

High Availability Configuration Guide

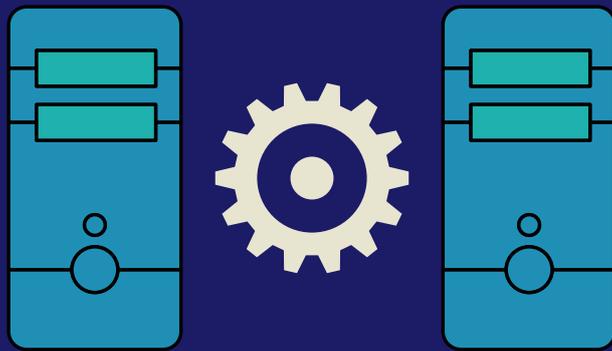


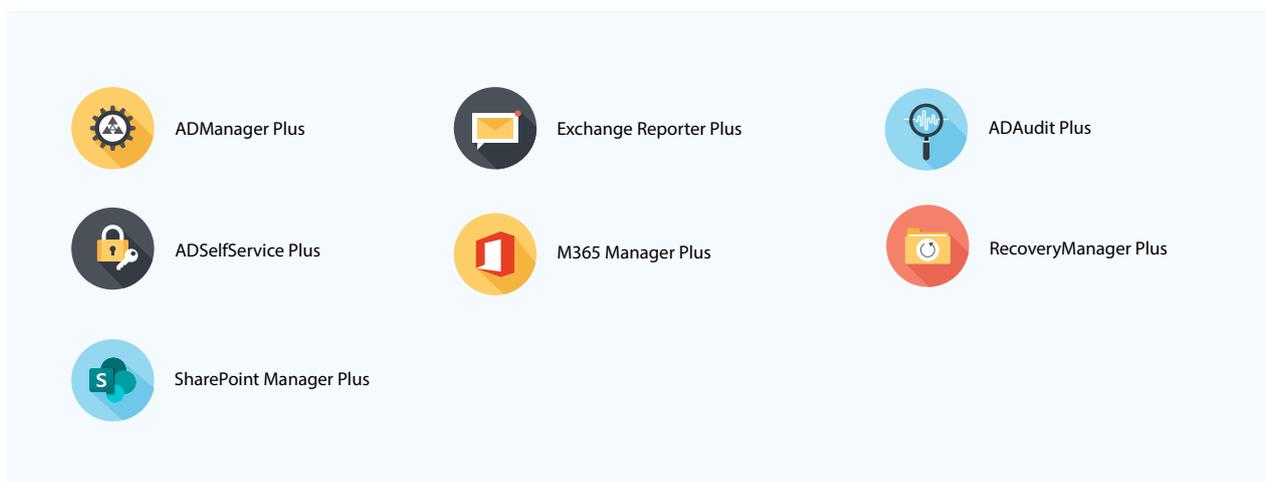
Table of Contents

Introduction	1
High availability for AD360	1
• Centralized configuration	1
• High availability architecture	2
• Important points to consider	2
Prerequisites	3
Configuration steps	3
• Disabling high availability	5

Overview

AD360 is an integrated solution from ManageEngine engineered to holistically address the identity and access management (IAM) needs of enterprises that use Windows Active Directory, Exchange, and Microsoft 365. AD360 solves a number of different challenges when managing AD, Exchange, and Microsoft 365 user identities with features such as user life cycle management, self-service password management, single sign-on, backup and recovery, and IT security and compliance.

AD360 has seven components



High availability for AD360

High availability describes a family of practices designed to deliver a specific level of availability by eliminating or mitigating failure modes.

