ManageEngine
ADManager Plus

Saving IT from CYBERSECURITY BURNOUT

Table of **contents**

Introduction

most vulnerable

Humans are the weakest link in a software supply chain

With people being one of the key foundational pillars of cybersecurity along with processes and technologies, it is highly imperative for cybersecurity professionals to be resilient against their occupational hazards.

Fortifying a network involves an equal contribution from security tools and the people behind them. While technology can deliver the necessary capabilities, it's the people who ensure that they are optimized to detect, avert and prevent cyberattacks from happening in the future.

As an occupational hazard, cybersecurity professionals can be highly prone to operational stress and fatigue, as the job demands precise analytical ability, attention, and visual perception. If neglected, this cumulative pressure will lead to **cybersecurity burnout** amongst IT professionals.

Why must companies worry about cybersecurity burnout?

Ignoring cybersecurity burnout can make organizations more susceptible to threats and adversaries that leverage employee negligence, apathy, and error. With phishing and other **social engineering attacks** on the rise, organizations must prevent security and administrative teams from becoming weary and insensitive to cyber risks. Therefore, addressing burnout in cybersecurity must be a top priority for organizations as it can drastically affect their security posture.

Another reason for the growing concern over fatigue is its presence across hierarchies. Even C-suite have started to feel the pinch of burnout, as a 2019 report by Nominet revealed that:

18-24 months
is the average tenure period of Chief Information Security Officers (CISO) in the United States.

91%
of CISOs work under moderate or highly stressful conditions.

65%
of IT and security professionals considered quitting due to burnout and low visibility into their IT networks.

Besides contributing to higher attrition rates, cybersecurity burnout affects the efficiency of IT security teams during high-risk, mission-critical situations where failure can have devastating effects.

In short, burnout can expand an organization's attack surface.

Causes of cybersecurity burnout

Although the thresholds for burnout differ from person to person, and the concept requires holistic discussion, it's safe to say that technology and processes play a major role. The 2022 Voice of the SOC Analyst report by Tines revealed that:

64%

of security analysts agreed that spending time on manual processes is the most frustrating part of their work.

Reporting, monitoring, and detection are the top tasks consuming an analyst's time.

Some of the major factors contributing to operational friction and fatigue include:

Repetitive processes

Performing mundane, mechanical, and time-intensive tasks repetitively can tire security teams and make them vulnerable to errors, while deterring them from focusing on meaningful tasks that require higher cognitive functioning. With the human element turning out to be the biggest liability, organizations must simplify repetitive tasks.

Case in point:

Take user lifecycle management, an integral component of identity governance. Apart from onboarding and offboarding, managing employees' digital identity lifecycle comprises of follow-up processes, such as:

- Granting/revoking access privileges and attributes as they move up or down the organizational hierarchy.
- Configuring user properties and removing them during offboarding.

Performing these operations manually across a high volume of employees can be time-consuming and error-prone.

Note: With least privilege access being the cornerstone to securing critical assets, human error in such cases (like granting undue privileges to a user, for example) can negatively impact an organization's access management and Zero Trust efforts.

Code-heavy operations

Navigating through the maze of code to perform tasks can be draining and time-consuming for IT administrators, who are entrusted with monitoring vast networks and are expected to derive quick insights about perceived threats.

Case in point:

Take the tasks that ensure visibility of a company's digital environment, such as:

- Log collection,
- Detecting anomalous logons
- File changes
- Inclusion of new processes

Achieving the above tasks can be extremely laborious if IT admins have to rely on scripting languages to retrieve such information.

Lack of scope for collaboration

Secure, organized, and seamless exchange of information between teams must be an essential feature for cybersecurity. Integration expedites data collection and makes security teams more responsive to serious adversaries. Lack of integration among solutions increases operational friction and also expands the attack surface.

Case in point:

Solutions that are rigid in terms of collaboration tend to add more redundant and unsecured procedures, such as

- file duplication
- creation of data silos
- over-reliance on e-mail for file sharing

How technology combats cybersecurity burnout

For technology to reduce cybersecurity burnout, it must eliminate redundant steps while also tapping into a technician's intuition. This combination will help reduce workforce burden, while offering a personalized and smooth user experience. Technology must bring in essential reforms such as:

Codeless or no-code automation

As mentioned above, having an intuitive user experience is key to reducing operator fatigue. Unlike code-driven processes that completely rely on the user's expertise to perform, a low-code or no-code platform can simplify processes by having predefined workflows and an interactive user interface in place.

