13.6.5 Windows Defender Facts

Windows Defender helps protect against slow performance and malware-caused security threats. Like most other anti-malware engines, Windows Defender uses definition files to identify harmful software. Windows Defender provides the following features to protect your computer:

Feature	Description
Scheduled Scanning	Scheduled scanning checks computer files for malware. Windows Defender can run three different types of scans: - A Quick scan checks file system locations that are most likely to be infected by spyware. - A Full scan checks all files in the file system, the registry, all currently running applications, and other critical areas of the operating system. - A Custom scan checks only the locations you specify. Windows Defender performs a quick scan at 2 a.m. each day. You can also manually initiate a scan, if necessary. The results of the scan are shown in the Home tab in Windows Defender.
Offline Scanning	Offline scanning causes the system to reboot and Windows Defender to run a scan in an offline state before returning to Windows. This allows some types of malware to be removed that normally can't be removed from a running system..
Real-Time Protection	Real-time protection alerts you when spyware or potentially unwanted software attempts to install itself or run on your computer. It also alerts you when programs attempt to change important Windows settings. Real-time protection uses security agents to monitor specific system components and software.
Cloud-Based Protection	Cloud-based protection provides real-time protection by sending Microsoft information about potential security threats discovered by Windows Defender. This feature requires automatic sample submission to be enabled.
Automatic Sample Submission	Automatic sample submission allows Windows Defender to send information to Microsoft for use in analyzing and identifying new malware.

Be aware of the following when working with Windows Defender:

- For best protection, keep the definition files up to date. By default, Windows Defender checks for new updates every time a system scan takes place. Windows Defender also uses Windows updates to automatically download definition files.
- Non-administrators can use Windows Defender to run scans.
- To run a program on the Quarantined Items list, you must restore it on your system. When you run it, Windows Defender will identify it again as a potential security threat. Select **Allow** to add the program to the list of allowed items so that you can run it in the future without a prompting.
- You can review past actions taken by Windows Defender through the History tab. You can also check for Windows Defender events in Event Viewer.
- In a corporate environment, use Group Policy to manage Windows Defender settings on domain members.
- If a third-party anti-malware scanner is installed on the system, Windows Defender may need to be disabled.