ManageEngine
AD360

Required privileges and permissions

Table of Contents

Document summary

AD360 and its components require Domain Admin privileges to carry out all the desired operations. If you do not wish to use a domain admin account, you can use a user account that has been granted sufficient privileges to carry out the desired operations. This guide elaborates all the necessary roles and permissions required for the various features of each component integrated with AD360.

Note: For some components, such as RecoveryManager Plus, you still need an account with admin privilege to use all the features.

Important points to consider

- We recommend configuring each component with a Domain Admin account to access all features without any hitches.

- AD360 automatically synchronizes various data related to domain settings, mail servers, etc., across the integrated components. So when you configure a component, say ADManager Plus, with Domain Admins privilege, the same will be synchronized with other integrated components, such as ADAudit Plus and ADSelfService Plus, even if you have manually configured a user account with lesser privileges in those components.

Required permissions

This section lists the permissions required by each component in AD360 to carry out the desired operations. Based on the components that you have integrated with AD360, you can manually grant only the required permissions to a user account, and configure that account in the integrated components.

Click on the links below to see the permissions required for a particular component.

- ADManager Plus
- ADSelfService Plus
- ADAudit Plus
- Exchange Reporter Plus
- O365 Manager Plus
- RecoveryManager Plus

ADManager Plus

Please refer to the following table which lists the permissions necessary for carrying out different management and reporting operations using ADManager Plus. Once the necessary permissions are granted to an account, configure that account in the Domain Settings of ADManager Plus.

Operation	Permissions Needed
User Management	
Create Users	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have permissions to create, delete, and manage user accounts or equivalent permissions in the relevant OU or container in Active Directory.
Modify Users	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have permissions to create, delete, and manage user accounts or equivalent permissions in the relevant OU or container in Active Directory. **Note:** It is also possible to grant the permissions to modify on specific attributes instead of the object as a whole.
Delete Users	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have permissions to create, delete, and manage user accounts or equivalent permissions in the relevant OU or container in Active Directory.
Computer Management	
Create Computers	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Computer Objects – Create selected objects in this folder' permission, or an equivalent permission in the relevant OU or container in Active Directory.

Modify Computers	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Computer Objects – Create selected objects in this folder: with write permission', or an equivalent permission in the relevant OU or container in Active Directory.
Delete Computers	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Computer Objects – Delete selected objects' permission, or an equivalent permission in the relevant OU or container in Active Directory.
Group Management	
Create Groups	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Create, manage and delete user groups' permission, or an equivalent permission in the relevant OU or container in Active Directory.
Modify Groups	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Create, manage and delete user groups' permission, or an equivalent permission in the relevant OU or container in Active Directory.
Delete Groups	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Create, manage and delete user groups' permission, or an equivalent permission in the relevant OU or container in Active Directory.

Contact Management	
Create Contacts	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Contact Objects – Create selected objects in this folder' permission, or an equivalent permission in the relevant OU or container in Active Directory.
Modify Contacts	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Contact Objects – Create selected objects in this folder: with write permission', or an equivalent permission in the relevant OU or container in Active Directory.
Delete Contacts	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Contact Objects – Delete selected objects in this folder' permission or an equivalent permission in the relevant OU or container in Active Directory.
GPO Management and Reporting	
Create GPOs	Must be a member of Group Policy Creator Owners group.
Enable/disable GPOs	Write permission on the 'flags' attribute of the GPO object to be managed.
Enable/disable user tconfiguration settings	Write permission on the 'flags' attribute of the GPO object to be managed.
Enable/disable computer configuration settings	Must be a member of Group Policy Creator Owners group.

Enable/disable/remove GPO links	• Write permission on the 'gPLink' attribute of the Site/Domain/OU object to add or remove links to them. • Write permission on the 'gPOptions' attribute of the Domain/OU object to Block/Unblock GPO Inheritance in them.
Edit GPO settings	Must be a member of Group Policy Creator Owners group.
Enforce GPO links	Write permission on the 'gPLink' attribute of the Site/Domain/OU object to enforce GPO links to them.
Reporting	• Read permission on the Site/Domain/OU objects (on gPLink attribute). • Read permission on the Domain/OU objects (on gPOptions attribute). • Read permission on the GPO objects (on flags, versionNumber, modifyTimeStamp, createTimeStamp attributes). **Note:** By default, • Domain Users group will have these rights to generate reports. • Domain admins and Enterprise admins will have all the above mentioned rights to perform all management/reporting operations.
File Permission Management	Read and write permissions on the relevant folders.
AD Reporting	
Generate Reports	View permission in the desired OUs/domains.
NTFS Reports	Read permission on the relevant folders.

