ManageEngine
AD360

Required privileges and permissions

Table of Contents

Document summary

AD360 and its components require varying levels of privileges to carry out all the desired operations. This guide elaborates all the necessary roles and permissions required for the various features of each component integrated with AD360.

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, and more across the integrated components. So, when you configure a component, say ADManager Plus, with Domain Admins privilege, the settings 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 the links below to see the permissions required for a particular component.

- ADManager Plus
- ADSelfService Plus
- ADAudit Plus
- Exchange Reporter Plus
- M365 Manager Plus
- RecoveryManager Plus
- SharePoint Manager 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.

Operation	Permissions Needed
User management	
Create Users	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have Read and Write permissions on all user objects in the required OU or container in AD.
Modify Users	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have Read, Write, and Read All Properties permissions on all user objects in the required OU or container in AD. **Note:** It is also possible to grant the permissions to modify 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 the Delete All Child Objects permission on all user objects in the required OU or container in AD.
Restore users	• The users modifying the permissions on the deleted objects container must be a member of the Domain Admins group. • The Active Directory Application Mode (ADAM) tool has to be downloaded and installed separately in domain controllers running Windows Server 2000 and 2003.
Computer Management	
Create computers	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have the Read and Write permissions on all computer objects in the required OU or container in AD.

Modify Computers	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have the Read, Write, and Read All Properties permissions on all computer objects in the required OU or container in AD.
Delete Computers	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have the Delete All Child objects permission on all computer objects in the required OU or container in AD.
Restore computers	• The users modifying the permissions on the deleted objects container must be a member of the Domain Admins group. • The Active Directory Application Mode (ADAM) tool has to be downloaded and installed separately in domain controllers running Windows Server 2000 and 2003.
Group Management	
Create Groups	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have the Read and Write permissions on all the group objects in the required OU or container in AD.
Modify Groups	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have the Read, Write, and Read All Properties permissions on all the group objects in the required OU or container in AD.
Delete groups	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have the Delete All Child Objects permission on all the group objects in the required OU or container in AD.
Restore groups	• The users modifying the permissions on the deleted objects container must be a member of the Domain Admins group. • The Active Directory Application Mode (ADAM) tool has to be downloaded and installed separately in domain controllers running Windows Server 2000 and 2003.

Contact management	
Create contacts	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have the Read and Write permissions on all contact objects in the required OU or container in AD.
Modify contacts	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have the Read, Write, and Read All Properties permissions on all contact objects in the required OU or container in AD.
Delete contacts	• Must be a member of the built-in Administrators group or Account Operators group, or • Must have the Delete All Child objects permission on all contact objects in the required OU or container in AD.
Restore contacts	• The users modifying the permissions on the deleted objects container must be a member of the Domain Admins group. • The Active Directory Application Mode (ADAM) tool has to be downloaded and installed separately in domain controllers running Windows Server 2000 and 2003.
GPO management and reporting	
Create GPOs	• Must be a member of Group Policy Creator Owners group.
Enable/disable GPOs	• Must have the **Edit setting** permission selected in the GPOs. **Note:** To learn how to delegate Edit setting permissions to a group or user in a GPO, refer to this document.
Enable/disable user configuration settings	• Must have the **Edit setting** permission selected in the GPOs. **Note:** To learn how to delegate permissions to a group or user in a GPO, refer to this document.
Enable/disable computer configuration settings	• Must have the **Edit setting** permission selected in the GPOs. **Note:** To learn how to delegate permissions to a group or user in a GPO, refer to this document.
Enable/disable/remove GPO links	• Must select **Link GPOs** in the Permissions drop-down list. **Note:** To learn how to delegate permissions to link GPOs, refer to this document.

Edit GPO settings	• Must have **Edit setting** permission selected in the GPOs. **Note:** To learn how to delegate permissions to a group or user in a GPO, refer to this document.
Enforce GPO links	• Must select **Link GPOs** in the Permissions drop-down list. Note: To learn how to delegate permissions to link GPOs, refer to this document.
Reporting	• Must have the Read permission on site, domain, and OU objects (gPLink attribute). Must have the Read permission on site, domain, and OU objects (gPOptions attribute). Read permission on GPO objects (flags, versionNumber, modifyTimeStamp, createTimeStamp attributes). Note: By default: ◦ The 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 and reporting operations.
Modify/remove NTFS permissions	• Must have Read and Write permissions on the relevant folders.
Modify/remove share permissions	• The share must be reachable from the machine where ADManager Plus is installed.
AD reporting	
Generate reports	• Must have the View permission in the desired OUs and domains.
NTFS reports	• Must have the Read permission on the relevant folders.

Exchange management **Creating Exchange mailboxes while creating the corresponding user account in AD**	
Exchange 2007	• Must have the Exchange Recipient Administrator role and Account Operator role.
Exchange 2010	• Must be a part of the Organization Management group.
Exchange 2013	• Must be a part of the Organization Management group.
Creating Exchange mailboxes for existing AD users	
Exchange 2007	• Must have the Exchange Recipient Administrator role and Account Operator role.
Exchange 2010	• Must be a part of the Organization Management group.
Exchange 2013	• Must be a part of the Organization Management group.
Setting mailbox rights	
Exchange 2007	• Must have the 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 the Organization Management group.
Exchange 2013	• Must be a part of the Organization Management group.
Exchange reporting	
Exchange reporting	• Must have the Exchange View Only Administrator role.

