Lesson 6: Configuring File Services and Disk Encryption

MOAC 70-411: Administering Windows Server 2012

Microsoft
Official Academic Course

WILEY

Overview

- Exam Objective 2.3: Configure File and Disk Encryption
- Securing Files

Securing Files

Lesson 6: Configuring File Services and Disk Encryption

Encryption Algorithms

Symmetric: Uses a single key to encrypt and decrypt data. You need to initially send or provide the secret key to both the sender and the receiver.

Asymmetric: Also known as public-key cryptography, uses two mathematically related keys. One key encrypts data and the second key decrypts the data.

Hash function: Is meant as one-way encryption. After the data has been encrypted, it cannot be decrypted.

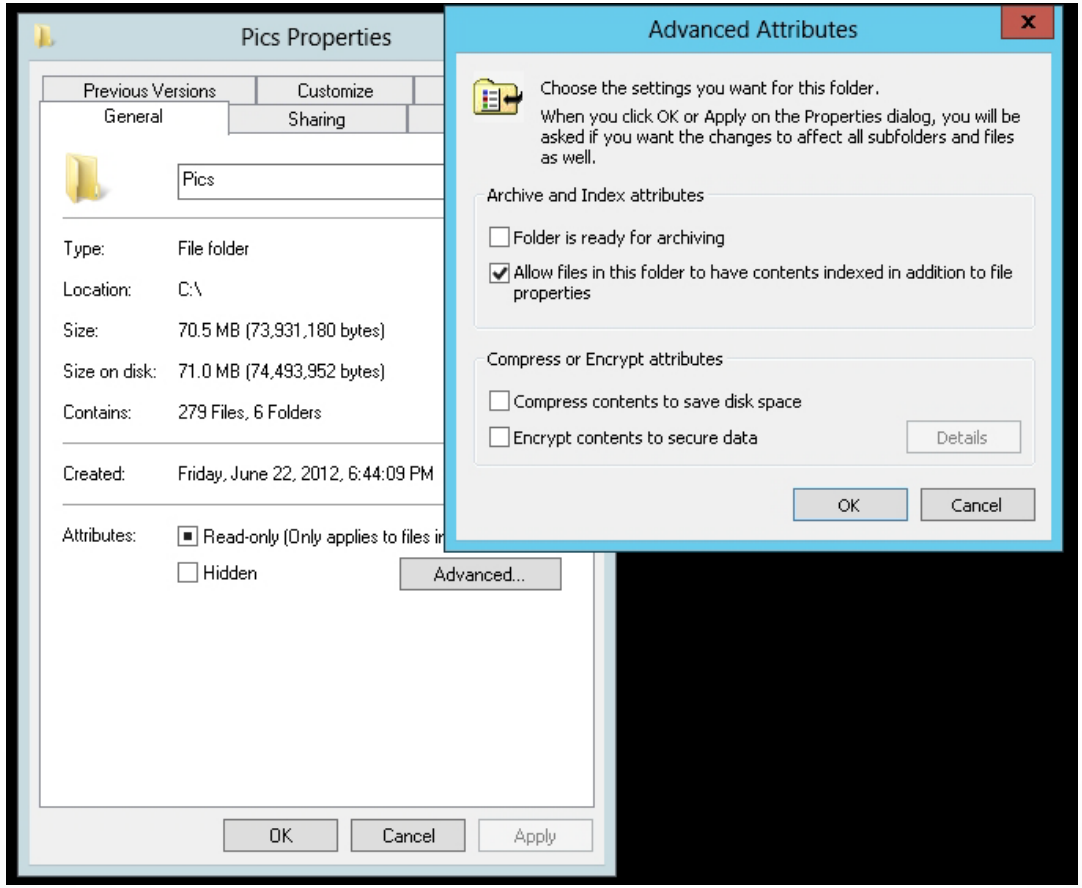
Encrypting Files with EFS

- 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.
- After a file has been encrypted, you do not have to manually decrypt an encrypted file before you can use it.
- EFS uses an encryption key to encrypt your data, which is stored in a digital certificate.

Configuring EFS

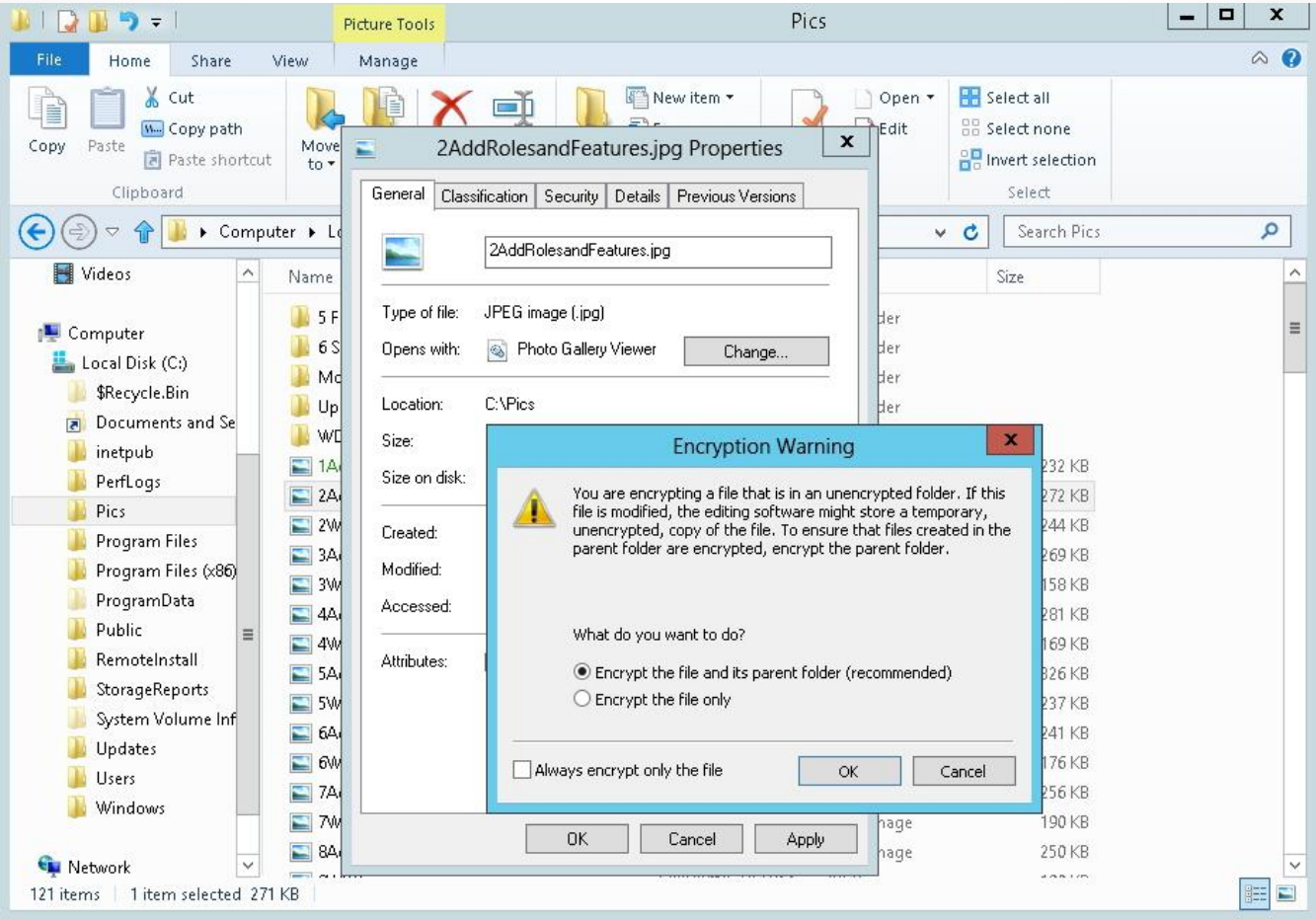
- To encrypt or decrypt a folder or file, enable or disable the encryption attribute.
- If you encrypt a folder, all files and subfolders created in the encrypted folder are automatically encrypted.
- Microsoft recommends that you encrypt at the folder level.
- You can encrypt or decrypt a file or folder using the `cipher` command.

Encrypt a Folder or File Using EFS



Displaying the Advanced Attributes dialog box

Encrypt a Folder or File Using EFS



Encrypting a file in an unencrypted folder

EFS Highlights

- 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.

EFS Highlights

- Files marked with the System attribute or that are in the root directory cannot be encrypted.
- 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 Cipher Command

- The `cipher.exe` command displays or alters the encryption of folders and files on NTFS volumes.
- Command options:
  - `/C`: Displays information on the encrypted file.
  - `/D`: Decrypts the specified files or directories.
  - `/E`: Encrypts the specified files or directories.
  - `/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.

Using the Cipher Command

- Command options (continued):
  - `/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`.

Using the Cipher Command

- Command options (continued):
  - `/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.

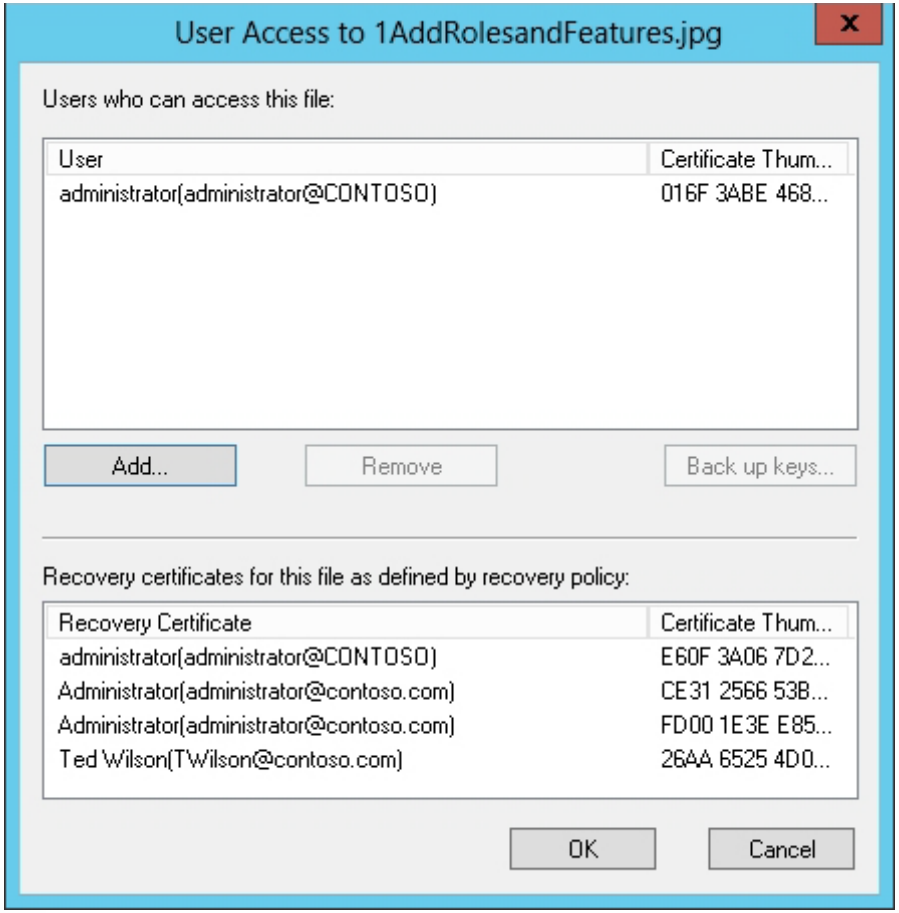
Using the Cipher Command

- Command options (continued):
  - `/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.

