



USER PROFILE WIZARD CORPORATE EDITION



USER GUIDE
RELEASE 24.7

**ForensiT Software Limited, Office 8, Ladywood House
Ladywood Works, Lutterworth, LE17 4HD, England.**

Copyright © 2025 ForensiT Software Limited. All Rights Reserved

Contents

Contents	2
Introducing User Profile Wizard	6
Installation.....	7
<i>Installing</i>	<i>7</i>
<i>Licensing</i>	<i>8</i>
<i>Deployment Files.....</i>	<i>8</i>
<i>What have I got?</i>	<i>9</i>
Overview	10
Getting Started	11
<i>Step 1 - Welcome</i>	<i>12</i>
<i>Step 2 – Config File.....</i>	<i>12</i>
<i>Step 3 – Domain Information.....</i>	<i>13</i>
<i>Step 4 – Domain Administrator</i>	<i>14</i>
<i>Step 5 – Workstation Information</i>	<i>15</i>
<i>Step 6 – Existing Domain</i>	<i>17</i>
<i>Step 7 – Update sIDHistory</i>	<i>18</i>
<i>Step 8 – User Account Options.....</i>	<i>19</i>
<i>Step 9 – VPN Settings.....</i>	<i>20</i>
<i>Step 10 – Run Options.....</i>	<i>21</i>
<i>Step 11 – Script Options.....</i>	<i>22</i>
<i>Step 12 – Follow on Script.....</i>	<i>23</i>
<i>Congratulations</i>	<i>24</i>
<i>What did we just do?</i>	<i>25</i>
Migrating User Profiles with User Profile Wizard	27
<i>Welcome</i>	<i>28</i>
<i>Select Computer.....</i>	<i>28</i>
<i>Select a User Profile</i>	<i>31</i>
<i>Select a User Profile (Personal Edition).....</i>	<i>33</i>
<i>User Account Information.....</i>	<i>34</i>

<i>Migrating Profile</i>	37
<i>Congratulations!</i>	38
Automating Enterprise Migrations	39
<i>Introduction</i>	39
<i>Return of the Deployment Kit</i>	40
<i>Rename workstations</i>	41
<i>Maintaining SID History</i>	43
<i>Rename user accounts</i>	45
<i>Rename Profile Folder</i>	46
<i>Skip migration if user is not found in lookup file</i>	47
<i>Enable ZeroConfigExchange</i>	47
<i>Migrating over a Client VPN</i>	48
<i>Initializing VPN mode... Fails. Invalid Handle</i>	49
<i>Script Options</i>	50
<i>Deploy using a Desktop management tool, like SCCM, or a Group Policy</i>	51
<i>Pre-installed Scripts</i>	52
<i>Running Additional Code</i>	53
<i>Next Steps</i>	55
<i>Create Single Deployment File</i>	56
<i>What did we just do?</i>	57
<i>Fine Tuning</i>	60
<i>The Migration Script</i>	61
<i>Deploying the Script From a Group Policy</i>	61
<i>Deploying a Single Deployment File from SCCM or your RMM Software</i>	62
<i>Advanced Scripting Options</i>	63
Migrating from domain to local accounts	64
<i>Using the GUI</i>	64
<i>Automating Domain to Local Migrations</i>	67
Migrating to Azure AD	69
<i>Azure Object IDs and the ForensiTAzureID.xml file</i>	69
<i>Generating a ForensiTAzureID.xml file</i>	70
<i>Joining to Azure AD</i>	72

<i>Creating a Provisioning Package</i>	72
<i>Configuring User Profile Wizard to migrate profiles to Azure AD</i>	76
<i>Migrating From an Existing Tenant</i>	78
<i>Migrating From a Hybrid Domain</i>	80
<i>Migrating to Office 365 GCC and GCC High Environments</i>	81
<i>Migrating to an Azure AD Account</i>	83
<i>Additional Notes on using a Provisioning Package</i>	86
.config Reference	87
Push migrations and the Command Line Console	93
<i>Push or Pull?</i>	93
<i>Migrating a remote machine</i>	94
<i>Using the command line</i>	95
<i>Automating Push Migrations</i>	96
Command Line Reference	98
<i>Command Line Parameters</i>	98
/COMPUTER computername (Optional)	98
/DOMAIN domainname (Optional)	99
/RENAME computername (Optional)	99
/UNJOIN workgroupname (Optional)	99
/TARGETACCOUNT accountname	99
/SOURCEACCOUNT accountname (Optional)	99
/SOURCEPROFILE profilefoldername (Optional)	99
/DOMAINADMIN domainadmin (Optional)	100
/DOMAINPWD password (Optional)	100
/LOCALADMIN localadmin (Optional)	100
/LOCALPWD password (Optional)	100
/KEY key (Optional)	100
/JOIN (Optional)	101
/NOJOIN (Optional)	102
/NOMIGRATE (Optional)	102
/NODEFAULT (Optional)	102
/DELETE (Optional)	102
/DISABLE (Optional)	102
/SILENT (Optional)	102
/NOREBOOT (Optional)	102
/REBOOTDELAY seconds (Optional)	102
/LOG logfile (Optional)	102
/RUNAS (Optional)	103
/HASH (Optional)	103
Frequently Asked Questions	104

<i>What does User Profile Wizard do?</i>	104
<i>What's a profile?</i>	104
<i>Why migrate profiles when moving to a Windows domain?</i>	104
<i>Why not just copy the data from the old profile?</i>	104
<i>Which version should I buy?</i>	105
<i>Will I have to visit every machine on my network to run the Wizard?</i>	105
<i>What version of Windows does the User Profile Wizard run on?</i>	105
<i>Can I use the free Personal Edition in a commercial environment?</i>	105
<i>What if I have a problem?</i>	106
<i>What isn't migrated?</i>	106
<i>What about group membership?</i>	106
<i>How does User Profile Wizard handle roaming profiles?</i>	106
Troubleshooting	107
<i>Finding Domain Controller Fails/ "The RPC server is unavailable"</i>	107
<i>User 'Name' not found in lookup file</i>	109
<i>Target user not found in Azure Object ID file</i>	109
<i>No DomainName domain account profiles were found</i>	110
<i>Configuring domains to maintain SID history</i>	111
<i>"The security database on the server does not have computer account for this workstation trust relationship"</i>	113
End User License Agreement	114

Introducing User Profile Wizard

Why User Profile Wizard?

A User Profile is where Windows stores your stuff. It is where your Desktop, Documents, Pictures and Music files are all saved. Your User Profile is also where Windows keeps all the information that makes your computer personal to you, like your desktop wallpaper, Internet favourites and the lists of documents you've recently opened.

As the Windows operating system has developed, User Profiles have become ever more important and are now an integral part of the way that Windows organizes data. In some circumstances however, this tying of data to a single user account can be a problem.

As businesses grow, IT requirements change. You might need to reconcile multiple Windows domains into a single Active Directory; you may be connecting your standalone computers to a domain for the first time; or you may be moving to cloud based services like Azure AD and Office 365. When you sign in with a new account, Windows will create a new profile for you and you lose all your data and settings.

This is the problem User Profile Wizard solves. ForensiT User Profile Wizard is a workstation migration tool that will migrate your original user profile to your new logon so that you can carry on using all your existing data, and keep the same settings that you've always had.

User Profile Wizard does not move, copy or delete any data. Instead it configures the existing profile "in place" so that it can be used by the user's new account. This makes the process both very fast and very safe.

This user guide is designed to introduce you to what User Profile Wizard can do. For example, by using the User Profile Wizard Deployment Kit you can build a scalable, enterprise solution to migrate tens of thousands of workstations, each with multiple user profiles.

User Profile Wizard has been developed to save you time, effort and money. We hope you like it.

Installation

Installing User Profile Wizard



You should run the User Profile Wizard setup program on a single “Administrator” machine. The setup program will install the User Profile Wizard application files and documentation, together with the User Profile Wizard Deployment Kit. You can then copy and distribute the User Profile Wizard application files.

The only files you need to run User Profile Wizard are Profwiz.exe and Profwiz.config. You do NOT need to run the setup program on all the machines you want to migrate.

Installing

To install User Profile Wizard run the setup program.

The setup program installs both User Profile Wizard and the User Profile Wizard Deployment Kit.

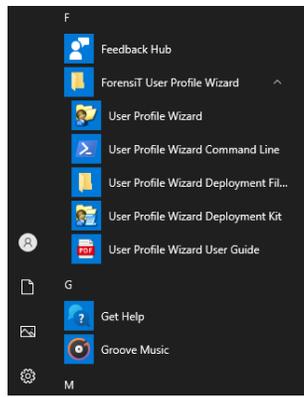
The *User Profile Wizard User Guide*, installed with User Profile Wizard, is a PDF file. If you need PDF reader software, you can download it free of charge from the Adobe website at <https://get.adobe.com/reader/>

Licensing

When you purchase User Profile Wizard you will be sent a link by email to download a **Profwiz.config** file. This file contains your licensing information.

To license User Profile Wizard, you simply need to copy the license file into the same folder as the User Profile Wizard executable file, Profwiz.exe.

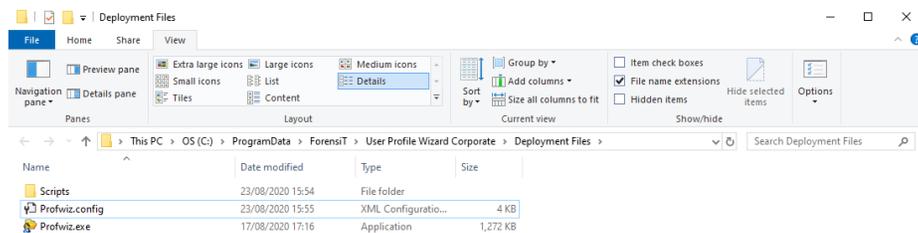
To copy the license file, click the “Start” button and find “ForensiT User Profile Wizard”. Click “Deployment Files” to open the Deployment Files folder. Copy your license config file into the folder.



Deployment Files

To run the User Profile Wizard on another machine you just need to copy the Profwiz.exe and Profwiz.config files. **No other files are required.**

The Profwiz.exe and Profwiz.config files can be copied to any convenient location such as a USB memory flash drive (memory stick or pen drive) or a network share.



What have I got?

The User Profile Wizard setup program installs five shortcuts on the start menu.



The User Profile Wizard User Guide. This document!



The Deployment Files folder. This folder contains the files needed to migrate a workstation to a new domain.



User Profile Wizard



The User Profile Wizard Command Line Console



The User Profile Wizard Deployment Kit

We will reference these icons throughout this user guide.

Overview



User Profile Wizard is designed to make migrating workstations to a new domain as easy as possible. Here's a high-level overview of the process for migrating from one domain to another:

1. Save your domain migration settings to Profwiz.config. To save your domain migration settings run the Deployment Kit. See the [Getting Started](#) chapter in this guide
2. Generate a migration script. If you want to automate workstation migrations, generate a script, again using the Deployment Kit. See [Automating Enterprise Migrations](#).
3. Test the migration process.
4. Deploy the migration files. Copy the migration files from the Project folder to a network share. Create a Computer Startup Group Policy Object to call the migration script, or deploy using a Desktop management tool like SCCM.
4. Test the deployed solution.
6. Migrate machines.

If you just want to migrate workstations interactively see [Migrating User Profiles with User Profile Wizard](#)

If you are looking to “push” migrations from a single administrator machine see [Push migrations and the Command Line Console](#)

User Profile Wizard can also be used to migrate devices to [Azure AD](#), or to migrate devices from a domain [back to a workgroup](#).

Getting Started

Using the Deployment Kit to save your domain migration settings



The settings User Profile Wizard needs to migrate workstations and profiles are saved in the **Profwiz.config** file.

Profwiz.config is a standard xml file. You can edit it in notepad or any xml editor of your choice. However, the easiest way to gather the settings that User Profile Wizard needs is to run the User Profile Wizard Deployment Kit.

The User Profile Wizard Deployment Kit is available from the Start menu: Start F-> ForensiT User Profile Wizard->User Profile Wizard Deployment Kit.

You don't *have* to use the Deployment Kit to be able to use User Profile Wizard, but if you don't save your settings to the Profwiz.config file you will have to enter them every time you want to migrate a machine.

In this section we will run through the basic settings needed to get User Profile Wizard up and running. We will return to the more advanced settings in "Creating Enterprise Migration Scripts" later in this user guide.

Step 1 - Welcome



When you start the User Profile Wizard Deployment Kit the first thing you see is the Welcome page. Click **Next** to continue.

Step 2 – Config File



The first thing the Deployment Kit asks you is whether you want to create a new migration project or edit an existing one. To get started choose “Create migration project”

ForensiT User Profile Wizard Deployment Kit - Step 2 of 13

Config File
Choose a config file option

What would you like to do?

Create a new migration project
Start by giving your migration project a name:
Homestead

Edit an existing migration project
Enter the Profwiz.config file path:
Browse...

< Back Next > Cancel

You can name your project anything you want. Keep in mind, however, that the name of the project will be the default name for your migration script. A good choice is the name of the new domain.

Step 3 – Domain Information



This is where we enter the name of the new domain. In this example, the new domain name is ‘HOMESTEAD’:

The options here are “Join Domain”, “Force Join”, “Join Workgroup”, and “Azure AD”

Join Domain tells User Profile Wizard to join a workstation to a new on-premises domain.

Force Join tells User Profile Wizard to join the workstation to the new domain *even if it is already joined* to the domain. This option is useful if you are replacing one domain with a domain of the same name. This option will configure the Wizard to join the computer to the new domain *even if* no profiles have been migrated.

Join Workgroup tells User Profile Wizard to unjoin a workstation from an existing domain and add the workstation to a workgroup. See the [Migrating from domain to local accounts](#) chapter later in this guide.

Azure AD tells User Profile Wizard to migrate profiles to new Azure AD accounts.

The **Azure ID File Path** is the path to the .xml file that User Profile Wizard uses to look up the Object IDs of new Azure AD user accounts. See [Migrating to Azure AD](#) later in this Guide.

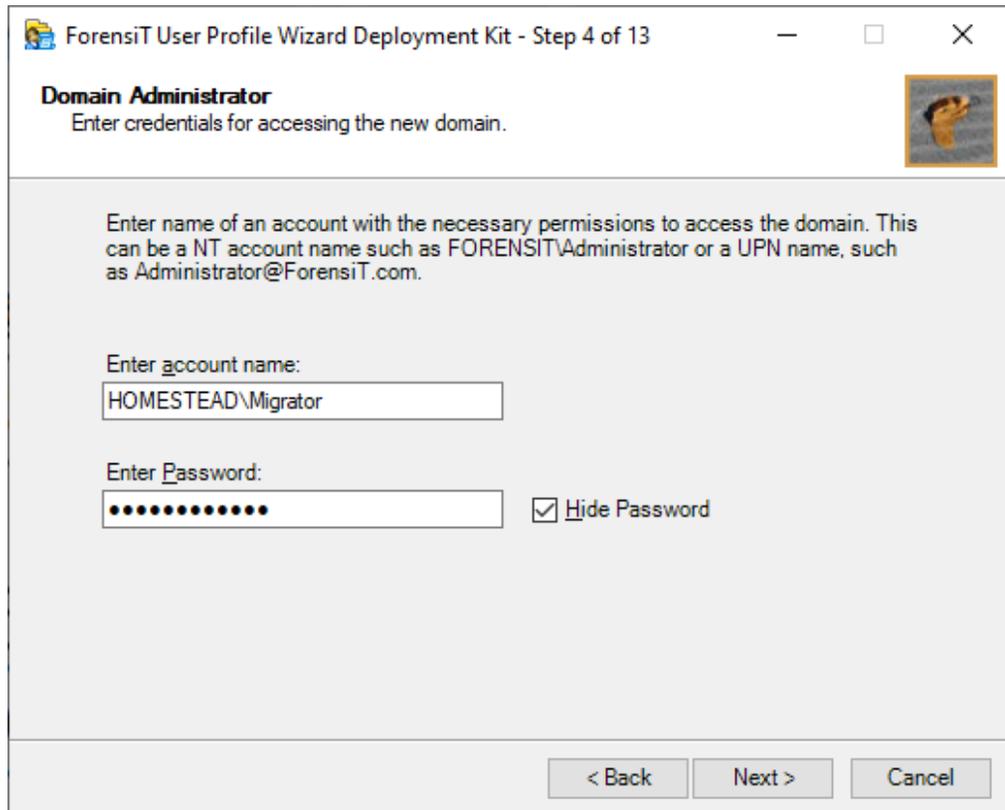
A **Provisioning Package** is used when joining a workstation to a new Azure AD tenant. For information about migrating to an Azure AD tenant, see [Migrating to Azure AD](#) later in this Guide.

Click **Next** to continue.

Step 4 – Domain Administrator



User Profile Wizard needs to know what user name and password you want to use to join your workstations to the new domain. Enter these here. The password will be encrypted when it is stored in Profwiz.config file.



ForensiT User Profile Wizard Deployment Kit - Step 4 of 13

Domain Administrator
Enter credentials for accessing the new domain.

Enter name of an account with the necessary permissions to access the domain. This can be a NT account name such as FORENSIT\Administrator or a UPN name, such as Administrator@ForensiT.com.

Enter account name:
HOMESTEAD\Migrator

Enter Password:
●●●●●●●●●● Hide Password

< Back Next > Cancel

Step 4 will not be displayed if you are migrating to Azure because the Wizard does not join the computer to Azure itself, your Provisioning Package does that.

Click **Next** to continue.

Step 5 – Workstation Information



Step 5 lets you specify two additional options for joining your workstations to the new domain.

ForensiT User Profile Wizard Deployment Kit - Step 5 of 13

Workstation Information
Enter workstation information.

If you want to add workstations to a specific AD container enter the full ADsPath of the container, e.g. OU=Workstations,DC=uk,DC=forensit,DC=com

Enter ADsPath:

Use lookup file to get new computer names.

Enter lookup file path:

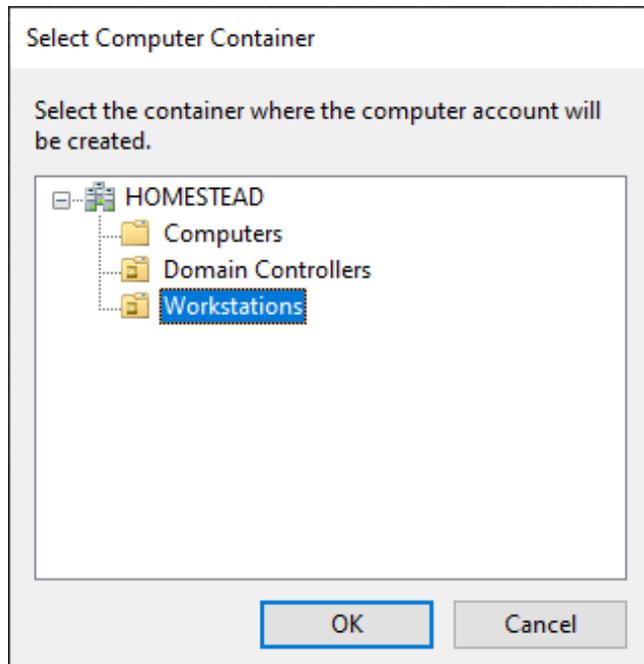
< Back Next > Cancel

Enter AdsPath lets you specify where in your Active Directory tree you want the workstation object to be created. To browse the Active Directory tree click **Browse...** You can then select the container of your choice. (See below.)

Use lookup file to get new computer names lets you rename the workstation when it is joined to the domain. We will cover this in “[Automating Enterprise Migrations](#)” later in this guide.

Step 5 will not be displayed if you are migrating to Azure because the Wizard will not join the computer to Azure itself, your Provisioning Package does that.

Click **Next** to continue.



Step 6 – Existing Domain



On Step 6 you tell User Profile Wizard whether you are migrating profiles from an existing on-premises domain or Azure AD tenant.

If you are migrating from an on-premises Active Directory, enter the existing domain name.

If you are migrating from a Hybrid domain, enter the existing AD domain name (the profiles are associated with the AD account even if the user is logging in with their Azure UPN, you can confirm this with whoami when logged on as one of the source accounts).

If you are migrating from an existing Azure AD tenant, check the box. The Deployment Kit will enter “azuread” in the existing domain name text box, regardless of the name of the existing tenant.

ForensiT User Profile Wizard Deployment Kit - Step 6 of 13

Existing Domain
Enter existing domain information.

Are you migrating from an existing Windows domain or Azure AD tenant?

Yes
 No

Enter existing domain name:
FARM

Migrating from existing Azure AD tenant

< Back Next > Cancel

Click **Next** to continue.

Step 7 – Update sIDHistory

At Step 7 you can choose whether to maintain the SID history of the source domain account.

ForensiT User Profile Wizard Deployment Kit - Step 7 of 13

Maintain SID History

Set SID history settings

If the old domain is available on your network at the time of your migration, you have the option of maintaining the SID history of the source domain account when a user logs on to the target domain.

Please note: User Profile Wizard does NOT require the old domain to be in place to successfully migrate a workstation to a new domain.

Update sIDHistory

Enter a domain Administrator account name for the the old domain:

Enter Password:

 Hide Password

< Back Next > Cancel

We will return to sIDHistory in “[Automating Enterprise Migrations](#)” later in this guide.

Step 7 will only be displayed if the migration is from one domain to another.

Step 8 – User Account Options

Step 8 allows you to set various options related to a user's existing user account.



ForensiT User Profile Wizard Deployment Kit - Step 8 of 13

User Account Options
Choose user account migration options

Use lookup file to get new account names.

Enter lookup file path:

Skip migration if user is not found in lookup file

Rename Profile Folder

Enable ZeroConfigExchange only if you are changing your Email configuration.

Enable ZeroConfigExchange

Use lookup file to get new account names allows you to map a user's existing account name to their new domain account name if the account names are different. We will cover this in "[Automating Enterprise Migrations](#)" later in this guide.

Rename Profile Folder enables you to rename the existing profile folder (usually `C:\Users\Username`) to match the user's new domain username. We will discuss this in more detail in the "[Automating Enterprise Migrations](#)" chapter later in this guide.

Enable ZeroConfigExchange enables Microsoft's ZeroConfigExchange for automatically configuring Outlook.

Click **Next** to continue.

Step 9 – VPN Settings

Step 9 enables you to save settings related to migrating over a Client VPN. We will return to these in “[Automating Enterprise Migrations](#)” later in this guide.

ForensiT User Profile Wizard Deployment Kit - Step 9 of 13

VPN Settings

Select options for migrating over a VPN

Enable offline password caching

Prompt user for password

Use default password for all users.

Enter default password:

Hide Password

< Back Next > Cancel

Step 9 is only an option if the migration is to a Domain, password caching is not required if the migration is to Azure or a local account.