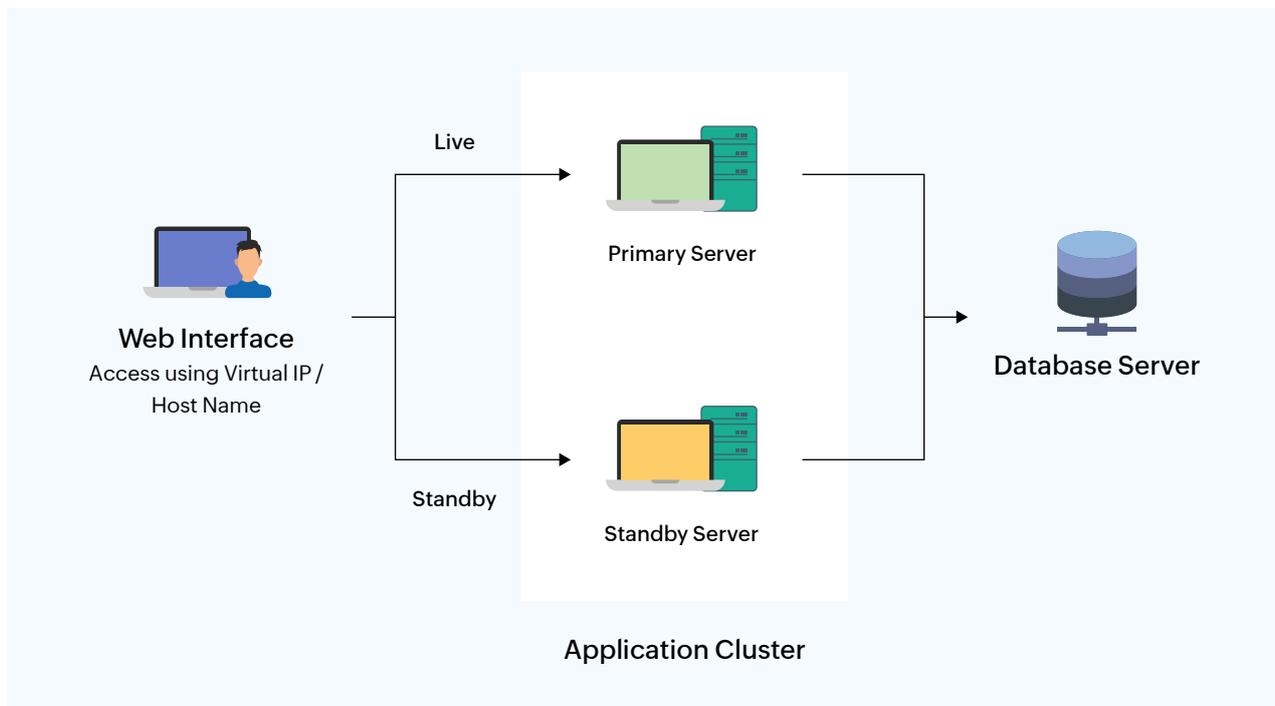
AD360 supports high availability in case of system and application failures. High availability is achieved through automatic failover: when the AD360 service running on one machine fails, another instance of the AD360 service running on a different machine will automatically take over.

Centralized configuration

You can set up and manage high availability for AD360 and its integrated components directly from the AD360 console. Currently, AD360 supports high availability configuration for AD360 and two of its components—ADManager Plus and ADSelfService Plus.

High availability architecture

You can set up and manage high availability for AD360 and its integrated components directly from the AD360 console. Currently, AD360 supports high availability configuration for AD360 and two of its components—ADManager Plus and ADSelfService Plus.



Important points to consider

- To implement high availability, you'll need to install AD360 and its components on two separate machines.
- The instance from which you are configuring high availability will act as the primary server. The other instance will act as the standby server.
- Both servers use the same database configured in the primary server. At any given time, the primary server will cater to user requests while the other will remain passive.
- Whenever the primary server experiences ten or more seconds of downtime, the standby server automatically becomes operational and services all requests.
- You'll need a virtual IP address for high availability configuration.

Prerequisites

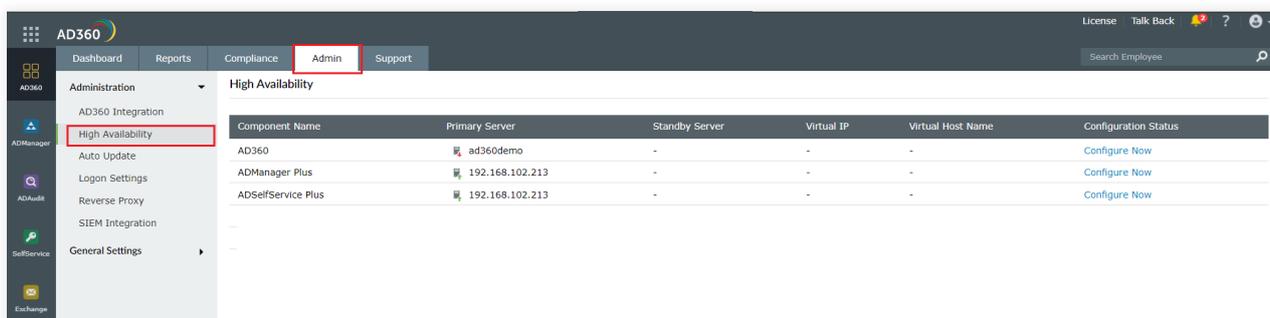
Before you start configuring high availability, ensure the following conditions are satisfied:

- Download and install the latest version of AD360 and its components on two separate machines. If you have already installed AD360 and its components, then update them to the latest build.
- Ensure both instances of AD360 and its components:
 - Are running as a service.
 - Have the same build architecture (32-bit or 64-bit) and build number.
 - Are connected to the same domain and subnet. For example, if your IP range is 172.21.x.x, then the primary server and standby servers should also lie in the IP range 172.21.x.x. Make sure the virtual IP address also lies in the IP range 172.21.x.x.
- The service account used to run AD360 service should have domain admin privileges.

Configuration steps

Follow the steps below to enable high availability.

1. Navigate to **Admin tab > Administration > High Availability**.
2. You will see AD360 and a list of available components that support high availability.



3. The steps for enabling high availability are exactly the same for both AD360 and its components. Let's see how to enable high availability for AD360.
4. Click **Configure Now** in the AD360 row.

High Availability

Primary Server

Component Name

Primary Server URL

Standby Server

* Standby Server Name/IP

* Admin Username

* Password

Virtual IP

* Virtual IP Address

Virtual Host Name

5. In the *Primary Server* section, the URL of the AD360 server you are currently accessing will be auto filled.

6. In the *Standby Server* section, enter the:

- a. URL of the AD360 standby server.
- b. Username and password of the built-in admin account in the AD360 standby server.

Note: For the integrated components, instead of using the default admin account you can provide the credentials of an account that has full access to all the features and settings of the component. For example, an account with super administrator privilege.

7. In the *Virtual IP* section, enter:

- a. A virtual IP address with which you can access both the primary and standby servers. When the product is accessed using this IP, the data is routed directly through the server that is active at that particular time.
- b. The Virtual Host Name.

Note: A virtual host name is the alias given to the virtual IP.

8. Click **Save**.

9. Follow steps 4 through 8 for the integrated components you want to enable high availability.

10. Once the settings are saved, restart the primary server first and then the standby server to activate high availability.

11. Once high availability is enabled, perform the following actions.
 - a. In AD360, add the virtual IP address to the Allowed IPs list (if it's enabled) in **Logon Settings** by navigating to **Admin tab > Administration > Logon Settings > Allow/Restrict IPs**.
 - b. In the ADSelfService Plus component,
 - i. Update the Access URL with the virtual IP address value.
 - ii. Add the virtual IP address value to the Admin Login page IP restriction list (if it's enabled) in **Logon Settings**.

Disabling high availability

High availability can be disabled only from the standby server. Follow the steps below to disable high availability.

1. Shut down the primary server.
2. Access AD360. This will automatically route you to the standby server.
3. Navigate to **Admin tab > High Availability** and click **Remove**.
4. Restart the standby server, and then restart the primary server.

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