

WINDOWS NT PROFILES

By Mark E. Donaldson

Copy A User Profile

User profiles are stored under the %systemroot%\profiles directory, but if you just try to copy this to someone else the new user will not have permission to use the profile. Instead the following procedure must be used:

1. Logon as an Administrator.
2. Start the System Control Panel Applet (Start - Settings - Control Panel - System).
3. Click the User Profiles tab.
4. You will see a list of all the profiles stored on the machine. Select the one which you wish to copy.
5. Click the "Copy to" button.
6. In the "Copy profile to" enter the location where you want it copied to. If you wanted to use as a roaming profile you would enter the netlogon location on a domain controller, usually %systemroot%\system32\Rep\Export\Scripts, you want the Export area not Import as anything in Export is copied to the import by the replication process.
7. In the "Permitted to use" click Change. Select Everyone and click Add or just the user who will use it, then click OK.
8. Click OK to start the copy.

You should then check that the file ntuser.dat has been created where you selected.

If you are not using roaming profiles but are instead just copying a profile for another domain user on the local machine you may just create a directory under profiles for the user and copy it there as per the instructions above.

If you do this you will find that when the user logs in for the first time for whom you copied the profile, they will not use the directory you created for them, but instead a <username>.000 will be created instead. This is because a mapping is used for the user to the Profile area and if the user logs in for the first time and a directory of its user name already exists it won't use it and will instead create a new area of the format <username>.nnn where nnn starts at 000.

The workaround to this is to logon as the domain user first, logout and then copy the profile as this will setup the correct mapping of the user to profile area. If this has already happened perform the instructions in **Defining The Profile Area To Use For A User**.

Defining The Profile Area To Use For A User

By default when a user logs on for the first time at a machine a directory under %systemroot%\profiles is created under the name of the user to hold the users profile, e.g. for user smith the area created would be %systemroot%\profiles\smith. Problems arise if the directory already exists and so an alternate directory <user name>.nnn will be created, starting with 000. This mapping is stored in the registry HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList. You can therefore force a user to use a specific profile area by performing the following:

1. Start the registry editor (regedit.exe).

WINDOWS NT PROFILES

By Mark E. Donaldson

2. Move to
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsT\CurrentVersion\ProfileList .
3. Find the SID that relates to the user (check the ProfileImagePath value) .
4. Once found double click on ProfileImagePath and remove the .nnn, e.g.
%SystemRoot%\Profiles\garfield.000 to %SystemRoot%\Profiles\garfield.
5. Click OK and close the registry editor.

The user should now login using the profile you originally copied for them. Once you are sure it works you can delete the <username>.nnn directory under %systemroot%\profiles. You should make sure the user has the right to user the original profile, for example if you have copied it to that location and granted rights accordingly.

Exporting A Profile

To be able to export your profile perform the following:

1. Logon as you.
2. Start the registry editor (regedt32.exe) .
3. Select the "HKEY_CURRENT_USER on Local Machine" window.
4. Move to Software\Microsoft\Protected Storage System Provider\<SID>.
5. Select Permissions from the Security menu.
6. Click Add.
7. Select Domain Admins (or whatever you want), access type READ and click Add. When finished click OK.

You should now be able to export this profile.

To be able to export someone else's profile perform the following:

1. Logon as an Administrator.
2. Start the registry editor (regedt32.exe).
3. Select the "HKEY_USERS on Local Machine" window.
4. From the registry menu select "Load hive".
5. Move to the persons profile area in the %systemroot%\Profiles\<name>, e.g.
d:\winnt\Profiles\batman.
6. Select the NTUSER.DAT file and click OPEN.

WINDOWS NT PROFILES

By Mark E. Donaldson

7. When asked for a key name enter their name (e.g. John) and click OK.
8. Now move to <user name>\Software\Microsoft\Protected Storage System Provider\<SID>.
9. Select Permissions from the Security menu.
10. Click Add.
11. Select Domain Admins (or whatever you want), access type READ and click Add. When finished click OK.
12. Select Unload Hive from the registry menu.
13. Close the registry editor.

You will now be able to export this users profile.

