

## REVIEW LESSON

MTA Course: 10753 Windows Operating System Fundamentals  
Lesson name: Windows Operating System Fundamentals 3.2  
Topic: Understand user account control (One 50-minute class period)  
File name: 10753\_WindowsOS\_RL\_3.2

### Lesson Objective

**3.2:** Understand user account control (UAC). *This objective may include but is not limited to:* understanding standard user vs. administrative user, understanding types of UAC prompts and levels.

### Preparation Details

#### Prerequisite student experiences and knowledge:

This MTA Certification Exam Review lesson is written for students who have learned about Microsoft Windows operating system 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 10753\_WindowsOS\_SA\_3.2 document.
- The instructor should have access to an existing system running Windows 7 Professional or a virtual machine with Windows 7 Professional installed for the purposes of demonstrating how to configure User Account Control (UAC).

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

- 10753\_WindowsOS\_RL\_3.2
- 10753\_WindowsOS\_SA\_3.2
- 10753\_WindowsOS\_SA\_3.2\_key
- 10753\_WindowsOS\_PPT\_3.2

## **Teaching Guide**

### **Essential Vocabulary**

**administrator account**—a user account that enables changes that will affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. Administrators also can make changes to other user accounts.

**digital signature**—security mechanism used on the Internet that relies on two keys, one public and one private, that are used to encrypt messages before transmission and to decrypt them on receipt.

**malicious software**—software created and distributed for harmful purposes, such as invading computer systems with viruses, worms, or innocent-looking plug-ins and extensions that mask other destructive capabilities.

**standard user account**—enables access to most of the capabilities of the computer. The user can use most programs that are installed on the computer and change settings that affect your user account. However, the user can't install or uninstall some software and hardware, delete files that are required for the computer to work, or change settings that affect other users or the security of the computer. If using a standard account, the user might be prompted for an administrator password before performing certain tasks.

**user account**—an established means for an individual to gain access to the system and its resources on a secure or multiuser computer system. Usually created by the system's administrator, a user account consists of information about the user, such as password, rights, and permissions.

**User Account Control (UAC)**—a feature in Windows that helps the user stay in control of the computer by issuing notices when a program makes a change that requires administrator-level permission. UAC works by adjusting the permission level of your user account. If you're doing tasks that can be done as a standard user, such as reading email, listening to music, or creating documents, you have the permissions of a standard user—even if you're logged on as an administrator.

## **Lesson Sequence**

### **Activating prior knowledge/lesson staging (5 minutes):**

Direct students to answer each question in their notes.

1. What is the most important rule for controlling access to resources? (To provide the least amount of access privileges required for users to perform their daily tasks)
2. What is a malicious program or software?(Software created and distributed for harmful purposes, such as invading computer systems in the form of viruses, worms, or innocent-seeming plug-ins and extensions that mask other destructive capabilities)

3. What does the UAC do? (Notifies the user before changes are made to the computer that require administrator-level permission)

**Lesson activity (40 minutes):**

1. Teacher instruction (20 minutes; see the “Suggested best practices” section below regarding this presentation)
2. Use the included Microsoft PowerPoint presentation to review understanding UAC.
3. Guided practice (20 minutes)
  - a. Students are to complete 10753\_WindowsOS\_SA\_3.2.

**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 the student responses and follow up with any student requiring additional help.

**Resources:**

- **Microsoft: User Account Control**  
*<http://windows.microsoft.com/en-US/windows7/products/features/user-account-control>*
- **Microsoft: TechNet: Inside Windows 7 User Account Control**  
*<http://technet.microsoft.com/en-us/magazine/2009.07.uac.aspx>*
- **Microsoft: Malware Protection Center**  
*<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx>*
- **Microsoft: What is a digital signature?**  
*<http://windows.microsoft.com/en-US/windows7/What-is-a-digital-signature>*
- **Microsoft: TechNet: User Account Control Step-by-Step Guide**  
*[http://technet.microsoft.com/en-us/library/cc709691 \(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc709691 (WS.10).aspx)*
- **Microsoft: TechNet: User Account Control in Windows 7 Best Practices**  
*[http://technet.microsoft.com/en-us/library/ee679793 \(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee679793 (WS.10).aspx)*

**Suggested best practices:**

- It should be emphasized that UAC should not be disabled on any systems. UAC is also useful for home use to help prevent malicious software from being installed. UAC will prompt for a password if any family member browses to a site that attempts to install any software. Creating standard user accounts at home can help maintain a stable operating system.

**Additional notes to the teacher:**

- The instructor should create standard user accounts on the students' workstations if they aren't already using them. This will help demonstrate the features of UAC.