Security and Rights Delegations for the Password Reset PRO Master Service

Applies to software versions 2.x.x and 3.x.x

Password Reset PRO Master Service

Delegated rights required for running the Password Reset PRO Master Service with a standard (non admin) domain user account:

A Windows Service is installed with our software called the "Password Reset PRO Master Service". This service runs as a "Network Service", reads and writes to Active Directory/LDAP and performs automated functions such as self service enrollment, password reset / changes, account unlocks, and other activities securely on behalf of the web portal user. This service also sends event alerts and a daily report email once every 24 hours. By default, the service is installed in a stopped state with "Local System" credentials to ensure the software is benign until you are ready to use it. Local System credentials are not sufficient to operate the service.

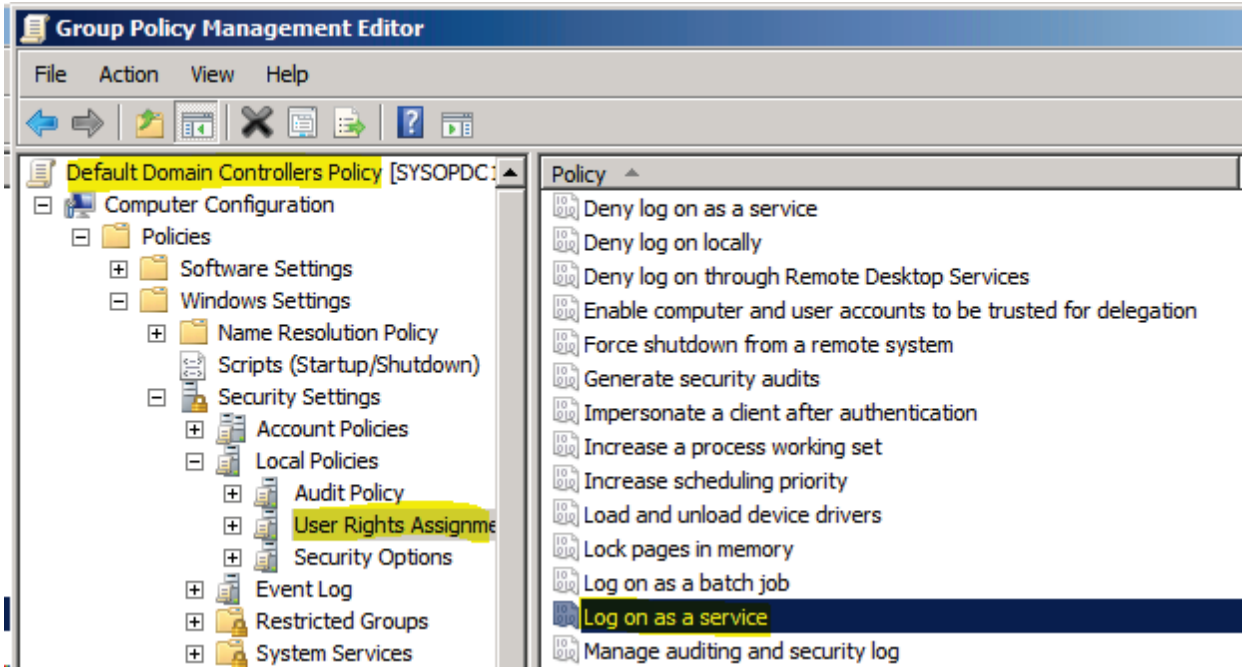
*** You MUST configure the service with appropriate domain\user credentials and domain policy to run this service as a Network Service in the domain, and the service must also have local admin rights on the server.*

1) **Ensure the standard (non admin) domain\user account used to run the Password Reset PRO Master Service is a member of the local\Administrators group of the Master Service server.**

2) **Configure delegated domain rights to run the service user account:**
   a. In a default unmodified 2003 domain, the domain\administrator and the Domain Admins AD group contain the necessary rights to allow user accounts to run Network Services on domain member servers. You must add your non-domain-admin delegated user account to the "Log on as a Service" policy setting available under the Domain Controllers OU default policy.

   b. If your domain is native 2008 or 2008R2, you must explicitly add the user account to the 'Log on as a Service' policy setting since this right is no longer inherited by the Domain Admins AD group or the domain\administrator account.

