ManageEngine ADSelfService Plus

Required privileges and permissions



ManageEngine) ADSelfService Plus

www.adselfserviceplus.com

Table of contents

Document summary	1
ADSelfService Plus overview	1
Required permissions	2
Configuring permissions	3
To delegate full control in ADUC to access all ADSelfService Plus features	_ 3
To delegate the right to reset user passwords in ADUC	. 8
To delegate the right to unlock user accounts in ADUC	. 12
To delegate the right to modify user attributes in ADUC	. 13
To delegate the right to read user PSO in ADUC	. 14
To delegate the right to modify members of a group in ADUC	. 15
To synchronize AD user objects with ADSelfService Plus	. 17
To delegate the right to create a computer account in ADUC	. 18
To delegate the right to modify user logon script path in ADUC	. 19
To view deleted users report	21
To install Windows login agent	21
To perform other actions	. 22

Document summary

This guide will walk you through the process of delegating an Active Directory user account with the required permissions for using the self-service features in ADSelfService Plus. ADSelfService Plus does not require "Domain Admin" membership in order to allow users to reset their passwords, unlock their accounts, update their profiles, or access any of its other features. Based on the principle of least privilege, you can delegate only the permissions required for the self-service operations to a user account manually.

Note: If you don't provide any authentication details while adding domains, ADSelfService Plus will get its privileges one of two ways:

- If ADSelfService Plus is installed to run as a console application and no credentials are provided, then by default it uses the permissions of the user who installed the product.
- If ADSelfService Plus is installed to run as a service and no credentials are provided, then by default it uses the permissions of the account used to run the service.

ADSelfService Plus overview

ManageEngine ADSelfService Plus, an integrated Active Directory self-service password management and single sign-on solution, helps reduce password reset tickets and spares end users the frustration caused by computer downtime. It offers,

- Self-service password reset and account unlock
- Password and account expiration notifier
- Password policy enforcer
- Enterprise single sign-on and password synchronizer
- Endpoint multi-factor authentication for machine logins
- Directory self-update and employee search

These features, designed to strike a balance between ensuring network security and ease-of-access, warrants improved ROI, and a productive IT workforce.

Required permissions

Feature	Permission(s) required
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
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
Configuration of high availability	Membership in Domain Admins group

Configuring permissions

To access all ADSelfService Plus features

For users to access all features of ADSelfService Plus, you'll need to grant the ADSelfService Plus service account the following permissions:

- 1. Right-click the **domain** in ADUC and select **Delegate Control** from the context menu.
- 2. Click **Next** in the welcome dialog box.
- 3. Click Add to select the user account or service account, then click OK followed by Next.
- 4. Select **Delegate the following common tasks** and check the **Reset user passwords and** force password change at next logon, Read all user information, and Modify the membership of a group boxes, then click Next.

Delegation of Control Wizard	×
Tasks to Delegate You can select common tasks or customize your own.	R
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 Modify the membership of a group Join a computer to the domain Manage Group Policy links Generate Resultant Set of Policy (Planning) Create a custom task to delegate 	
< Back Next > Cancel	Help

- 5. Click Finish and repeat steps 1-3.
- 6. Select Create a custom task to delegate and click Next.
- 7. Select **Only the following objects in the folder.** In the given list, select **User Objects.**

Delegation of Control Wizard
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:
 Site Settings objects Sites Container objects Subnet objects Subnets Container objects Trusted Domain objects User objects
 Create selected objects in this folder Delete selected objects in this folder
< Back Next > Cancel Help

8. Select the **General** box. Under Permissions, check the boxes for **Read** and **Write** before clicking **Next**.

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	P
Show these permissions: General Property-specific Creation/deletion of specific child objects	
Permissions: Full Control Read Vite Create All Child Objects Delete All Child Objects Read All Properties	
< <u>B</u> ack <u>N</u> ext > Cancel	Help

- 9. Click Finish and repeat steps 1-3.
- 10. Select Create a custom task to delegate and click Next.
- 11. Select **Only the following objects in the folder**. In the given list, select **Computer Objects** and **Create selected objects in this folder**.

egation of Control Wizard	×
Active Directory Object Type Indicate the scope of the task you want to delegate.	P
Delegate control of:	
O This folder, existing objects in this folder, and creation of new objects in this fold	ler
Only the following objects in the folder:	
 Computer objects Connection objects Contact objects document objects documentSeries objects domainRelatedObject objects Create selected objects in this folder Delete selected objects in this folder 	×
< Back Next > Cancel	Help

12. Select the General box. Under Permissions, check Read before clicking Next.

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	P
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 	•
< Back Next > Cancel	Help

- 13. Click Finish and repeat steps 1-3.
- 14. Select Create a custom task to delegate and click Next.
- 15. Select Only the following objects in the folder. In the given list, select msDS-PasswordSettings objects and msDS-PasswordSettingsContainer objects. Click Next.

