ManageEngine ADManager Plus

Permissions required for the AD account configured in ADManager Plus



Table of contents

Use	er Management	
i	Create Users	
ii	Modify Users	
iii	Delete Users	
iv	Restore users	
Со	ntact Management	
i	Create Contacts	
ii	Modify Contacts	
iii	Delete Contacts	
iv	Restore Contacts	
Со	mputer Management	
i	Create Computers	
ii	Modify Computers	
iii	Delete Computers	
iv	Restore Computers	
Gro	oup Management	
i	Create Groups	
ii	Modify Groups	
iii	Delete Groups	
iv	Restore Groups	
GP	O Management and Reporting	
AD	Reporting	
File	e Permission Management	
Exc	change Management and Reporting	
Mio	crosoft 365 Management and Reporting	
Act	tive Directory migration	
Go	ogle Workspace Management and Reporting	
Hig	gh Availability	

To carry out the desired Active Directory (AD) management and reporting operations,

ADManager Plus must be provided with the necessary permissions. This can be done by entering the credentials of a user account which has been granted the necessary permissions in the Domain Settings section ADManager Plus' Admin tab.

To modify Privileged Groups, you need to log in with a user account that is a member of the Administrators Group. If you do not want to use a domain admin account, you can log in with a user account that has been granted sufficient privileges to carry out the necessary operations.

The following sections contain the least privileges that have to be assigned to a user account for performing the required operation.

User Management

This section provides a detailed explanation on the permissions required to create, modify and delete user accounts.

Operation: Create users

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Read and Write permissions on all user objects of the required OU.

Steps to grant the permissions to create a user account.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control**. The Delegation of Control wizard will pop-up
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- 5. Select the **Only objects in this folder** option and select the **User objects** checkbox. Also select the **Create selected objects** in this folder option as indicated in the following image.

ndicate the scope of the task you want to delegate.	
Delegate control of:	
This folder, existing objects in this folder, and creation of	new objects in this folder
Only the following objects in the folder:	
transportStack objects	^
Trusted Domain objects	
v User objects x25Stack objects	
x25×400Link objects	
x400Link objects	~
Create selected objects in this folder	0105
Delete selected objects in this folder	
x400Link objects x400Link objects Create selected objects in this folder Delete selected objects in this folder	

- Click on Next. Under the Show these permissions section, select General and Property-specific options.
- Under the permissions section, select the Read and Write permissions and click on Next as indicated in the following image.

Select the permissions you want to delegate.	Ĩ
Show these permissions:	
General	
Property-specific	
Creation/deletion of specific child objects	
Permissions:	
Full Control	^
Read	
Write	
Create All Child Objects	
Delete All Child Objects	
Read All Properties	~

8. Click Finish.

Operation: Modify users

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Read, Write, Read All Properties permissions on all user objects of the required OU.

Steps to grant the permissions to modify a user account.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- 5. Select the **Only objects in this folder** option and select the **User objects** option as indicated in the following image.

Active Directory Object Type Indicate the scope of the task you want to delegate.	
Delegate control of:	
O This folder, existing objects in this folder, and creation	of new objects in this folder
Only the following objects in the folder:	
transportStack objects	^
Trusted Domain objects	
✓ User objects	
x25X400Link objects	
x400Link objects	~
Create selected objects in this folder	
Delete selected objects in this folder	
Delete selected objects in this folder	

- Click on Next. Under the Show these permissions section, select General and Property-specific options.
- 7. Under the permissions section, select the **Read**, **Write and Read all properties** permissions and click on **Next** as indicated in the following image.

Permissions	(P)
Select the permissions you want to delegate.	Į.
Show these permissions:	
General	
Property-specific	
Creation/deletion of specific child objects	
Permissions:	-
Permissions:	^
Permissions: Full Control Read	^
Permissions: Full Control Read Write	^
Permissions: Full Control Read Write Create All Child Objects	^
Permissions: Full Control Read Write Create All Child Objects Delete All Child Objects	^
Permissions: Full Control Read Write Create All Child Objects Delete All Child Objects Read All Properties	-
Permissions: Full Control Read Write Create All Child Objects Delete All Child Objects Read All Properties	•

8. Click Finish.

Operation: Delete users

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Delete All Child Objects permission on all user objects of the required OU.

Steps to grant the permissions to delete a user account.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control**. The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- Select the Only objects in this folder option and select the User objects checkbox.
 Also select the Delete selected objects in this folder option as indicated in the following image.

Indicate the scope of the task you want to delegate.	9
Delegate control of:	
O This folder, existing objects in this folder, and creation of	new objects in this folder
Only the following objects in the folder:	
transportStack objects	^
Trusted Domain objects	
User objects	
x25Stack objects	
x25X400Link objects	
	*
Create selected objects in this folder	
Delete selected objects in this folder	

- Click on Next. Under the Show these permissions section, select General and Creation/Deletion of specific child objects options.
- Under the permissions section, select the Delete all child objects permission and click on Next as indicated in the following image.

	(a)
Select the permissions you want to delegate.	ľ
Show these permissions:	
✓ General	
Property-specific	
Creation/deletion of specific child objects	
P <u>e</u> rmissions:	
Full Control	^
Write	
Head Write Create All Child Objects	
☐ Head ☐ Wite ☐ Create All Child Objects ☑ Delete All Child Objects	
 ☐ Read ☐ Write ☐ Create All Child Objects ☑ Delete All Child Objects ☐ Read All Properties 	Ţ.
☐ Read ☐ Write ☐ Create All Child Objects ☑ Delete All Child Objects ☐ Read All Properties	v

8. Click Finish.

Operation: Restore users

Permissions needed:

- 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.