Sharing Files Protected with EFS with Others

- When EFS was originally created, an EFS file could be accessed only by 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.

Share a File Protected with EFS with Others



Opening the User Access dialog box

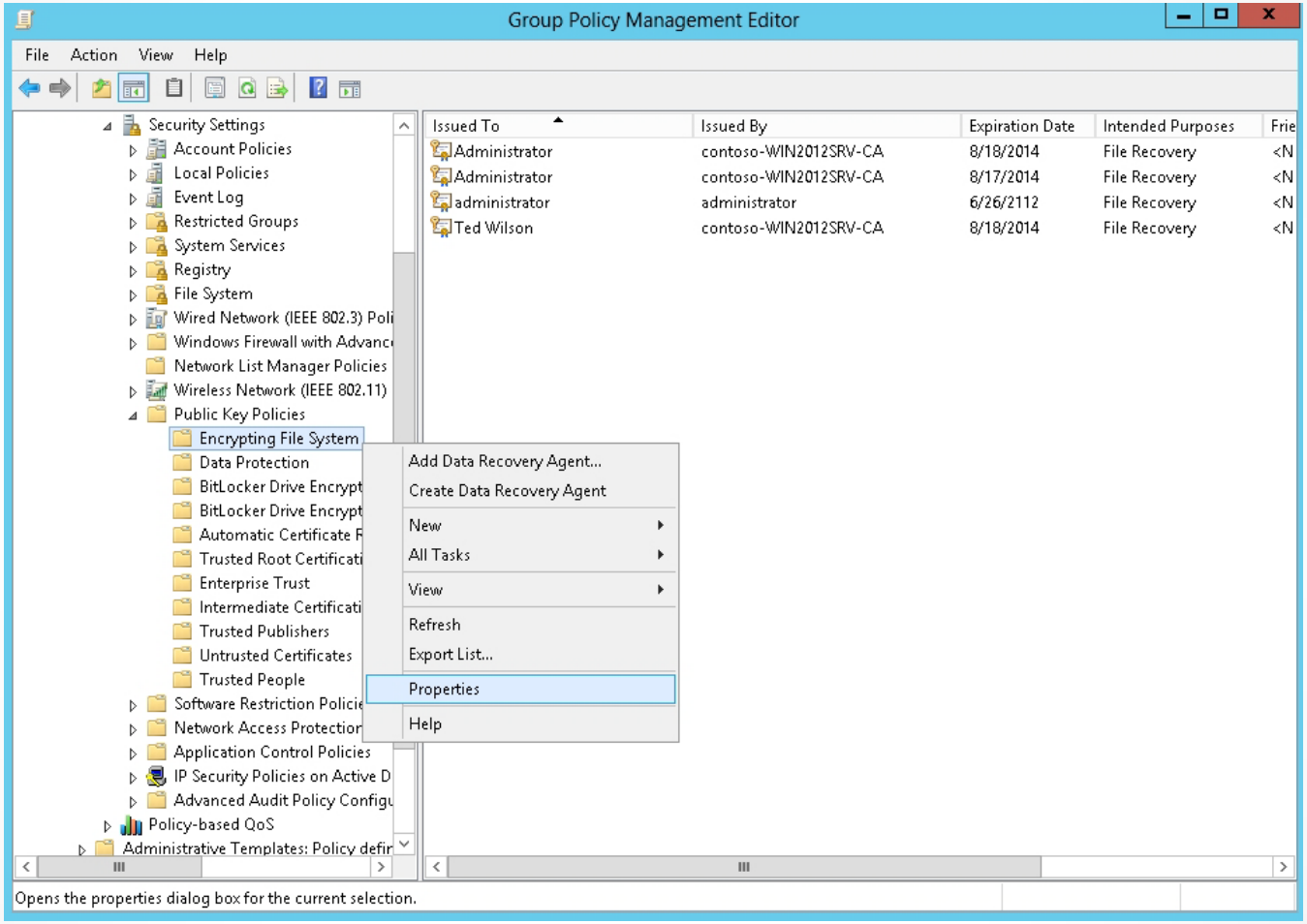
Share a File Protected with EFS with Others

Opening the Encrypting File System dialog box

Configuring EFS with Group Policies

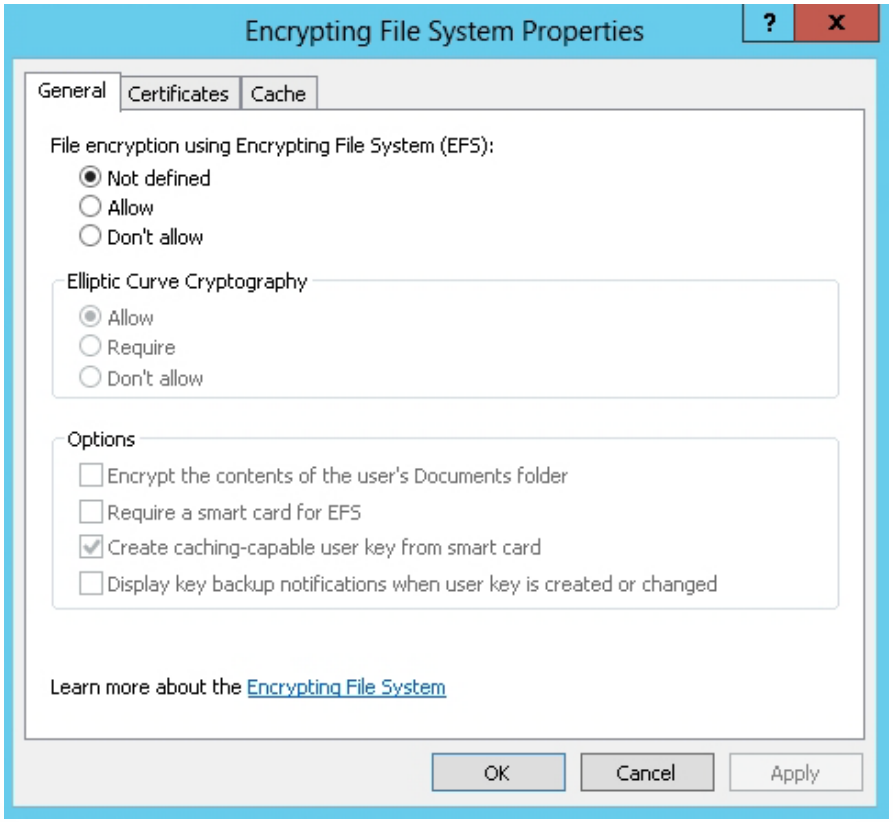
- You can use group policies to manage the use of EFS.
- To establish an EFS policy, right-click *Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Encrypting File System* and select *Properties*.

Configuring EFS with Group Policies



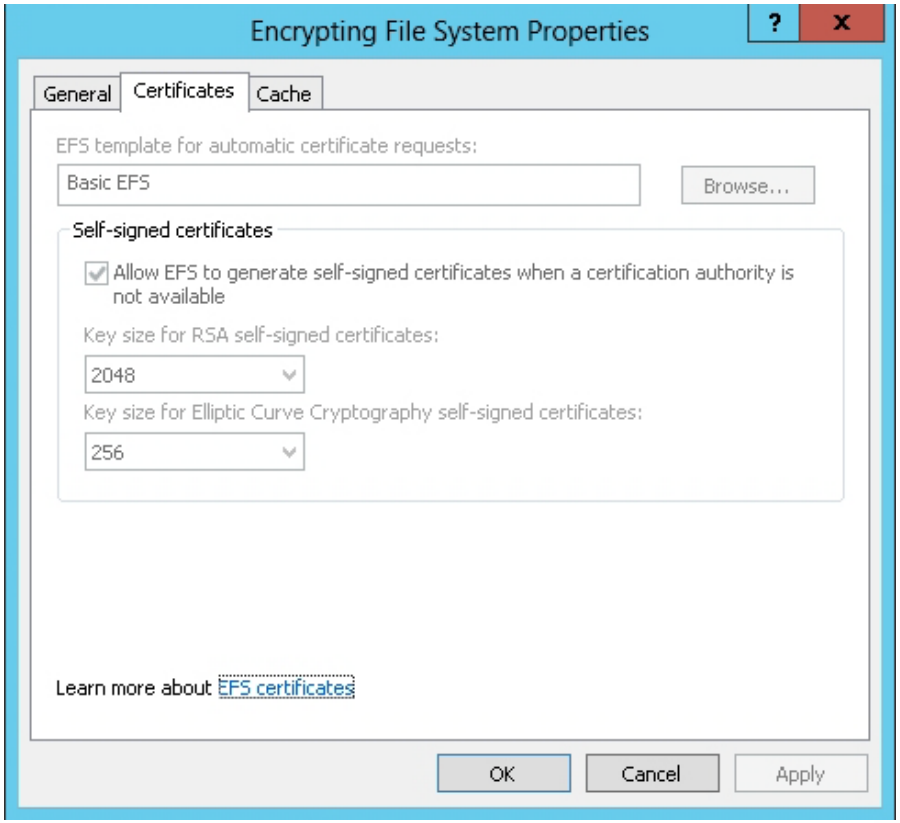
Selecting Encrypting File System properties

