

STUDENT ACTIVITY 3.3_KEY: REMOVE MALICIOUS SOFTWARE

MTA Course: 10753 Windows Operating System Fundamentals

Topic: Remove malicious software

File name: 10753_WindowsOS_SA_3.3_key

Lesson Objective

3.3: Remove malicious software. *This objective may include but is not limited to:* understanding Windows Defender, Action Center, the Malicious Software Removal tool, Windows Registry, and Microsoft Forefront Endpoint Protection.

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

- A workstation with Windows 7 Professional or Enterprise edition installed
- Malicious Software Removal Tool from Microsoft
 - <http://www.microsoft.com/security/pc-security/malware-removal.aspx>
 - The removal tool has both x86 and x64 versions.
- Alternative option:
 - A virtual machine with Windows 7 Professional or Enterprise edition installed

Directions to the student:

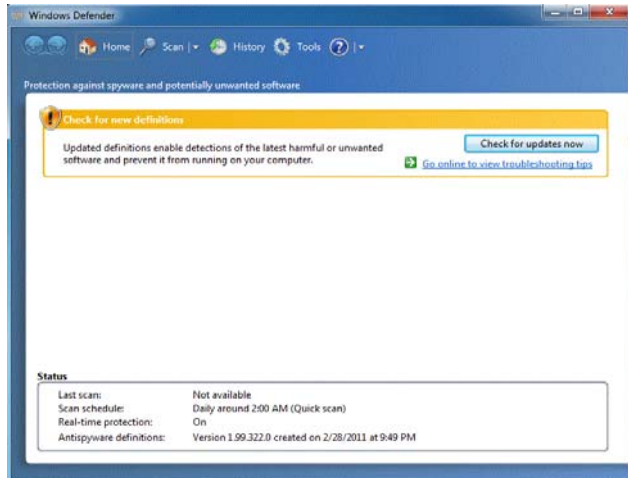
Complete the following hands-on activities. The screenshots in the activity may look different from your system. Answer the questions as you work through the activities. Verify your answers with the instructor.

Malicious Software Removal Tool

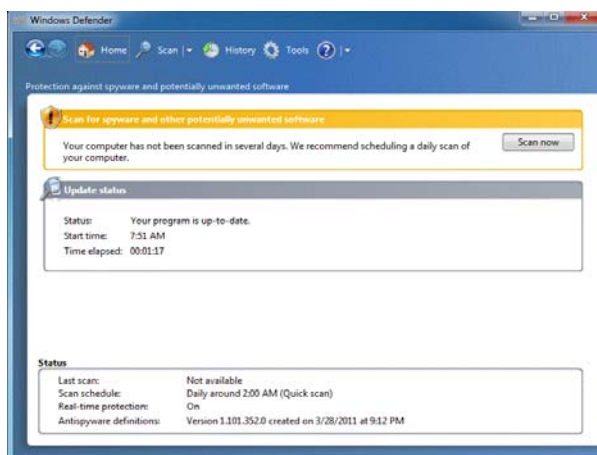
1. Authenticate into your system using the credentials provided by your instructor.
2. Obtain the Malicious Software Removal Tool from your instructor, or browse to and download the appropriate tool here:
 - a. x86(32-Bit) version:
 - i. <http://www.microsoft.com/downloads/en/details.aspx?FamilyId=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displaylang=en>

Windows Defender

1. Authenticate into your system using the credentials provided by your instructor.
2. Click Start and select Control Panel. Type **Windows Defender** in the Search field and press ENTER.

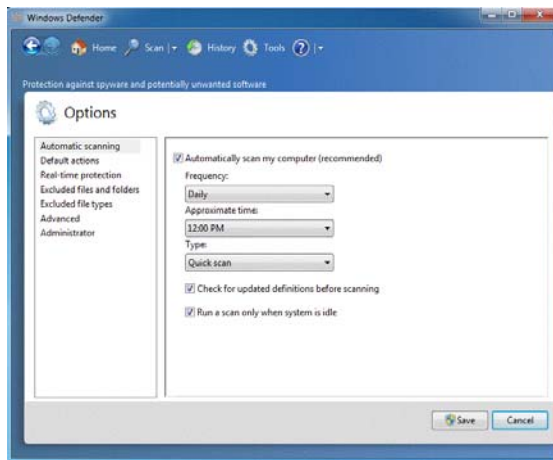


3. Windows Defender may need to check for new updates. Click Check For Updates Now to get the latest definitions.
4. After the updates are completed, you receive a warning, as shown here, that your system hasn't been scanned in several days and it is recommended that you schedule a daily scan. Click Scan.



5. Take note of the resources that Windows Defender scans. The software not only scans the important files but also thoroughly scans the registry files, which are files used to personalize each user's experience and maintains configurations of installed software and profiles.
6. After the scan completes, click the Tools icon on the upper menu.
7. To schedule this program to scan on a regular basis, click the Options link in the Settings area.

8. Select the Automatically Scan My Computer (Recommended) check box.
9. Change the approximate time to 12:00 P.M., as shown here.



10. Click the Default Actions option in the left pane.
11. What are the three options for severe alert items?
 - a. Recommended Action Based on Definitions
 - b. Remove
 - c. Quarantine
12. Click the Advanced option in the left pane.
13. What are the five options available on the Advanced menu?
 - a. Scan Archive Files
 - b. Scan Email
 - c. Scan Removable Drives
 - d. Use Heuristics
 - e. Create Restore Point
14. Select the Scan Removable Drives check box.
15. Click Save.
16. Verify your answers with the instructor.