Steps to grant the permissions required to restore a deleted AD user

Any object deleted from AD is stored in the deleted objects container and can be restored before the end of its tombstone lifetime period. To restore a deleted AD object, non-administrators must have sufficient permission to access this container. To grant the required permissions:

- 1. Log in to your **domain controller** and launch the ADAM tools Command Prompt.
- 2. Specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus, DC=com" /takeownership



Note:

- Every domain in a forest will have its own deleted objects container, so it's essential to specify the domain name of the deleted objects container for which you would like to modify permissions.
- Replace **admanagerplus** and **com** with your domain components.
- To grant permission to a security principal to access the deleted objects container, specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP



Note: Replace "LukeJohnson" with the security principal of your choice.

- 4. Next, connect to the default naming context, right-click on the domain root, and select Properties.
- 5. In the **Security** tab, click **Advanced.**
- 6. Add the user or group, and select the following rights:
 - a. Reanimate tombstones

B	Permission Entry for lyncforb	
Delete mslmaging-PSPs objects	Create Shared Folder objects	^
Create MSMQ Queue Alias objects	Delete Shared Folder objects	
Delete MSMQ Queue Alias objects	Create User objects	
Create msPKI-Key-Recovery-Agent object	cts Delete User objects	
Delete msPKI-Key-Recovery-Agent object	ts 🗌 Add GUID	
Create msRTCSIP-ApplicationContacts o	bjects 🗌 Add/remove replica in domain	
Delete msRTCSIP-ApplicationContacts o	bjects Allow a DC to create a clone of itself	
Create msRTCSIP-ConferenceDirectories	objects Change PDC	
Delete msRTCSIP-ConferenceDirectories	objects 🗌 Create inbound forest trust	
Create msRTCSIP-ConferenceDirectory o	bjects Enable per user reversibly encrypted password	
Delete msRTCSIP-ConferenceDirectory o	bjects Generate resultant set of policy (logging)	
Create msRTCSIP-Domain objects	Generate resultant set of policy (planning)	_
Delete msRTCSIP-Domain objects	Manage replication topology	=
Create msRTCSIP-EdgeProxy objects	Migrate SID history	
Delete msRTCSIP-EdgeProxy objects	Monitor active directory replication	
Create msRTCSIP-GlobalContainer objec	ts Read only replication secret synchronization	
Delete msRTCSIP-GlobalContainer object	ts 🖌 Reanimate tombstones	
Create msRTCSIP-GlobalTopologySetting	g objects Replicating Directory Changes	
Delete msRTCSIP-GlobalTopologySetting	g objects Replicating Directory Changes All	
Create msRTCSIP-GlobalTopologySetting	gs objects 🛛 Replicating Directory Changes In Filtered Set	
Delete msRTCSIP-GlobalTopologySetting	gs objects Replication synchronization	
Create msRTCSIP-LocationContactMapp	oing objects Run Protect Admin Groups Task	
Delete msRTCSIP-LocationContactMapp	ing objects 🛛 Unexpire password	
Create msRTCSIP-LocationContactMapp	oings objects Update password not required bit	
Delete msRTCSIP-I ocationContactMapp	inas obiects	¥
		OK Cancel

b. Create User objects

Permissi	on Entry for lyncforb	
Create msDS-GroupManagedServiceAccount objects	Delete oncRpc objects	
Delete msDS-GroupManagedServiceAccount objects	Create Organizational Unit objects	
Create msDS-ManagedServiceAccount objects	Delete Organizational Unit objects	
Delete msDS-ManagedServiceAccount objects	Create Printer objects	
Create msDS-QuotaContainer objects	Delete Printer objects	
Delete msDS-QuotaContainer objects	Create rFC822LocalPart objects	
Create msImaging-PSPs objects	Delete rFC822LocalPart objects	
Delete mslmaging-PSPs objects	Create Shared Folder objects	
Create MSMQ Queue Alias objects	Delete Shared Folder objects	
Delete MSMQ Queue Alias objects	✓ Create User objects	
Create msPKI-Key-Recovery-Agent objects	Delete User objects	
Delete msPKI-Key-Recovery-Agent objects	Add GUID	
Create msRTCSIP-ApplicationContacts objects	Add/remove replica in domain	
Delete msRTCSIP-ApplicationContacts objects	Allow a DC to create a clone of itself	
Create msRTCSIP-ConferenceDirectories objects	Change PDC	
Delete msRTCSIP-ConferenceDirectories objects	Create inbound forest trust	
Create msRTCSIP-ConferenceDirectory objects	Enable per user reversibly encrypted password	
Delete msRTCSIP-ConferenceDirectory objects	Generate resultant set of policy (logging)	
Create msRTCSIP-Domain objects	Generate resultant set of policy (planning)	
Delete msRTCSIP-Domain objects	Manage replication topology	
Create msRTCSIP-EdgeProxy objects	Migrate SID history	
Delete msRTCSIP-EdgeProxy objects	Monitor active directory replication	
Create msRTCSIP-GlobalContainer objects	Read only replication secret synchronization	
Delete msRTCSIP-GlobalContainer objects	Reanimate tombstones	
Crosta mcBTCSID GlabalTanalam Setting abjects	Poplicating Directory Changes	

c. Write all properties

		Permissio	n Entry for lyncforb	
Principal:	adminUser (adminUser@lyncforb.local)	Select a principal		
Туре:	Allow	*		
Applies to:	This object and all descendant objects	~		
Permissions	5:			
	Full control		Create msRTCSIP-MCUFactories objects	
	List contents		Delete msRTCSIP-MCUFactories objects	
	Read all properties		Create msRTCSIP-MCUFactory objects	
	Write all properties		Delete msRTCSIP-MCUFactory objects	
	Delete		Create msRTCSIP-MonitoringServer objects	
	Delete subtree		Delete msRTCSIP-MonitoringServer objects	
	Read permissions		Create msRTCSIP-Pool objects	
	Modify permissions		Delete msRTCSIP-Pool objects	
	Modify owner		Create msRTCSIP-Pools objects	
	All validated writes		Delete msRTCSIP-Pools objects	
	All extended rights		Create msRTCSIP-TrustedMCU objects	
	Create all child objects		Delete msRTCSIP-TrustedMCU objects	
	Delete all child objects		Create msRTCSIP-TrustedMCUs objects	
	Create Computer objects		Delete msRTCSIP-TrustedMCUs objects	
	Delete Computer objects		Create msRTCSIP-TrustedProxies objects	
	Create Contact objects		Delete msRTCSIP-TrustedProxies objects	

Note: Apply the Reanimate tombstones rights to the object being secured and its descendant objects.

