Lesson 6: Configuring File Services and Disk Encryption MOAC 70-411: Administering

Windows Server 2012





Overview

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

Securing Files

Lesson 6: Configuring File Services and Disk Encryption

© 2013 John Wiley & Sons, Inc.

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

L	Pics Properties	Advanced Attributes
Previous V General Dub Type: Location: Size: Size on disk: Contains:	Ersions Customize Sharing Pics File folder C:\ 70.5 MB (73,931,180 bytes) 71.0 MB (74,493,952 bytes) 279 Files, 6 Folders Evider to the 22,2212, 0.44,00 byte	Choose the settings you want for this folder. When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well. Archive and Index attributes Folder is ready for archiving Allow files in this folder to have contents indexed in addition to file properties Compress or Encrypt attributes Compress contents to save disk space Encrypt contents to secure data Details
Attributes:	Read-only (Only applies to files in Hidden A	OK Cancel dvanced Apply

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.

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

- 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.

- 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.

- 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.
 - o /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

User Access to 1AddRolesandFeatu	ures.jpg
Users who can access this file:	
User	Certificate Thum
administrator(administrator@CONTOSO)	016F 3ABE 468
Add Remove	Back up keys
Recovery certificates for this file as defined by recovery policy.	:
Recovery Certificate	Certificate Thum
administrator(administrator@CONTOSO)	E60F 3A06 7D2
Administrator(administrator@contoso.com)	CE31 2566 538
Administrator(administrator@contoso.com)	FD00 1E3E E85
Ted Wilson(TWilson@contoso.com)	26AA 6525 4D0
OK	Cancel

Opening the User Access dialog box

Share a File Protected with EFS with Others

Encrypting File System					
To share file access with o OK.	ther users, select thei	r certificates from the list and click			
Issued to	Friendly name	Expiration Date			
🔄 twilson	None	7/22/2112			
administrator	None	7/21/2112			
<		>			
Find User	OK	Cancel View Certificate			

Opening the Encrypting File System dialog box

- 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.

<u>I</u>	Group Policy Manag	gement Editor			x
File Action View Help					
🗢 🄿 🔁 🖬 📋 🖾 🗟 🖬					
▲ Security Settings ∧ > Account Policies > > Event Log > > Event Log > > Restricted Groups > > System Services > > Registry > > File System > > Wired Network (IEEE 802.3) Poli > > Windows Firewall with Advance Network List Manager Policies > Windows Firewall with Advance Network (IEEE 802.11) > Public Key Policies Public Key Policies Data Protection BitLocker Drive Encrypt Automatic Certificate F Trusted Root Certificate F Intermediate Certificate F Intermediate Certificate F Intermediate Certificate F Intermediate Certificate F Software Restriction Policies	Issued To A Administrator Administrator administrator Ted Wilson Add Data Recovery Agent Create Data Recovery Agent View A All Tasks M All Tasks View A Refresh Export List Properties Help	Issued By contoso-WIN2012SRV-CA contoso-WIN2012SRV-CA administrator contoso-WIN2012SRV-CA	Expiration Date 8/18/2014 8/17/2014 6/26/2112 8/18/2014	Intended Purposes File Recovery File Recovery File Recovery File Recovery	Frie <n <n <n< th=""></n<></n </n
Administrative Templates: Policy defir	<				>
Opens the properties dialog box for the current selection					

Selecting Encrypting File System properties

Encrypting File System Properties ? ×
General Certificates Cache
File encryption using Encrypting File System (EFS): Not defined Allow Don't allow
Elliptic Curve Cryptography
Allow Require Don't allow
Options
Encrypt the contents of the user's Documents folder
Require a smart card for EFS
Create caching-capable user key from smart card
Display key backup notifications when user key is created or changed
Learn more about the <u>Encrypting File System</u>
OK Cancel Apply

Using the Encrypting File System Properties General tab

Encrypting File System Properties
General Certificates Cache
EFS template for automatic certificate requests:
Basic EFS Browse
Self-signed certificates
Allow EFS to generate self-signed certificates when a certification authority is not available
Key size for RSA self-signed certificates:
2048 🗸
Key size for Elliptic Curve Cryptography self-signed certificates:
256 🗸
Learn more about EES certificates
OK Cancel Apply

