



Unified identity security, built for modern enterprises

Protect human and non-human identities with
centralized governance, continuous monitoring, and
strong access controls.

ManageEngine AD360 Overview

ManageEngine AD360 is an enterprise IAM solution that comes with powerful capabilities such as automated identity life cycle management, secure SSO, adaptive MFA, approval-based workflows, UBA-driven identity threat protection and historical audit reports. AD360's intuitive interface and powerful capabilities make it the ideal solution for your modern IAM needs, including fostering a Zero Trust environment.

Components of AD360

AD360 is composed of seven modular components, each designed to address a specific set of identity and access management capabilities. Organizations can deploy individual modules or a combination of modules based on their business, security, and compliance requirements.

- ✓ **ADManager Plus:** Unified AD, Exchange, and Microsoft 365 management and reporting tool.
- ✓ **ADAudit Plus:** UBA-driven auditor for AD, file servers, and Windows Server.
- ✓ **ADSelfService Plus:** Integrated self-service password management and SSO tool.
- ✓ **Exchange Reporter Plus:** Reporting, auditing, monitoring, and content search tool for Exchange Server, Exchange Online, and Skype for Business.
- ✓ **M365 Manager Plus:** Managing, reporting, auditing, monitoring, automation, and alerting tool for Microsoft 365 services.
- ✓ **Recovery Manager Plus:** Back up and restoration tool for AD, Azure AD, Microsoft 365, Google Workspace, on-premises Exchange servers, and Zoho WorkDrive.
- ✓ **SharePoint Manager Plus:** Managing, auditing, and securing tool for SharePoint Online and on-premises SharePoint servers.

ADManager Plus

ADManager Plus is an identity management solution that supports hybrid AD management and reporting, risk assessment, identity life cycle management, risk exposure management, access certification, workflow orchestration, and integration with various enterprise applications to manage, govern, and secure enterprise identities.

1. Identity life cycle & access governance

- ✓ Event-driven automation for user provisioning and deprovisioning.
- ✓ Granting and revoking access across enterprise applications.
- ✓ Regular access certification for users, groups, mailboxes, and Teams.
- ✓ Review permissions across AD, Microsoft 365, and NTFS file servers.

2. Centralized administration & delegation

- ✓ One-step user provisioning across AD, Exchange, Microsoft 365, and Google Workspace.
- ✓ Management of GPOs, shared mailboxes, remote mailboxes, and contacts.
- ✓ Migration of users, groups, and GPOs across trusted domains.
- ✓ Non-invasive role-based delegation without elevating technician privileges.

3. Automation, workflows & operational efficiency

- ✓ Scheduled execution of critical AD tasks through automation.
- ✓ Multi-level approval workflows for user requests.
- ✓ SLA-based validation and prioritization of tasks.
- ✓ Integrated workflows to maintain control over automated actions.

4. Risk visibility & security posture management

- ✓ Risk assessment for AD and Microsoft 365 environments.
- ✓ Risk scoring based on likelihood and impact of threats.
- ✓ Visual mapping of attack paths to privileged AD groups.
- ✓ Continuous monitoring of exposed groups and privilege escalation risks.

ADSelfService Plus

ADSelfService Plus is an identity security solution that delivers secure, seamless access to enterprise resources while enabling a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need.

1. Adaptive MFA

- ✓ Enforce MFA for Windows, macOS, Linux machines, VPNs, OWA, and enterprise applications.
- ✓ Support for 20+ authentication methods including FIDO2, biometrics, TOTP, YubiKey, and Microsoft Authenticator.
- ✓ Enable offline MFA for Windows and macOS logins to protect remote users.
- ✓ Apply conditional access using IP address, time of access, geolocation, and device used.

2. Enterprise SSO

- ✓ Integrate enterprise applications with Active Directory for centralized authentication.
- ✓ Allow users to access multiple applications with a single login.
- ✓ Reduce credential-based attacks using passwordless authentication.
- ✓ Back passwordless login with MFA for enterprise applications.