Using predefined workflows that come along with low-code or no-code platforms, teams can automate mundane, repetitive tasks by exercising just a few clicks. Having such simplified process in place helps SOC and other cybersecurity teams reduce their mean time to detect (MTTD) and mean time to recover (MTTR), thereby bolstering overall performance.

Enhanced interoperability

Better collaboration guarantees better harmony. With **remote work** being a reality now and in the future, organizations must rely on integration between applications to gain quicker, more reliable insights directly from trusted sources and proactively act upon them. With composability being a sought-out feature to take businesses to the next level, organizations must use solutions that can feed information from each other and have a unified data repository, rather than relying on isolated data silos.

Delegation of tasks

As organizations expand, so do their endpoints, administrative tasks, network infrastructure, and other resources. To not just withstand, but excel in keeping up with these growing needs, administrators must delegate tasks to employees belonging to other departments. By delegating tasks, teams can perform to the best of their abilities, while reducing operational fatigue and human error in the process.

How ManageEngine's ADManager Plus makes IT teams happy and efficient

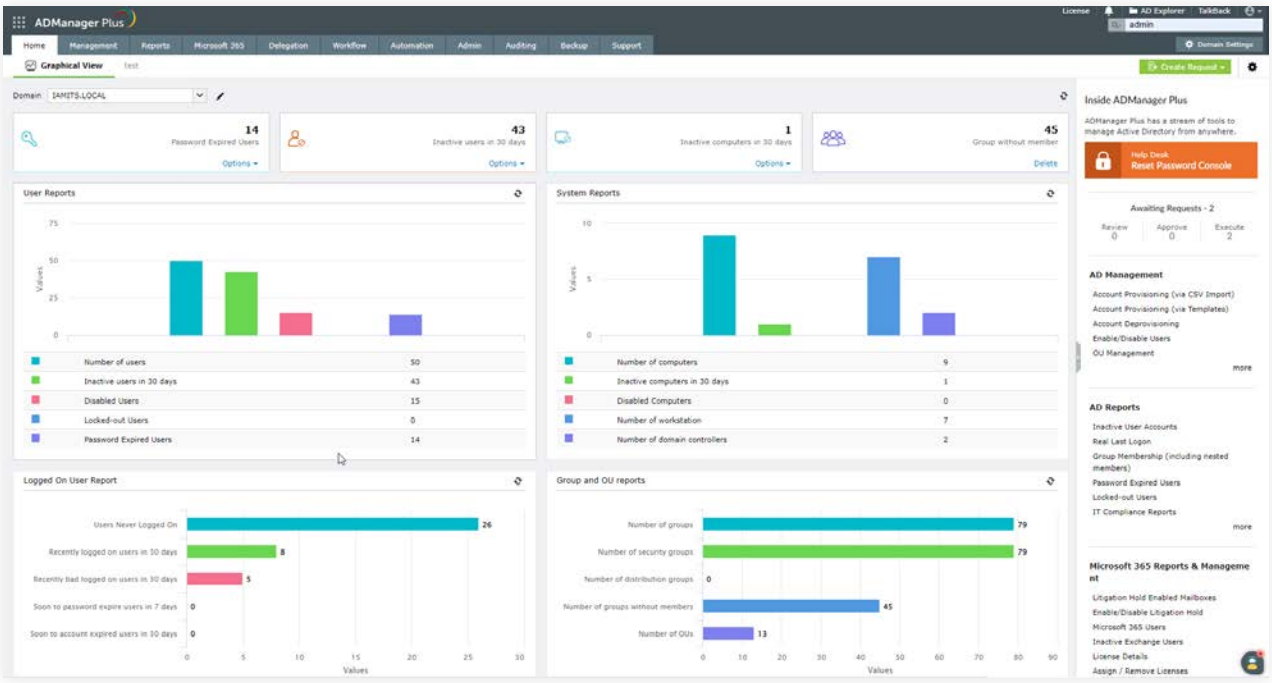
ManageEngine's Active Directory management solution, ADManager Plus, offers a single-window experience for users to perform Active Directory-related administrative and security tasks with ease, irrespective of their complexity. Some of the salient features of ADManager Plus that aids burnout prevention amongst cybersecurity professionals include:

User interface

Right from custom dashboards to drag-and-drop operations, ADManager Plus offers an intuitive user interface (UI) where complex AD-related information is represented as lists, graphs, summaries, reports, and more. With a simple, no-code approach towards data collection, ADManager Plus aids in swift and concise decision-making among IT teams.

