ManageEngine
ADManager Plus

Active Directory management challenges of 2021 and how to overcome them

Introduction

2020 tested organizations' cyber resilience like never before. When the COVID-19 pandemic sent shock waves across organizations of different industries and sizes alike, IT teams were forced to quickly come up with sweeping changes to enable remote work for employees and ensure business continuity.

This hasty move at unprecedented speed and scale paved the way for security vulnerabilities that were cleverly exploited by cybercriminals.

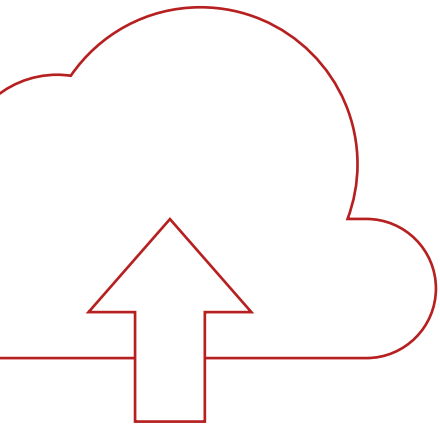
Now that organizations are comfortable with the new normal, it's time for IT teams to re-evaluate their strategies to discover if and where their old strategies fall short, and prioritize their efforts to plug any security loopholes waiting to be exploited by cybercriminals.

In this e-book, we'll discuss five Active Directory management challenges IT admins may face in 2021 and how to overcome these challenges using ManageEngine's ADManager Plus, a unified Active Directory, Exchange, and Microsoft 365 management and reporting solution.

Accelerating cloud adoptions

Forrester predicts that in 2021 remote work will rise to 300 percent of pre-COVID-19 levels. The increase in remote work will proportionately accelerate the cloud adoption rate of organizations worldwide. In the same report, Forrester also predicts that the global public cloud infrastructure market will grow 35 percent, reaching $120 billion in 2021.

What was once a "nice to have" for employees and organizations became a "must-have" during the pandemic, and this trend is expected to continue in the future.



According to a Gartner survey, 48 percent of employees will work remotely after the pandemic, compared to 30 percent pre-pandemic. Another Gartner survey revealed that 82 percent of company leaders plan to allow employees to work remotely at least some of the time.

In organizations that have employees both on-site and working remotely, it becomes a huge challenge for IT teams to adapt to managing a new, more complex hybrid workforce. Managing users across on-premises AD and the cloud-based Microsoft 365 creates unnecessary confusion, repetition, and delays.

IT admins have to juggle between multiple consoles to manage their AD, Exchange Server, and Microsoft 365 environments. This burdens the IT administrator and also increases the time taken to accomplish each task. Besides, using just Microsoft's native tools and PowerShell scripts to manage a hybrid environment only adds to the complexity.

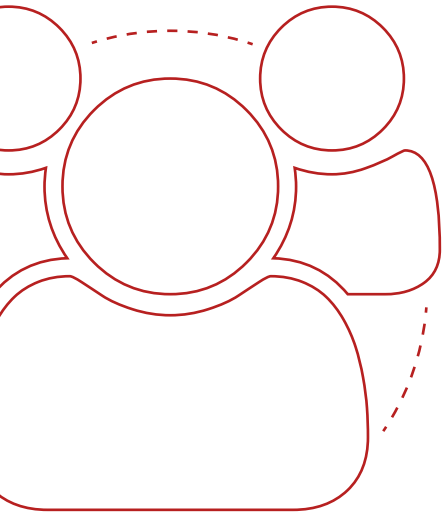
ADManager Plus empowers IT admins to manage and report on AD, Microsoft 365, and Exchange objects, all from a single, web-based console. This eliminates the unnecessary burden of struggling with multiple consoles and using PowerShell scripts.

Bottlenecks in the employee onboarding process

While industries such as aviation, retail, finance, real estate, and automotive are among the worst affected by the pandemic—resulting in record job losses—other industries such as healthcare are ramping up hiring to meet demand.

As organizations that shifted to remote work get increasingly comfortable with and reliant on their new setup day by day, the demand for digital tools enabling remote work is also expected to increase proportionately. The booming e-learning industry is another major reason the digital economy will see steady growth.