Configuring EFS with Group Policies



Using the Encrypting File System Properties General tab

Configuring EFS with Group Policies

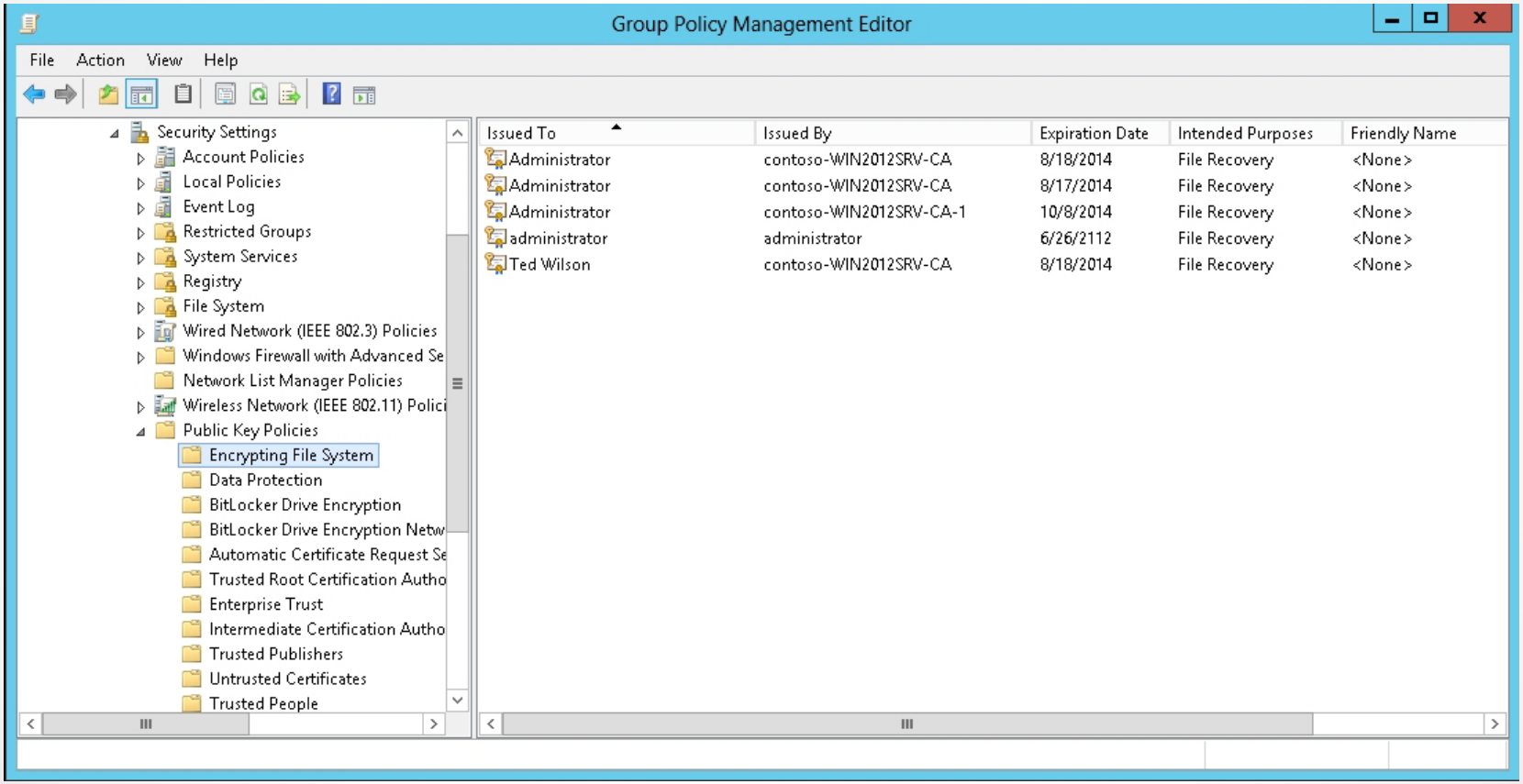


Using the Encrypting File System Properties Certificates tab

Configuring the EFS Recovery Agent

- A ***data recovery agent (DRA)*** 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 organization.
  - An enterprise CA is required.

Add Recovery Agents for EFS

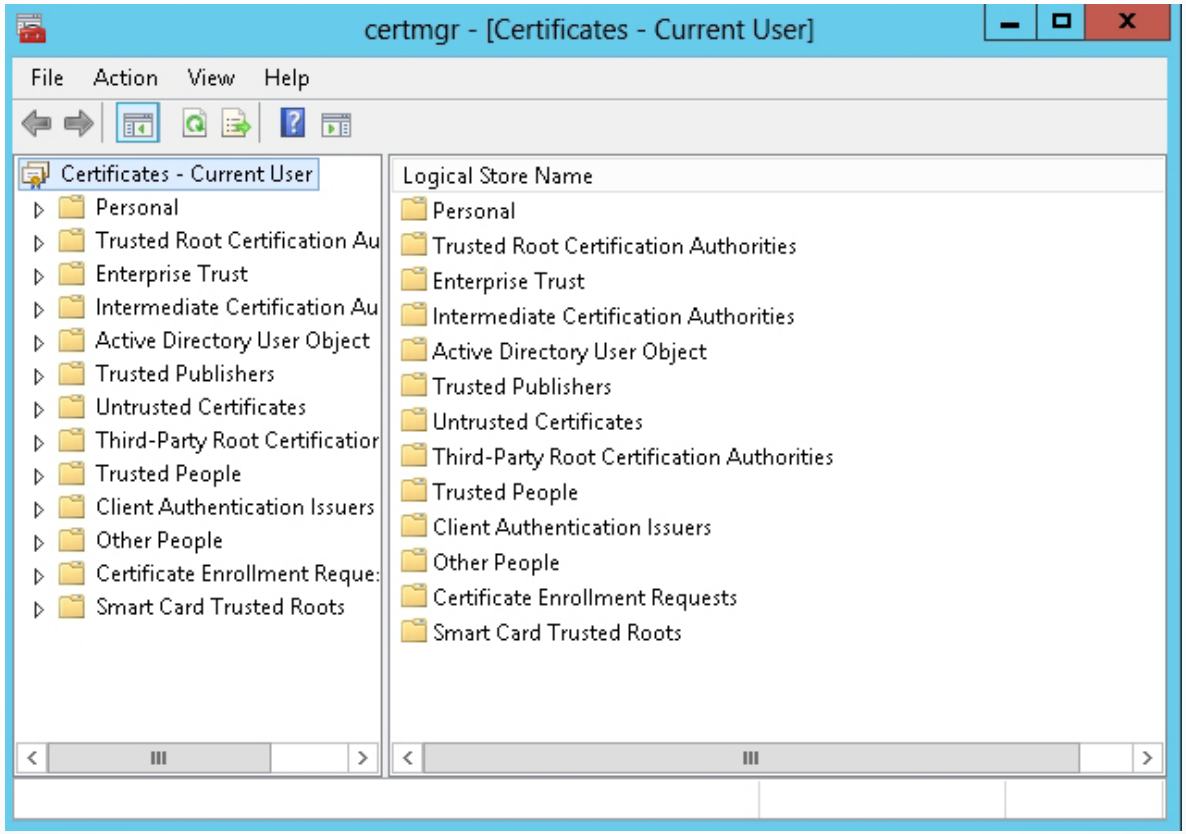


Viewing the Encrypting File System certificates

Managing EFS Certificates

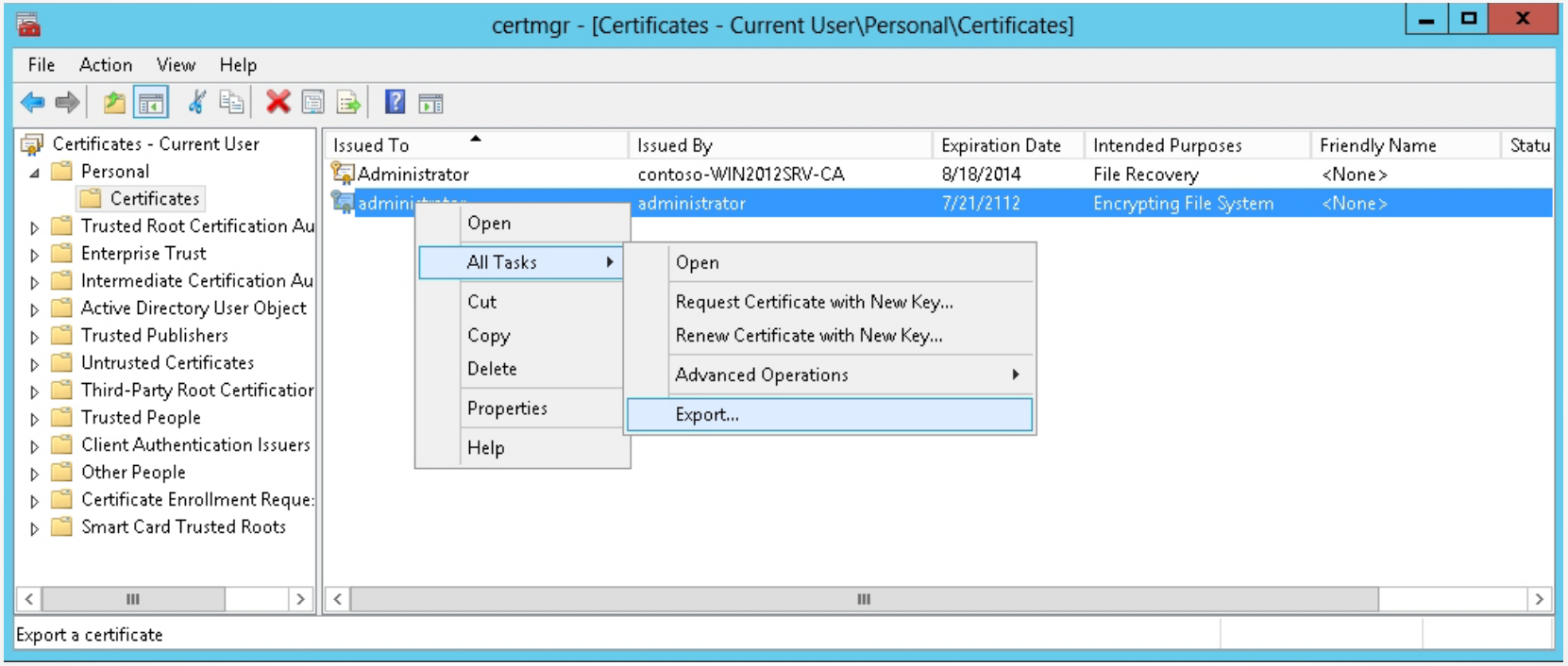
- The first time you encrypt a folder or file, an encryption certificate is automatically created.
- Back up your encryption certificate!
- If your certificate and key are lost or damaged and you don't have a backup, you won't be able to use the files that you have encrypted.