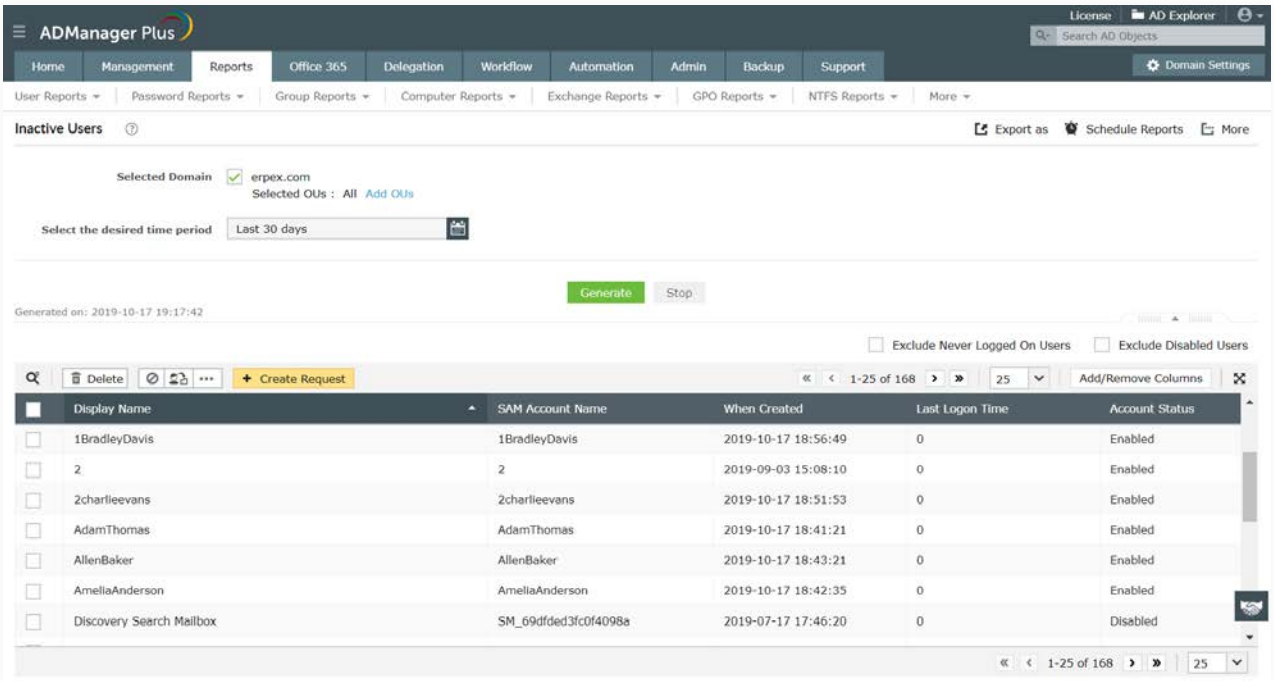
The dashboards also enable users to make the following customizations:

- Add widgets to group together the necessary reports based on the needs of the organization.
- View OU-specific data in the dashboard.
- Have reports of each domain in a separate tab.
- Add the most frequently used management actions and reports to the quick links section.

