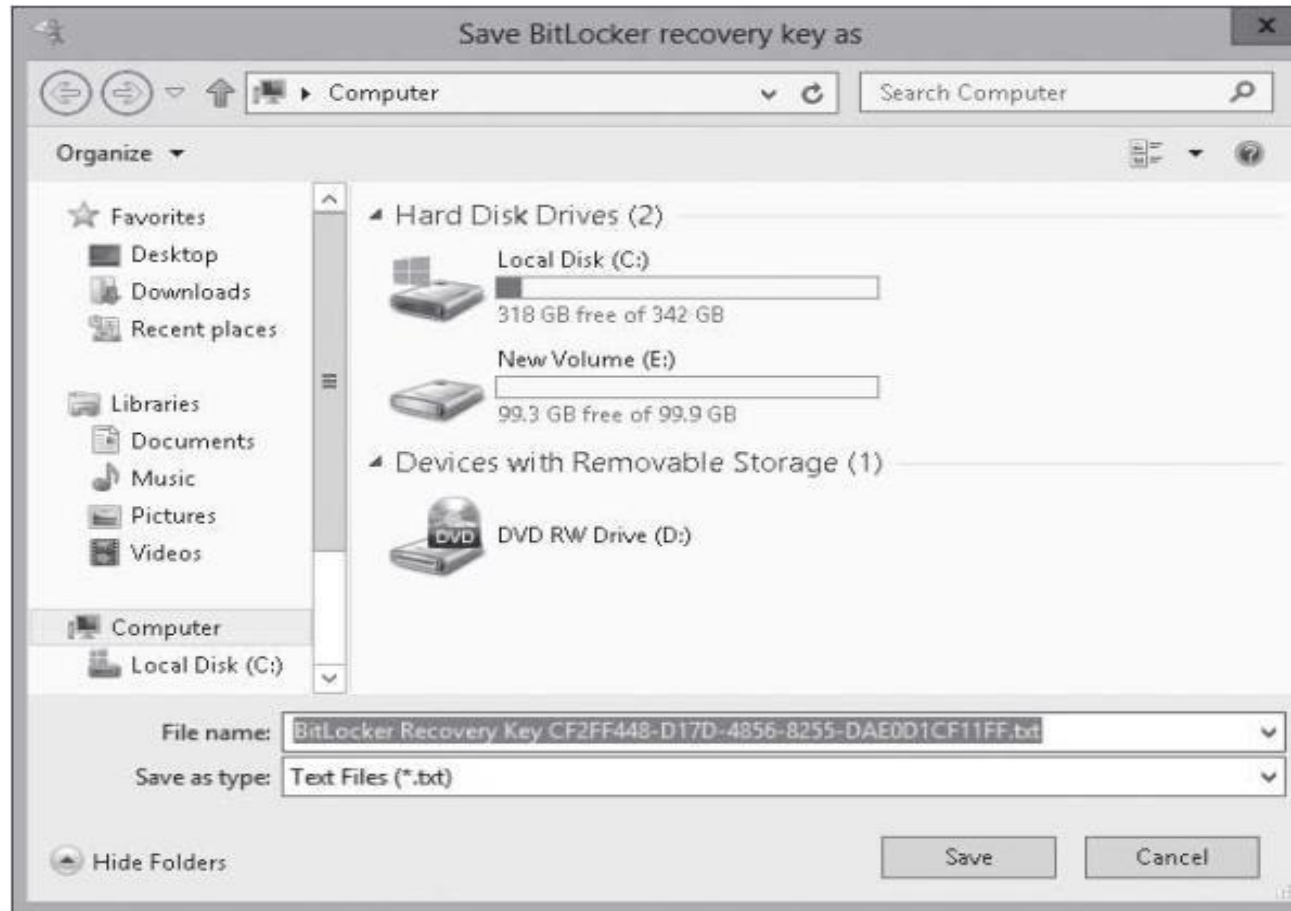
Securing Files and Disks



Using the How do you want to back up your recovery key? Page

6. When the Save BitLocker recovery key as dialog box appears, click Save.

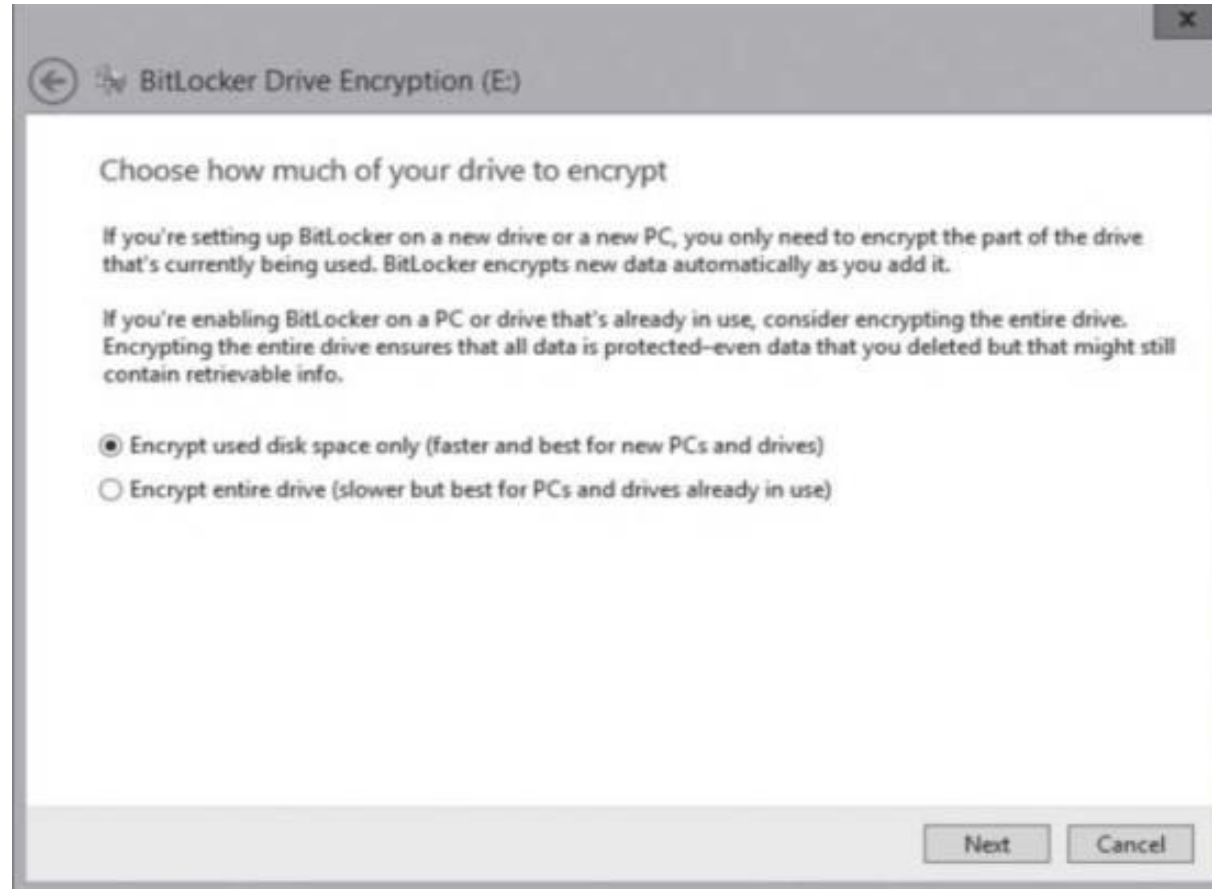
Securing Files and Disks



Using the Save BitLocker recovery key as dialog box

7. After the file is saved, make sure the key is stored in a safe place. Then click Next.
8. On the Choose how much of your drive to encrypt page, select either Encrypt used disk space only or the Encrypt entire drive option, and then click Next.