   Add user account to the "Log on as a Service" policy setting. This is required to run a Network Service.



c. **NOTE:** If you have specific Group Policies (GPO) in your environment that control your servers, and your Master Service server falls under the scope of management of a specific GPO, you may need to add the selected user account to the "Log on as a Service" policy setting in the appropriate GPO. This right is required to run a Network Service on any domain member server.

3) Delegating AD rights to the service account user: (Go down a couple of pages for step-by-step screenshots)

Lastly, you must delegate rights to the domain\user service account for your user objects contained in the domain (or your target OUs). For the example below we have created a user account in AD called "PasswordResetPROServiceAccount". Run the Active Directory "Delegate Control" wizard and select the following permission set to assign appropriate permissions:

a. Password Reset PRO:

You chose to delegate control of objects
in the following:

domain.com

The groups, users, or computers to which you
have given control are:

PasswordResetProServiceAccount (PasswordResetProServiceAccount@domain.com)

They have the following permissions:

Read All Properties
Change Password
Reset Password
Write altSecurityIdentities
Write lockoutTime
Write userAccountControl

For the following object types:
User

4) Running DSACLS commands on the delegated Password Reset PRO service account user:

Next (highly recommended), you must ensure that the same delegated permissions are applicable to user accounts who are members of protected Active Directory security groups (Domain Admins, Server Operators, Backup Operators, etc). If you do not want members of these protected AD groups to be able to use the self service portal, skip this step. Otherwise, you must run the following commands to assign the appropriate permissions to the AdminSDHolder object:

Note that you MUST replace the items in **RED with your correct internal AD domain name! For example, "DC=**mydomain**,DC=**local**" and "**mydomain.local\MyServiceAccount**" – You MUST use proper capitalizations for the service account name.

If you run these commands from a 2008 server command prompt, you must run the command prompt "as Administrator".

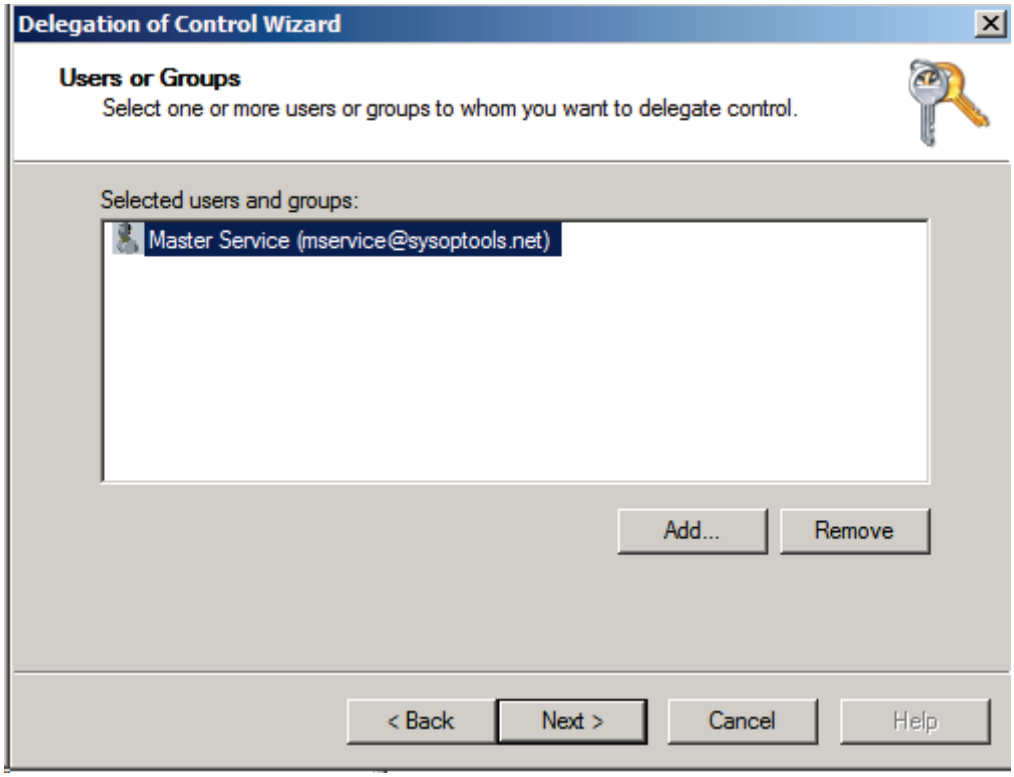
```
dsacls CN=AdminSDHolder,CN=System,DC=domain,DC=com /G DOMAIN\PasswordResetProServiceAccount:RP
dsacls CN=AdminSDHolder,CN=System,DC=domain,DC=com /G DOMAIN\PasswordResetProServiceAccount:CA;"Change Password"
dsacls CN=AdminSDHolder,CN=System,DC=domain,DC=com /G DOMAIN\PasswordResetProServiceAccount:CA;"Reset Password"
dsacls CN=AdminSDHolder,CN=System,DC=domain,DC=com /G DOMAIN\PasswordResetProServiceAccount:WP;altSecurityIdentities
dsacls CN=AdminSDHolder,CN=System,DC=domain,DC=com /G DOMAIN\PasswordResetProServiceAccount:WP;lockoutTime
dsacls CN=AdminSDHolder,CN=System,DC=domain,DC=com /G DOMAIN\PasswordResetProServiceAccount:WP;userAccountControl
```