7. Click **OK**.

Note: Only objects deleted after the delegation of the above-mentioned permissions can be restored.

Contact Management

This section provides a detailed explanation on the permissions required to create, modify and delete contacts in AD.

Operation: Create contacts

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Read and Write permissions on all contact objects of the required OU.

Steps to grant the permissions to create a contact account.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- Select the Only objects in this folder option and select the Contact objects checkbox.
 Also select the Create selected objects in this folder option as indicated in the image below:

Delegate control of:	
O This folder, existing objects in this folder, and creation of new object	ts in this folder
Only the following objects in the folder:	
certification Authority objects	^
Computer objects	
Connection objects	
Contact objects	
document objects	
	*

- Click on Next. Under the Show these permissions section, select General and Property-specific options.
- 7. Under the permissions section, select the Read and Write permissions and click on Next.
- 8. Click Finish.

Operation: Modify contacts

- Permissions needed:
- Must be a member of the Account Operators Group
- Must have the Read, Write, Read All Properties permissions on all user objects of the required OU.

Steps to grant the permissions to modify a contact account.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- 5. Select the **Only objects in this folder** option and select the Contact objects option as indicated in the following image.

Indicate the scope of the	e task you want to delegate.		
Delegate control of:			
O This folder, existing o	bjects in this folder, and creatio	n of new objects in this folde	r
Only the following ob	ects in the folder:		
certification Aut	nority objects		^
Computer object	ts		
Connection obj	ects		

document Serie	s objects		
<u> </u>			*
Create selected	bjects in <mark>t</mark> his folder		
Delete selected	bjects in this folder		

- Click on Next. Under the Show these permissions section, select General and Property-specific options.
- 7. Under the permissions section, select the **Read**, **Write** and **Read all properties** permissions and click on **Next**.
- 8. Click Finish.

Operation: Delete contacts

- Permissions needed:
- Must be a member of the Account Operators Group
- Must have the Delete All Child objects permission on all contact objects of the required OU.

Steps to grant the permissions to delete a contact account.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option.
- 5. Select the Only objects in this folder option and select the Contact objects checkbox.Also select the Delete selected objects in this folder option as depicted in the image below:

Indicate the scope of the task you want to delegate.	Ĩ
Delegate control of:	
\bigcirc This folder, existing objects in this folder, and creation of	new objects in this folder
Only the following objects in the folder:	
certification Authority objects	^
Computer objects	
document objects	
document Series objects	~
VI Delete selected objects in this folder	

- Click on Next. Under the Show these permissions section, select General and Creation/Deletion of specific child objects options.
- 7. Under the permissions section, select the Delete all child objects permission and click on Next.
- 8. Click Finish.

Operation: Restore contacts

Permissions needed:

-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.

Steps to grant the permissions required to restore a deleted AD contact

Any object deleted from AD is stored in the deleted objects container and can be restored before the end of its tombstone lifetime period. To restore a deleted AD object, non-administrators must have sufficient permission to access this container. To grant the required permissions:

- 1. Log in to your **domain controller** and launch the ADAM tools Command Prompt.
- 2. Specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus, DC=com" /takeownership



Note:

- Every domain in a forest will have its own deleted objects container, so it's essential to specify the domain name of the deleted objects container for which you would like to modify permissions.
- Replace **admanagerplus** and **com** with your domain components.
- To grant permission to a security principal to access the deleted objects container, specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP



Note: Replace "LukeJohnson" with the security principal of your choice.

- 4. Next, connect to the default naming context, right-click on the domain root, and select Properties.
- 5. In the **Security** tab, click **Advanced.**
- 6. Add the user or group, and select the following rights:
 - a. Reanimate tombstones

Permissi	ion Entry for lyncforb	
Delete msImaging-PSPs objects	Create Shared Folder objects	
Create MSMQ Queue Alias objects	Delete Shared Folder objects	
Delete MSMQ Queue Alias objects	Create User objects	
Create msPKI-Key-Recovery-Agent objects	Delete User objects	
Delete msPKI-Key-Recovery-Agent objects	Add GUID	
Create msRTCSIP-ApplicationContacts objects	Add/remove replica in domain	
Delete msRTCSIP-ApplicationContacts objects	Allow a DC to create a clone of itself	
Create msRTCSIP-ConferenceDirectories objects	Change PDC	
Delete msRTCSIP-ConferenceDirectories objects	Create inbound forest trust	
Create msRTCSIP-ConferenceDirectory objects	Enable per user reversibly encrypted password	
Delete msRTCSIP-ConferenceDirectory objects	Generate resultant set of policy (logging)	
Create msRTCSIP-Domain objects	Generate resultant set of policy (planning)	
Delete msRTCSIP-Domain objects	Manage replication topology	
Create msRTCSIP-EdgeProxy objects	Migrate SID history	
Delete msRTCSIP-EdgeProxy objects	Monitor active directory replication	
Create msRTCSIP-GlobalContainer objects	Read only replication secret synchronization	
Delete msRTCSIP-GlobalContainer objects	Reanimate tombstones	
Create msRTCSIP-GlobalTopologySetting objects	Replicating Directory Changes	
Delete msRTCSIP-GlobalTopologySetting objects	Replicating Directory Changes All	
Create msRTCSIP-GlobalTopologySettings objects	Replicating Directory Changes In Filtered Set	
Delete msRTCSIP-GlobalTopologySettings objects	Replication synchronization	
Create msRTCSIP-LocationContactMapping objects	Run Protect Admin Groups Task	
Delete msRTCSIP-LocationContactMapping objects	Unexpire password	
Create msRTCSIP-LocationContactMappings objects	Update password not required bit	
Delete msRTCSIP-LocationContactMannings objects		 _