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

I Group Policy Management Editor							
File Action View Help							
🗢 🌳 🙍 🖬 📋 🖾 🗟 🖬							
🔺 🚋 Security Settings 🛛 🔨	Issued To 📩	Issued By	Expiration Date	Intended Purposes	Friendly Name		
Account Policies	🔄 Administrator	contoso-WIN2012SRV-CA	8/18/2014	File Recovery	<none></none>		
Local Policies	🔄 🖾 Administrator	contoso-WIN2012SRV-CA	8/17/2014	File Recovery	<none></none>		
⊳ 🚊 Event Log	🛱 Administrator	contoso-WIN2012SRV-CA-1	10/8/2014	File Recovery	<none></none>		
Restricted Groups	🛱 administrator	administrator	6/26/2112	File Recovery	<none></none>		
▷ iiia System Services	😨 Ted Wilson	contoso-WIN2012SRV-CA	8/18/2014	File Recovery	<none></none>		
▷ iii Registry				,			
File System							
Wired Network (IEEE 802.3) Policies							
Windows Firewall with Advanced Se							
📔 Network List Manager Policies 🛛 😑							
Wireless Network (IEEE 802.11) Polici							
⊿ Public Key Policies							
Encrypting File System							
🚞 Data Protection							
📔 BitLocker Drive Encryption							
📔 BitLocker Drive Encryption Netw							
Automatic Certificate Request Se							
Trusted Root Certification Autho							
Enterprise Trust							
Intermediate Certification Autho							
Trusted Publishers							
Untrusted Certificates							
Irusted People							

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.

🖀 certmgr - [Certificates - Current User] 📃 🗖 🗙						
FileActionViewHelpImage: Second	Logical Store Name Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Active Directory User Object Trusted Publishers Untrusted Certificates Third-Party Root Certification Authorities Trusted People Client Authentication Issuers Other People Certificate Enrollment Requests Smart Card Trusted Roots					
< III >						

Opening the certmgr console

a		certmgr - [Ce	rtificates - Current User\Person	al\Certificates]			x
File Action View Help							
🗢 🄿 🖄 🖬 🔏 🛱	🗟 🚺						
🗊 Certificates - Current User	Issued To	^	Issued By	Expiration Date	Intended Purposes	Friendly Name	Statu
⊿ 🧮 Personal	🛱 Administrat	or	contoso-WIN2012SRV-CA	8/18/2014	File Recovery	<none></none>	
 Certificates Trusted Root Certification Au Enterprise Trust 	🙀 admini	Open	administrator	7/21/2112	Encrypting File System	<none></none>	
 Enterprise Trust Intermediate Certification Au Active Directory User Object Trusted Publishers Untrusted Certificates Third-Party Root Certification 		All Tasks	Open Request Certificate with New Ke Renew Certificate with New Key Advanced Operations	y 			
 Trusted People Client Authentication Issuers Other People Certificate Enrollment Reque: Smart Card Trusted Roots 		Help	Export				
< III >	<		Ш				>
Export a certificate							

Exporting a certificate

📀 🔄 Certificate Export Wizard	x
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	_
Do you want to export the private key with the certificate?	
○ Yes, export the private key	
No, do not export the private key	
Learn more about <u>exporting private keys</u>	
Next Cance	el

Exporting the private key on the Export Private Key page

🕞 🍠 Certificate Export Wizard	×
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
O Base-64 encoded X.509 (.CER)	
 Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible 	
 Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible 	
Delete the private key if the export is successful	
Export all extended properties	
O Microsoft Serialized Certificate Store (.SST)	
Learn more about <u>certificate file formats</u>	
Next Can	icel

Selecting the Personal Information Exchange on the Export File Format page

© 2013 John Wiley & Sons, Inc.

📀 🍠 Certificate Export Wizard	×
Security To maintain security, you must protect the private 	key to a security principal or by
Group or user names (recommended)	
	Add Remove
Password:	_
Confirm password:	
Learn more about <u>protecting private keys</u>	
	Next Cancel

Selecting Password on the Security page

	x
📀 🥩 Certificate Export Wizard	
File to Export Specify the name of the file you want to export	
	-
Elle hame:	
<u>N</u> ext Cance	el 🛛

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

- 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 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

- 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

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

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

Add f Encry	eatures that are required for BitLocker Drive ption?			
You car role ser	not install BitLocker Drive Encryption unless the following vices or features are also installed.			
En	hanced Storage			
⊿ Re	mote Server Administration Tools			
4	Feature Administration Tools			
	BitLocker Drive Encryption Administration Utilities [Tools] BitLocker Recovery Password Viewer			
[Tools] BitLocker Recovery Password Viewer				
✓ Inc	lude management tools (if applicable)			

Opening the Add Roles and Features Wizard

Determine Whether You Have TPM

4	BitLocker Drive Encryption	
📀 💿 マ 👚 🎭 « All Contro	IP ► BitLocker Drive Encryption 🗸 🗸	Search Control Panel
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unautho with BitLocker. Operating system drive	orized access by protecting your drives
	C: BitLocker off	🚫
	Fixed data drives New Volume (E:) BitLocker off	\odot
	Removable data drives - BitLocker To Insert a removable USB flash drive to use BitLo	o GO ocker To Go.
See also TPM Administration Disk Management Privacy statement		

Displaying the BitLocker Drive Encryption window

Determine Whether You Have TPM

1 Trusted	Platform Module (TPM) Management on Local Co	mputer 📃 🗖 🗙
 File Action View Window Help File Action View Window Help File Provide the second second	TPM Management on Local Computer Compatible TPM cannot be found Compatible Trusted Platform Module (TPM) cannot be found on this computer. Verify that this computer has a 1.2 TPM and it is turned on in the	Actions TPM Management on Local View New Window from Here Refresh Help
	BIOS.	

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

🛞 🏘 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

© 2013 John Wiley & Sons, Inc.

📀 🎭 BitLocker Drive Encryption (E:)	x
How do you want to back up your recovery key? If you forget your password or lose your smart card, you can use your recovery key to access your drive.	
 Save to a USB flash drive 	
✦ Save to a file	
 Print the recovery key 	
What is a recovery key?	
Next Cancel	

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

© 2013 John Wiley & Sons, Inc.



Using the Save BitLocker recovery key as dialog box



Using the Choose how much of your drive to encrypt page

	X
📀 🏶 BitLocker Drive Encryption (E:)	
Are you ready to encrypt this drive? You'll be able to unlock this drive using a password. Encryption might take a while depending on the size of the drive. Until encryption is complete, your files won't be protected.	
	Start encrypting Cancel

Using the Are you ready to encrypt this drive? page

BitLocker Drive Encryption Control Panel Applet

A	BitLocker Drive Encryption	_ D X
📀 💿 マ 👚 🎭 « All Contro	ol P 🕨 BitLocker Drive Encryption 🛛 🗸 🖒	Search Control Panel
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unau with BitLocker. Operating system drive	(
	C: BitLocker off	\odot
		🎯 Turn on BitLocker
	Fixed data drives	
	New Volume (E:) BitLocker on	\odot
		 Back up recovery key Change password Remove password Add smart card Turn on auto-unlock Turn off BitLocker
	Removable data drives - BitLocker	To Go
See also PPM Administration So Disk Management	Insert a removable USB flash drive to use B	itLocker To Go.
Privacy statement		

Showing the BitLocker applet options for a BitLockerencrypted 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 preprovisioning, 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

Se Provid	e the unique identifiers for your organization	٢
Provide the unique identifiers for y	our organization <u>P</u> revious Setting <u>N</u> ext Setting	
 Not <u>Configured</u> Comment: <u>Enabled</u> <u>Disabled</u> Supported on: 	Windows 7 operating systems	
Options:		2
BitLocker identification field: TestID Allowed BitLocker identification field: TestID	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 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

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:
 - o Choose how BitLocker-protected operating system drives can be recovered.
 - o Choose how BitLocker-protected fixed drives can be recovered.
 - o Choose how BitLocker-protected removable drives can be recovered.

