ManageEngine
AD360

A SIX-STEP GUIDE TO ENHANCE HYBRID IT SECURITY

With recommendations from CISA's SCuBA Guidelines 2023

Table of Contents

Introduction

When the phrase "identity is the new perimeter" came to prevalence in the IT industry, it became evident that traditional, on-premises IT architectures were phasing out.

Conventional, on-premises infrastructure that uses the castle and moat approach to solve its security requirements has been replaced with the "never trust, always verify" approach. Moreover, the emergence of remote and hybrid workforce models have further accelerated cloud adoption.

However, the process of shifting assets from on-premises data centers to the cloud cannot be done rapidly. Organizations that maintain a risk-averse approach to security often prefer to store sensitive information on-premises as they cannot afford for it to be exposed to external actors in transit. Besides, on-premises data centers offer several advantages, such as lower latency of encryption controls and effective control over infrastructure and accessibility.

Before migrating to the cloud, organizations must ensure that:

- Their workloads and legacy applications are compatible with a cloud-based environment.
- Their migration strategy aligns with data compliance and security requirements.
- Data classification is performed so that sensitive on-premises data is migrated to the new cloud environment with ample security controls.
- The transition is seamless and cost-effective. Large-scale migrations can be expensive, complex, and time-consuming for businesses. This can create operational laxity and friction among disparate teams across an organization.
- Employees are trained with the necessary skills to become accustomed to the changes.

To implement workload placements and digital accelaration strategies without causing large-scale disruptions to productivity, organizations deploy hybrid IT.

What is hybrid IT infrastructure?

Hybrid IT refers to an organizational architecture that combines both on-premises and cloud-based (public, or private, or both) IT infrastructures. With having such multi-vendor environments in place, businesses can leverage the unique advantages of both on-premises resources (such as the private storage of sensitive data and decreased downtime for applications) and cloud-native assets (such as scalability and cost optimization due to the absence of server maintenance).

For example, organizations opting for a hybrid environment comprised of on-premises AD and Azure AD can enhance their process agility in select areas while allowing business-critical legacy applications and data to function until they are optimized for migration (Fig. 1).