b. Create Contact objects

Pe	rmission Entry for lyncforb	
ermissions:		
Full control	Create msRTCSIP-MCUFactories objects	
List contents	Delete msRTCSIP-MCUFactories objects	
Read all properties	Create msRTCSIP-MCUFactory objects	
Write all properties	Delete msRTCSIP-MCUFactory objects	
Delete	Create msRTCSIP-MonitoringServer objects	
Delete subtree	Delete msRTCSIP-MonitoringServer objects	
Read permissions	Create msRTCSIP-Pool objects	
Modify permissions	Delete msRTCSIP-Pool objects	
Modify owner	Create msRTCSIP-Pools objects	
All validated writes	Delete msRTCSIP-Pools objects	
All extended rights	Create msRTCSIP-TrustedMCU objects	
Create all child objects	Delete msRTCSIP-TrustedMCU objects	
Delete all child objects	Create msRTCSIP-TrustedMCUs objects	
Create Computer objects	Delete msRTCSIP-TrustedMCUs objects	
Delete Computer objects	Create msRTCSIP-TrustedProxies objects	
Create Contact objects	Delete msRTCSIP-TrustedProxies objects	
Delete Contact objects	Create msRTCSIP-TrustedProxy objects	
Create friendlyCountry objects	Delete msRTCSIP-TrustedProxy objects	
Delete friendlyCountry objects	Create msRTCSIP-TrustedServer objects	
Create Group objects	Delete msRTCSIP-TrustedServer objects	
Delete Group objects	Create msRTCSIP-TrustedService objects	
Create groupOfUniqueNames objects	Delete msRTCSIP-TrustedService objects	
Delete groupOfUniqueNames objects	Create msRTCSIP-TrustedServices objects	

c. Write all properties

		Permissio	n Entry for lyncforb	
Principal:	adminUser (adminUser@lyncforb.local)	Select a principal		
Туре:	Allow	~		
Applies to:	This object and all descendant objects	~		
Permissions	· · · · · · · · · · · · · · · · · · ·			
			Create mski CSIP-MCUFactories objects	
	List contents Pead all proportion		Create msRTCSIP-MCUPactories objects	
	Write all properties			
	Delete		Create mcPTCSIP-Micoractory objects	
			Delate msRTCSIP MonitoringServer objects	
			Delete mski CSIP-MonitoringServer objects	
	Read permissions		Create mski CSIP-Pool objects	
			Create mskit CSIP-Pools objects	
	All validated writes		Delete msKTCSIP-Pools objects	
	All extended rights		Create msRTCSIP-TrustedMCU objects	
	Create all child objects		Delete msRTCSIP-TrustedMCU objects	
	Delete all child objects		Create msRTCSIP-TrustedMCUs objects	
	Create Computer objects		Delete msRTCSIP-TrustedMCUs objects	
	Delete Computer objects		Create msRTCSIP-TrustedProxies objects	
	Create Contact objects		Delete msRTCSIP-TrustedProxies objects	

Note: Apply the Reanimate tombstones rights to the object being secured and its descendant objects.

7. Click OK.

Note: Only objects deleted after the delegation of the above-mentioned permissions can be restored.

Computer Management

This section provides a detailed explanation on the permissions required to create, modify and delete computers in AD.

Operation: Create computers

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Read and Write permissions on all computer objects of the required OU.

Steps to grant the permissions to create a computer account.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- Select the Only objects in this folder option and select the Computer objects checkbox.
 Also select the Create selected objects in this folder option as indicated in the following image.

Active Directory Object Type Indicate the scope of the task you want to delegate.	
Delegate control of:	
O This folder, existing objects in this folder, and creation of i	new objects in this folder
Only the following objects in the folder:	
certificationAuthority objects	^
Computer objects	
Connection objects	
Connection objects	
Connection objects	

- Click on Next. Under the Show these permissions section, select General and Property-specific options.
- 7. Under the permissions section, select the Read and Write permissions and click on Next.
- 8. Click Finish.

Operation: Modify computers

- Permissions needed:
- Must be a member of the Account Operators Group
- Must have the Read, Write, Read All Properties permissions on all computer objects of the required OU.

Steps to grant the permissions to modify a computer account.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- 5. Select the **Only objects in this folder** option and select the **Computer objects** checkbox as depicted in the image below:

Indicate the scope of th	Type e task you want to deleg	ate.	(a)
Delegate control of			6
 This folder, existing a 	bjects in this folder, and	creation of new objects in this	s folder
Only the following ob	jects in the folder:		
certification Aut	hority objects		^
🗹 Computer objec	zts		
Connection obj	ects		
Contact objects	3		
document obje	cts		
	s objects		*
documentSerie	bjects in this folder		
Create selected	objects in this folder		

- Click on Next. Under the Show these permissions section, select General and Property-specific options.
- 7. Under the permissions section, select the **Read**, **Write** and **Read all properties** permissions and click on **Next**.
- 8. Click Finish.

Operation: Delete computers

- Permissions needed:
- Must be a member of the Account Operators Group
- Must have the Delete All Child objects permission on all computer objects of the required OU.

