ManageEngine
ADManager Plus

5 tell-tale signs you're heading for a COMPLIANCE VIOLATION

www.admanagerplus.com

Overview

When it comes to managing users' identities and access rights, Active Directory (AD) plays a vital role. Changes made in AD not only impact an organization's security, but they also affect its compliance with IT regulations. It's no surprise that compliance auditors are keen to review the activities carried out in AD.

The penalty for noncompliance can result in hefty fines, as well as a loss of customer trust for organizations. It's best to proactively and regularly check your organization's compliance posture to avoid the last minute jitters you might experience from a compliance audit.

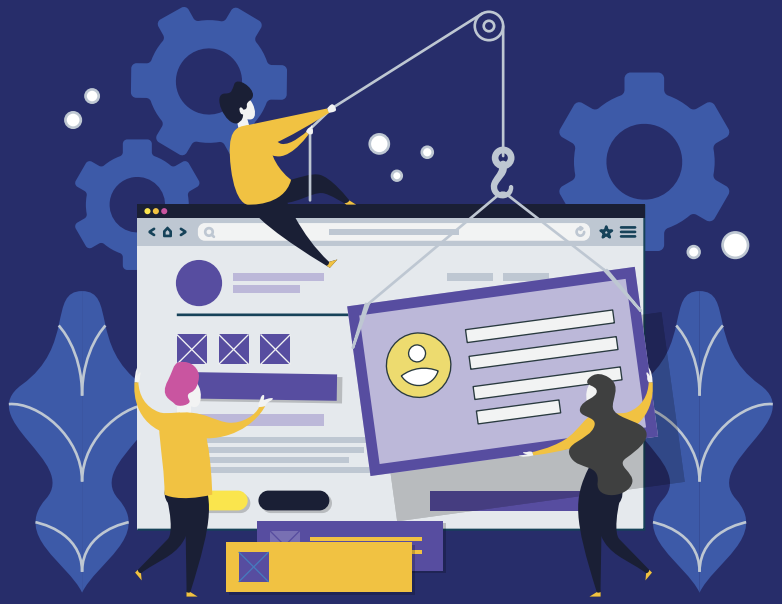
Sign 1

NO CHANGE MANAGEMENT SYSTEM

Making changes in AD permissions without having them reviewed first can unintentionally expose sensitive business data to security vulnerabilities. It's essential to have an access control policy in place for every critical action in AD to prevent users from gaining unauthorized privileges. The best course of action is to follow a review process where every user change request is evaluated by a manager before it's transferred to an IT admin. Each request, such as access to crtical shares or changes to group membership, must be reviewed by an IT manager or team lead to ensure that enterprise resources are not compromised

ManageEngine's ADManager Plus enables customizable workflows that help you streamline and monitor AD tasks. With this capability, users can raise requests to access resources which can be reviewed by a designated authority before the IT admin executes the task.

LEARN MORE



Sign 2

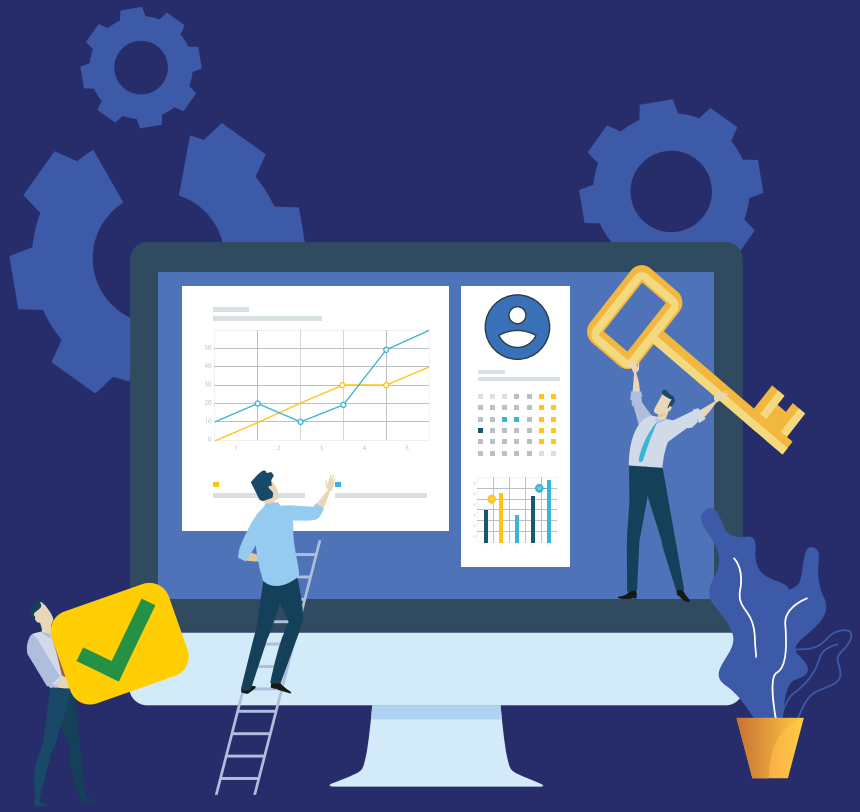
NO ROLE-BASED PRIVILEGES

IT admins routinely create user accounts, assign them relevant permissions, and modify existing privileges. If there is no checklist containing user access details by department, IT admins will not be able to grant permissions to users uniformly. Sometimes, users are added to the wrong groups, which can lead to users having excessive permissions or less privileges than required for their role.

