Abstract
This guide explains how to use the Active Directory Migration Tool version 3 (ADMT v3) to restructure your operating environment. You can use ADMT v3 to migrate objects between Active Directory forests, between Active Directory domains in the same forest, or from Microsoft® Windows NT® 4.0 source domains to Active Directory. ADMT v3 can also perform security translation from Windows NT 4.0 domains to Active Directory and between different Active Directory forests.
Contents

ADMT v3 Migration Guide ................................................................. 11
Windows NT 4.0 Domain Restructure to an Active Directory Forest ...... 11
Interforest Active Directory Domain Restructure .............................. 12
Intraforest Active Directory Domain Restructure .............................. 12
Terms and Definitions ................................................................ 13
Active Directory Migration Tool ..................................................... 14
Using an Include File ..................................................................... 15
   SourceName Field .................................................................... 16
   TargetName Field ................................................................... 17
   TargetRDN, TargetSAM, and TargetUPN Fields ....................... 17
   Renaming Objects .................................................................... 18
   Using Scripts .......................................................................... 18
Windows NT 4.0 Domain Restructure to an Active Directory Forest ........ 20
Overview of Restructuring Windows NT 4.0 Domains to an Active Directory Forest ......................................................... 20
Process for Restructuring Windows NT 4.0 Domains to an Active Directory Forest ................................................................. 21
Windows NT 4.0 Domain Migration Background Information ....................... 22
Planning to Restructure Windows NT 4.0 Domains to an Active Directory Forest ................................................................. 22
Assign Object Locations and Roles ................................................... 23
Developing a Migration Test Plan ..................................................... 25
Creating a Migration Rollback Plan .................................................. 28
Planning for User Profile Migration ................................................. 29
Establishing Administrative Procedures .......................................... 30
   Administering User Accounts .................................................. 31
   Administering Global Groups .................................................. 31
Creating an End-User Communication Plan .................................... 31
   General Information ............................................................... 31
   Impact .................................................................................. 32
   Logon Status during Migration ............................................... 32
   Premigration Steps ................................................................. 32
Migrating Accounts Without Using SID History .................................................................176
Migration of All User Accounts ........................................................................................178
Translating Security in Add Mode ......................................................................................183
Remigration of User Accounts and Workstations in Batches .............................................187
  Translating Local User Profiles .......................................................................................188
  Migrating Workstations in Batches .................................................................................192
  Remigrating User Accounts in Batches .........................................................................196
  Remigrating All Global Groups Following User Account Migration ............................201
Remigration of All Global Groups After All Batches Are Migrated .................................201
Translating Security in Remove Mode ..............................................................................205
Migrating Resources .......................................................................................................209
Migration of Workstations and Member Servers ............................................................209
Migrating Domain and Shared Local Groups ..................................................................214
Migration of Domain Controllers ...................................................................................218
Completing the Migration ...............................................................................................218
Translating Security on Your Member Servers ...............................................................219
Decommissioning the Source Domain ............................................................................223
Intraforest Active Directory Domain Restructure ............................................................223
Overview of Restructuring Active Directory Domains Within a Forest Using ADMT v3..224
Process for Restructuring Active Directory Domains Within a Forest Using ADMT v3 ..225
Background Information for Restructuring Active Directory Domains Within a Forest
  Using ADMT v3 .............................................................................................................225
  Closed Sets and Open Sets .........................................................................................226
  Users and Groups .......................................................................................................226
  Resources and Local Groups ........................................................................................228
  SID History ................................................................................................................228
Assigning Resource Access to Groups ..........................................................................229
Preparing to Restructure Active Directory Domains Within a Forest .........................229
Evaluate the New Active Directory Forest Structure ................................................... 230
Identify the Source Domains ..................................................................................... 231
Identify and Evaluate the OU Structure of the Target Domain ................................... 231
Assign Domain Object Roles and Locations .............................................................. 231
Plan for Group Migration ......................................................................................... 233
Plan for Test Migrations ......................................................................................... 235
Create a Rollback Plan ............................................................................................. 237
Create an End-User Communication Plan .................................................................. 239
General Information ............................................................................................... 239
Impact ...................................................................................................................... 239
Logon Status During Migration ................................................................................ 239
Premigration Steps ................................................................................................... 240
Expected Changes .................................................................................................... 240
Scheduling and Support Information ........................................................................ 240
Create Migration Account Groups ........................................................................... 240
Install ADMT v3 ....................................................................................................... 242
Prerequisites for Installing ADMT ............................................................................ 242
Installing ADMT Using the Default Database Store ............................................... 243
Installing ADMT Using a Preconfigured SQL Database ....................................... 245
Plan for Service Account Transitioning ..................................................................... 247
Example: Preparing to Restructure Active Directory Domains ................................... 251
Migrating Domain Objects Between Active Directory Domains ................................... 252
Migrate Groups ........................................................................................................ 252
Migrate Universal Groups ......................................................................................... 253
Migrate Global Groups ............................................................................................. 257
Migrate Service Accounts ......................................................................................... 261
Migrate User Accounts ............................................................................................ 266
Migrating OUs and Subtrees of OUs ......................................................................... 267
Migrate Accounts ..................................................................................................... 268
ADMT v3 Migration Guide

As part of deploying Active Directory® directory service, you might choose to restructure your environment. Before doing so, you must determine when and how you want to restructure it. Organizations with an existing domain structure running Microsoft® Windows NT® Server 4.0 might perform an in-place upgrade of some Windows NT 4.0 domains and restructure others. After you deploy Active Directory, you might decide to further reduce the complexity of your environment by either restructuring domains between forests or restructuring domains within a single forest.