3. Workforce Self-Service

- ✓ Enable users to reset passwords and unlock accounts without help desk intervention.
- ✓ Allow users to update directory attributes such as email address, mobile number, and photograph.
- ✓ Provide a searchable corporate directory with organizational charts.
- ✓ Let users manage email group subscriptions based on role changes.

4. Remote Workforce Enablement

- ✓ Automatically update cached credentials on user devices with or without VPN.
- ✓ Provide a secure web-based portal for domain and enterprise password changes.
- ✓ Send password and account expiry notifications via SMS, email, or push notifications.
- ✓ Support secure password changes for remote and on-premises users.

ADAudit Plus

ADAudit Plus is a cybersecurity visibility solution to fortify the security resilience of on-premises, cloud, and hybrid AD environments. ADAudit Plus helps reduce the attack surface of your hybrid IT ecosystem by proactively monitoring critical changes and identifying security gaps across on-premises and multi-cloud environments.

1. Identity and access change monitoring

- ✓ Audit changes to Active Directory users, groups, computers, OUs, administrative groups, DNS, schema, and permissions.
- ✓ Track detailed AD object change history with old and new attribute values.
- ✓ Monitor Microsoft Entra ID sign-ins, user, device, group, role, and application changes across hybrid environments.
- ✓ Audit Group Policy Objects (GPOs), including creation, deletion, modification, and setting-level changes with full change history.

2. Identity threat detection and response

- ✓ Detect 25+ AD attacks including Kerberoasting, Golden Ticket, DCSync, pass-the-hash, and ransomware.
- ✓ Receive real-time alerts on who performed what change, when, and from where across AD and Entra ID.
- ✓ Detect anomalous activities such as repeated logon failures, unusual logon times, and privilege escalation using UBA.
- ✓ Automate responses by executing scripts to disable accounts, shut down machines, or end user sessions.

3. Insider threat detection

- ✓ Use User Behavior Analytics (UBA) to identify abnormal user and privileged account behavior.
- ✓ Monitor privileged user activity across AD schema, configuration, users, groups, OUs, and GPOs.
- ✓ Detect first-time use of privileges and suspicious administrative actions.
- ✓ Identify behavioral anomalies such as accessing critical data outside business hours or clearing audit logs.

4. Compliance reporting

- ✓ Leverage 250+ built-in reports covering AD, Entra ID, file servers, Windows servers, and workstations.
- ✓ Use out-of-the-box compliance reports for GDPR, HIPAA, PCI DSS, SOX, ISO 27001, GLBA, and more.
- ✓ Perform forensic and root cause analysis using detailed audit trails and archived logs.
- ✓ Configure real-time email and SMS alerts for compliance and security-critical events.

Exchange Reporter Plus

Exchange Reporter Plus is a ready-to-deploy reporting, change auditing, monitoring, and content search solution for Exchange Server, Exchange Server Subscription Edition (SE), Exchange Online, and Skype for Business Server.

1. Exchange reporting & visibility

- ✓ Mailbox, distribution list, public folder, and organization reports.
- ✓ OWA, ActiveSync, email traffic, and storage reports.
- ✓ Compliance reports for Exchange Server and Exchange Online.
- ✓ Skype for Business reports including conferencing and messaging.

2. Exchange auditing & alerting

- ✓ Track mailbox logons and non-owner mailbox activities.
- ✓ Monitor mailbox permission, property, and distribution list changes.
- ✓ Audit admin, delegate, and non-owner activities.
- ✓ Receive real-time email alerts for critical changes.

3. Exchange monitoring & performance management

- ✓ Monitor Exchange service health and endpoint availability.
- ✓ Track database availability groups (DAGs) and email queues.
- ✓ Monitor server storage and database performance.
- ✓ Track client connectivity and overall server status.