Also, the vaccine rollout and general optimism about the economy has led to a spike in hiring. Even companies that had to lay off employees due to COVID-19 may need to fill existing and new positions.



In most cases, during the onboarding process, the HR manager exports the user details in a CSV file from their human resource management system (HRMS) and shares the file with the IT team via email. The IT admin then creates new user accounts—either individually or in bulk using PowerShell scripts—and grants appropriate access to resources based on the role of the employee. This process creates unnecessary bottlenecks since it is challenging to ensure real-time collaboration between the HR department and the IT department. Also, creating user accounts manually is often tedious, time-consuming, and error-prone.

ADManager Plus' capability to integrate with HRMS applications helps overcome all the above challenges. Once the user details are entered in the HRMS application, you can use ADManager Plus to automatically provision accounts in AD, Microsoft 365, Exchange, Skype for Business, and Google Workspace. Also, any changes made in the HRMS application thereafter are reflected across all accounts in real time.

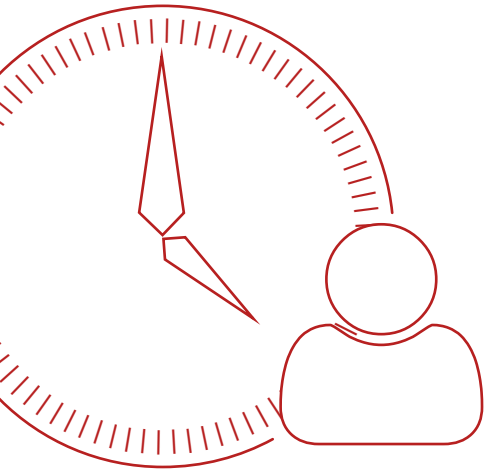
Increase in contingent workers

Gartner predicts that organizations will look to increase hiring of contingent workers to maintain more flexibility in workforce management post-COVID-19.

Although a contingent worker's tenure is limited, they must be given appropriate access to company resources based on their role and job function.

However, once their job is done and they are no longer part of the organization, all the access pertaining to their user account must be revoked and the account must be purged permanently. If this action is done manually on an ad hoc basis, there is a risk of account compromise attacks if the IT administrator forgets to delete the contingent worker's account.

The risk is higher if the account belonged to a privileged user.



This is why it's crucial to identify such inactive accounts and immediately purge them. However, the only way to ensure that all inactive accounts are removed immediately is by automating the process. While native AD has provisions to track down and eliminate inactive user accounts, it cannot remove them in bulk or automate the process.

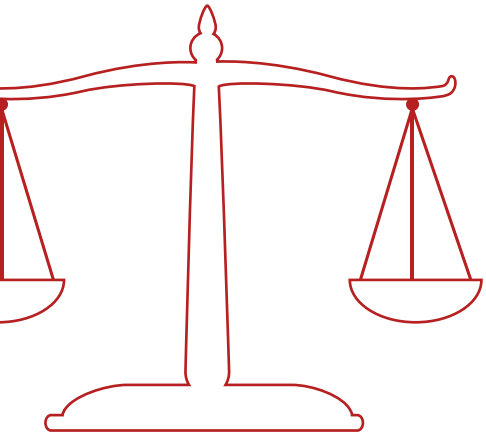
ADManager Plus lets you effortlessly report on all inactive user accounts, disabled user accounts, and expired user accounts. Right from these reports, you can delete or disable these accounts in bulk instantly. If required, you can also move them to a separate organizational unit, quarantine them for a desired period, and then delete them eventually. Best of all, you can automate these tasks and specify how often you want this automation to run.

Increased legal risk associated with expanded employee data collection

According to Gartner, even before the pandemic, organizations were increasingly using nontraditional employee monitoring tools to keep track of employee activities.

Organizations use passive tracking methods that include monitoring virtual clock-in and clock-out times; computer and work phone usage; employee emails, chats, and other internal communications; and employee location or movement. While some companies use this data to track productivity, others monitor employee engagement and well-being to understand employee experience better.

Gartner's analysis shows that this trend will only accelerate in 2021 given the increased adoption of remote work due to the pandemic.