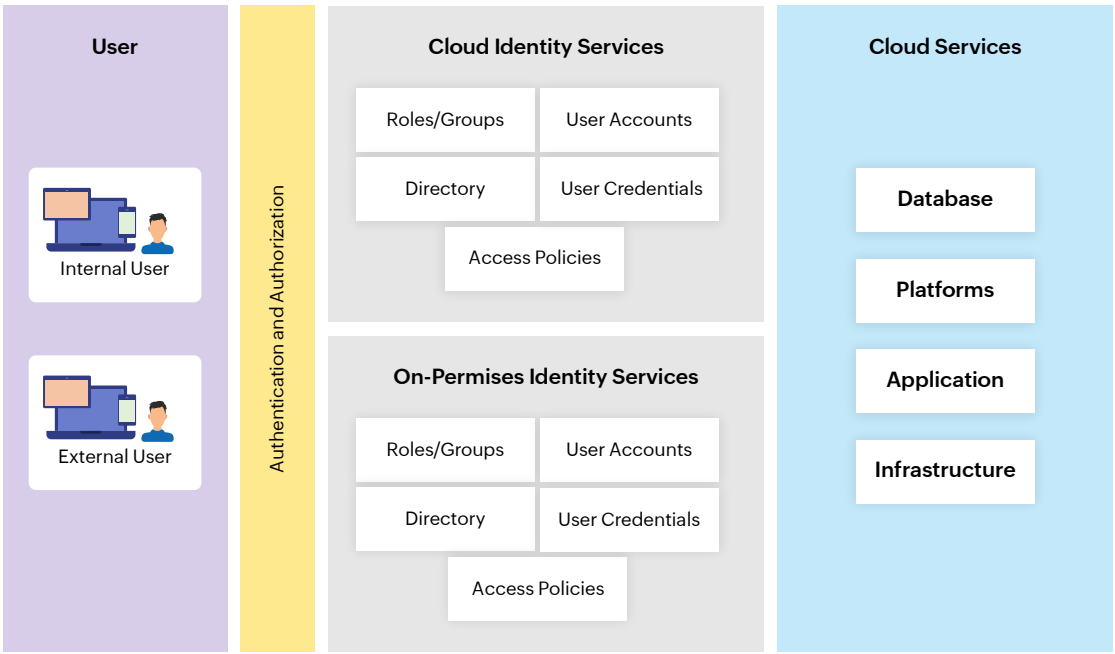

Figure 1. Hybrid Identity Architecture

Security challenges of hybrid IT infrastructure

Organizations find it cumbersome when they have to deploy multiple security tools to manage and secure on-premises and cloud resources. Due to a lack of unification, identity and access management (IAM) strategies—an essential security requirement for organizations—take a major hit. This creates security and operational gaps, which are illustrated below:

Challenge	Description	Use case
Duplication of efforts	In hybrid environments, administrators are often forced to manage two or more identity profiles for employees across diverse environments, thereby complicating user provisioning, backup and recovery of assets (including objects, OUs, policy changes, and attributes), and other administrative workloads.	Your organization hires a new employee, and you are entrusted with provisioning their user identity across multiple environments (e.g., on-premises AD, Azure AD, Microsoft 365, and Google Workspace) within your office network. If you are brave enough to manually accomplish this task using native tools, then congratulations—*you have successfully made your work three times harder.*
Repetitive credentials	Repetitive credentials can be seen as the combined outcome of duplicated efforts and inconsistent policy management. When multiple applications are scattered across distinct environments and there is no unified authentication system, employees tend to repeat their passwords due to password fatigue. The accumulation of bad password practices weakens an organization's security posture.	Using the same password across multiple applications and devices connected to your organizational network makes your company vulnerable to credential stuffing and brute-force attacks.
Low visibility	IT admins and SOC teams are often flooded with an abundance of data from multiple sources (with many of them made redundant due to duplication). With such a clogged view of data, security personnel have to sift through large volumes of logs to monitor the network for suspicious activity. This gives threat actors more time for lateral movement.	Some of the Indicators of Compromise (IoCs) of a potential cyberattack in an AD environment include: • A new child process spawned by a dissimilar parent process ID or executed in an obscure path other than C:\Windows\System32 or C:\Program Files. • Repeated requests by a single user to access privileged files or assets. • Repeated failed logins by a single user or multiple users. Identifying abnormal events with a high rate of success requires comprehensive auditing that combines continuous monitoring, custom-configured alerts, and the correlation of such events using data structures (e.g., graphs and pie charts). Relying on native Event Viewer tools will make this process tedious and time-consuming.

Erroneous compliance reporting	Documentation forms the cornerstone of any compliance standard. When an organization deploying hybrid IT does not have cross-platform monitoring and reporting capabilities, compliance auditing becomes an inaccurate, time-consuming process where administrators have to gather data from multiple data silos. Such piecemeal approach to reporting can potentially lead your organization into paying hefty sums as penalties.	A few of the common requirements across compliance standards are: • Monitor and regulate who accesses what assets, when, and from where. • Ensure passwords are secure. • Monitor login activity across the organizational network. • Create reports on users' life cycles across the organization, such as users created, attributes modified, and accounts deleted • Create reports illustrating the amount of organizational traffic. Without a provision to automate and centralize evidence collection, it is not feasible for organizations to ensure that their security measures align with compliance requirements.

AD360: Securing hybrid IT on a single pane of glass

ManageEngine's hybrid enterprise IAM solution, AD360, centralizes the essential capabilities required to secure the surface of hybrid IT environments. It also empowers IT teams to gain information about the moving parts of their hybrid environments through audit trail documentation.

With AD360, organizations can:

- Consistently implement IT policies.
- Reduce IT admin and SOC workloads by eliminating manual, repetitive processes.
- Reduce mean time to detect (MTTD) levels.
- Gain granular visibility into their organizational environment.
- Avoid process duplication and silos.
- Streamline compliance auditing.
- Bridge interoperability gaps between different teams.

Some of the salient features of AD360 that ensure interoperable security controls for hybrid enterprises include:

Unified identity life cycle management

With AD360, IT admins can automate the creation, modification, and deletion of users across AD, Google Workspace, Microsoft 365, Microsoft Exchange Server, and Skype for Business from a single console, bypassing the need to repeat these processes for every environment.