4. Exchange content search & migration

- ✓ Perform keyword-, pattern-, and attribute-based mailbox searches.
- ✓ Download attachments containing suspected sensitive data.
- ✓ Schedule mailbox content searches and view content in HTML format.
- ✓ Migrate users from Exchange Server to Exchange Online with mailbox mapping and scheduling.

M365 Manager Plus

M365 Manager Plus is a comprehensive Microsoft 365 administration solution that helps execute your cloud administrative tasks effectively. Effortlessly perform bulk management of users, groups, mailboxes, sites, teams, licenses, and more by importing a simple CSV file. Automate these routine tasks with custom automation policies to ease your workload.

1. Microsoft 365 management

- ✓ Manage users, groups, contacts, mailboxes, public folders, mobile devices, sites, Teams, channels, team members, and more from a single console.
- ✓ Create and modify Microsoft 365 objects in bulk by simply importing a CSV file.
- ✓ Standardize and predefine user, group, contact, mailbox, and license settings with custom object creation templates.
- ✓ Notify users of password expiration to prevent account lockouts, and reset passwords in bulk.
- ✓ Ensure secure sign-ins by configuring multi-factor authentication for users in bulk.

2. Microsoft 365 reporting

- ✓ Get detailed information on all facets of Microsoft 365 services with over 700 preconfigured reports.
- ✓ Use built-in filters to customize reports based on period of generation, attributes, users, and more.
- ✓ Schedule reports to be generated periodically, and have them emailed to you.
- ✓ Export the reports to multiple formats including PDF, XLSX, HTML, and CSV.
- ✓ Embed report summaries in the form of graphs and charts as widgets in the dashboard for quick understanding.

3. Microsoft 365 auditing, alerting and monitoring

- ✓ Perform extensive audits on admin and non-admin activities in all Microsoft 365 services to ease your security concerns.
- ✓ Take immediate action with real-time notifications for critical events.
- ✓ Monitor Microsoft 365 features and endpoints around-the-clock.
- ✓ Get instant notifications when a decline in service health is detected.

4. Microsoft 365 automation and delegation

- ✓ Automate routine management tasks such as user provisioning, mailbox creation, license modification, and more.
- ✓ Create event-driven policies to execute automated tasks at specified time intervals.
- ✓ Delegate tasks such as password reset, account unlock, and address attribute changes to non-admin users.
- ✓ Delegate the rights of one tenant to another with the cross-tenant delegation to ensure critical tasks are always taken care.

Recovery Manager Plus

RecoveryManager Plus is a unified enterprise backup and restoration tool that can help you overcome any disaster caused by unwanted changes in your IT environment. Back up your AD, Microsoft Entra ID, Microsoft 365, Google Workspace, Exchange, and Zoho WorkDrive environments from a single console and restore any object, site, or mailbox whenever you need it.

1. Active Directory backup

- ✓ Back up domain controllers and restore them to any previous state.
- ✓ Back up and restore all Active Directory (AD) objects, such as users, groups, OUs, GPOs, computers, contacts, and more, in a single click.
- ✓ Restore individual object attributes to any of their past values instantly.
- ✓ Roll back your entire AD to a previous backup state to undo all changes made after the backup point.

2. Microsoft Entra ID backup

- ✓ Back up all Microsoft Entra ID objects, like users, groups, devices, applications, service principals, directory roles, subscribed SKUs, and domains.
- ✓ Search for particular changes from different backup versions and restore just the modified object or attribute instantly.
- ✓ Restore deleted Microsoft Entra ID objects and their attributes, including their group memberships, in a single click.
- ✓ Roll back your entire Microsoft Entra ID, or even individual objects, to a previous backup point and undo all changes made to objects after that point.

3. Microsoft 365 backup

- ✓ Back up your entire Exchange Online tenant, including all emails, calendar entries, contacts, journals, notes, posts, and tasks.
- ✓ Back up all SharePoint Online site collections, sites, lists, and document libraries.
- ✓ Back up and restore all files and folders in your OneDrive for Business environment.
- ✓ Back up all channels, posts, and files in Microsoft Teams.

