

Copilot

To **harden** your **Ubuntu** operating system in accordance with the **CIS benchmarks**, follow these steps:

1. Understand the CIS Benchmarks:

- Familiarize yourself with the **CIS Ubuntu Linux Benchmarks**. These guidelines provide secure configuration recommendations for Ubuntu systems.
- You can download the latest CIS Benchmark for Ubuntu in **PDF format** from the [CIS website](#) .

2. Assess Your System:

- Use tools like **CIS-CAT Pro** to scan your system against the CIS Benchmark. This will help you identify areas where your system conforms or deviates from the secure configuration recommendations.
- Ensure you have the appropriate **CIS Benchmark version** for your Ubuntu release (e.g., 22.04 LTS, 20.04 LTS, etc.) .

3. Automate Hardening Efforts:

- Consider using **CIS Build Kits** to automate hardening tasks. These kits provide **Group Policy Objects (GPOs)** for Microsoft Windows and **Bash shell scripts** for Unix and Linux environments.
- The **CIS Hardened Images** are pre-configured VM images that align with the CIS Ubuntu Linux Benchmark. You can use these images to create secure virtual machines .

4. Implement CIS Benchmark Recommendations:

- Some key recommendations include:
 - **Removing non-secure programs**
 - **Disabling unused filesystems**
 - **Disabling unnecessary ports or services**
 - **Auditing privileged operations**
 - **Restricting administrative privileges** .

5. Stay Updated:

- Regularly check for updates to the CIS Benchmarks and apply them as needed.
- Leverage **Canonical's automation tooling**, such as the **Ubuntu Security Guide (USG)**, to facilitate the application of these benchmarks .

Remember that **security is an ongoing process**. Regularly review and adjust your system's configuration to stay protected against cyber threats.  