AD360 eases user life cycle management by allowing IT admins to orchestrate AD tasks in bulk, such as user creation, modification, and deprovisioning, using template-based creation. These customizable templates leverage CSV imports (find a sample CSV file here) and integrations with Human Capital Management (HCM) solutions (Fig. 2) for attributes, such as designation and group name.

AD360 supports integration with the following HCM applications:

- MS SQL
- Oracle
- Ultipro
- Workday
- BambooHR
- Zoho People

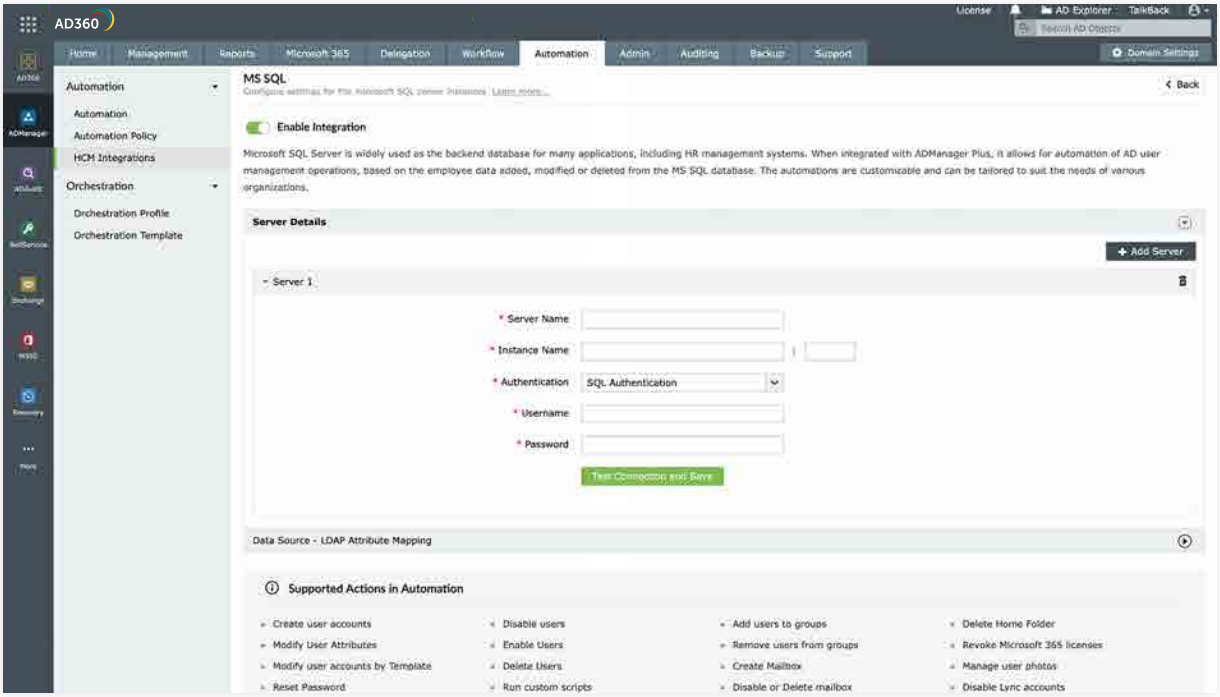

Figure 2. AD360's MS SQL integration.

Furthermore, admins can eliminate errors and redundant efforts by applying AD360's controlled, approval-based automation workflows to execute tasks in bulk (Fig. 3).

