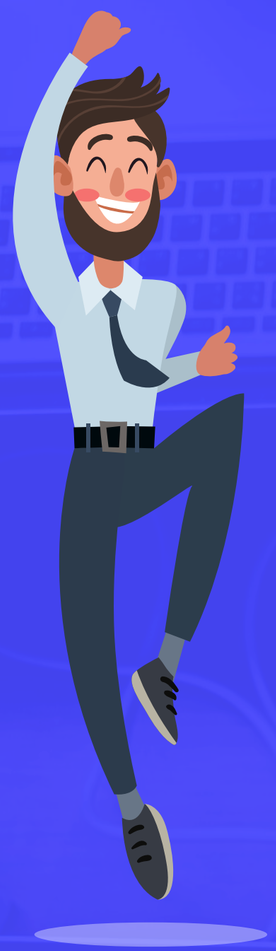
ManageEngine
AD360



AD admin's guide for effective permissions management and reporting




A comprehensive Active Directory management and reporting solution.

Getting started.

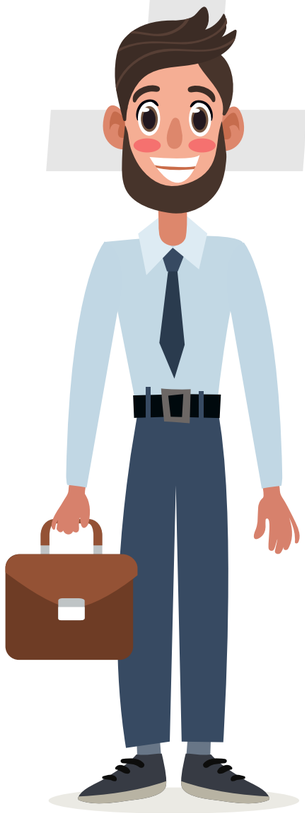
A planned approach to secure permissions assignment.

tip #1

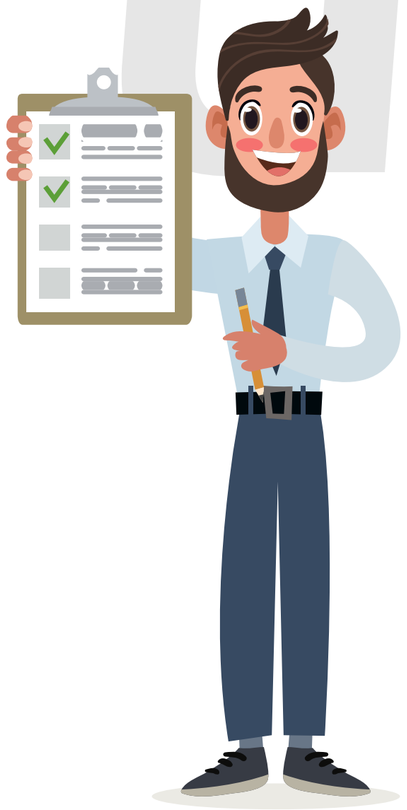
Numerous research studies have revealed that, ***insider threats*** *are estimated to be the single biggest cause for security attacks. They can go undetected for years as it is hard to distinguish harmful actions from regular work.*

Establish the ***principle of least privilege*** *to restrict the occurrence of insider attacks. Grant users access to only those systems and data that pertains to their job. Maintain a quick reference sheet for all access lists on your file servers.*

Learn more *on how to granularly manage Active Directory share permissions with group/OU based access restrictions.*



tip#2



Admins need to have ***complete visibility of share and folder permissions, permissions inheritance*** *and should have the capability to drill down to granular details to ensure total security of their organization.*

Compliance standards like ***GDPR, GLBA, PCI etc., require comprehensive auditing of access and share permissions****. Often reports of file share permissions granted to specific groups or a particular user come in handy.*

Learn more *on how to generate reports on access permissions of all NTFS folders, files and their properties, and ensure compliance to IT standards.*

Staying compliant with ease.

Track and report on changes to access permissions.

tip#3

Plug security loopholes.

Prevent data leaks and don't pay a ransom.

*Often **permissions are set too broadly**—to the delight of hackers and internal data thieves. Admins are generally not equipped to track the changing roles of workers, organizational changes that modify group authorizations, and job terminations.*

*Rather than working on an ad-hoc basic, it's important for admins to **have a foundational policy**—the simpler the better.*

***Learn more** on how to monitor critical accounts and their access permissions; perform root cause analysis with provision to **search ACEs**, and modify or instantaneously revoke all permissions on the occurrence of a data leak.*

https://www.manageengine.com/active-directory-360/

ManageEngine

tip#4

Users are often tempted to act on opportunities to swindle business critical data when given ***access over an unrestricted time frame.***

Folder owners can ***create workflow requests to securely share folders and files*** *with permissions that range from full control to simply listing the folder's contents. Active Directory administrators can then access all these requests, and approve or reject from a single dashboard.*

Learn more *on how to configure* ***time-restricted folder sharing****, eliminating the need to revisit the permission settings to extend or roll-back the sharing of resources.*

Harden data security.

Easy, safe, and time-restricted file sharing.

https://www.manageengine.com/active-directory-360/

ManageEngine

ManageEngine
AD360

About AD360

AD360 is an integrated solution that takes care of identity and access management, IT compliance, and security of your AD, Exchange, and cloud applications. It supports user life cycle management; multi-platform user provisioning; single sign-on for cloud applications; password self-service; real-time auditing, monitoring, and alerting; and pre-packaged compliance reports. AD360 also allows you to automate or delegate common administrative tasks to help desk technicians while still retaining control through approval workflows. For more information about AD360, visit https://www.manageengine.com/active-directory-360/

$ Get Quote

Download

30-day trial and try this feature now.