

Copilot

To establish secure access control for **MySQL** on **Ubuntu**, following the **CIS (Center for Internet Security)** benchmarks is crucial. These guidelines provide prescriptive recommendations for securing your MySQL installation. Here's how you can set up access control securely:

1. Download the CIS Benchmark:

- Obtain the **CIS Oracle MySQL Enterprise Edition 8.0 Benchmark**.
- This document offers guidance for establishing a secure configuration posture for **MySQL Enterprise Edition 8.0** on Ubuntu Linux (but it applies to other Linux distributions as well).

2. Review the Benchmark:



- Familiarize yourself with the recommendations related to **access control**.
- Understand the best practices for user authentication, authorization, and privilege management.

3. Implement Access Control Measures:

- **Root User:** Change the default **root** password and restrict its usage.
- **User Accounts:** Create separate user accounts for different purposes (e.g., application-specific users, administrators).
- **Principle of Least Privilege:** Assign minimal privileges to each user account. Avoid granting unnecessary permissions.
- **Password Policies:** Enforce strong password policies for user accounts.
- **Host-Based Authentication:** Configure MySQL to allow connections only from trusted hosts.
- **SSL/TLS Encryption:** Enable SSL/TLS for secure communication between clients and the MySQL server.
- **Audit Logging:** Enable MySQL's audit plugin to track user activity.

4. Regularly Review and Update:

- Security is an ongoing process. Regularly review the CIS Benchmark and update your access control configurations as needed.

Remember that adhering to these security practices will enhance the protection of your MySQL database on Ubuntu.  

For detailed steps and specific configuration settings, refer to the **CIS Oracle MySQL Enterprise Edition 8.0 Benchmark**. It provides comprehensive guidance tailored to MySQL security.