

Successful Preservation of User Profiles on Windows® 2000 and XP Workstations when switching Active Directory Domains

Matt Bradford

October 7, 2005

Contents

1 Abstract	3
2 Prerequisites	3
3 Create a profile for the new domain	4
3.1 If both domains are in the Domain drop-down	4
3.2 If the NEWCOMPANY domain isn't in the Domain drop-down . .	4
3.2.1 Login to workstation using an account with Local Adminis- tration rights	5
3.2.2 Disjoin the workstation from the MYDOMAIN domain . .	5
3.2.3 Join the workstation to the NEWCOMPANY domain . . .	5
3.2.4 Login as the new user on the new domain	6
3.2.5 Re-join the workstation to the MYDOMAIN domain	6
4 Step 2. Migrating the profile	7
4.1 Open the User Profiles dialog	7
4.2 Copy the User's Profile	7
4.3 Allow the new domain account access to the profile	7

CONTENTS

5	Join the NEWCOMPANY domain	8
5.1	Disjoin the MYDOMAIN domain	8
5.2	Join the NEWCOMPANY domain	8
6	Finalizing the process	8
6.1	Login to the NEWDOMAIN domain	8
6.2	Items of issue	9
6.2.1	Login with domain administrator privileges	9
6.2.2	Login again with the user's account	9
7	Conclusion	9

1 Abstract

Microsoft's Active Directory (AD) provides a very intuitive interface to combining complex technologies such as Kerberos, LDAP and DNS into one centrally-organized system. However, unless the AD layout is fully planned from the start, many complications can be encountered if the organization or network structure changes.

One such problem is keeping profiles in tact when dis-joining a workstation from one domain and joining it to another. This document attempts to address this problem with a structured outline of what needs to be done, and why.

2 Prerequisites

Before we begin a migration, we need to make sure we have the necessary accounts. We will need the following:

- The user's username. For this article, we will assume we are migrating the account of Joe Bloggs, username "jbloggs". The password of this user must be known, or the user must be present to type it when required.
- A Domain Administrator account for the domain we're leaving.
- A Domain Administrator account for the domain we're joining.
- A Local Administrator account for the local PC. The Local Administrator account is not strictly required, but if something goes wrong during the changeover process and a machine needs to be rebooted, the Local Administrator account will be needed to join a machine back to a domain.

As mentioned, we will be migrating user "jbloggs". His original AD domain is mydomain.net, appearing to the user as MYDOMAIN, and we will be migrating him to the newcompany.com domain, appearing to the user as NEWCOMPANY. The "jbloggs" account exists on both systems. The account name does not need to be the same in theory, but this hypothesis has not been tested.

We also need to locate the user's current profile. Under a default Windows® install, this will be c:\Documents and Settings\jbloggs. One can discover the path to one's profile by examining the %USERPROFILE% environment variable.

Finally, we will provide commands for use with the *netdom* utility, which comes with Windows® 2000 and XP Admin Packs. The GUI equivalents may be used, but describing how to use them is outside the scope of this article.

Once we have all these things, we may continue.

3 Create a profile for the new domain

3 Create a profile for the new domain

What one does here is determined by what one sees at the login prompt. To be brief, if one can see both the MYDOMAIN and NEWCOMPANY domains from the domain drop-down on the login screen, this task becomes easier. If one cannot, then two options exist.

The first option is to create a trust between the two domains — the process for doing so is outside the scope of this article. The second option is to join the new domain temporarily, and then revert to the original domain. I do not suggest that this method is the only method for achieving what we need to achieve, but I would suggest it is a safe method.

Regardless of which lot you have been dealt, what we are ultimately trying to achieve in this step is to make Windows® create an empty profile for “jbloggs” associated with the NEWCOMPANY domain. This becomes important later when we need to migrate the profile.

3.1 If both domains are in the Domain drop-down

In this case, it is simply a matter of logging the user in under the new NEWCOMPANY domain, and logging them out again. Windows automatically creates a new profile for jbloggs based on the local machine’s default profile, and will have the name “jbloggs.NEWCOMPANY”. This can be confirmed by evaluating the %USERPROFILE% environment variable whilst the user is logged into the new domain.

If this completes successfully, you can skip ahead to section 4.

If something goes wrong...

If the user is unable to login to the domain for whatever reason, the trust between the two domains may not be set up correctly, or the user’s credentials may not be correct. Ensure that the credentials are correct on another machine that is already a member of this domain, and try again. If this fails, one may be required to resort to case 2, listed below.