Steps to grant the permissions to delete a computer account.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control**. The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- 5. Select the **Only objects in this folder** option and select the **Computer objects** checkbox as depicted in the image below:

Indicate the scope of the ta	rpe ask you want to deleg	gate.	2
Delegate control of:			
O This folder, existing obje	ects in this folder, and	creation of new objects	in this folder
Only the following object	ts in the folder:		
certification Author	ity objects		^
Computer objects			
Contact objects	5		
document objects			
document Series o	bjects		~
Create selected obj	ects in this folder		
	ects in this folder		
	ects in this folder		

- Click on Next. Under the Show these permissions section, select General and Creation/Deletion of specific child objects options.
- 7. Under the permissions section, select the **Delete all child objects permission** and click on Next.
- 8. Click Finish.

Operation: Restore computers

Permissions needed:

- 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.

Steps to grant the permissions required to restore a deleted AD computer

Any object deleted from AD is stored in the deleted objects container and can be restored before the end of its tombstone lifetime period. To restore a deleted AD object, non-administrators must have sufficient permission to access this container. To grant the required permissions:

- 1. Log in to your **domain controller** and launch the ADAM tools Command Prompt.
- 2. Specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus, DC=com" /takeownership



Note:

- Every domain in a forest will have its own deleted objects container, so it's essential to specify the domain name of the deleted objects container for which you would like to modify permissions.
- Replace **admanagerplus** and **com** with your domain components.
- To grant permission to a security principal to access the deleted objects container, specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP



Note: Replace "LukeJohnson" with the security principal of your choice.

- 4. Next, connect to the default naming context, right-click on the domain root, and select Properties.
- 5. In the **Security** tab, click **Advanced.**
- 6. Add the user or group, and select the following rights:
 - a. Reanimate tombstones

A	Permission Entry for lyncforb		x
Delete mslmaging-PSPs objects	Create Shared Folder objects		^
Create MSMQ Queue Alias objects	Delete Shared Folder objects		
Delete MSMQ Queue Alias objects	Create User objects		
Create msPKI-Key-Recovery-Agent objects	Delete User objects		
Delete msPKI-Key-Recovery-Agent objects	Add GUID		
Create msRTCSIP-ApplicationContacts obje	cts 🗌 Add/remove replica in domain		
Delete msRTCSIP-ApplicationContacts obje	cts 🗌 Allow a DC to create a clone of itself		
Create msRTCSIP-ConferenceDirectories ob	jects Change PDC		
Delete msRTCSIP-ConferenceDirectories ob	jects Create inbound forest trust		
Create msRTCSIP-ConferenceDirectory obje	ects Enable per user reversibly encrypted password		
Delete msRTCSIP-ConferenceDirectory obje	cts Generate resultant set of policy (logging)		
Create msRTCSIP-Domain objects	Generate resultant set of policy (planning)		_
Delete msRTCSIP-Domain objects	Manage replication topology		=
Create msRTCSIP-EdgeProxy objects	Migrate SID history		
Delete msRTCSIP-EdgeProxy objects	Monitor active directory replication		
Create msRTCSIP-GlobalContainer objects	Read only replication secret synchronization		
Delete msRTCSIP-GlobalContainer objects	Reanimate tombstones		
Create msRTCSIP-GlobalTopologySetting of	bjects Replicating Directory Changes		
Delete msRTCSIP-GlobalTopologySetting of	bjects 🛛 Replicating Directory Changes All		
Create msRTCSIP-GlobalTopologySettings of	objects Replicating Directory Changes In Filtered Set		
Delete msRTCSIP-GlobalTopologySettings c	objects 🗌 Replication synchronization		
Create msRTCSIP-LocationContactMapping	g objects 🛛 🗌 Run Protect Admin Groups Task		
Delete msRTCSIP-LocationContactMapping	objects 🛛 🗌 Unexpire password		
Create msRTCSIP-LocationContactMapping	js objects 🛛 Update password not required bit		
Delete msRTCSIP-LocationContactManning	is objects		×
	ОК	Can	cel

b. Create Computer objects

	Pe	ermission Entry for lyncforb
Principal:	adminUser (adminUser@lyncforb.local) Select a prin	cipal
Type:	Allow	
Applies to:	This object and all descendant objects \vee	
Permissions		
rennissions		Create msRTCSIP-MCUFactories objects
	List contents	Delete msRTCSIP-MCUFactories objects
	Read all properties	Create msRTCSIP-MCUFactory objects
	Write all properties	Delete msRTCSIP-MCUFactory objects
	Delete	Create msRTCSIP-MonitoringServer objects
	Delete subtree	Delete msRTCSIP-MonitoringServer objects
	Read permissions	Create msRTCSIP-Pool objects
	Modify permissions	Delete msRTCSIP-Pool objects
	Modify owner	Create msRTCSIP-Pools objects
	All validated writes	Delete msRTCSIP-Pools objects
	All extended rights	Create msRTCSIP-TrustedMCU objects
	Create all child objects	Delete msRTCSIP-TrustedMCU objects
	Delete all child objects	Create msRTCSIP-TrustedMCUs objects
	Create Computer objects	Delete msRTCSIP-TrustedMCUs objects
	Delete Computer objects	Create msRTCSIP-TrustedProxies objects
	Create Contact objects	Delete msRTCSIP-TrustedProxies objects

c. Write all properties

		Permissio	n Entry for lyncforb	
Principal:	adminUser (adminUser@lyncforb.local)	Select a principal		
Туре:	Allow	~		
Applies to:	This object and all descendant objects	~		
Permissions	s:			
			Create msRTCSIP-MCUFactories objects	
	List contents			
	Wite all properties		Create mskitCSIP-MCUFactory objects	
	Write all properties		Delete msRTCSIP-McOractory objects	
			Delete mskrcSiP-MonitoringServer objects	
	Nead permissions		Delete mskit CSIP-Pool objects	
	Modify permissions		Delete mski CSIP-Pool objects	
	Modify owner		Create mskitCSIP-Pools objects	
	All validated writes			
	Create all child objects		Delete msRTCSIP-TrustedMCU objects	
	Delete all child objects		Create msRTCSIP-TrustedMCUs objects	
	Create Computer objects		Delete msRTCSIP-TrustedMCUs objects	
	Delete Computer objects		Create msRTCSIP-TrustedProxies objects	
	Create Contact objects		Delete msRTCSIP-TrustedProxies objects	

Note: Apply the Reanimate tombstones rights to the object being secured and its descendant objects.

