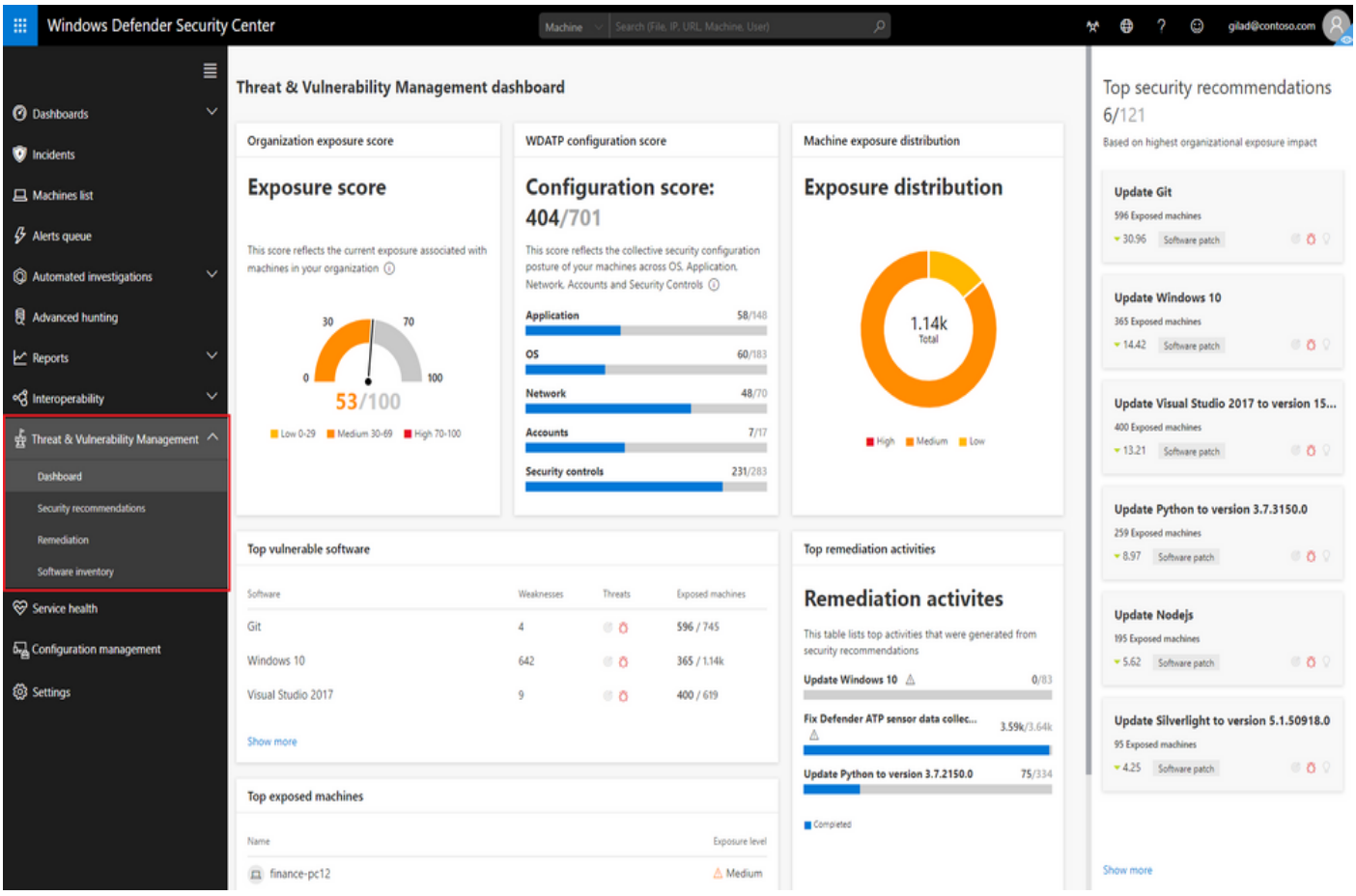
EXPERIMENT NO 1

Windows Defender

AIM: To Prevent PC against latest threats using Windows Defender.

