ManageEngine
Password Manager Pro

8 Must-dos for a Perfect Privileged Account Management Strategy

The experts agree:
Privileged account management (PAM) is one of the top security projects for organizations. With that in mind, here's a set of 8 must-dos that every head of IT should implement to drive a strong PAM program.

01 Bring all your privileged accounts under one roof.

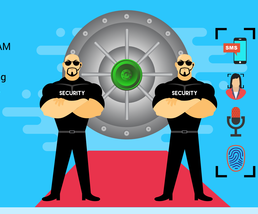
Run a fully automated program that regularly scans your network, detects new accounts, and adds them to a central vault. To prevent undesired access, reinforce protection around the vault with well-known encryption algorithms such as AES-256.

02 Decide who can access what.

Chart well-defined roles with minimum required access privileges for the members of your IT team, and ensure that all activities around the vault are traceable to authorized employees.

03 Combine something you know with something you have.

Implement multi-factor authentication for both PAM administrators and end users to ensure that the person logging in is who they claim to be. Knowing a password is no longer enough to keep sensitive resources secure.



04 Think before you share.

Provide employees or contractors access to IT assets without disclosing credentials in plaintext. Allow users to launch one-click connections to target devices from your PAM tool's interface, without viewing or manually entering the credentials.

05 Start automatically resetting passwords.

Make automatic password resets an integral part of your PAM strategy. Replace default, unchanged passwords with strong, unique passwords that are regularly reset.

06 Foster a need-to-know culture.

Require users to send a request to your organization's PAM administrator whenever they need specific account credentials to access a remote asset. You can also provision users with temporary, time-based access to these credentials, and automatically reset the credentials once the stipulated time expires.

07 Let APIs do the talking.

Use secure APIs to allow applications to query your PAM tool directly and retrieve privileged account credentials to communicate with another application or a remote asset.

08 Make sure everything is audited.

Capture every single user operation and establish accountability and transparency for all PAM-related actions. Go a step further and integrate your PAM tool with an event logging tool and consolidate PAM activities with other events from the rest of your organization to receive intelligent tips about unusual activities.