**Note that the “Read All Properties” permission assignment above is actually redundant as, by default, the “Authenticated Users” built-in group has been granted this same permission. The explicit permission assignment above is provided for clarity and as a fail-safe in the event this default permission assignment is removed or modified.

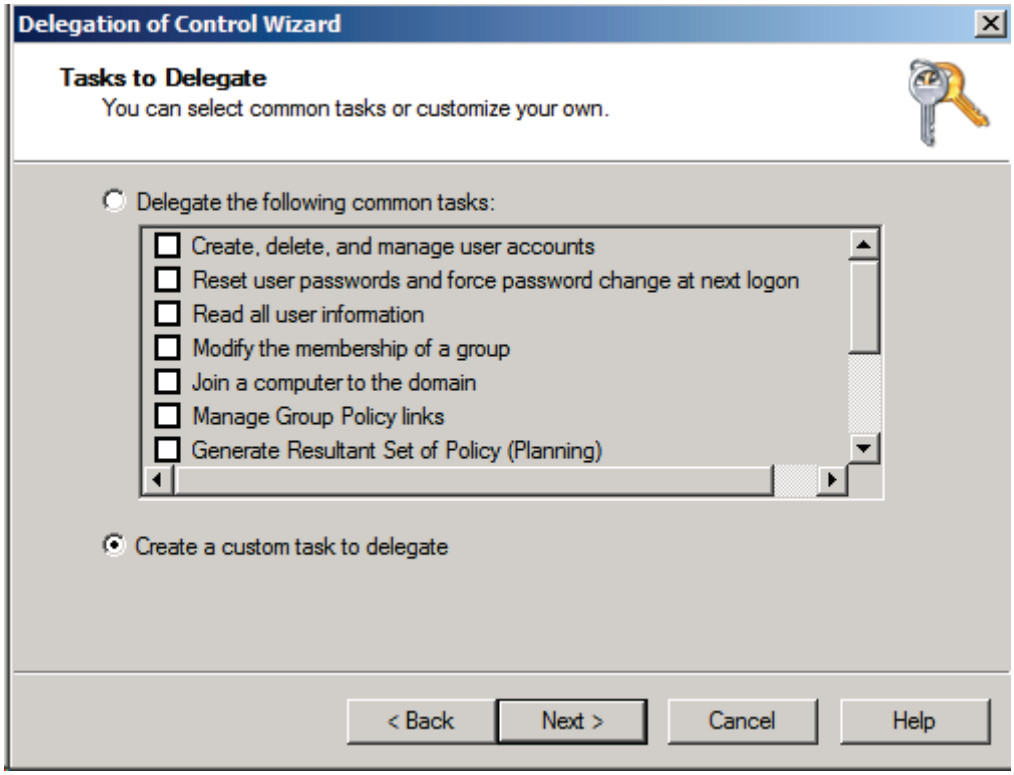
5) **Apply the delegated service user to the Password Reset PRO Master Service.**
   Open Windows Services on the Master Server and configure the Password Reset PRO Master Service > Log On property with the chosen delegated domain\user account. The Service Control Manager will grant the “logon as a service” user right to the selected user account, and will take effect when the service is started or restarted.