Windows Defender Advanced Threat Protection (now rebranded as Microsoft Defender for Endpoint) is a post-breach solution that detects, investigates, and responds to security threats on your network. Microsoft Defender for Endpoint keeps your network secure by continuously evaluating and identifying existing weaknesses in your system, addressing security concerns, and investigating security attacks that take place. It is important to note that Microsoft Defender for Endpoint is not an anti-virus product (and cannot be substituted for one), but a post-breach solution that complements the capabilities of anti-virus solutions. Microsoft Defender for Endpoint is designed to help you after your network security has been breached.

Threat and vulnerability management



Windows Advanced Threat Protection consistently performs real-time analysis on endpoints. It retains visibility over all software in a device. It is constantly working on identifying and assessing any security vulnerabilities that might exist in any of the applications on your device.

With Windows Defender Advanced Threat Protection, you can see your overall exposure score, vulnerable software and machines in your network, and what you can do to remediate the issues.

When it discovers any weakness or vulnerability in any device, it promptly alerts you and provides recommendations to remediate it.

Attack surface reduction

We can reduce the risk of a potential threat by minimizing areas where cyberattacks can take place. This can be done through various controls put in place by Windows Defender for Endpoint, such as only allowing applications marked as 'trusted' to run on the device, allowing you to restrict certain behaviors in files and applications, as well as preventing untrusted websites, applications and files from accessing all areas in the device.

Next generation protection

Windows Defender for Endpoint leverages Microsoft's sophisticated technology and ongoing research in machine learning and threat resistance to provide you with behavior-based antivirus protection, cloud-delivered blocking, and constant product updates.

Endpoint detection and response

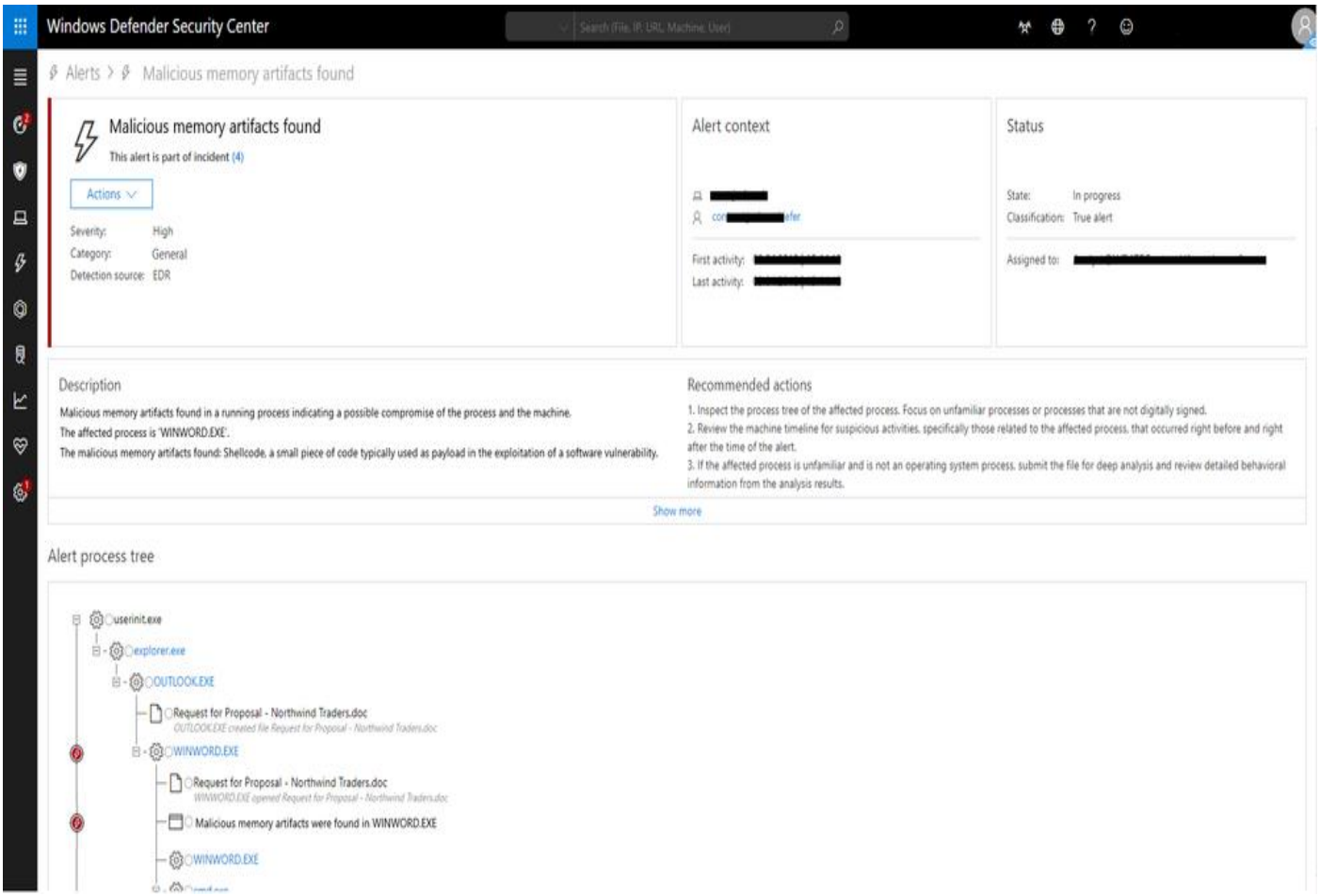
Being a post-breach solution, Windows Defender Advanced Threat Protection offers endpoint detection and response (EDR) capabilities that identify and warn you about suspicious activities.

