ManageEngine
AD360

Buyer's guide

Your all-in-one AD360 handbook

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

Index

01 Introduction 2
- What is IAM? 2
- Why do organizations need an IAM solution? 2

02 What is AD360? 3

03 Why should I consider AD360? 3
- What AD360 offers 3
- Gartner recommended critical IAM capabilities in AD360 4

04 What are AD360's components? 6

05 How will AD360 benefit me if I already use any of its components? 7
- If you use ADManager Plus 7
- If you use ADSelfService Plus 9
- If you use ADAudit Plus 11
- If you use Exchange Reporter Plus 12
- If you use M365 Manager Plus 14
- If you use RecoveryManager Plus 15

06 How will AD360 benefit me in my industry? 16
- Healthcare sector 16
- Finance and banking sector 17
- Government sector 18

07 What do I get with each edition of AD360? 20

08 What do people say about AD360? 21
- Peer reviews 21
- Analyst reviews 22

09 What is the architecture of AD360? 23
- AD360's modules 23
- Communication process between modules 25
- User roles and their authentication 25
- Technology used 26

10 Where can I get more information? 27

Introduction

What is IAM?

Identity and access management (IAM) is a framework that encompasses the policies and processes required to govern users' identities and their access to resources within an organization. IAM consists of three key components: identification, authentication, and authorization. Thus, an IAM solution is one that facilitates these components under one umbrella.

Why do organizations need an IAM solution?

With the number of data breaches rising exponentially, organizations need to adopt governance practices and tools to prevent threats and increase operational efficiency. Gaining access to the corporate perimeter is easier than ever due to remote work. For many organizations, an enormous amount of the workload is stored and shared across a wide variety of on-premises and cloud applications, leading them to use granular access control solutions to keep up with authentication demands.

IAM solutions help securely manage the digital identities of users. Tracking changes to users' privileges and access to critical resources or data can help in identifying privilege access abuse. IAM solutions protect the organization against security incidents by setting parameters in the system to detect anomalous activities that otherwise go undetected. These IAM security features help build an effective security infrastructure.

What is AD360?

AD360 is an IAM solution suite. It's a modular solution with multiple components that take care of a myriad of IAM needs, from automating mundane tasks like user life cycle management to implementing strong authentication mechanisms. AD360 has a simple and straightforward console from where you can manage and protect your Windows Active Directory (AD), Exchange Server, and Microsoft 365 environments. It also takes care of your identity governance and administration (IGA) demands and ensures business continuity with backup and restoration of critical data.

Why should I consider AD360?

What AD360 offers

Any organization that's serious about IAM should have its key processes implemented. AD360 goes beyond the basic components of IAM and offers functionalities for implementing frameworks such as Zero Trust and hybrid cloud monitoring. Here's how AD360 can help meet your demands:

You're on the lookout for	How AD360 can help
Identity and life cycle management	Beat IT disruptions by automating painstaking routines like provisioning, deprovisioning, and password resets. Empower your workforce with seamless identity self-service for on-premises and cloud applications.
Privileged access management	Closely monitor all privileged access pathways to mission-critical assets within your network. Enforce fine-grained access restrictions and request-based approval workflows for privileged accounts. Achieve dual control over privileged access with real-time session monitoring and anomaly detection. Effectively cut down standing privileges and privileged account sprawl by provisioning just-in-time privilege elevation for domain accounts.
Hybrid cloud management	Secure your hybrid cloud infrastructure where data is stored. Monitor network traffic and gain granular visibility across your offline-online environment. Develop cross-platform risk profiles, and enable adaptive access to resources on strict contextual authentication.

Compliance management	Ensure stress-free regulatory compliance with complete control over sensitive information and how it's shared. Build and maintain a strong cybersecurity framework to meet the demands of data privacy regulations.
Zero Trust implementation	Adopt Zero Trust to protect your growing network perimeter. Verify every user, employee, contractor, and respective endpoint before establishing trust with behavior-based security analytics. Make informed choices about data, people, devices, workloads, and networks. Enable single sign-on (SSO) for quick, secure access to corporate resources, and implement multi-factor authentication (MFA) to strengthen security.

Don't just take our word for it. The following list highlights the 15 capabilities Gartner considers critical for an IAM solution, and you can implement them all using AD360.