Delegation of Control Wizard 🛛 🔀
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:
 msDS-ManagedServiceAccount objects msDS-OptionalFeature objects msDS-PasswordSettings objects msDS-PasswordSettingsContainer objects msDS-QuotaContrainer objects msDS-QuotaControl objects Create selected objects in this folder Delete selected objects in this folder
<pre>< Back Next > Cancel Help</pre>

16. Select the General box. Under Permissions, check Read before clicking Next.

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	R
Show these permissions:	
🔽 General	
Property-specific	
Creation/deletion of specific child objects	
Permissions:	
Full Control	_
Write Crasta All Child Objects	
	<u> </u>
< Back Next > Cancel	Help

17. Click Finish.

Self-service password reset

In order for this feature to work, you need to delegate the *permission to reset users' passwords* in the ADUC console. To do this, follow the steps below:

- 1. Right-click the OU or domain in ADUC and select Delegate Control from
- 2. Click **Next** in the welcome dialog box.

Delegation of Control Wizard	×
	Welcome to the Delegation of Control Wizard
	This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.
	To continue, click Next.
	< Back Next > Cancel Help

- 3. Click Add to select the ADSelfService Plus user account or service account, then click OK.
- 4. Click Next.

Delegation of Control Wizard 🛛 🔀
Users or Groups Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
SspServiceAccount (sspServiceAccount@praveen.com)
Add Remove
<pre></pre>

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.	P
C 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 Modify the membership of a group Join a computer to the domain Manage Group Policy links Generate Resultant Set of Policy (Planning) Create a custom task to delegate 	
< Back Next > Cancel	Help

6. Select **Only the following objects in the folder**. In the given list, select **User objects and click Next**

Delegation of Control Wizard	×
Active Directory Object Type Indicate the scope of the task you want to delegate.	P
Delegate control of:	
C This folder, existing objects in this folder, and creation of new objects in this folder.	der
Only the following objects in the folder:	
 Site Settings objects Sites Container objects Subnet objects Subnets Container objects Trusted Domain objects User objects 	
 Create selected objects in this folder Delete selected objects in this folder 	
< Back Next > Cancel	Help

- 7. Check the General and Property-specific boxes.
- 8. Under Permissions, check the boxes for **Reset password, Read pwdLastset**, and **Write pwdLastset** before clicking **Next**.

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	P
Show these permissions: General Property-specific Creation/deletion of specific child objects	
Permissions: Reset password Send as Receive as Read and write general information Read and write account restrictions Read and write logon information	
< Back Next > Cancel	Help

Delegation of Control Wizard				×
Permissions Select the permissions you	u want to delegate	э.		P
Show these permissions:				
🔽 General				
Property-specific				
🔲 Creation/deletion of sp	ecific child object	ts		
Permissions:				
Read profilePath				-
Write profilePath				
Read pwdLastSet				
				<u> </u>
	< Back	Next >	Cancel	Help

9. Click Finish.

Note: This permission only enables password reset.

Self-service account unlock

For this feature to work, you need to delegate the *permission to unlock users' accounts* in the ADUC console. To do this:

- 1. Right-click the OU or domain in ADUC and select Delegate Control from the context menu.
- 2. Click Next in the welcome dialog box.
- 3. Click **Add** to select the ADSelfService Plus user account or service account, then click **OK**.
- 4. Click Next.
- 5. Select Create a custom task to delegate and click Next.
- 6. Select **Only the following objects in the folder**. In the given list, check **User objects** and click **Next**.

7	Check the General	and Property	-snecific hoxes
/	Check the General	and FIODERV	-SDecinc DOXE

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	P
Show these permissions: General Property-specific Creation/deletion of specific child objects	
Permissions: ✓ Read lockoutTime ✓ Write lockoutTime Read loginShell ✓ Write loginShell Read Logon Name ✓ Write Logon Name	
< Back Next > Cancel	Help

- 8. Under Permissions, check the **Read lockoutTime** and **Write lockoutTime** boxes and click **Next**.
- 9. Click Finish.

Note: This permission only enables account unlock.

Directory self-update

To utilize this feature, you need to delegate the *permission to modify user attributes* in the ADUC console. Follow the steps below to do so:

- 1. Right-click the OU or domain in ADUC and select Delegate Control from the context menu.
- 2. Click **Next** in the welcome dialog box.
- 3. Click Add to select the user account or service account, then click OK.
- 4. Click Next.
- 5. Select Create a custom task to delegate and click Next.
- 6. Select **Only the following objects in the folder**. In the given list, select **User objects** and click **Next**.
- 7. Check the General and Property-specific boxes.

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	P
Show these permissions:	
🔽 General	
Property-specific	
Creation/deletion of specific child objects	
Permissions:	
	▲
Read All Properties	T
< Back Next > Cancel	Help

- 8. Under Permissions, check the **Read** and **Write** boxes (or select the **Read** and **Write** boxes of specific attributes that need to be available for end user self-update), and click Next.
- 9. Click Finish.

Note: This permission only enables self-update.

Display fine-grained password policy

If you want to display the exact password policy requirements in the reset/ change password screen for users with fine-grained password policy enabled, then you need to delegate the *permission to read the users' Password Settings Objects (PSOs)* in ADUC. Follow the steps below to do this:

- 1. Right-click the OU or domain in ADUC and select Delegate Control from the context menu.Click **Next** in the welcome dialog box.
- 2. Click Add to select the user account or service account, then click OK.
- 3. Click Next.
- 4. Select Create a custom task to delegate and click Next.
- Select Only the following objects in the folder. In the given list, select msDS-PasswordSettings objects and msDS-PasswordSettingsContainer objects before clicking Next.

Delegation of Control Wizard	×
Active Directory Object Type Indicate the scope of the task you want to delegate.	P
Delegate control of:	4
 I his rolder, existing objects in this rolder, and creation of new objects in this rol Only the following objects in the folder: 	der
 msDS-OptionalFeature objects msDS-PasswordSettings objects msDS-PasswordSettingsContainer objects msDS-QuotaContainer objects msDS-QuotaControl objects msFVE-RecoveryInformation objects 	
 Create selected objects in this folder Delete selected objects in this folder 	
< Back Next > Cancel	Help

7. Check the General box.

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	P
Show these permissions:	
✓ General	
Property-specific	
Creation/deletion of specific child objects	
Permissions:	
Full Control	_
	-
< <u>B</u> ack <u>N</u> ext > Cancel	Help

- 8. Under Permissions, select Read and click Next.
- 9. Click Finish.

Note: This permission only fetches the password policy.

Self-service mail group subscription

To use this feature, you need to delegate the *permission to modify members of a group* in the ADUC console. Follow the steps below to do so:

- 1. Right-click the OU or domain where the group containing members that require modification belongs in ADUC, and select Delegate Control from the context menu.
- 2. Click **Next** in the welcome dialog box.
- 3. Click Add to select the user account or service account, then click OK. Click Next.
- 4. Select Create a custom task to delegate and click Next.
- 5. Select **Only the following objects in the folder**. In the given list, select **Group objects** and click **Next**.

elegation of Control Wizard	×
Active Directory Object Type Indicate the scope of the task you want to delegate.	R
Delegate control of:	
$\odot~{ m I}$ his folder, existing objects in this folder, and creation of new objects in this folde	r
Only the following objects in the folder:	
 ☐ friendlyCountry objects ☑ Group objects ☑ groupOfUniqueNames objects ☑ groupPolicyContainer objects ☑ ieee802Device objects ☑ InetOrgPerson objects 	
Create selected objects in this folder Delete selected objects in this folder	
< <u>B</u> ack <u>N</u> ext > Cancel	Help

- 6. Check the boxes for **General** and **Property-specific**.
- 7. Under Permissions, check the **Read Members** and **Write Members** boxes and click **Next**.

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	P
Show these permissions: <u>G</u> eneral <u>P</u> roperty-specific <u>C</u> reation/deletion of specific child objects	
Permissions:	
< <u>B</u> ack <u>N</u> ext > Cancel	Help

8. Click Finish.

Note: This permission only enables mail group subscription.

Synchronizing AD user objects with ADSelfService Plus

To synchronize Active Directory objects with ADSelfService Plus without any issue, you need to provide the Replicate Directory Changes permission to the user or service account used in ADSelfService Plus. To do this, follow the steps below:

- 1. In the ADUC console, right-click the domain or OU and select Properties.
- 2. Under the Security tab, click Add to select the user or service account.
- 3. In the **Permissions** section, **Allow** the **Replicate Directory Changes** permission.