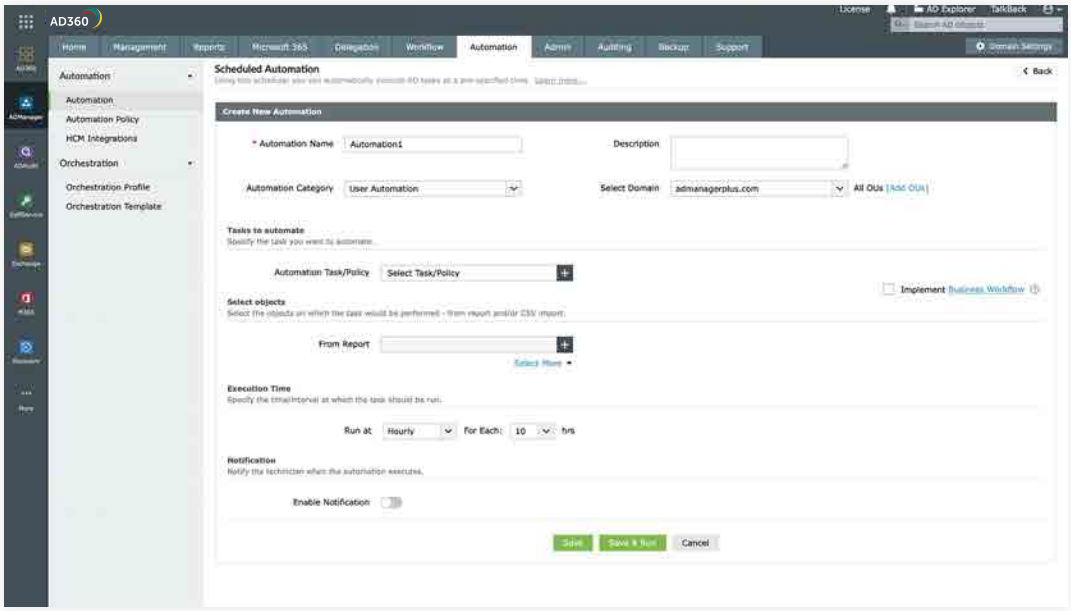

Figure 3. AD360's automation for user onboarding.

Centralized MFA for endpoints

In its Secure Cloud Business Applications (SCuBA) guidelines for hybrid identity solutions architecture, the Cybersecurity and Infrastructure Security Agency (CISA) recommends implementing MFA and SSO to secure hybrid enterprises and make them resistant to phishing.

AD360 prevents the explosion of entry points by implementing endpoint MFA services that accommodate over 20 authentication factors (Fig. 4). This wide array of options ensures that companies do not have to solely rely on hardware devices (such as YubiKey) or disrupt user productivity to verify their employees.

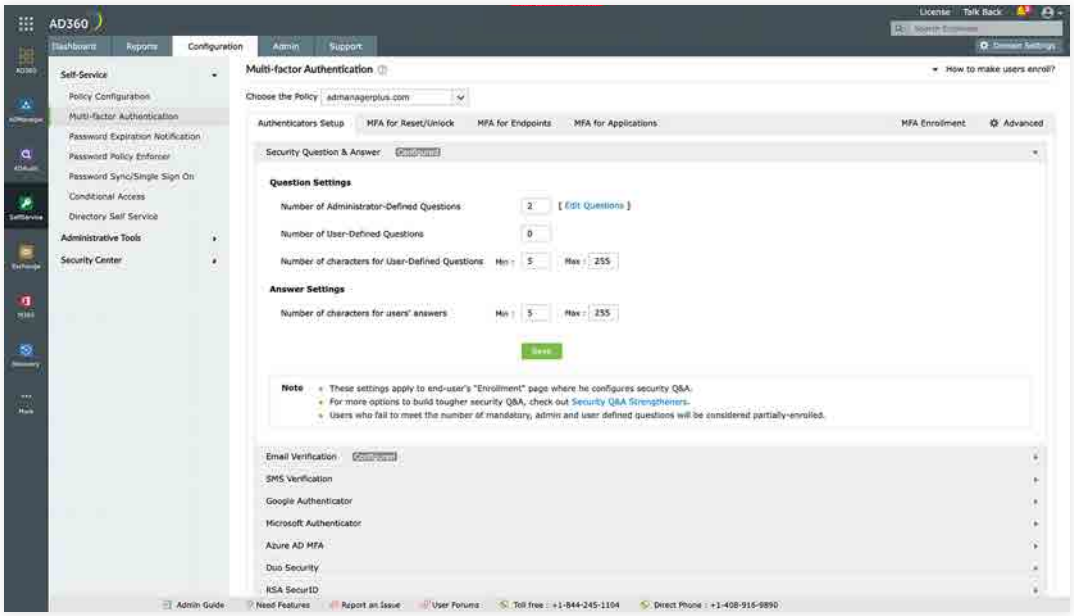

Figure 4. AD360's MFA configurations.