Exchange Management Creating Exchange mailboxes while creating the corresponding user account in AD	
Exchange 2003	Permission to create a user in AD, and Exchange Administrator to the administrative group where the Exchange Server resides.
Exchange 2007	Must have Exchange Recipient Administrator role and Account Operator role.
Exchange 2010	Must be a part of Organization Management group.
Exchange 2013	Must be a part of Organization Management group.
Creating Exchange mailboxes for existing Active Directory users	
Exchange 2003	Exchange Administrator to the administrative group where the Exchange Server resides.
Exchange 2007	Exchange Recipient Administrator role and Account Operator role.
Exchange 2010	Must be a part of Organization Management group.
Exchange 2013	Must be a part of Organization Management group.
Setting mailbox rights	
Exchange 2003	Exchange View Only administrator role, Administer information store permission on the mailbox store where the mailbox is located.

Exchange 2007	Exchange view only administrator role, Administer information store permission and write permissions on the mailbox store where the mailbox is located.
Exchange 2010	Must be a part of Organization Management group.
Exchange 2013	Must be a part of Organization Management group.
Exchange 2013	Must be a part of Organization Management group.
Exchange Reporting	View Only Administrator role.
Office 365 management and reporting **Management** Recommended: Use an account that has the Global Admin role.	
Office 365 Management	User Management Admin role.
Exchange Online	Exchange Administrator role.
Reporting	
Office 365	View Only Administrator role.
Exchange Online	User Management Admin.

G Suite (Google Apps) management and reporting	
Management	API scopes: https://www.googleapis.com/auth/admin.directory.user https://www.googleapis.com/auth/admin.directory.group https://www.googleapis.com/auth/admin.directory.orgunit
Reporting	API scopes: https://www.googleapis.com/auth/admin.directory.user

Backup and Recovery	
AD backup and recovery	Must be a member of the Domain Admins group

Integrations	
ServiceNow	• To perform AD management actions from ServiceNow console, the user should have **ITIL** and **x_manen_admanager.admanager_admin** roles assigned in ServiceNow. • To raise AD management actions in ServiceNow, the user should have **x_manen_admanager.admanager_requester** role assigned in ServiceNow.
Zendesk	• Must be an administrator to configure ADManager Plusserver details. • **Staff** role privileges to perform AD actions from tickets.
MSSQL	Should have permissions to **Select** for table and schema.
Oracle	Should have permissions to **Select** for table and schema.
Workday	Should have access to the Workday web services and rights to view user details in the organization.
Ultipro	Should be a web service account and have permissions to access the fields used in Data Source - LDAP mapping during configuration
BambooHr	Should have permissions to access the fields used in Data Source - LDAP mapping during configuration.

ADSelfService Plus

Please refer the following table which lists the permissions necessary for carrying out different self-service operations and to leverage other features in ADSelfService Plus. Once the permissions are granted to an account, configure that account in the Domain Settings of ADSelfService Plus.

Operation	Permissions Needed
Self-service password reset	**Reset password** for user objects. **Read pwdLastSet** for user objects. **Write pwdLastSet** for user objects.
Self-service account unlock	**Read lockoutTime** for user objects. **Write lockoutTime** for user objects.
Self-update user attributes	**Read** for user objects. **Write** for user objects. **Note:** It is also possible to grant the permissions to modify read and write on specific attributes instead of the object as a whole.
Synchronize deleted AD user objects	**Allow** Replicating Directory Changes
Display fine-grained password policy	**Read** for msDS-PasswordSettings objects. **Read** for msDS-PasswordSettingsContainer objects.
Self-service mail group subscription	**Read** Members for group objects. **Write** Members for group objects.
NTLM single sign-on	**Create** for computer objects. **Read** for computer objects.
Force enrollment using logon script	**Read scriptPath** for user objects. **Write scriptPath** for user objects.
View deleted users report	Membership in Domain Admins group.
GINA installation	Membership in Domain Admins group.

ADAudit Plus

ADAudit Plus instantly starts auditing Active Directory, when configured with a Domain Admin account. When you do not want to provide a Domain Admin account, manually assign the permissions listed in the table below to a user account. Then configure this account through ADAudit Plus Domain Settings page for data collection, processing and report generation.