Back Up an EFS Certificate



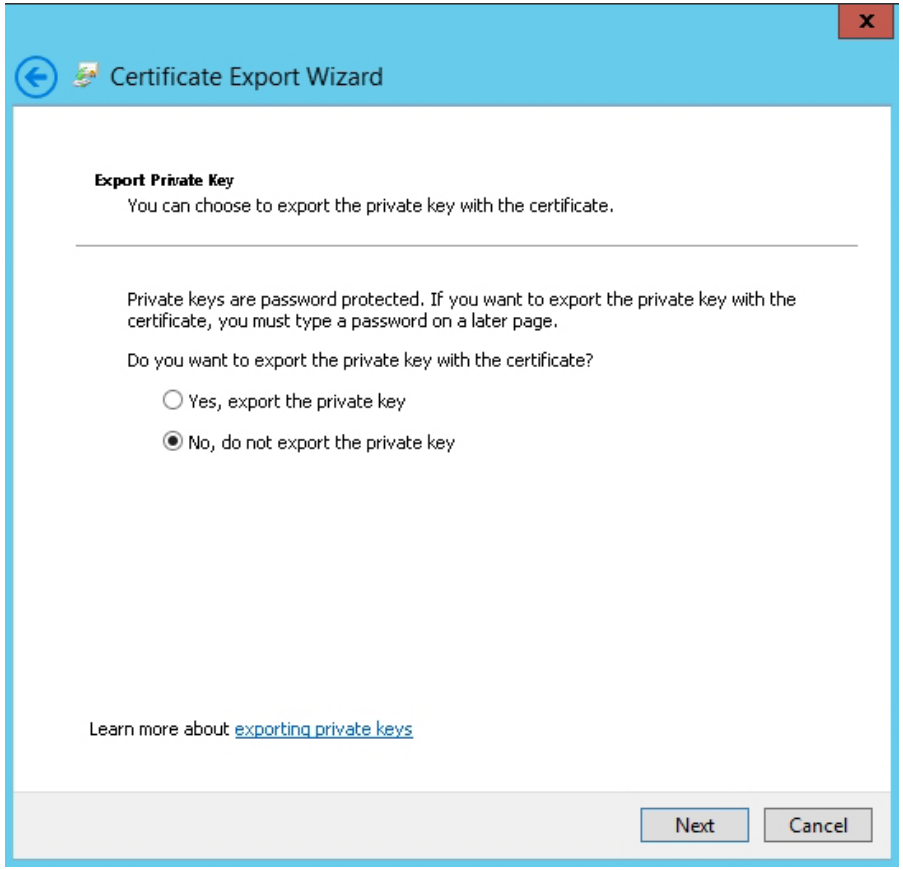
Opening the certmgr console

Back Up an EFS Certificate



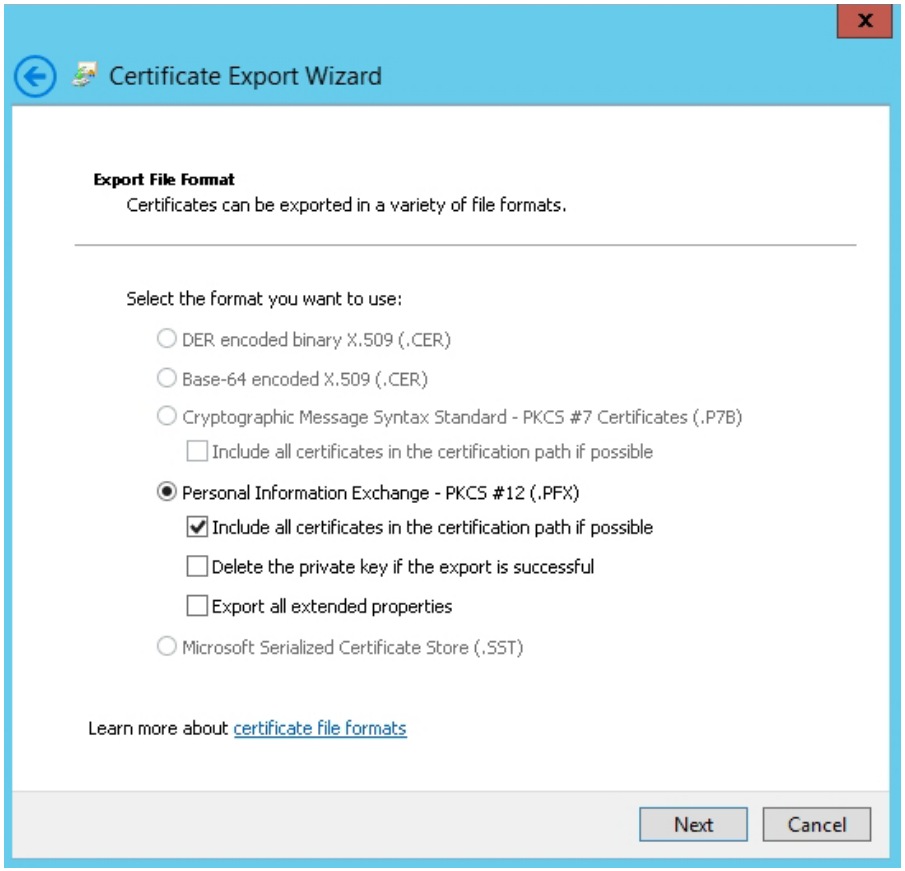
Exporting a certificate

Back Up an EFS Certificate



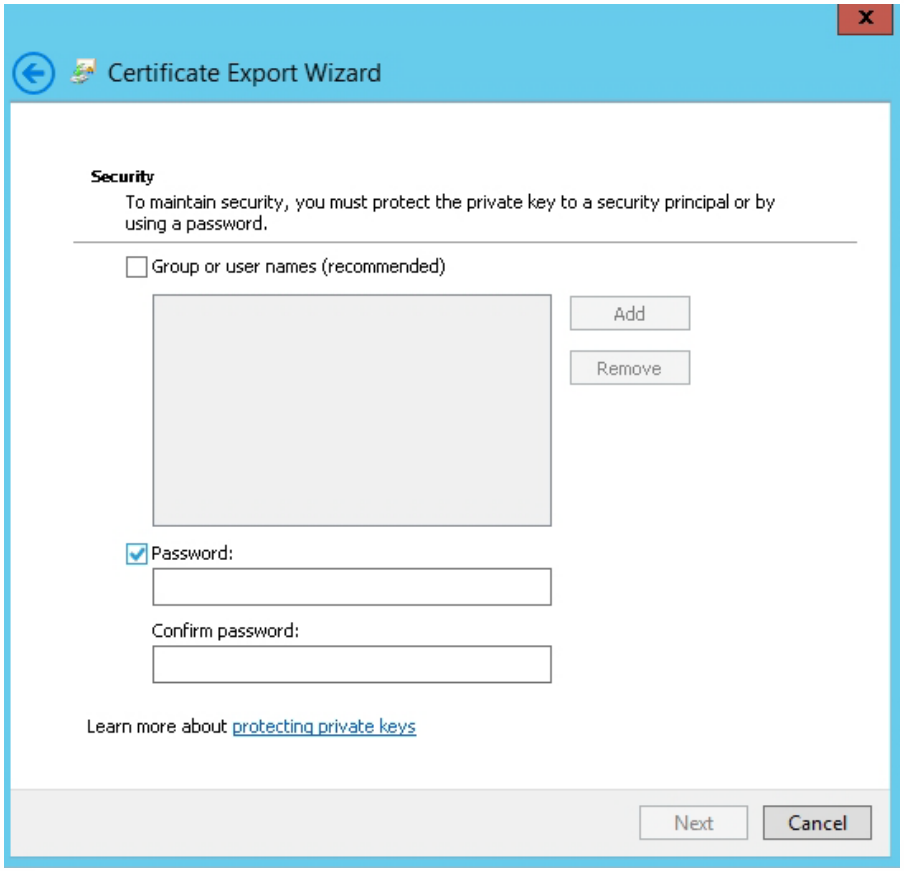
Exporting the private key on the Export Private Key page

Back Up an EFS Certificate



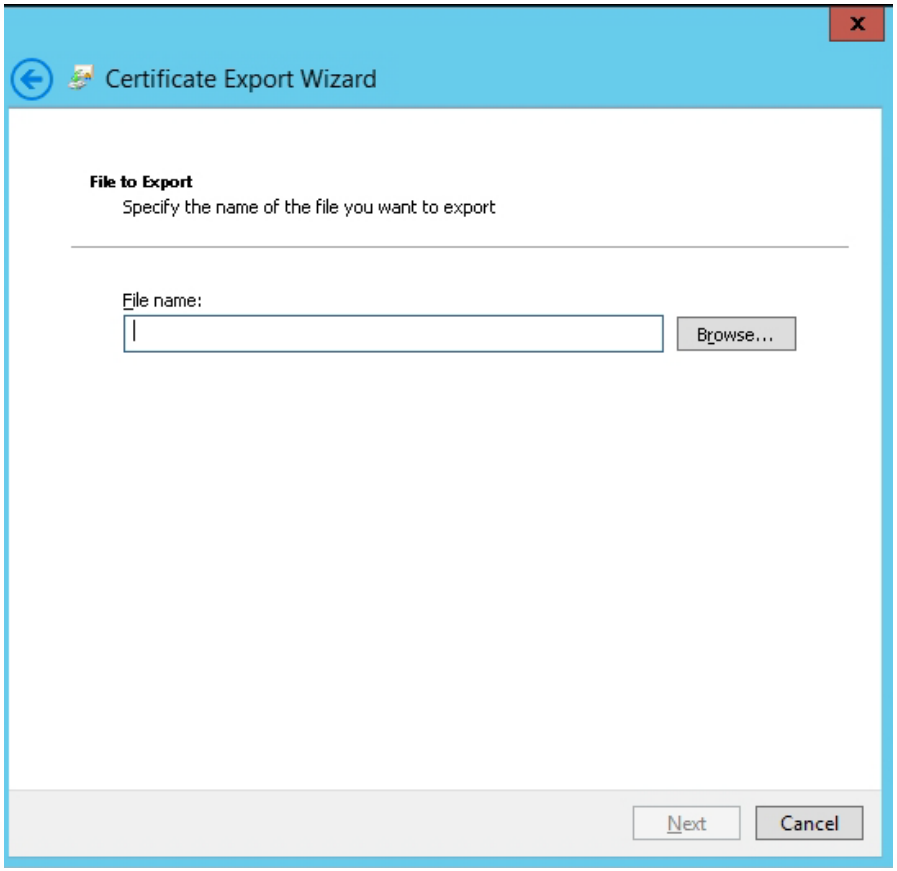
Selecting the Personal Information Exchange on the Export File Format page

Back Up an EFS Certificate



Selecting Password on the Security page

Back Up an EFS Certificate



Specifying the filename (and its location) on the File to Export page

Encrypting Files with BitLocker

- ***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.