Once suspicious activity is detected in your network, you will immediately be alerted and provided with data to investigate the threat and make an informed decision about your next steps.

The Defender for Endpoint dashboard gives you access to in-depth data and analysis of different aspects of your security system from a centralized portal.

The endpoint detection and response in Windows Defender for Endpoint primarily consist of the following features and capabilities:

- **Alerts:** When a threat is detected, you will instantly receive an alert in your dashboard, along with basic information such as what the threat is, which device it has been found in, how severe it is, etc.
- **Investigation:** Your security team can investigate the threat further through features such as a timeline of events, which gives you a complete history of the threat since it arrived in your system, along with the list of machines that it has infected.
- **Remediation:** You will also be provided with a set of recommended next steps based on the behavior of the threat, and you can choose which action you would like to take.



Observation : Thus, Windows Defender has been successfully analyzed.

EXPERIMENT NO 2

Microsoft Security Essentials

Aim: To Protect PC using Microsoft Security Essentials.

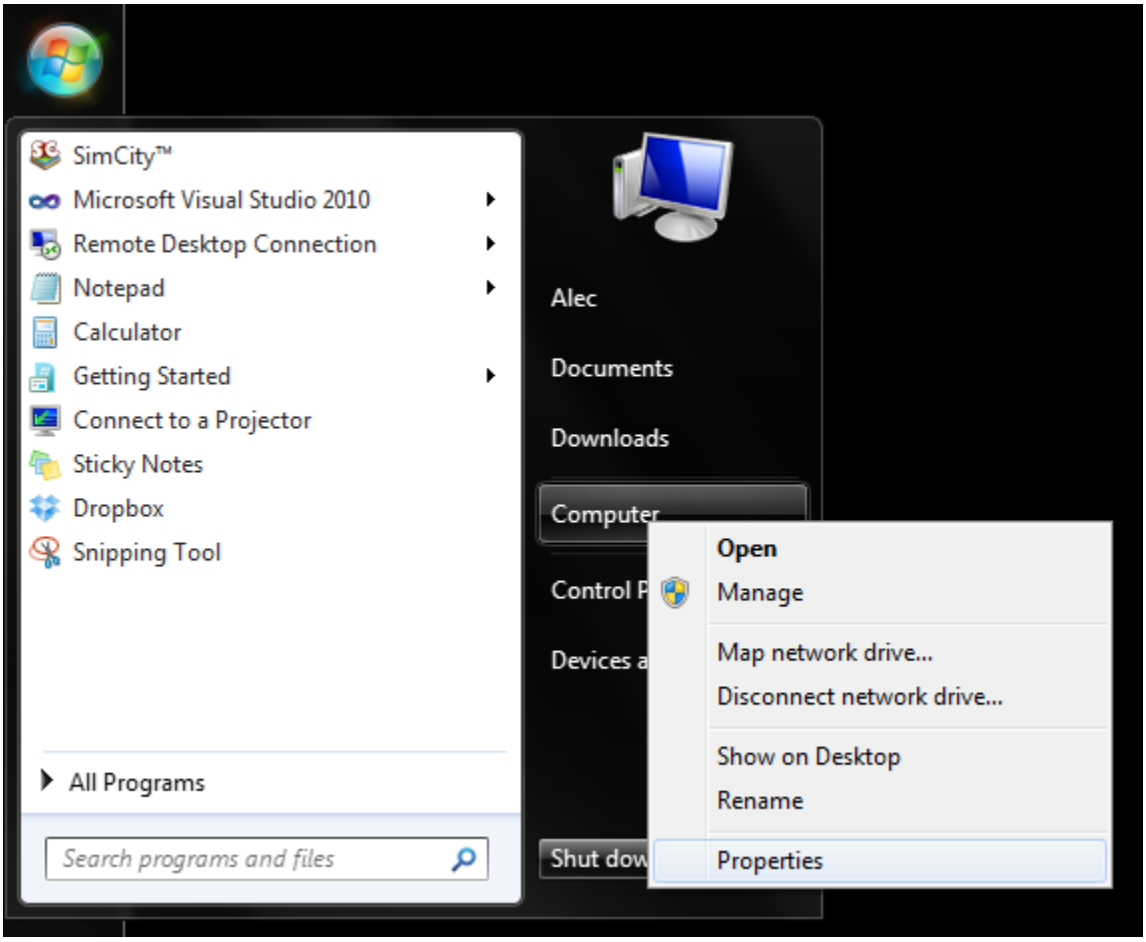
Description

To install Microsoft Security Essentials on Windows 7, follow these steps.