AD360's endpoint MFA feature secures access to:

- Windows, macOS, and Linux machines.
- VPN logins.
- Endpoints supporting RADIUS, such as Citrix Gateway, VMware Horizon, and Microsoft Remote Desktop Gateway (i.e., RDP).
- Outlook Web Access logins.
- Cloud applications.
- Microsoft 365 logins.

Furthermore, AD360 elevates the user experience by providing password synchronization and self-service password reset (SSPR). SSPR ensures that employees can change passwords on their own without IT intervention, thus freeing up IT teams to take up more pressing challenges.

SSO for endpoints

CISA's recommendations for hybrid identity solutions architecture also guide organizations to deploy SSO solutions to enable one-click authentication across on-premises and cloud solutions. AD360's SSO feature supports SAML, OAuth, and OpenID Connect protocols and can be used to simultaneously authenticate on-premises and SaaS applications (Fig. 5).

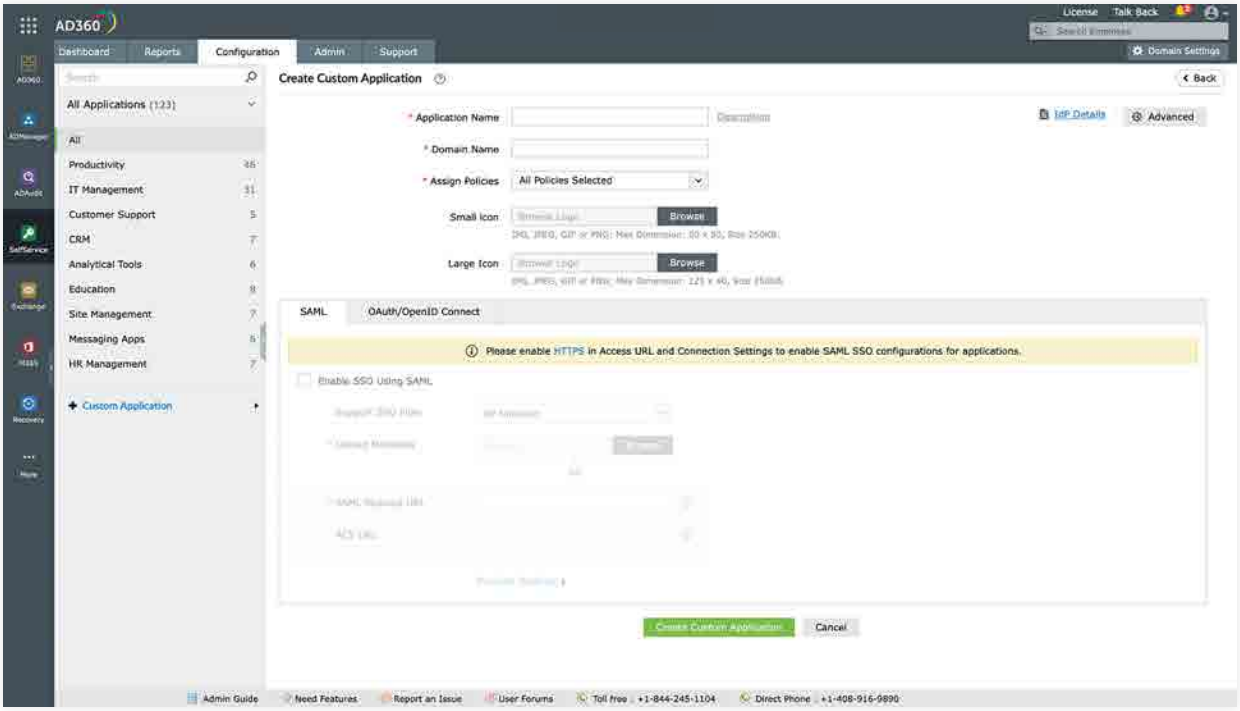

Figure 5. AD360's SSO configurations for custom applications.

