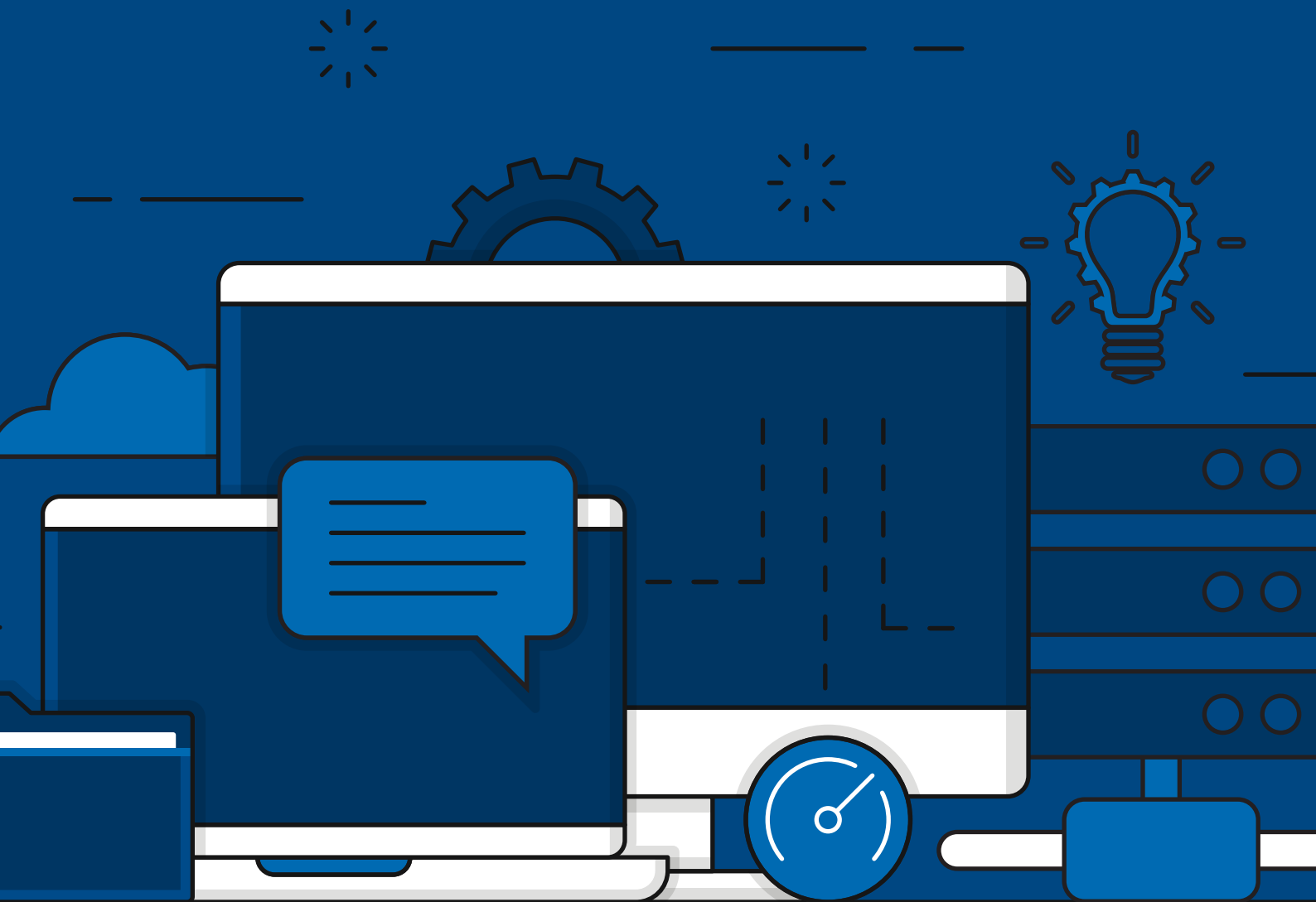
ManageEngine
AD360

System and port requirements



System requirements

Hardware requirements

The following table lists the recommended hardware requirements for ManageEngine AD360 and its components. The RAM and required disk space may vary based on the components you've integrated with AD360 and the amount of data processed by each component.

Hardware		Recommended
Processor		**3GHz or faster**
Screen resolution		1,024x768 pixels or higher
RAM	AD360	4GB **Note:** Based on the components that you integrate with AD360, you will have to allocate additional RAM for the product to run at optimal efficiency. Please check the following rows for the additional RAM required by each individual component. If you plan on integrating more than two components with AD360, we recommend you install no more than two components on a single machine.
	ADManager Plus	6GB (8GB if it is a virtual machine)
	ADAudit Plus	16GB
	ADSelfService Plus	16GB
	Exchange Reporter Plus	16GB
	M365 Manager Plus	16GB
	RecoveryManager Plus	16GB
	SharePoint Manager Plus	8GB* (16GB if it is a virtual machine)
Disk space	AD360	10GB minimum **Note:** Based on the components that you integrate with AD360, you will have to ensure additional disk space. Please refer to the following rows for the recommended disk space required by each component.
	ADManager Plus	50GB **Note:** Based on the number of scheduled reports and automations running in parallel, additional disk space might be necessary.