Encrypting Files with BitLocker

BitLocker system requirements:

- A computer with TPM
- A removable USB memory device, such as a USB flash drive
- 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.
  - Both partitions must be formatted with the NTFS file system.
- A BIOS that is compatible with TPM and supports USB devices during computer startup

Encrypting Files with BitLocker

- BitLocker supports NTFS, FAT16, FAT32 and ExFAT on USB, Firewire, SATA, SAS, ATA, IDE, and SCSI drives.
- BitLocker does not support:
  - CD File System, iSCSI, Fibre Channel, eSATA, or Bluetooth
  - Dynamic volumes; it supports only basic volumes

Encrypting Files with BitLocker

BitLocker has five operational modes for OS drives, which define the steps involved in the system boot process. From most to least secure:

- TPM + startup PIN + startup key
- TPM + startup key
- TPM + startup PIN
- Startup key only
- TPM only

Encrypting Files with BitLocker

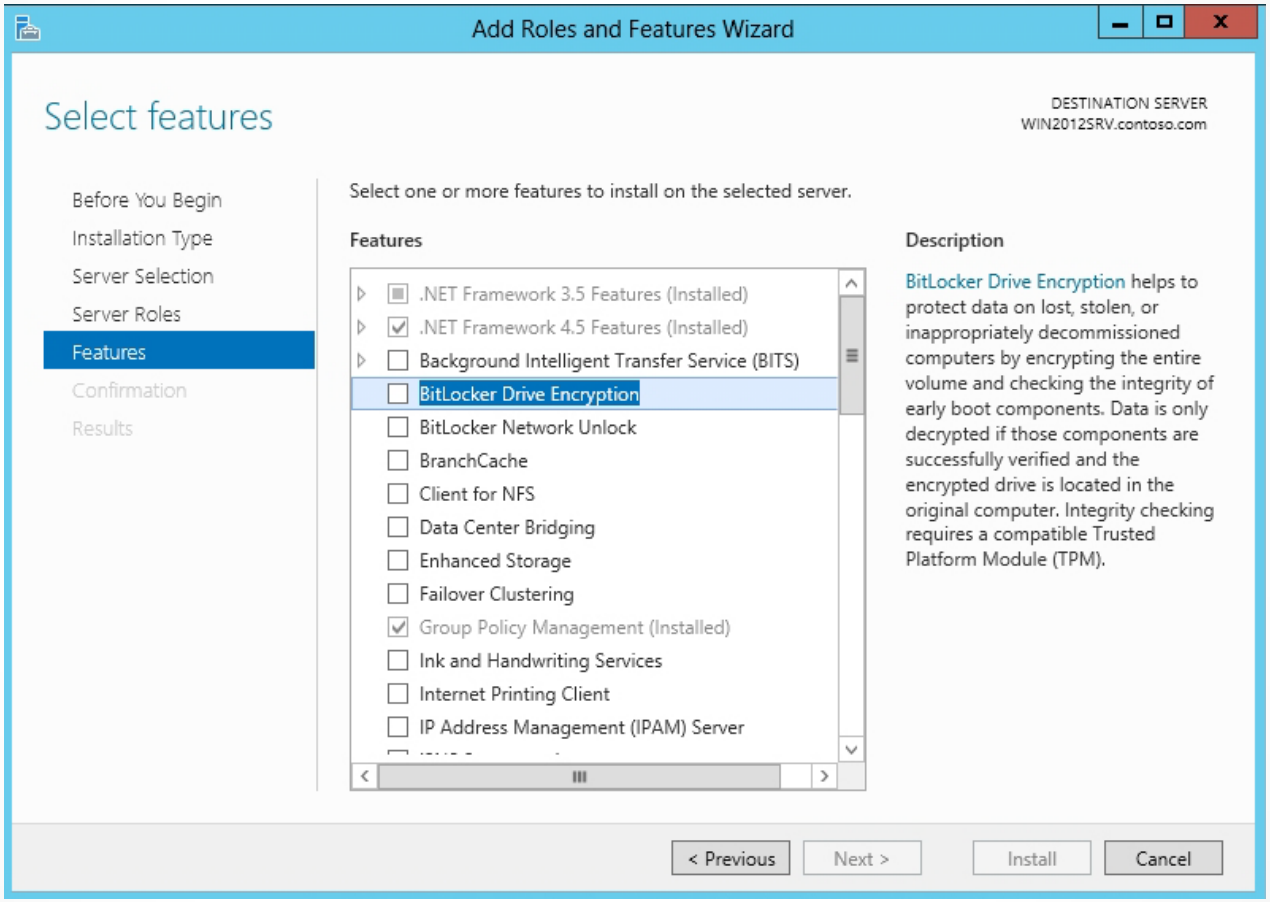
When you use BitLocker on fixed and removable data drives that are not the OS volume, you can use one of these:

- Password
- Smart card
- Automatic Unlock

Configuring BitLocker Encryption

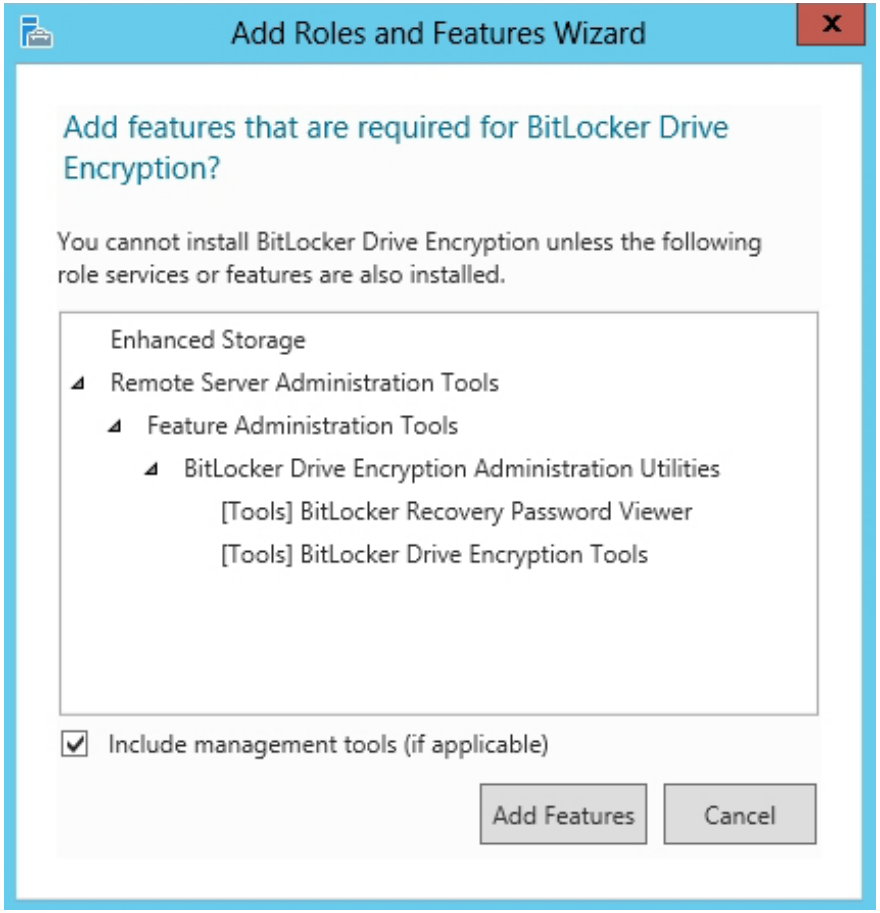
- Before you can use BitLocker on a server running Windows Server 2012, you must first install BitLocker using Server Manager.
- You can then determine whether you have TPM and turn on BitLocker.