You can use the Active Directory Migration Tool version 3 (ADMT v3) to restructure your environment. ADMT can perform object migrations and security translation as necessary, so that users can maintain access to network resources during the restructure process. To download ADMT v3, see http://go.microsoft.com/fwlink/?LinkId=75627.

The following sections briefly explain the main restructure scenarios for using ADMT. After you determine the appropriate scenario for your environment, follow the steps that are provided later in this guide for that scenario.

Note

These guidelines were previously published as part of Designing and Deploying Directory and Security Services in the Windows Server 2003® Deployment Kit (http://go.microsoft.com/fwlink/?LinkId=76005). Designing and Deploying Directory and Security Services explained how to restructure domains within a forest by using the Active Directory Migration Tool (ADMT) version 2. This guide explains how to perform the same process by using ADMT version 3.

Windows NT 4.0 Domain Restructure to an Active Directory Forest

Because of its greater scalability, an Active Directory environment requires fewer domains than a Windows NT 4.0 environment. Instead of performing an in-place upgrade of your Windows NT 4.0 domains, it might be more efficient to consolidate a number of smaller Windows NT 4.0 account and resource domains into a few, larger Active Directory domains.
Interforest Active Directory Domain Restructure

An interforest restructure might be performed for business changes such as mergers or acquisitions. When you migrate objects between forests as part of the restructuring process, both the source and target domain environments exist simultaneously. This enables you to roll back to the source environment during the migration, if necessary.

Important

All target domains must be operating at the Windows 2000 native or Windows Server 2003 functional level.

Intraforest Active Directory Domain Restructure

When you restructure Windows Server 2003 domains in a Windows Server 2003 forest, you can consolidate your domain structure and reduce administrative complexity and overhead. Unlike the process for restructuring Windows Server 2003 domains between forests, when you restructure domains in a forest, the migrated accounts no longer exist in the source domain.

Important

All target domains must be operating at the Windows 2000 native or Windows Server 2003 functional level.

The following table lists the differences between an interforest and an intraforest domain restructure.

<table>
<thead>
<tr>
<th>Migration Consideration</th>
<th>Interforest Restructure</th>
<th>Intraforest Restructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object preservation</td>
<td>Objects are cloned rather than migrated. The original object remains in the source location to maintain user access to resources.</td>
<td>Objects are migrated and no longer exist in the source location.</td>
</tr>
<tr>
<td>SID history maintenance</td>
<td>Maintaining SID history is optional.</td>
<td>SID history is required.</td>
</tr>
<tr>
<td>Password retention</td>
<td>Password retention is optional.</td>
<td>Passwords are always retained.</td>
</tr>
</tbody>
</table>
### Migration Consideration

<table>
<thead>
<tr>
<th>Local profile migration</th>
<th>Interforest Restructure</th>
<th>Intraforest Restructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must use tools such as ADMT to migrate local profiles.</td>
<td></td>
<td>For workstations that run the Microsoft Windows® 2000 Server operating system and later, local profiles are migrated automatically because the user's GUID is preserved. However, you must use tools such as ADMT to migrate local profiles for workstations that run Windows NT 4.0 and earlier.</td>
</tr>
</tbody>
</table>

| Closed sets | You do not need to migrate accounts in closed sets. | You must migrate accounts in closed sets. |

### Terms and Definitions

The following terms apply to the Active Directory domain restructure process.

**Migration** The process of moving or copying an object from a source domain to a target domain, while preserving or modifying characteristics of the object to make it accessible in the new domain.

**Domain restructure** A migration process that involves changing the domain structure of a forest. A domain restructure can involve either consolidating or adding domains, and can take place between forests or in a forest.

**Migration objects** Domain objects that are moved from the source domain to the target domain during the migration process. Migration objects can be user accounts, service accounts, groups, or computers.

**Source domain** The domain from which objects are moved during a migration. When restructuring Active Directory domains between forests, the source domain is an Active Directory domain in a different forest from the target domain.