Move Object Within A Forest

The Windows 2000 Resource Kit ships with the MOVETREE.EXE utility which can be used to move organization units, users or computers between domains in a single forest. This is useful for the consolidation of domains or to reflect organization restructuring.

Certain objects cannot be moved with MOVETREE such as Local and Domain Global groups and if the container they are in is moved these objects will be placed in an "orphan" container in the "LostAndFound" container in the source domain.

Associated data is not moved with MOVETREE such as policies, profiles, logon scripts and personal data. To accomplish the movement of these items you should write custom scripts using the 'Remote Administration Scripts'.

The syntax of MOVETREE is:

```
MoveTree [/start | /continue | /check] [/s SrcDSA] [/d Dst] [/sdn SrcDN] [/ddn DstDN] [/u Domain\Username] [/p Password] [/quiet]
```

- /start - Start a move tree operation with /check option by default. Instead, you could be able to use /startnocheck to start a move tree operation without any check.
- /continue - Continue a failed move tree operation.
- /check - Check the whole tree before actually move any object.
- /s <SrcDSA> - Source server's fully qualified primary DNS name. Required.
- /d <DstDSA> - Destination server's fully qualified primary DNS name. Required.
- /sdn <SrcDN> - Source sub-tree's root DN. Required in Start and Check case. Optional in Continue case.

WINDOWS NT PROFILES

By Mark E. Donaldson

- /ddn <DstDN> - Destination sub-tree's root DN. RDN plus Destination Parent DN. Required.
- /u - <Domain\UserName> - Domain Name and User Account Name. Optional.
- /p <Password> - Password. Optional.
- /quiet - Quiet Mode. Without Any Screen Output. Optional

You should first run in /check mode as this will perform a test without actually performing the move. Any errors will be displayed and also written to the file movetree.err in your current directory. If the test is OK run with the /start option. An example use would be:

```
C:\> movetree /check /s titanic.market.savilltech.com /d pluto.legal.savilltech.com  
/sdn OU=testing,DC=Market,DC=Savilltech,DC=COM  
/ddn OU=test2,DC=Legal,DC=Savilltech,DC=COM
```

This would move the OU testing from domain market.savilltech.com to test2 in domain legal.savilltech.com.

Restrict Access To Registry Editor

Using the registry editor (regedt32.exe):

1. Highlight HKEY_USERS and Load Hive from the Registry menu.
2. Browse to the users profile directory who you want to restrict the registry tools for and select NTUser.dat.
3. When prompted for Key Name, input their UserID.
4. Navigate to \Software\Microsoft\Windows\CurrentVersion\Policies.
5. If no System sub-key exists, Add Key. Then Add Value of DisableRegistryTools (under the System key) using type REG_DWORD and set it to 1.
6. Unload Hive from the Registry menu.

Configure Roaming Profiles

When you sit at a computer and change its attributes, such as the wallpaper, when someone else logs on they still have the environment that they last had when they logged on, and this is achieved using a profile for the user which is stored locally in the %systemroot%/profiles/<username>, e.g. d:\winnt\profiles\savillj.

If the user then sat at a different computer they would not have their setup, to achieve a profile that follows the user to different NT machines (a roaming profile) you need to store the users profile on a network share, that can be downloaded each time the user logs on. When the user logs off the network profile is updated, and a copy of the profile is saved locally. To configure roaming profiles perform the following:

WINDOWS NT PROFILES

By Mark E. Donaldson

1. Start User Manager for Domains (Start - Programs - Administrative Tools - User Manager for Domains).
2. Double click on the user.
3. Click the Profiles button.
4. In the User Profile Path enter the network share location where the profile should go, \\<servername>\<share name>\<user name>.
5. Click OK to finish.

To make the profile mandatory, i.e. the user cannot change it, rename the file ntuser.dat to ntuser.man which is located at the base of the profile location.

Profiles are cached locally to machines, however this can be disabled by performing the following:

1. Start the registry editor (regedit.exe).
2. Move to
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon.
3. Create a value called DeleteRoamingCache of type DWORD (Edit - New - Dword).
4. Set the value to 1.