Install BitLocker



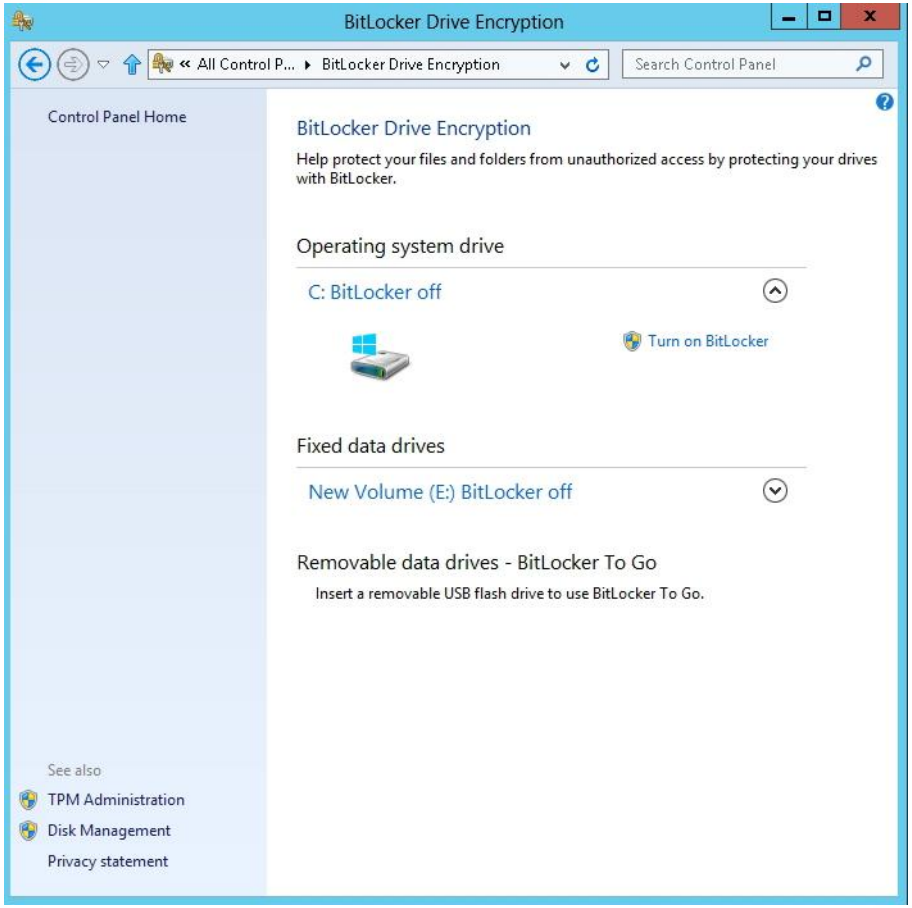
Using the Select Features page

Install BitLocker



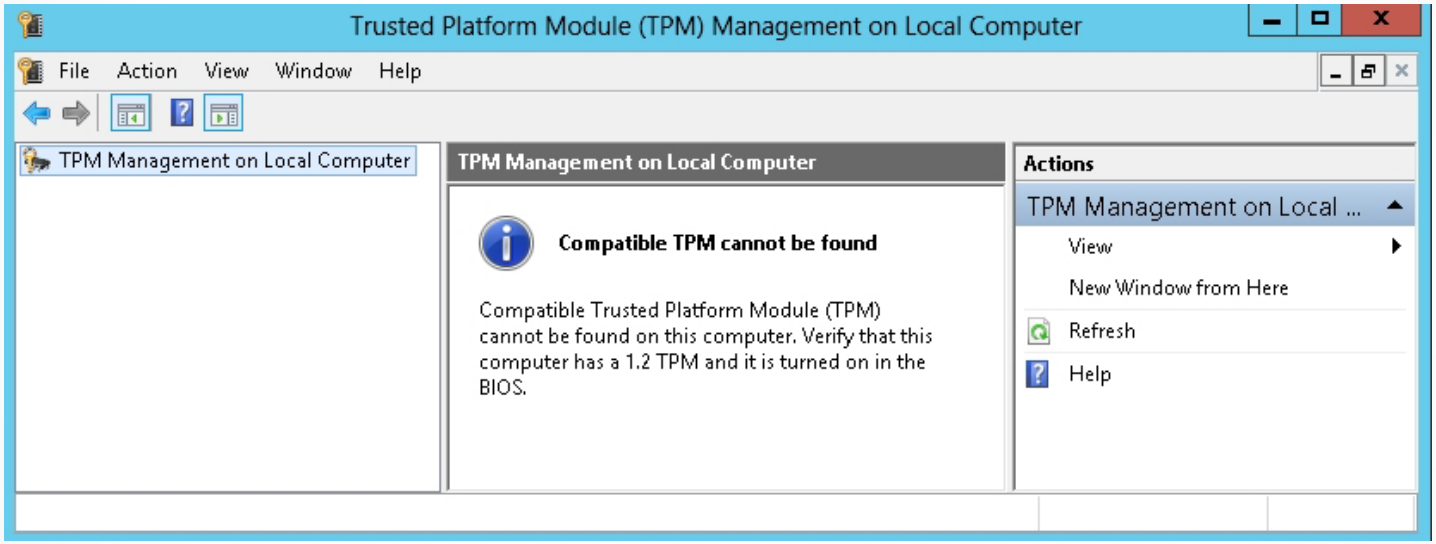
Opening the Add Roles and Features Wizard

Determine Whether You Have TPM



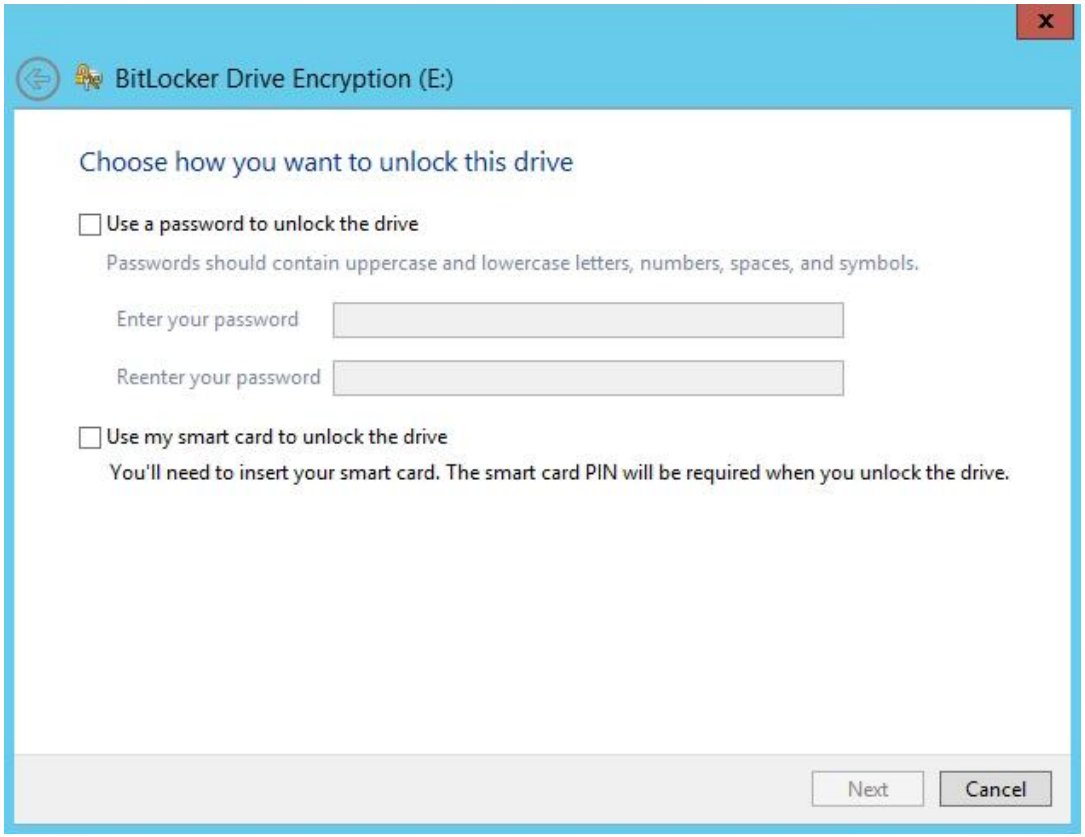
Displaying the BitLocker Drive Encryption window

Determine Whether You Have TPM



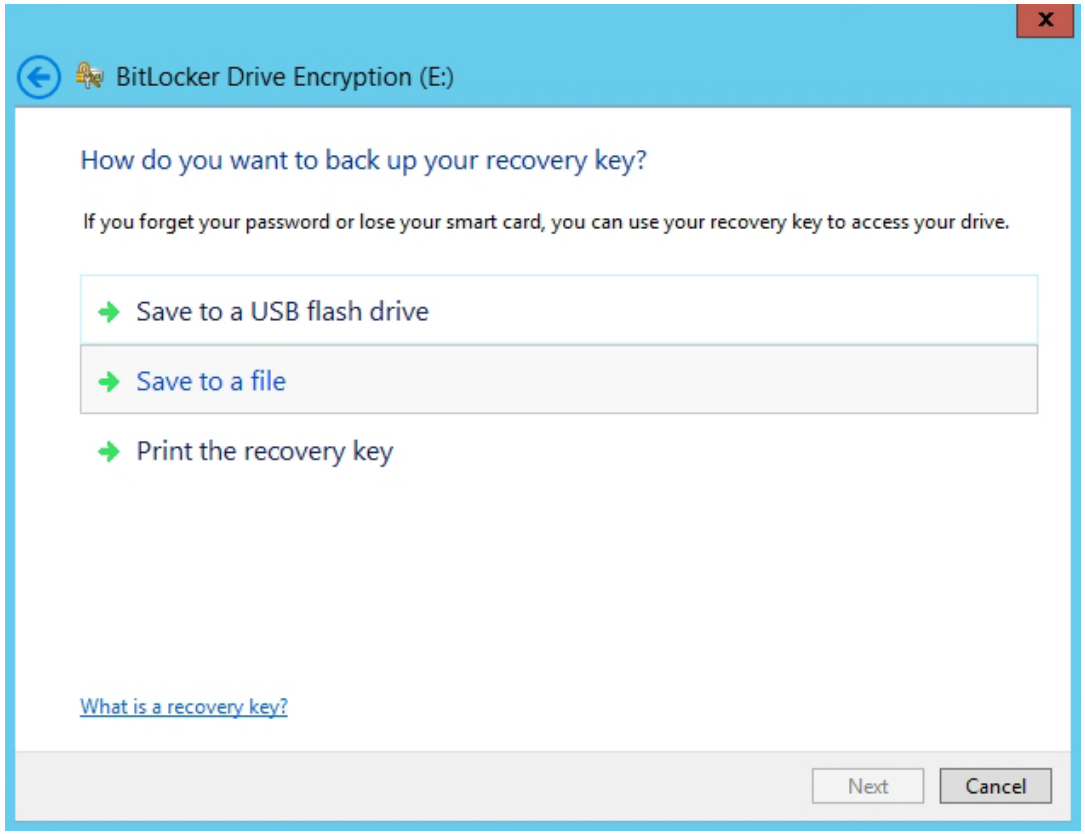
Showing that the system does not have Compatible Trusted Platform Module (TPM)

Turn On BitLocker



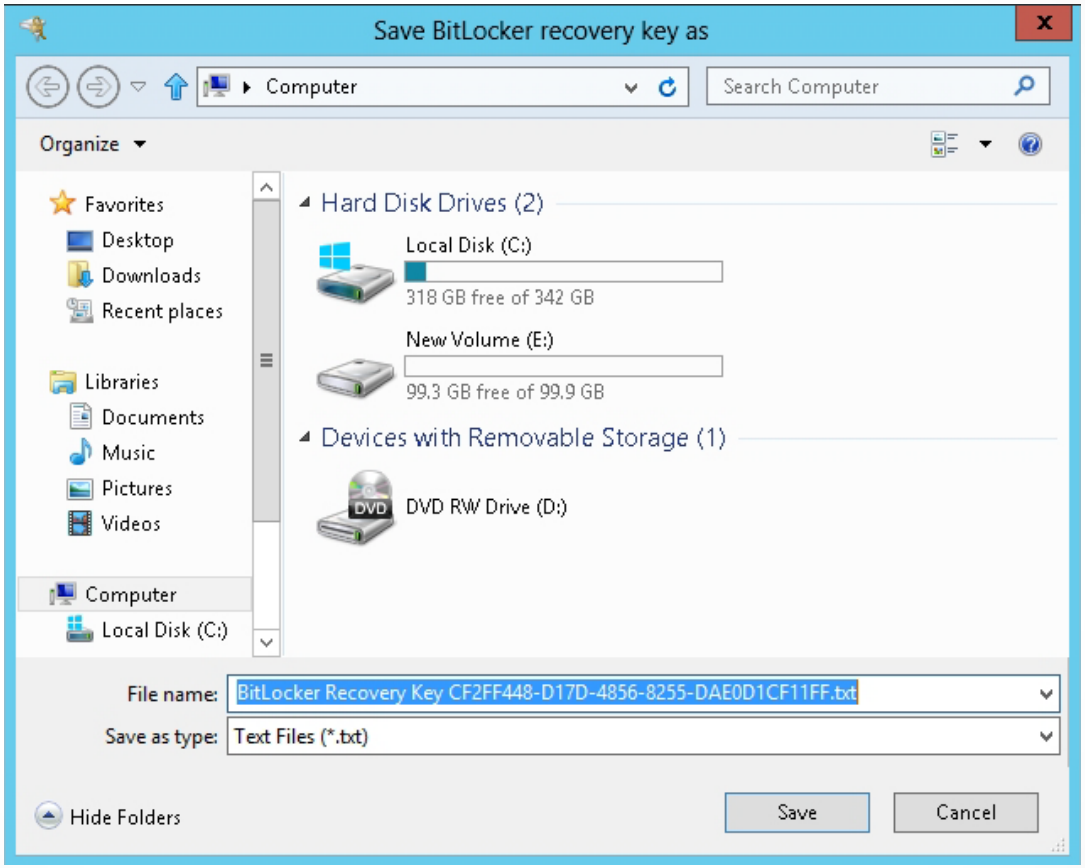
Using the Choose how you want to unlock this drive page