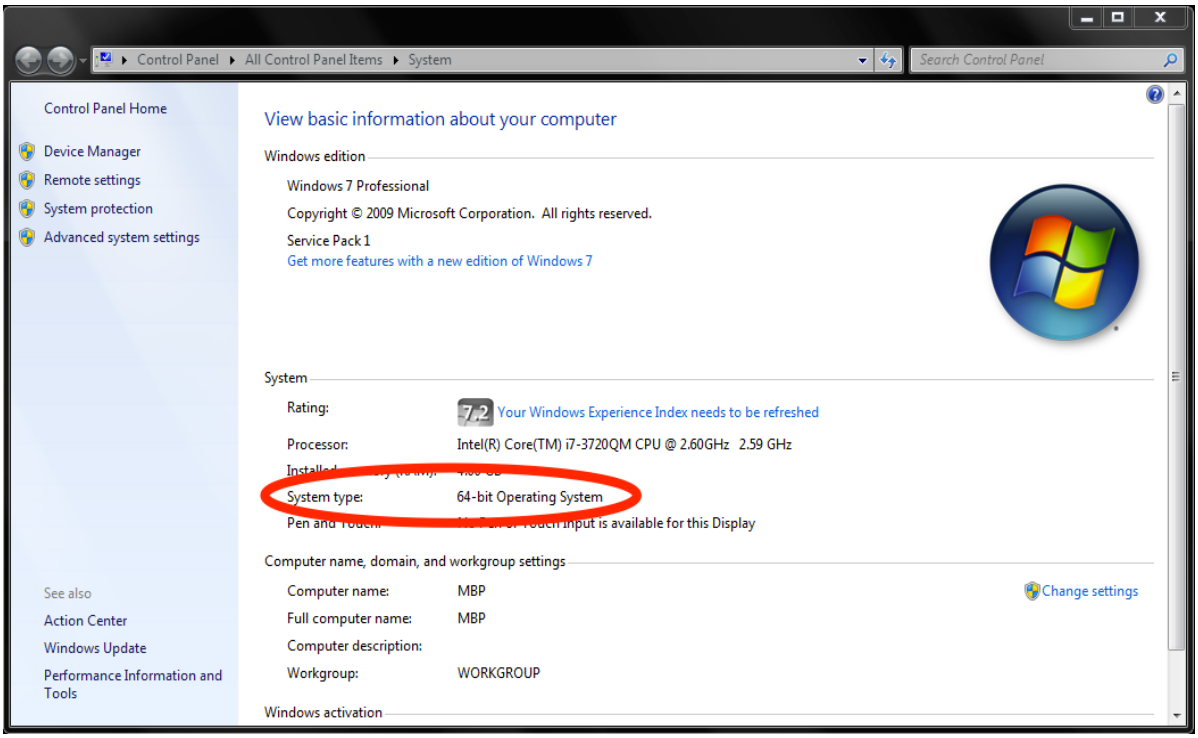
Instructions

Identify If You Have a 32-bit or 64-bit Version

1. Open the System Properties by selecting the Start button, right-clicking Computer, and then selecting Properties.



2. Under the System heading, you can view the system type.



