ManageEngine
AD360

ManageEngine AD360

Use cases

www.manageengine.com/active-directory-360/

Table of Contents

About AD360

ManageEngine AD360 is an integrated identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. From user provisioning, self-service password management, and Active Directory (AD) change monitoring, to single sign-on (SSO) for enterprise applications, AD360 helps you perform all your IAM tasks from a single console that is simple and easy to use.

With AD360, you can just choose the modules you need, and start addressing IAM challenges across on-premises, cloud, and hybrid environments all in one place.

USE CASE 1

Automating employee onboarding

User onboarding is a process that often spans multiple departments, including HR, IT, and the new employee's department. As a result, user provisioning becomes a complex, time-consuming, and often error-prone process. Although AD is useful for many things, efficiently creating accounts for multiple users at the same time isn't one of them. With Active Directory Users and Computers (ADUC), not only do you have to move through multiple steps to create a single account, but you also have to manually assign all the entitlements required by that user. This is where automated user provisioning comes into play.

How AD360 helps

With AD360, IT administrators can set up policies to automatically create accounts for new employees.

- **One-click multi-platform provisioning:** It's not just for AD; users accounts can be provisioned in Microsoft 365, Google Workspace, Exchange Server, and Skype for Business in a single click.
- **Automated group membership assignment during provisioning:** Assign group memberships for users during provisioning with customizable templates. You can also use these templates to assign logon hours, home folders, managers, and much more during account creation.
- **Bulk creation of user accounts:** Create user accounts for multiple users by using templates, importing users from a CSV file, or integrating with HR databases.
- **Integration with human resources management systems (HRMS):** Integrate AD360 with HRMS such as Zoho People, UltiPro, BambooHR, Workday, and automatically create, modify or delete users' AD accounts whenever their corresponding accounts are modified in the HR applications.

USE CASE 2

Managing group memberships and NTFS permissions to control privileged accesses

Almost all business-critical data is stored on an organization's network and computers. Because of how sensitive this data is, it's crucial that only those who need it have access to it. However, even with this approach, vulnerabilities in your network or an employee gone rogue could lead to a data breach. All an attacker has to do is gain access to a privileged user account or become a member of a group with sufficient privileges; maintaining control over these accounts is essential.

How AD360 helps

AD360 offers privileged access management, which can be used to set up a secure environment where only trusted users can access certain files, folders, and groups.

- **Continuous group membership reports and management:** See which groups have what privileges, as well as which users belong to groups with privileges. These reports make it easy to identify any incorrect permissions granted to users, which can be immediately revoked using the group management features from within the reports.
- **NTFS permission reports and management:** Discover who has what type of privileges over important files and folders with complete audit trails using built-in reports. Modify NTFS and share permissions for multiple users in a single click to remove incorrect permissions.
- **Real-time alerts on critical group membership changes:** Receive real-time alerts whenever a new member is added to a group with privileges. The list of privileged groups to be monitored is customizable, so only the most important changes will trigger an alert.

USE CASE 3

Cleaning up stale accounts to plug potential security gaps

When a user leaves an organization, all the accounts associated with that user should be properly disposed of, as per the organization's policies. However, since it's not uncommon for organizations to have thousands of objects in AD, some of these unused, stale accounts inevitably slip through the cracks. All it takes is one inactive admin account to unlock the potential for a data breach. Periodically keeping an eye out for stale accounts and properly disposing of them requires time and effort, especially if you plan to do this on your own.

How AD360 helps

With AD360, you can automatically identify and cleanup inactive, disabled, and expired user accounts, as well as groups without members. This way, you can ensure security gaps created by stale accounts in yAD aren't exploited by attackers.

- **Automate identification and deletion of stale accounts:** Set up schedulers to automatically scan AD for inactive user accounts based on last logon time, disabled accounts, or expired accounts, and then delete them.
- **Perform complete cleanup using a customizable delete policy:** Make sure the cleanup is performed by defining delete policies, which will automatically delete users' home folders, roaming profiles, and Exchange mailboxes—it'll even remove their accounts in Microsoft 365 and Google Workspace when the account is deleted in Active Directory.

USE CASE 4

Detecting and mitigating threats like malicious logins, lateral movement, privilege abuse, data breaches, and malware

In an organization with a large number of users, it is impossible for the administrator to individually monitor each account for any abnormal actions such as multiple login failures due to wrong passwords, a usually dormant account being used to access critical resources, or a privileged account trying to access data in a server that it has never accessed before. These actions are possible actions of threat actors and can result in data theft

How AD360 helps

AD360 applies machine learning and statistical analytics and creates a baseline of normal behavior specific to each user, and generates alerts about deviations from this norm.

- **Baseline detection engine:** Processed log data is used to create a baseline of normal logon, file, user management, and process activities specific to each user.
- **Anomaly detection engine:** Incoming log data and baselines are compared to detect anomalies.
- **Threat reports and alerts:** Security professionals are notified of anomalies in real time via email or SMS, and anomalies can be viewed as reports.

USE CASE 5

Automating compliance for all major audits including the GDPR, SOX, HIPAA, and PCI DSS

No matter what industry you belong to, there is a good chance that your organization falls under the purview of at least one compliance mandate such as SOX, HIPAA, PCI DSS, FISMA, GLBA, and the GDPR. Most of today's compliance audits are accomplished as point-in-time audits, meaning that at least once a year reports are generated on the desired security settings and configurations. The goal of any compliance regulation and audit is to verify that proper security standards are in place. However, some organizations neglect this task by dedicating minimal effort. If just an hour is set aside annually to conduct an audit, that leaves 364 days and 23 hours where security settings and configurations might be ripe for exploitation.

How AD360 helps

To effectively uphold compliance and ensure proper security measures are in place, you need to constantly generate reports to establish whether the changes to AD objects are in accordance with compliance regulations. AD360 helps you accomplish that.

- **Prepackaged compliance reports:** AD360 comes prepackaged with reports that are specific to each compliance law.
- **Create custom reports:** You can create your own custom reports or simply customize the prepackaged reports to meet specific compliance requirements.
- **Automate compliance report generation:** AD360 comes with a powerful scheduler that you can use to automatically generate compliance reports at periodic intervals, and email them to relevant individuals.

USE CASE 6

Securing Windows, macOS, and Linux endpoints, OWA, and VPN with multi-factor authentication

Your company, by choice or due to compliance laws, has updated its IT policy to require multi-factor authentication (MFA). You decide to set up MFA for local and remote desktop logons to endpoints (Windows, macOS, and Linux machines), OWA, and VPN. With MFA enabled, users will first need to enter their passwords, they verify their identity using a second-factor. So how do you enable MFA for all these systems and applications?

How AD360 helps

AD360 supports MFA for Windows, macOS, and Linux logons, OWA, and VPN.

- **Supports more than 18 authentication methods:** AD360 supports more than 15 authentication methods such as email and SMS-based passcodes, biometric authentication, YubiKey Authenticator, Duo Security, RADIUS authentication, and RSA SecurID.
- **Ensure 100% enrollment:** Automate user enrollment by importing users' domain information through CSV files, or force enrollment using login scripts.
- **Selective MFA enforcement:** You can enforce MFA for all the users in an organization, or only for users with privileges that are at higher risk of a security attack by creating OU and group-based policies.
- **Get detailed reports:** Gain comprehensive insights on user activities, such as identity verification failures and login attempts, and also find users with weak passwords.

USE CASE 7

Eliminating the number one source of help desk tickets —password reset and account unlock tickets

Forgetfulness is in our nature. It’s part of what makes us human, but we shouldn't let it impede the efficiency of the help desk. Password reset tickets often consume much of the help desk's attention, which pushes more critical IT issues to the back burner.

How AD360 helps

AD360 supports self-service password reset and account unlock features that give end users the power to securely reset their passwords and unlock their own accounts.