7. Click OK.

Note: Only objects deleted after the delegation of the above-mentioned permissions can be restored.

Group Management

This section provides a detailed explanation on the permissions required to create, modify and delete groups in AD.

Operation: Create Groups

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Read and Write permissions on all the group objects of the required OU.

Steps to grant the permissions to create groups.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- Select the Only objects in this folder option and select the Group objects checkbox.
 Also select the Create selected objects in this folder option as depicted in the following image.

Indicate the scope of the task you want to delegate.	1
Delegate control of:	
O This folder, existing objects in this folder, and creation of new	v objects in this folder
Only the following objects in the folder:	
Group objects	^
groupOfUniqueNames objects	
InetOrgPerson objects	
IntelliMirror Group objects	
IntelliMirror Group objects	

- Click on Next. Under the Show these permissions section, select General and Property-specific options.
- 7. Under the permissions section, select the Read and Write permissions and click on Next.
- 8. Click Finish.

Operation: Modify Groups

Permissions needed:

- Must be a member of the Account Operators Group

- Must have the Read, Write, Read All Properties permissions on all the group objects of the required OU.

Steps to grant the permissions to modify groups.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option
- 5. Select the **Only objects in this folder** option and select the **Group objects** checkbox as indicated in the following image.

Indicate the scope of the task you want to delegate.	¢
Delegate control of:	
O This folder, existing objects in this folder, and creation of	new objects in this folder
Only the following objects in the folder:	
Group objects	^
groupOfUniqueNames objects	
groupPolicyContainer objects	
IntelliMirror Group objects	
	•
Create selected objects in this folder	
Delete endeste distincts in this folder.	

- Click on Next. Under the Show these permissions section, select General and Property-specific options.
- 7. Under the permissions section, select the **Read**, **Write** and **Read all** properties **permissions** and click on **Next**.
- 8. Click Finish.

Operation: Delete Groups

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Delete All Child Objects permission on all the group objects of the required OU.

Steps to grant the permissions to delete groups.

- 1. Logon to your Domain controller and launch the Active Directory Users and Computers.
- 2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
- 3. Click Next, add the required user account and click Next.
- 4. Select the Create a custom task to delegate option.
- Select the Only objects in this folder option and select the Group objects checkbox.
 Also select the Delete selected objects in this folder option as depicted in the image below:

Indicate the scope	of the task you want to delegate.	5
Delegate control of:		
O This folder, existi	ng objects in this folder, and creation of ne	ew objects in this folder
Only the followin	g objects in the folder:	
Group obje	ects iiqueNames objects	<u>^</u>
group Polic	yContainer objects	
ieee802De	vice objects son objects	
	Group objects	~
Create selec	ted objects in this folder	
Delete selec	ted objects in this folder	

- Click on Next. Under the Show these permissions section, select General and Creation/Deletion of specific child objects options.
- 7. Under the permissions section, select the Delete all child objects permission and click on Next.
- 8. Click Finish.

Operation: Restore groups

Permissions needed:

- 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.

Steps to grant the permissions required to restore a deleted AD group

Any object deleted from AD is stored in the deleted objects container and can be restored before the end of its tombstone lifetime period. To restore a deleted AD object, non-administrators must have sufficient permission to access this container. To grant the required permissions:

- 1. Log in to your **domain controller** and launch the ADAM tools Command Prompt.
- 2. Specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus, DC=com" /takeownership



Note:

- Every domain in a forest will have its own deleted objects container, so it's essential to specify the domain name of the deleted objects container for which you would like to modify permissions.
- Replace **admanagerplus** and **com** with your domain components.
- To grant permission to a security principal to access the deleted objects container, specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP



Note: Replace "LukeJohnson" with the security principal of your choice.

- 4. Next, connect to the default naming context, right-click on the domain root, and select Properties.
- 5. In the **Security** tab, click **Advanced.**
- 6. Add the user or group, and select the following rights:
 - a. Reanimate tombstones