Gartner recommended critical IAM capabilities in AD360

1. **Identity life cycle management and fulfillment:**
Streamline the identity management of users, including those of temporary employees or contractors, using automated user life cycle management for provisioning, role changes (reprovisioning), and deprovisioning user accounts.

2. **Entitlement management:**
Eliminate redundancy and human errors and improve business processes by automating entitlement management.

3. **Approval-based workflows:**
Build purpose-oriented business workflows. Create the required levels of approval by including the rights of the stakeholders. Define the approval flows for business processes, such as user account creation, modification, or permissions management.

4 **Real-time change auditing:**

Get audit reports on privileged user activity, insider threat detection, and root cause analysis. Monitor and be notified about logon activity and ACL or password changes. Also, audit Azure AD, removable storage, workstations, servers, files, and folders. Generate out-of-the box reports for mandates like the GDPR, SOX, PCI, HIPAA, FISMA, and GLBA.

5 **Policy and role management:**

Set up role-based access control to define and assign granular roles for stakeholders, enforce the principle of least privilege, and distribute duties of privileged accounts to prevent privilege escalation.

6 **Access certification:**

Review user access rights with detailed reports and ensure they comply with the internal security policy.

7 **User authentication methods:**

Avoid impersonation attacks using biometrics and other advanced authentication methods. Step up your security by implementing MFA to access endpoints and applications.

8 **Adaptive authentication:**

Enforce risk-based adaptive authentication using factors such as user location, IP address, time of previous logon, or device footprint.

9 **SaaS application enablement:**

Set up SAML 2.0-based SSO for hundreds of enterprise SaaS applications, like Salesforce, ServiceNow, and Slack.

10 **Nonstandard application enablement:**

Configure custom scripts that facilitate identity provisioning for in-house applications. Go beyond mainstream target systems like AD, Azure AD, and Office 365 and extend AD360's IAM capabilities to ServiceNow, Salesforce, and other third-party applications.

11 **Access requests:**

Enable self-service group management through which users can request membership to AD groups to gain access to a set of specific IT resources. By enabling an approval workflow for self-service group management, application and resource owners can control who gets to be a member of a particular group.

12 **Reporting and ML-based user behavior analytics:**
Detect, investigate, and mitigate threats, such as malicious logins, lateral movement, malware attacks, and privilege abuse, with ML-based user behavior analytics; remediate these threats and more with automated responses.

13 **Ease of deployment:**
No prerequisites or complicated deployment. Start managing identities in your on-premises, cloud, or hybrid IT environment within minutes.

14 **API target enablement:**
Facilitate the sharing of data between AD360 and any third-party application or web service with REST APIs.

15 **High availability:**
Ensure high availability in case of system and application failures. High availability is achieved through automatic failover; when the AD360 service running on one machine fails, another instance of the AD360 service running on a different machine will automatically take over.

What are AD360's components?

AD360 comprises of six modules, each of which manages a particular set of functionalities. You can choose the necessary modules according to your organization's requirements. Let's take a look at the individual modules and what they do:

1 **ADManager Plus:** AD, Exchange, and Microsoft 365 management and reporting.

2 **ADSelfService Plus:** Self-service password management, and SSO and MFA implementation.

3 **ADAudit Plus:** UBA-driven auditing and threat detection for AD, file servers, and Windows Servers.

4 **Exchange Reporter Plus:** Reporting, auditing, monitoring, and content searching for Exchange Server, Exchange Online, and Skype for Business.

5 **M365 Manager Plus:** Management, reporting, auditing, monitoring, automation, and alerting for Microsoft 365 services.

6 **Recovery Manager Plus:** Enterprise backup and restoration for AD, Microsoft 365 and Exchange, Azure, and Google Workspace servers.

How will AD360 benefit me if I already use one of its modules?

The prime advantage of using AD360 is you can simply add more modules as your requirements evolve, which means you can take care of all your IAM needs from one single console. Further, any changes or settings configured are seamlessly synced across the modules to enable efficient implementation of your IAM strategies.