3.2 If the NEWCOMPANY domain isn’t in the Domain drop-down

To some, this method may seem like we’re taking two steps back in order to take one step forward. Again, this is only a suggestion, but in the experience I have had with migrating workstations between domains, nothing is ever certain. This method aims to be a stable and repeatable process, which may in the end save some headaches.

3.2 If the NEWCOMPANY domain isn't in the Domain drop-down

3.2.1 Login to workstation using an account with Local Administration rights

Only administrators can Join or Disjoin domains. Logging in with a Local Administrator account allows us to do so.

3.2.2 Disjoin the workstation from the MYDOMAIN domain

Open a command line (cmd.exe). Type *hostname* to show the hostname of the current workstation. In this case, we will pretend we are removing arbitrary workstation “workstation-l1-s23”.

Remove the computer from the MYDOMAIN domain using the following command:

```
netdom remove workstation-l1-s23 /domain:mydomain.net
    /userd:Administrator /passwordd:*
```

This will prompt for the password for the Administrator account on the MYDOMAIN domain. If this command completes successfully, the workstation will no longer belong to the MYDOMAIN domain, and accounts from it will no longer be recognized. This means that if one were to logout or reboot the machine, only the accounts on the local machine will authenticate.

For the overcautious, you may like to reboot and login again with local administrator rights before you continue, but most of the time it will not be necessary.

If something goes wrong...

If the computer does not disjoin from the domain, you may want to ensure your credentials are correct. Make special note of the error produced by *netdom.exe* (This is why we use the command line utilities). In either case, it may be best to reboot the machine after tinkering if it does not disjoin cleanly.

3.2.3 Join the workstation to the NEWCOMPANY domain

Again on the command line, type the following to join it to the NEWCOMPANY domain. The last argument is only required if one wishes to place the current workstation in a particular Organizational Unit (OU) on the domain controller whilst joining. If one does not mind the current workstation being placed in the default “Computers” OU, then one may omit the entire */ou:...* argument.

```
netdom join workstation-l1-s23 /domain:newcompany.com
    /userd:Administrator /passwordd:*
    /ou:ou=desktop,ou=computers,ou=research,dc=newcompany,dc=com
```

3.2 If the NEWCOMPANY domain isn't in the Domain drop-down

This will prompt for the password for the Administrator account on the NEWCOMPANY domain. Once this completes, this workstation will belong to the NEWCOMPANY domain, and accounts from the NEWCOMPANY domain will be able to login to this workstation.

If something goes wrong...

If the computer does not join correctly, again, take note of the error message. The error messages are often somewhat informative, and a quick search on the Internet should reveal steps to take to correct them. If you did not reboot after the last step, maybe now is a good time to do so.

3.2.4 Login as the new user on the new domain

We now return to the login prompt, and select the NEWCOMPANY domain from the domain drop-down. The old MYDOMAIN domain may or not be present in the list — that doesn't matter for now. Enter in (or get Joe to enter in) the credentials for the “jbloggs” account on the NEWCOMPANY domain.

This puts us on par with what was accomplished under Case 1. A new profile is created based on the local machine's default profile, and we'll finally have a profile with the name “jbloggs.NEWCOMPANY”. This can be confirmed by evaluating the %USERPROFILE% environment variable whilst the user is logged into the new domain.

3.2.5 Re-join the workstation to the MYDOMAIN domain

This may seem like a silly idea. The reason for all this joining and dis-joining is due to the dependencies that exist in this process. Ultimately, we wish to copy the old user's profile into the new user's profile. But we can't do this without the workstation having created an empty profile for the new account to begin with. To overcome this, we've joined the machine to the new domain, and logged in using the new account, thus creating our empty profile.

So now we have the profile, we need to use a windows tool in the next step to properly copy the profiles. However, one will find that in this tool, the accounts from the old domain will no longer be listed as their username and will appear as “(Account Unknown)”, and more importantly, the tool will not allow the profile to be copied anywhere. So hopefully now it's clear why we must join the old domain.

Quickly, this can be done using the same commands as above. Again, the */ou:...* argument may be omitted.

```
netdom remove workstation-l1-s23 /domain:newcompany.com
      /userd:Administrator /passwordd:*
```

4 Step 2. Migrating the profile

```
netdom join workstation-l1-s23 /domain:mydomain.net
        /userd:Administrator /passwordd:*
        /ou:ou=desktop,ou=computers,ou=research,dc=newcompany,dc=com
```

Follow the precautions mentioned during the beginning of this process. Once the workstation is back on the MYDOMAIN domain, we may continue.

