What is the Protected Users group?

Protected Users is a built-in Active Directory security group that applies non-negotiable credential protections to its members: it blocks NTLM authentication, disables weak RC4 and DES Kerberos encryption, prevents the account from being delegated, and stops credentials from being cached on machines. The effect is to shrink the attack surface of privileged accounts, blunting Pass-the-Hash, delegation abuse, and credential theft, with the trade-off that members must use Kerberos-compatible, modern access paths.

HOW IT WORKS

01 How to use it

- Add Tier 0 and other highly privileged accounts to Protected Users, after validating they do not depend on NTLM, delegation, or credential caching.
- Combine with Credential Guard and LAPS for layered protection.
- Do not add service accounts blindly, since many rely on the very features the group disables.
- Confirm a modern, Kerberos-only access path for every member.
- Review membership regularly as privileged accounts change.

HOW TO DEFEND

- No NTLM: members can only authenticate with Kerberos.
- No weak Kerberos crypto: RC4 and DES are refused, only AES is used.
- No delegation: the account cannot be delegated (constrained or unconstrained).
- No credential caching: the account's credentials are not cached on the machines it logs in to, and it gets shorter ticket lifetimes.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Kerberos Authentication Overview

[3] NIST SP 800-115 Technical Guide to Security Testing

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-protected-users-group

Open online