6) **You should now be all set to allow users to enroll and use the Self Service Web Portal.**

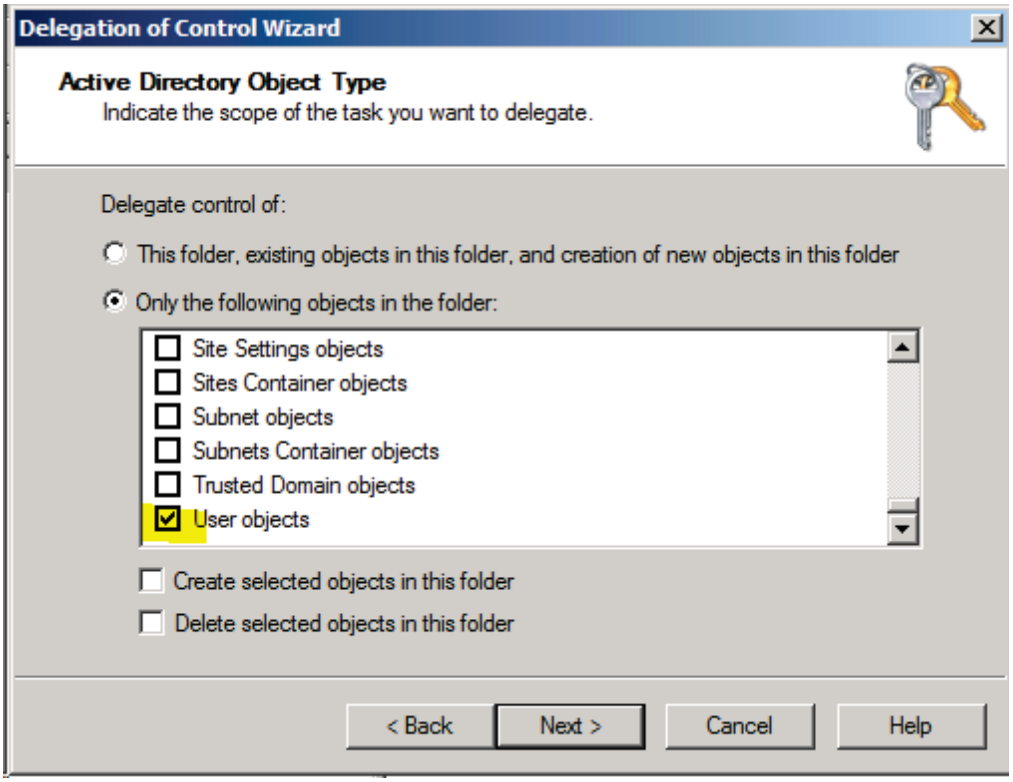
Screenshots of the Delegation Wizard steps are as follows.
Note that you must choose specific options on the Wizard screens in order to find the correct properties to delegate, so please follow the screenshots closely:

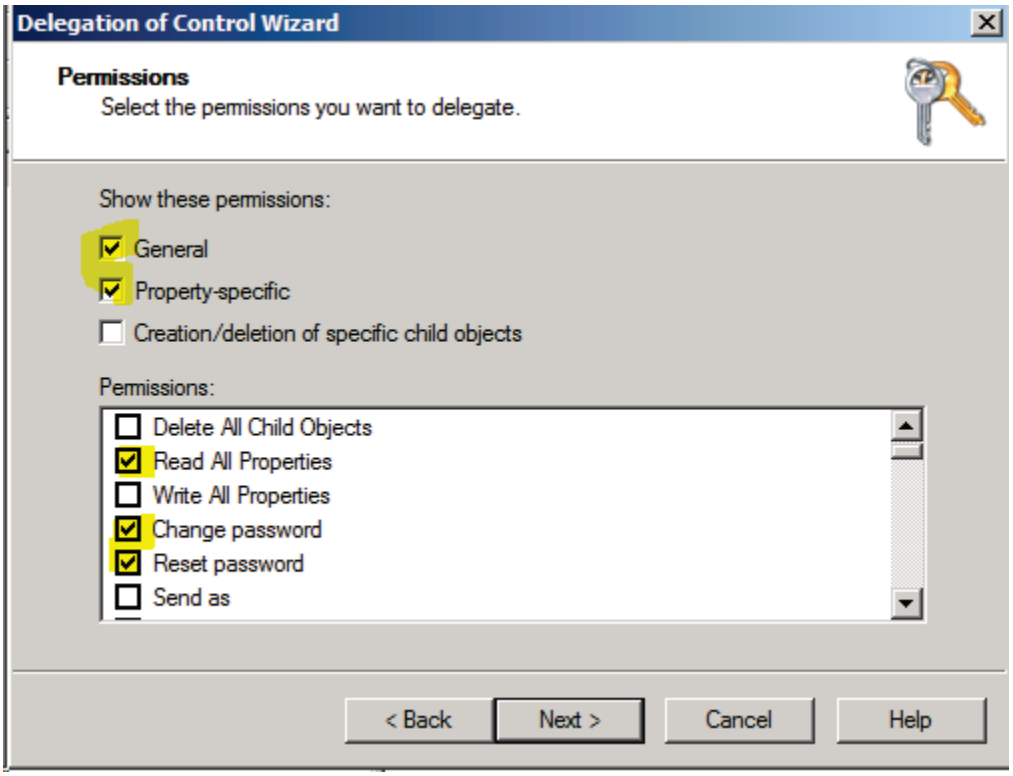
1. 

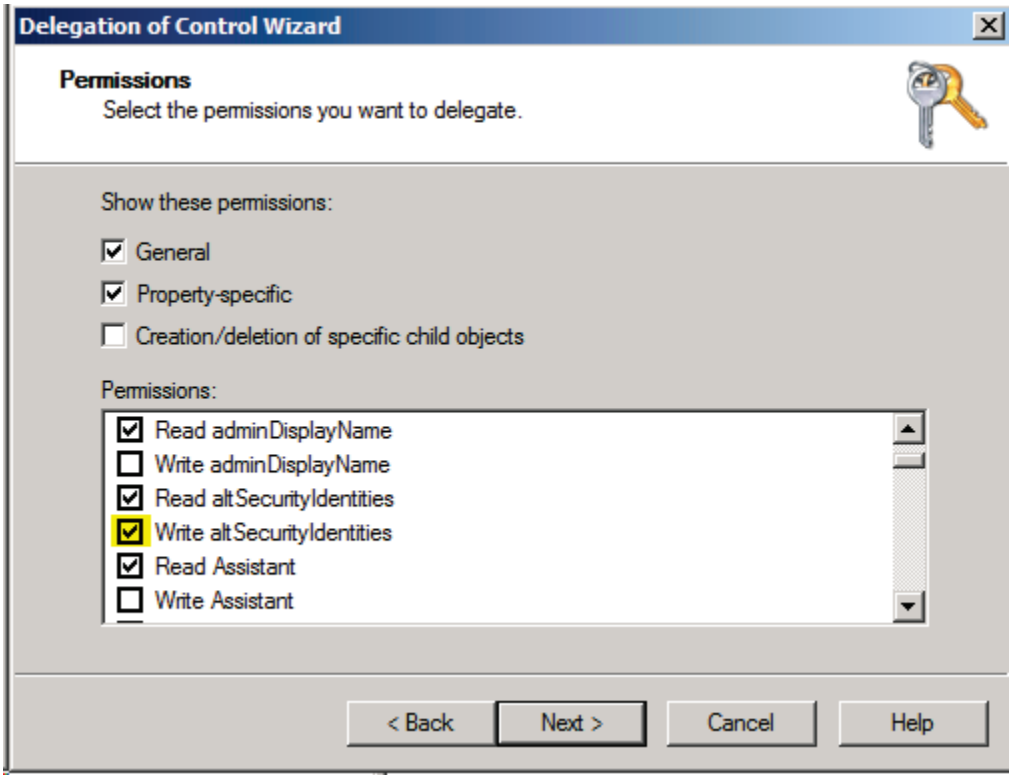
2.