Step 10 – Run Options

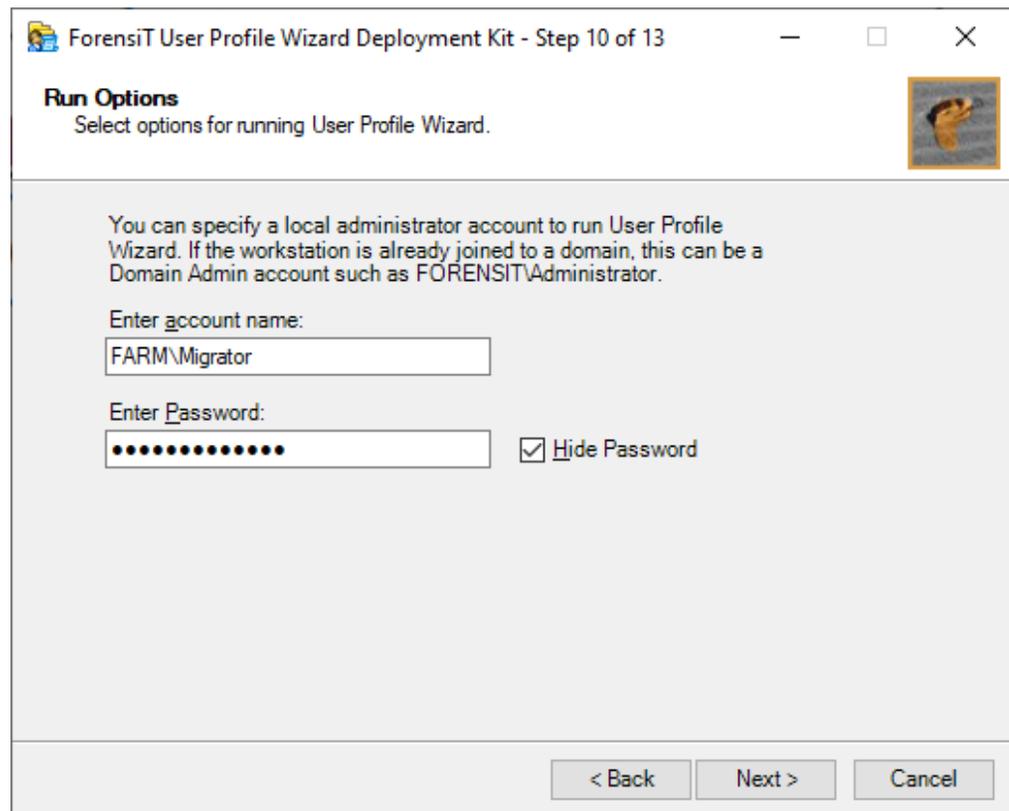


User Profile Wizard needs to be run with Administrator credentials on the workstation that is being migrated. If you are migrating a workstation remotely, User Profile Wizard will need to connect to the machine using Administrator credentials for the remote machine.

The credentials must be an account with local admin rights on the computer that you are migrating, the account can be either a local account or a Domain account.

If the account is a local account, specify only the account name, no ‘\.’ is required.

Enter the Administrator credentials here.

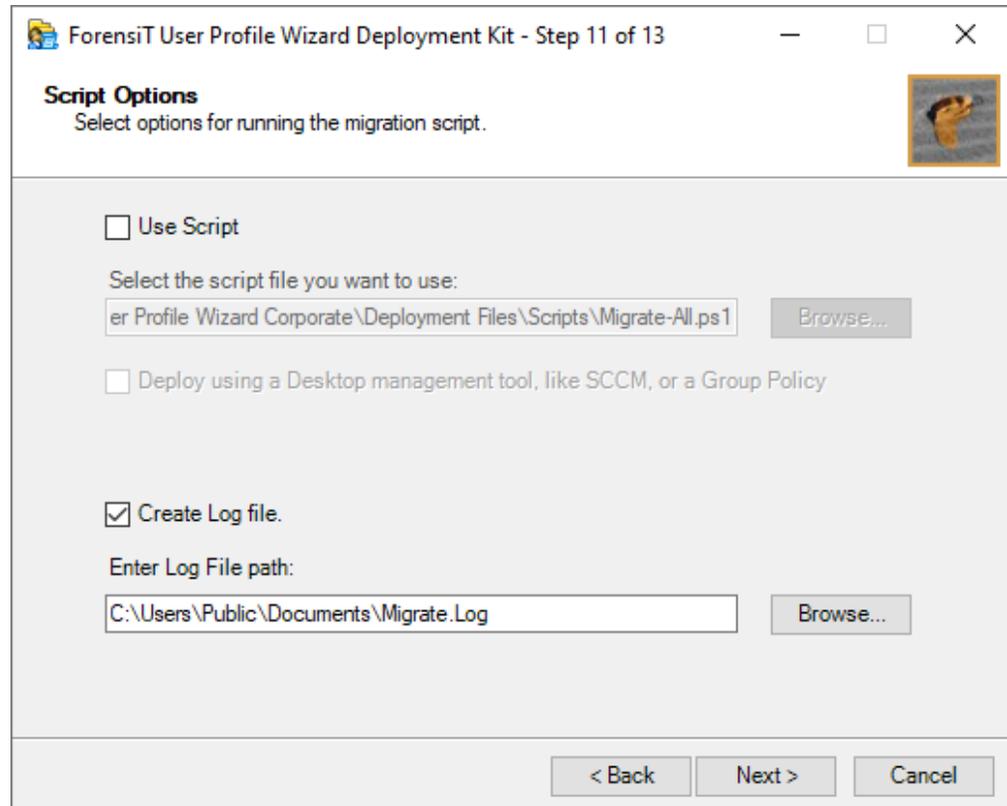


Click **Next** to continue.

Step 11 – Script Options



Step 11 is where you specify your scripting options to automate the migration process. We will return to here in the “[Automating Enterprise Migrations](#)” chapter in this guide. For now we will just uncheck the “Use Script” box.



ForensiT User Profile Wizard Deployment Kit - Step 11 of 13

Script Options
Select options for running the migration script.

Use Script

Select the script file you want to use:
er Profile Wizard Corporate\Deployment Files\Scripts\Migrate-All.ps1

Deploy using a Desktop management tool, like SCCM, or a Group Policy

Create Log file.

Enter Log File path:
C:\Users\Public\Documents\Migrate.Log

Enter the log file path

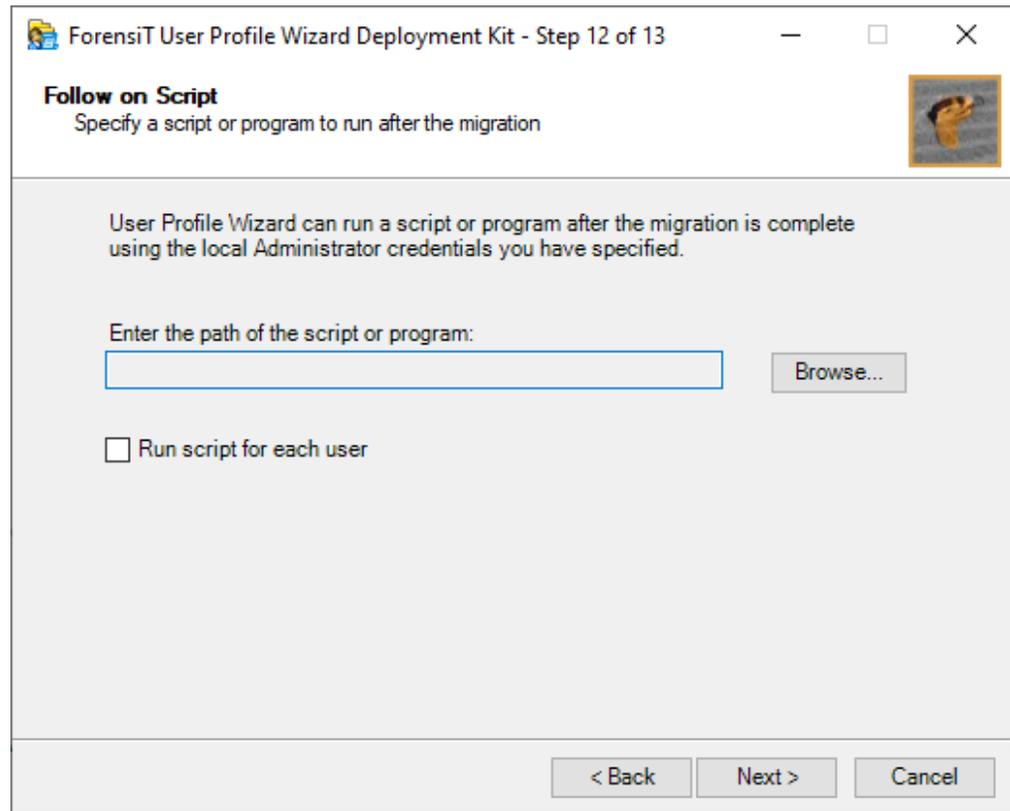
User Profile Wizard will save a migration log file to the location you specify. The default is C:\Users\Public\Documents\Migrate.log. Take note of the log file path! If you ever need to contact ForensiT Support, we will always ask you for the log file.

Click **Next** to continue.

Step 12 – Follow on Script



User Profile Wizard has the ability to run any Windows Script or executable in the security context of the local administrator account you specify in step 10.



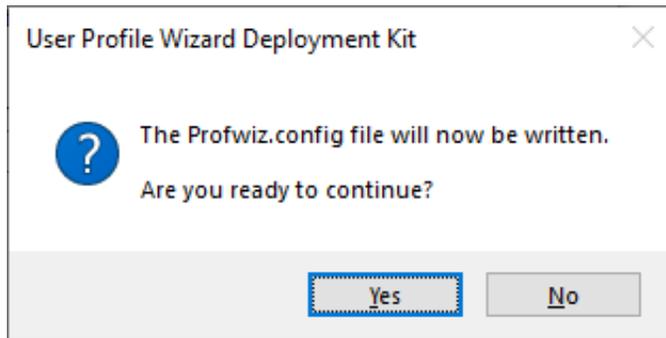
Step 12 lets you specify the additional “Follow on” code you want to run. Again, we will return to this in [“Automating Enterprise Migrations”](#) later in this guide

Click **Next** to continue.

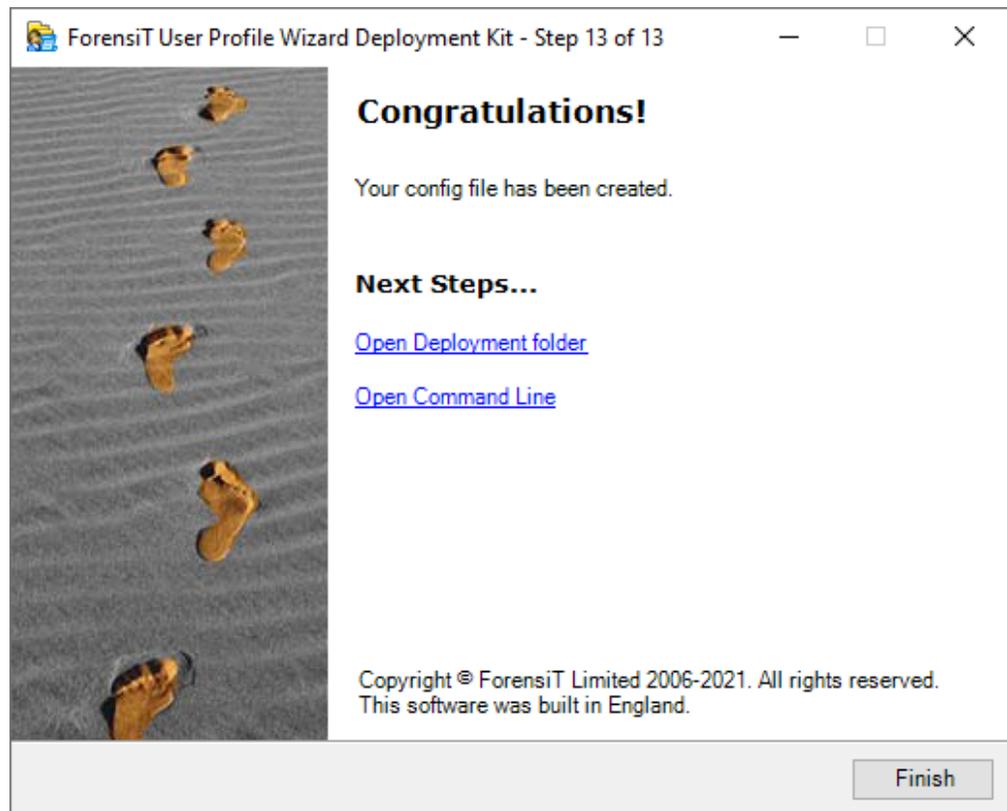
Congratulations



That's it! When you click Next at Step 10, the Deployment Kit tells you it is ready to write the configuration file.



Click **Yes**.





What did we just do?

By running the Deployment Kit, we have committed the information and settings needed to migrate workstations and profiles to the Profwiz.config file. If you open up the Profwiz.config file it looks like this:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ForensiTUserProfileWizard xmlns="http://www.ForensiT.com/schemas">
  <Parameters>
    <!-- ForensiT User Profile Wizard run options -->
    <!-- Note: options set here are overridden by parameters passed on
the command line -->

    <!-- Domain -->
    <Domain>HOMESTEAD</Domain>
    <AdsPath>OU=Workstations,DC=homestead,DC=local</AdsPath>

    <!-- Azure AD -->
    <Azure></Azure>
    <AzureObjectIDFile></AzureObjectIDFile>
    <ProvisioningPackage></ProvisioningPackage>
    <GCC></GCC>

    <!-- Options -->
    <ForceJoin>False</ForceJoin>
    <NoJoin>False</NoJoin>
    <NoDefault>False</NoDefault>
    <Delete></Delete>
    <Disable></Disable>
    <UnJoin>False</UnJoin>
    <Workgroup></Workgroup>
    <ForceRoamingOption></ForceRoamingOption>

    <!-- Credentials -->
    <DomainAdmin>HOMESTEAD\Migrator</DomainAdmin>
    <DomainPwd>E05D7D768B3070C43E2CC49206D0A60B</DomainPwd>
    <LocalAdmin>FARM\Migrator</LocalAdmin>
    <LocalPwd>C64F7B1C7BC43F02E13901DF447A8F89</LocalPwd>
    <SetsIDHistory>False</SetsIDHistory>
    <OldDomainAdmin></OldDomainAdmin>
    <OldDomainPwd></OldDomainPwd>
    <Key>i$3C+3YzM</Key>

    <!-- Corporate Edition Settings -->
    <Silent>False</Silent>
    <NoMigrate>False</NoMigrate>
    <NoReboot>False</NoReboot>
    <RemoveAdmins>False</RemoveAdmins>
    <MachineLookupFile></MachineLookupFile>
    <Log>C:\Users\Public\Documents\Migrate.Log</Log>

    <!-- Script Settings -->
    <RunAs></RunAs>
```

```

<Hash></Hash>
<RunScriptPerUser>False</RunScriptPerUser>
<RunAsSystem></RunAsSystem>

<!-- Settings for migrating all profiles -->
<All>False</All>
<OldDomain>FARM</OldDomain>
<UserLookupFile></UserLookupFile>
<Exclude>ASPNET,Administrator,defaultuser0</Exclude>

<!-- Advanced Settings -->
<Persist>False</Persist>
<NoGUI>False</NoGUI>
<SkipOnExistingProfile>False</SkipOnExistingProfile>
<SkipOnDisabledAccount>False</SkipOnDisabledAccount>
<SkipOnNoUserLookup>False</SkipOnNoUserLookup>
<FailOnMachineNameNotFound>False</FailOnMachineNameNotFound>
<UseExistingComputerAccount>False</UseExistingComputerAccount>
<ServicePath></ServicePath>
<RenameProfileFolder>True</RenameProfileFolder>
<ProtocolPriority></ProtocolPriority>
<DC></DC>
<CopyProfile>False</CopyProfile>
<DeepScan>1</DeepScan>