**Target domain** The domain to which objects are moved during a migration.

**Built-in accounts** Default security groups that have common sets of rights and permissions. You can use built-in accounts to grant permissions to any accounts or groups that you designate as members of these groups. Built-in account security identifiers (SIDs) are identical in every domain and therefore built-in accounts cannot be migration objects.
Active Directory Migration Tool

ADMT allows you to migrate objects in Active Directory forests. It includes wizards that automate migration tasks such as migrating users, groups, service accounts, computers, and trusts, and performing security translation.

You can perform ADMT tasks by using the ADMT console, a command line, or a script. When running ADMT at the command line, it is often more efficient to use an option file to specify command-line options. You can use the ADMT option file reference shown in the listing that follows to assist you in creating option files. Examples of command-line syntax are provided for each task that you must perform to restructure the domains within the forest.

The following listing shows common options that apply to several migration tasks. Each type of migration task has a section that lists options that are specific to that task. The section name corresponds to the task name when you run ADMT at the command line. Items can be commented out with a semicolon. In the following listing, the default values are commented out.

```
[Migration]
;IntraForest=No
;SourceDomain="source_domain_name"
;SourceOu="source_ou_path"

;TargetDomain="target_domain_name"
;TargetOu="target_ou_path"
;PasswordOption=Complex
;PasswordServer=""
;PasswordFile=""
;ConflictOptions=Ignore
;UserPropertiesToExclude=""
;InetOrgPersonPropertiesToExclude=""
;GroupPropertiesToExclude=""
;ComputerPropertiesToExclude=""

[User]
;DisableOption=EnableTarget
;SourceExpiration=None
;MigrateSIDs=Yes
;TranslateRoamingProfile=No
;UpdateUserRights=No
;MigrateGroups=No
;UpdatePreviouslyMigratedObjects=No
;FixGroupMembership=Yes
;MigrateServiceAccounts=No
;UpdateGroupRights=No

[Group]
;MigrateSIDs=Yes
```
When running ADMT at the command line, you do not need to include an option in your command if you want to accept the default value. In this guide, however, tables that list possible parameters and values are provided for reference. The tables list the command-line equivalent of each option that is shown in the corresponding ADMT console procedure, including those where you accept the default value.

You can copy the option file reference into Notepad and save it by using a .txt file name extension.

As an example, to migrate a small number of computers, you might type each computer name at the command line, using the /N option, and then list other migration options within an option file as follows:

```
ADMT COMPUTER /N "computer_name1" "computer_name2" /O:"option_file.txt"
```

`computer_name1` and `computer_name2` are the names of computers in the source domain that you are migrating in this batch.

**Using an Include File**

When you migrate a large number of users, groups, or computers, it is more efficient to use an include file. An include file is a text file in which you list the user, group, and computer objects that you want to migrate, with each object on a separate line. You must use an include file to rename objects during the migration.

You can list users, groups and computers together in one file or you can create a separate file for each object type. Then specify the include file name with the /F option, as follows:
To specify the names of users, groups, or computers, use one of the following conventions:

- The Security Accounts Manager (SAM) account name. To specify a computer name in this format, you must append a $ to the computer name. For example, to specify a computer with the name Workstation01, use Workstation01$.

- The Windows NT 4.0 account name. This includes the domain name and the SAM account name. For example, the Windows NT 4.0 account name of a computer named Workstation01 that is in the Asia domain is Asia\Workstation01$.

- The relative distinguished name (also known as RDN). For example, cn=Workstation01. If you specify the account as a relative distinguished name, you must specify the source organizational unit (OU).

- The canonical name. This can be specified as DNS domain name/ou_path/object_name, or ou_path/object_name; for example, Asia.trccorp.treyresearch.net/Computers/Workstation01 or Computers/Workstation01.

The following sections describe the fields of an include file and provide examples for each:

**SourceName Field**

The *SourceName* field specifies the name of the source object. You can specify either an account name or a relative distinguished name. If you only specify source names, it is optional to define a header on the first line in the file.

The following example illustrates a header line that specifies the *SourceName* field. The example also shows a source object name that is specified in several formats. The second line specifies an account name. The third line specifies an account name in Windows NT 4.0 account name format. The fourth line specifies a relative distinguished name.

```
SourceName
name
domain\name
CN=name
```
TargetName Field

The TargetName field can be used to specify a base name that is used to generate a target relative distinguished name, a target SAM account name, and a target user principal name (UPN). The TargetName field cannot be combined with other target name fields discussed later in this section.

\[\text{Note}\]

The target UPN is only generated for user objects, and only a UPN prefix is generated. A UPN suffix is appended using an algorithm that is dependent upon whether a UPN suffix is defined for the target OU or target forest. If the object is a computer, the target SAM account name includes a "$" suffix.

The following example of input generates the target relative distinguished name, target SAM account name, and target UPN as "CN=newname", "newname" and "newname" respectively.

SourceName,TargetName
oldname, newname

TargetRDN, TargetSAM, and TargetUPN Fields

You can use the TargetRDN, TargetSAM, and TargetUPN fields to specify the different target names independently of each other. You can specify any combination of these fields in any order.

TargetRDN specifies the target relative distinguished name for the object.