Securing Files and Disks



Using the Choose
how much of your
drive to encrypt page

9. On the Are you ready to encrypt this drive? click Start encrypting.

Securing Files and Disks



Using the Are you ready to encrypt this drive? page

10. When the drive is encrypted, click Close.

Securing Files and Disks

When the encryption process is complete, you can open the BitLocker Drive Encryption Control Panel to ensure that the volume is encrypted, or turn off BitLocker, such as when performing a BIOS upgrade or other system maintenance.

The BitLocker Control Panel applet enables you to recover the encryption key and recovery password at will. The following figure shows the following options available after you use BitLocker to encrypt a drive:

- Back up a recovery key
- Change the password
- Add smart card
- Turn off Bit Locker

You should consider carefully how to store this information because it allows access to the encrypted data. It is also possible to escrow this information into Active Directory. Standard users can change the password or PIN if they know the current PIN or password. By default, a user has five attempts to type in the current PIN or password. When this happens, the administrator has to reset the volume PIN or password, or the system needs to be rebooted. To make sure that a password or pin is not too easy to guess, you can define how complex the password is using a group policy. To define the complexity, enable and configure the Configure use of passwords for fixed data drives settings found in Computer Configuration\ Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\.

Securing Files and Disks



Showing the BitLocker applet options for a BitLocker-encrypted volume

Configuring Bitlocker To Go

BitLocker To Go is a new feature in Windows 7 and Windows Server 2008 R2 that enables users to encrypt removable USB devices, such as flash drives and external hard disks. While BitLocker has always supported the encryption of removable drives, BitLocker To Go enables you to use the encrypted device on other computers without having to perform an involved recovery process. Because the system is not using the removable drive as a boot device, a TPM chip is not required. To use BitLocker To Go, insert the removable drive and open the BitLocker Drive Encryption Control Panel. The device appears in the interface with a Turn on BitLocker link just like that of the computer's hard disk drive.

Bit LOCKER PRE-PROVISIONING

Starting with Windows 8, BitLocker supports **pre-provisioning**, which allows BitLocker to be enabled before the operating system is installed. During pre-provisioning, Windows generates a random encryption key that BitLocker uses to encrypt the volume. The random encryption key is stored on the disk, unprotected. After Windows is installed, users can fully protect the encryption key for the pre-provisioned volume by activating BitLocker on the volume and selecting the BitLocker to unlock method. To enable BitLocker pre-provisioning, you use a customised Windows Pre-installation Environment (WinPE) image and execute the following command:

Manage-bde –on x:

You need to protect the drive letter (x). After Windows is installed, the BitLocker status for the volume is BitLocker Waiting for Activation.

Configuring Bitlocker Policies

If for some reason, the user loses the startup key and/or startup PIN needed to boot a system with BitLocker, the user can supply the recovery key created during the BitLocker configuration process and regain access to the system. If the user loses the recovery key, you can use a data recovery agent designated within Active Directory to recover the data on the drive.

Similar to EFS, a data recovery agent is a user account that is an administrator who is authorized to recover BitLocker drives for an entire organization with a digital certificate on a smart card. In most cases, administrators of Active Directory Domain Services (AD DS) networks use DRAs to ensure access to their BitLocker-protected systems while avoiding maintaining a large number of individual keys and PINs.

Securing Files and Disks

It is a little bit more complicated to create a DRA for BitLocker than it is for EFS. To create a DRA for BitLocker, you must do the following:

- Add the user account you want to designate to the Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\BitLocker Drive Encryption container in a GPO or to the system's Local Security Policy.
- Configure the Provide the unique identifiers for your organization policy setting in the Computer Configuration\Policies\Administrative Templates\Windows Components\ BitLocker Drive Encryption container with unique identification fields for your BitLocker drives.
- Enable DRA recovery for each type of BitLocker resource you want to recover:
 - Choose how BitLocker-protected operating system drives can be recovered.
 - Choose how BitLocker-protected fixed drives can be recovered.
 - Choose how BitLocker-protected removable drives can be recovered