4. Security, storage, and recovery controls

- ✓ Defend against ransomware by storing backups in immutable cloud repositories like Azure Blob Storage, AWS S3, or Wasabi.
- ✓ Store your backups within your premises in local repositories, NAS, or cloud repositories like Azure Blob Storage, Azure Files, AWS S3, or Wasabi as needed.
- ✓ Define a custom retention policy to specify how long backups will be held in your repository.
- ✓ Forward backup and recovery audit logs to a syslog server, enabling centralized monitoring and enhanced security visibility.

SharePoint Manager Plus

SharePoint Manager Plus is a reporting, auditing, management, monitoring, and migration tool for hybrid SharePoint. It helps administrators carry out SharePoint on-premises and online tasks effortlessly with its easy-to-use interface.

1. SharePoint management

- ✓ Manage SharePoint permissions centrally by granting, revoking, copying, moving, auditing, and cleaning up user and group access across multiple site collections in bulk.
- ✓ Manage SharePoint groups efficiently by creating and deleting groups, and bulk adding, removing, copying, or moving users across multiple site collections.
- ✓ Administer site collections centrally by bulk assigning or removing site collection administrators, restoring permission inheritance, and managing audit settings across multiple site collections.
- ✓ Manage SharePoint permissions at a granular level by bulk granting, revoking, and copying or moving access for users and groups across sites, document libraries, folders, and files.

2. SharePoint reporting

- ✓ Gain centralized visibility into the entire SharePoint environment by viewing detailed information and statistics for farms, web applications, site collections, sites, users, groups, and content databases.
- ✓ View detailed information on lists, document libraries, folders, and files, including storage usage, permission inheritance, and creation or modification details for a specified duration.
- ✓ View detailed user and group permissions across sites and content, including access granted directly or via SharePoint/AD groups, and identify externally or anonymously shared items and users.
- ✓ Analyze SharePoint usage and activity through traffic, activity, and statistical reports, along with IIS log analysis covering site, page, keyword hits, user activity, and access trends.

3. SharePoint auditing and monitoring

- ✓ Track and report on site and site collection changes across the environment, including deletions, modifications, administrative changes, site activity, and audit setting updates.
- ✓ Monitor and report on document and list activity, including creations, deletions, modifications, downloads, permission changes, and check-in/check-out actions across specified periods.
- ✓ Track security and access-related changes, including permission level updates, group and administrator modifications, and sharing or external access activities across the environment.
- ✓ Monitor and analyze content usage and risk by tracking file and folder activity, access patterns, and comprehensive audit analytics.

4. SharePoint delegation

- ✓ Delegate site-level management tasks to department heads or team leaders, allowing them to manage users, permissions, and activities within assigned sites without full administrative control.
- ✓ Assign specific SharePoint sites to compliance or auditing teams so they can generate and analyze permission reports without requiring broader administrative access.
- ✓ Delegate auditing responsibilities to compliance officers or security administrators to track permission changes, file activities, and user actions for compliance and security purposes.
- ✓ Grant task-specific access to migration technicians to manage migration jobs and mappings during SharePoint migration projects without exposing full administrative privileges.



Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus
Exchange Reporter Plus | RecoveryManager Plus

About AD360

ManageEngine AD360 is a unified identity platform that seamlessly connects people, technology, and experiences while giving enterprises full visibility and control over their identity infrastructure. It offers automated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing, compliance, and identity analytics—all from a single, intuitive console. With extensive out-of-the-box integrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems to enhance security and streamline identity operations. Trusted by leading enterprises across healthcare, finance, education, and government, AD360 simplifies identity management, fortifies security, and ensures compliance with evolving regulatory standards.

For more information, please visit www.manageengine.com/active-directory-360/.

\$ Get Quote

↓ Download