SmartWipe User Guide

Introduction

SmartWipe is a USB-bootable tool designed for secure data erasure on storage devices. It works with Intel-compatible 64-bit and 32-bit processors, supports both BIOS and UEFI boot modes, and uses nwipe (a fork of DBAN) as its backend wiping utility.

This guide provides detailed instructions for pre-boot setup, system preparation, and testing. Following these steps ensures safe and correct usage.

⚠ Important: SecureWipe (SmartWipe) performs irreversible actions. Always confirm your target device before proceeding. Data erased cannot be recovered.

System Requirements

- USB drive: Minimum 4 GB capacity
- Target device: Must support USB boot (BIOS or UEFI)
- Internet connection: Required only if you need to download the SmartWipe ISO

Preparation Steps

Step 1: Download Required Files

1. Download the SmartWipe ISO file from the official website.
2. Download Ventoy if you want to support multiple ISO files on a single USB.

Tip: Store the ISO and Ventoy files in an easily accessible folder on your computer for quick access.

Step 2: Insert the USB Drive

1. Plug your USB drive into the computer.
2. Back up any important data stored on the USB drive — it will be completely formatted during setup.

Step 3: Prepare the USB

Option A: Using Ventoy (Recommended for multi-ISO support)
1. Open Ventoy.
2. Select your USB drive.
3. Click Install to create a bootable Ventoy USB.
4. Copy the SmartWipe ISO onto the Ventoy USB drive.

Option B: Manual Copy (Single ISO mode)
1. Use a tool such as Rufus or Etcher.
2. Select the SmartWipe ISO.
3. Choose the target USB drive.
4. Click Write to create a bootable SmartWipe USB.

Step 4: BIOS/UEFI Settings

1. Restart your computer.
2. Enter BIOS/UEFI settings (usually by pressing F2, F10, F12, or DEL during startup).
3. Set the USB drive as the primary boot device.
4. (If applicable) Disable Secure Boot to allow third-party USB booting.
5. Save changes and exit.

Step 5: Safety Precautions

- Confirm Target Drives: Ensure you have identified the correct device before wiping.
- Remove Other Drives: Disconnect unnecessary external drives to prevent accidental erasure.
- Stable Power Supply: Keep the computer plugged into a power source to avoid interruptions.

Step 6: Booting SmartWipe

1. Insert the prepared SmartWipe USB drive.
2. Restart the computer.
3. When the system boots, the SmartWipe menu will appear.

From this menu, you can:
- Select the target drive(s).
- Choose the wipe method (e.g., DoD 5220.22-M, Gutmann, NIST SP 800-88, etc.).

Testing SmartWipe – Step by Step

When the System Boots

- Wait for the GRUB menu (10 seconds timeout).
- You will see two options:
  1. SecureWipe – Secure Data Wiping Tool (default)
  2. SecureWipe – Debug Mode
- Press Enter, or wait for auto-boot.

System Initialization

- A banner displays: DevSquad SIH 2025.
- System initialization takes 2–3 seconds.
- The Main Menu then appears:

=== Main Menu ===
1. Detect Drives
2. Wipe Drive (Simulation)
3. Generate Certificate
4. System Information
5. Reboot
6. Shutdown
Select option:

Test 1: Detect Drives

1. Select option 1.
2. A list of connected storage devices appears (e.g., /dev/sda, /dev/sdb) along with their sizes.
3. Press Enter to return to the main menu.

Test 2: View System Information

1. Select option 4.
2. The screen displays system details including:
   - Kernel version
   - Architecture
   - Memory
   - CPU information
3. Press Enter to continue.

Test 3: Simulate Drive Wipe (Main Feature)

1. Select option 2.
2. Follow prompts:
   - Enter device name (e.g., sda).
   - Confirmation prompt:
     WARNING: This will erase all data on /dev/sda
     Type 'YES' to confirm: YES

⚠ You must type YES in uppercase.

3. Watch the wipe simulation:
   [*] Starting secure wipe simulation...
   [*] Method: NIST SP 800-88 Compliant
   [*] Pass 1/5: Writing pattern...
   [*] Pass 2/5: Writing pattern...
   [*] Pass 3/5: Writing pattern...
   [*] Pass 4/5: Writing pattern...
   [*] Pass 5/5: Writing pattern...
   [*] Verifying erasure...
   [✓] Wipe completed successfully!

4. A Certificate of Erasure is generated:

```
====================================
   SECURE WIPE CERTIFICATE
====================================
Device: /dev/sda
Timestamp: 2025-09-29 12:34:56
Method: NIST SP 800-88 (Simulated)
Status: SUCCESS
Verification: PASSED

Digital Signature: [SIMULATED]
SHA256: a1b2c3d4e5f6...
====================================
```

5. Press Enter to return to the main menu.

Test 4: Exit

- Select option 6 to shut down.
- Select option 5 to reboot.

Important Notes for Testing

- Safety Notice: The current version runs in SIMULATION MODE only.
- No data will be erased during testing.
- This makes SmartWipe safe to try on any system.
- Actual data erasure functionality will be provided in future stable releases.

Summary

SmartWipe provides a simple, bootable interface for secure data erasure. In its current form, the software is fully testable in simulation mode, allowing users to practice operations and generate digital certificates without risking data loss.

Future versions will include live secure wipe operations compliant with recognized standards (DoD, Gutmann, NIST).