4	Permission Entry for lyncforb	
Delete mslmaging-PSPs objects	Create Shared Folder objects	^
Create MSMQ Queue Alias objects	Delete Shared Folder objects	
Delete MSMQ Queue Alias objects	Create User objects	
Create msPKI-Key-Recovery-Agent objects	Delete User objects	
Delete msPKI-Key-Recovery-Agent objects	Add GUID	
Create msRTCSIP-ApplicationContacts objec	ts Add/remove replica in domain	
Delete msRTCSIP-ApplicationContacts object	ts Allow a DC to create a clone of itself	
Create msRTCSIP-ConferenceDirectories obje	ects Change PDC	
Delete msRTCSIP-ConferenceDirectories obje	ects Create inbound forest trust	
Create msRTCSIP-ConferenceDirectory object	ts Enable per user reversibly encrypted password	
Delete msRTCSIP-ConferenceDirectory object	ts Generate resultant set of policy (logging)	
Create msRTCSIP-Domain objects	Generate resultant set of policy (planning)	
Delete msRTCSIP-Domain objects	Manage replication topology	=
Create msRTCSIP-EdgeProxy objects	Migrate SID history	
Delete msRTCSIP-EdgeProxy objects	Monitor active directory replication	
Create msRTCSIP-GlobalContainer objects	Read only replication secret synchronization	
Delete msRTCSIP-GlobalContainer objects	Reanimate tombstones	
Create msRTCSIP-GlobalTopologySetting ob	jects Replicating Directory Changes	
Delete msRTCSIP-GlobalTopologySetting obj	jects Replicating Directory Changes All	
Create msRTCSIP-GlobalTopologySettings of	bjects Replicating Directory Changes In Filtered Set	
Delete msRTCSIP-GlobalTopologySettings of	bjects Replication synchronization	
Create msRTCSIP-LocationContactMapping	objects 🗌 Run Protect Admin Groups Task	
Delete msRTCSIP-LocationContactMapping	objects 🗌 Unexpire password	
Create msRTCSIP-LocationContactMappings	s objects 🛛 Update password not required bit	
Delete msRTCSIP-LocationContactMannings	s objects	Y
		OK Cancel

b. Create Group objects

Pe	ermission Entry for lyncforb	
Permissions:		
Full control	Create msRTCSIP-MCUFactories objects	
List contents	Delete msRTCSIP-MCUFactories objects	
Read all properties	Create msRTCSIP-MCUFactory objects	
Write all properties	Delete msRTCSIP-MCUFactory objects	
Delete	Create msRTCSIP-MonitoringServer objects	
Delete subtree	Delete msRTCSIP-MonitoringServer objects	
Read permissions	Create msRTCSIP-Pool objects	
Modify permissions	Delete msRTCSIP-Pool objects	
Modify owner	Create msRTCSIP-Pools objects	
All validated writes	Delete msRTCSIP-Pools objects	
All extended rights	Create msRTCSIP-TrustedMCU objects	
Create all child objects	Delete msRTCSIP-TrustedMCU objects	
Delete all child objects	Create msRTCSIP-TrustedMCUs objects	
Create Computer objects	Delete msRTCSIP-TrustedMCUs objects	
Delete Computer objects	Create msRTCSIP-TrustedProxies objects	
Create Contact objects	Delete msRTCSIP-TrustedProxies objects	
Delete Contact objects	Create msRTCSIP-TrustedProxy objects	
Create friendlyCountry objects	Delete msRTCSIP-TrustedProxy objects	
Delete friendlyCountry objects	Create msRTCSIP-TrustedServer objects	
Create Group objects	Delete msRTCSIP-TrustedServer objects	
Delete Group objects	Create msRTCSIP-TrustedService objects	
Create groupOfUniqueNames objects	Delete msRTCSIP-TrustedService objects	

c. Write all properties

		Permissio	n Entry for lyncforb	
Principal:	adminUser (adminUser@lyncforb.local)	Select a principal		
Туре:	Allow	~		
Applies to:	This object and all descendant objects	~		
Permissions	s: k			
	Full control		Create msRTCSIP-MCUFactories objects	
	List contents		Delete msRTCSIP-MCUFactories objects	
	Read all properties		Create msRTCSIP-MCUFactory objects	
	Write all properties		Delete msRTCSIP-MCUFactory objects	
	Delete		Create msRTCSIP-MonitoringServer objects	
	Delete subtree		Delete msRTCSIP-MonitoringServer objects	
	Read permissions		Create msRTCSIP-Pool objects	
	Modify permissions		Delete msRTCSIP-Pool objects	
	Modify owner		Create msRTCSIP-Pools objects	
	All validated writes		Delete msRTCSIP-Pools objects	
	All extended rights		Create msRTCSIP-TrustedMCU objects	
	Create all child objects		Delete msRTCSIP-TrustedMCU objects	
	Delete all child objects		Create msRTCSIP-TrustedMCUs objects	
	Create Computer objects		Delete msRTCSIP-TrustedMCUs objects	
	Delete Computer objects		Create msRTCSIP-TrustedProxies objects	
	Create Contact objects		Delete msRTCSIP-TrustedProxies objects	

Note: Apply the Reanimate tombstones rights to the object being secured and its descendant objects.

7. Click OK.

Note: Only objects deleted after the delegation of the above-mentioned permissions can be restored.

GPO Management and Reporting

Operation	Permissions needed
Create GPOs	- Must be a member of the Group Policy Creator Owners group
Enable/disable GPOs	- Must have Edit setting permission selected on the GPOs.
	Note: To learn how to delegate Edit setting permissions to a
	group or user on a GPO, refer to this document.
Enable/disable user configuration settings	- Must have Edit setting permission selected on the GPOs.
	Note: To learn how to delegate permissions to a group or user on a GPO, refer to this document.
Enable/disable computer configuration settings	- Must have Edit setting permission selected on the GPOs.
	Note: To learn how to delegate permissions to a group or user on 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 group
	policy objects, refer to this document.
Edit GPO settings	- Must have Edit setting permission selected on the GPOs.
	Note: To learn how to delegate permissions to a group or
	user on 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 group
	policy objects, refer to this document.
Reporting	- Must have the Read permission on the Site/ Domain/OU objects (on gPlink attribute).
	- Must have the Read permission on the Site/ Domain/OU objects (on gPOptions attribute).
	- Must have the 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
	nanagementreporting operations.

AD Reporting

Operations	Permissions needed
Generate all AD reports	- Must have the <i>View</i> permission in the desired OUs/domains.
Generate all NTFS reports	- Must have the <i>Read</i> permission on the relevant folders

Note: Besides the permissions listed above, the *Replication Directory Changes* permission has to be granted for effective data synchronization between AD and ADManager Plus if the service account does not have domain administrative privileges.