	ADAudit Plus	100GB **Note:** Based on the number of users and audit events captured, additional disk space might be necessary.
	ADSelfService Plus	200GB (SSD preferred)
	Exchange Reporter Plus	200GB (SSD preferred) **Note:** Based on your organization's size, mailbox size, traffic volume, and Outlook Web Access logins, additional disk space might be necessary.
	M365 Manager Plus	500GB (SSD preferred) **Note:** Based on your tenant size, mailbox size, and traffic volume, additional disk space might be necessary.
	RecoveryManager Plus	**Active Directory and Entra ID Backup:** This requirement varies based on the number of AD objects, Entra ID objects, the size of your domain controller, and the retention period that you set for your backups. RecoveryManager Plus has a best case compression ratio of 2:1 for domain controller backups. **Exchange, Microsoft 365, Google Workspace, and Zoho Workdrive Backup:** This requirement varies based on the number of backed-up Exchange (on-premises and online) mailboxes, the size of your SharePoint Online and OneDrive for Business sites, size of your Zoho WokrDrive teams, and the retention period that you set for your backups. If the total size of the mailboxes, SharePoint Online, and OneDrive for Business sites is 1TB, make sure that you have 1TB of free disk space to store the full backup and all subsequent incremental backups.
	SharePoint Manager Plus	50GB

Software requirements

Supported platforms

ManageEngine AD360 can be installed in the following operating systems.

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows 11
- Windows 10
- Windows 8
- Windows 7

The ADAudit Plus component can audit the following environments.

- Windows Server 2003 and above
- Azure Active Directory (Check system requirements under 'Via Office365 Cmdlet')
- AD FS 2.0 and above
- Windows workstations XP and above
- Windows File Server 2003 and above
- NetApp Filer - Data ONTAP 7.2 and above
- NetApp Cluster - Data ONTAP 8.2.1 and above
- EMC Storage Systems - Celerra, VNX, VNXe, Unity, and Isilon
- Windows Failover Cluster with SAN
- Synology - DSM 5.0 and above

The Exchange Reporter Plus component can manage, audit, and report on the following environments.

- Exchange Server 2019
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010
- Exchange Server 2007
- Exchange Server 2003

The RecoveryManager Plus component can backup and restore the following AD environments.

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

The RecoveryManager Plus component can backup and restore the following Exchange environments.

- Exchange Server 2019
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 SP3
- Exchange Server 2010 SP2
- Exchange Server 2010 SP1

The SharePointManager Plus component can manage, audit, and secure the following SharePoint environments.

- SharePoint Online
- SharePoint 2019
- SharePoint 2016
- SharePoint 2013
- SharePoint 2010
- SharePoint Subscription Edition

Supported browsers

AD360 requires one of the following browsers to be installed in the system:

- Internet Explorer 9 and above
- Microsoft Edge (all versions)
- Mozilla Firefox 4 and above
- Google Chrome 10 and above

Supported databases

ManageEngine AD360 and its components support the following databases.

- PostgreSQL (the default database bundled with the product)
- Microsoft SQL Server

Product ports

The following table lists the default ports used by AD360 and its components. They can be modified during or after installation.

Product	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 following ports are common across all components in AD360.
Allow outbound and inbound connections to all the ports listed below on the source and destination server respectively.

Required ports	Protocols	Service	Source	Destination
25	SMTP	SMTP	AD360	SMTP
88	TCP and UDP	Kerberos	AD360	Domain controllers
135	TCP	RPC	AD360	Domain controllers
139	TCP	NetBIOS session	AD360	Domain controllers
389	TCP and UDP	LDAP	AD360	Domain controllers
445	TCP and UDP	SMB	AD360	Domain controllers
636	TCP and UDP	LDAP over SSL	AD360	Domain controllers
3268	TCP	LDAP using Global Catalog	AD360	Domain controllers
3269	TCP	LDAP SSL using Global Catalog	AD360	Domain controllers
49152, 65535*	TCP	RPC	AD360	RPC randomly allocated high TCP ports

Component-specific ports

Besides the ports listed in the above tables, you will also need to open the following ports based on the services used by each component.