Turn On BitLocker



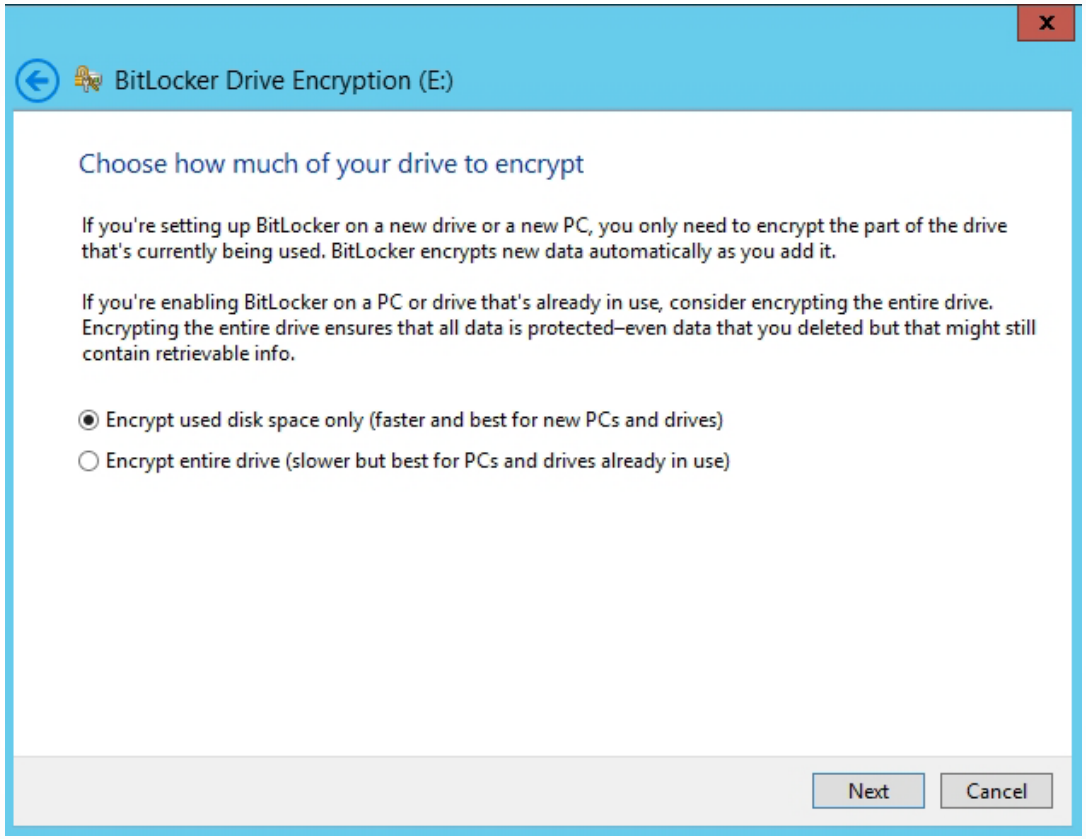
Using the How do you want to back up your recovery key? page

Turn On BitLocker



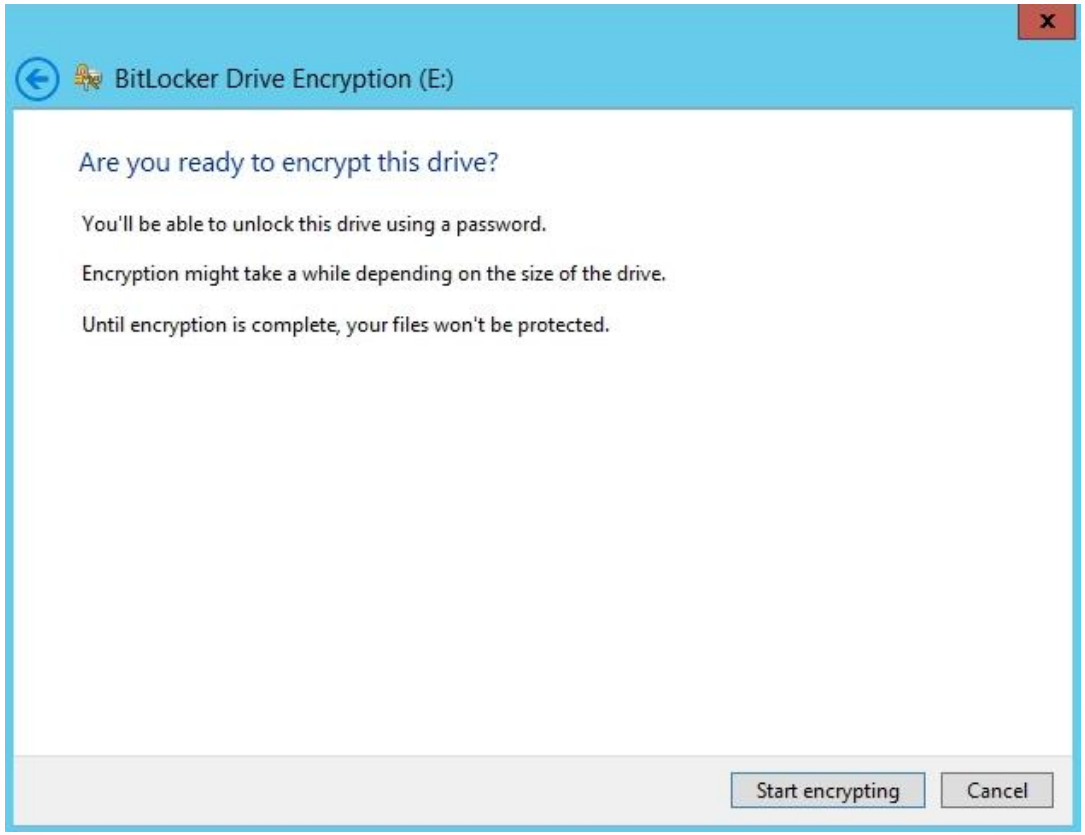
Using the Save BitLocker recovery key as dialog box

Turn On BitLocker



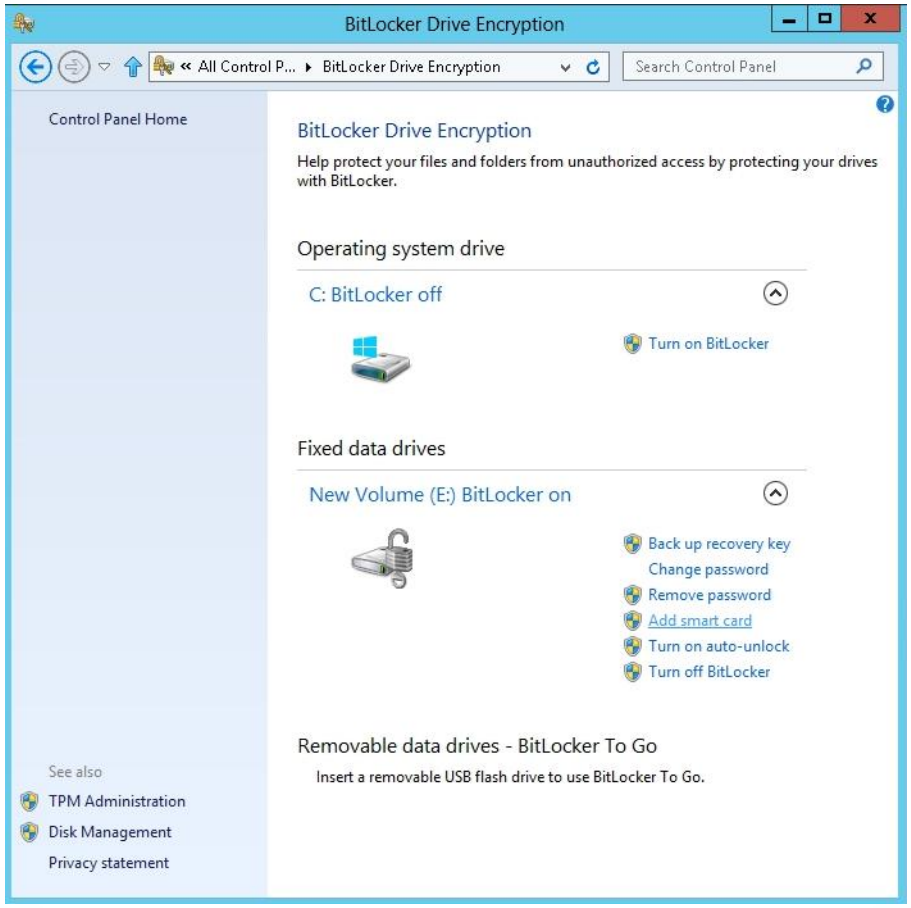
Using the Choose how much of your drive to encrypt page

Turn On BitLocker



Using the Are you ready to encrypt this drive? page

BitLocker Drive Encryption Control Panel Applet



Showing the BitLocker applet options for a BitLocker-encrypted volume

BitLocker To Go

- Was introduced in Windows 7 and Windows Server 2008 R2.
- Enables users to encrypt removable USB devices, such as flash drives and external hard disks.
- Does not require a TPM chip because the system does use the removable drive as a boot device.

Configuring BitLocker To Go

1. Insert the removable drive.
2. Open the BitLocker Drive Encryption Control Panel.
3. The device appears in the interface with a *Turn on BitLocker* link just like that of the computer's hard disk drive.