Move Users From One Machine to Another

If you just want to replace the PDC of a domain with a new machine, the easiest way is to install the new machine as a BDC and then promote to the PDC which removes the need of adding/removing users.

If you actually want to merge two domains or just move some accounts the procedure below should help. You will need the resource kit utility addusers.exe.

1. Log on as an Administrator on the machine that has the accounts you wish to move.
2. Run the command addusers /d <file name>. This will create a comma separated file with details of all accounts and groups.
3. You don't want the information about global or local groups (such as Administrators etc) so edit the file and remove the [Global] and [Local] sections and their content.
4. Copy the file to the machine you want to create the accounts on or a network drive.
5. Log on as an Administrator on the machine that the accounts should be added, if a domain, log on to the PDC.
6. Run the command addusers /c <file name>. This will read in the file and create the accounts.
7. You could then delete the accounts off the original machine using addusers /e <file name>

WINDOWS NT PROFILES

By Mark E. Donaldson

Configure Default Settings For New Users

When a new user logs in for the first time a copy of the default user profile (ntuser.dat) is copied into the users profile. To set default settings for a user you can edit the default ntuser.dat file. Anything you define under HKEY_CURRENT_USER can be changed by editing ntuser.dat.

To change default settings for a new user on a workstation perform the following:

1. Start the registry editor (regedt32.exe).
2. Select the "HKEY_USERS on Local Machine" window.
3. Select "Load Hive" from the Registry menu.
4. Move to %systemroot%\Profiles\Default User (e.g. d:\winnt\Profiles\Default User).
5. Select Ntuser.dat and click Open.
6. When it asks for a key name enter anything, e.g. defuser.
7. Now select the username (e.g. defuser) in the "HKEY_USERS on Local Machine" window and make the changes (for example you could change the wallpaper by changing defuser\Control Panel\Desktop\Wallpaper). Note - If you add new keys make sure everyone has at least read access otherwise it will not be copied.
8. When you have made the changes select "Unload Hive" from the Registry menu.
9. Close the registry editor.

Anyone logging onto the machine will now pick up these default settings.

To configure a default NTUSER.DAT for a domain perform the above and logon as a user to take these settings. You now need to export these out to the PDC.

1. Logon as an Administrator.
2. Start the System Control Panel Applet (Start - Settings - Control Panel - System).
3. Click the User Profiles tab.
4. You will see a list of all the profiles stored on the machine. Select the one which has the settings you wish to use as the default for the domain.
5. Click the "Copy to" button.
6. In the "Copy profile to" enter the location of the Netlogon share of the PDC (usually %systemroot%\system32\Rep\Export\Scripts, you want the Export area not Import as anything in Export is copied to the import by the replication process), e.g. h:\winnt\system32\rep\export\scripts (if h was mapped to the c\$ drive of the PDC). In the "Permitted to use" click Change. Select Everyone and click Add, then click OK.

WINDOWS NT PROFILES

By Mark E. Donaldson

7. Click OK to start the copy.
8. You should then check that the file ntuser.dat has been created where you selected.

Determine User SID

Perform the following:

1. Start the registry editor.
2. Move to:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProfileList.
3. Select each SID under this in turn and look at the ProfileImagePath and at the end of this string is the name of the user.
4. Close the registry editor

If you knew the SID and just wanted to know the user name you could use the REG.EXE command (with Resource Kit Supplement 2), e.g. reg query

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList\<SID>\ProfileImagePath" e.g. reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1843332746-572796286-2118856591-000\ProfileImagePath".

And again this will show the ProfileImagePath giving you the user.

Disable Control Panel Applets

Using policies it is possible to disable the display control panel applet, however it can also be accomplished using the registry editor:

1. Start the registry editor (regedit.exe).
2. Move to
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System.
3. From the Edit menu select New - DWORD value.
4. Enter a name of NoDispCPL and press enter.
5. Double click the new value and set to 1.
6. Close the registry editor

The change takes immediate effect and if you try and run the display control panel applet either by right clicking on the desktop and selecting properties or starting from the control panel applet you will receive the message "Your system administrator disabled the Display control panel".