Shadow Password Files - what they are, why they protect logins, and safe basics

Gridinsoft Help Center

What it is

Shadow password files are special system files on Unix/Linux that store the password hashes (not the actual passwords) for user accounts. Public info about users lives in /etc/passwd, while the sensitive, hashed passwords are kept in /etc/shadow, which only the system (root) can read. Hashes are salted and created with strong algorithms, so even if someone sees them, they can’t easily turn them back into your password.

Why it matters

Keeping hashes in a locked-down file makes it much harder for attackers or nosy apps to steal logins. If the system is set up right, regular users - and most programs - can’t read the password data at all.

How it works

- When you set a password, the system makes a salted hash and stores it in /etc/shadow.

- Login tools check your password by hashing what you typed and comparing the result - your real password is never stored.

- File permissions keep /etc/shadow off-limits to everyone except the system.

Red flags

- Password hashes showing up in /etc/passwd (they should not be there).

- /etc/shadow readable by non-admins (wrong permissions).

- Lots of failed login attempts or unknown users appearing.

- Manual edits to these files by someone who isn’t an admin.

Do it right

- Don’t hand-edit /etc/passwd or /etc/shadow; use system tools like passwd, useradd, usermod.

- Keep default permissions on /etc/shadow (system-only access).

- Use strong, unique passwords and a password manager; enable MFA if offered.

- Remove/lock accounts you don’t use and keep the system updated.