TargetSAM specifies the target SAM account name for the object. For computers, the name must include a "$" suffix to be a valid SAM account name for a computer.

TargetUPN specifies the target UPN for the object. You can specify either just the UPN prefix or a complete UPN name (prefix@suffix). If the name that you specify contains a space or a comma, you must enclose the name in double quotation marks (" ").

SourceName,TargetRDN
oldname, CN=newname

SourceName,TargetRDN,TargetSAM
oldname, "CN=New RDN", newsamname

SourceName,TargetRDN,TargetSAM,TargetUPN
oldname, "CN=last, first", newsamname, newupnname

\[\text{Note}\]

A comma within the CN value must be preceded with an escape (\") character or the operation will fail, and ADMT will record an invalid syntax error in the log file.
SourceName, TargetSAM, TargetUPN, TargetRDN

oldname, newsamname, newupnname@targetdomain, "CN=New Name"

Renaming Objects

Use the following format in an include file to rename computer, user, or group objects during migration:

- Use SourceName, TargetRDN, TargetSAM, and TargetUPN as column headings at the top of the include file. SourceName is the name of the source account, and it must be listed as the first column heading. The TargetRDN, TargetSAM, and TargetUPN column headings are optional, and you can list them in any order.
- You must specify the account name as user name, relative distinguished name, or canonical name. If you specify the account name as a relative distinguished name, you must also specify the source OU.

The following are examples of valid include files in which the rename option is used:

SourceName, TargetSAM

abc, def

This include file entry changes the TargetSAM account name for user "abc" to "def." The TargetRDN and the TargetUPN, which are not specified in this include file, do not change as a result of the migration.

SourceName, TargetRDN, TargetUPN

abc, CN=def, def@contoso.com

This include file entry changes the TargetRDN for user abc to CN=def and the TargetUPN to def@contoso.com. The TargetSAM for user abc does not change as a result of the migration.

⚠️ Important

You must specify CN= before using an RDN value.

Using Scripts

The sample scripts provided in this guide reference the symbolic constants that are defined in a file named AdmConstants.vbs. The listing that follows shows the ADMT constants Microsoft Visual Basic® Scripting Edition (VBScript) file. The constants are also provided in the ADMT installation folder, in the TemplateScript.vbs file, in the %systemroot%\WINDOWS\ADMT directory.
To use the sample scripts in the guide, copy the ADMT constants VBScript file into Notepad, and save it as AdmtConstants.vbs. Be sure to save it in the same folder where you plan to save the sample scripts that are provided in this guide.

<table>
<thead>
<tr>
<th>Option Explicit</th>
</tr>
</thead>
<tbody>
<tr>
<td>' ADMT Scripting Constants</td>
</tr>
<tr>
<td>' PasswordOption constants</td>
</tr>
<tr>
<td>Const admtComplexPassword = &amp;H0001</td>
</tr>
<tr>
<td>Const admtCopyPassword = &amp;H0002</td>
</tr>
<tr>
<td>Const admtDoNotUpdatePasswordsForExisting = &amp;H0010</td>
</tr>
<tr>
<td>' ConflictOptions constants</td>
</tr>
<tr>
<td>Const admtIgnoreConflicting = &amp;H0000</td>
</tr>
<tr>
<td>Const admtMergeConflicting = &amp;H0001</td>
</tr>
<tr>
<td>Const admtRemoveExistingUserRights = &amp;H0010</td>
</tr>
<tr>
<td>Const admtRemoveExistingMembers = &amp;H0020</td>
</tr>
<tr>
<td>Const admtMoveMergedAccounts = &amp;H0040</td>
</tr>
<tr>
<td>' DisableOption constants</td>
</tr>
<tr>
<td>Const admtLeaveSource = &amp;H0000</td>
</tr>
<tr>
<td>Const admtDisableSource = &amp;H0001</td>
</tr>
<tr>
<td>Const admtTargetSameAsSource = &amp;H0000</td>
</tr>
<tr>
<td>Const admtDisableTarget = &amp;H0010</td>
</tr>
<tr>
<td>Const admtEnableTarget = &amp;H0020</td>
</tr>
<tr>
<td>' SourceExpiration constant</td>
</tr>
<tr>
<td>Const admtNoExpiration = -1</td>
</tr>
<tr>
<td>' Translation Option</td>
</tr>
<tr>
<td>Const admtTranslateReplace = 0</td>
</tr>
<tr>
<td>Const admtTranslateAdd = 1</td>
</tr>
<tr>
<td>Const admtTranslateRemove = 2</td>
</tr>
<tr>
<td>' Report Type</td>
</tr>
<tr>
<td>Const admtReportMigratedAccounts = 0</td>
</tr>
<tr>
<td>Const admtReportMigratedComputers = 1</td>
</tr>
<tr>
<td>Const admtReportExpiredComputers = 2</td>
</tr>
<tr>
<td>Const admtReportAccountReferences = 3</td>
</tr>
<tr>
<td>Const admtReportNameConflicts = 4</td>
</tr>
<tr>
<td>' Option constants</td>
</tr>
</tbody>
</table>
Restructuring Windows NT 4.0 domains to an Active Directory forest involves migrating the contents of a number of Windows NT 4.0 domains into a smaller number of Active Directory domains. By restructuring your environment to an Active Directory forest, you can take advantage of new and enhanced Active Directory features, while reducing the complexity of your organization and the associated administrative costs.