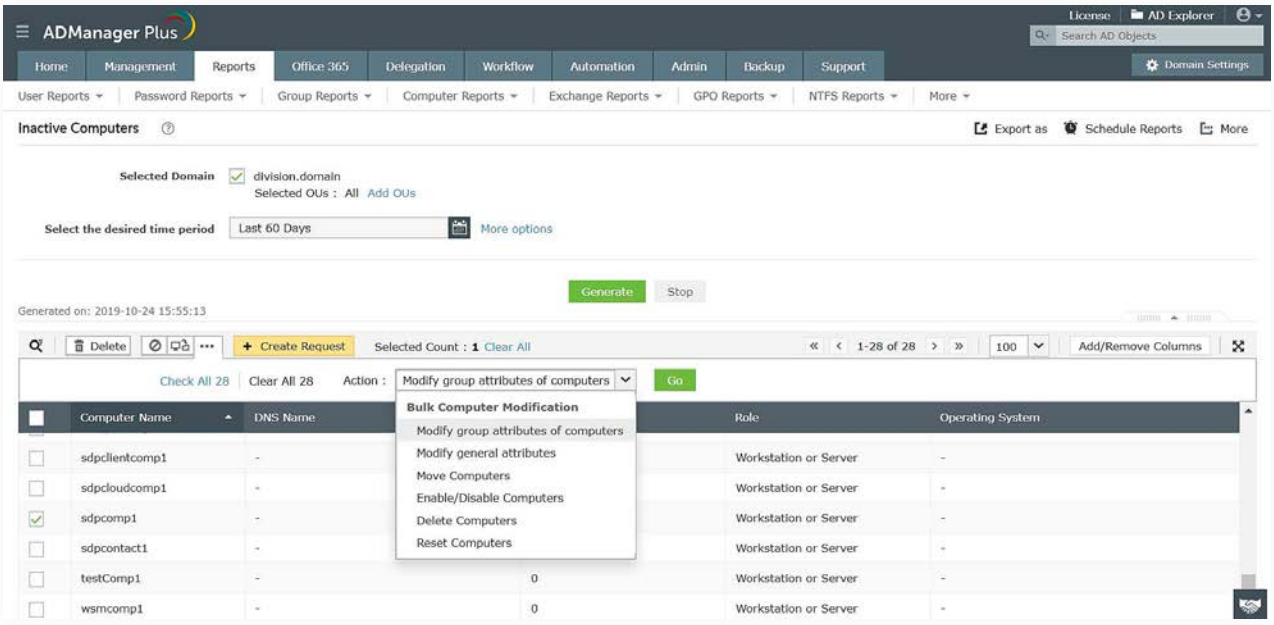


ADManager Plus dashboard

Report generation comes in handy during operations that require high visibility, such as user deprovisioning, where IT administrators can generate reports of inactive accounts before offboarding them.



ADManager Plus Inactive Users report



ADManager Plus' Inactive Computers report

Automation of tasks

ADManager Plus de-stresses IT teams by automating routine AD tasks while also enabling them to control and supervise automation workflows based on their organizations' unique requirements.

With ADManager Plus, organizations can:

- Automate crucial routine AD tasks.
- Schedule the execution of automated tasks at a desired time.
- Define an automation policy to help automate a task and execute any other supplementary tasks in a sequence at a specified schedule.
- Implement business workflows in automations to retain control and accountability whenever necessary.
- Get a clear picture of the automated tasks' history anytime.
- Delete or modify outdated automations.

The automation capabilities of ADManager Plus can be applied in high-risk tasks such as **user lifecycle management.** IT administrators can perform time-bound onboarding and offboarding of user accounts and supplementary actions such as AD cleanup, deleting, disabling, or moving accounts to a different OU, among many other tasks.

With composite features that can supervise several moving parts within the Active Directory, ADManager Plus delivers Identity Governance and Administration (IGA) to organizations with minimal human effort.

Bonus Tip:

Data backup plays a crucial role during employee offboarding. With the combined deployment of ADManager Plus and Recovery Manager Plus, ManageEngine's comprehensive backup and recovery solution, companies can foolproof their data preservation strategies. Using Recovery Manager Plus, organizations can:

- Scheduled automatic backups of their AD, Azure AD, Microsoft 365, Google Workspace, and Exchange environments.
- Encrypt and store the backups within their premises or on in Azure Blob Storage.
- Define a retention period for their backups and automatically discard the older backups and saved on storage fees.
- Back up and restore entire Exchange Online tenants - including emails, calendar entries, contacts and more.

By implementing the above features, automated user lifecycle management comes to a full circle.