Securing Files and Disks

Provide the unique identifiers for your organization

Provide the unique identifiers for your organization

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: Windows 7 operating systems

Options:

BitLocker identification field:

Allowed BitLocker identification field:

Help:

This policy setting allows you to associate unique organizational identifiers to a new drive that is enabled with BitLocker. These identifiers are stored as the identification field and allowed identification field. The identification field allows you to associate a unique organizational identifier to BitLocker-protected drives. This identifier is automatically added to new BitLocker-protected drives and can be updated on existing BitLocker-protected drives using the manage-bde command-line tool. An identification field is required for management of certificate-based data recovery agents on BitLocker-protected drives and for potential updates to the BitLocker To Go Reader. BitLocker will only manage and update data recovery agents when the identification field on the drive matches the value configured in the identification field. In a similar manner, BitLocker will only update the BitLocker To Go Reader when the identification field on the drive matches the value configured for the identification field.

The allowed identification field is used in combination with the "Deny write access to removable drives not protected by BitLocker" policy setting to help control the use of removable

OK Cancel Apply

Configuring the Provide the unique identifiers for your organization policy setting

Securing Files and Disks

Choose how BitLocker-protected fixed drives can be recovered

Choose how BitLocker-protected fixed drives can be recovered Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: Windows 7 operating systems

Options:

☒ Allow data recovery agent

Configure user storage of BitLocker recovery information:

Allow 48-digit recovery password

Allow 256-bit recovery key

☐ Omit recovery options from the BitLocker setup wizard

☒ Save BitLocker recovery information to AD DS for fixed data drives

Configure storage of BitLocker recovery information to AD DS:

Backup recovery passwords and key packages

Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives

Help:

This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

The "Allow data recovery agent" check box is used to specify whether a data recovery agent can be used with BitLocker-protected fixed data drives. Before a data recovery agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding data recovery agents.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

Select "Omit recovery options from the BitLocker setup wizard" to prevent users from specifying recovery options when they turn on BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you turn on BitLocker, instead BitLocker recovery options for the drive are determined by the policy setting.

In "Save BitLocker recovery information to Active Directory"

Configuring how BitLocker-protected fixed drives can be recovered

Managing BitLocker Certificates

Similar to EFS, you should back up the necessary digital certificates and keys. You can use the Certificate Management console to back up any digital certificates, such as DRA certificates. It has also been mentioned earlier that you can use the Control Panel to back up the recovery key. You can configure BitLocker Drive Encryption to back up recovery information for BitLocker-protected drives and the TPM to AD DS. Recovery information includes the recovery password for each BitLocker-protected drive, the TPM owner password, and the information required to identify which computers and drives the recovery information applies to. To store information in Active Directory, you can enable the Store BitLocker Recovery Information in AD DS.

Securing Files and Disks

Store BitLocker recovery information in Active Directory Domain Services (Windows ...

Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)

Previous Setting Next Setting

☒ Not Configured Comment:

☐ Enabled

☐ Disabled

Supported on: Windows Server 2008 and Windows Vista

Options:

☐ Require BitLocker backup to AD DS

If selected, cannot turn on BitLocker if backup fails (recommended default).

If not selected, can turn on BitLocker even if backup fails. Backup is not automatically retried.

Select BitLocker recovery information to store:

A recovery password is a 48-digit number that unlocks access to a BitLocker-protected drive.

A key package contains a drive's BitLocker encryption key secured by one or more recovery passwords.

Help:

This policy setting allows you to manage the Active Directory Domain Services (AD DS) backup of BitLocker Drive Encryption recovery information. This provides an administrative method of recovering data encrypted by BitLocker to prevent data loss due to lack of key information. This policy setting is only applicable to computers running Windows Server 2008 or Windows Vista.

If you enable this policy setting, BitLocker recovery information is automatically and silently backed up to AD DS when BitLocker is turned on for a computer. This policy setting is applied when you turn on BitLocker.

Note: You might need to set up appropriate schema extensions and access control settings on the domain before AD DS backup can succeed. More information about setting up AD DS backup for BitLocker is available on Microsoft TechNet.