Real-time change auditing

A pertinent recommendation by CISA for hybrid identity solutions is using AI- and ML-powered solutions to perform accurate risk assessments by determining "standard user behaviors, what assets are most at risk, and who should be attempting to access specific resources."

With its ML-powered capabilities, AD360 performs continuous monitoring of hybrid AD assets with built-in user behavior analytics (UBA) capabilities and an expansive repository of over 150 preconfigured AD reports (Fig. 6). With UBA, organizations can set a baseline of identity behavior for employees so that IT admins can get clearer visibility into unusual activities.

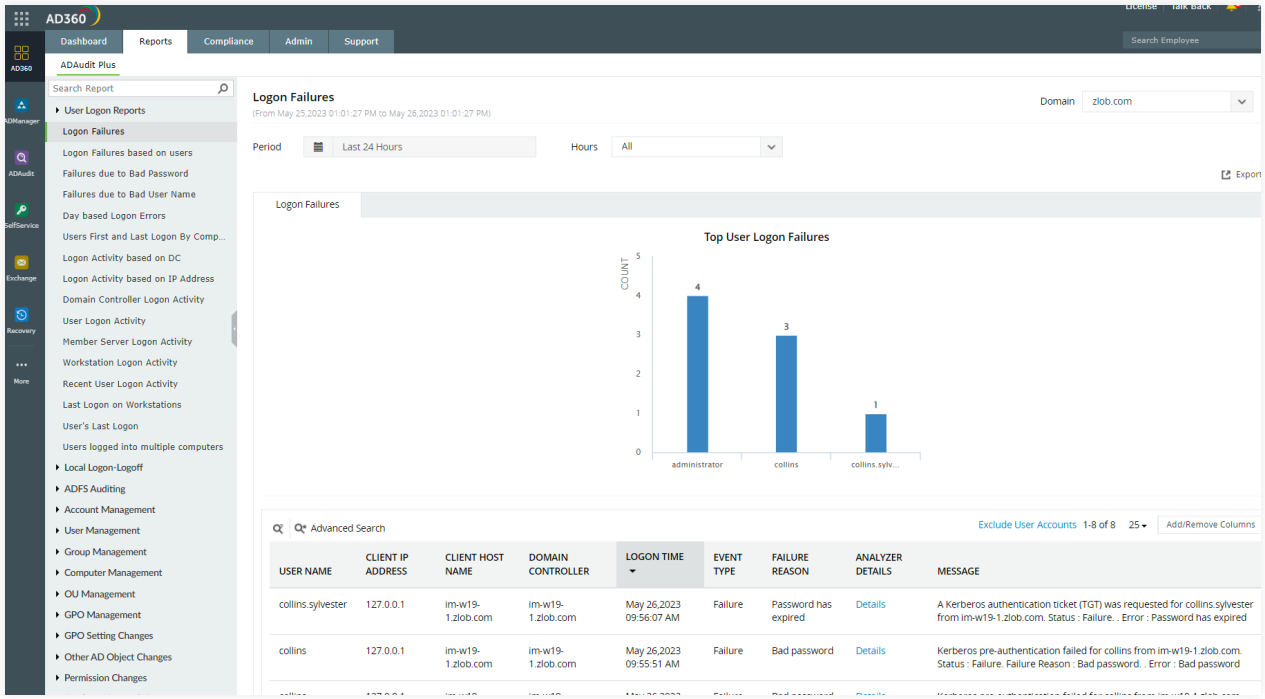

Figure 6. AD360's report library

Using AD360's AD auditing module, IT and SOC teams can thwart ransomware and other malicious activities by:

- Getting notified of suspicious activities across on-premises AD and Azure AD via alerts.
- Tracking employee behavior to identify potential insider attacks.
- Getting notified about privilege escalation and attempts to gain unauthorized access. For example, AD360 features reports that track anomalous login activities, such as failed logins, a high volume of login attempts, and dwell time for a session.
- Keeping a close eye on critical Windows assets using file integrity monitoring, an AD360 feature that notifies you of unusual file and folder changes.
- Performing forensic analysis with AD360's audit trail of user activity.