Note:

The functionalities mentioned below are not exhaustive. The solution can be tailored to suit your organization's needs. If you'd like to know how AD360 can help you specifically, you can contact us at:

ad360-support@manageengine.com +1.844.245.1108 (toll-free)

Here's how you can benefit from upgrading to AD360 if you use one of the following components:

If you use ADManager Plus

With ADManager Plus, you can manage user accounts and privileges in bulk. However, to boost your organization's security, it's also necessary to monitor the actions and privileges of user accounts. By upgrading to AD360, you can:

Perform AD and Azure AD security auditing

Audit critical changes in your Windows environment, such as modifications to AD users, groups, GPO settings, the schema, FSMO roles, sites, and other objects.

Monitor changes to local administrative group memberships, local users, user rights, local policies, scheduled tasks, and processes on your member servers.

Gain full visibility into Azure AD changes, such as modifications to users and devices, group memberships and roles, applications, and licenses.

Track successful and failed logons, account lockouts, logons from disabled accounts, MFA-enabled logon failures, and more.

Perform user activity monitoring

Track privileged user activities; monitor the active and idle time spent by employees at their workstations; monitor user logons; and be notified about sudden, atypical user login behavior, such as an unusual login time, by tracking deviations from the baseline.

Perform real-time file access auditing

Monitor privilege abuse by tracking accesses in real time to see who changed which file or folder, when, and from where across Windows, NetApp, EMC, Synology, Huawei, and Hitachi file systems.

Reduce password reset-related help desk calls

Enable self-service password resets and account unlocks regardless of whether users are in the office, on the move, or at home.

Remind users of their upcoming AD password or account expiration date via email, SMS, or push notifications. Send multiple notifications at regular intervals so alerts don't go unnoticed, ensuring users change their passwords before they expire.

Enhance password security

Greatly enhance security by using factors like IP address, business hours, device used, or geolocation to enforce access control decisions automatically.

Add MFA for cloud application, VPN, virtual desktop infrastructure, machine (Windows, Mac, and Linux), Outlook Web Access (OWA), and Exchange Admin Center logins.

Enforce fine-grained password policies with stronger password settings to privileged users.

Prevent employees from using passwords that have previously been exposed.

Enable data backup and recovery

Back up all AD objects, like users, groups, GPOs, OUs, Exchange attributes, DNS records, computers, and contacts, at regular intervals and restore them either partially or completely.

Track, locate, and revert any unwanted modifications to AD objects, DNS configurations, mailbox items, and other Exchange- and M365-related attributes.

Roll back your entire AD and Azure AD, individual objects, or even specific attributes to a previous backup point and undo all changes made after that point.

Hold backup data for a defined retention period, and discard the oldest full backup to save storage space.

Perform recovery operations without having to restart domain controllers (DCs), ensuring the DCs are continuously available.

If you use ADSelfService Plus

With ADSelfService Plus, you can bolster your password management and improve security. By upgrading to AD360, you can also:

Enhance AD password management

Reset passwords in bulk across AD, Exchange Server, Microsoft 365, Google Workspace, and Lync or OCS environments.

Automate periodic password changes for users, set unique passwords for multiple users at once, and perform password management from built-in reports.

Detect and resolve AD account lockouts faster with real-time alerts

Get instant notifications when critical user accounts are locked out with details such as locked-out time and which machine they used.

Analyze and troubleshoot account lockouts effectively by tracking down the source of authentication failure.

Create an approval-based workflow for password reset requests

While enabling self-service for employees, redirect help desk tickets to your IT service provider and define who should review and approve the tickets.

Stay in control of AD automation by receiving notifications via email or SMS about the execution of any automated task.

Track employee activity in real time

Track when employees log on and log off in real time, and detect privilege abuse by monitoring user activity.

Keep a close eye on users in your enterprise by continuously auditing user accounts to discover improper, accidental, or even malicious changes.

Ensure accountability by maintaining a foolproof record of all file accesses and modifications along with all AD object modifications and user login information.

Perform identity life cycle management

Provision, modify, and deprovision accounts and mailboxes for multiple users at once across AD, Exchange servers, Microsoft 365 services, and G Suite from a single console.

If you use ADAudit Plus

ADAudit Plus helps you identify signs of a threat by monitoring for and alerting you about any suspicious behavior. By upgrading to AD360, you can also manage critical aspects of AD in the event of a breach. With the upgrade, you can:

Perform privilege management

Protect important files and groups containing business-critical information and prevent accidental or intentional misuse of privileged resources by being vigilant about users' access rights. Elevate the access rights only for trusted users and check on them regularly using predefined reports.