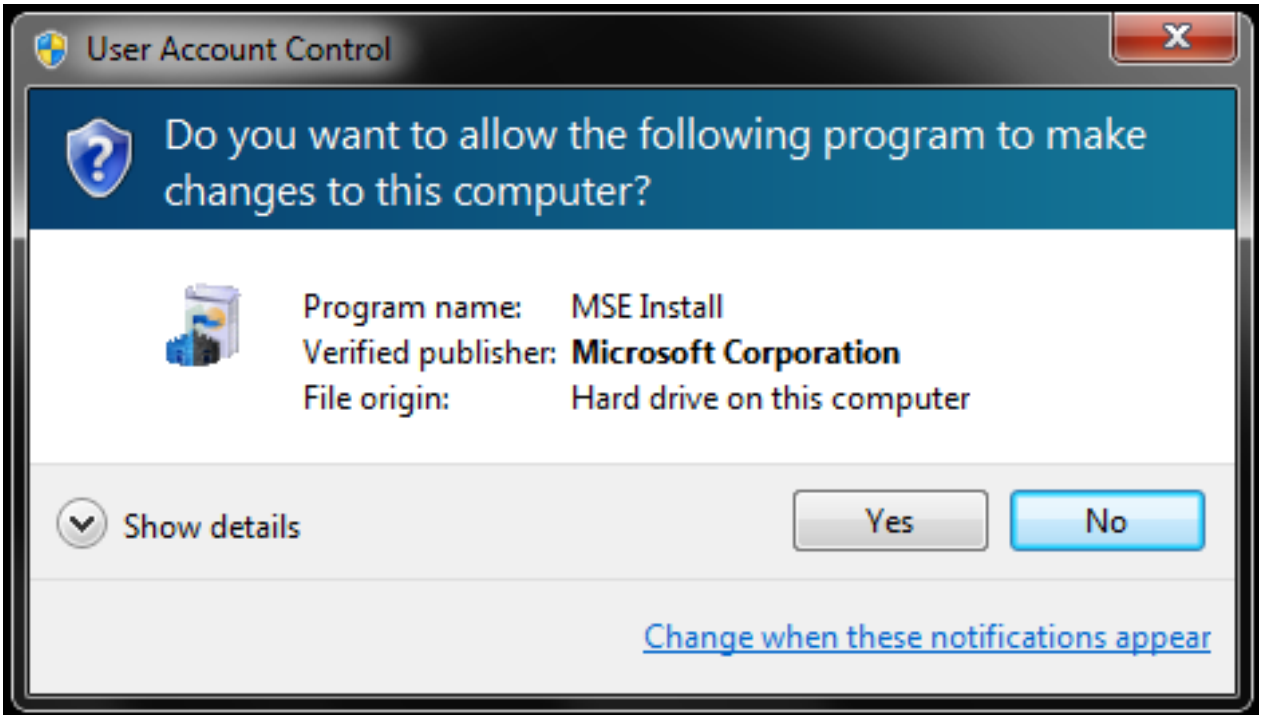
Install Security Essentials

Once you have determined which operating systems version you have installed, download and install the corresponding version of Microsoft Security Essentials.