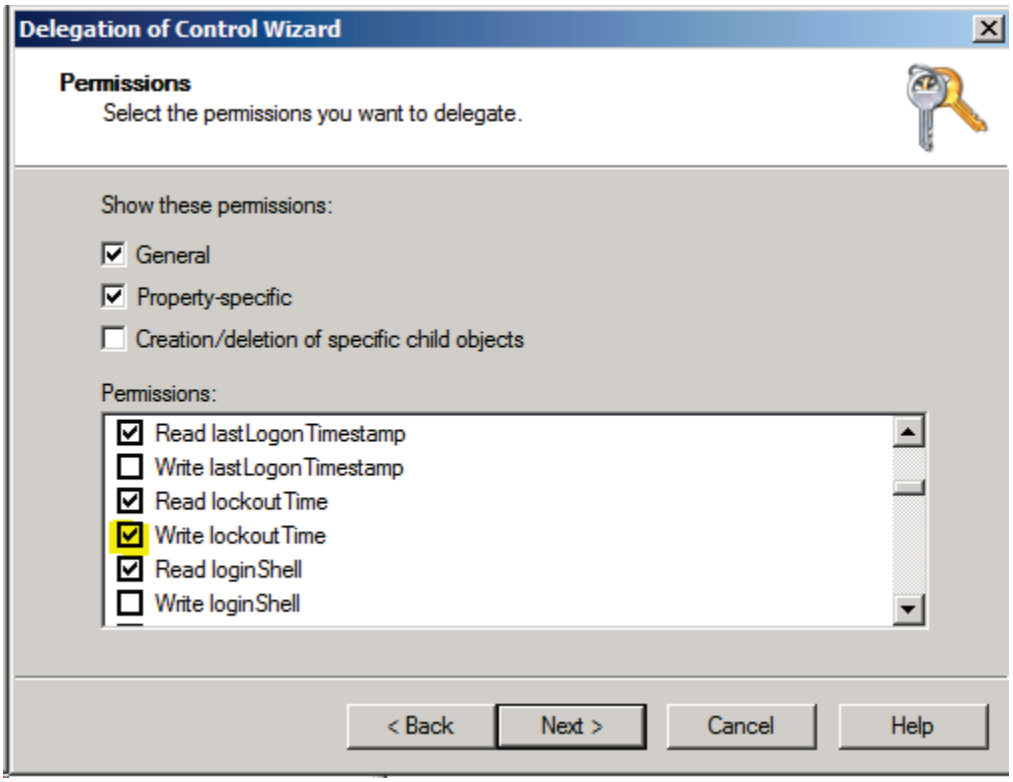

Delegation of Control Wizard
Tasks to Delegate
You can select common tasks or customize your own.
Delegate the following common tasks:
Create, delete, and manage user accounts
Reset user passwords and force password change at next logon
Read all user information
Modify the membership of a group
Join 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

