Windows Encryption Lab

Objective:

Learn how to use BitLocker to Go for removable drive encryption, BitLocker to secure the operating system drive, and Encrypting File System (EFS) for encrypting specific files and folders.

Part 1: Use BitLocker to Go - Encrypt a Removable Drive

Objective: Use BitLocker to Go to encrypt a removable storage drive and protect its contents from unauthorized access.

1. Connect a Removable Drive:

- Insert a USB flash drive or an external hard drive into your computer.

2. Enable BitLocker to Go:

- Open Settings > Privacy & Security > Device encryption.

- Select Manage BitLocker to open the BitLocker Drive Encryption window.

- In the Removable data drives – BitLocker To Go section, select your connected drive and click Turn on BitLocker.

3. Set Up Encryption Options:

- Choose how you want to unlock the drive. You can choose Use a password to unlock the drive or Use my smart card to unlock the drive if supported.

- Enter a strong password, confirm it, and click Next.

4. Save the Recovery Key:

- Select an option to back up your recovery key (e.g., Save to your Microsoft account, Save to a file, or Print the recovery key).

- Click Next after saving the recovery key securely.

5. Choose Encryption Mode:

- Select Compatible mode to use the drive on older Windows systems or New encryption mode if you only need to use it on Windows 10/11.

- Click Next and then Start Encrypting to begin encryption.

6. Complete the Process:

- Wait for BitLocker to encrypt the drive. You can now safely remove and store the drive, knowing it is protected with BitLocker.

Practice Questions:

- Why is it important to save the BitLocker recovery key securely?

- When might you choose Compatible mode over New encryption mode?

Part 2: Encrypt the Operating System Drive with BitLocker

Objective: Encrypt the operating system (OS) drive to secure the entire system and protect it from unauthorized access.

1. Enable BitLocker for the OS Drive:

- Open Settings > Privacy & Security > Device encryption.

- Under BitLocker Drive Encryption, select your OS drive (usually C:) and click Turn on BitLocker.

2. Choose an Unlock Option:

- Select Enter a password or Use a smart card to unlock the drive at startup.

- Enter and confirm a strong password, then click Next.

3. Back Up Your Recovery Key:

- Choose where to save the BitLocker recovery key: Microsoft account, File, or Print. This recovery key is essential for accessing your system if you forget your password.

- After saving the recovery key, click Next.

4. Choose Encryption Settings:

- Select Encrypt used disk space only for faster encryption on new devices or Encrypt entire drive for higher security on previously used systems.

- Click Next.

5. Select Encryption Mode:

- Choose New encryption mode if you plan to use the drive only on Windows 10/11 systems, or Compatible mode for cross-compatibility with older Windows versions.

- Click Next and then Start Encrypting to begin encryption of the OS drive.

6. Restart and Verify:

- Once encryption is set up, restart your computer. You'll be prompted to enter your BitLocker password to unlock the drive during boot.

- After logging in, verify encryption by checking the BitLocker Drive Encryption status in Settings.

Practice Questions:

- What are the differences between Encrypt used disk space only and Encrypt entire drive options?

- How does BitLocker encryption protect the system if the device is lost or stolen?

Part 3: Use Encrypting File System (EFS) to Encrypt Specific Files and Folders

Objective: Use Encrypting File System (EFS) to encrypt individual files and folders to protect sensitive data without encrypting the entire drive.

1. Select a File or Folder to Encrypt:

- Navigate to a file or folder you want to encrypt. Right-click on it, select Properties, and then click Advanced.

2. Enable Encryption:

- In the Advanced Attributes dialog, check the box for Encrypt contents to secure data and click OK.

- Click Apply in the Properties window.

3. Choose Encryption Application Scope:

- If encrypting a folder, you'll be prompted to apply encryption either to the folder only or to the folder and all subfolders and files within it.

- Select the preferred option and click OK.

4. Verify Encryption:

- The encrypted file or folder name will now appear in green in File Explorer, indicating that EFS is applied.

5. Backup Your EFS Certificate:

- Open Control Panel > System and Security > Backup and Restore > Create a system image.

- Click Create a system image or use certmgr.msc to export your EFS certificate and keys for future access.

Practice Questions:

- When is EFS encryption preferable over full-disk encryption with BitLocker?

- What steps would you take to recover EFS-encrypted data if the user profile is deleted?

Final Questions

1. How do BitLocker and EFS differ in terms of scope and use cases?
2. Describe a scenario where BitLocker to Go would be essential for data security.
3. Why is it necessary to back up recovery keys and certificates when using encryption tools?