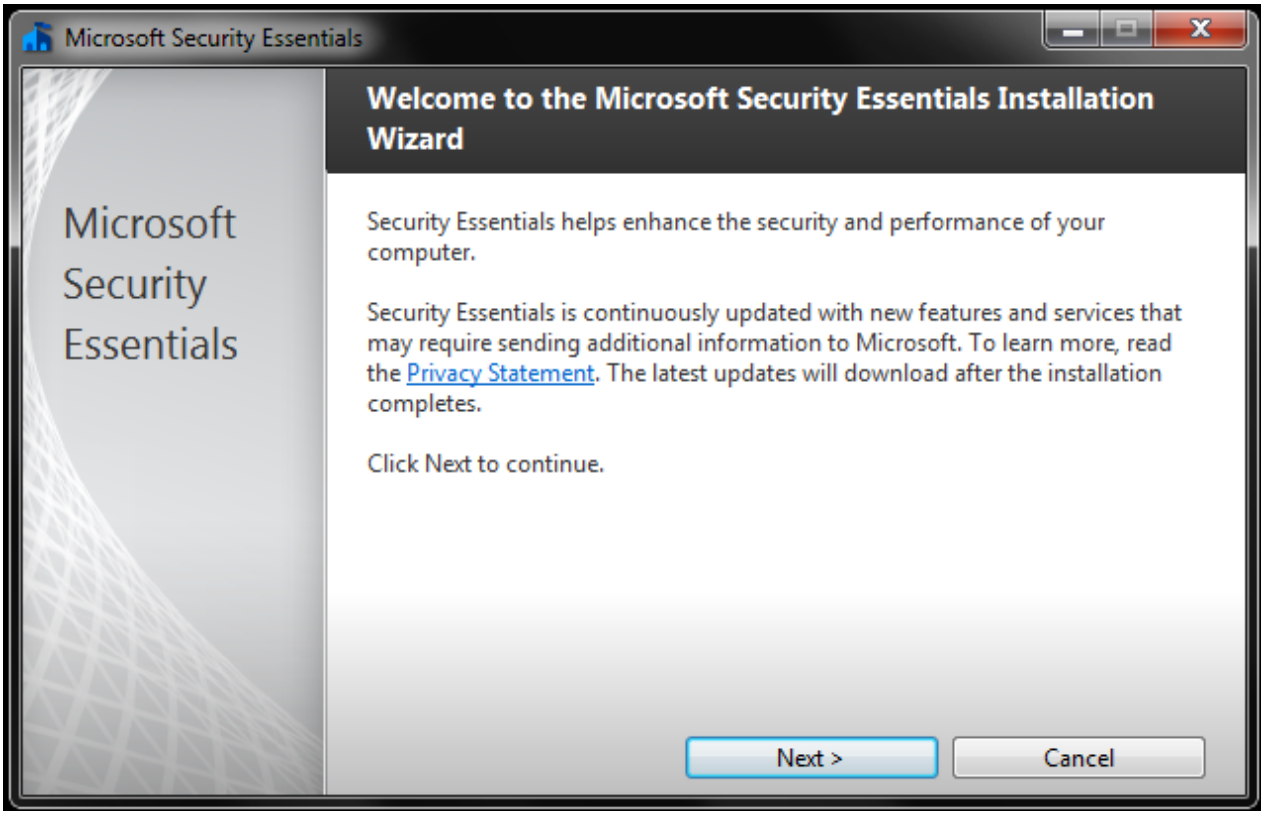
1. Download Microsoft Security Essentials from the Microsoft site.

- If your computer is running a 64-bit operating system, download the ENUS\amd64\MSEInstall.exe option.
- If your computer is running a 32-bit operating system, download the ENUS\x86\MSEInstall.exe option.