Microsoft 365 management and reporting

Management

Recommended: Use an account that has the Global Admin role.

Operation	Role name
Manage users, contacts, and groups	• User Administrator
Reset passwords, and block or unblock administrators	• Privileged Authentication Administrator
Manage role assignments in Azure AD	• Privileged Role Administrator
Update mailbox properties	• Exchange Administrator
Manage Microsoft Teams	• Teams Administrator
Get reports on all Microsoft 365 services	• Global Reader

Reporting

Operation	Scope
Get audit logs and mailbox reports	• Security Reader
Exchange Online reporting	• Exchange Administrator

The roles and permissions (minimum scope) required for an Azure AD application configured in ADManager Plus are listed below.

Module	API Name	Permission	Scope
Management	Microsoft Graph	User.ReadWrite.All	Create, modify, delete, or restore users.
		Group.ReadWrite.All	Create, modify, delete, or restore groups. Add or remove group members and owners.
Reporting	Microsoft Graph	User.Read.All	Get user and group member reports.
		Group.Read.All	Get group reports.
		Contacts.Read	Get contact reports.
		Reports.Read.All	Get usage reports.
		Organization.Read.All	Get license detail reports
		AuditLog.Read.All	Get audit-log-based reports.
	Azure Active Directory Graph	Domain.Read.All	Get domain-based reports.

Google Workspace 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	• Must be a member of the Domain Admins group.
Google Workspace	• Must have a service account with Global Administrator privileges for your Google Workspace tenant.

AD migration	
User migration	• Enterprise Admin
Integrations	
ServiceNow	• To perform AD management actions from the ServiceNow console, the user should have the ITIL and x_manen_admanager.admanager_admin roles assigned in ServiceNow. • To raise AD management actions in ServiceNow, the user should have the x_manen_admanager.admanager_requester role assigned in ServiceNow.
Zendesk	• Must be an administrator to configure ADManager Plus server details. • Must have 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.

For more information on how to provide the service account with the required privileges, please refer to this document.

ADSelfService Plus

Please refer to the following table which lists the permissions necessary for carrying out different self-service operations and to leverage other features in 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 the Domain Admins group.
GINA installation	• Membership in the Domain Admins group.
High availability configuration	• Membership in the Domain Admins group.

For more information on how to provide the service account with the required privileges, please refer to this document.

ADAudit Plus

Please refer to the following table which lists the permissions necessary to audit your AD, Azure AD, and file servers in your environment using ADAudit Plus.

Operation	Permissions Needed
Read event logs	• Manage Auditing and Security Log Privilege • Membership in the Event Log Readers group • DCOM Permission • WMI Permission
Configure audit policy automatically	Membership in the Group Policy Creator Owners group.
Audit file shares	Membership in the Local Administrators group.
Audit Azure AD	Microsoft Graph API permissions: • Application.Read.All • AuditLog.Read.All • Directory.Read.All • IdentityRiskEvent.Read.All • Group.Read.All • User.Read.All

Exchange Reporter Plus

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

Operation	Permissions Needed
Essential data gathering **Note:** This is a mandatory requirement to perform other operations	• LDAP Read privilege over all GC Objects • Invoke-Command PowerShell Read privilege • WMI Query Read privilege • Database files Read privilege
Exchange Server distribution list membership	• LDAP Read privilege • View-Only Recipents RBAC
Exchange Server mailbox account properties	• LDAP Read privilege • View-Only Recipents RBAC
Exchange Server public folder properties	• LDAP Read privilege • View-Only Recipents RBAC
Exchange Server traffic logs	• LDAP Read privilege • IIS logs folder access • View-Only Recipents RBAC for Active Sync Reports
Exchange Server OWA logs failed OWA logs	• LDAP Read privilege • View-Only Recipents RBAC
Exchange Server mailbox permission	• LDAP Read privilege • View-Only Recipents RBAC
Exchange Server distribution group permission	• LDAP Read privilege • View-Only Recipents RBAC
Exchange Server content report generation	• LDAP Read privilege • Exchange Web Services Read privilege
Exchange Server audit reports	• Exchange Server Event Logs Read privilege • Domain Controller Event Logs Read privilege

Exchange Server advanced audit reports	• View-Only Audit Logs RBAC • View-Only Configuration RBAC
Exchange Server monitoring	• WMI Query Read privilege • Database Folder path Read access • Invoke-Command PowerShell Read Access - Storage • Monitoring • View-Only Configuration - All Other Categories
Exchange Server content search	• Full access permissions for all mailboxes, or • ApplicationImpersonation roles

Exchange Online

Operation	Role name	Scope
Reporting	Global Reader	Get reports on all Microsoft 365 services.
	Security Reader	Get audit logs and mailbox reports.
Auditing	Security Reader	Get audit logs and sign-in reports.