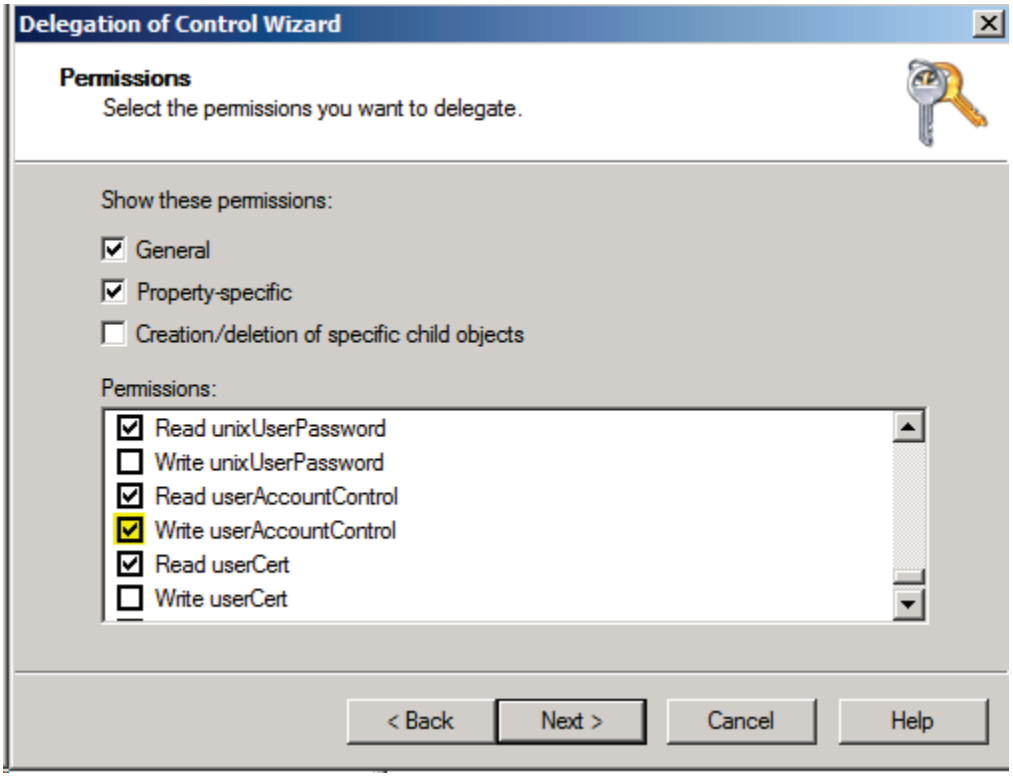
3.


Delegation of Control Wizard
Active Directory Object Type
Indicate 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:
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

4. 
Delegation of Control Wizard
Permissions
Select the permissions you want to delegate.
Show these permissions:
General
Property-specific
Creation/deletion of specific child objects
Permissions:
Delete All Child Objects
Read All Properties
Write All Properties
Change password
Reset password
Send as
< Back
Next >
Cancel
Help

5. 
Delegation of Control Wizard
Permissions
Select the permissions you want to delegate.
Show these permissions:
General
Property-specific
Creation/deletion of specific child objects
Permissions:
Read adminDisplayName
Write adminDisplayName
Read altSecurityIdentities
Write altSecurityIdentities
Read Assistant
Write Assistant
< Back
Next >
Cancel
Help

6. 
Delegation of Control Wizard
Permissions
Select the permissions you want to delegate.
Show these permissions:
General
Property-specific
Creation/deletion of specific child objects
Permissions:
Read lastLogonTimestamp
Write lastLogonTimestamp
Read lockoutTime
Write lockoutTime
Read loginShell
Write loginShell
< Back
Next >
Cancel
Help

7. 
Delegation of Control Wizard
Permissions
Select the permissions you want to delegate.
Show these permissions:
General
Property-specific
Creation/deletion of specific child objects
Permissions:
Read unixUserPassword
Write unixUserPassword
Read userAccountControl
Write userAccountControl
Read userCert
Write userCert
< Back
Next >
Cancel
Help

8. 

END OF GUIDE

Enterprise Support Team
SysOp Tools, Inc.
1-877-SYSOPTOOLS
Direct / Fax 213-995-5060
www.sysoptools.com