Overview of Restructuring Windows NT 4.0 Domains to an Active Directory Forest

If you are upgrading from Windows NT 4.0 domains to an Active Directory forest, you can consolidate your existing account and resource domains by restructuring them into a smaller number of larger Active Directory domains. You can restructure Windows NT 4.0 domains into Active Directory domains running the Microsoft Windows 2000 Server operating system or Microsoft Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition operating systems.

Before you begin to restructure your Windows NT 4.0 domains, ensure that your organization has designed an Active Directory logical structure and a site topology. In a Windows 2000 Server environment, ensure that any domains that you plan to use as target domains are operating in Windows 2000 native mode. In a Windows Server 2003 environment, ensure that for any domains that you plan to use as target domains, you have raised the Active Directory domain functional level to Windows 2000 native or Windows Server 2003.
For more information about performing an in-place upgrade of Windows NT 4.0 domains, see Upgrading Windows NT 4.0 Domains to Windows Server 2003 Active Directory ([http://go.microsoft.com/fwlink/?LinkId=76027](http://go.microsoft.com/fwlink/?LinkId=76027)).

After the restructuring process is complete, you can take advantage of the features available in Active Directory. By consolidating multiple Windows NT 4.0 account and resource domains into a single or a few Active Directory domains, you can create an Active Directory domain structure that is more efficient than your existing Windows NT 4.0 domain structure.

### Process for Restructuring Windows NT 4.0Domains to an Active Directory Forest

Restructuring Windows NT 4.0 domains to an Active Directory forest involves completing the necessary planning and preparation tasks in the appropriate order, and then migrating Windows NT 4.0 accounts and resources to an Active Directory domain or domains.

The following figure shows the process for restructuring Windows NT 4.0 domains to an Active Directory forest.
Windows NT 4.0 Domain Migration
Background Information

Restructuring Windows NT 4.0 domains involves migrating user, group, and computer objects from a Windows NT 4.0 account or resource source domain into an Active Directory target domain. The target domain can either be a newly created Active Directory domain or a Windows NT 4.0 domain that has had an in-place upgrade.

After the migration process is complete, clients can log on to the original Windows NT 4.0 domain or the new Active Directory domain for authentication. Clients can also access resources in either the source or the target domain, until the source domain is decommissioned.

To successfully consolidate Windows NT 4.0 account and resource domains into Active Directory domains, it is important to be familiar with the capabilities of both operating systems in the context of restructuring. You must also be familiar with the tools that support object migrations.

The migration process between forests is considered to be non-destructive because the migration objects continue to exist in the source domain until the source domain is decommissioned. Because a Windows NT 4.0 domain cannot be part of an Active Directory forest, when objects are migrated from a Windows NT 4.0 domain to an Active Directory domain, they are copied from the source domain to the target domain. The source account primary security identifier (SID) can be maintained in the SID history of the object. You can use the Active Directory Migration Tool (ADMT) version 3 or a third-party restructuring tool to restructure domains.

For more information about domain migration, SIDs, and SID history, see Domain Migration Cookbook (http://go.microsoft.com/fwlink/?LinkId=77370).

Planning to Restructure Windows NT 4.0 Domains to an Active Directory Forest

Planning your domain restructure involves:

- Assigning object locations and roles.
- Creating a test plan.
- Creating a rollback plan for use if the migration fails.
- Planning for user profile migration.
• Establishing administrative procedures to ensure that users can continue to log on to the network and access resources during the migration.

• Creating an end-user communication plan.

The following figure shows the planning steps associated with restructuring Windows NT 4.0 domains to an Active Directory forest.

---

Assign Object Locations and Roles

Large organizations are likely to be migrating thousands of user, group, and resource objects from numerous Windows NT 4.0 domains to Active Directory domains. It is important to keep track of these objects by assigning them roles and locations in the target domain. It is useful to document the assignments for all of the objects that you are migrating in object assignment worksheets.

Create one worksheet for account objects, such as users, groups, and service accounts, and one worksheet for resource objects, such as workstations, profiles, and domain controllers. In your worksheets, list the source and target locations for all objects to be migrated. For information about identifying service accounts to be migrated, see Service Account Identification, later in this guide.
Note

Built-in accounts (such as Administrators, Users, and Power Users) and well-known accounts (such as Domain Admins and Domain Users) cannot be ADMT migration objects.

For a worksheet to assist you in documenting account object assignments, see "User and Group Object Assignment Table — Windows NT 4.0 Source" (DSSRENT_1.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink?LinkId=14384).

The following figure shows an example of a completed worksheet for assigning user and group objects.

<table>
<thead>
<tr>
<th>User and Group Object Assignment Table - Windows NT 4.0 Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepared By</td>
</tr>
<tr>
<td>Source Domain Name</td>
</tr>
<tr>
<td>Target Domain Name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Source Location</th>
<th>Target Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Group</td>
<td>Boston domain</td>
<td>east\Boston Groups OU</td>
</tr>
<tr>
<td>Accounting</td>
<td>Group</td>
<td>Boston domain</td>
<td>east\Boston Groups OU</td>
</tr>
<tr>
<td>JBrown</td>
<td>User</td>
<td>Boston domain</td>
<td>east\Boston Users OU</td>
</tr>
<tr>
<td>MiNguyen</td>
<td>User</td>
<td>Boston domain</td>
<td>east\Boston Users OU</td>
</tr>
<tr>
<td>!Scheduler</td>
<td>Service Account</td>
<td>Boston domain</td>
<td>east\Service Accounts OU</td>
</tr>
</tbody>
</table>

Creating a resource object assignment worksheet also involves identifying the target organizational unit (OU) for each object and noting the physical location and role in the target domain. For a worksheet to assist you in documenting resource object assignments, see "Resource Object Assignment Table — Windows NT 4.0 Source" (DSSRENT_2.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink?LinkId=14384).
Developing a Migration Test Plan

ADMT v3 does not include a test migration option which was available in previous versions of ADMT. Develop a test plan to assist you in systematically testing each object after it is migrated to the new environment, and identifying and correcting any problems that might occur. Testing to verify that your migration is successful helps ensure that users who are migrated from the source domain to the target domain can:

- Log on.
- Access resources based on group membership.
- Access resources based on user credentials.

Testing also helps ensure that users are able to access the resources that you migrate.
After your testing is complete, you can proceed with migrating small pilot groups and then gradually increase the size of each batch of migration objects in your production environment.

Use the following process to test the migration of your account object and resource objects:

1. Create a test user in the source domain. Include this test user with your migrations.
2. Join that user to the appropriate global groups to enable resource access.
3. Log on to the source domain as the test user, and verify that you can access resources as appropriate.
4. After you translate the user profile, migrate the workstation of the user, migrate the user account, log on to the target domain as the test user, and verify that the user has retained all necessary access and functionality. For example, you might test to verify that:
   - The user can log on successfully.
   - The user has access to all appropriate resources, such as file and print shares; access to services such as messaging; and access to line-of-business applications. It is especially important to test access to internally developed applications that access database servers.
   - The user profile was successfully translated, and the user retains desktop settings, desktop appearance, shortcuts, and access to the My Documents folder. Also, verify that applications appear in and start from the Start menu.

   **Note**
   You cannot migrate every user property when you migrate user accounts. For more information about user properties that cannot be migrated, see Migrate User Accounts, later in this guide.

After you migrate resources, log on as the test user in the target domain, and verify that you can access resources as appropriate.

If any steps in the test process fail, identify the source of the problem, and determine whether you can correct the problem before the object needs to be accessible in the target domain. If you cannot correct the problem before access to the object is required, roll back to your original configuration to ensure access to the user or resource object. For more information about creating a rollback plan, see Creating a Rollback Plan, later in this guide.

As part of your test plan, create a migration test matrix. Complete a test matrix for each step that you complete in the migration process. For example, if you migrate 10 batches of users, complete the test matrix 10 times, once for each batch that you migrate. If you migrate 10 member servers, complete the test matrix for each of the 10 servers.
For a worksheet to assist you in creating a test matrix, see Migration Test Matrix (DSSREER_3.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink?LinkId=14384).

The following figure shows an example of a completed migration test matrix.

<table>
<thead>
<tr>
<th>Migration Test Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepared By</strong></td>
</tr>
<tr>
<td><strong>Source Forest Name</strong></td>
</tr>
<tr>
<td><strong>Target Forest Name</strong></td>
</tr>
<tr>
<td><strong>Source Domain Name</strong></td>
</tr>
<tr>
<td><strong>Target Domain Name</strong></td>
</tr>
<tr>
<td><strong>Test Name</strong></td>
</tr>
<tr>
<td>Create test user for users in Sales department &quot;batch&quot;</td>
</tr>
<tr>
<td>Join user to sales group</td>
</tr>
<tr>
<td>Log on to source domain and verify access to required resources</td>
</tr>
<tr>
<td>Log on to target domain</td>
</tr>
<tr>
<td>Verify access to file and print shares</td>
</tr>
<tr>
<td>Verify access to customer management application</td>
</tr>
<tr>
<td>Verify user desktop settings and access to My Documents Folder</td>
</tr>
<tr>
<td>Verify that applications appear and start from the Start menu</td>
</tr>
</tbody>
</table>
Creating a Migration Rollback Plan

Reduce the risk of disrupting end users in your organization by establishing a rollback plan. In general, it is possible to isolate and resolve any problems that occur during each phase of the migration. However, it is important to analyze potential risks and identify the levels of user impact and downtime that might necessitate rolling back the migration. You might be required to roll back your migration if any of the following occur:

- Users cannot log on to their accounts after migration.
- Users cannot access resources after migration.
- User migration is incomplete; for example, passwords did not migrate.
- User migration was successful, but user workstation migration or local profile translation failed.