Group or user names: Administrators (SARAVANAN\Administrator) Pre-Windows 2000 Compatible Access (SA Incoming Forest Trust Builders (SARAVANA ENTERPRISE DOMAIN CONTROLLERS SspServiceAccount (sspServiceAccount)	s) RAVANAN AN\Incomir saravana.c	\Pre-Win g Forest om) ≡ ∨
A	dd	Remove
Permissions for sspServiceAccount	Allow	Deny
Read only replication secret synchronization Reanimate tombstones Replicating Directory Changes Replicating Directory Changes All Replicating Directory Changes In Filtered Set		
For special permissions or advanced settings, cli Advanced.	ck	Advanced

4. Click OK.

Single sign-on to ADSelfService Plus via NTLMv2

For this feature to work, you need to delegate the *permission to create and read computer accounts* in the ADUC console. To do this, follow the steps below:

- 1. Right-click the Computers OU or domain in ADUC and select Delegate Control from the context menu.
- 2. Click Next in the welcome dialog box.
- 3. Click Add to select the ADSelfService Plus user account or service account, then click OK.
- 4. Click Next.
- 5. Select Create a custom task to delegate and click Next.
- 6. Select **Only the following objects in the folder**. In the given list, select **Computer objects** and **Create selected objects in this folder** and click **Next**.

Delegation of Control Wizard
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:
 bootableDevice objects certificationAuthority objects Computer objects Connection objects Contact objects document objects
Create selected objects in this folder Delete selected objects in this folder
< Back Next > Cancel Help

- 7. Check the General box.
- 8. Under Permissions, check the **Read** box and click **Next**.

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	P
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	
	•
< Back Next > Cancel	Help

9. Click Finish.

Note: This permission only enables you to configure NT LAN Manager (NTLMv2) SSO to ADSelfService Plus.

Force enrollment using a logon script

To use this feature, you need to delegate the *permission to modify the user scriptPath* in the ADUC console. Follow the steps below to do this:

- 1. Right-click the OU or domain in ADUC and select Delegate Control from the context menu.
- 2. Click **Next** in the welcome dialog box.
- 3. Click Add to select the user account or service account, then click OK.
- 4. Click Next.
- 5. Select Create a custom task to delegate and click Next.
- 6. Select **Only the following objects in the folder**. In the following list, check **User objects** and click **Next**.

Delegation of Control Wizard 🛛 🗙
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:
 Site Settings objects Sites Container objects Subnet objects Subnets Container objects Trusted Domain objects User objects
 Create selected objects in this folder Delete selected objects in this folder
< Back Next > Cancel Help

- 7. Check both the General and Property-specific boxes.
- 8. Under Permissions, check the **Read scriptPath** and **Write scriptPath** boxes and click **Next**.

Delegation of Control Wizard	×
Permissions Select the permissions you want to delegate.	R
Show these permissions:	
🔽 General	
Property-specific	
Creation/deletion of specific child objects	
Permissions:	
Read roomNumber	▲
Write roomNumber	
Read scriptPath	
Write scriptPath	
Read secretary	
Write secretary	•
< Back Next > Cancel	Help

9. Click Finish.

Note: This permission only enables logon script path modification.

To view a deleted users report

The minimum requirement to view this report is membership in the **Domain Admins** group.

To perform GINA installation

The minimum requirement to perform GINA installation from ADSelfService Plus' web console is membership in the **Domain Admins** group.

If Domain Admin credentials are not available for use, you can install GINA manually via Group Policy Objects (GPOs) or using System Center Configuration Manager (SCCM).

Folder permissions for other actions

The service account used to run ADSelfService Plus and the local user account used to start ADSelfService Plus must be granted **full control** permission to the product installation folder. Otherwise, you won't be able to:

- Install service packs
- Generate reports
- Start up the product
- Apply licenses
- Update dashboard graphs
- Back up and restore data
- Display employee photos and offer users self-update options

Dbject name: C:\ManageE	ngine\ADSelfService	Plus
Group or user names:		
SCREATOR OWNER		
SYSTEM		
Administrators (PRAVEE	NVAdministrators)	
👗 sspServiceAccount (ssp	ServiceAccount@prav	een.com)
Sers (PRAVEEN/Users	:)	
	Add	Remove
Dermissions for		
sspServiceAccount	Allow	Deny
sspServiceAccount	Allow	Deny
Fernissions for sspServiceAccount Full control Modify		Deny
Full control Modify Read & execute		Deny
Full control Full control Modify Read & execute List folder contents		
Full control Full control Modify Read & execute List folder contents Read	Allow V V V V V	

To configure high availability

The minimum requirement to configure high availability in ADSelfService Plus is membership in the Domain Admins group. Domain Admin privileges are only mandatory during the initial setup of high availability. Once high availability has been configured, the service account can be changed to one with lesser privileges based on other features configured. Ensure that folder sharing between both the instances is uninterrupted.

Our Products

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

ManageEngine ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces. For more information about ADSelfService Plus, visit https://www.manageengine.com/products/self-service-password.

\$ Get Quote

🛨 Download