<!-- Outlook Settings -->
<ZeroConfigExchange>False</ZeroConfigExchange>

<!-- VPN Settings -->
<VPN>False</VPN>
<DefaultUserPwd></DefaultUserPwd>
</Parameters>

```

We will go through each of the config file elements later, but hopefully you can recognize the information we've entered: the `<Domain>` element holds the name of the new domain entered at Step 3; the `<AdsPath>` element specifies the Active Directory container where the workstation object will be created, this was selected in Step 5; the `<DomainAdmin>` and `<DomainPwd>` elements hold the new domain credentials – with the password now encrypted – that were entered at Step 4, and so on.

Now that we have saved the settings, it is time to run User Profile Wizard.

Migrating User Profiles with User Profile Wizard

This chapter will show you how to use the Wizard to interactively migrate an existing user profile so that it can be used by a user's new domain account



In this chapter we will run User Profile Wizard interactively in GUI mode using the settings in the Profwiz.config file we created in the previous chapter. Skipped the previous chapter and came straight here? No problem – you will just have to enter the settings as you go.

Migrating a workstation using the User Profile Wizard GUI is *deliberately easy*. You can do it in a few clicks.



Welcome

When you start User Profile Wizard the first thing you see is the Welcome page.

Click **Next** to continue.

Select Computer

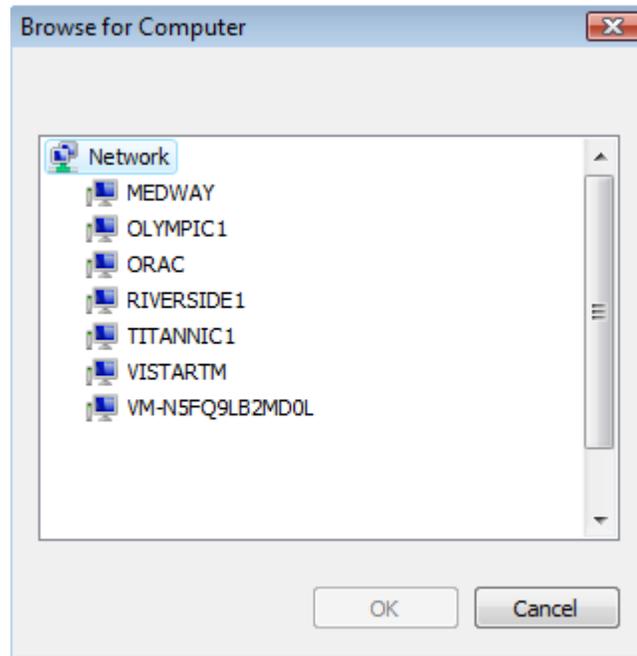


The first option you have is to choose the workstation you want to migrate. This can be the Local Computer – the computer User Profile Wizard is running on, or another computer on the network.

The screenshot shows a dialog box titled "User Profile Wizard" with a close button (X) in the top right corner. The main heading is "Select Computer" with a sub-instruction: "Select the computer where you want to migrate a user profile." There is a small eye icon in the top right of the dialog. Two radio buttons are present: "Local Computer (the computer this wizard is running on)" which is unselected, and "Another Computer:" which is selected. To the right of "Another Computer:" is a text input field containing "DESKTOP-6E0VUDV" and a "Browse..." button. At the bottom of the dialog are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

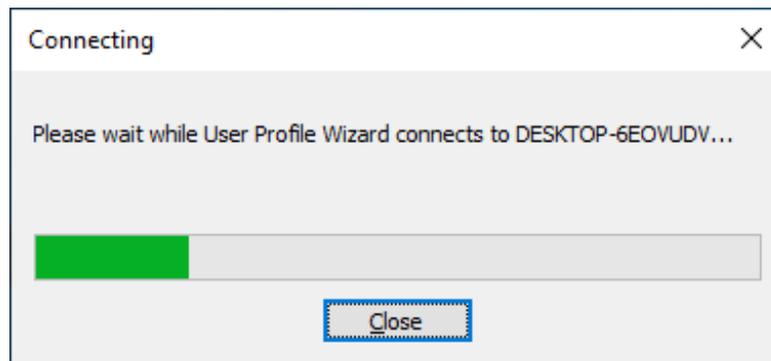
You can enter the name of a computer directly in the edit box, or you can click **Browse...** to find a machine on the network.

MIGRATING USER PROFILES



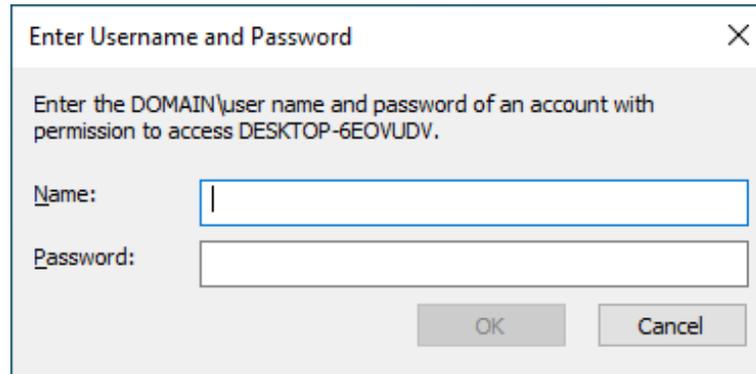
Click **Next** to continue.

User Profile Wizard will now attempt to connect to the workstation.



If you have saved Administrator credentials for the workstation in the Profwiz.config file, User Profile Wizard will use the credentials to connect to the workstation. If you haven't done this, or if the credentials in the Profwiz.config file are invalid, you will be prompted:

MIGRATING USER PROFILES



Enter Username and Password

Enter the DOMAIN\user name and password of an account with permission to access DESKTOP-6EOVUDV.

Name:

Password:

OK Cancel

Troubleshooting: If you encounter an Access Denied message or cannot connect, please check the following;

User Profile Wizard only uses standard Microsoft File and Printer sharing. File and Printer Sharing must be enabled and the machines must be discoverable. To troubleshoot, try typing `\\Computername` from Start/Run from another machine and see if it will connect. This is normally all you need.

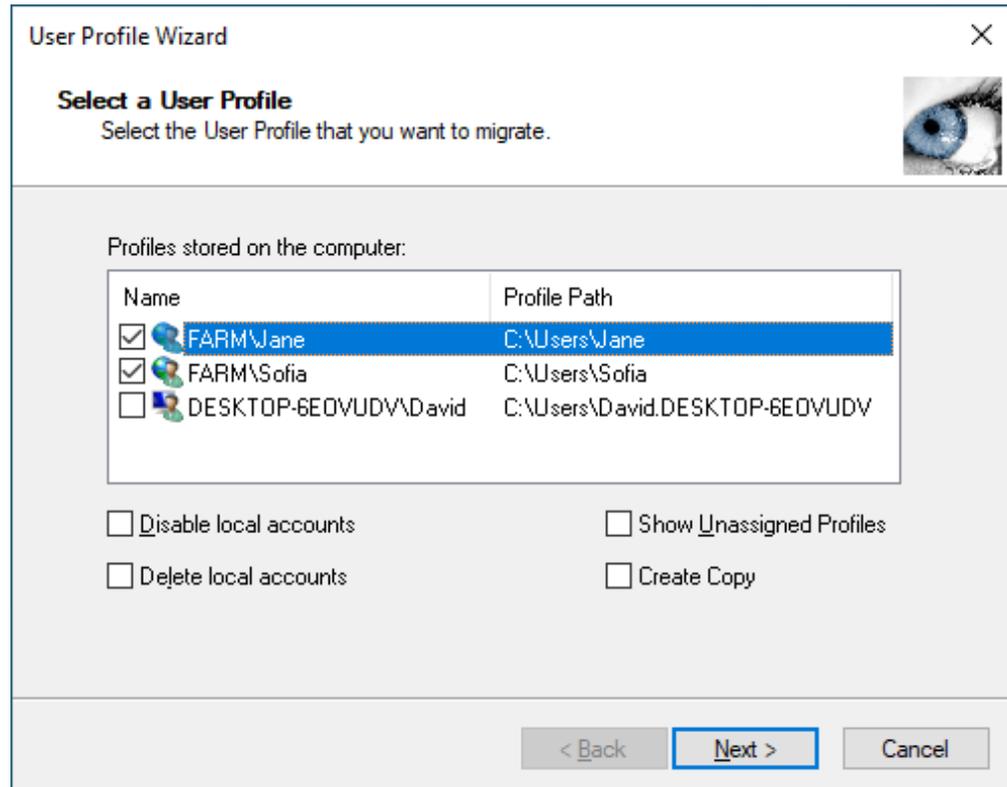
By default, Windows 7 (and later) prevents **local accounts** from accessing administrative shares through the network – this is a common reason for “Access Denied”. To enable administrative shares you have to make a registry change. Run Regedit and add the following registry value:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Policies\System
Name: LocalAccountTokenFilterPolicy
Data Type: REG_DWORD (32-bit)
Value: 1



Select a User Profile

The next step is to select the existing profiles that the new user accounts will use.



User Profile Wizard lists the profiles assigned to each user account. You just need to select the account names of the users whose profiles you want to migrate. If you have the Corporate or Professional Edition you can select multiple accounts.

Disable Local Accounts

If a profile you have selected is currently assigned to a local account, you can tell the wizard to disable the account after the migration is completed by checking the “Disable Account” checkbox.

Delete Local Accounts

If a profile you have selected is currently assigned to a local account, you can tell the wizard to delete the account after the migration is completed by checking the “Delete Account” checkbox.

Unassigned Profiles

User Profile Wizard lists the currently assigned profile: that is, the profile that each user is currently using. Note that this is not necessarily the user's original profile.

For example, say that Jane leaves your organization and Alice takes over her position. It is decided that it makes sense to run User Profile Wizard to assign Jane's profile to Alice. Alice, however, has already logged onto Jane's machine and already has a profile.

What happens to Alice's profile? The answer is nothing. The profile stays on the machine, but it is not used by anyone, it is "unassigned." To list these unassigned profiles, tick the "Show Unassigned Profiles" box. The first time you do this, you will get a warning. This is because profiles sometimes become corrupted so that Windows cannot read them. When this happens Windows creates a new profile for a user. If you look in the profiles directory, usually "C:\Users", you will sometimes see profile folders with names like USER.DOMAIN. These are profiles Windows has created because it cannot read the user's original profile. It is obviously not a good idea to use a corrupted profile, and the User Profile Wizard warns you of the possibility.

The User Profile Wizard lists unassigned profiles with the unknown user icon. It will also list the profiles for user accounts that have been deleted from the machine. In this case, the actual user name is not available and you will only see the user account SID (Security Identifier.)

The User Profile Wizard will always try to resolve the domain and account associated with a particular profile. However, this is not always possible - for example, if a domain is no longer available on the network. In these circumstances you should be able to work out the profile you want to migrate by looking at the profile path.

Create Copy

By default, User Profile Wizard does not move, copy or delete any data. Instead it configures the existing profile "in place" so that it can be used by the user's new account. This makes the migration process both very fast and very safe. By contrast, "Create Copy" will create a copy of the original profile and assign the copy to the user's new account.

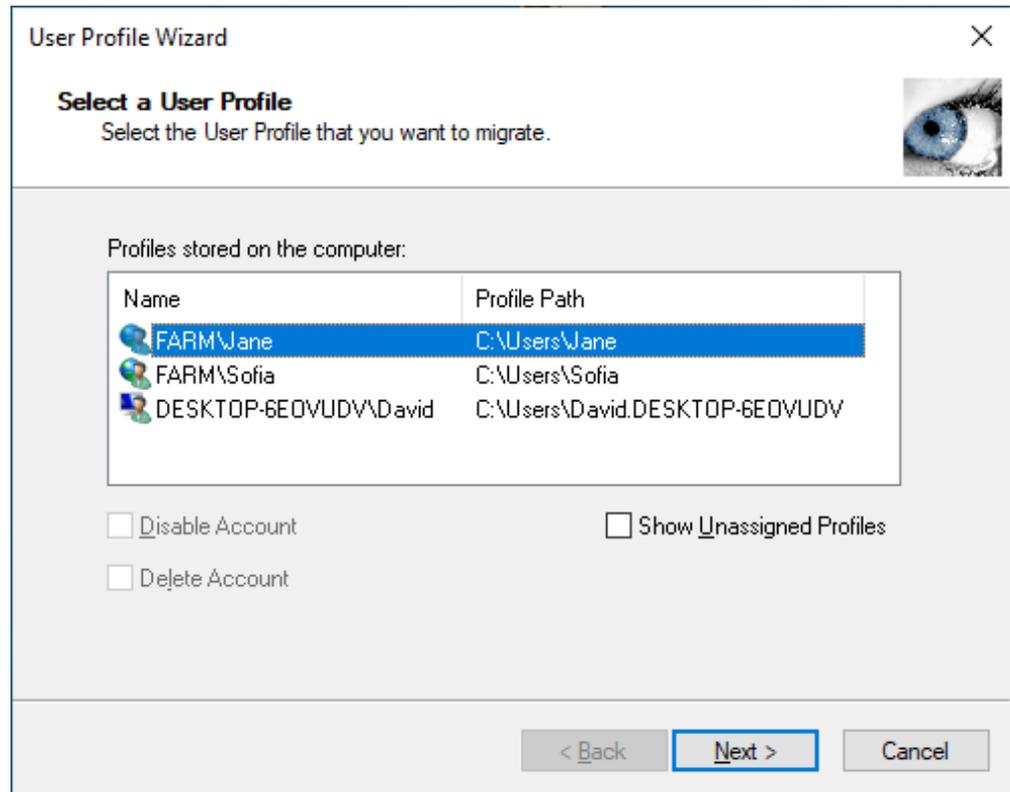
You should think carefully before choosing to copy a profile. Copying a profile will significantly slow the migration process, and will obviously take up disk space.

Copying a profile is not an option in the Personal Edition.

When you're ready, click **Next** to continue

Select a User Profile (Personal Edition)

The Personal Edition only allows you to select one profile to migrate at a time.





User Account Information

This is the page where you enter information about the new user who will be given access to an existing profile.

The screenshot shows a dialog box titled "User Profile Wizard" with a close button (X) in the top right corner. The main title is "User Account Information" and the instruction is "Specify the domain and account name for the user you would like to use the profile." There is a small eye icon in the top right of the dialog. The form contains the following fields and options:

- Label: "Enter the domain, or select the local computer name:"
- Text box: "HOMESTEAD" with a dropdown arrow.
- Checkbox: "Azure AD" (unchecked).
- Checkbox: "Join Domain" (checked).
- Checkbox: "Join Workgroup" (checked).
- Label: "Enter the account name:"
- Text box: "JSmith"
- Checkbox: "Set as default logon" (checked).

At the bottom right, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

Enter the domain

Enter the name of the domain, or Azure AD tenant, of the user account that will be given access to the existing profile.

If there is a `<Domain>` setting in the Profwiz.config file, the domain name will appear in the "Enter the domain" combo box. If your machine is already joined to a domain, that domain name will also appear in the combo box.

If the "Enter the domain" box is blank, and you are joining your machine to a new domain, type the new domain name.

You can also choose the local machine name by clicking on the down arrow. This will allow you to migrate a profile to a local user account if you want to.

MIGRATING USER PROFILES

Azure AD

Tick the Azure AD box if the domain you are joining is an Azure AD tenant.

If `<Azure>` is set to `True` in your `Profwiz.config` file, this box will already be ticked.

Join Domain

If your machine is not already joined to a domain, or if you enter a new domain name, the "Join Domain" check box is checked by default. Remove the tick if you do **not** want the machine to be joined to the domain or the Azure AD tenant you have specified.

If the machine is already joined to the domain, the "Join Domain" check box is filled in. To force user Profile Wizard to join the machine to the domain again, click the check box to enter a tick. For example, if you are migrating to a new domain that is the same name as the old domain, you should tick the "Join Domain" box to force the Wizard to join the computer to the new domain.

Join Workgroup

If you want to unjoin your machine from a domain and add the machine to a workgroup instead, tick the "Join Workgroup" check box. The "Join Workgroup" check box will only be enabled if you have selected the local computer name in the "Enter the domain" box, and the machine is already joined to a domain. See the [Migrating from domain to local accounts](#) chapter later in this guide for more information.

Enter the account name

The "Enter the account name" text box will be different depending on whether you are migrating more than one user account profile and whether you have specified a user lookup file (see [Rename user accounts](#) below).

If you have only selected one profile to migrate, and have not specified a user lookup file, the "Enter the account name" text box will be blank and you will need to enter the user's new account name. This can be a plain Windows account name like "JSmith" or an account name in UPN (User Principle Name) format, for example, `jsmith@auron.net`.

If you have selected more than one profile to migrate, and have not specified a user lookup file, the "Enter the account name" text box will be greyed out and read "Using matching account names":

MIGRATING USER PROFILES



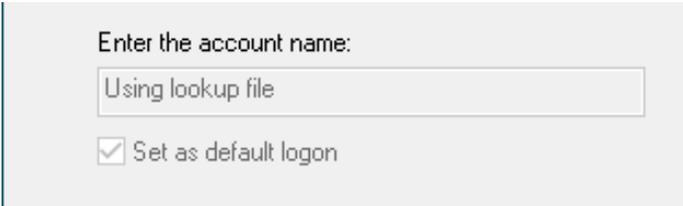
Enter the account name:

Using matching account names

Set as default logon

This means that User Profile Wizard will look for an account in the new domain that matches the name of the old user account. So if the user's account name is currently "Jane", User Profile Wizard will look for an account called "Jane" in the new domain. If the account cannot be found in the new domain, the profile will not be migrated.

If you have selected more than one profile to migrate, and *have* specified a user lookup file, the "Enter the account name" text box will be greyed out and read "Using lookup file":



Enter the account name:

Using lookup file

Set as default logon

This means that User Profile Wizard will search the user lookup file for the user's existing account name to try and find a new account name for the user. If it finds a match, the new account name will be used. If the user's account name is not found, User Profile Wizard will look for an account in the new domain that matches the user's existing account name.

Finally, if you have selected a single profile to migrate and have specified a user lookup file, if User Profile Wizard finds a match for the user's existing account name, the new user account name will appear in the "Enter the account name" text box.

Default Logon

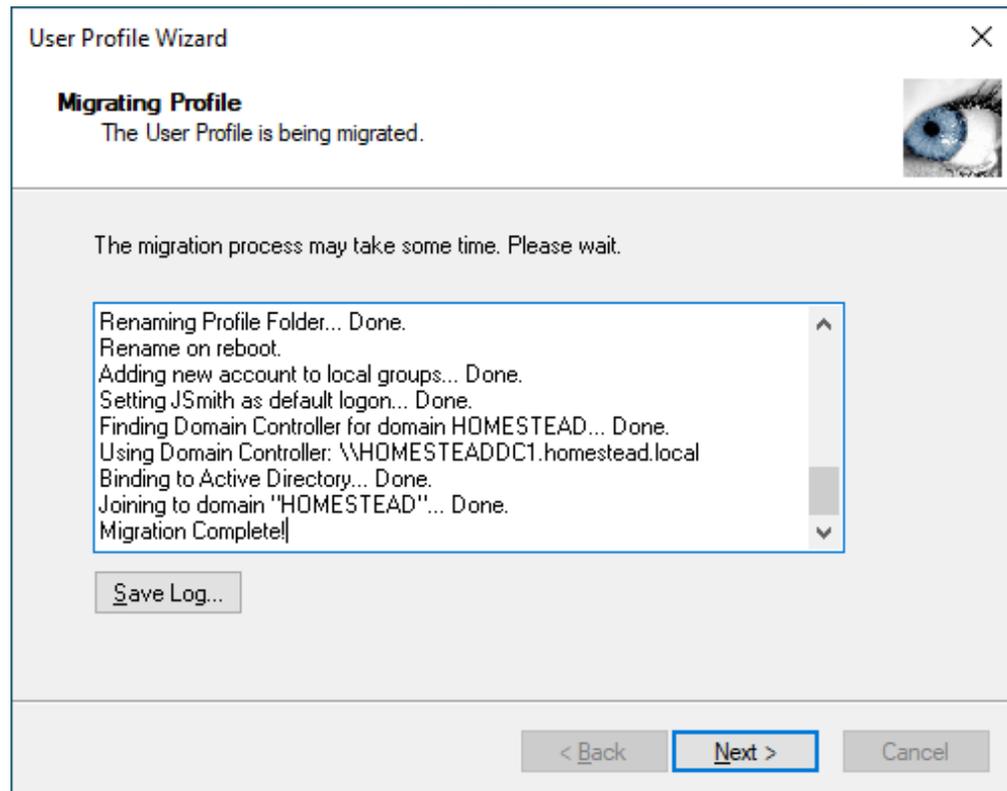
By default, the Wizard will set the account you specify to be the default logon on the machine. Remove the tick in the "Set as default logon" text box if you do not want the default logon to change.

Click **Next** to continue.



Migrating Profile

As soon as you click Next, the configuration process begins. User Profile Wizard will update the progress window at each stage.



If you are joining your machine to the domain – and you haven’t saved domain credentials to the Profwiz.config file - you will be prompted for a username and password with the necessary permissions.

Save Log...

When the migration is complete, the “Save Log...” button will become active, allowing you to save the output in the progress window. This is useful if there has been an error which you need to investigate. Should you ever need to contact ForensiT Support, we will almost always ask you for a migration log.

When configuration is complete click **Next**.



Congratulations!

You're done. If there were any problems, you can click **Back** and check the progress window for errors. Click **Finish** to close the Wizard.

The machine will now reboot.

You're about to be signed out

Your system settings have changed and the computer needs to restart. Your computer will restart in 10 seconds.

Close

Automating Enterprise Migrations

In this chapter we discuss automating enterprise migrations using scripting, and more advanced options for migrating workstations and profiles

Introduction



In the previous chapter we saw how easy it was to migrate a workstation using User Profile Wizard in GUI mode. However, if you need to migrate a large number of machines – hundreds, thousands, or tens of thousands – it is not practical to run the Wizard manually to migrate every workstation.

User Profile Wizard has been designed from the ground up to automate workstation migrations. In this chapter we see how easily this can be done. We will also return to the some of the more advanced settings we didn't cover in the “Getting Started” chapter:

- Migrate all workstation profiles
- Map user accounts to new domain account names
- Rename workstations
- Migrate over a Client VPN
- Securely run additional code

To migrate the workstations, we will use a migration script, generated by the Deployment Kit, that will be called when the user logs on with their existing user account. The scenario here is that after the user logs on to the existing domain, the migration script will call User Profile Wizard which will migrate all the user profiles on the machine and join it to the new domain. The machine will then reboot, and the user will logon to the new domain with their new domain account.

Return of the Deployment Kit



The first thing we will do is modify the Profwiz.config file that we created in the “Getting Started” chapter earlier. To do this we will run the User Profile Wizard Deployment Kit again. We could just edit Profwiz.config manually, but this is easier. Additionally, this time we will create a migration script.

By default, the Deployment Kit picks up the last Profwiz.config file you configured, so we just need to choose “Edit an existing migration project” and click **next**.

The Deployment Kit reads the settings we have already configured so we just need to click next at Step 3 and Step 4.

Rename workstations

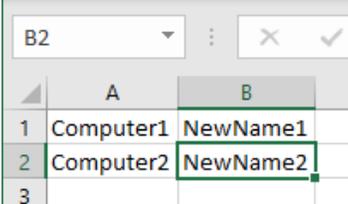
User Profile Wizard can rename workstations when they are joined to a domain. To do this the Wizard needs to be able to map the old computer name to the new computer name. It does this by looking up the old computer name in a “look-up” file.

A look-up file is just a plain comma-separated text file. Computer names are listed in a look-up file as follows:

Computer1,NewName1

Computer2,NewName2

Note If you are using Excel to create a .csv file, put the old name and new name in different columns:



The screenshot shows an Excel spreadsheet with two columns, A and B, and three rows. The first row contains 'Computer1' in column A and 'NewName1' in column B. The second row contains 'Computer2' in column A and 'NewName2' in column B. The third row is empty. The spreadsheet is displayed in a window with a formula bar at the top showing 'B2'.

	A	B
1	Computer1	NewName1
2	Computer2	NewName2
3		

Save as “CSV (Comma delimited)(*.csv)”

If you have used Excel to create the csv, please check the file in a text editor such as Notepad to ensure that Excel has not added any additional formatting such as speech marks or used a semi colon as a delimiter instead of a comma.

We can specify the look-up file at Step 5 when running the Deployment Kit.



The location of the lookup file is relative to the machine where User Profile Wizard is running. So, if you were migrating a remote machine the lookup file could be on your hard drive.

In our example, however, we want to be able to run User Profile Wizard from a script. In this case we need to put the look-up file in a location where everyone has access, so we are putting in on a network share on the *old* domain.

Note Generally, you should always use a UNC path to specify a network share, not a mapped drive like P:\Share. The reason for this is that if User Profile Wizard is running using Administrator credentials, the drive will not be mapped for the Administrator user account.

Maintaining SID History

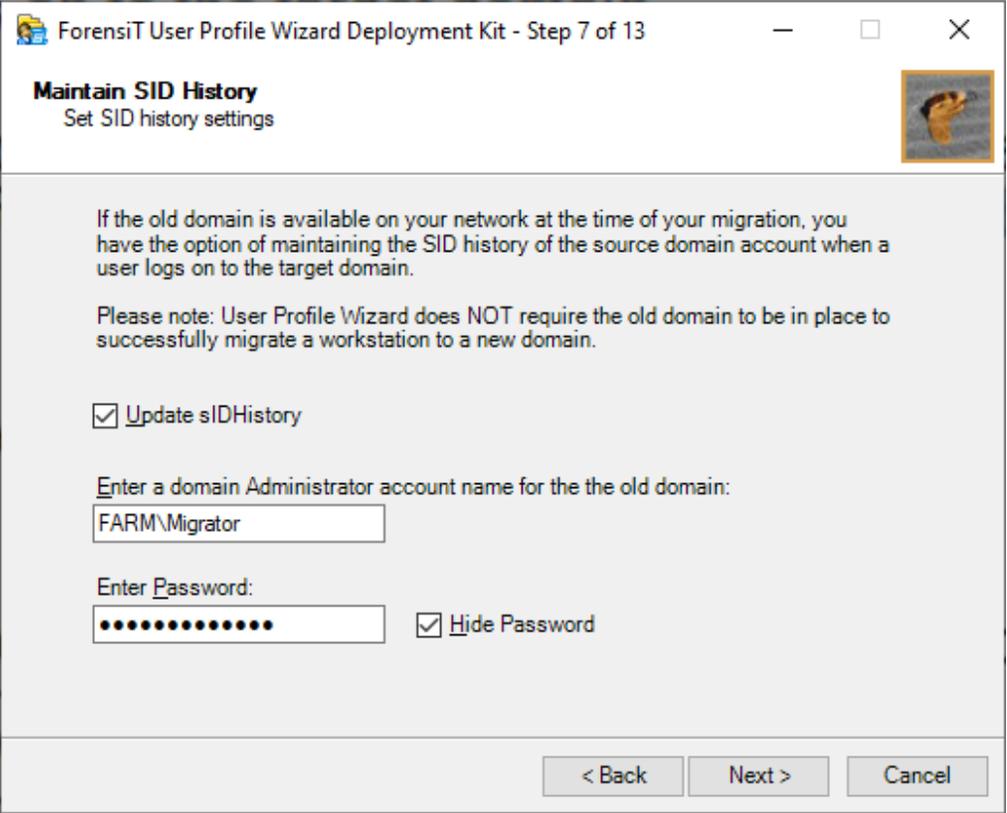
Maintaining the SID history of a user's old domain account when they logon to the new domain is a powerful mechanism for granting the new domain user account access to the network and local resources enjoyed by the old domain account.

Setting the SID history is a security sensitive operation. To set the SID history, data must be exchanged between Domain Controllers on the old (source) domain and new (target) domain. It follows that both domains need to be available when the migration takes place. You must also provide domain Administrator credentials for *both* domains.

It is very important to stress here that Maintaining SID history is **OPTIONAL**.

User Profile Wizard does NOT need to set the SID history in order to migrate a user to a new domain.

User Profile Wizard does NOT need the old domain to be in place.



The screenshot shows a Windows dialog box titled "ForensiT User Profile Wizard Deployment Kit - Step 7 of 13". The main heading is "Maintain SID History" with the subtitle "Set SID history settings". The dialog contains the following text and controls:

If the old domain is available on your network at the time of your migration, you have the option of maintaining the SID history of the source domain account when a user logs on to the target domain.

Please note: User Profile Wizard does NOT require the old domain to be in place to successfully migrate a workstation to a new domain.

Update sIDHistory

Enter a domain Administrator account name for the the old domain:

Enter Password:
 Hide Password

At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

AUTOMATING ENTERPRISE MIGRATIONS

To have User Profile Wizard update the SID history of the new domain account, tick **Update SIDHistory** box and enter the credentials of a domain administrator for the old (source) domain.

Additional configuration of both the old and new domains will be required. See [Configuring domains to maintain SID history](#) in the “Troubleshooting” section below.

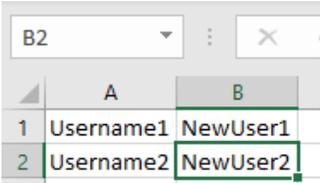
Rename user accounts

It may be the case that when you migrate to your new domain, your users will have new account names. In exactly the same way that User Profile Wizard can map old workstation names to new workstations names, it can map old user account names to new user account names.

A look-up file is just a plain comma-separated text file. User names are listed in a look-up file as follows; oldaccountname,newaccountname

```
Username1,NewUser1
Username2,NewUser2
```

Note If you are using Excel to create a .csv file, put the old name and new name in different columns.



	A	B
1	Username1	NewUser1
2	Username2	NewUser2

Save as “CSV (Comma delimited)(*.csv)”.

If you have used Excel to create the csv, please check the file in a text editor such as Notepad to ensure that Excel has not added any additional formatting such as speech marks or used a semi colon as a delimiter instead of a comma.

If you are migrating from an existing Azure AD tenant, you can use the UPN, so if you are migrating to a new tenant from an existing tenant, the user names can be listed in a look-up file as follows:

```
username1@oldtenant.onmicrosoft.com,newuser1@newtenant.onmicrosoft.com
```

Similarly, if you are migrating from an Azure AD tenant back to an on-premises domain, the lookup file might look like this:

```
username1@oldtenant.onmicrosoft.com,newuser1
```

*Do **not** use a UPN if you are migrating from an on-premises domain.*

We enter the path to the user account look-up file in Step 8 of the Deployment Kit.



ForensiT User Profile Wizard Deployment Kit - Step 8 of 13

User Account Options
Choose user account migration options

Use lookup file to get new account names.

Enter lookup file path:

Skip migration if user is not found in lookup file

Rename Profile Folder

Enable ZeroConfigExchange only if you are changing your Email configuration.

Enable ZeroConfigExchange

< Back Next > Cancel

Rename Profile Folder

By default, the name of a user's profile folder will be their account name. For example, Jane's profile will typically be C:\Users\Jane. If Jane's account name changes when her workstation is migrated to a new domain, it may be useful – perhaps for support purposes - to change the name of her profile folder to her new user account name. For example, her profile folder could be renamed C:\Users\JSmith.

User Profile Wizard can rename the profile folder for us when the profile is migrated. To set this option using the Deployment Kit we just need to check the **Rename Profile Folder** check box at Step 8.

Some care should be taken when choosing to rename profile folders. Some legacy applications save the path to the profile and may no longer work if the profile folder name is changed. You should always test renaming profiles in your environment before migrating your user's machines with this option.

Skip migration if user is not found in lookup file

By default, User Profile Wizard will always try and migrate a profile to a new user account. So if it finds an old domain account profile for Jane, it will search in the lookup file for Jane's new domain account name. If it finds one, it will use that. If it doesn't find one, it will still try and migrate the profile, but using the original account name: so in this example, it will look for a "Jane" account in the new domain, and migrate the profile to that account if it finds it.

There are times when you may not want this to happen. Ticking the "Skip migration if user is not found in lookup file" does exactly what it says.

Enable ZeroConfigExchange

By setting this option, User Profile Wizard will write the necessary registry values to enable Microsoft's ZeroConfigExchange for automatically configuring Outlook.

You should only enable ZeroConfigExchange if you are *changing* your email configuration. By default User Profile Wizard will migrate Outlook settings unchanged.

For more information on ZeroConfigExchange please refer to the relevant Microsoft documentation.

Migrating over a Client VPN

Migrating over a Client VPN requires special handling. The problem is not so much with the migration itself, but what happens afterwards.

Most VPN connections are made by the user when they are logged on to Windows using software such as Cisco's VPN client. When a machine is migrated to a new domain it needs to reboot: however, as soon as it reboots the VPN connection is lost.

The problem is that after the machine reboots the user cannot logon again – there is no VPN connection to authenticate to the domain and Windows cannot cache the logon credentials until the user does authenticate.

To avoid this “Catch-22” situation and allow the user to logon offline, User Profile Wizard is able to cache the user's logon credentials itself during the migration.

To enable password caching, tick the “Enable offline password caching” check box.



ForensiT User Profile Wizard Deployment Kit - Step 9 of 13

VPN Settings
Select options for migrating over a VPN

Enable offline password caching

Prompt user for password

Use default password for all users.

Enter default password:

..... Hide Password

< Back Next > Cancel

To cache the user's logon credentials, User Profile Wizard needs to know a password to cache, the password does not have to be their actual new account password. There are two options for specifying the password.

Firstly, you can simply prompt the user for their new domain account password:

Keep in mind however, that if more than one user account profile is being migrated on a workstation, the logged on user will be prompted to supply a password for all the other users as well! For this reason, it is best to use this option with the `Migrate-LastLoggedOnUser.ps1` script. (Step 11.) If you are running the Wizard as SYSTEM on the computer, the User will not see the above prompt because the Wizard is running in the SYSTEM context.

Secondly, you can set a default logon password that will be used by *all* users that are migrated. To do this, choose “Use default password for all users” and enter the password. The password does not have to be their actual new account password, it is only a password to allow the user to log on with the new account for the first time before connectivity to the new DC can be established via the Client VPN.

Initializing VPN mode... Fails. Access is denied.

and

Initializing VPN mode... Fails. Invalid Handle.

The only time we ever see an issue with using VPN credential caching is if there is an Anti-Virus or security program or setting blocking the software from working correctly. Caching domain credentials is a low-level operation, and this can be flagged as suspicious by some third-party applications.

If you get an error, you will need to configure your Anti-Virus program to allow User Profile Wizard to work.

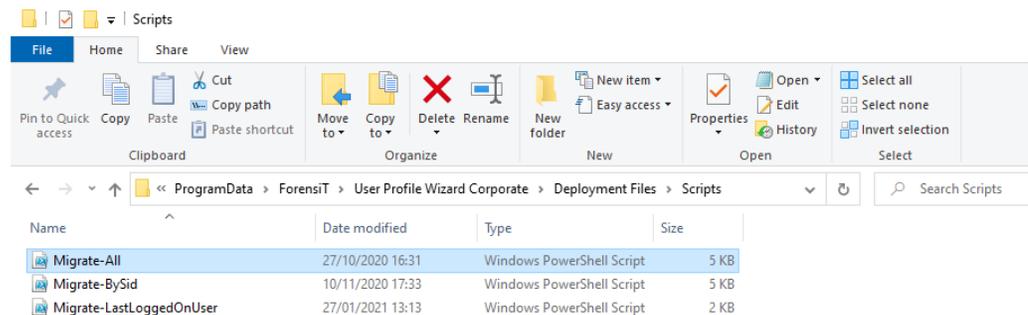
Check that [Enhanced LSA Protection](#) is not enabled by checking the **RunAsPPL** registry key is set to 0 or the key is not present. If it is set to 1 or 2, this will prevent the Wizard from caching a password.

Script Options

The script options page is where we start to automate User Profile Wizard, and begin to harness the real power of the software.



Tick **Use Script** and then select the migration script that you want to use. You can use one of the scripts that are pre-installed in the “Scripts” folder; or, you can of course use a script you have developed yourself.



[The pre-installed scripts are described below.](#)

Deploy using a Desktop management tool, like SCCM, or a Group Policy

Deploying your migration using a Desktop Management tool, or Computer Startup script Group Policy is highly recommended. In these circumstances, the migration will run in the security context of the SYSTEM account, so you do not want User Profile Wizard to use any alternative credentials, or show any prompts. Ticking **Deploy using a Desktop management tool, like SCCM, or a Group Policy** makes these necessary changes for you.

In addition, any lookup files, and any follow-on script, will be copied to your project folder for easy deployment, and the paths automatically adjusted in your Profwiz.config file

Pre-installed Scripts

Migrate-All.ps1

This is the default migration script. The script will attempt to migrate all the profiles on a workstation that match your criteria to new user accounts: so all profiles from an old domain, or all local account profiles. This is the recommended script in most circumstances.

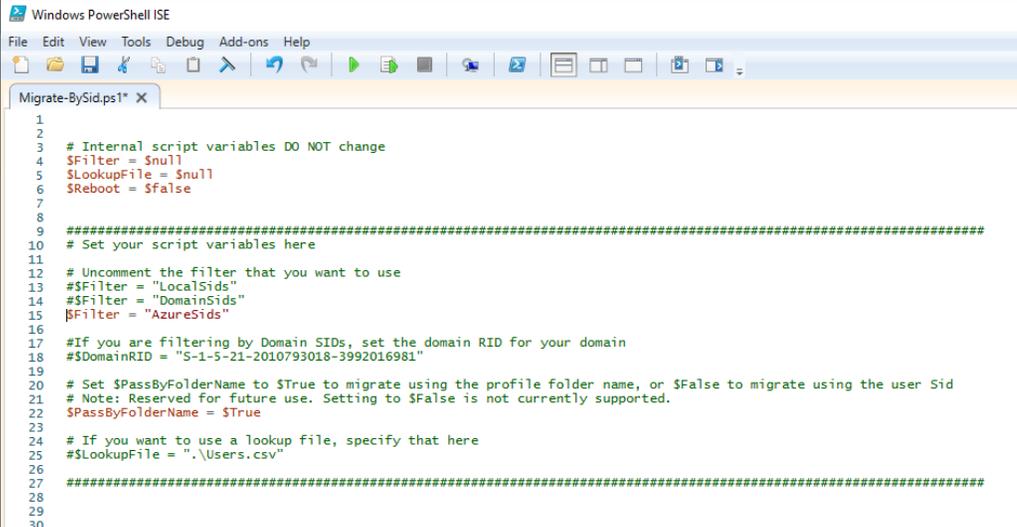
Migrate-LastLoggedOnUser.ps1

The script gets the last logged on user information from the registry, and migrates that user's profile to a new account.

Migrate-BySid.ps1

This script offers you a great deal of flexibility. Instead of just working with the profile list in the registry, which means that the user SID must be able to be resolved to a user account name, the script uses the Profwiz.exe /SOURCEPROFILE parameter to directly migrate the profile. In order to select the profiles that you want to migrate, you filter them based on the type of user SID.

Here we filter on Azure SIDs by uncommenting that filter:



```

1
2
3 # Internal script variables DO NOT change
4 $Filter = $null
5 $LookupFile = $null
6 $Reboot = $false
7
8
9 #####
10 # Set your script variables here
11
12 # Uncomment the filter that you want to use
13 # $Filter = "LocalSids"
14 # $Filter = "DomainSids"
15 $Filter = "AzureSids"
16
17 # If you are filtering by Domain SIDs, set the domain RID for your domain
18 # $DomainRID = "S-1-5-21-2010793018-3992016981"
19
20 # Set $PassByFolderName to $True to migrate using the profile folder name, or $False to migrate using the user Sid
21 # Note: Reserved for future use. Setting to $False is not currently supported.
22 $PassByFolderName = $True
23
24 # If you want to use a lookup file, specify that here
25 # $LookupFile = ".\Users.csv"
26
27 #####
28
29
30

```

Note that if you want to filter by domain SIDs, you need to enter the RID (the Relative Identifier) of the domain – which is just the first part of the user SID – so the script knows what to look for.

Running Additional Code

User Profile Wizard allows you to run a “follow-on” file – an executable file, a script or a batch file - in the security context of the local administrator account you specify for running the migration. This has proved very useful for customers who need to carry out additional tasks using administrator permissions.

To specify the code to run, you just need to select the file in Step 12.

Note this file must already exist. This is because the Deployment Kit will generate a security hash of the file. The security hash ensures that only the code you specify will run: if the code is changed in anyway, User Profile Wizard will return a “Hash Error”.



You have the option to **Run script for each user**. If you check this box, User Profile Wizard will call the script each time a user profile is successfully migrated. If you do not check this box, the script will only be called once - after the workstation has been successfully joined to the new domain.

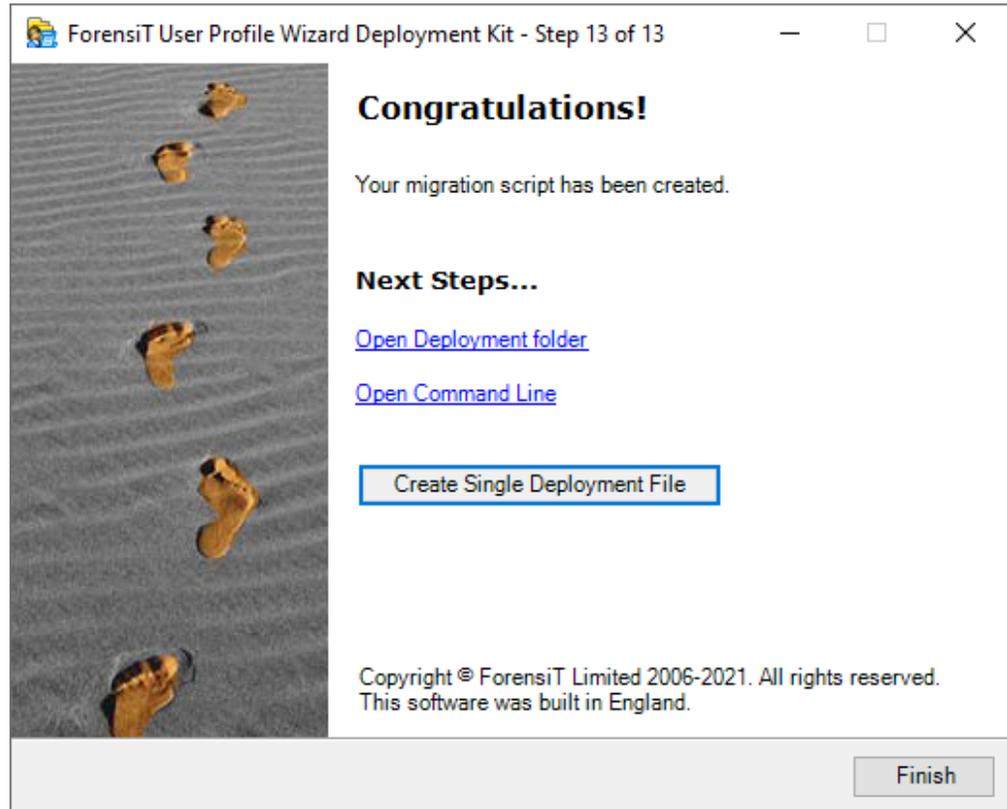
AUTOMATING ENTERPRISE MIGRATIONS

For additional information on scripting, please see [Advanced Scripting Options](#) later in this guide.

When we click **next** we are asked to confirm that we want to create the migration script.

Next Steps...

When the changes have been written to the Profwiz.config file and the script file has been created, the Deployment Kit offers us two options.



Open Deployment Folder does just that, and gives you access to your migration files.

Open Command Line opens the User Profile Wizard command Line in the project folder.

```

User Profile Wizard Command Line - Homestead
ForensiT User Profile Wizard Command Line Console
UPW:>pwd
Path
----
C:\ProgramData\ForensiT\User Profile Wizard Corporate\Deployment Files\Homestead
UPW:>
    
```

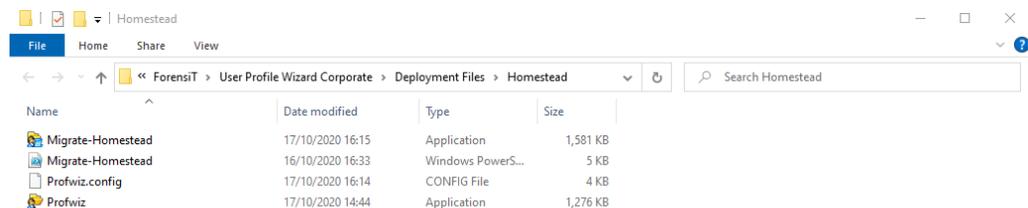
Create Single Deployment File

Deploying a single file is often easier than managing multiple files, such as lookup files and follow-on scripts. The User Profile Wizard Deployment Kit can create a single deployment file that can contain all the files needed for the migration.

When you click the **Create Single Deployment File** button, your deployment files – Profwiz.exe, Profwiz.config, the migration script, together with any lookup files, and any follow-on file - are all embedded in the single deployment file. The Deployment Kit creates a single deployment executable file with the same name as the migration script. In our example here, it is called Migrate-Homestead.exe (see below.)

The Single Deployment File (exe) is the only file that you need to distribute to and execute on the computers that you are migrating.

Because the Single Deployment File includes all the required files, if you make any changes to any of the files (config file or any lookup files for example), you will need to run through the Deployment Kit and create a new Single Deployment File (exe) so that the updated files are included in the new Single Deployment File.



If there is not an option to **Create Single Deployment File** on Step 13 of the Deployment Kit, this is because a Migration script has not been selected on Step 11.

What did we just do?

Here's the Profwiz.config file after we have made our changes

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ForensiTUserProfileWizard xmlns="http://www.ForensiT.com/schemas">
  <Parameters>
    <!-- ForensiT User Profile Wizard run options -->
    <!-- Note: options set here are overridden by parameters passed on
the command line -->

    <!-- Domain -->
    <Domain>HOMESTEAD</Domain>
    <AdsPath>OU=Workstations,DC=homestead,DC=local</AdsPath>

    <!-- Azure AD -->
    <Azure></Azure>
    <AzureObjectIDFile></AzureObjectIDFile>
    <ProvisioningPackage></ProvisioningPackage>
    <GCC></GCC>

    <!-- Options -->
    <ForceJoin>False</ForceJoin>
    <NoJoin>False</NoJoin>
    <NoDefault>False</NoDefault>
    <Delete></Delete>
    <Disable></Disable>
    <UnJoin>False</UnJoin>
    <Workgroup></Workgroup>
    <ForceRoamingOption></ForceRoamingOption>

    <!-- Credentials -->
    <DomainAdmin>HOMESTEAD\Migrator</DomainAdmin>
    <DomainPwd>E05D7D768B3070C43E2CC49206D0A60B</DomainPwd>
    <LocalAdmin>FARM\Migrator</LocalAdmin>
    <LocalPwd>0D157CC3FFDF26A28E5E6EBBF2947EACCA46701C7B1FD94E</LocalPwd>
    <SetsIDHistory>True</SetsIDHistory>
    <OldDomainAdmin>FARM\Administrator</OldDomainAdmin>

<OldDomainPwd>19D4B916174883D062305FD56480033519FCB46E1E3374E3</OldDomain
Pwd>
    <Key>i$3C+3YzM</Key>

    <!-- Corporate Edition Settings -->
    <Silent>False</Silent>
    <NoMigrate>False</NoMigrate>
    <NoReboot>False</NoReboot>
    <RemoveAdmins>False</RemoveAdmins>

<MachineLookupFile>\\FARMDC1\Migration\Computers.csv</MachineLookupFile>
    <Log>C:\Users\Public\Documents\Migrate.Log</Log>

    <!-- Script Settings -->
    <RunAs>\\FARMDC1\Migration\Follow-on.ps1</RunAs>
```

```

<Hash>CFC3A397772258F27892401B5053B792E984BBAE1714EE154F8DB3E7D1BAA373760
428FC575D7F60</Hash>
  <RunScriptPerUser>False</RunScriptPerUser>
  <RunAsSystem></RunAsSystem>

  <!-- Settings for migrating all profiles -->
  <All>True</All>
  <OldDomain>FARM</OldDomain>
  <UserLookupFile>\\FARMDC1\Migration\Users.csv</UserLookupFile>
  <Exclude>ASPNET,Administrator,defaultuser0</Exclude>

  <!-- Advanced Settings -->
  <Persist>False</Persist>
  <NoGUI>True</NoGUI>
  <SkipOnExistingProfile>False</SkipOnExistingProfile>
  <SkipOnDisabledAccount>False</SkipOnDisabledAccount>
  <SkipOnNoUserLookup>False</SkipOnNoUserLookup>
  <FailOnMachineNameNotFound>False</FailOnMachineNameNotFound>
  <UseExistingComputerAccount>False</UseExistingComputerAccount>
  <ServicePath></ServicePath>
  <RenameProfileFolder>True</RenameProfileFolder>
  <ProtocolPriority></ProtocolPriority>
  <DC></DC>
  <CopyProfile>False</CopyProfile>
  <DeepScan>1</DeepScan>

  <!-- Outlook Settings -->
  <ZeroConfigExchange>False</ZeroConfigExchange>

  <!-- VPN Settings -->
  <VPN>True</VPN>

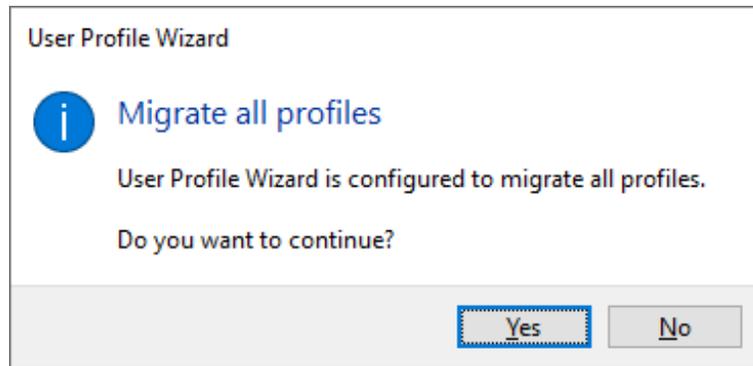
  <DefaultUserPwd>FBB504A258C10555E6A7EAE85D5B6C2FF84AD9FECFD2303D</Default
  UserPwd>
  </Parameters>

```

Perhaps the most important setting we have changed is the `<All>` element – the one that tells User Profile Wizard to migrate all profiles when migrating a workstation.

If you double-click on Profwiz.exe now, you no longer get the Wizard GUI. This is because you cannot migrate all profiles on a machine using the GUI, so setting `<All>` to **True** forces the Wizard to run in command-line (CLI) mode.

As a fail-safe to stop you accidentally migrating your Administrator machine, the Wizard will warn you if you do try and run it in GUI mode.



You will **not** see this warning if you run the Wizard from a script, or from the command line, or if you are migrating a remote machine. You will also suppress this prompt if you explicitly tell the Wizard not to run in GUI mode by setting the Profwiz.config element to 'True':

```
<NoGUI>True</NoGUI>
```

Fine Tuning



There are a couple of tweaks that we can make to the Profwiz.config file to fine-tune the migration process.

We have told User Profile Wizard to migrate all the user account profiles on the workstation. However, there may be some standard accounts that we do not want to migrate; for example, the Administrator account. To have User Profile Wizard exclude certain user accounts from the migration we just have to add the account names to the `<Exclude>` element in the Profwiz.config file. Multiple accounts are separated by commas:

```
<Exclude>ASPNET,Administrator</Exclude>
```

To edit the Profwiz.config file just open it up in Notepad.

Another useful option is `<RemoveAdmins>`. In order to minimize disruption to the end user, User Profile Wizard adds the new domain user account to any local groups that the old user account was *individually* a member of. Experience has shown us, however, that users have often been added to the local Administrators account. Joining a new domain is a good time to clean up these permissions. By setting `<RemoveAdmins>` to 'True' you can tell User Profile Wizard not to add the user's new domain account to the local Administrators group.

```
<RemoveAdmins>True</RemoveAdmins>
```

The Migration Script



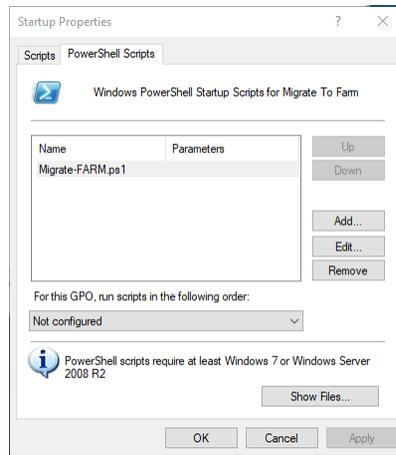
The only job of the migration script is to call User Profile Wizard to migrate a workstation. In order to do that, the script checks whether the machine has already been migrated (and quits if it has.)

Deploying the Script From a Group Policy

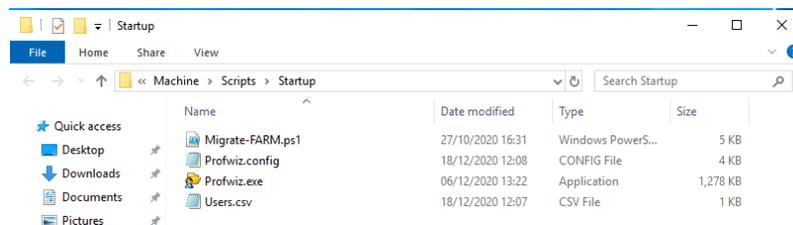


We have now configured User Profile Wizard to automatically migrate workstations to the new domain. The next step is to deploy the files.

Call your migration .ps1 script from the Computer Startup Script Group Policy “PowerShell Scripts” tab. In this example the script is called “Migrate-FARM.ps1”



Click the “Show Files...” button and copy all your Project migration files (Profwiz.exe, Profwiz.config, the migration script and lookup files) into the folder that opens.



If you chose “Deploy using a Desktop management tool, like SCCM, or a Group Policy” at Step 11, the paths on your Profwiz.config will have been automatically adjusted:

```
<UserLookupFile>Users.csv</UserLookupFile>
```

In order to deploy the Wizard via Group Policy, you must tick the ‘Deploy using a Desktop management tool, like SCCM, or a Group Policy’ on Step 11 of the Deployment Kit in order to configure the Wizard to run as SYSTEM.

Deploying a Single Deployment File from SCCM or your RMM Software.

If you have SCCM, Intune or any kind of RMM (Remote Monitoring and Management) software that can deploy and execute an exe on a computer, you can simply deploy a Single Deployment File (exe): that’s the only file you need!

RMM tools will generally execute the software as SYSTEM on the computer, if this is the case with your RMM, you must tick the ‘Deploy using a Desktop management tool, like SCCM, or a Group Policy’ on Step 11 of the Deployment Kit in order to configure the Wizard to run as SYSTEM.

Advanced Scripting Options



This section assumes you are familiar with scripting.

User Profile Wizard gives you option of running a “follow-on” script either after the migration to the domain is complete, or after each user profile is migrated.

When User Profile Wizard calls the script after a user’s profile is migrated, it passes the script two parameters: the new target user account name, and the new target user account SID. What’s more, User Profile Wizard makes the target user’s registry available under HKEY_USERS, which means that your follow-on script can directly manipulate registry values for the target user.