If user impact or downtime reaches a level that you have defined as unacceptable in your organization, you can implement your rollback plan and continue to operate in your premigration environment. Because the source domain remains intact during the restructure, you can restore the original environment by completing a few key steps.

To roll back to the premigration environment after migrating account objects:

1. Enable the user accounts in the source domain (if you disabled the accounts during the migration process).
2. Notify the users to log off from the target domain.
3. Notify the users to log on to the source domain.
4. Verify that users are able to access resources.
5. Verify that the logon scripts and user profiles for users work as configured in the source domain.

The rollback process for resource objects is similar to that for account objects. To roll back to the premigration environment after migrating resource objects:

1. Change the domain membership for the server or workstation to the source domain.
2. Restart the server or workstation.
3. Log on as a user, and verify that you can access the resource.

Note

If you need to modify objects such as member servers or domain controllers in order to migrate them to the target domain, back up all the data before making the modifications and performing the migration.
Planning for User Profile Migration

User profiles store user data and information about the user’s desktop settings. User profiles can either be roaming or local, and the migration process differs slightly for each. Profiles are translated during the migration process. Only the primary security identifier (SID) is used to assign a profile to a user; SIDs in SID history are ignored. If you translate profiles in add mode, the user accounts in the target and the source domains have access to the profile. In this way, if you roll the user account back to the source domain, the user account in the source domain can use the profile. If you translate profiles in replace mode, you must retranslate the profile by using a SID mapping file to restore the environment to the premigration state.

⚠️ Important

If you need to roll back to your original configuration, notify users that profile changes made in the target domain are not reflected in the source domain.

Some organizations might choose not to migrate user profiles. Other organizations might choose to replace users’ workstations during the user account migration process, and use a tool such as the User State Migration Tool (USMT) to migrate user data and settings to the users’ new computers. The following table summarizes the migration requirements for user profiles.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Migration Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roaming profiles</td>
<td>User profiles are stored centrally on servers. Profiles are available to the user, regardless of the workstation in use.</td>
<td>Select the Translate roaming profiles option on the User Options page in the User Account Migration Wizard. Then, translate local user profiles for a batch of users immediately after you migrate those users.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
<td>Migration Requirements</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local profiles</td>
<td>User profiles are stored locally on the workstation. When a user logs on to another workstation, a unique local user profile is created.</td>
<td>Translate local profiles as a separate step from the user account migration process. Select the User profiles option on the Translate Objects page of the Security Translation Wizard. Translate local user profiles for a batch of users immediately after migrating those users.</td>
</tr>
<tr>
<td>Profiles not managed</td>
<td>Same as local profiles.</td>
<td>Users lose their existing profiles when their user accounts are migrated.</td>
</tr>
<tr>
<td>Hardware refresh</td>
<td>User state information is stored locally on the workstation.</td>
<td>Migrate as a separate step from the user account migration. Migrate the profiles to the user’s new computer by means of a tool such as USMT.</td>
</tr>
</tbody>
</table>

**Establishing Administrative Procedures**

You must define how the objects that you are migrating are to be administered during the restructure process. By establishing administrative procedures for migration objects, you can preserve the objects both in the source and the target domains. Consequently, you can fall back to the premigration environment, if the restructure process is not successful.

Plan for the administration and management of the following types of account migration objects:

- User accounts, including SIDs
- Global group memberships
Administering User Accounts

During the migration process, user accounts exist in both the source and the target domains. Continue to administer the accounts in the source domain while the migration is taking place. Use the **Migrate and merge conflicting objects** option in ADMT to remigrate user accounts as often as necessary during the migration process. This ensures that changes made to the account in the source domain are propagated to the account in the target domain. This operation merges the existing account and the new account, so that administration of the object can continue in the source domain for the duration of the migration process.

Administering Global Groups

Continue to administer the groups in the source domain during the migration process. Remigrate groups as often as necessary by using the **Migrate and merge conflicting objects** option in ADMT. This ensures that changes made to group membership in the source domain are propagated to the group in the target domain.

Creating an End-User Communication Plan

Develop a plan to inform all affected users about the upcoming account migration, to ensure that they understand their responsibilities, the impact of the migration, and who to contact for help and support.

Before you begin the user migration process, send a notice to all users who are scheduled to be migrated. Because you typically migrate users in batches of approximately one hundred users at a time, it is also helpful to send a final notice to the users in each batch two to three days before their batch is scheduled. If your organization maintains an intranet, publish the account migration schedule and the information contained in the user mail on an easily accessible Web page.