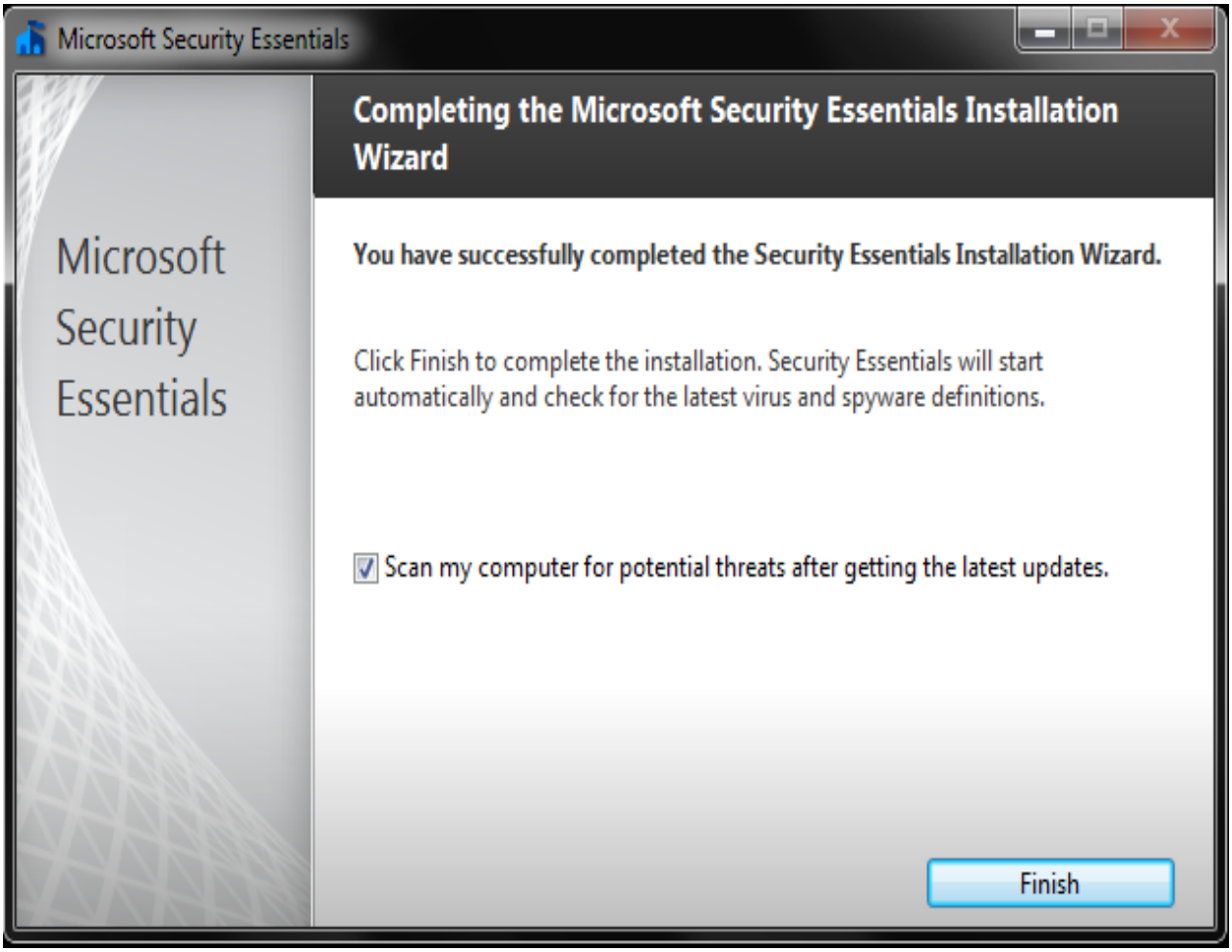
2. Once the download finishes, double-click the file to run the installer. You may get a pop-up box asking you to "allow the following program to make changes to this computer." Select Yes.