Operation: Generate BitLocker reports

Permissions needed:

- Must have the View permission in the desired OUs and domains

Steps to grant permissions to view BitLocker recovery keys

- 1. Log in to your domain controller and launch Active Directory Users and Computers.
- 2. Locate and right-click the **domain** or **OU** for which you wish to grant the required permissions and select **Delegate Control**. The Delegation of Control wizard will pop-up.
- 3. Click Next.
- 4. Select the desired user account or group, and click Next.
- 5. Select Create a custom task to delegate and click Next.

Delegation of Control Wizard	×
Tasks to Delegate You can select common tasks or customize your own.	R
O Delegate the following common tasks:	
 Create, delete, and manage user accounts Reset user passwords and force password change at next logon Read all user information Create, delete and manage groups Modify the membership of a group Manage Group Policy links Generate Resultant Set of Policy (Planning) 	
Create a custom task to delegate	
< Back Next > Cancel	Help

6. Select the Only the following objects in the folder option, check msTPM-InformationObject objects and msFVE-RecoveryInformation objects, and then click Next.

Delegation of Control Wizard	×
Active Directory Object Type Indicate the scope of the task you want to delegate.	R
Delegate control of:	
O This folder, existing objects in this folder, and creation of new objects in this folder	er
Only the following objects in the folder:	
msDS-ValueType objects msFVE-RecoveryInformation objects msieee80211-Policy objects msImaging-PostScanProcess objects msImaging-PSPs objects msKds-ProvRootKey objects	^ •
Create selected objects in this folder Delete selected objects in this folder	
< Back Next > Cancel	Help

- 7. Under the Show these permissions section, select General and Property-specific.
- 8. Under the *Permissions* section, select the **Read**, **Write**, and **Read All Properties** permissions, and then click **Next**.

Permissions Select the permissions yo	ou want to deleg	ate.		P
Show these permissions:				
General				
Property-specific				
Creation/deletion of s	pecific child obje	ects		
Permissions:				
Full Control				
Read				
Write				
Read All Properties				
Write All Properties				
		Marida	0 1	

9. Click Finish.



File Permission Management

Operations	Permissions needed
Modify/Remove NTFS permissions	- Must have the 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

Exchange Management

Operations	Exchange versions	Permissions needed
Creating Exchange mailboxes while creating a corresponding user account in AD	Exchange 2007	- Must have 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 Active Directory 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	All versions	- Must have the Exchange View Only Administrator role.

Note: Only enterprise admins can perform cross-forest Exchange management.

Microsoft 365 Management and Reporting

The roles and permissions (minimum scope) required for a service account configured in ADManager Plus are listed below.

Module	Role name	Scope
Management	User administrator	Manage users, contacts, and groups.
	Privileged authentication administrator	Reset passwords and block or unblock administrators.
	Privileged role admin	Manage role assignments in Azure Active Directory.
	Exchange administrator	Update mailbox properties.
	Teams service admin	Manage Microsoft Teams.
Reporting	Global reader	Get reports on all Microsoft 365 services.
	Security reader	Get read-only access to security features, sign-in reports, and audit logs.

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

Module	API name	Permission	Scope
Management	Microsoft Graph	User.ReadWrite.All	User creation, modification, deletion, and restoration
		Group.ReadWrite.All	Group creation, modification, deletion, and restoration; adding or removing members and owners
Reporting	Microsoft Graph	User.Read.All	Reports on users and group members
		Group.Read.All	Group reports
		Contacts.Read	Contact reports
		Reports.Read.All	Usage reports
		Organization.Read.All	License detail reports
		AuditLog.Read.All	Audit log reports
	Azure Active Directory Graph	Domain.Read.All	Domain-based reports

To know about the prerequisites for configuring a Microsoft 365 account in ADManager Plus, click here.

Active Directory migration

Operations	Permissions needed
User migration	Enterprise admin

Google Workspace Management and Reporting

Operations	Permissions needed
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 https://www.googleapis.com/auth/admin.directory.domain. readonly
Reporting	API scopes: https://www.googleapis.com/auth/admin.directory.user

To know about the pre-requisites for configuring a G Suite (Google Apps) account in ADManager Plus, click here.

High Availability Prerequisites

High availability refers to a system or component which aims to ensure an agreed level of operational performance for a higher than normal period. ADManager Plus helps administrators maintain high availability for a server in case of failure of the primary server.

ADManager Plus achieves this by employing a high availability architecture which designates a backup server to act as a shield to the primary server.

- The same database is used for both the servers and at any given time, a single server will cater to user requests and the other will be inactive.
- Whenever the primary server runs encounters unplanned downtime, the standby server becomes operational and takes control of components.

Prerequisites:

- Both the primary and the secondary server must be in the same subnet.
- The user account configured in both the services must be a member of the Domain Admins group while configuring high availability in ADManager Plus.

Note:

Later on, you can remove this user account from the Domain Admins group. However, ensure that this user account has the NTFS and share permissions on both the primary and the secondary servers along with C\$(admin share).

If you need any further assistance or information, please write to support@admanagerplus.com or call us at +1 844 245 1108.

Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus | M365 Manager Plus | RecoveryManager Plus

ManageEngine) ADManager Plus

ADManager Plus is an identity governance and administration (IGA) solution that simplifies identity management, ensures security, and improves compliance. With ADManager Plus, manage the user life cycle from provisioning to deprovisioning, run access certification campaigns, orchestrate identity management across enterprise applications, and protect data on your enterprise platforms with regular backups. Use over 200 reports to gain valuable insights into identities and their access rights. Improve the efficiency of your IGA operations with workflows, automations, and role-based access control policies. ADManager Plus' Android and iOS applications help with on-the-go AD and Azure AD management.

For more information about ADManager Plus, visit manageengine.com/products/ad-manager/.

± Download