Set up a secure environment where trusted users are temporarily granted permission to access certain files, folders, and groups, and ensure users have only the required rights.

Generate and export reports on access permissions for all NTFS folders and files and their properties for Windows file servers and NetApp servers to quickly view and analyze file-level security settings applied to critical files and folders in their environments.

Perform user life cycle management and automation

Effortlessly generate a list of inactive user accounts, disabled user accounts, and expired user accounts in the form of reports and delete or disable these accounts in bulk instantly.

Automate critical tasks, specify how often you want automations to run, and view a history of automations to keep track of the status of all automations. View when the automation was run, the total number of tasks it includes, which of them are pending, and which of them have been executed.

Enhance password security:

Enable SSO and MFA for all SAML-based applications, which allows users to use just one set of credentials to access all their commonly used applications.

Leverage a multi-platform password synchronizer to automatically synchronize Windows AD and Azure AD password resets, changes, and account unlocks for user accounts across multiple other platforms, such as Google apps, M365, Salesforce, Zoho, Zendesk, and ServiceNow.

Roll back AD changes

Undo any changes made to AD that are detected by ADAudit Plus through periodic backups of AD data. Roll back AD objects, like users, groups, GPOs, OUs, Exchange attributes, DNS records, computers, and contacts, to an earlier state and undo any changes performed.

Compare backup snapshots across multiple versions to get an overview of all previous values and the current value of an AD object before you perform any restoration.

Perform recovery operations without having to restart DCs, ensuring continuous availability for the DCs.

If you use Exchange Reporter Plus

Along with the benefits of using Exchange Reporter Plus, upgrading to AD360 brings a host of additional features for both AD management and Exchange Server management. You can:

Manage mailboxes

Configure remote mailboxes in Exchange while creating new AD accounts for users individually or in bulk using a CSV file.

Add multiple email addresses for users while ensuring they all map to the same mailbox; enable or disable Exchange services attributes, including Outlook Mobile Access, OWA, POP3, and IMAP4; and set delivery restrictions on the size of the emails users send and receive.

Easily set or reset the "send on behalf" and forwarding addresses.

Change the storage limits of users' mailboxes.

Migrate mailboxes in bulk to the required Exchange server and delegate the migration task accordingly. Set mailbox rights in bulk using templates, and manage Exchange Servers 2003, 2007, 2010, and 2013.

Enforce better cloud security with granular password policies

Create and manage password policies for multiple cloud applications, including Exchange Online, from a centralized console—no more jumping between multiple cloud applications every time your organization's IT security policy changes.

Extend AD password policy controls to cloud applications, like Exchange Online; enforce tighter password policies on privileged accounts and implement more lenient password policies on normal user accounts.

Extend the granular password policy controls that govern AD to cloud applications, and ensure that the passwords for all accounts have the same complexity rules, expiration dates, etc. This makes password management easier for both end users and administrators, and it greatly reduces password-related issues.

Back up mailbox items, perform granular restorations, and stay compliant with retention policies

Back up mailboxes and mailbox items, such as emails, calendar entries, contacts, journals, notes, posts, tasks, draft emails, deleted items, junk mail, outgoing emails, permanently deleted items, and all group mailboxes, and archive mailboxes from both on-premises Exchange Server and Exchange Online tenants.

Restore entire mailboxes or specific mailbox items to the same mailbox they were backed up from or to a different mailbox in the same Exchange Online tenant or Exchange organization. Export an entire mailbox to PST format for archival.

Define a retention period for your backups, and automatically discard olderbackups and stay compliant with retention policies.

If you use M365 Manager Plus

AD360 can bolster the functionalities of M365 Manager Plus by not only offering more monitoring capabilities for your environment but also enabling data backup and recovery for peace of mind. With AD360, you can:

Perform user management

Manage Exchange Server and AD from a single console with runtime mailbox provisioning, deprovisioning, and delegation; set mailbox rights in bulk using templates; and apply multiple Exchange policies, like a sharing policy, a role assignment policy, a retention policy, a Unified Messaging policy, and an ActiveSync policy, all at once.

Create dynamic distribution groups and configure all their attributes at once, provision new resource mailboxes in Exchange and Microsoft 365, and modify resource mailboxes in Exchange.

Generate a list of inactive users from ADManager Plus through scheduled reports, automate the process of removing M365 licenses, and control license-related costs.