BitLocker 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.
- To enable BitLocker pre-provisioning, use a customized Windows Preinstallation Environment (WinPE) image and execute the following command:

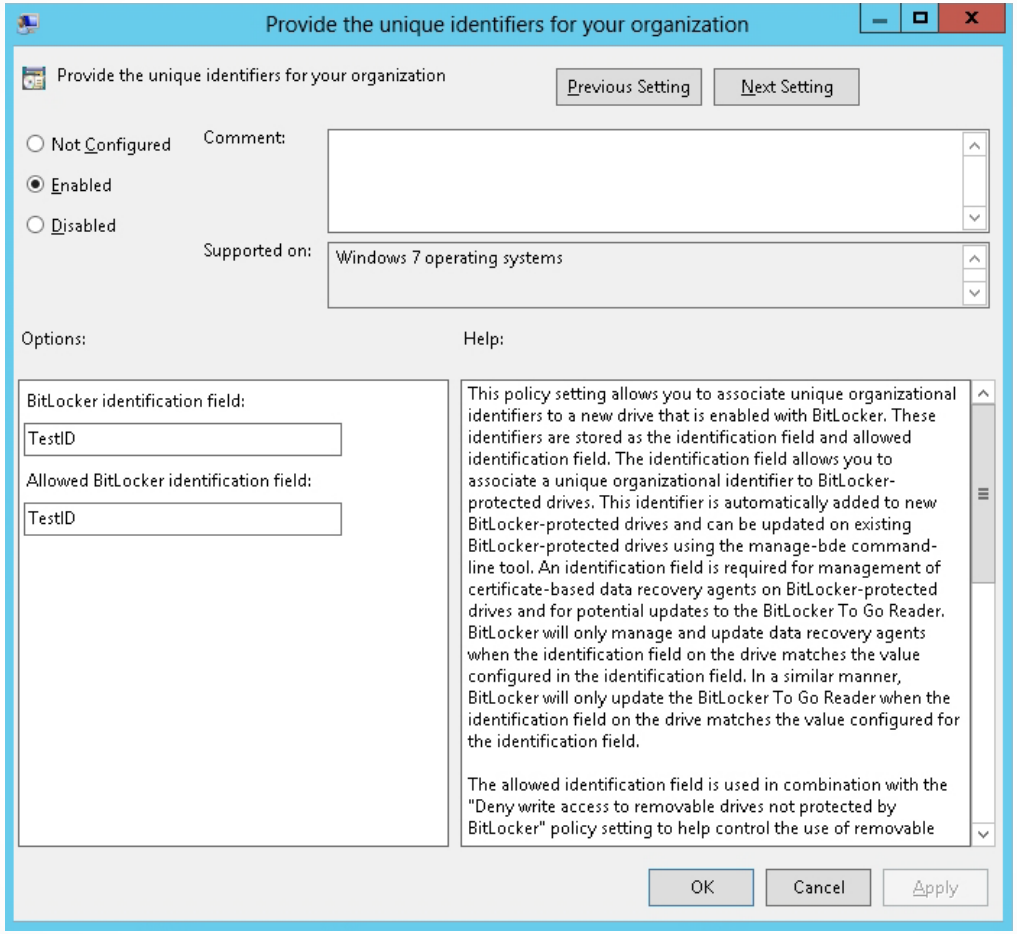
```
Manage-bde -on x:
```

Configuring BitLocker Policies

To create a data recovery agent (DRA) for BitLocker:

- 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.

Configuring BitLocker Policies



Configuring the Provide the unique identifiers for your organization policy setting

Configuring BitLocker Policies

To create a data recovery agenty (DRA) for BitLocker (continued):

- 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.

Configuring BitLocker Policies

Choose how BitLocker-protected fixed drives can be recovered

Choose how BitLocker-protected fixed drives can be recovered

Previous Setting | Next Setting

- Not Configured
- Enabled
- Disabled

Comment:

Supported on: Windows 7 operating systems

Options:

- [x] 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
- [x] 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

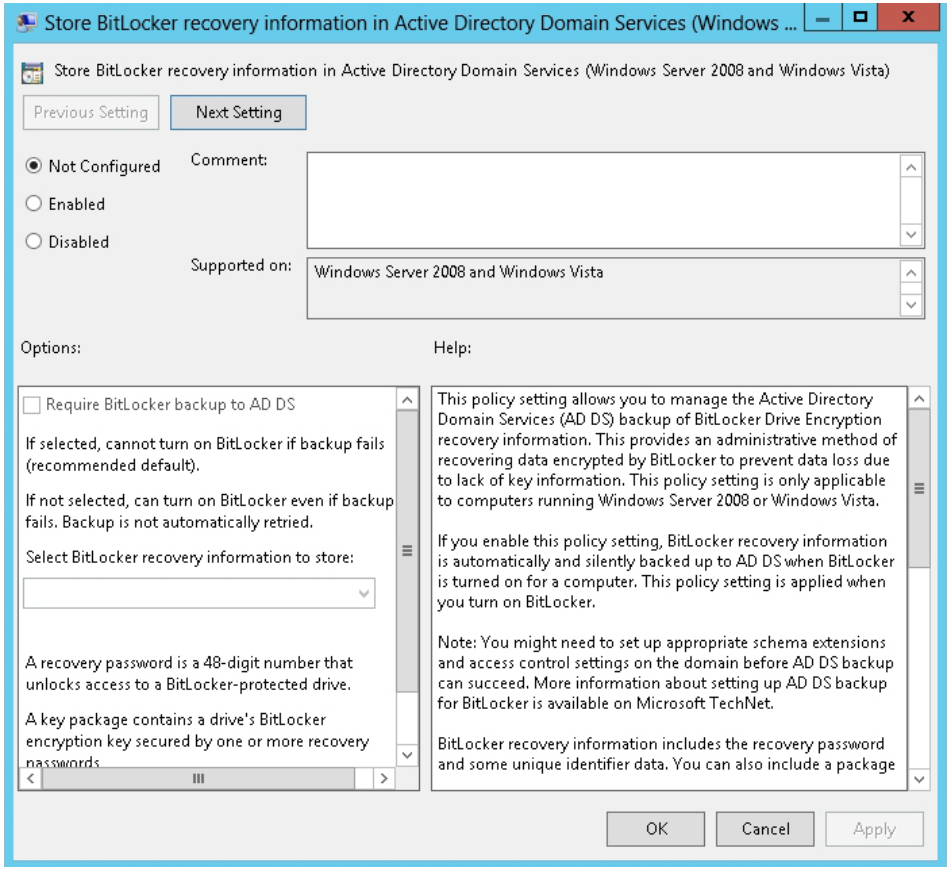
OK | Cancel | Apply

Configuring how BitLocker-protected fixed drives can be recovered

Managing BitLocker Certificates

- Back up the necessary digital certificates and keys.
- Configure BitLocker Drive Encryption to back up recovery information for BitLocker-protected drives and the TPM to AD DS.

Managing BitLocker Certificates



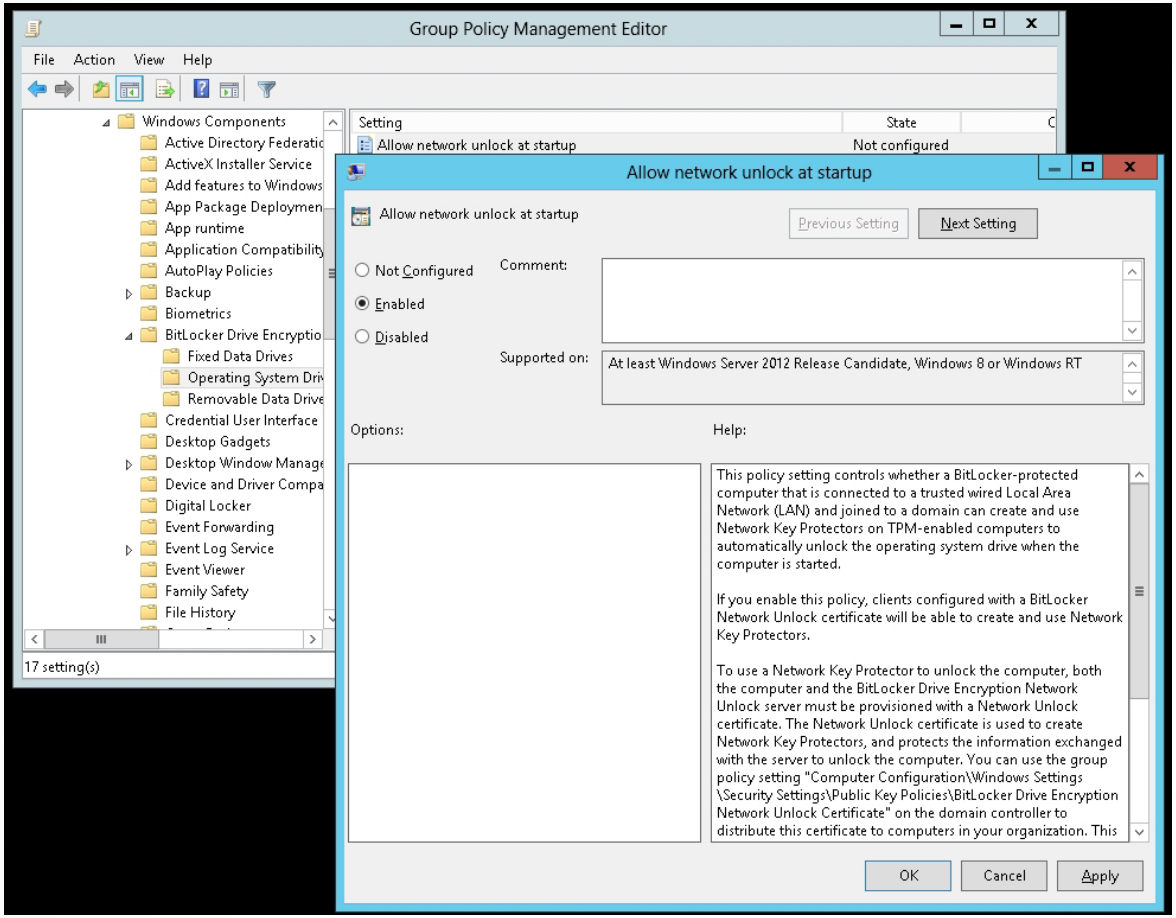
Enabling Store BitLocker Recovery Information in AD DS

Configuring the Network Unlock Feature

Hardware and software requirements:

- Windows 8 installation on UEFI firmware with UEFI DHCP drivers
- BitLocker Network Unlock feature using Server Manager
- Windows Server 2012 Windows Deployment Services (WDS) role
- DHCP server, separate from the WDS server and the domain controller
- A Network Unlock certificate
- Network Unlock Group Policy settings configured

Configuring the Network Unlock Feature



Configuring Network Unlock Group Policy settings

Configuring the Network Unlock Feature

- Network Unlock works similarly to the TPM plus startup key, but instead of reading a startup key from a USB device, Network Unlock uses an unlock key.
- The key is composed of a key that is stored on the machine's local TPM and a key that Network Unlock receives from Windows Deployment Services.
- If the WDS server is unavailable, BitLocker cannot communicate with a WDS server and instead displays the startup key unlock screen.

Lesson 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.
- 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.

Lesson Summary

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