Permissions needed	Steps to grant the required permission
Manage Auditing and Security Log Privilege	• Add the user in 'Manage auditing and security log' policy (Computer Configuration → Windows Settings → Security Settings → Local Policies → User Rights Assignment). • Use a GPO and push this setting to all servers that are being audited.
Member of Event Log Readers	• Open Active Directory Users and Computers → Built-in Container. • Add user as a member of Event Log Readers group.
DCOM & WMI Permission	• The user must have the DCOM & WMI permission in the **Domain Controller with the PDC emulator role** of the domain. • **DCOM Permission:** Component Services → Computers → My Computer → Right Click and go to Properties • In **COM Security** tab, **click** Edit Limits of Launch and Activation Permissions. • In Security Limits, add the user and select the **Allow** checkbox for all permissions for that user. • **WMI Permission:** Go to Start → Run 'wmimgmt.msc' → Security Tab → CIMV2 → Security → Add the user and select the **Allow** checkbox for all permissions for that user.
Member of Group Policy Creator Owners	• Open Active Directory Users and Computers → Users Container → Add user as a member of **Group Policy Creator Owners** group.
Member of Local Administrators Group	• Open Local Users and Groups → Groups → Add user as a member of **Local Administrators** group **(On every monitored file servers for file server auditing).**

Exchange Reporter Plus

Exchange Reporter Plus requires an account that has the permissions listed in the table below.

Operations	Permissions needed
Exchange reporting, auditing, and monitoring	The user account should be part of the following groups: • **For Exchange 2010, 2013, and 2016:** Organization Management and Domain Admins groups. • **For Exchange 2003 and 2007:** Exchange View only Administrator and Domain Admins groups.
Email Traffic Reports	• **Exchange 2013 and 2016:** \\ \C$Program Files\Microsoft\ ExchangeServer\V15\TransportRoles\Logs\MessageTracking • **Exchange 2010:** \\ \C$Program Files\Microsoft\ExchangeServer \V14\TransportRoles\Logs\MessageTracking • **Exchange 2007:** \\ \C$\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking.

Outlook Web Access and ActiveSync reports	• The user account must be granted at least **Read Only permission** on the following directories:
	  ◦ IIS 6.0: \\ \C$\WINDOWS\system32\LogFiles\W3SVC1\
	  ◦ IIS 7.0/8.0: \\ \C$\inetpub\logs\LogFiles\W3SVC1\
	• You must enable csCookie in IIS server.

Mailbox and Public Folder Content reports	The user account should have a valid mailbox which, • should not be hidden from the GAL (Global Address List). • should have logged on to their designated mailbox at least once. • Any valid user credential with **send as** and **full access** permissions on the mailboxes, about which information is to be gathered
Public Folder Properties and Conten reports	Read access to Public Folders.
Skype for Business Server Reporting	The user should be a part of CsAdministrator or CsViewOnlyAdministrator group.

Exchange Online reporting and auditing	The user account should be assigned the following roles: • View-Only Audit Logs role • View-Only Configuration role • View-Only Recipient role

O365 Manager Plus

O365 Manager Plus requires the following Office 365 roles and permissions to be assigned to the user account:

Operations	Roles and permissions needed
Exchange Online reporting and auditing	• View-Only Audit Logs role • View-Only Configuration role • View-Only Recipient role
Accessing reporting, auditing, alerting, and monitoring for other services	• Reports Reader role
Office 365 management	• User management administrator role • Exchange administrator role
Office 365 monitoring	• Service administrator role

Email content search	• Permission to access the REST APIs listed below:
	  ◦ Windows Azure Active Directory
	  ◦ Microsoft Graph API

RecoveryManager Plus

RecoveryManager Plus provides administrators the ability to back up and restore their Active Directory, Exchange Server, Exchange Online, SharePoint Online, and OneDrive for Business environments.

The following table will explain the level of privileges required to back up and restore using RecoveryManager Plus.

Operations	Roles and permissions needed	Remarks
Active Directory backup and restoration	• Domain administrator • Schema administrator*	* If you wish to store the passwords of user accounts when they are deleted, ensure that the account configured in RecoveryManager Plus is assigned the schema administrator role. If you choose to save the passwords of user accounts, RecoveryManager Plus will modify the AD schema and instruct AD to retain the Unicode-pwd attribute when a user is deleted. The schema administrator role is required to modify the schema accordingly.
Exchange Server backup and restoration	Organization Management	
Exchange Online backup and restoration	Organization Management	
SharePoint Online backup and restoration	SharePoint admin	
OneDrive for Business backup and restoration	SharePoint admin	

About AD360

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 change monitoring, to single sign-on (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 from within a single console.

$ Get Quote Download