Configuring BitLocker Policies

See Choose how BitLocker-pro	otected fixed drives can be recovered
Choose how BitLocker-protected fixed drives can be	recovered Previous Setting Next Setting
Not <u>C</u> onfigured Comment: Enabled Disabled	
Windows / ope	rating systems
Options:	Help:
✓ 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	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.
Compare scorege of Dictocker recovery information to AD DS: Backup recovery passwords and key packages On ot enable BitLocker until recovery information is stored to AD DS for fixed data drives < III >	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 BitLockerprotected drives and the TPM to AD DS.

Managing BitLocker Certificates

Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista) Previous Setting Next Setting • Not Configured Comment: • Enabled Windows Server 2008 and Windows Vista • Disabled Supported on: Ørtions: Help: Previous Active backup to AD DS Previous Active Directory If selected, cannot turn on BitLocker if backup fails (recommended default). This policy setting allows you to manage the Active Directory Tomain Services (AD DS) blackup of BitLocker to prevent data loss due to computers running Windows Server 2008 or Windows Vista. If not selected, cannot 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 recovery password is a 48-digit number that unlocks access to a BitLocker-protected drive. A recovery password is a 48-digit number that unlocks access to a BitLocker information to store: III BitLocker is available on Microsoft TechNet.	Store BitLocker recovery infor	mation in Ac	ctiv	ve Directory Domain Services (Windows 📒 🗖	x
 Not Configured Comment: Enabled Disabled Supported on: Windows Server 2008 and Windows Vista Options: Help: Options: Help: If selected, cannot turn on BitLocker if backup fails (recommended default). If not selected, can turn on BitLocker if backup fails (recommended default). If not selected, can turn on BitLocker even if backup fails (recommended default). If not selected, can turn on BitLocker even if backup fails (recovering data encrypted by BitLocker to prevent data loss due to lack of key 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. A recovery password is a 48-digit number that unlocks access to a BitLocker-protected drive. A key package contains a drive's BitLocker encovery information includes the recovery password and sciences to a BitLocker recovery information includes the recovery password and science recovery information includes the recovery password and science recovery information include a package with the secure of the package encourse is a bitLocker is available on Microsoft TechNet. BitLocker recovery information includes the recovery password and science recovery information include a package 	Store BitLocker recovery informatio Previous Setting Next Setting	n in Active Din	rect	ory Domain Services (Windows Server 2008 and Windows Vista)	
Options: Help: Options: Help: If selected, cannot turn on BitLocker if backup fails (recommended default). 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. Select BitLocker recovery information to store: If you enable this policy setting is applied when you turn on BitLocker of the policy setting is applied when you turn on BitLocker. A recovery password is a 48-digit number that unlocks access to a BitLocker-protected drive. Note: You might need to set up appropriate schema extensions and access control settings on the domain before AD DS backup for BitLocker is available on Microsoft TechNet. A key package contains a drive's BitLocker encovery information includes the recovery password and some unique identifier data. You can also include a package without a package	 Not Configured Comment: Enabled Disabled Supported on: 	Windows Serv	ver	2008 and Windows Vista	<
 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 not selected, can turn on BitLocker even if backup fails. Backup is not automatically retried. Select BitLocker recovery information to store: 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 for BitLocker is available on Microsoft TechNet. A key package contains a drive's BitLocker encryption key secured by one or more recovery If uncertainty and some unique identifier data. You can also include a package 	Options:			Help:	×
	Require BitLocker backup to AD DS If selected, cannot turn on BitLocker if b (recommended default). If not selected, can turn on BitLocker ev fails. Backup is not automatically retried Select BitLocker recovery information to A recovery password is a 48-digit numb unlocks access to a BitLocker-protected A key package contains a drive's BitLock encryption key secured by one or more nasswords III	en if backup b store: = er that drive. ker recovery v >		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 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	

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.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.