BitLocker recovery information includes the recovery password and some unique identifier data. You can also include a package

OK Cancel Apply

Enabling Store BitLocker
Recovery Information in AD
DS

Bitlocker And Encrypting File System (EFS)

There are several differences between BitLocker Drive Encryption and the Encrypting File System.

BitLocker is designed to help protect all of the personal and systems files on the drive Windows is installed on if your computer is stolen, or if unauthorised users try to access the computer. EFS is used to help protect individual files on any drive on a per-user basis.

NURTURE
Education Solutions
TOMORROW'S HERE

BitLocker vs. Encrypting File System (EFS)

- BitLocker encrypts all personal and system files on the drive where Windows is installed, or on data drives on the same computer. EFS encrypts individual files on any drive.
- BitLocker does not depend on the individual user accounts associated with files. BitLocker is either on or off, for all users or groups. EFS encrypts files based on the user account associated with it. If a computer has multiple users or groups, each can encrypt their own files independently.
- BitLocker uses the Trusted Platform Module (TPM), a special microchip in some newer computers that supports advanced security features. EFS does not require or use any special hardware.
- You must be an administrator to turn BitLocker encryption on or off once it's enabled. You do not have to be an administrator to use EFS.
- You can use BitLocker Drive Encryption and the Encrypting File System together to get the protection offered by both features. When using EFS, encryption keys are stored with the computer's operating system. While these are encrypted, that level of security could potentially be compromised if a hacker is able to boot or access the system drive. Using BitLocker to encrypt the system drive can help protect these keys by preventing the system drive from booting or being accessed if it is installed into another computer.

Self Assessment Question

1. Which encryption technology would you use to protect individual files on a computer running Windows Server 2012?

- a. EFS
- b. BitLocker
- c. IPsec
- d. SSL

Answer: EFS

Self Assessment Question

2. When using EFS, which of the following the encryption key is stored?

- a. Text file
- b. Passkey
- c. Digital certificate
- d. Token

Answer: Digital certificate

Self Assessment Question

3. What happens when you move an EFS-encrypted file to a FAT32 volume?
- a. It remains encrypted.
 - b. It is re-encrypted.
 - c. It is decrypted.
 - d. You have the option to decrypt or encrypt.

Answer: It is decrypted.

Self Assessment Question

4. Which encryption algorithm uses a single key to encrypt and decrypt data?

- a. Symmetric
- b. Asymmetric
- c. Hash function
- d. Anti-metric

Answer: Symmetric

Self Assessment Question

5. How do you define the DRAs?

- a. Registry
- b. Active Directory Users and Computers
- c. GPOs
- d. Active Directory Sites and Services

Answer: GPOs

Self Assessment Question

6. How do you decrypt an EFS-encrypted file for a person who has left an organisation?
- a. Create the master certificate to encrypt the certificate, and then decrypt the certificate.
 - b. Use a USB with the username and username password in a text file.
 - c. Remove the computer with the files from the domain.
 - d. Use a DRA.

Answer: Use a DRA.

Self Assessment Question

7. If you do not have a TPM on your computer, which key can be used to store while using BitLocker?
- a. A text file on a CD or DVD
 - b. A second hard drive
 - c. The BIOS Setup programme
 - d. USB memory device

Answer: USB memory device

Self Assessment Question

8. Which Windows technology is used to encrypt a USB disk device?

- a. BitLocker
- b. BitLocker To Go
- c. EFS
- d. SSL

Answer: BitLocker To Go

Self Assessment Question

9. Which command do you use to encrypt a folder with EFS?
- a. Use the EFS command.
 - b. Use the cypher command.
 - c. Use the Encrypt command
 - d. Use the EFSTConfig command

Answer: Use the cypher command.

Self Assessment Question

10. How do you configure Windows to automatically encrypt a users Documents folder?

- a. Use the Control Panel.
- b. Use the cypher command.
- c. Use group policies.
- d. Use the Security tab in Windows Explorer.

