ManageEngine AD360

Solution Architecture

ManageEngine
AD360

Introduction

ManageEngine AD360 is an integrated solution that combines a suite of components to meet your identity governance and administration (IGA) demands. With its straightforward interface, you can pick just the components you need and start addressing IGA challenges across your Windows AD, Exchange Server, and Microsoft 365 environments from a single console.

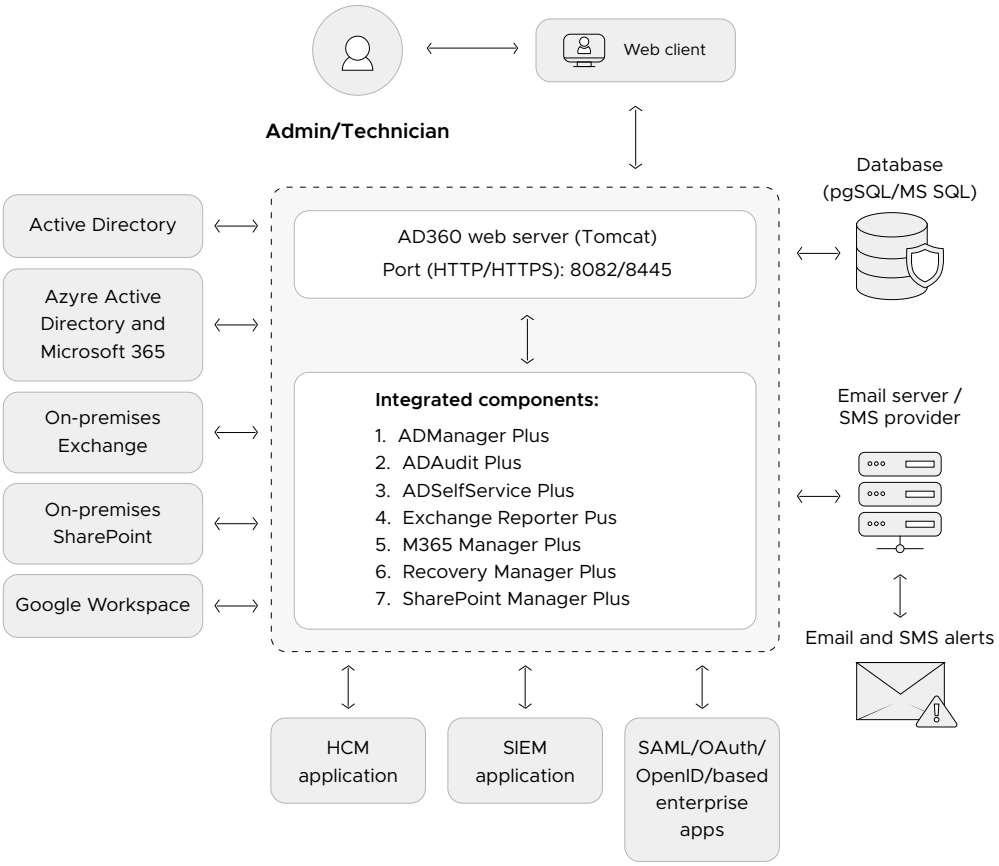
Highlights of ManageEngine AD360

- **Identity life cycle management:** Provision, deprovision, and manage identities across multiple platforms in bulk.
- **Automation:** Leverage custom automation policies to accomplish monotonous administrative tasks without human intervention.
- **Orchestration:** Create event-driven orchestration policies that automatically carry out a chain of tasks like adding and revoking accesses post provisioning and de-provisioning, respectively.
- **Real-time auditing and alerting:** Leverage nearly 1,000 predefined audit reports to ensure compliance, prevent unauthorized access, mitigate threats, and more.
- **User behavior analytics (UBA):** Detect insider attacks, prevent identity theft, secure privileged accounts, and more with UBA-driven change monitoring.
- **Delegation and workflows:** Create custom help desk roles to ease administrative burden and retain control over these tasks through the approval workflow.
- **MFA for endpoints:** Secure endpoints with advanced MFA techniques including biometrics, YubiKey, and Google Authenticator.
- **SSO and self-service password management:** Grant one-click access to enterprise applications using SSO. Empower users to reset passwords and unlock accounts securely on their own.
- **Comprehensive reporting:** Gain powerful insights into your AD, Exchange, Microsoft 365, and SharePoint ecosystems with over 700 preconfigured reports.
- **Backup and disaster recovery:** Back up and restore AD, Azure AD, Microsoft 365, Google Workspace, and on-premises Exchange data.