So, for example, if we want to write the user’s new account name to a “ScriptUpdate” string value under the SOFTWARE\ForensiT\Update key, we could do something like this:

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
UpdateUserReg.ps1 X Run Selection (F8)
1 $accountName = $args[0]
2 $userSid = $args[1]
3
4 $regUpdatepath = "Registry::HKEY_USERS\$userSid\SOFTWARE\ForensiT\Update"
5
6 if (-not (Test-Path $regUpdatepath)) {
7     New-Item -Path $regUpdatepath -Force
8 }
9
10 Set-ItemProperty -Path $regUpdatepath -Name ScriptUpdate -Value $accountName
11
12
```

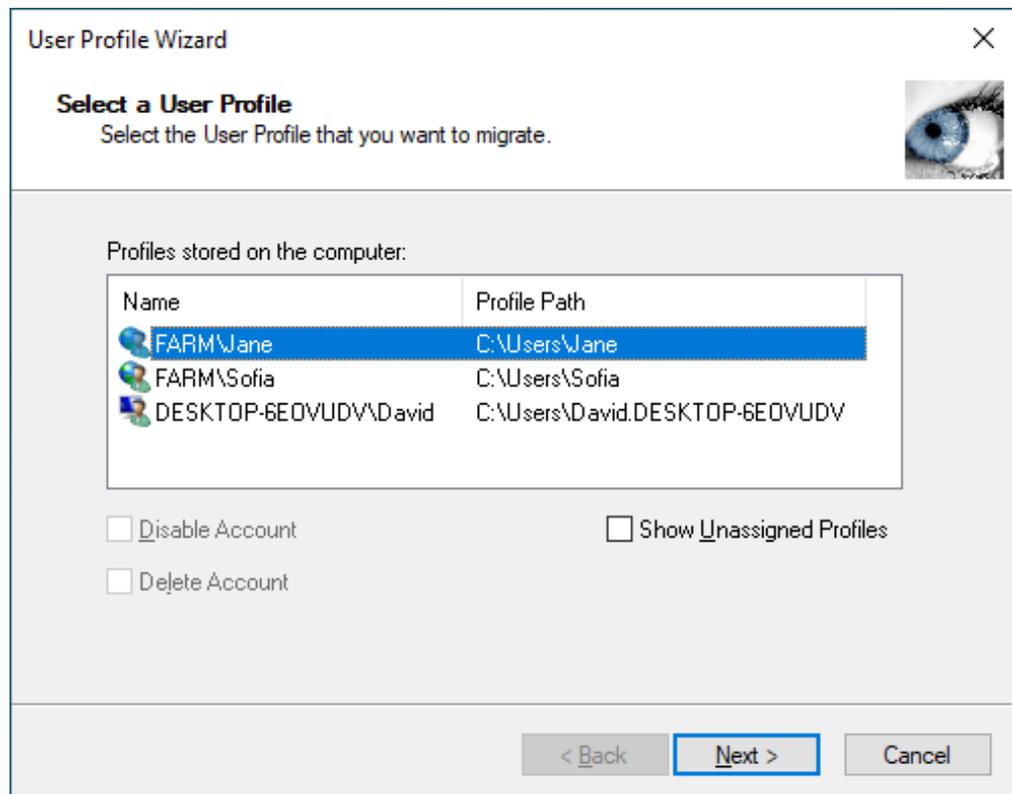
Migrating from domain to local accounts

It is just as easy to use User Profile Wizard to migrate a domain account profile to a local account.

With the growth of Office 365 and cloud-based services, more and more people are finding they no longer need to run their own domain, and want to migrate their computers back to a workgroup. User Profile Wizard makes the migration very easy.

Using the GUI

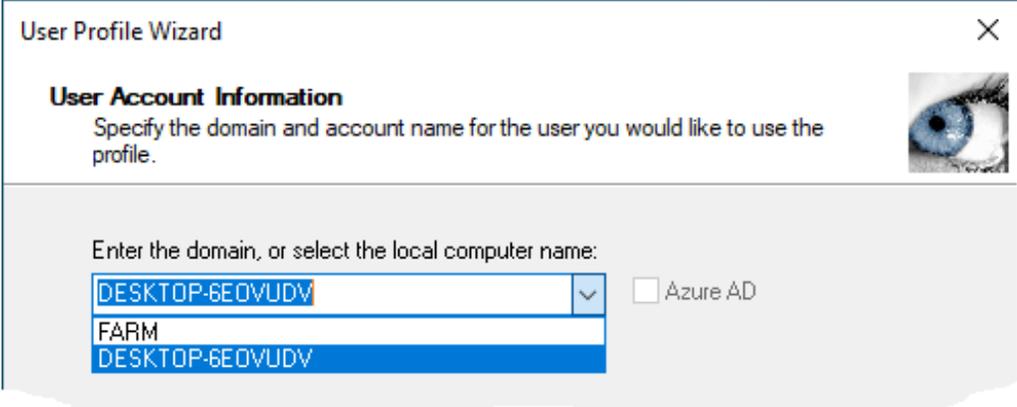
To migrate a domain account profile to a local user account, select the profile that you want to migrate on the “Select a User Profile” page.



Click **Next**.

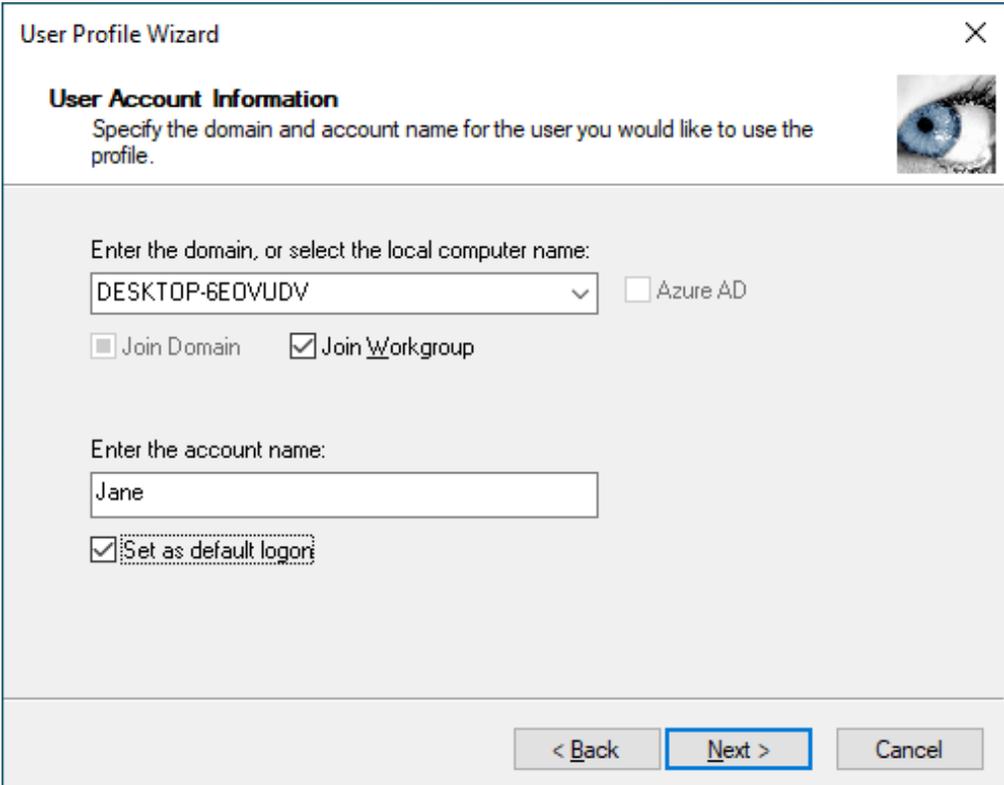
MIGRATING FROM DOMAIN TO LOCAL ACCOUNTS

On the “User Account Information” page, select the local computer name from the drop-down list



The screenshot shows the 'User Profile Wizard' window with the 'User Account Information' section. The instruction reads: 'Specify the domain and account name for the user you would like to use the profile.' Below this, there is a text prompt: 'Enter the domain, or select the local computer name:'. A dropdown menu is open, displaying three options: 'DESKTOP-6E0VUDV' (highlighted in blue), 'FARM', and 'DESKTOP-6E0VUDV'. To the right of the dropdown is an unchecked checkbox labeled 'Azure AD'.

When you have selected the local computer name, the **Join Workgroup** check box will become active. If you tick **Join Workgroup** User Profile Wizard will automatically remove the computer from the domain and join it to a workgroup.



The screenshot shows the 'User Profile Wizard' window with the 'User Account Information' section. The instruction reads: 'Specify the domain and account name for the user you would like to use the profile.' Below this, there is a text prompt: 'Enter the domain, or select the local computer name:'. A dropdown menu is open, displaying three options: 'DESKTOP-6E0VUDV' (highlighted in blue), 'FARM', and 'DESKTOP-6E0VUDV'. To the right of the dropdown is an unchecked checkbox labeled 'Azure AD'. Below the dropdown are two checkboxes: 'Join Domain' (unchecked) and 'Join Workgroup' (checked). Below these is another text prompt: 'Enter the account name:'. A text box contains the name 'Jane'. Below the text box is a checked checkbox labeled 'Set as default logon'. At the bottom of the window are three buttons: '< Back', 'Next >' (highlighted in blue), and 'Cancel'.

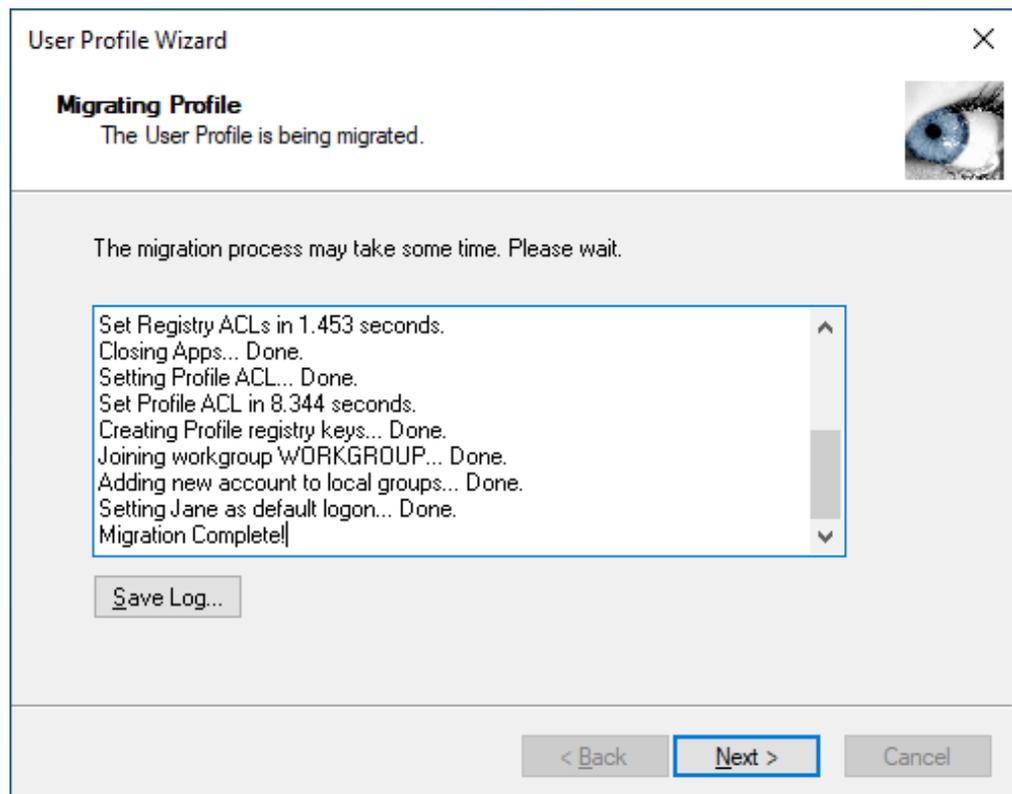
The default Windows workgroup name is WORKGROUP. If you have the Corporate or Professional Edition of User Profile Wizard, you can specify a different workgroup

MIGRATING FROM DOMAIN TO LOCAL ACCOUNTS

name by editing the <Workgroup> value in Profwiz.config. (See the [Profwiz.config Reference](#) chapter below.)

Finally, enter the name of the local account that you want to use the profile. The user account must already exist.

That's it! Click **Next** and User Profile Wizard will do the rest - migrating the domain account profile to the local account and unjoining from the domain, if that is what you chose.



Automating Domain to Local Migrations

The Deployment Kit supports automating User Profile Wizard for domain to local migrations. Please also refer to the [Getting Started](#) chapter if you skipped it to get here.

At Step 3, tick the **Join Workgroup** box if you want to unjoin your computers from the existing domain and add them to a workgroup. The Deployment Kit will then “grey out” the domain options and User Profile Wizard will be configured to migrate profiles to local accounts.

Domain Information
Enter information about the new domain

Enter the name of the new domain:
 Azure AD

Join Domain Join Workgroup
 Force Join

Azure ID file path:

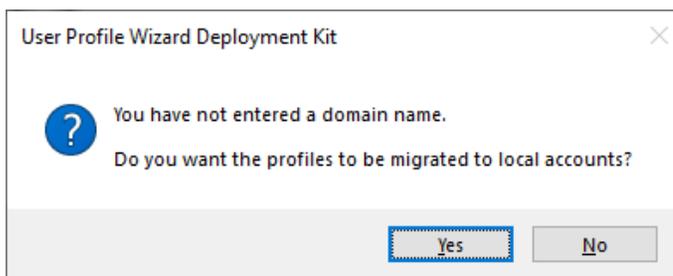
Use Provisioning Package
 Provisioning Package:

< Back Next > Cancel

As previously mentioned, the default Windows workgroup name is WORKGROUP. You can specify a different workgroup name by editing the <Workgroup> value in Profwiz.config. (See the [Profwiz.config Reference](#) chapter below.)

If you want to migrate profiles to local accounts but *not* unjoin from the existing domain, leave the “Enter the name of the new domain” box blank and just click **Next**. The Deployment Kit will warn you about what you are doing.

MIGRATING FROM DOMAIN TO LOCAL ACCOUNTS



The Deployment Kit automatically adjusts what options are shown based on the choices you make. Because you have chosen to migrate profiles to local accounts, the domain-only options are hidden. This means that when you click **Next** you are taken to Step 6.

At Step 6 you must enter the name of the existing domain. (There is no option to say “no” to the question “Are you migrating from an existing Windows domain?”)

In all other ways, the options are the same as those available when you are migrating a computer to a new domain.

Migrating to Azure AD

User Profile Wizard enables you to migrate user profiles to Azure AD accounts, but additional configuration steps are required.

Azure Object IDs and the ForensiTAzureID.xml file

In order to migrate a user a profile to an Azure AD user account, User Profile Wizard needs to know the Object ID of the user account. The Object ID can be found on your Azure AD portal (<https://portal.azure.com/>) and can also be queried using the Microsoft Graph PowerShell module.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Azure AD > Users | All users > Test User | Profile. The main content area displays the profile for 'Test User' (User). The profile card includes a profile picture with the initials 'TU', the email address 'Test@azureforensit.onmicrosoft.com', and a 'User Sign-ins' section. Below the profile card, the 'Identity' section is expanded, showing fields for Name (Test User), User name (Test@azureforensit.onmicrosoft.com), and Object ID (ea432ff8-46dd-4114-a4c3-622a16a7438a). The Object ID field is circled in red. The 'Job info' section is also visible at the bottom.

It is impractical to have to install the Microsoft Graph PowerShell module on each machine you want to migrate, so User Profile Wizard uses a file to look up the Object ID of the Azure AD user account you want to migrate the user profile to. By default this file is called **ForensiTAzureID.xml**. (Corporate and Professional Editions customers can change the name of the file.)

Generating a ForensiT AzureID.xml file

To generate the ForensiT AzureID.xml file that User Profile Wizard will need to migrate profiles to your new Azure AD accounts, you need to run the **Save-AzureADUser.ps1** PowerShell script.

Save-AzureADUser.ps1 is installed with the Corporate and Professional Editions of User Profile Wizard and can also be downloaded from <https://github.com/ForensiT/PowerShell>.

Open the “User Profile Wizard Command Line” from the Start Menu->F->ForensiT User Profile Wizard, and run Save-AzureADUser.ps1. Alternatively, run Save-AzureADUser.ps1 from a PowerShell command prompt.

Note: The Save-AzureADUser.ps1 script uses the Microsoft Graph PowerShell module to query Azure AD to get a list of user Object IDs. If the Graph PowerShell module is not installed, the script will attempt to install it. To install the Microsoft Graph PowerShell module, the script needs to be run with Admin permissions.¹

```

Administrator: User Profile Wizard PowerShell
ForensiT User Profile Wizard Command Line Console
UPW:>Save-AzureADUser.ps1
The Microsoft.Graph PowerShell module is not installed. Do you want to install it now? (Y/n): Y

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\admin\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y

```

¹ Obviously Save-AzureADUser.ps1 is a script! If you have not enabled PowerShell scripting, you need to do so by entering **set-executionpolicy remotesigned** in an Admin PowerShell console.

When you run the script, you will be prompted to authenticate to your Azure AD.

Sign in to your account

×



Sign in

mia@jackrabbitslims.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Next

Once you have done that, the script will create the ForensiTAzureID.xml file in the “Deployment Files” folder.

```
Azure user ID file created: C:\ProgramData\ForensiT\User Profile Wizard Corporate\Deployment Files\ForensiTAzureID.xml
UPW:>
```

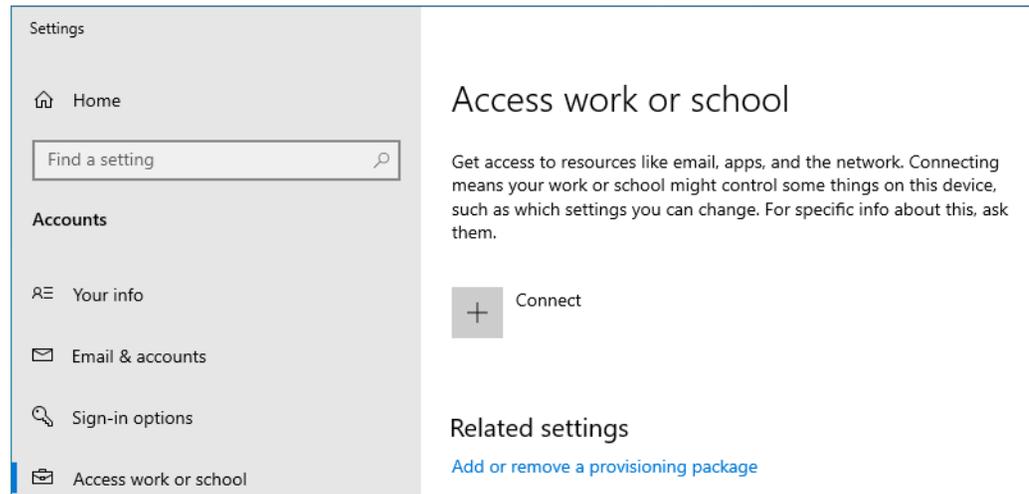
If you open the ForensiTAzureID.xml file in Notepad, you will see a list of entries containing the Object ID, Display Name, and User Principle name of your Azure AD users, like this:

```
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type='text/xsl' href='style.xsl'?>
<ForensiTAzureID ObjectID="1ebcfff5-fd20-4eb3-9a8c-f97bff045039"
Name="jackrabbitslims.onmicrosoft.com" DisplayName="Jack Rabbit Slims">
  <User>
    <UserPrincipalName>marilyn@jackrabbitslims.onmicrosoft.com</UserPrincipalName>
    <ObjectId>b5bf1089-e738-4fa5-ab77-470c16423d7c</ObjectId>
    <DisplayName>Marilyn Monroe</DisplayName>
  </User>
  <User>
    <UserPrincipalName>Mamie@jackrabbitslims.onmicrosoft.com</UserPrincipalName>
    <ObjectId>5454018d-6005-444d-9c34-b1196ff0b5f4</ObjectId>
    <DisplayName>Mamie van Doren</DisplayName>
  </User>
```

Joining to Azure AD

Microsoft do not offer any programmatic way to join a device to Azure AD. There are therefore, only two ways to do it.

Firstly, you can join a computer to Azure AD “manually” using the “Connect” option in “Access work or school” in “Settings”.



You can use User Profile Wizard to migrate profiles to Azure AD accounts before or after you join the machine to your Azure AD organization. Remember however, that the user will not be able to sign-in and use their profile until the machine has been joined.

The second way to join a machine to Azure AD is to use a Provisioning Package. The Corporate and Professional Editions of User Profile Wizard have built-in support for installing a Provisioning Package. It is by creating a Provisioning Package that you can automate the migration of a device to Azure AD with User Profile Wizard.

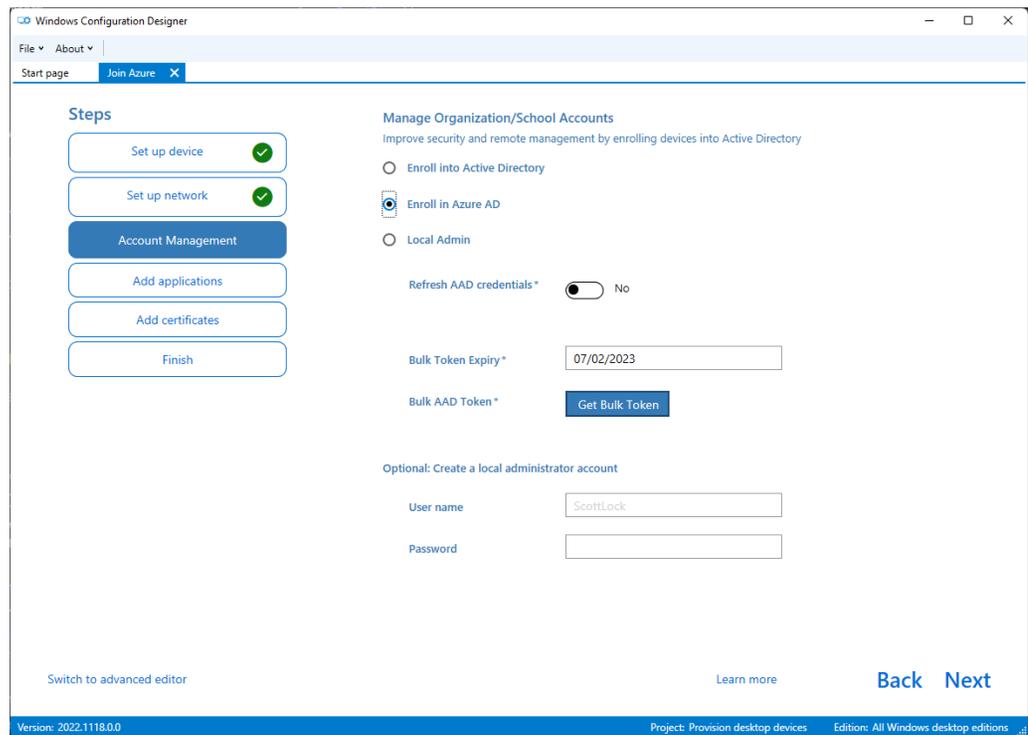
Creating a Provisioning Package

To create a Provisioning Package, you need to use Microsoft’s **Windows Configuration Designer**. Windows Configuration Designer is installed as part of the [Windows Assessment and Deployment Kit \(ADK\) for Windows 10](#), is also available as an [app in the Microsoft Store](#).

We will not repeat Microsoft’s instructions for creating a Provisioning Package here; please refer to Microsoft’s own documentation. However, it is not difficult to do.

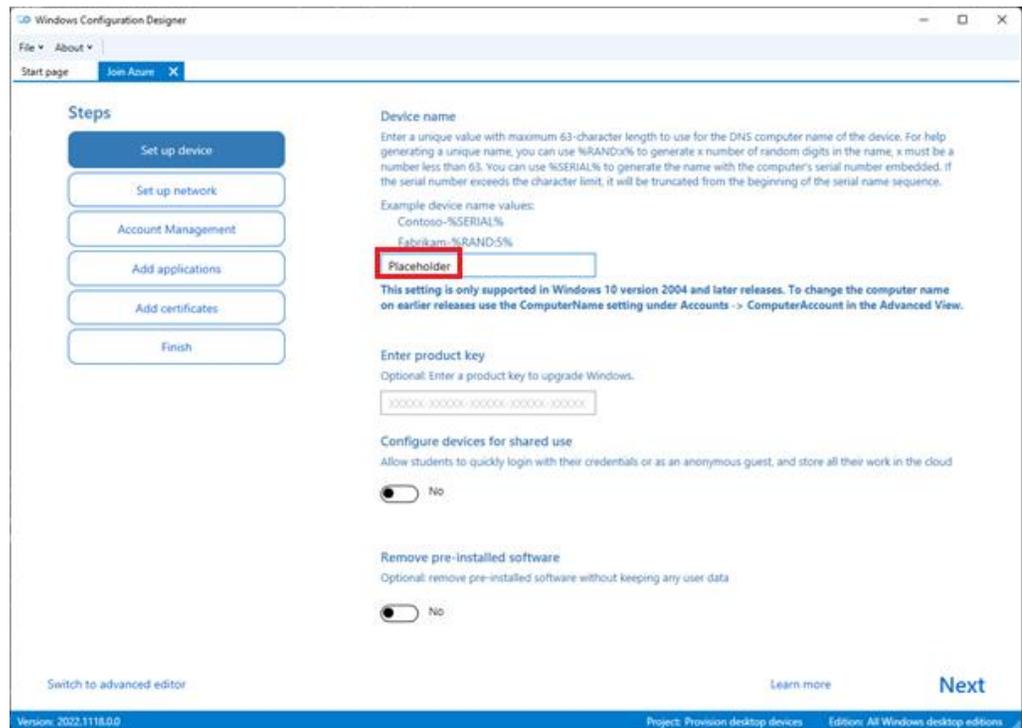
Windows Configuration Designer gives you a large number of settings that you can configure, but if you are only interested in joining to Azure AD, you can start with the simpler interface.

The key setting is under “Account Management” where you specify that you want to enroll machines in Azure AD, and you generate the bulk AAD token that is needed to do that. When you get the bulk token, you will be prompted to authenticate to your Azure AD.



When using the simpler interface, WCD forces you to rename your machines. This is frequently not ideal. However, there is a way around this. For now, you have to put something in the Device Name box in order to progress, for example ‘Placeholder’ as per below.

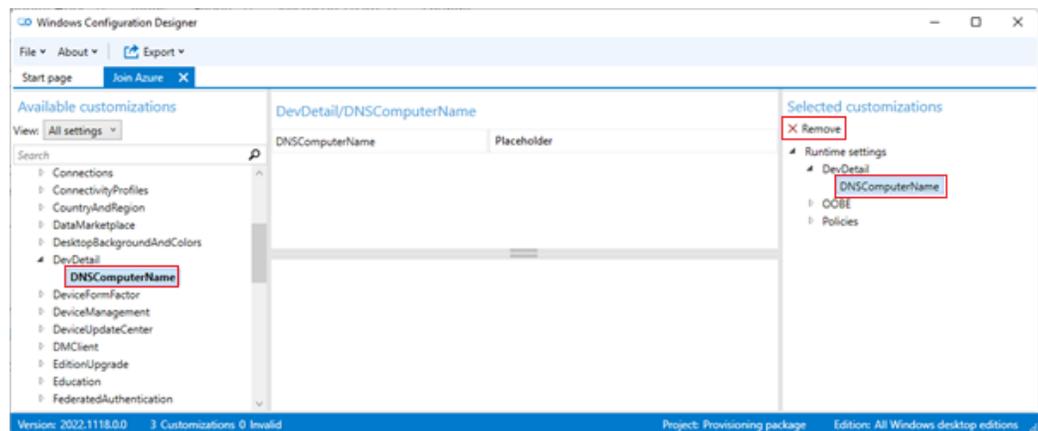
MIGRATING TO AZURE AD



When you get to “Finish” do *not* click the “Create” button. Instead, click “Switch to advanced Editor” in the bottom left-hand corner of the Designer. Be warned! Once you switch to the advanced editor, you can’t go back.

Now find “DNSComputerName” under “DevDetail” within “Available Customizations” in the left-side panel.

Then, in the right-side “Selected customizations” panel, also select “DNSComputerName”. You will now have the open to **Remove** renaming the computer from your Provisioning Package file.



When you're done, click on the "Export" Menu and choose "Provisioning Package". When you have finished running the Windows Configuration Designer, you will have a .ppkg file that you will be able to use to join your machines to Azure AD.

Windows Configuration Designer will have created a Package_{GUID} user account, it is this account that the Provisioning Package uses to join the computer to Azure. Please ensure that this account has MFA disabled and that MFA is not required in order to join a computer to Azure.

You can test the Provisioning Package independently, to prove it is working correctly by installing it using the PowerShell cmdlet **Install-ProvisioningPackage**. The PowerShell console will report any issues with installing the Provisioning Package.

Windows joins the computer to Azure when the computer is *next* rebooted after the Provisioning Package is installed, this is why you do not see the 'Other User' option immediately on the first reboot. If the Provisioning Package is working, the 'Other User' option does appear after a while, or you may be able to reboot the computer again after a couple of minutes in order to speed up the option appearing.

If there are any problems with Windows joining the computer to Azure AD using the Provisioning Package, please check for errors and more information in Event Viewer under **Applications and Services Logs > Microsoft > Windows > User Device Registration > Admin**

A Provisioning Package can fail to join a computer to Azure for a number of reasons, it is highly recommended that you have a local account that you can use to join the computer to Azure manually if the Provisioning Package fails to do so.

Configuring User Profile Wizard to migrate profiles to Azure AD

Configuring User Profile Wizard to migrate profiles to Azure AD is simply a case of checking the **Azure AD** box at Step 3 of the Deployment Kit, and entering the name of your Azure AD tenant:

ForensiT User Profile Wizard Deployment Kit - Step 3 of 13

Domain Information
Enter information about the new domain

Enter the name of the new domain:
Jack Rabbit Slims Azure AD

Join Domain Join Workgroup
 Force Join

Azure ID file path:
ForensiT AzureID.xml

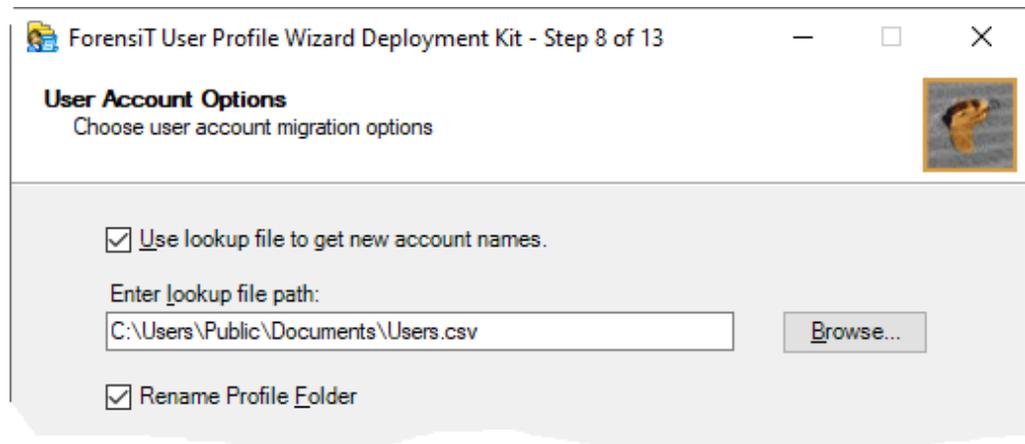
Use Provisioning Package
Provisioning Package:
ForensiT AzureAD.ppkg

You will also need to specify the location of your **ForensiT AzureID.xml** file. (See above.) By default, User Profile Wizard will look for the ForensiT AzureID.xml file in the same directory as Profwiz.exe.

Additionally you have the option of specifying a Provisioning Package. You do not have to, but if you don't User Profile Wizard will not be able to join the machine to your Azure AD tenant, and you will need to do that yourself.

If you are not going to use a Provisioning Package and are migrating from an existing on-premises domain, you can check the **Join Workgroup** checkbox, so User Profile Wizard will remove the workstations from the existing domain. You cannot join a device to Azure AD if it is still joined to an on-premises domain.

If you are migrating profiles to Azure AD user accounts, obviously the name of the new user account cannot be the same as the name of the existing user account. As a result, unless you only want to migrate one profile at a time, you need to specify a user lookup file when running the Deployment kit.



Note. Just to be clear: the user lookup file maps the user’s *existing* account name to their new Azure AD User Principle Name. So if a user is currently signing into their machine as “Marilyn”, and their new Azure AD User Principle Name is marilyn@jackrabbitslims.onmicrosoft.com, the entry in the lookup file would be

Marilyn,marilyn@jackrabbitslims.onmicrosoft.com

The user lookup file is not the same file as the ForensiT AzureID.xml file. User Profile Wizard will get the user’s new Azure AD User Principle Name from the user lookup file, and then look up the User Principle Name in the ForensiT AzureID.xml file to get the Object ID of the new Azure AD user.

Migrating From an Existing Tenant

There is no real difference when migrating from an existing Azure AD tenant, to when you are migrating from an on-premises domain.

To automate the migration, you specify that you are migrating from an existing tenant at Step 6 of the Deployment Kit. This sets the existing domain name as “azuread”, rather than your existing tenant name.

ForensiT User Profile Wizard Deployment Kit - Step 6 of 13

Existing Domain
Enter existing domain information.

Are you migrating from an existing Windows domain or Azure AD tenant?

Yes
 No

Enter existing domain name:
azuread

Migrating from existing Azure AD tenant

< Back Next > Cancel

“azuread” will generally be correct for migrating from an existing tenant. However, if the tenant is, or has been, linked to an on-premises domain, Windows may be using the on-premises domain name as the tenant name. If you are in any doubt, run **whoami** from a PowerShell when signed-in with an old tenant user account, and Windows will return the username in the format *DOMAIN\username*. You need to be using whatever *DOMAIN* is as the existing domain name.

The Deployment Kit makes the following changes to your Profwiz.config file:

```
<!-- Domain -->  
<Domain>Jack Rabbit Slims</Domain>  
<AdsPath></AdsPath>  
  
<!-- Azure AD -->  
<Azure>True</Azure>  
<AzureObjectIDFile>ForensiTAzureID.xml</AzureObjectIDFile>  
<ProvisioningPackage>ForensiTAzure.ppkg</ProvisioningPackage>  
<GCC></GCC>
```

Note that If you are migrating from an existing Azure AD tenant, you can use the UPN in the user lookup file. So if you are migrating to a new tenant from an existing tenant, the user names can be listed in a look-up file as follows:

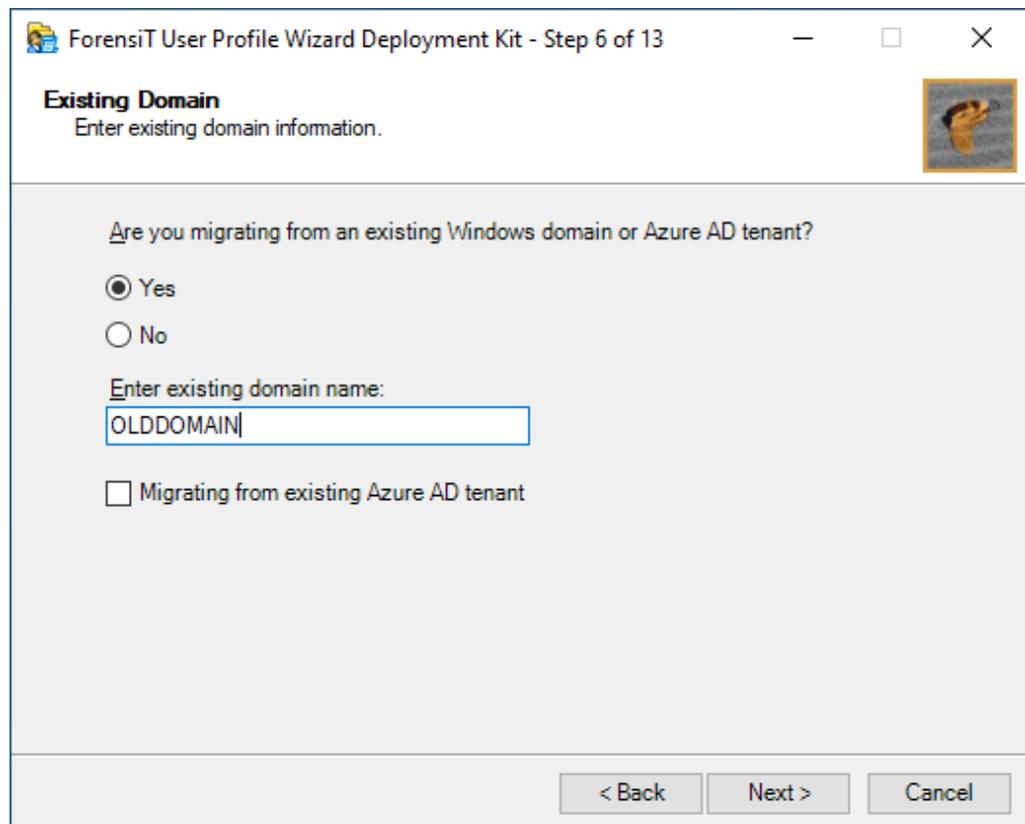
username1@oldtenant.onmicrosoft.com,newuser1@newtenant.onmicrosoft.com

Migrating From a Hybrid Domain

If you are migrating from a Hybrid domain, the <OldDomain> needs to be your on-premises AD domain. Remember that in a Hybrid domain, the computers are only joined to Azure AD via the AD domain – as soon as you unjoin the machines from the AD domain, they are unjoined from Azure AD as well. You need to re-join to Azure AD separately. However, User Profile Wizard can do this for you using a Provisioning Package.

When migrating from a Hybrid domain, on Step 6 of the Deployment Kit you should specify the old AD Domain name because the profiles will be associated with the AD account, even if the user is logging on with their Azure UPN. You can confirm this with whoami when logged on to one of the source accounts, whoami will return;

OldDomain\username



Migrating to Office 365 GCC and GCC High Environments

In a “Commercial” (“normal”) Office 365 environment, Azure AD user accounts have a SID (Security IDentifier) in the following format:

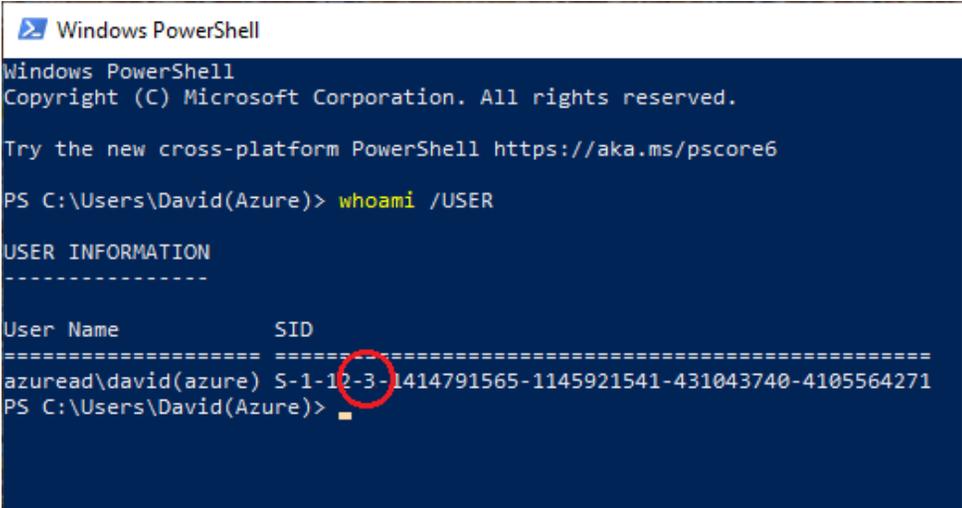
S-1-12-1-1414791565-1145921541-431043740-4105564271

The “1” highlighted is a RID (Relative IDentifier”), and is always “1” in commercial Office 365 environments. In Office 365 GCC and GCC High environments, this is not the case. The RID may, for example, be “3”, or “8”, or possibly another number:

S-1-12-3-1414791565-1145921541-431043740-4105564271

For User Profile Wizard to correctly migrate the user profile, it needs to know the correct RID for the GCC environment you are migrating to.

If you do not know what the RID is, a simple way is to run **whoami /USER** from a command prompt, when signed-in with a GCC user account



```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\David(Azure)> whoami /USER

USER INFORMATION
-----

User Name          SID
-----
azuread\david(azure) S-1-12-3-1414791565-1145921541-431043740-4105564271
PS C:\Users\David(Azure)>

```

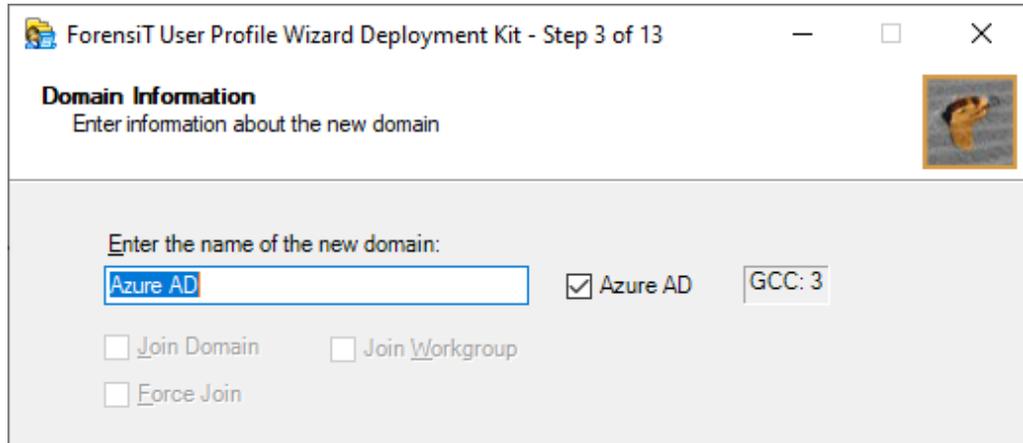
Once you know the RID, you just need to add it to the <GCC> value in your Profwiz.config file:

```

<!-- Azure AD -->
<Azure>True</Azure>
<AzureObjectIDFile>ForensiTAzureID.xml</AzureObjectIDFile>
<ProvisioningPackage>ForensiTAzure.ppkg</ProvisioningPackage>
<GCC>3</GCC>

```

If you run the Deployment Kit, having set your GCC RID, it will be reported at Step 3:



Migrating to an Azure AD Account

Migrating a profile to an Azure AD account is the same as migrating to an on-premises domain account.

When you get to the “User Account Information” page, User Profile Wizard will fill in the “Enter the domain” box with the Azure AD name from the Profwiz.config file. The **Azure AD** box will be checked.

User Profile Wizard

User Account Information
Specify the domain and account name for the user you would like to use the profile.

Enter the domain, or select the local computer name:
 Jack Rabbit Slims Azure AD

Join Domain Join Workgroup

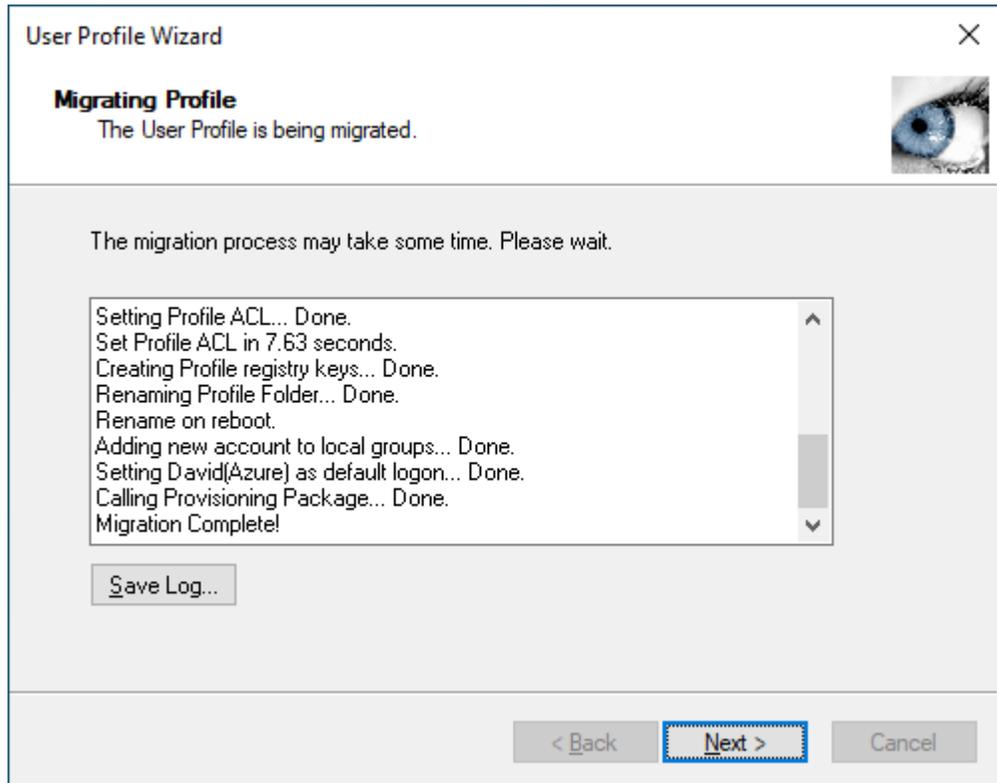
Enter the account name:

i Azure AD
Enter your work or school account email address

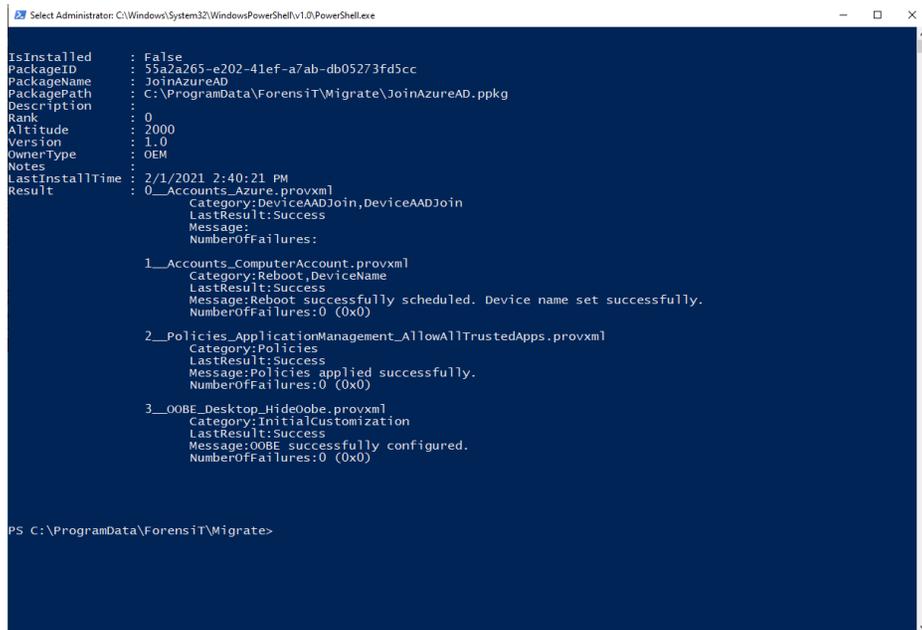
< Back Next > Cancel

If you have specified a user lookup file, and you have only selected one profile to migrate, User Profile Wizard will populate the “Enter the account name” box. If you have specified more than one profile to migrate, “Enter the account name” will be set to “Using lookup file”.

The migration begins when you click **Next**.



User Profile Wizard calls the Provisioning Package at the end of the migration. It will then (optionally) display the output:



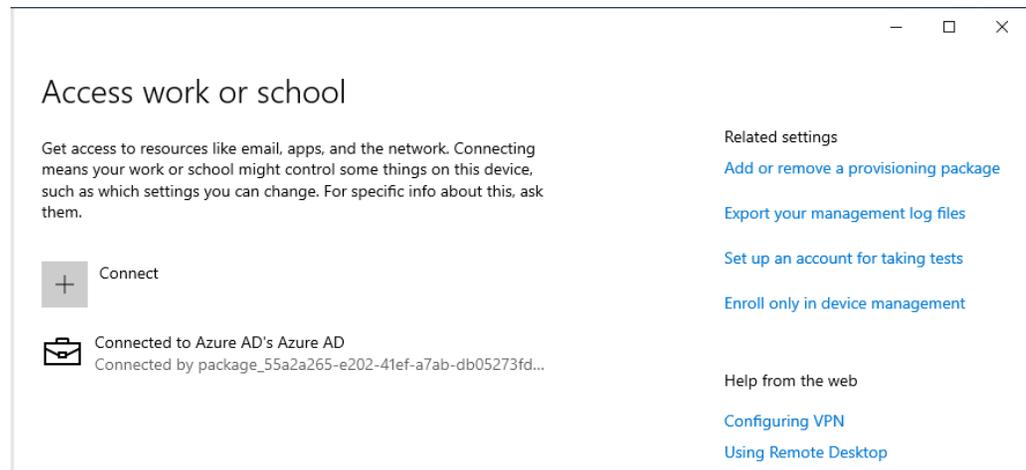
Note that the output says “IsInstalled” is False. This is normal. The Provisioning Package will not be run until the machine reboots. The important thing is that LastResult is “Success” in the four sections under “Result”.

The output is also saved to C:\ProgramData\ForensiT\Log\ProvisioningPackage.log.

To suppress the output, set the <Silent> value to *True* in your Profwiz.config file.

If you have installed a Provisioning Package, Windows will reboot the machine. This cannot be avoided.

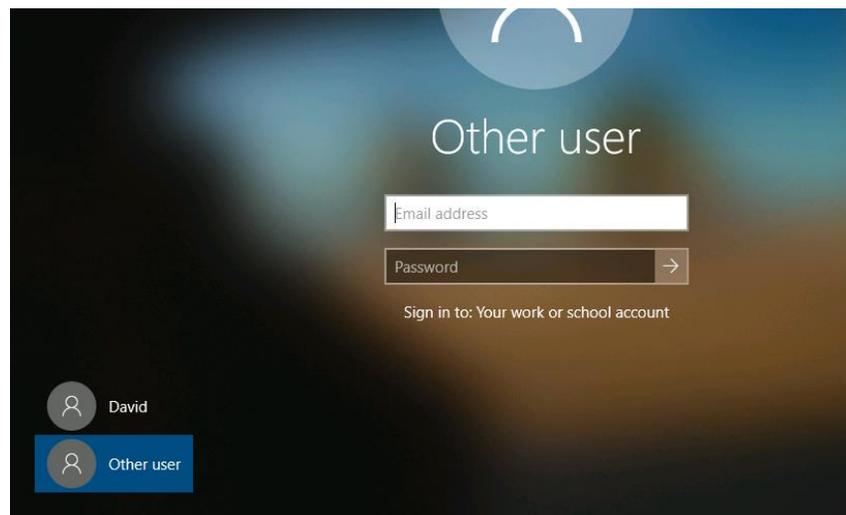
Once the machine has rebooted, you can check the installation of the Provisioning Package under “Access work or school” in “Settings”



Details of the Provisioning Package can be found under “Add or remove a provisioning package”

Additional Notes on using a Provisioning Package

In our own testing we have noticed that the Provisioning Package takes some time to take effect after the machine has rebooted. One consequence of this is that you may not be able to sign-in with an Azure AD account immediately after the machine reboots because the “Other user”/ “Sign in to: Your work or school account” option is not shown until provisioning is complete.



You can test the Provisioning Package independently, to prove it is working correctly by installing it using the PowerShell cmdlet **Install-ProvisioningPackage**. The PowerShell console will report any issues with installing the Provisioning Package.

Windows joins the computer to Azure when the computer is *next* rebooted after the Provisioning Package is installed, this is why you do not see the ‘Other User’ option immediately on the first reboot. If the Provisioning Package is working, the ‘Other User’ option does appear after a while, or you may be able to reboot the computer again after a couple of minutes in order to speed up the option appearing.

If there are any problems with Windows joining the computer to Azure AD using the Provisioning Package, please check for errors and more information in Event Viewer under **Applications and Services Logs > Microsoft > Windows > User Device Registration > Admin**

A Provisioning Package can fail to join a computer to Azure for a number of reasons, it is highly recommended that you have a local account that you can use to join the computer to Azure manually if the Provisioning Package fails to do so.

.config Reference

This Chapter details the settings in the Profwiz.config file

```
<!-- ForensiT User Profile Wizard run options -->
<!-- Note: options set here are overridden by parameters passed
on the command line -->
```

```
<!-- Domain -->
<Domain></Domain>
```

This is the name of the new domain the machine is joining. This can either be an on-premises domain, or an Azure AD tenant.

