



2010 NIST Special Publication 800-115

Guidance for Assessing and Improving the Security of Windows Operating Systems

1. Introduction
This document provides guidance for assessing and improving the security of Windows operating systems. It is intended for system administrators and security professionals who are responsible for maintaining the security of Windows-based systems. The document covers the following topics:

- 1.1. Overview of Windows Security
- 1.2. Security Assessment Tools
- 1.3. Security Configuration Guidelines
- 1.4. Incident Response Procedures

2. Security Assessment Tools
This section discusses various tools used for assessing the security of Windows operating systems. These tools help identify vulnerabilities, misconfigurations, and other security issues. Some of the tools mentioned include:

- 2.1. Windows Security Center
- 2.2. Windows Defender
- 2.3. Windows Firewall
- 2.4. Windows Update



3. Security Configuration Guidelines
This section provides detailed guidelines for configuring Windows operating systems to enhance their security. These guidelines cover various aspects of system configuration, including:

- 3.1. User Account Control (UAC)
- 3.2. Windows Firewall Settings
- 3.3. Windows Defender Settings
- 3.4. Windows Update Settings
- 3.5. Windows Security Center Settings