Answer: Use group policies.

Self Assessment Question

11. “You are the administrator for a large communications company. Company uses Windows Server 2012 R2, and users files are encrypted using EFS”. Which command-line command would you use to change or modify the EFS files?

- a. Convert
- b. Cypher
- c. Gopher
- d. Encrypt

Answer: Cypher

Self Assessment Question

12. Cathy is the payroll manager at your company. The day before the payroll is processed, Cathy is involved in a minor car accident and spends two days in the hospital. She has Windows 7 installed as a part of a workgroup and has encrypted the payroll files with EFS. All of the EFS settings for the computer are set to default values. How can these files be accessed in her absence?
- a. The Administrator user account can access the files by backing up the files, restoring the files on the computer where the recovery agent is located, and disabling the files' Encrypt The Contents To Secure Data option.
 - b. The Administrator user account can access the files by using the unencrypt command-line utility.
 - c. The Administrator user account can access the files by using the encrypted command.
 - d. Unless a DRA has been configured, there will be no access to the files.

Answer: Unless a DRA has been configured, there will be no access to the files.

Self Assessment Question

13. You have a 10MB image file that you want to email to another user in the Marketing department. Which of the following should you do in order to email the image?

- a. Encrypt the image with EFS.
- b. Configure compression on the directory in which the image file is stored.
- c. Compressed (Zipped) folder.-Right-click the image file and select Send To
- d. Use the Compact command-line utility.

Answer: Compressed (Zipped) folder.-Right-click the image file and select Send To

Self Assessment Question

14. You are the Human Resources administrator for your company and have recently been assigned a Windows 7 laptop computer. You have added a new directory named HR to the computer and want to ensure that all files that are stored within the HR directory are encrypted. You will use the cypher utility to accomplish this. Which of the following options should you use with the cypher utility?

- a. /D
- b. /E
- c. /R
- d. /X

Answer: /E

Self Assessment Question

15. Identify the steps, in order, to encrypt a file using EFS. Not all of the steps will be used.

- a. _____ Open the File menu and select Encryption.
- b. _____ Click OK.
- c. _____ Right-click the files and click Properties.
- d. _____ Select Encrypts contents to secure data.
- e. _____ Select Encrypt using EFS.
- f. _____ Click the Advanced tab.
- g. _____ Click the Protect tab.

Answer: c->f->d->b

Self Assessment Question

16. Identify the steps, in order, to back up the EFS certificates. Not all of the steps will be used.

- a. _____ Expand Personal and click Certificates.
- b. _____ Expand Certificates, and expand EFS.
- c. _____ Open certmgr.msc.
- d. _____ Right-click the EFS certificate and click Export.
- e. _____ Right-click the EFS certificate and click Backup.
- f. _____ Specify the cer format.
- g. _____ Specify the pfx format.
- h. _____ Select to export the private key.
- i. _____ Specify the location.
- j. _____ Specify the password.

Answer: c->a->d->h->g->j->i

Self Assessment Question

17. Identify the steps, in order, to protect a drive with BitLocker. Not all of the steps will be used.

- a. _____ Save recovery key to USB device.
- b. _____ Click System and Security.
- c. _____ Click Turn on BitLocker.
- d. _____ Click Encryption.
- e. _____ Specify a password.
- f. _____ Open Control Panel.
- g. _____ Encrypt the drive.
- h. _____ Test the drive.
- i. _____ Click BitLocker Drive Encryption.