```
<AdsPath></AdsPath>
```

The AdsPath of the Active Directory container where the computer account will be created. If this is blank the computer account will be created in the default “Computers” container.

```
<!-- Azure AD -->
<Azure></Azure>
```

Set to *True* if you are joining an Azure AD domain.

```
<AzureObjectIDFile></AzureObjectIDFile>
```

Path to a xml file that has the ObjectIDs of the Azure AD user accounts.

```
<ProvisioningPackage></ProvisioningPackage>
```

Path to the Provisioning Package to join the device to the Azure AD tenant.

```
<GCC></GCC>
```

The RID (Relative Identifier) of the Office 365 GCC environment you are migrating to.

```
<!-- Options -->
<ForceJoin>False</ForceJoin>
```

Force the machine to join `<Domain>` even if it is already joined to a domain of the same name or if the Wizard has not migrated any profiles. This option is useful if you are replacing one domain with a domain of the same name.

```
<NoJoin>False</NoJoin>
```

Do not join the machine to the domain.

```
<NoDefault>False</NoDefault>
```

Do not set the new domain account as the default workstation logon

```
<Delete>False</Delete>
```

Delete the local account when migration is completed

```
<Disable>False</Disable>
```

Disable the local account when migration is completed

```
<UnJoin>False</UnJoin>
```

Unjoin the machine from a domain and join it to a workgroup.

```
<Workgroup></Workgroup>
```

The name of the workgroup to join. If no name is specified, the default Windows WORKGROUP is used.

```
<ForceRoamingOption></ForceRoamingOption>
```

Override auto discovery of roaming profiles.

```
<!-- Credentials -->
```

```
<DomainAdmin></DomainAdmin>
```

The name of an account with the necessary permissions to add the machine to <Domain>

```
<DomainPwd></DomainPwd>
```

The <DomainAdmin> account password, either in plain text or encrypted by a <Key>. Passwords are automatically encrypted by the Deployment Kit.

```
<LocalAdmin></LocalAdmin>
```

The name of a local administrator account. User Profile Wizard must be run with Administrator privileges.

```
<LocalPwd></LocalPwd>
```

The <LocalAdmin> account password, either in plain text or encrypted by a <Key>. Passwords are automatically encrypted by the Deployment Kit.

```
<SetsIDHistory>False</SetsIDHistory>
```

Maintain the SID history.

```
<OldDomainAdmin></OldDomainAdmin>
```

The name of an account with Domain Administrator permissions on <OldDomain>

```
<OldDomainPwd></OldDomainPwd>
```

The <OldDomainAdmin> account password, either in plain text or encrypted by a <Key>. Passwords are automatically encrypted by the Deployment Kit.

```
<Key></Key>
```

The key to decrypt encrypted <DomainPwd> and <LocalPwd> passwords. This is automatically set by the Deployment Kit when it encrypts passwords.

To generate an encrypted password manually type Profwiz /KEY at the command line without any other parameters.

```
<!-- Corporate Edition Settings -->
```

```
<Silent>False</Silent>
```

Do not show any error messages

```
<NoMigrate>False</NoMigrate>
```

Run User Profile Wizard but do not migrate any profiles. You can use this option just to join a machine to a domain, or just to run a follow-on script.

```
<NoReboot>False</NoReboot>
```

Do not reboot the machine after it has been migrated

```
<RemoveAdmins>False</RemoveAdmins>
```

Remove users' local administrator rights when the machine joins the domain

```
<MachineLookupFile></MachineLookupFile>
```

Path to a "look up" file to map old computer names to new computer names.

A look-up file is just a plain comma-separated text file. Computer names are listed in a look-up file as follows:

```
Computer1,New_ComputerName1
Computer2,New_ComputerName2
```

```
<Log></Log>
```

Path to the log file where User Profile Wizard will write the output from the migration process.

```
<!-- Script Settings -->
<RunAs></RunAs>
```

The path of a "follow-on" script or executable file to run after the migration. By default, the script runs after the machine has been joined to the new domain (but before the machine reboots) using the `<LocalAdmin>` credentials. However this behaviour can be altered using the `<RunScriptPerUser>` and `<RunAsSystem>` values below.

```
<Hash></Hash>
```

The security hash of the script or executable file specified by `<RunAs>`. This is automatically generated by the Deployment Kit. To generate a hash manually type Profwiz /KEY at the command line without any other parameters.

```
<RunScriptPerUser>False</RunScriptPerUser>
```

This tells User Profile Wizard to run the follow-on script after each profile is migrated, rather than after the machine has been joined to the new domain.

```
<RunAsSystem>False</RunAsSystem>
```

By default, User Profile Wizard will run the follow-on script in the security context of the `<LocalAdmin>` account. However, by setting `<RunAsSystem>` to True, the script will run the follow-on script in the security context of the SYSTEM account.

```
<!-- Settings for migrating all profiles -->
<All>False</All>
```

Migrate all profiles on the workstation

```
<OldDomain></OldDomain>
```

The name of the old Source domain. User Profile Wizard will migrate account profiles from this domain. If `<OldDomain>` is blank, User Profile Wizard will migrate local account profiles.

You can specify more than one Source domain. The list of domains needs to be *colon delimited*, so like this: `<OldDomain>OLD1:OLD2:OLD3</OldDomain>`

```
<UserLookupFile></UserLookupFile>
```

Path to a “look up” file to map old user account names to new user account names.

```
<Exclude>ASPNET,Administrator</Exclude>
```

A list of user account names whose profiles will not be migrated to the new domain.

```
<!-- Advanced Settings -->
```

```
<SkipOnExistingProfile>False</SkipOnExistingProfile>
```

In some cases, you may need to migrate user profiles on a machine that has already been joined to a new domain. In such cases a user may already have a new domain account profile which will be lost if they are assigned their old profile. `<SkipOnExistingProfile>` tells User Profile Wizard not to migrate the user’s old profile if this is the case.

```
<SkipOnDisabledAccount>False</SkipOnDisabledAccount>
```

Tells User Profile Wizard not to migrate a profile if the user’s account is disabled in the new domain.

```
<NoGUI>False</NoGUI>
```

Force User Profile Wizard to run in command line (CLI) mode

```
<FailOnMachineNameNotFound>False</FailOnMachineNameNotFound>
```

If set to ‘True’ User Profile Wizard will only migrate a workstation if it is listed in the `<MachineLookupFile>`

```
<RenameProfileFolder>False</RenameProfileFolder>
```

Renames the user’s profile folder (typically C:\Users*username*) to their new domain account name.

```
<ProtocolPriority></ProtocolPriority>
```

By default, User Profile Wizard uses Windows’ NetBIOS based APIs to join a machine to a domain. You can override this behaviour by setting the `<ProtocolPriority>` value to ‘LDAP’ If you do this you **must** set a `<AdsPath>` value.

Forcing User Profile Wizard to use LDAP can be useful in a number of circumstances. For example, if there are NetBIOS name resolution issues on your network, using LDAP means that DNS name resolution will be used instead. Using LDAP can also be useful when renaming computer accounts. Using NetBIOS, the computer account object is first created in Active Directory with the *existing* computer name and *then* it is renamed – a two stage process. Using LDAP gives a finer degree of control, allowing the computer account object to be created with the new name in one step.

```
<DC></DC>
```

Specify the Domain Controller you want to use to join workstations to a domain. This setting is dependent on `<ProtocolPriority>` being set to LDAP.

In some circumstances you may want to specify which Domain Controller User Profile Wizard uses when joining a machine to a domain. Essentially there are two types of operations involved when User Profile Wizard talks to a Domain Controller – read and write. For read operations we leave it to Windows to get the name of the nearest DC. For write operations, however, you can specify the DC that you want User Profile Wizard to use. The value must be a DNS server name prefixed with two back slashes. Note that specifying the DC is dependent on using LDAP, which in turn means that you have to set a `<AdsPath>` value:

```
<ProtocolPriority>LDAP</ProtocolPriority>
<DC>\\britannic2.britannic.forensit.com</DC>
```

When using a `<DC>` value it is normal to see two different DCs reported in the log file.

If Windows is not returning the DC that you would like the computer to use for the read operations, you should configure this within AD Sites and Services.

```
<CopyProfile>False</CopyProfile>
```

Create a copy of the original profile and assign the copy to the new domain account.

You should think carefully before setting the `<CopyProfile>` value to ‘True’. There is usually no need to create a copy of the original profile. By default, User Profile Wizard works by configuring the existing profile so that it can be used by the user’s new domain account: no data is moved, copied or deleted – this makes the process intrinsically safe, as well as very fast. By creating a copy of the profile you will make the migration process *much* slower.

However, there are circumstances where you may need to create copy profiles. For example, on shared workstations which are not already joined to a domain, users may all logon with one account. If you want to move the machine into Active Directory, you can create a copy of the profile for each user account so that each user can logon with their own username, but still retain their familiar desktop.

```
<!-- Outlook Settings -->
```

PROFWIZ.CONFIG REFERENCE

```
<ZeroConfigExchange>False</ZeroConfigExchange>
```

If True, enables Microsoft's ZeroConfigExchange for automatically configuring Outlook.

```
<!-- VPN Settings -->
```

```
<VPN>True</VPN>
```

Enable VPN password caching mode. See [Migrating over a VPN](#).

```
<DefaultUserPwd></DefaultUserPwd>
```

The default user password that will be cached. See [Migrating over a VPN](#).

Push migrations and the Command Line Console

In this chapter we discuss running User Profile Wizard from the command line, looking particularly at push migrations

Push or Pull?



User Profile Wizard gives you the option to “push” migrations to remote workstations from a central administrator or “console” machine– which is very cool. But is a push migration a better solution than a “pull” migration, which is where a workstation initiates a migration by running a migration script?

Overall pull migrations offer better scalability. Generally, it is more efficient for a machine to initiate the migration itself. Using this methodology User Profile Wizard has proved to be extremely effective over hundreds of thousands of migrations.

Using scripting is also very flexible. You can customize a script to handle difficult or unusual migration scenarios in ways that cannot be achieved with a push migration.

Push migrations are obviously dependent on the workstation that is to be migrated being on the network at the time you want to migrate it. Additionally, there is probably greater administrator oversight required – even if the push migration is automated.

Sometimes, however, you do not have any choice. If your organization does not have an existing domain, or you don’t have access to some form of Electronic Distribution Software (ESD) like SCCM (SMS), Marimba or Tivoli to launch the migration, you probably will be looking for a push solution that doesn’t involve you visiting every desk.

Migrating a remote machine



To migrate a remote machine from the command line, we just have to use the `/COMPUTER` switch.

What's going to happen here is that User Profile Wizard will use the settings in the `Profwiz.config` file we created in the **Automating Enterprise Migrations** chapter to migrate the workstation `WORKSTATION1` to the new domain. (Note: `<All>` is set to "true.")

```

Administrator: User Profile Wizard Command Line
UPW:>Profwiz /COMPUTER WORKSTATION1
UPW:>

ForensiT User Profile Wizard 20.0
Licensed to ForensiT (50 Seats) Serial No. 9BDCC4FE
Copyright (c) 2002-2020 ForensiT Ltd
www.ForensiT.com

Connecting to WORKSTATION1...

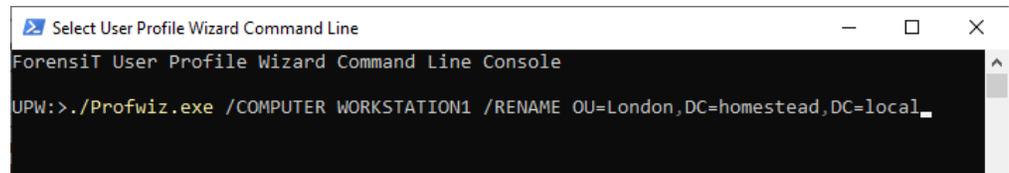
Creating migration service... Done.
Starting migration service... Done.
Target device: WORKSTATION1
OS build 10.0.19041.388. Version 2004.
Migrating user account "test"
Finding Domain Controller for domain HOMESTEAD... Done.
Using Domain Controller: \\HOMESTEADDC1.homestead.local.
Binding to Active Directory... Done.
Getting FQDN for user "test"... Done.
Getting Domain SID... Done.
SID is S-1-5-21-2010793018-3992016981-3654859121-1110
Checking for roaming profile...Done.
No roaming profile path set.
Processing UWP Apps... Done.
Setting Registry ACLs... Done.
Set Registry ACLs in 1.31 seconds.
Closing Apps... Done.
Setting Profile ACL... Done.
Set Profile ACL in 3.547 seconds.
Creating Profile registry keys... Done.
Renaming Profile Folder... Done.
Adding new account to local groups... Done.
Finding Domain Controller for domain HOMESTEAD... Done.
Using Domain Controller: \\HOMESTEADDC1.homestead.local.
Binding to Active Directory... Done.
Joining to domain "HOMESTEAD" ... Done.
Rebooting remote computer... Done.
Migration Complete!

```

Here `Profwiz.exe` is on the PowerShell path (`$Env:Path`); you will probably need to use `./Profwiz.exe` instead.

Using the command line

Parameters passed on the command line override the settings in the Profwiz.config file. This is useful if we just want to quickly change a parameter for a particular machine, or group of machines. For example, we may want to change the container where the computer account is created. We can change this with the /RENAME parameter:



```
Select User Profile Wizard Command Line
ForensiT User Profile Wizard Command Line Console
UPW:> ./Profwiz.exe /COMPUTER WORKSTATION1 /RENAME OU=London,DC=homestead,DC=local_
```

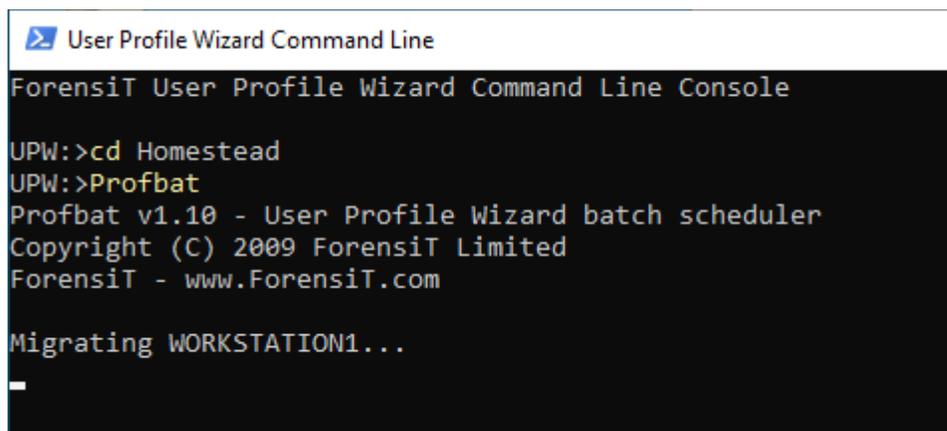
When we do this, all the other migration settings are still read from the Profwiz.config file.

All the command line parameters are listed in the **Command Line Reference** chapter later in this guide.

Automating Push Migrations

In the section above we saw how to push a migration to a single machine. But what if you need to push a migration to *a lot* of machines?

Profbat is a utility that can automate the migration of computers listed in a file. It is automatically installed with the Corporate Edition of User Profile Wizard, and can be accessed from the User Profile Wizard Command Line Console. You just need to **cd** to your Project folder and type **Profbat**:



```

User Profile Wizard Command Line
ForensiT User Profile Wizard Command Line Console
UPW:>cd Homestead
UPW:>Profbat
Profbat v1.10 - User Profile Wizard batch scheduler
Copyright (C) 2009 ForensiT Limited
ForensiT - www.ForensiT.com

Migrating WORKSTATION1...
-

```

Profbat will read the list of computers to be migrated from the file specified by the `<MachineLookupFile>` value in the Profwiz.config file. The file specified is used to rename machines, of course. If you *don't* want to rename a machine the machine lookup file entry needs to be something like this:

```
Old_name,Old_name
```

Each line of the csv must be terminated with a carriage return, even if there is only one.

You should set the `<All>` attribute value in the Profwiz.config file to 'True'

Profbat takes the log file path in the Profwiz.config file and appends the name of the machine being migrated to create a log file for each machine. So, for example, if you have the line

```
<Log>C:\Migration\Logs\Migrate.log</Log>
```

Profbat will create a series of log files named

```

C:\Migration\Logs\Migrate_machine1.log
C:\Migration\Logs\Migrate_machine2.log
C:\Migration\Logs\Migrate_machine3.log
...etc...

```

Optionally you can set some options for Profbat in Profwiz.config file. The following attributes can be added under `<!-- Advanced Settings -->`:

```
<ProfBatProcessLimit>8</ProfBatProcessLimit>
```

This specifies the number of machines Profbat will attempt to migrate at once. The default is 16.

```
<ProfBatRetryLimit>3</ProfBatRetryLimit>
```

This specifies the number of times Profbat will attempt to migrate a machine if the migration fails – for example, if the machine is not on the network. If this is not set, Profbat will keep trying indefinitely.

```
<ProfBatRetryDelay>2</ProfBatRetryDelay>
```

This specifies the number of minutes Profbat will wait before trying to migrate a machine again. The default is 1 minute.

Command Line Reference

This Chapter details User Profile Wizard's Command Line Parameters.

Command Line Parameters

Type **./Profwiz /?** at a command prompt and you will see the following screen:

```

User Profile Wizard Command Line
ForensIT User Profile Wizard Command Line Console
UPW: > ./Profwiz /?
UPW: >
Usage: Profwiz [/COMPUTER computername] [[/DOMAIN domainname] [/RENAME newcomputername] [/UNJOIN workgroupname]]
[/TARGETACCOUNT targetaccountname] [[/JOIN] | [/NOJOIN]] [/NODEFAULT] [/NOMIGRATE]
[[/SOURCEACCOUNT sourceaccountname] | [/SOURCEPROFILE sourceprofilefolder]]
[[/DELETE] | [/DISABLE]] [/NOREMOVE]
[/DOMAINADMIN domainlogon] [/DOMAINPWD password] [/LOCALADMIN localadministrator] [/LOCALPWD password]
[/KEY key] [/SILENT] [[/NOREBOOT] | [REBOOTDELAY seconds]]
[/LOG logfile] [/RUNAS script] [/HASH hash]

/COMPUTER - The name of the computer you want to migrate
/DOMAIN - The name of the domain
/RENAME - The full ADsPath of the new computer name
/UNJOIN - Unjoin the computer from a domain and add to a workgroup
/TARGETACCOUNT The domain user account name
/SOURCEACCOUNT The user account whose profile will be migrated
/SOURCEPROFILE The profile folder that will be migrated

/DOMAINADMIN - The domain account name to use to connect to the domain during migration
/DOMAINPWD - The DOMAINADMIN account password
/LOCALADMIN - The local administrator account that should be used during migration
/LOCALPWD - The LOCALADMIN account password
/KEY - Key to decrypt encrypted passwords.
To generate an encrypted password use /KEY without any other parameters.

/JOIN - Join the local machine to the domain even if the profile migration fails
/NOJOIN - Do not join the local machine to the domain
/NOMIGRATE - Do not migrate a user profile

/NODEFAULT - Do not set the domain account as the default logon
/DELETE - Delete the local account when migration is completed
/DISABLE - Disable the local account when migration is completed
/SILENT - Do not show any error messages
/NOREBOOT - Do not reboot machine
/REBOOTDELAY - The number of seconds to wait before rebooting

/LOG - Write results to a log file

/RUNAS - Run script or executable after successful migration
/HASH - Script File Security Hash
To generate security hash use /KEY without any other parameters.