Enhance password security

Extend AD password policy controls to cloud applications, like Exchange Online; enforce tighter password policies on privileged accounts and implement more lenient password policies on normal user accounts.

Add an extra layer of protection for Microsoft 365 users by enabling MFA. In addition to Windows credentials, users logging in for Microsoft 365 SSO can be required to use other authentication factors, such as verification codes, Duo Security, biometric authentication, or Google Authenticator.

Enable M365 backup and recovery

Back up all the files and folders in your OneDrive for Business environment and restore them to any of their backed-up versions instantly. Users experience no downtime in Microsoft 365 services while their OneDrive data is backed up.

Preview content, attachments, and documents from Microsoft 365 backups before restoring them.

Store your Microsoft 365 backups on-premises or in your Azure Blob Storage and Azure file shares.

Back up just the changes made to mailboxes and sites since the last backup cycle.

If you use RecoveryManager Plus

With the confidence that your data is backed up and safe in case of a disaster thanks to RecoveryManager Plus, you can use AD360 to revamp your AD environment without worrying about your data and gain additional security functionalities. When you upgrade, you can:

Track files and folders in real time

Monitor privilege abuse by tracking accesses in real time to see who changed which file or folder, when, and from where across Windows, NetApp, EMC, Synology, Huawei, and Hitachi file systems.

Detect and respond to internal threats

Set up a threshold for baseline parameters of user behavior; if the threshold is breached, it may be an indicator of a rogue insider or a hacked account. In such cases, apart from being alerted, you can also set up an incident workflow as a first response to counter these attacks.

Perform identity life cycle management

Reset or change user account passwords in bulk, and automate other identity management processes, like provisioning, deprovisioning, and bulk user management.

Enhance password security

Enhance your network's security by setting up MFA for endpoint and application logins using methods such as fingerprint authentication or a time-based OTP. You can also set strong password policies to ensure that a weak password doesn't compromise the security of your entire network.

How will AD360 benefit me in my industry?

Healthcare sector

With the confidence that your data is backed up and safe in case of a disaster thanks to RecoveryManager Plus, you can use AD360 to revamp your AD environment without worrying about your data and gain additional security functionalities. When you upgrade, you can:

Secure confidential PHI

Review security incident reports, track changes in real time at the attribute level, spot undesired changes and revert them to the correct value immediately, and track and audit user access to systems that contain protected health information (PHI).

Find and track sensitive ePHI, monitor file accesses and modifications, and report on overexposed sensitive files.

Achieve HIPAA compliance:

Ensure effective information security control through continuous and thorough monitoring.

Always stay in the know with over 200 preconfigured reports to view changes made in the system, track user actions, access data logs, and modify data.

Prove healthcare compliance with GDPR and HIPAA standards with around-the-clock monitoring and instant email alerts.

Administer granular password policies

Enforce fine-grained password policies for OUs and groups, and implement a stringent password policy for privileged users who have access to PHI.

Prevent users from setting passwords that are dictionary words, easy-to-crack patterns, or passwords that have been compromised due to data breaches.

Implement MFA

Enforce MFA for different users based on domain, OU, or group memberships, all while ensuring a seamless login experience.

Privilege assignment and monitoring

Assign only the required level of access to a patient's health information to doctors, nurses, health insurance executives, and others who are directly responsible for that patient.

Identify and get alerts on telltale signs of privilege abuse, such as unusually large volumes of file modifications or attempts to access critical files.

Spot privilege escalation attacks by monitoring and auditing changes made to security groups.

Finance and banking sector

Monitor access to sensitive financial data

Get information regarding who changed which file or folder, when, and from where, along with failed attempts to change a file, across your Windows, NetApp, EMC, Synology, Huawei, and Hitachi file systems.

Keep tabs on data access rights by monitoring folder owner and permission changes, and be alerted about changes to critical files and folders via email and SMS.

Prevent inappropriate access to financial data by leveraging ADAudit Plus' machine learning capabilities to spot unusual volumes of file changes and changes occurring at unusual times.

Analyze and refine share permissions with NTFS reports

Gain complete visibility and prevent unauthorized access to NTFS partitions and shares with preconfigured access permissions reports for folders, files, and server shares.

See which users and groups have access to folders in a specified path with predefined reports on AD access control permissions for users and groups.