Required ports	Protocols	Service	Source	Destination
ADManager Plus				
80, 443	HTTP/HTTPS	Microsoft 365 or Google Workspace servers	ADManager Plus server	Microsoft 365 and Google Workspace
ADAudit Plus				
137	TCP and UDP	NetBIOS name resolution RPC/ named pipes (NP)	ADAudit Plus server	Monitored computers
138	UDP	NetBIOS datagram	ADAudit Plus server	Monitored computers
139	TCP	NetBIOS session RPC/NP	ADAudit Plus server	Monitored computers
445	TCP and UDP	SMB RPC/NP	ADAudit Plus server	Monitored computers
465	TCP	SSL	ADAudit Plus server	SMTP servers
587	TCP	TLS	ADAudit Plus server	SMTP servers
ADSelfService Plus				
42	TCP	Host name server protocol	ADSelfService Plus server	Domain controller
53	TCP/UDP	DNS	ADSelfService Plus server	DNS server
67	UDP	DHCP	ADSelfService Plus server	DHCP server
137	UDP	NetBIOS	ADSelfService Plus server	Domain controller
138	UDP	Netlogon	ADSelfService Plus server	Domain controller

139	TCP	Netlogon	ADSelfService Plus server	Domain controller
464	TCP/UDP	Kerberos	ADSelfService Plus server	Domain controller
593	TCP/UDP	RPC	ADSelfService Plus server	Domain controller
2535	TCP/UDP	DHCP	ADSelfService Plus server	Domain controller
5985	TCP	WinRM-HTTP	ADSelfService Plus server	Domain controller
Exchange Reporter Plus				
53	TCP	DNS	Exchange Reporter Plus server	Domain controller
80	TCP	PowerShell	Exchange Reporter Plus server	Exchange server
443 (SSL)	TCP	PowerShell	Exchange Reporter Plus server	Exchange server
445	TCP and UDP	Log collection	Exchange Reporter Plus server	Monitored servers
5985	TCP	Windows PowerShell default psSession port	Exchange Reporter Plus server	Exchange server
5986	TCP	Windows PowerShell default psSession port	Exchange Reporter Plus server	Domain controller
M365 Manager Plus				
80	TCP	PowerShell	M365 Manager Plus server	Microsoft 365
443 (SSL)	TCP	PowerShell	M365 Manager Plus server	Microsoft 365

465	TCP	SSL	M365 Manager Plus server	SMTP server
587	TCP	TLS	M365 Manager Plus server	SMTP server
RecoveryManager Plus				
80	TCP	Powershell	Recovery Manager Plus server	Exchange Server
443	TCP	Powershell	Recovery Manager Plus server	Exchange Server
137	UDP	Netlogon	Recovery Manager Plus server	Domain controller
138	UDP	Netlogon	Recovery Manager Plus server	Domain controller
443	HTTPS	Microsoft 365 and Google Workspace	Recovery Manager Plus server	Microsoft 365 and Google Workspace
443 (SSL)	TCP	Powershell	Recovery Manager Plus server	Microsoft 365
464	TCP and UDP	Kerberos change/ set password	Recovery Manager Plus server	Domain controller
5985	TCP	Windows Power Shell default psSession port	Recovery Manager Plus server	Domain controller
5986 (SSL)	TCP	Windows Power Shell default psSession port	Recovery Manager Plus server	Domain controller
9290	HTTPS	Elasticsearch database	Recovery Manager Plus server	Elasticsearch database
33310	TCP	Postgres database	Recovery Manager Plus server	RecoveryManager Plus server

SharePoint Manager Plus				
80	HTTPS	Microsoft 365 SharePoint	SharePoint Manager Plus server	Microsoft 365
443	HTTPS	Microsoft 365 SharePoint	SharePoint Manager Plus server	Microsoft 365
368/639	TCP and UDP	Connect to Active Directory	SharePoint Manager Plus server	Domain controller
445	TCP/SMB	To collect IIS logs	SharePoint Manager Plus server	IIS server
5985	TCP	Windows PowerShell default psSession port	SharePoint Manager Plus server	SharePoint server
5986 (SSL)	TCP	Windows PowerShell default psSession port	SharePoint Manager Plus server	SharePoint server
9200	TCP	Elasticsearch database	Elasticsearch database	SharePoint Manager Plus server
33315	TCP	Database port	SharePoint Manager Plus server	SharePoint Manager Plus server

***Note:** If you are using Windows Firewall, you can open dynamic ports 49152-65535 on the monitored computers by enabling the inbound rules listed below.

1. Remote Event Log Management (NP-In)
2. Remote Event Log Management (RPC)
3. Remote Event Log Management (RPC-EPMAP)

If you still face any issue after opening all these ports, please refer this link. Open the ports mentioned in the above link based on the operating system you're running.

Microsoft SQL database-related ports

If an external Microsoft SQL database is used, the following ports have to be opened:

Port	Protocol	Service
1433	TCP	To communicate with the Microsoft SQL Server default instance.
1434	UDP	To communicate with the Microsoft SQL Server default instance.