UPW: > _
    
```

In this section we will describe each command line parameter in turn.

/COMPUTER computername (Optional)

The name of the computer you want to migrate.

If you do not specify a computer name the local computer will be migrated.

/DOMAIN domainname (Optional)

The name of the domain of the user account that will be given access to a profile.

If you do not specify a domain name, User Profile Wizard will look for ACCOUNT on the local machine.

/RENAME computername (Optional)

Rename the computer, or add computer to a specific AD container.

You can use the /RENAME switch in two situations. Firstly, as part of your migration to a Windows domain you may simply want to rename your workstations. Secondly, you may not want your Workstations to be in the default "Computers" container in Active Directory when they join the domain.

If you are renaming a machine you must specify the full ADsPath of the new computer name after the switch. For example, if you want to rename a computer and add it to the "Workstations" container you would type the following:

```
/RENAME CN=Workstation1,OU=Workstations,DC=uk,DC=forensit,DC=com
```

If you just want to add the machine to the container, use the container AdsPath:

```
/RENAME OU=Workstations,DC=uk,DC=forensit,DC=com
```

/UNJOIN workgroupname (Optional)

Unjoin the computer from a domain and add it to a workgroup. If the workgroup name is not specified, the computer will be added to the default WORKGROUP workgroup.

/TARGETACCOUNT accountname

The name of the account that will be given access to an existing profile.

/SOURCEACCOUNT accountname (Optional)

The account whose profile will be migrated.

This can be a domain account whose profile is stored locally. To specify a domain account use the format Domain\User.

/SOURCEPROFILE profilefoldername (Optional)

As an alternative to specifying a /SOURCEACCOUNT name, you specify the name of the profile folder that you want to migrate. You should only do this if the original user account SID cannot be resolved to an account name – for example, if the original on-

COMMAND LINE REFERENCE

premises domain is no longer accessible. You should just use the profile folder name, so if you want to migrate the C:\Users\Jayla profile, you would use

```
/SOURCEPROFILE Jayla
```

The Migrate-BySid.ps1 script uses this parameter.

/DOMAINADMIN domainadmin (Optional)

The name of an account with the necessary permissions to add the machine to the DOMAIN.

/DOMAINPWD password (Optional)

The DOMAINADMIN account password, either in plain text or encrypted by a KEY.

/LOCALADMIN localadmin (Optional)

The name of a local administrator account.

User Profile Wizard must be run with Administrator privileges. Using the LOCALADMIN parameter you can specify a local administrator account to run User Profile Wizard.

Because by default domain administrators have local administrator privileges, if the machine is already a member of a domain, you can specify a domain administrator account from the current domain as follows:

```
/LOCALADMIN OLD_DOMAIN\Administrator
```

/LOCALPWD password (Optional)

The LOCALADMIN account password, either in plain text or encrypted by a KEY.

/KEY key (Optional)

The key to decrypt encrypted DOMAINPWD and LOCALPWD passwords.

To generate an encrypted password use /KEY without any other parameters.

Having plain text passwords in your script files is not good security practice. To help you avoid this, User Profile Wizard gives you the option of encrypting your DOMAINADMIN and LOCALADMIN passwords. To do this, run the wizard with just the /KEY switch, for example:

```
UPW:>./Profwiz /KEY
```

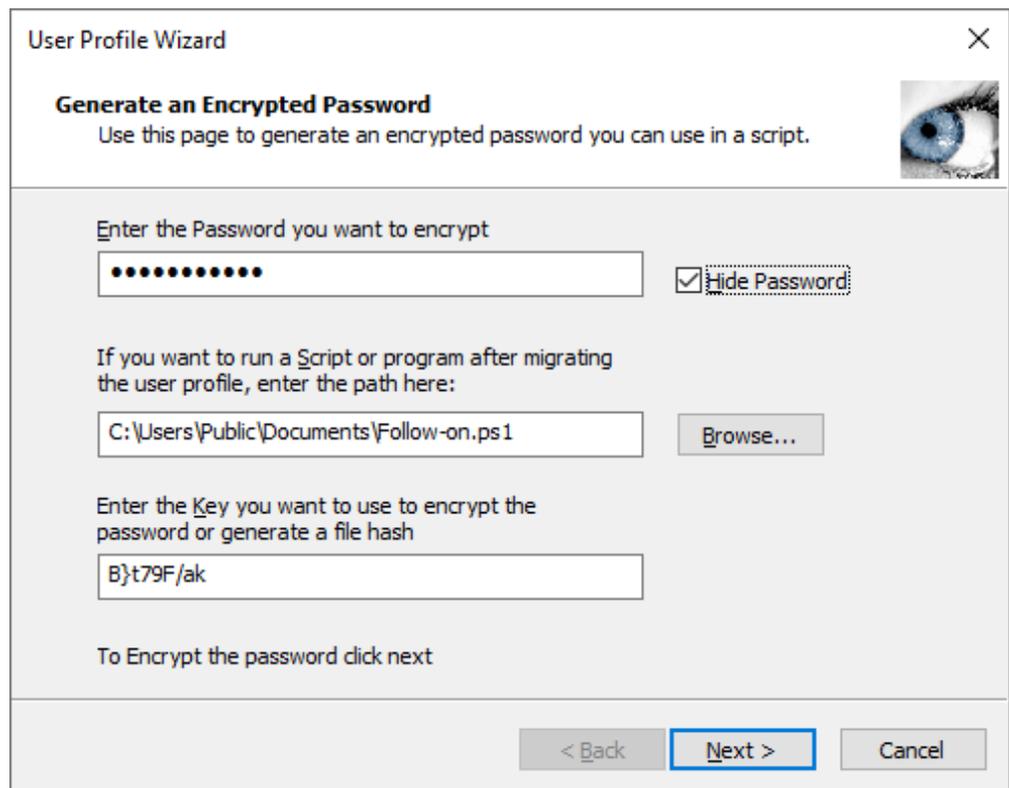
This will bring up the “Generate an Encrypted Password” wizard (see below.)

COMMAND LINE REFERENCE

Enter the plain text password in the “Enter the password” text box.. If you want the User Profile Wizard to run a script or program after the migration is complete, you can enter the path in the text box. For more information see “/HASH” below. Finally, enter a “key” word that User Profile Wizard will use to encrypt and decrypt the password – this should be completely unrelated to the password to stop anyone guessing what the password might be. Click “Next”

The encrypted password is generated in the “encrypted password” window on the next page, and a secure hash of any script or file you want to run is generated in the “file hash” window.

If you are encrypting both a DOMAINADMIN and a LOCALADMIN password, you **must** use the **same** key.



The screenshot shows a dialog box titled "User Profile Wizard" with a close button (X) in the top right corner. The main heading is "Generate an Encrypted Password" with a sub-heading "Use this page to generate an encrypted password you can use in a script." and a small eye icon. The dialog contains three main sections: 1. "Enter the Password you want to encrypt" with a text box containing ten dots and a checked "Hide Password" checkbox. 2. "If you want to run a Script or program after migrating the user profile, enter the path here:" with a text box containing "C:\Users\Public\Documents\Follow-on.ps1" and a "Browse..." button. 3. "Enter the Key you want to use to encrypt the password or generate a file hash" with a text box containing "B)t79F/ak". At the bottom, there is a prompt "To Encrypt the password click next" and three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

/JOIN (Optional)

Join the local machine to the domain even if the profile migration fails.

COMMAND LINE REFERENCE

/NOJOIN (Optional)

Do not join the local machine to the new domain.

/NOMIGRATE (Optional)

If you are performing an enterprise-wide domain migration, you may have some machines that you want to join to your new domain which don't have any profiles you want to migrate. By using the /NOMIGRATE switch you can script the User Profile Wizard to migrate these machines without needing to call on any other tools.

/NODEFAULT (Optional)

Do not set the domain account as the default logon

/DELETE (Optional)

Delete the local account when migration is completed

If LOCALACCOUNT is a user account local to the machine, you can use /DELETE to delete it.

/DISABLE (Optional)

Disable the local account when migration is completed

If LOCALACCOUNT is a user account local to the machine, you can use /DISABLE to disable it.

/SILENT (Optional)

Do not show any error messages

/NOREBOOT (Optional)

Do not automatically reboot the machine after migration.

/REBOOTDELAY seconds (Optional)

Set the number of seconds User Profile Wizard waits before rebooting the machine after it is migrated. During this time a warning is displayed advising the user that their machine needs to reboot. This setting does not apply to remote migrations.

/LOG logfile (Optional)

Write results to a log file.

This is highly recommended. Should you ever need to contact ForensiT Support regarding a migration issue, we will always ask you for your log file.

If you use the /LOG switch without specifying a logfile, a log file will be created in your "My Documents" folder.

/RUNAS (Optional)

If you are performing an enterprise-wide domain migration, there may well be configuration changes you want to make to your workstations which have nothing to do with migrating user profiles or joining the machine to the new domain. It is also almost certain that any configuration changes you do want to make will require local administrator permissions. The User Profile Wizard has a secure mechanism for passing the local administrator account and password via the `/LOCALADMIN`, `/LOCALPWD` and `/KEY` parameters. By using the `/RUNAS` parameter you get User Profile Wizard to securely run any PowerShell script or executable file for you in the security context of a local administrator account.

/HASH (Optional)

Just passing a script or executable to the User Profile Wizard to run is not secure. Scripts might be edited, or executable files replaced by a malicious user wishing to run their own code on a workstation. To stop this happening, you should use the `/HASH` parameter to pass a security hash of the file you want to run.

The security hash guarantees that **only** the file you specify gets run - unchanged. If a script is altered *at all* – even by a single character – the User Profile Wizard will not run it.

To generate a security hash, run the User Profile Wizard with just the `/KEY` parameter and specify the script or executable you want to run. (See above.)

Frequently Asked Questions

This chapter gives answers some commonly asked questions..

What does User Profile Wizard do?

User Profile Wizard migrates your current user profile to your new domain account so that you can keep all your existing data and settings.

What's a profile?

A profile is where Windows keeps all your personal data and settings. Your profile is where your "Documents", "Pictures" and "Music" files are stored, and where your Internet favorites and cookies are kept. Windows keeps track of your personal settings in your profile, like your desktop wallpaper and the lists of documents you've recently opened. Most of the changes you make to personalize your applications are also kept in your profile, as well as files like dictionaries and playlists.

Why migrate profiles when moving to a Windows domain?

As far as Windows is concerned, when you logon to your machine using your domain logon you are a completely different person. Because Windows thinks you're a different person, it sets up a new profile for you and you lose all your personal settings. Not only that, unless your new domain account has Administrator rights on your machine, you lose access to all your data as well. What the User Profile Wizard enables you to do is migrate your original profile with your new domain logon so that you can carry on using your old settings. This is a major benefit to your users. Installing a Windows Domain infrastructure is a major undertaking but, believe it or not, your end users won't be as excited about it as you! All they want to do is get on with their jobs. Using the User Profile Wizard will significantly reduce disruption to your business

Why not just copy the data from the old profile?

Well, you could. But that is going to be a time consuming, labour intensive, not say costly operation. What data do you copy? Even if you copy all your files, what about the

FREQUENTLY ASKED QUESTIONS

configuration information that Windows stores in the registry? Using the User Profile Wizard is just much easier and much less disruptive.

Which version should I buy?

Which version of User Profile Wizard you need depends on how you want to do the migration.

If you want to automate the migration you will need the Corporate Edition. The Corporate Edition of User Profile Wizard is licensed per seat, that is, for each computer you migrate.

User Profile Wizard Professional is licensed per technician and allows you to migrate an unlimited number of machines. However, it does not have the automation features of the Corporate Edition, limiting you to migrating one computer at a time via the GUI. There is a feature comparison here: <http://www.forensit.com/comparison.html>

Will I have to visit every machine on my network to run the Wizard?

Absolutely not. The User Profile Wizard has two distinct modes of operation. You can run the Wizard in graphical mode like all the other Wizards you're familiar with in Windows, but you can also run the User Profile Wizard from a command line. This means that the User Profile Wizard can be run from a PowerShell or VB script, or from a batch file. With the User Profile Wizard Deployment Kit you can build a scalable, enterprise solution, utilizing a single deployment file, to migrate tens of thousands of workstations. Automating User Profile Wizard is only possible if you have the Corporate.

What version of Windows does the User Profile Wizard run on?

The User Profile Wizard is supported on Windows 7, Windows 10 and Windows 11.

Can I use the free Personal Edition in a commercial environment?

Yes. You are welcome to use the free Personal Edition of User Profile Wizard in your business if it meets your needs. The Personal Edition does not have all the features of the Corporate and Professional Editions, of course.

What if I have a problem?

Customers who have purchased the Corporate or Professional Editions should email support@ForensiT.com. Support for the free version of User Profile Wizard is available via the ForensiT Support Forum at <http://forum.forensit.com/>

What *isn't* migrated?

User Profile Wizard cannot migrate encrypted data. This includes encrypted files, but also Internet and Outlook passwords which will need to be re-entered after the migration. This also means that although the personal certificates will be migrated, any private keys will not be.

What about group membership?

When migrating to a domain, the User Profile Wizard automatically adds the new account that will use the profile to the same groups as the local account whose profile you want migrate. This is to help in the migration to the domain. So for example, if your local machine account is a member of the "Power Users" group, the User Profile Wizard will add your domain account to the "Power Users" group. If you are sharing profiles between local accounts, group membership is not affected.

How does User Profile Wizard handle roaming profiles?

User Profile Wizard works with the local copy of any domain profile. If users on the old domain have roaming profiles, a copy of their profile will be held locally on their machine. User Profile Wizard will configure this existing local profile so that it can be used by their new domain account. After the user has logged on with their new domain account (in fact when they first log off) Windows will synchronize the local copy with the domain copy on new domain in the normal way.

Troubleshooting

This chapter discusses some problems occasionally seen when running User Profile Wizard.

Finding Domain Controller Fails/ “The RPC server is unavailable”

SYMPTOMS

When you run the User Profile Wizard, the Wizard reports that it cannot find the domain controller for the domain, or the migration fails because “The RPC server is unavailable”.

RESOLUTION

There is probably a DNS configuration problem. You need rectify the problem so that the Wizard can correctly resolve the new Domain Controller name.

CAUSE

It sometimes happens that a new domain is added to a network without the existing domain (or domains) being reconfigured. Commonly, if there is an existing DNS server, there is no “Forwarders” entry pointing to the DNS server for the new domain.

On Windows Server you can add a new Forwarder entry for the new domain as follows.

1. Run dnsmgmt. (DNS from the "Administrative Tools" menu.)
2. Select the existing DNS server.
3. Select ‘Conditional Forwarders’

TROUBLESHOOTING

4. Right click and select 'New Conditional Forwarder' and add a new Forwarder entry for the new domain.

New Conditional Forwarder

DNS Domain:
target.local

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
✘ 192.168.1.101	TARGETDC	The server with this IP ...

Delete
Up
Down

User '*Name*' not found in lookup file

In order to script and automate migrations (if the user names are changing), the Wizard uses a user lookup csv file to map the old account name to the new as described [here](#).

If there is a problem with the lookup file and the Wizard cannot find the user in the lookup file, the log file will provide information to help identify the problem.

If the log reports;

```
Migrating user account "olduser"  
User 'olduser' not found in lookup file.
```

This indicates that source account name is not found in the user lookup csv file that the Wizard is using, this could be because the user is not present or the formatting or encoding of the file is incorrect.

Please open the User Lookup csv file in Notepad to confirm that there is no additional formatting such as speech / quote marks and that the file is formatted and structured correctly. The file should read;

```
olduser,newuser
```

If this is a migration to Azure, the file should read;

```
olduser,newuser@yourazuredomain.com
```

Where `newname@yourazuredomain.com` is the UPN for the new user that is listed in the Object ID xml file.

Target user not found in Azure Object ID file

This indicates that the target UPN as specified for this user in the user lookup csv file is not present in the Azure Object ID xml file that the Wizard is using.

Please remember that the Azure Object ID xml file lists the accounts for the target / new Azure tenant. Please open the xml file in Notepad and update the user lookup csv file to specify the destination UPN that is present in the xml for this user.

No *DomainName* domain account profiles were found.

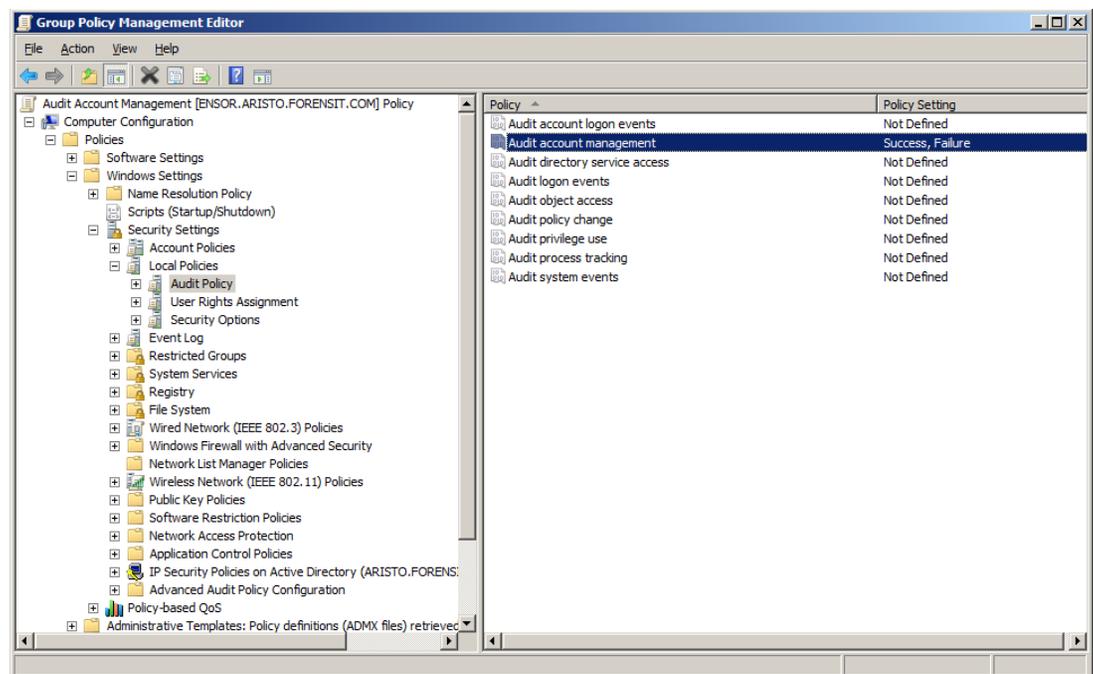
The <OldDomain> name specified in the config file is incorrect (specified on Step 6 of the Deployment Kit).

“azuresync” will generally be correct for migrating from an existing tenant. However, if the tenant is, or has been, linked to an on-premises domain, Windows may be using the on-premises domain name as the tenant name. If you are in any doubt, run **whoami** when signed-in with an old user account, and Windows will return the username in the format *DOMAIN\username*. You need to be using whatever *DOMAIN* is as the existing <OldDomain> name specified on Step 6 of the Deployment Kit.

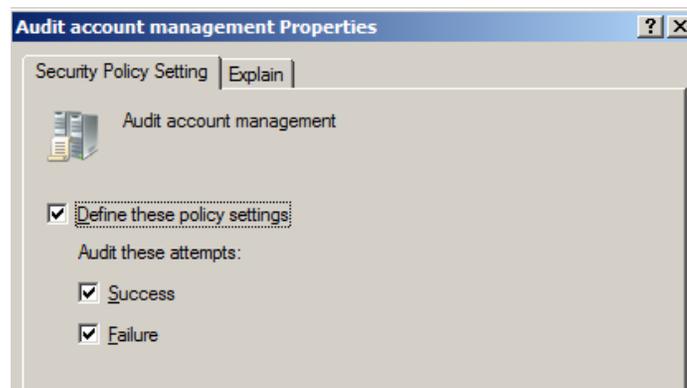
Configuring domains to maintain SID history

Additional configuration is required of both the source and target domains to allow SID history to be maintained across the user's old and new domain accounts. These additional configuration requirements are related to the auditing of the operation to update the SIDHistory attribute on the user account object.

A group policy to enable Audit account management must be created on *both* the source and target domains. The group policy is set under “Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy”



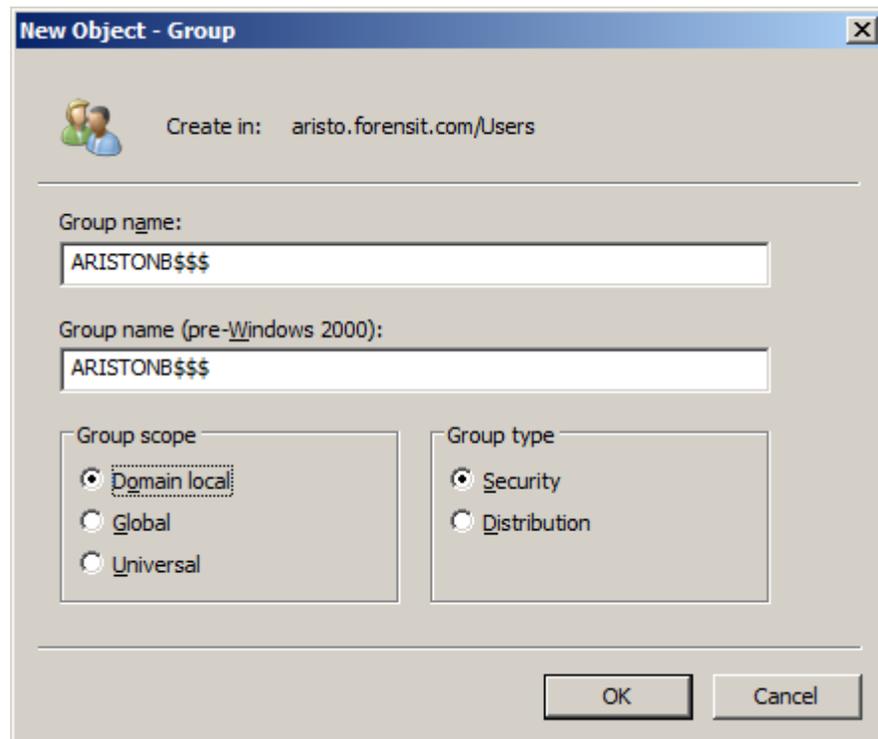
The policy must be defined for both success and failure:



TROUBLESHOOTING

If, after making these policy setting changes, you continue to get an error stating “The operation requires that destination domain auditing be enabled” or “The operation requires that source domain auditing be enabled”, open an elevated command prompt on the appropriate DC and type **gpupdate /force** to apply the GP.

As well as creating the Audit account management group policy, you will also need to create a new “Domain local” group on the source domain. The group must have the name of the source domain appended with ‘\$\$\$’. Here the NetBIOS name of the source domain is ‘ARISTONB’, so the group is called ‘ARISTONB\$\$\$’:



Finally, if you receive an error stating that “The handle is invalid” when migrating an account with sIDHistory, run **regedit** on the source domain PDC and open the “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA” registry key. Create a new DWORD (32-bit) Value called **TcpipClientSupport** and set the value to 1. The DC will need to be restarted for the setting to take effect.

“The security database on the server does not have computer account for this workstation trust relationship”

SYMPTOMS

This error shows up when you try and logon after a machine has been migrated to a new domain.

RESOLUTION

If it is possible, the best solution is to disable the Group Policy setting the DNS suffix in the old domain before the migration; the policy will stay in place until changed.

You can create a Group Policy in the new domain to set the correct DNS suffix, but this may take more than one reboot to take effect.

CAUSE

Generally, this problem occurs where customers set the workstation Primary DNS suffix via a Group Policy: if the Group Policy is not reset for the new domain the error will occur.

The DNS suffix should be set correctly by User Profile Wizard at the end of the migration; it may then be reset again by the (incorrect) Group Policy later. You can check the Primary DNS Suffix by going to System Properties -> “Computer Name” tab -> “Change...” and then “More...” after seeing the error.

End User License Agreement

END-USER LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (an individual or a single entity) and ForensiT for the ForensiT User Profile Wizard software later referred to as the 'SOFTWARE'. By installing, copying, or otherwise using the SOFTWARE, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE.

SOFTWARE LICENSE

The SOFTWARE is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE is licensed, not sold.

1. **GRANT AND TERM OF LICENSE.** ForensiT grants you a personal, non-exclusive, non-transferable and royalty-free right to install and use one copy the SOFTWARE on a single computer (workstation or server) and to make a complete copy of the installed SOFTWARE for backup purposes. This License shall continue in effect until terminated by ForensiT, but shall terminate immediately at any time you fail to comply with the limitations set forth in this License.

2. **DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.** All rights of any kind in the SOFTWARE which are not expressly granted in this License are entirely and exclusively reserved to and by ForensiT. You may not rent, lease, modify, alter, translate, reverse engineer, disassemble, decompile or create derivative works based on the SOFTWARE, or remove any proprietary notices or labels that it contains.

3 **CHANGED TERMS.** ForensiT shall have the right to change or add to the terms of this License at any time and to change, discontinue, or impose conditions on any aspect of the SOFTWARE. Such changes shall be effective upon notification by any means reasonable to give you actual or constructive notice or upon posting of such terms on the SOFTWARE.

4. **NO WARRANTIES.** ForensiT expressly disclaims any warranty for the SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE AND ANY RELATED DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OR CONDITIONS OF ANY

END USER LICENSE AGREEMENT

KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU.

NO LIABILITY FOR DAMAGES. To the maximum extent permitted by applicable law, in no event shall ForensiT or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profit, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of, or inability to use, this ForensiT product, even if ForensiT has been advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you. ForensiT's aggregate liability and that of its suppliers under or in connection with this agreement shall be limited to the amount paid for the software, if any.

5. PUBLICITY. Unless You notify ForensiT otherwise in writing, You hereby grant to ForensiT a limited license to use your trade and business names, trademarks, service marks, logos, domain names and other distinctive brand features (whether registered or not) (collectively, the "Brand Features") in any presentations, marketing materials, customer lists, and financial reports produced for, by or on behalf of ForensiT.

6. GENERAL . This License constitutes the entire agreement between you and ForensiT with respect to the SOFTWARE and supersedes any other agreement written or oral. If any provision of this License is held unenforceable, that provision shall be enforced to the maximum extent permissible so as to give effect the intent of this License, and the remainder of this License shall continue in full force and effect. This License shall be governed by the laws of the United Kingdom.