Track failed attempts to access or modify files and folders, which are often the first sign of a security threats, with around-the-clock auditing.

Spot suspicious user behavior

Leverage machine learning and statistical analytics to create a baseline of normal behavior specific to each user and get instant alerts when deviations from this norm are observed.

Detect anomalies instantly in user logons, account lockouts, and permission changes, and actively respond to threats by configuring automatic responses to incidents.

Leverage continuous privileged user activity monitoring to audit administrator activity, track privileged user access to critical data, and detect privilege escalation and lateral movement patterns.

Government sector

Compliance management

Stay compliant using out-of-the-box, automated reports for regulations such as FISMA, NIST, GPG 13, CJIS, ISO20000, ISO 27001, GDPR, CPRA, and LGPD.

Privilege assignment and monitoring

Assign only the required level of access to sensitive documents to officials based on their authority.

Identify and get alerts on telltale signs of privilege abuse, such as unusually large volumes of file modifications or attempts to access critical files.

Spot privilege escalation attacks by monitoring and auditing changes made to security groups.

Implement MFA

Enforce MFA for different users based on domain, OU, or group memberships, all while ensuring a seamless login experience.

Administer granular password policies

Enforce fine-grained password policies for OUs and groups, and implement a stringent password policy for privileged users who have access to sensitive personal information.

Prevent users from setting passwords that are dictionary words, easy-to-crack patterns, or passwords that have been compromised due to data breaches.

Back up and recover your data

Keep all your critical information and AD configurations backed up in case they need to be restored.

Perform recovery operations without having to restart DCs, ensuring continuous availability for the DCs.

What do I get with each edition of AD360?

Features	Standard	Professional
AD management		
Over 150 AD reports	✓	✓
AD user management	✓	✓
AD computer management	✓	✓
Multiple domain management	✓	✓
Help desk delegation	✓	✓
Report scheduling	✗	✓
AD group and contact management	✗	✓
OU-based administration	✗	✓
Workflows and automations	✗	✓
GPO management	✗	✓
AD auditing		
AD logon activity monitoring	✓	✓
AD user, group, computer, OU, and GPO change auditing	✓	✓
AD alerts and email notifications	✓	✓
GPO settings auditing	✗	✓
User, computer, group, and OU attribute change auditing	✗	✓
New and old value AD object attribute auditing	✗	✓
OU, user, group, computer, and GPO permission change auditing	✗	✓
File server and NetApp filer auditing	Add-on	Add-on
Workstation and member server auditing	Add-on	Add-on
Password self-service		
Password reset and account unlock	✓	✓
Employee directory update and people search	✓	✓
Multi-platform password synchronizer	✓	✓
Password and account expiry notifications	✓	✓
Password changes	✓	✓
ADSelfService Plus GINA or Credential Provider extension	✗	✓
External MSSQL database support	✗	✓

Exchange reporting		
Email traffic reporting	✓	✓
OWA usage statistics reporting	✓	✓
Mailbox size and growth reporting	✓	✓
Storage growth tracking	✓	✓
Mailbox permission reporting	✓	✓
Exchange Server auditing	✗	✓

What do people say about AD360?

What your peers say about AD360

"

It has competitive features and is [an] easy [and] user-friendly application. The other important factor is our experience with ManageEngine's incredible technical support team, who were prompt on support pre- and post-trial of the product.

Thomas Cook Ltd

Travel; India

"

Prior to ADAudit Plus, we had no visibility into our AD infrastructure. Now, we're able to monitor all AD transactions as far as group changes, user creation, security, authentication logs, and much more.

Harvard Medical School

Education; Massachusetts, USA

> Microsoft doesn't have any reporting tools built into Exchange Server. We relied on PowerShell scripting for getting the necessary details. Exchange Reporter Plus has eradicated the need for PowerShell scripting.

Samsung SDS
Electronics; USA

What analysts say about AD360

The world of threats is ever-evolving, and the solutions should evolve accordingly. AD360 is a solution that goes beyond basic IAM with capabilities to tackle an organization's identity and governance demands. This has also been noted by **Martin Kuppinger** of **KuppingerCole Analysts**, who said:

> AD360 also supports authentication in a way that goes beyond what commonly is found in that category of products.