The roles and permissions, or minimum scope, required by an Azure AD application configured for Exchange Reporter Plus are listed below.

Module	API Name	Permission	Scope
Reporting	Microsoft Graph	User.Read.All	Get user and group member reports.
		Group.Read.All	Get group reports.
		Contacts.Read	Get contact reports.
		Files.Read.All	Get OneDrive for Business reports.
		Reports.Read.All	Get usage reports.

		Organization.Read.All	Get license detail reports.
		AuditLog.Read.All	Get audit-log-based reports.
		ChannelMember.Read.All (not available in Chinese tenant)	Get Microsoft Teams channel member reports.
		Application.Read.All	Get Azure AD application details.
		Sites.Read.All	Get SharePoint site details.
		Policy.Read.All	Configure conditional access policy details.
		Calendars.Read	Get users' calendar details.
	Office 365 Management	ActivityFeed.Read	Read the audit data for the organization.
Auditing	Office 365 Management	ActivityFeed.Read	Read the activity data for the organization.

Skype for Business Server reporting

Skype for Business Server Reporting	• The user should be a part of CsAdministrator or CsViewOnlyAdministrator group.

For more information on how to provide the service account with the required privileges, please refer to this document.

M365 Manager Plus

The roles and permissions, or minimum scope, required by a service account configured for M365 Manager Plus are listed below.

Operation	Role name	Scope
Management	User administrator	Manage users, contacts, and groups.
	Privileged Authentication Administrator	Reset passwords, and block or unblock administrators.
	Privileged Role Administrator	Manage role assignments in Azure AD.
	Exchange Administrator	Update mailbox properties.
	Teams Administrator	Manage Microsoft Teams.
Reporting	Global Reader	Get reports on all Microsoft 365 services.
	Security Reader	Get audit logs and mailbox reports.
Auditing and alerting	Security Reader	Get audit logs and sign-in reports.

Note:

- If an Azure AD application is not configured for M365 Manager Plus, the **Service Support Administrator** role is required for the Monitoring feature.

- An Azure AD application needs to be configured for M365 Manager Plus in order to use the **Content Search** feature.

The roles and permissions, or minimum scope, required by an Azure AD application configured for M365 Manager Plus are listed below.

Module	API Name	Permission	Scope
Management	Microsoft Graph	User.ReadWrite.All	Create, modify, delete, or restore users.
		Group.ReadWrite.All	Create, modify, delete, or restore groups. Add or remove group members and owners.
		AdminsitrativeUnit. ReadWrite.All	Add members to administrative units.
		RoleManagement. ReadWrite.Directory	Add directory roles to users.
Reporting	Microsoft Graph	User.Read.All	Get user and group member reports.
		Group.Read.All	Get group reports.
		Contacts.Read	Get contact reports.
		Files.Read.All	Get OneDrive for Business reports.
		Reports.Read.All	Get usage reports.
		Organization.Read.All	Get license detail reports.
		AuditLog.Read.All	Get audit-log-based reports.
		ChannelMember.Read.All (not available in Chinese tenant)	Get Microsoft Teams channel members report.
		Application.Read.All	Get Azure AD application details.
		Sites.Read.All	Get SharePoint site details.
		Policy.Read.All	Configure conditional access policy details.
		Calendars.Read	Get users' calendar details.
	Office 365 Management	ActivityFeed.Read	Read the audit data for the organization.

Auditing and Alerting	Office 365 Management	ActivityFeed.Read	Read the activity data for the organization.
Monitoring	Microsoft Graph	ServiceHealth.Read.All	Get health and performance reports.
Content Search	Microsoft Graph	Mail.Read	Get content search reports.
Configuration	Microsoft Graph	Application.ReadWrite.All	Modify the application details.

RecoveryManager Plus

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

Operation	Role name	Scope
AD 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.
Azure AD backup and restoration	Administrator with the global admin role	
Exchange backup and restoration	Administrator who's a member of the organization management role group	
Exchange Online backup and restoration	SharePoint administrator	
Google Workspace backup and restoration	Google Workspace domain administrator	

SharePoint Manager Plus

SharePoint Manager Plus requires the following Microsoft 365 roles and permissions to be assigned to the user account.

SharePoint on-premises

Note: The site collection admin permission is required for the respective site collections to perform any operations.

Operation	Permissions Needed
Reporting, management, and migration	• User should be a member of the built-in administrator group of the SharePoint server. • User should be a member of the Farm Administrators group. Open Central Web Administration and add the user to the Farm Administrator group. • Require this GPO setting if the product is not installed on a SharePoint server.
Auditing	Site collection audit settings must be enabled for the respective site collections.
IIS log reports	User should be a member of the built-in administrator group of the IIS server.

Microsoft 365 SharePoint

Note: The site collection admin permission is required for the respective site collections to perform any operations.

For the service account used to configure SharePoint Manager Plus

Reporting, management, and migration	SharePoint administrator role
Auditing	Audit log and View only audit log roles

For Azure applications	
Reporting, management, and migration	Sites.FullControl.All
Auditing	Office 365 Exchange Onlin
Monitoring	Office 365 Management APIs
Mail server	Microsoft Graph

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

About 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