ManageEngine
ADManager Plus

4 tips

AD admin's guide for effective permissions management and reporting

Get started right away

Stay compliant with ease

Plug security loopholes

Harden data security

Getting started.

A planned approach to secure permission management.

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

To prevent the occurrence of insider attacks, implement the ***principle of least privileges***. Grant users access to only those systems and data that pertain to their job. Maintain a quick reference sheet for all access lists on your file servers.

Learn more on how to ***granularly manage share permissions*** with group- or OU-based access restrictions.

tip#2

Admins need to have c**omplete visibility of share and folder permissions and permissions inheritance.** *They also require the capability to drill down to granular details to ensure total security of their organization.*

Compliance standards like **GDPR, GLBA, PCI DSS, and more** *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 for IT auditing.*

Learn more *on how to generate reports on access permissions of all NTFS folders, files, 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**, like access to an entire file server instead of a specific file or folder -- much to the delight of hackers and internal data thieves. Admins are generally not equipped to track the changing roles of users, organizational changes that modify group authorizations, and job terminations.

Rather than working on an ad-hoc basis, it's important to have a foundational policy that specifies **to who, how and within what time-frame** should share permissions be granted.

Learn more on how to **monitor critical accounts and their access permissions**; assist in root cause analysis with provisions to **search ACEs**, and modify or instantaneously revoke all permissions in case of a data leak.

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 share folders and files** with permissions that range from full control to simply listing the folder's contents over a designated time frame. Active Directory administrators can then process all these requests, and approve or reject from a single dashboard.

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

Harden data security.

Easy, safe, and time-bound file sharing.

About ADManager Plus

ADManager Plus is an integrated solution that takes care of identity and access management, and security of your AD, Exchange, and cloud applications. It supports user life cycle management; multi-platform user provisioning; and pre-packaged compliance reports. ADManager Plus 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 ADManager Plus, visit

https://www.manageengine.com/products/ad-manager/

$ Get Quote   ⤓ Download

30-day trial and try this feature now.