However, with more employee data comes legal risk. Forrester predicts that regulatory and legal activity regarding employee privacy will double in 2021.

According to Forrester, while European regulators are already enforcing privacy rules to protect employees' personal data, countries such as Brazil, India, and Thailand will soon do the same. As for the US, the battle to determine what is a reasonable expectation of workplace privacy will be fought in the courts—as a result, employee privacy lawsuits will increase in 2021.

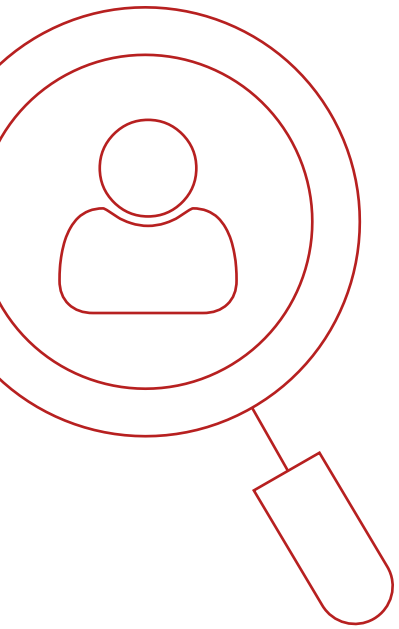
To ensure compliance with regulations such as SOX, HIPAA, PCI DSS, the GLBA, and the GDPR, organizations must have elaborate records of all the data collected on employees' day-to-day activities. Though becoming compliant with these regulations enhances security, it becomes tiring to stay compliant with them due to their stringent nature.

Much of the data these regulations pertain to involves organizational activities occurring in AD, but most organizations lack a comprehensive reporting system for activity in AD. Unfortunately, using native AD tools is highly laborious and time-consuming.

ADManager Plus has a comprehensive reporting system that can fulfill various compliance management needs. It delves into the core of Windows and AD to fetch data required for audit compliance. This data is exportable and presented in a user-friendly format with plenty of filters that allow you to view only the required data. You can conveniently extract and export any piece of information that is required to meet regulatory compliance mandates such as HIPAA, PCI DSS, the GLBA, SOX, and the GDPR.

New working conditions may drive up the risk of human error

Ensuring IT security has always been an ongoing challenge for security teams. The pandemic has made it an even greater challenge. As more and more employees have started working remotely, security teams are under extreme pressure to enable seamless collaboration among employees and ensure that the "new normal" working conditions do not create any security vulnerabilities.



Some organizations found themselves already equipped with the right technologies and protocols to sustain a sudden transition to remote work, while some organizations were forced to adopt remote work hastily to maintain business continuity. However, the scale at which this transition had to occur was certainly not anticipated by IT teams on either side.

As this is somewhat unfamiliar territory for IT teams that are already overburdened, mistakes are bound to happen. These mistakes could be an unintended modification or deletion that affects a single user, perhaps preventing them from logging in or accessing a file, or it could be an error that brings down the whole domain controller and affects multiple users at once.

These mistakes often lead to business disruptions and downtime that can cost a fortune. While you really can't eliminate these risks, having a reliable fail-safe mechanism in place can save a lot of time, productivity, and revenue loss due to downtime caused by security incidents.

With ADManager Plus, administrators can back up all changes in AD, however big or small. In the event of a security incident or a failure, AD can be easily restored to its original state without restarting the domain controllers. Additionally, it also helps in carrying out a full-blown inspection of your AD environment to diagnose what went wrong and why, with the help of predefined reports on recently modified users, AD management tasks performed by technicians, and more.

Our Products

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

ManageEngine ADManager Plus is a web-based Windows AD management and reporting solution that helps AD administrators and help desk technicians accomplish their day-to-day activities. With an intuitive, easy-to-use interface, ADManager Plus handles a variety of complex tasks and generates an exhaustive list of AD reports, some of which are essential requirements to satisfy compliance audits. It also helps administrators manage and report on their Exchange Server, Office 365, and G Suite environments, in addition to AD, all from a single console.

For more information about ADManager Plus, visit
www.manageengine.com/products/ad-manager/

ManageEngine
ADManager Plus

$ Get Quote

Download