Answer: f->b->i->c->e->a->g

Summary

- Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk. Decryption is the process of converting data from encrypted format back to its original format.
- Encrypting File System (EFS) can encrypt files on an NTFS volume that cannot be used unless the user has access to the keys required to decrypt the information.
- To encrypt or decrypt a folder or file, you enable or disable the encryption attribute just as you set any other attribute, such as read-only, compressed, or hidden.
- The cipher.exe command displays or alters the encryption of folders and files on NTFS volumes.
- In later versions of NTFS, if you need to share an EFS-protected file with other users, you need to add the user's encryption certificate to the file.
- To help you manage the use of EFS, you can use group policies and to meet your organization's security needs.
- If for some reason, a person leaves the company or a person loses the original key, so that the encrypted files cannot be read, you can set up a data recovery agent (DRA) to recover EFS-encrypted files for a domain.
- BitLocker Drive Encryption (BDE) is the feature in Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 that uses a computer's TPM.
- A Trusted Platform Module (TPM) is a microchip that is built into a computer. It is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft.
- Network Unlock provides an automatic unlock of operating system volumes at system reboot when connected to a trusted wired corporate network.

Assignments

1. You have just purchased 75 new laptops that will be given to the sales team and 50 new laptops that will be given to the engineering team. Last year, a person from the marketing department left her computer, which had details about upcoming products, at the hotel. This information was leaked to the Internet. What can you do to make sure that if this happens again, the information is still safe?
2. You have a user who encrypts many of his data files with EFS. So his manager tries to open the files but cannot read the files because the user does not have the correct key. What can you do to unlock these files?
3. Why is encryption available in the NTFS file system and not in the FAT32 file system?
4. Explain the difference between EFS and BitLocker Encryption System.

Assignments

5. Microsoft's Encryption File System (EFS) is a cryptography system for windows Operating system that uses the Windows NTFS file system. Explain how to turn on and use EFS
6. Discuss how BitLocker and BitLocker To Go protect data.
7. What are the BitLocker hardware and software requirements?
8. Why are two partitions required? Why does the system partition have to be so large?
9. What versions of Windows Vista include BitLocker? Can I use BitLocker on a Windows XP–based computer?
10. What is the difference between disabling and decrypting when I turn off BitLocker?

Securing Files and Disks

Document Links

Topics	URL	Notes
EFS	https://www.elcomsoft.com/WP/advantages_and_disadvantages_of_efs_and_effective_recovery_of_encrypted_data_en.pdf	This link explains the EFS, advantages and disadvantages of EFS, EFS Recovery Agent
EFS Concept	https://en.wikipedia.org/wiki/Encrypting_File_System	This link explains the EFS, Operations of EFS
EFS Concept	https://www.techopedia.com/definition/3356/encrypting-file-system-efs	This link explains the features of EFS

Securing Files and Disks

Document Links

Topics	URL	Notes
FSRM	https://docs.microsoft.com/en-us/windows-server/storage/fsrm/fsrm-overview	This link explains about FSRM, features and application of File server resource manager
Bit Locker	https://en.wikipedia.org/wiki/BitLocker	This link explains about Bit Locker, history and operations of Bit Locker
Bit Locker Concept	https://study.com/academy/lesson/what-is-bitlocker-drive-encryption.html	This link explains the Encryption using Bit Locker

Securing Files and Disks

Video Links

Topics	URL	Notes
EFS	https://www.youtube.com/watch?v=2jipY0RmgX8	This video explains the Enabling EFS In an Organisation
EFS Concept	https://www.youtube.com/watch?v=rnuCitzSgQ8	This video explains the operations of EFS
EFS Concept	https://www.youtube.com/watch?v=laRDf7QuHyk	This video explains the procedure for Encryption
Bit Locker Concept	https://www.youtube.com/watch?v=SvVWJV4BQtk	This video explain how to encrypt drive using Bit Locker

Securing Files and Disks

E-Book Links

URL
1. <u>http://stealthgerbil.com/files/pdf/MCSA%20Windows%20Server%202012%20Complete%20Study%20Guide%20-%20Exams%2070-410,%2070-411,%2070-412,%20and%2070-417.pdf</u>
2. <u>https://www.tutorialspoint.com/windows_server_2012/windows_server_2012_tutorial.pdf</u>
3. <u>http://download.microsoft.com/download/0/C/B/0CB33133-C6F7-48A6-B7CC-D927988FCB32/Microsoft_Press_ebook_Introducing_Windows_Server_2012_PDF.pdf</u>