Some of AD360's features that Kuppinger appreciates are:

User behavior analytics

"AD360 comes with a strong set of auditing features...The focus is on optimizing administrative processes and identifying critical entitlements, orphaned accounts, and fraudulent user behavior. Part of this are the UBA capabilities that are [in] AD360. Based on that, the behavior of users can be monitored and outliers can be identified easily. The technology is based on ML algorithms."

Approval workflows

"Workflows finally help in managing access beyond the IT team. AD tasks can result in tickets that are used in multi-stage workflows. This also allows for creating user request portals for various types of users, approvals of entitlement requests by the responsible managers, or approvals for controlled access to file shares."

Task automation

"AD360 delivers more in-depth integration with the supported target environments, e.g. by supporting the creation of Microsoft Exchange mailboxes and automating other types of typical tasks in these environments. Thus, it also can serve as an extension to standard IGA tools by delivering in-depth management of AD and some of the connected systems."

What is the architecture of AD360?

AD360's modules

There are three modules in AD360, which are as follows:

- The web client
- The application server
- The database

The web client

AD360 provides a web-based client that any machine connected to the same network as the AD360 web server can access using a web browser. The web client can be accessed by entering the IP address or the hostname, followed by the port number of the AD360 web server as the URL.

For example, if the IP address is 192.168.98.17 and the port number is 8082, the URL would be as follows: https://192.168.98.17:8082

<Login page>

Once the administrator's credentials are authenticated, the AD360 dashboard displays all the necessary information on one screen with easy access to the solution's various features. The dashboard can be customized to suit individual requirements.

The application server

AD360's application server comprises of a Tomcat server that:

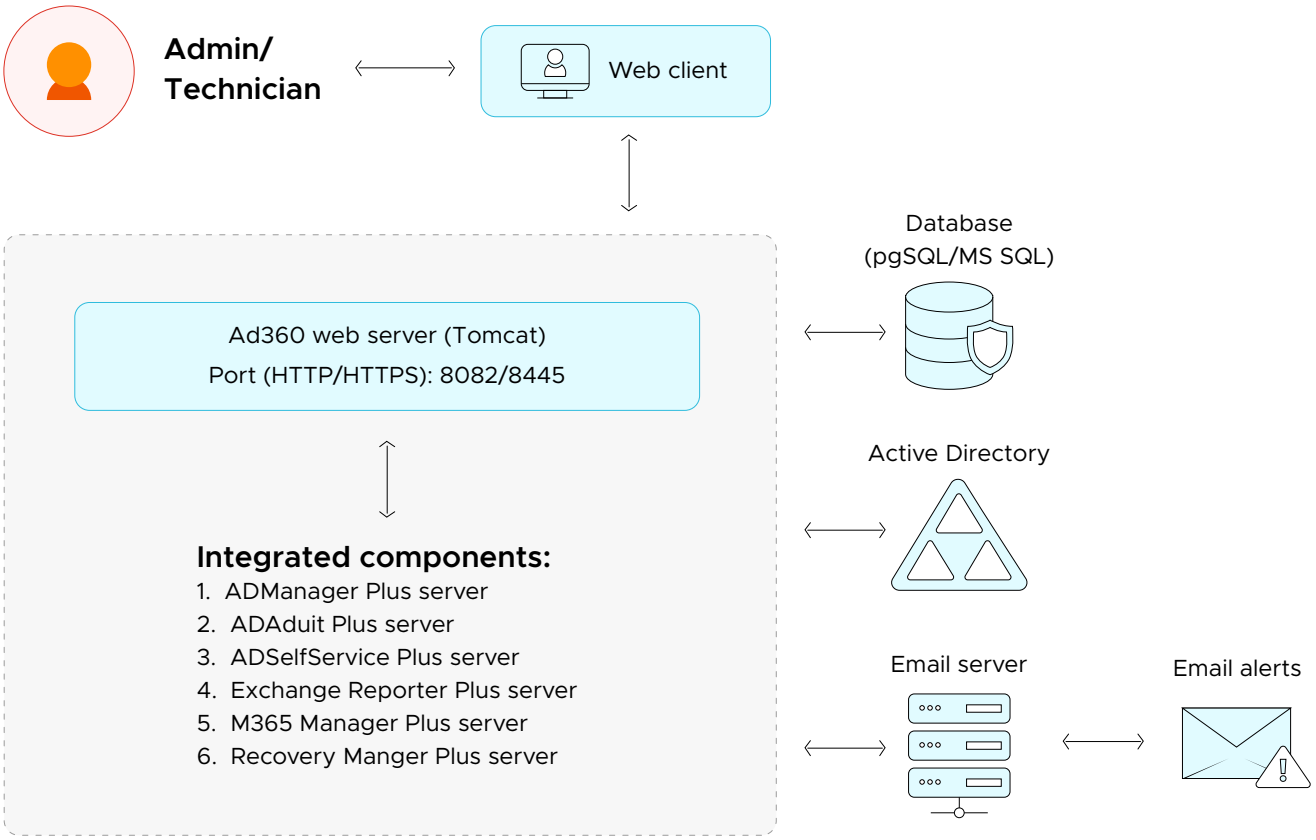
- **Manages AD360's individual components:**
  AD360's various components are in constant communication with each other. This ensures that if you make any changes to one of the components, such as modifying the domain settings or admin credentials, the changes are synced across all the other components.