For example, an employee in marketing and an employee in HR must each have permissions for different resources specific to their role. Similarly, when users are being transferred to a different location, they should be given access to resources that their job demands and nothing more.

ADManager Plus has customizable templates to streamline the creation and modification of AD objects; you can also define rules and attributes based on security groups, logon hours, and contact details that can be updated automatically based on department or role.

LEARN MORE

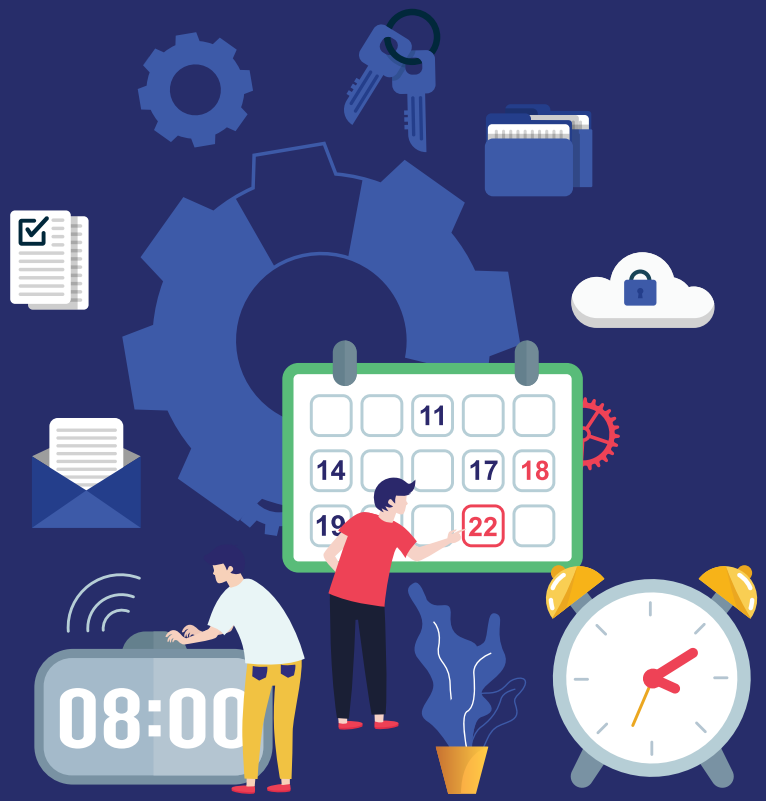


Sign 3
PRIVILEGE CREEP

When users join the organization, IT admins grant them permissions to access resources relevant to their job function. Over time, for different tasks or projects, users might be granted permission to different resources. These access rights should be revoked after the task is completed. It's a good practice for IT admins to periodically review all user access rights by role against a checklist of permissions. Users might have access to top-level security groups or critical folders and files that is no longer necessary for their role. Periodically tracking all permissions assigned to users for a specific project and revoking them after the project is completed resolves this problem; however, this task can be tedious.

ADManager Plus offers an automated time-bound group permissions management feature so IT admins can assign users to specific groups and revoke them after a specified period of time. Additionally, the tool provides predefined reports on NTFS and Share permissions so you can identify servers and shares in your organization, and verify the level of access each individual user or group has for them.

LEARN MORE



Sign 4
LACK OF PERIODIC REVIEW

Are you preparing reports for compliance officers last minute? It's essential to identify unauthorized access to critical files and folders well in advance so that you can take corrective steps and avoid non-compliance issues. A recommended best practice is to periodically check access permissions. If you don't have information about who can access sensitive folders and who resides in which security groups, it's only a matter of time before your organization's data security is at risk. Most native tools don't offer the flexibilty of obtaining granular AD information through reports. Real-time alerts about when a user account, security group, or a password is changed can prompt you to take immediate action.

ADManager Plus provides actionable, pre-defined reports for PCI DSS, SOX, HIPAA, GLBA, GDPR, POPIA and FISMA compliance regulations. You can also automate the entire compliance reporting process by scheduling reports to be sent to the key stakeholders responsible for managing compliance programs.

LEARN MORE

Sign 5

STALE ACCOUNTS BUILD UP

IT housekeeping is an important part of preventing attackers from gaining unauthorized entry to an organization's resources. Inactive user accounts and computers are entry points for cyberattackers looking to gain access to accounts with elevated permissions, or to remotely access sensitive files and financial data. It's also risky to leave security groups that grant permissions unprotected.

Using ADManager Plus, you can configure deprovisioning using an automation that identifies dormant objects, removes their privileges, moves them to a different container, and deletes their accounts. To simplify this process, the Disable/Delete policy feature in ADManager Plus enables you to remove associated Microsoft 365 and Google Workspace accounts, export the user's mailbox to a specified location, and revoke applicable software licenses.

LEARN MORE

Download a 30-day, free trial to try these features and enjoy all the benefits **ADManager Plus** offers.

$ Get Quote Download

Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus | M365 Manager Plus | RecoveryManager Plus

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/.