AD360 components and their use

There are seven different components in AD360, each with a unique set of features. You can pick the components based on your business requirements to solve your IGA challenges.

- **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, and on-premises Exchange servers.
- **SharePoint Manager Plus:** Managing, auditing, and securing tool for SharePoint Online and on-premises SharePoint servers.



AD360 modules

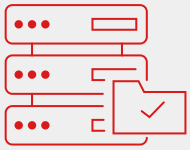
Web client

AD360 provides a web-based client that can be accessed from a web browser by entering the IP address or the hostname followed by the port number of the AD360 web server as the URL.

Example: http://ad360-server:8082 or http://192.45.89.71:8082

The web client can be accessed from any machine that is connected to the same network as the AD360 web server.

Server



The AD360 web server constitutes a Tomcat server. This is used for:

- **Managing the integrated components:** The different components of AD360 communicate with each other for SSO, domain settings, and more. With AD360, you don't have to keep jumping to every individual component to update changes in the domain settings, admin credentials, and so on. Once you update the change in any one of the components, AD360 will make a REST API call to the other components and sync the change across all of them.
- **Providing a holistic reporting view:** AD360 gives you a bird's-eye view of your entire IT environment by fetching reports across the ADAudit Plus, Exchange Reporter Plus, and M365 Manager Plus components through a REST API call and presenting them in a single console.
- **Sending out email alerts:** The AD360 server communicates with mail servers to send alerts on license expiration, product downtime and startup, product updates, and more.

Database

- AD360 comes bundled with a PostgreSQL (pgSQL) database.
- You can also migrate the built-in pgSQL database to a Microsoft SQL server or an external pgSQL database based on your preference.
- This product database stores admin credentials, domain configuration settings, reverse proxy settings, and more. The AD360 web server fetches them as and when required.

Note:
To ensure security, sensitive information such as the admin credentials are encrypted using the bcrypt algorithm.

Communication between the client, server, and database

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

Authentication

AD360 supports two user roles:

- **Administrators**
- **Technicians**

While technicians will only have access to the dashboard, features, and reports section for which they have been authorized, administrators will be able to access the domain settings, schedule auto-updates, access reverse proxy and SIEM integration settings, and perform other actions for AD360 and its integrated components.

Administrator login

- An administrator account is verified using product authentication.
- An administrator's 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 Lightweight Directory Access Protocol 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 stack

- 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.
- Java Database Connectivity also allows servers to communicate using HTTP or HTTPS.

Component ports

Product ports	HTTP	HTTPS
AD360	8082	8445
ADManager Plus	8080	8443
ADAudit Plus	8081	8444
ADSelfService Plus	8888	9251
Exchange Reporter Plus	8181	8887
M365 Manager Plus	8365	9365
RecoveryManager Plus	8090	8558
SharePoint Manager Plus	8085	8086

The AD360 database runs on port 33305. For more information regarding ports and system requirements, refer to this document.

Related documents

Here are some documents you may find helpful

Resource	What's it about?
Admin guide	This all-inclusive guide provides step-by-step instructions on how to configure the product and use its various settings.
Privileges and permissions guide	This guide lists the permissions required for using the various features of AD360.
SSL configuration guide	This guide provides step-by-step instructions on how to apply an SSL certificate in the product and enable a secure connection (HTTPS) between the browser and the AD360 server.
Database migration guide	This guide will help you migrate product data from the built-in pgSQL database to an MS SQL database.
Reverse proxy guide	This guide provides step-by-step instructions on how to enable a reverse proxy for AD360.
High availability configuration guide	This guide provides step-by-step instructions on how to enable high availability for AD360 and the components that support it.

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

ManageEngine
AD360

AD360 is a unified identity and access management solution that helps manage identities, secure access, and ensure compliance. It comes with powerful capabilities like automated identity life cycle management, secure single sign-on, adaptive MFA, approval-based workflows, UBA-driven identity threat protection, and historical audit reports of AD, Exchange Server, and Microsoft 365. AD360's intuitive interface and powerful capabilities make it the ideal solution for all your IAM needs, including fostering a Zero Trust environment.

$ Get Quote Download