Integration

ADManager Plus moves away from data silos by offering out-of-box integration with several solutions, which include:

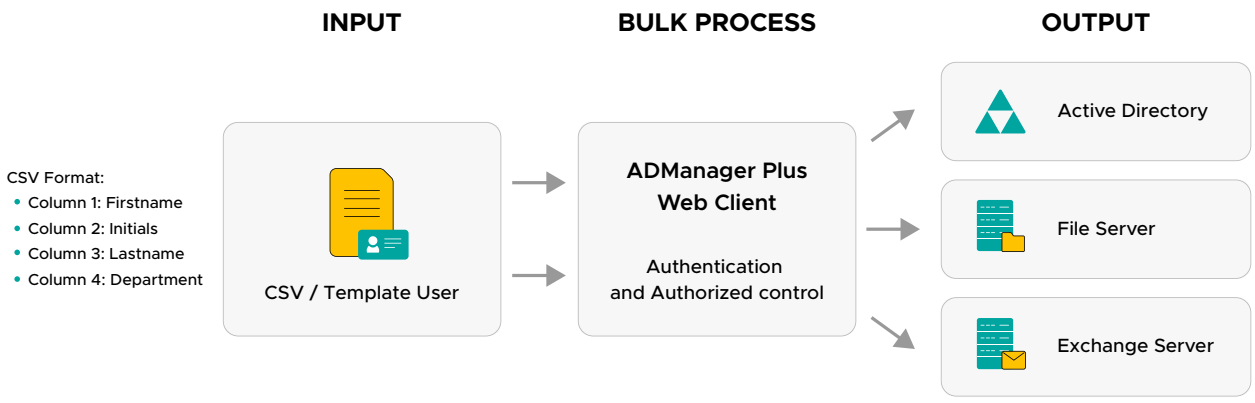
Help desk software:
ServiceDesk Plus, ServiceDesk Plus Cloud, Jira, ServiceNow, and Zendesk

Human Resource Management Systems (HRMS):
Zoho People, ultipro, Workday, and BambooHR

Databases:
Oracle and MS SQL Server
Splunk and syslog servers.

Simplification of bulk processes

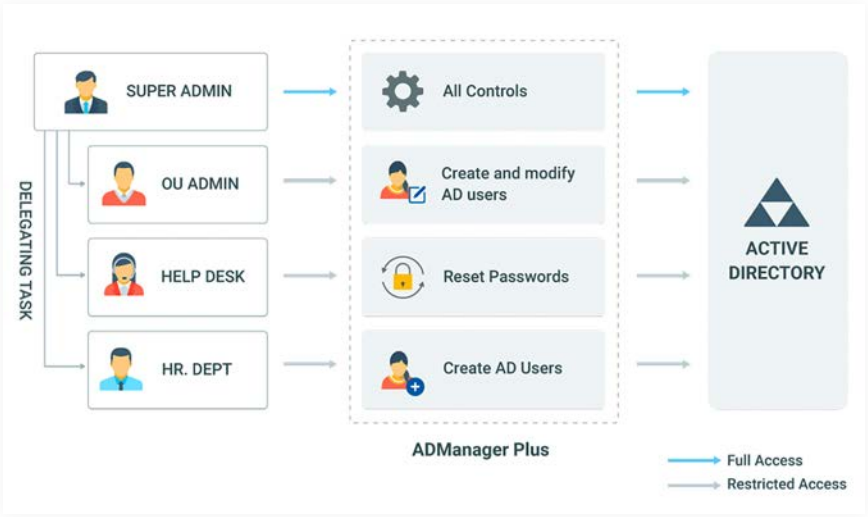
ADManager Plus specializes in drastically reducing high-volume AD operations such as bulk user management, for example. Administrators can now create and manage user accounts by importing a CSV file that contains the list of users and their corresponding attributes. With the reactive user account management feature, you can manage multiple attributes of user accounts in just a single step.



ADManager Plus' Bulk User Management Flow

Delegation of AD tasks

ADManager Plus empowers administrators to delegate simple AD tasks (password resets, unlocking users, creating users in Microsoft 365, assigning Microsoft 365 licenses, etc.) to non-administrative users like help desk technicians, with appropriate access controls. With these capabilities, companies can adapt to changes without overworking IT teams.



ADManager Plus delegation flow

About ADManager Plus

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

$ Get Quote Download

Value add-on

Evaluating and upgrading your organization's cybersecurity posture becomes more actionable with the IAM assessment tool. Get a comprehensive view of your organization's Identity and Access Management capabilities.

Take the IAM assessment