4 Step 2. Migrating the profile

Now we have a blank profile for the new account on the NEWCOMPANY domain, and we are still joined to the old MYDOMAIN domain. We now must copy the old jbloggs profile into the new jbloggs.NEWCOMPANY profile. Please note that simply copying the files from one profile to the other will NOT work successfully. There are a few Windows® permission and registry issues that must be modified, which the tool used to copy profiles does for us.

4.1 Open the User Profiles dialog

This is found in the “System Properties” dialog, which can be accessed by clicking the “system” icon from the control panel, or right-clicking on “My Computer” and selecting properties, or even with the key combination <WinKey> + <Pause>. Navigate to the “Advanced” tab, and select “Settings” in the “User Profiles” area.

4.2 Copy the User’s Profile

Find the user’s profile in the list. In our case, it will be MYDOMAIN\jbloggs. Click the “Copy To” button¹. A directory browser will appear - we wish to select the directory of the new domain’s profile – jbloggs.NEWCOMPANY. Click OK to select this directory, but DO NOT click OK on the “Copy To” dialog.

4.3 Allow the new domain account access to the profile

Here we allow the jbloggs account from the NEWCOMPANY domain to access the new profile after it’s been copied. This is achieved by clicking “Change” in the “Permitted to use” area of the “Copy To” dialog still visible on the screen. Click “Change”; the “Select User or Group” dialog appears. Click “Location” and select the NEWCOMPANY domain, and click OK. Type “jbloggs” in the text box, and click “Check Names”. The name should resolve correctly. If it does not, try NEWCOMPANY\jbloggs.

¹If both the “Delete” and “Copy To” buttons are grayed out, it means that the profile’s files are still in use — A reboot will fix this.

5 Join the NEWCOMPANY domain

Click OK to close the “Select User or Group” dialog, and click OK to start copying the profile. This may take some time.

5 Join the NEWCOMPANY domain

The steps from 3.2.3 and 3.2.5 can be followed to achieve this. We firstly disjoin our current MYDOMAIN domain, and then join the NEWCOMPANY domain. These commands can be entered in on the command line.

5.1 Disjoin the MYDOMAIN domain

Steps from 3.2.3 can be followed here. Briefly, the command line method for achieving this is as follows:

```
netdom remove workstation-l1-s23 /domain:mydomain.net  
/userd:Administrator /passwordd:*
```

5.2 Join the NEWCOMPANY domain

Steps from 3.2.5 can be followed here. Briefly, the command line method for achieving this is as follows:

```
netdom join workstation-l1-s23 /domain:newcompany.com  
/userd:Administrator /passwordd:*  
/ou:ou=desktop,ou=computers,ou=research,dc=newcompany,dc=com
```

It's probably advisable to reboot after this.

6 Finalizing the process

6.1 Login to the NEWDOMAIN domain

We should now have the NEWDOMAIN appearing in the Domain drop down of the Windows® login window. Select it, and login using the user's account (jbloggs). The user's profile should have been transferred correctly, and the user's settings and applications should still be present.

6.2 Items of issue

6.2 Items of issue

The user may find that some files that he or she used to have access to now deny them access. This is due to the permissions and ownership properties of the files and directories on the file system. This can be fixed using a Domain Administrator account.

6.2.1 Login with domain administrator privileges

Using an Domain Administrator account for the NEWCOMPANY domain, login to the workstation. Find the troublesome files or directories, open the properties for them, and click the “Security” tab².

Click the “Add” button, and add the jbloggs account from the NEWCOMPANY domain. Give this user the necessary permissions to access the files or directories in question. In most cases, “Full Control” is appropriate.

6.2.2 Login again with the user’s account

The user should now have permissions to access these files. Optionally, they may wish to take ownership of the files and directories they now have. This can be done from the “Owner” tab found in the “Advanced” section of the security tab that was opened from 6.2.1.

7 Conclusion

As seen, this is not an easy process, and should not be done without preparation. I would recommend the following tips:

- Before working on production machines, try and even re-try this process on a test machine, joined to the original domain.
- After migration, do not delete the user’s old profile straight away. There is always the chance that something went wrong and is not discovered until later, or the machine may have to be joined back to the old domain. Instead, wait a set period of time for everything to settle down, and then delete the old profiles.

²If you have made a selection of both files and directories, and tried to open the properties, the Security tab will not be present. I don’t know why this is; but the workaround is to simply do files and directories separately.