Kerberos - What it is, how tickets work, and setup best practices

Gridinsoft Help Center

What it is

Kerberos is a ticket-based login system that lets users and services prove who they are on a network without sending passwords. It uses a trusted Key Distribution Center (KDC) to hand out encrypted tickets so both sides can verify each other safely. Common in Windows domains and many enterprise apps.

Why it matters

Kerberos gives you strong, mutual authentication and reduces password exposure on the wire. That means fewer chances for credential theft and easier single sign-on across company services.

How it works - quick tour

- Sign in once: you authenticate to the KDC and receive a Ticket-Granting Ticket (TGT).

- Ask for access: when you open an app, you request a service ticket from the KDC.

- Prove and connect: your device shows the service ticket to the app, which verifies it and lets you in.

- Time bound: tickets expire, limiting damage if one is stolen.

Quick notes

- Kerberos uses symmetric encryption under the hood.

- Modern deployments prefer AES, not the older DES.

- Accurate time sync is required or logins can fail.

Best practices

- Enforce strong passwords and MFA where supported.

- Keep domain controllers and clients patched and clocks in sync.

- Limit service account privileges and rotate keys regularly.

- Monitor for suspicious ticket use, like Pass-the-Ticket attempts.