FastPass Password Manager
Version 3.5.1
# Table of Contents

1. Introduction ..................................................................................................................................................................... 4  
   1.1 Purpose ................................................................................................................................................................... 4  
   1.2 Audience ................................................................................................................................................................. 4  
   1.3 References .............................................................................................................................................................. 4  
   1.4 How to use this document ...................................................................................................................................... 4  
   1.5 Terms ...................................................................................................................................................................... 4  
2. Delegating Standard Task Permissions via ADUC ............................................................................................................ 5  
3. Delegating Custom Property Permissions via ADUC ..................................................................................................... 11  
4. Delegating permissions via the command-line ............................................................................................................. 15  
5. Getting permission to work for users in protected groups ........................................................................................... 16  
6. Removing delegated permissions .................................................................................................................................. 18
1. Introduction

The document is targeted the FastPass Password Manager Version 3.5.1

1.1 Purpose

The purpose of this document is to describe how to configure permission delegation in Microsoft Active Directory for the use of FastPass Password Manager. In the first section this is done using the Windows GUI, in the second section the same is achieved using the command line. Please be aware that users who are members of protected groups will not get affected by the delegated permission (and will there for not be able to use FastPass) before the commands are issued for the adminSDfolder in AD – please look at section 5 for details regarding this.

Notice that this document isn’t part of the official product documentation but just delivered to customers and partners as a service to transfer some knowledge about how to make this advanced configuration in Windows AD.

1.2 Audience

The intended audience of this document is personnel responsible for administration of the solution.

1.3 References

This document refers to the following documents:

None.

1.4 How to use this document

This document has a very limited scope and is expected to be read all in complete.

1.5 Terms

The following technical and product specific terms are used without further explanation throughout the document.
2. Delegating Standard Task Permissions via ADUC

First we start Active Directory Users and Computers (ADUC).

Right-Click the OU you want to delegate permissions for.

Select Delegate Control.

Click Next in the Delegation of Control Wizard.
Add the users and/or groups you want to delegate permissions to. And click Next.

Select the standard task to delegate. In this case we have chosen the permission to reset user passwords and force password change at next logon. Then click Next.
Click Finish to set the permissions in Active Directory.

Go back to ADUC and right-click the OU we chose before. This time select Properties. If you only have the following tabs visible:

You need to enable Advanced Features by activating it in the View menu.
Now we can see some more tabs:

By selecting the Security tab, we can see the group and user we chose before. Because the permissions we delegated do not constitute one of the standard permissions, the special permissions is checked. Click Advanced to see the permissions up close.
Here we can see that the group and user have been given the Reset Password permission for User objects only, and a Read/write Property permission. By selecting this permission and clicking Edit, we can see the specific property.

Here we can see that the permission set is to Allow the Read and Write pwdLastSet properties.
And for the Reset Password permission, it is the Reset Password property.

We could also have set these permissions manually, but it is easier to do it via the Delegation of Control wizard.
3. Delegating Custom Property Permissions via ADUC

First we start Active Directory Users and Computers (ADUC).

Right-Click the OU you want to delegate permissions for and select Delegate Control.

Click Next in the Delegation of Control Wizard.
Add the users and/or groups you want to delegate permissions to. And click Next.

Select Create a custom task to delegate. Then click Next.
Now select what kind of objects you want to delegate permissions for. Here I have selected only User objects. Notice that if you select the check boxes, permissions to create and delete user objects will also be delegated. You can also choose all objects in the current container by selecting the first radio button. After making your selections, click Next.

On the next page in the wizard, deselect General and select the Property-specific checkboxes. Now choose the different properties you want to delegate permissions for. Here I have chosen the following property:

- lockoutTime
Click Finish to set the permissions in Active Directory.

As with the Standard Task delegation, you can go back to ADUC and check the permissions. Follow the procedure in the previous chapter.
4. Delegating permissions via the command-line

If you install the support tools from the CD, you can also use the command-line tool dsacls to add, change and remove permissions in Active Directory. The following two commands will do exactly the same for the delegategroup:

\texttt{dsacls "cn=adminsholder, cn=system, dc=mydomain, dc=com" /I:S /G "domain\Delegategroup:CA;Reset Password";user}

\texttt{dsacls "cn=adminsholder, cn=system, dc=mydomain, dc=com" /I:S /G domain\Delegategroup:RPWP;pwdLastSet;user}

To delegate a permissions to a single property, e.g. lockoutTime:

\texttt{dsacls "cn=adminsholder, cn=system, dc=mydomain, dc=com" /I:S /G domain\Delegategroup:RPWP;lockoutTime;user}

Note: Please change the DN and groups names to values matching your system.

Further description of the tool can be found at:

\url{http://technet2.microsoft.com/windowsserver/en/library/ffd71dba-386e-463e-9529-f0b77d708ca01033.mspx}
5. Getting permission to work for users in protected groups

As part of the AD design AD will not let delegated permissions work on accounts who has a membership of protected groups – which means that users that are members of these groups – e.g. Account Operators cannot reset their Password using the FastPass user with delegated rights. The problem is that a member of protected groups does not inherit the Delegated permissions. To get that working we must Grant Reset Password etc. rights to the Privileged Active Directory FastPass user account on the AdminSDHolder object in AD. This will allow the account to reset the password of every user who is a member of the groups listed below under “AdminSDHolder Secured Groups”

Granting Permissions on the AdminSDHolder Object

Important: When making a change to the AdminSDHolder security descriptor, please realize this change is applied on every object whose security descriptor is managed by the Active Directory to match the AdminSDHolder. This includes, among others, members of the Domain Admins and Enterprise Admins security groups.

To delegate Reset Password rights to the FastPass user to the AdminSDHolder, use DSACLs at a command line as follows:

dsacls "cn=adminsdholder,cn=system,dc=mydomain,dc=com" /G "Domain\Delegategroup:CA;Reset Password"

dsacls "cn=adminsdholder,cn=system,dc=mydomain,dc=com" /G "Domain\Delegategroup:RPWP;pwdLastSet"

dsacls "cn=adminsdholder,cn=system,dc=mydomain,dc=com" /G "Domain\Delegategroup:RPWP;lockoutTime"

Note: Please modify the distinguishedName and FastPass account in the commands above to match your system.

In order to propagate the changes of inheritable ACEs to descendent objects, domain controllers runs a background task called the Security Descriptor Propagator Update task.

You can force the propagation to occur using the following receipt:

1. Go to Start, click Run, type LDP.exe, and click OK.
2. On the Connection menu in the LDP console, click Connect.
3. On the Connect window, type the server name you want to connect to into the Server field, ensure 389 is listed in the Port field, and then click OK.
4. On the Connection menu, click Bind.
5. On the Bind window, select the Bind as currently logged on user option or select the Bind with credentials option. If you selected the latter, enter the credentials you want to bind with. Click OK.
7. On the Modify window, FixUpInheritance into the Attribute field, type Yes into the Value field, select the Add operation, and then click Enter.
8. The Modify window should look like this:
The amount of time that this takes to complete depends on the size of your Active Directory environment. The larger the environment, and the more Security Descriptors that have changed, the longer it will take the process to run. You can monitor the DS Security Propagation Events counter in the NTDS Performance object to determine when this has completed, which will be indicated by a counter value of 0.
6. Removing delegated permissions

Go through ADUC and remove the permissions, use dsacl or download the tool DSRevoke from the Microsoft web site.

How to use Dsacls.:

http://support.microsoft.com/kb/281146

DSRevoke.: