ManageEngine
ADManager Plus

5 Active Directory mistakes that can ruin your enterprise's security efforts

www.admanagerplus.com

Security threats from external sources should be a constant concern for any organization. However, most organizations don’t even realize that today’s most damaging security threats are coming from within organizations. It's time for the IT industry to step-up the security game by identifying common pitfalls in managing Active Directory (AD) and taking relevant measures to plug security gaps.

Here are the top five mistakes in AD management that are too costly to ignore along with ADManager Plus' solution for each of them.

Mistake 1

Granting excessive permissions to users or groups.

One way to keep permissions as simple as possible is to grant full control permissions to every user. However, doing so would be a recipe for disaster. Any user receiving more permission than they need—like permissions to view, modify, or delete sensitive files—can lead to data loss, breaches, incorrect modifications, and more. Rather than providing full permissions to each user, a recommended best practice is employing the principle of least privileges: only grant the minimal amount of privileges that each user needs to complete their work. To further reduce risks, administrators should review permissions of users and groups before granting them any new permissions. Additionally, granting permissions to users on a temporary basis is a great way to ensure that permissions aren't misused at a later point in time.

ADManager Plus can help you granularly assign permissions to users and groups for a specified period of time. You can also view which permissions are granted to each user and group, and modify them accordingly using preconfigured reports.

Mistake 2

Assigning group memberships incorrectly.

When users are added to groups in AD, they might be indirectly added to top-level security groups due to nested group memberships. Generally, group memberships are assigned at the time of user provisioning and are only modified for limited occasions like a promotion or a transfer to different department or location. However, before reassigning memberships, it's recommended that you run a report, identify each user's group memberships, and revoke inappropriate permissions. Role-based templates will come in handy when you want to assign users to groups based on their designation or team.

ADManager Plus provides detailed reports on groups, clearly showing which nested groups each user, group, contact, and computer belongs to.

Mistake 3

Failing to clean up stale accounts.

When an employee leaves an organization, their account should be stripped of its privileges, then deprovisioned; if this isn't done, that ex-employee's account will become stale. Malicious insiders could leverage stale accounts to access your organization's resources. Additionally, software licenses are costly, so administrators should free-up licenses from unused accounts and reassign them to active users. You need to periodically identify inactive user accounts and apply a deprovisioning policy to keep your AD clean.

ADManager Plus allows you to automatically identify stale accounts, strip them of their group memberships, revoke all their permissions, remove Office 365 licenses, and delete or disable them. Learn how ADManager Plus simplifies deprovisioning with its delete and disable policy.

Mistake 4

Delegating tasks without specifying appropriate boundaries.

Delegation can get tricky when you're using the built-in delegation control wizard. When users are granted permissions to perform certain actions in AD such as creating users or resetting their passwords, enforcing necessary restrictions becomes essential so that permissions aren't misused by those users.

With ADManager Plus, you can securely delegate permissions to the help desk without actually elevating their permissions in AD. ADManager Plus also has help desk audit reports to track help desk technicians' actions. Learn more.

Mistake 5

Making data entry errors.

User provisioning is often a long-winded, manual process. Onboarding can't go smoothly if new users are added to the wrong groups, assigned incorrect licenses, or had their home folders or profile path misconfigured. Similarly, user modifications based on events such as changes to their location, role, or designation mean that administrators have to spend time and effort reexamining the existing permissions of the user to make any necessary changes, leaving plenty of room for error.

ADManager Plus offers customizable rule-based templates that have pre-loaded values based on department, location, or designation, which makes user account management a breeze for IT administrators.

ManageEngine
ADManager Plus

ADManager Plus is an identity governance and administration (IGA) solution that simplifies identity management, ensures security, and improves compliance. With ADManager Plus, manage the user life cycle from provisioning to deprovisioning, run access certification campaigns, orchestrate identity management across enterprise applications, and protect data on your enterprise platforms with regular backups. Use over 200 reports to gain valuable insights into identities and their access rights. Improve the efficiency of your IGA operations with workflows, automations, and role-based access control policies. ADManager Plus' Android and iOS applications help with on-the-go AD and Azure AD management. For more information about ADManager Plus, visit manageengine.com/products/ad-manager/.

$ Get Quote

⤓ Download