"(ManageEngine's) products are very good and allow us to manage AD more efficiently than Windows could ever think of allowing us to."

—Gartner® Peer Insights™ review of AD360

Accurate compliance auditing

AD360 offers out-of-the-box reports for the following data compliance regulations: the GDPR, SOX, HIPAA, the PCI DSS, ISO/IEC 27001, FISMA, and the GLBA (Fig. 7). These built-in reports ease the process of compliance auditing while also reassuring organizations that their security efforts are in line with the industry's standards.

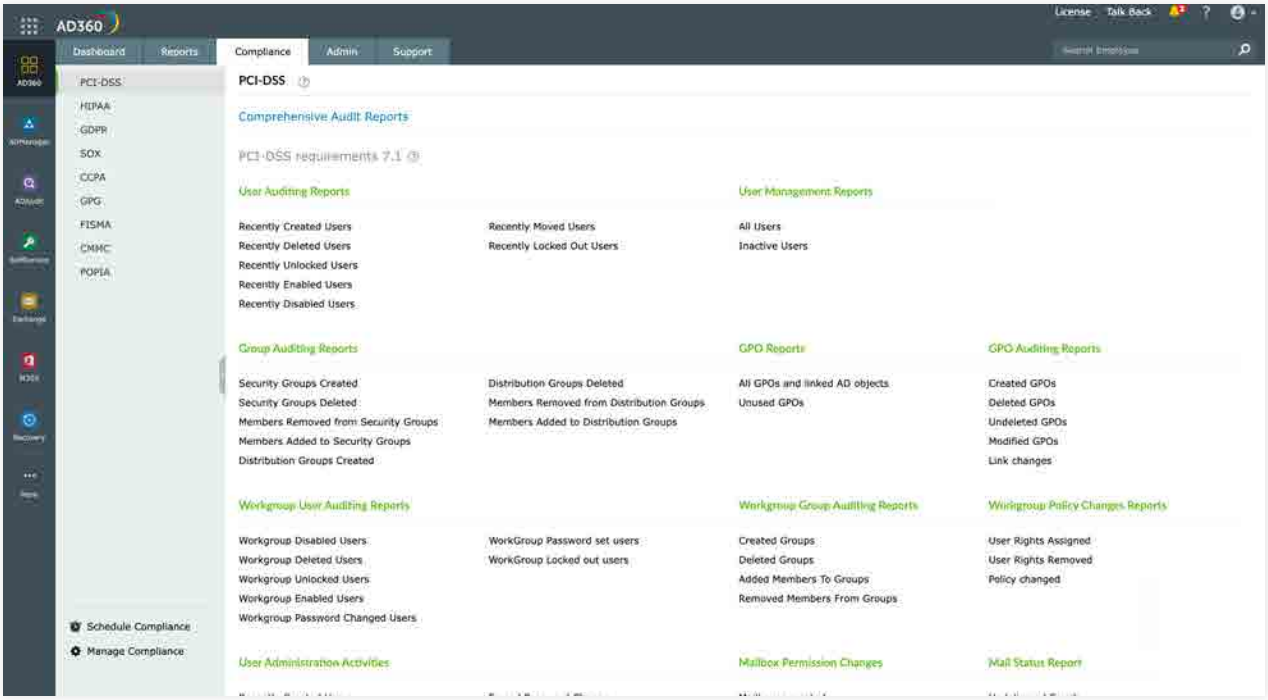

Figure 7. AD360's compliance reports.

Unified backup and recovery

Instead of deploying multiple backup and recovery solutions, deploy AD360—a single console for backing up your on-premises AD, Azure AD, Google Workspace, and Exchange (on-premises and online) environments and restoring key processes within a few clicks.

Bonus tip: Take the IAM assessment to get a holistic reality check of your organization's IAM and cybersecurity posture.

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

About ManageEngine AD360

AD360 is an integrated IAM solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. From user provisioning, self-service password management, and AD change monitoring to SSO for enterprise applications, AD360 helps you perform all your IAM tasks with a simple, easy-to-use interface. With AD360, you can just choose the components you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments—all from a single console.

$ Get Quote Download