- **Provides a holistic reporting view:**
  AD360 gives you a bird's-eye view of your entire IT environment by gathering information and reports from all the components and displaying them in a centralized console using easy-to-read charts and graphs.

- **Sends out email alerts:**
  The AD360 server communicates with email servers to send alerts on license expiration, product downtime and startup, product updates, and more.

The database

AD360 comes bundled with a PostgreSQL (pgSQL) database. You can also migrate the built-in pgSQL database to MS SQL or an external pgSQL database if you wish to do so. This product database stores admin credentials, domain configuration settings, reverse proxy settings, and more. The AD360 web server fetches these details as and when necessary. Sensitive information such as the administrator credentials are encrypted using the bcrypt algorithm to ensure secure storage.



Communication process between modules

- To log in to the web client, users have to verify themselves as detailed in the authentication section below.

- Whenever the user tries to view a report or update the administration settings (domain configuration, admin credentials, reverse proxy, auto-update, and more), the client sends a request to the AD360 web server. Communication between the client and the AD360 web server can be secured by enabling HTTPS after applying an SSL certificate.

- Based on the request received from the client, the AD360 web server swings into action. It makes a REST API call to the respective components to fetch the reports or, if there's an update in the administration settings, it stores the necessary details in the product database and then makes a REST API call to the integrated components to sync the changes across all of them.

User roles and their authentication

AD360 supports two user roles:

- Administrators
- Technicians

Note:

While technicians only have access to the dashboard and reports, administrators have complete access, and they can can modify domain settings, schedule an auto-update, access reverse proxy and SIEM integration settings, and perform other actions in AD360 and its integrated components.

Administrator login

- An administrator account is verified using product authentication, and the credentials are stored in the database and encrypted with the bcrypt algorithm.

- When the user tries to log in, the AD360 web server uses the Java Authentication and Authorization Service to fetch the credentials stored in the database.

- If the credentials entered by the user and those fetched from the database match, the user will be successfully logged in.

Technician login

- A technician's identity is verified using domain authentication.
- Once the user enters their credentials, the AD360 web server uses LDAP to communicate with AD.
- The user will be granted access to the product once AD verifies the user.
- Additionally, the administrator can also enable SSO with AD or smart card authentication for technician logins.

Note:

A technician created in any of the integrated components will be assigned AD360 technician privileges automatically when they first log in to the solution.

Technology used

- The client side of the application is developed using Ember.js.
- The server-side framework is developed using Jakarta Servlet.
- AD360 uses Java Database Connectivity to connect to pgSQL and MS SQL databases. It also allows servers to communicate using HTTP or HTTPS.

Where can I get more information?

Resource	Description
Admin guide	A one-stop guide that covers everything administrators should know to set up and run AD360.
Privileges and permissions guide	An elaboration of all the necessary roles and permissions required for the various features of each component integrated with AD360.
Database migration guide	A walkthrough of the database migration process from the built-in PostgreSQL database to MS SQL.
Reverse proxy guide	A guide to the process of using AD360 as a reverse proxy server for the products integrated with it.

To get a personalized demo of AD360:

Click here to request a demo

To get a customized quote for AD360:

Click here to get a quote

For more details or speak to someone:

ad360-support@manageengine.com +1.844.245.1108 (toll-free)