- **MFA:** AD360 verifies users’ identities through more than 15 authentication methods such as biometrics, Yubikey, Duo Security, SMS and email-based verification codes, and RSA SecurID.
- **Logon screen integration and mobile apps:** With AD360, users can reset their passwords directly from their Windows, MacOS, and Linux logon screens, as well as from their mobile devices.
- **Automated and forced enrollment:** IT administrators can automatically enroll users by importing data from a CSV file or an external database. Users can also be forced to enroll when they log in to their machines.

USE CASE 8

Effective Microsoft 365 license management

If not managed properly, Microsoft 365 licenses can significantly add to a company's operating expenses. It's necessary to understand user requirements before assigning employees licenses, and to keep an eye on inactive users, and unused Microsoft 365 licenses to optimize license management. Each employee's use of Microsoft 365 services and applications differ based on the nature of their work, and some may not use Microsoft 365 at all.

For example, the finance department may not need Skype for Business as much as they need Exchange Online or OneDrive for Business. On the other hand, support personnel rely heavily on Skype for Business as they need to connect with clients, but will probably never utilize Power BI.

How AD360 helps

Unlike the Microsoft 365 Admin Center, AD360 helps add, remove, and change Microsoft 365 licenses in bulk, without having to use a single PowerShell script.

- **Remove licenses of inactive Microsoft 365 users:** Idle Microsoft 365 users still consume Microsoft 365 licenses, adding to business costs. Using the management module in AD360's Inactive Mailboxes report, admins can find idle user accounts and remove their licenses.

- **Add Microsoft 365 licenses to unlicensed users:** Admins can find users who don't have a Microsoft 365 license with the Unlicensed Users report. Using the advanced filter option, it's easy to identify users based on their job title, department, city, and other attributes, and then add the Microsoft 365 licenses they need.

USE CASE 9

A ransomware attack on Exchange Online, OneDrive for Business, or Google Workspace encrypts all mails and files in your environment

Ransomware attacks are not just limited to laptops and physical systems; they have found their way into Exchange Online, OneDrive for Business, and Google Workspace. The desktop applications of OneDrive for Business and Google Workspace and their syncing patterns allows threat actors to encrypt files in those shared folders which are then synced back to the respective cloud counterparts.

How AD360 helps

In case of ransomware attack on your enterprise applications, AD360 allows you to restore the entire application to their latest, unaffected, backed up state.

- **Complete restoration:** Restore all mailbox items, site, and drive items to their most recent backed up state, thereby undoing the harm caused by the ransomware.
- **Minimal RPO:** Depending on your configured backup frequency, you can achieve a maximum Recovery Point Objective (RPO) of 1 day.

Other key features of AD360

1. **Approval workflow:** Establish control over crucial management tasks without giving up usability by enabling approval workflows.
2. **Delegate tasks to help desk technicians:** Delegate common tasks—like resetting passwords, disabling accounts, generating reports, and more—to help desk technicians.
3. **More than 1000 preconfigured reports:** Receive reports on all facets of your AD, Azure Active Directory, Microsoft 365, Google Workspace, and Exchange environment.
4. **Real-time password synchronization:** Sync AD passwords with Microsoft 365, Google Workspace, Salesforce, IBM iSeries, Oracle Database, and more, all in real time.
5. **Password policy strengthener:** Enforce advanced password policy settings, such as dictionary rule and pattern restriction based on OUs and groups to strengthen the passwords of domain users.
6. **Azure Active Directory Management:** Reduce the amount of time spent on management tasks by enabling administrators and technicians to manage users, groups, and licenses all in bulk.
7. **Unified enterprise application backup:** Back up all your enterprise applications such as AD, Azure Active Directory, Microsoft 365, Google Workspace, and Exchange from a single console.

Conclusion

An IT administrator faces many challenges in a typical day and no two challenges are alike. Deploying individual applications to deal with each problem increases the complexity and the possibility that critical events will be missed. Utilizing an integrated solution like AD360 provides IT admins with a comprehensive tool to tackle all problems from a single console.