

REVIEW LESSON

MTA Course: 10753 Windows Operating System Fundamentals

Lesson name: Windows Operating System Fundamentals 4.3

Topic: Understand encryption (One 50-minute class period)

File name: 10753_WindowsOS_RL_4.3

Lesson Objective

4.3: Understand encryption. *This objective may include but is not limited to:* understanding BitLocker, encrypting file systems (EFS), and compression

Preparation Details

Prerequisite student experiences and knowledge:

This MTA Certification Exam Review lesson is written for students who have learned about Microsoft Windows fundamentals. Students who do not have the prerequisite knowledge and experiences cited in the objective will find additional learning opportunities using resources such as those listed in the “Resources” section at the end of this review lesson.

Instructor preparation activities:

- Make copies available of the Student Activity document 10753_WindowsOS_SA_4.3.
- The instructor should have access to an existing system running Microsoft Windows 7 Professional or a virtual machine with Windows 7 Professional for the purposes of demonstrating encryption and compression.

Resources, software, and additional files needed for this lesson:

- 10753_WindowsOS_SA_4.3
- 10753_WindowsOS_SA_4.3_key
- 10753_WindowsOS_PPT_4.3

Teaching Guide

Essential Vocabulary

compress—to reduce the size of a set of data, such as a file or a message, so that it can be stored in less space or transmitted with less bandwidth.

cryptography—the science of providing security for information. It has been used historically as a means of providing secure communication between individuals, government agencies, and military forces. Today, cryptography is a cornerstone of the modern security technologies used to protect information and resources on both open and closed networks.

encryption—the process of coding plaintext to create ciphertext.

public (asymmetric) key encryption—uses different keys for encrypting and decrypting information.

symmetric key encryption—uses the same key for encrypting and decrypting information.

Lesson Sequence

Activating prior knowledge/lesson staging (5 minutes):

Direct students to answer each question in their notes.

1. What feature of Windows 7 allows you to secure your data on portable devices such as laptops? (BitLocker.)
2. Within Windows, can you encrypt and compress a file? (No, you can either encrypt or compress, but not both.)
3. How are EFS keys protected? (The user password is used to protect the EFS key.)

Lesson activity (40 minutes):

1. Teacher instruction (20 minutes; see the “Suggested best practices” section below regarding this presentation)
 - a. Use the included Microsoft PowerPoint presentation to review encryption.
2. Guided practice (20 minutes)
 - a. Direct students to complete the Student Activity document 10753_WindowsOS_SA_4.3.

Assessment/lesson reflection (5 minutes):

1. In the same notes that they created for the “Activating prior knowledge/lesson staging” section at the beginning of the class, direct students to check their initial answers and make any changes if necessary.
2. Instruct students to write and submit any questions they have or any topics about which they would like more assistance.
3. After class, look through student responses and follow up with any students requiring additional help.

Resources:

- **Microsoft: TechNet: The Encrypting File System**
<http://technet.microsoft.com/en-us/library/cc700811.aspx>
- **Microsoft: Encrypt or decrypt a folder or file**
<http://windows.microsoft.com/en-US/windows7/Encrypt-or-decrypt-a-folder-or-file>
- **Microsoft: TechNet: How Do I: Get Started with the Encrypting File System in Windows 7? (Video)**
<http://technet.microsoft.com/en-us/windows/ee430894.aspx>
- **Microsoft: TechNet: BitLocker Drive Encryption Overview**
<http://technet.microsoft.com/en-us/library/cc732774.aspx>
- **Microsoft: TechNet: BitLocker Drive Encryption Deployment Guide for Windows 7**
[http://technet.microsoft.com/en-us/library/dd875547\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/dd875547(W.S.10).aspx)
- **Microsoft: Best practices for NTFS compression in Windows**
<http://support.microsoft.com/kb/251186>
- **Microsoft: BitLocker Drive Encryption**
<http://windows.microsoft.com/en-US/windows7/products/features/bitlocker>
- **Microsoft: TechNet: Cryptography for Network and Information Security**
<http://technet.microsoft.com/en-us/library/cc962027.aspx>
- **Microsoft: TechNet: Encryption**
<http://technet.microsoft.com/en-us/library/cc962028.aspx>

Suggested best practices:

- Demonstrating how EFS is user- or password-based by logging in with separate user accounts will help the students better understand how EFS works. It is also important to warn students that EFS can be a very dangerous feature if you do not keep track of your keys, especially your password, because when encryption is performed, the keys are based on the password the user is logged on with.
- Demonstrating BitLocker To Go shows the students how to lock and unlock the drives after it has been encrypted.