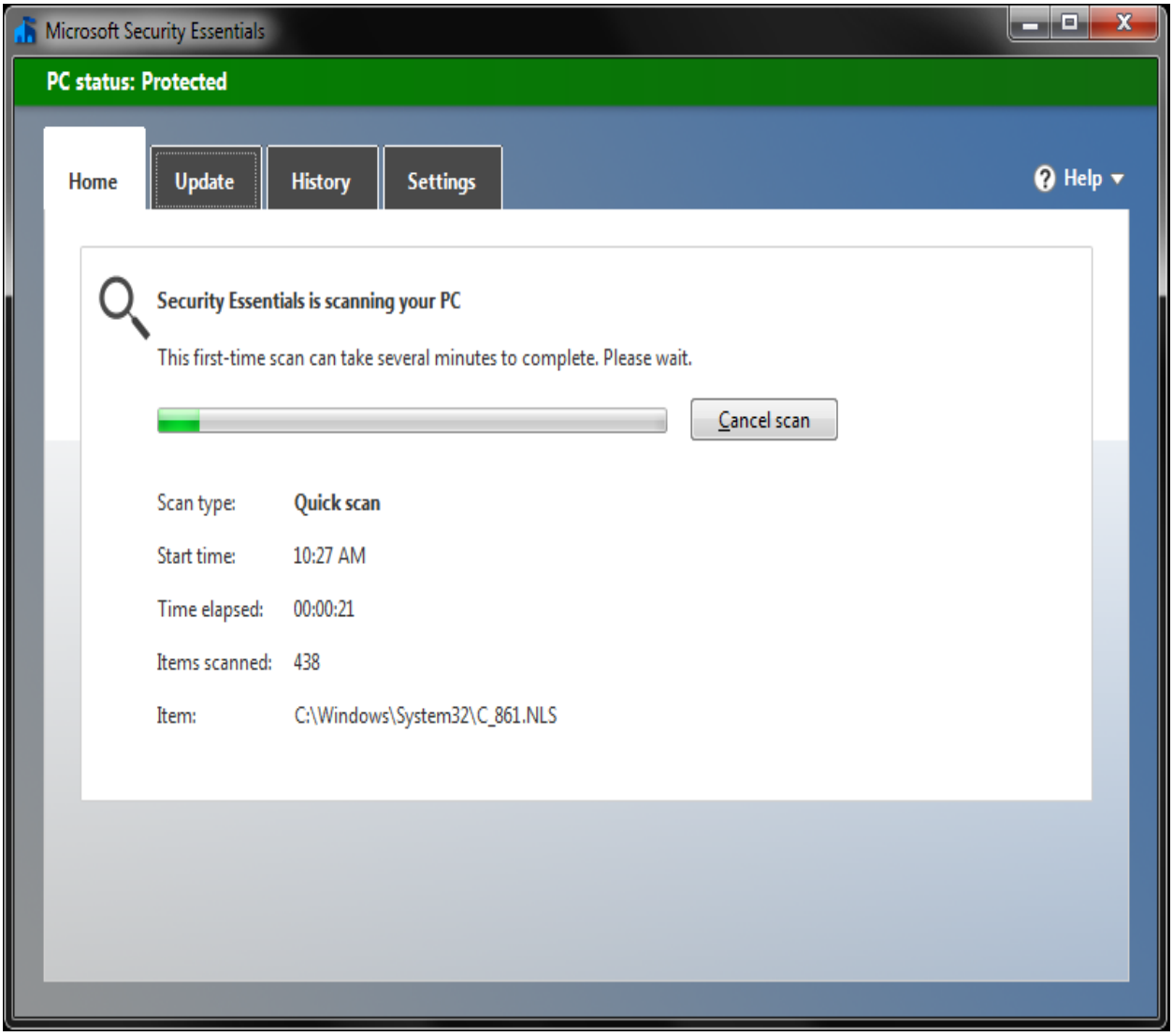
3. Once the installer extracts and runs, select Next



- Read through the Software License Terms, and select I Accept.
- Select Join the Customer Experience Improvement Program and then Next.
- Check the box for If no firewall is turned on, turn on Windows Firewall and select Next.
- Confirm that you don't have any other anti-virus programs installed, then select Install.
- When the program successfully installs, you should see the message, You have successfully completed the Security Essentials Installation Wizard.



9. Select Finish, and allow Microsoft Security Essentials to perform an initial scan of your computer.



Observation: Microsoft Security Essentials scanned for virus and protect the system from intruders