Include the following information in your end-user communication.

**General Information**

Alert users to the fact that their user accounts are scheduled to be migrated to a new domain. Point users to a Web page or internal resource where they can find additional information, and view a migration schedule.
Inform users of their new domain name. Be sure to let them know that their account passwords will not change. Let users know that the original domain account will be disabled immediately following the migration, and the disabled account will be deleted after a specified period of time. This is not needed if they log on with user principal names (UPNs).

**Impact**

Make sure that users understand that when their account is migrated, they might be unable to access some resources, such as Web sites, shared folders, or resources that individuals in their group or division do not widely use.

Provide information to users about whom to contact for assistance in regaining access to required resources.

**Logon Status during Migration**

Make sure that users understand that during the migration process, they will be unable to log on to the domain or access e-mail or other resources. Be sure to specify the period of time for which they will be unable to log on.

**Premigration Steps**

Alert users to any steps that they need to complete before the migration process begins. For example, they must decrypt files encrypted by means of Encrypting File System (EFS). Failure to decrypt encrypted files will result in loss of access to encrypted files following the migration.

Users must also ensure that their computers are connected to the network when their account is scheduled to be migrated.

**Expected Changes**

Describe other changes that users can expect to experience following the migration, such as changes in use of smart cards, secure e-mail, or instant messaging if applicable.

**Scheduling and Support Information**

Provide information about where users can go to find more information; for example, an internal Web site where you post information about the migration. Also, provide information about whom to contact if a user has a conflict with the date scheduled for the migration.
Preparing the Source and Target Domains for Restructuring

Before you restructure your Windows NT 4.0 domains, ensure that your target domains are set to a mode or functional level that supports restructuring. In a Windows 2000 Server environment, the target domains must be operating in Windows 2000 native mode. In a Windows Server 2003 environment, the target domains must be at the Windows 2000 native or Windows Server 2003 Active Directory domain functional level.

The following figure shows the steps involved in preparing the source and target domains for restructuring.

- Plan to restructure Windows NT 4.0 domains to an Active Directory forest
- Prepare the source and target domains for restructuring
- Restructure account domains
- Restructure resource domains
- Install high encryption software
- Establish required trusts
- Establish migration accounts
- Configure the source and target domains to migrate SID history
- Configure the target OU structure for administration
- Install ADMT
- Identify service accounts
Installation of High Encryption Software

ADMT includes the Password Export Server (PES) service to securely copy account passwords from the source domain to the target domain. When you are migrating accounts and passwords between domains, one source domain controller must have the PES service installed and configured. If you are migrating passwords, both the computer on which ADMT is installed in the target domain and the PES service in the source domain require 128-bit high encryption.

Note

Installing high encryption in a Windows NT 4.0 domain does not affect the ability of domain controllers to replicate, nor does it affect the user logon process or users' access to resources.

This encryption is standard on domain controllers running Windows Server 2003 or Windows 2000 Server Service Pack 3 (SP3) or later. If you plan to install ADMT on a computer that does not support 128-bit high encryption by default, install the 128-bit high encryption pack from Windows 2000 High Encryption Pack (http://go.microsoft.com/fwlink/?LinkId=76037).

For the PES in the Windows NT 4.0 source domain, install the 128-bit high encryption pack from Internet Explorer High Encryption Pack 4.0 (http://go.microsoft.com/fwlink/?LinkId=76038).

Important

The high encryption pack exists for North America Windows NT 4.0 Service Pack 6a. If you need high encryption on an international Windows NT 4.0 domain controller, you need to install Microsoft Internet Explorer® 4.1 or later and the high encryption pack for this Internet Explorer version.

Establishing Required Trusts

Before you can migrate accounts and resources from a Windows NT 4.0 source domain to an Active Directory target domain, you must ensure that the appropriate external trusts are in place. Trust relationships between the domains enable ADMT to migrate objects and translate local user profiles from the source to the target domains. In addition, depending on how trust relationships are configured, users in the source domains can access resources in the target domains. Moreover, users in the target domains can access resources in source domains that have not yet been migrated.
To migrate users and global groups, you must establish a one-way trust between the Windows NT 4.0 source account domain and the target domain, so that the source domain trusts the target domain.

To migrate resources or translate local profiles, you must do one of the following:

- Create a one-way trust between the source resource domain and the target domain, so that the source resource domain trusts the target domain. Migrated users in the target domain can access resources in source resource domains that have not yet been migrated.
- Create a two-way trust between the source resource domain and the target domain. Users that have been migrated to the target domain can access resources in the source domain.

For more information about creating trusts, see Creating Domain and Forest Trusts (http://go.microsoft.com/fwlink/?LinkId=77381).

### Establishing Migration Accounts

To migrate accounts and resources between forests, you must establish migration accounts and assign the appropriate credentials to those accounts. ADMT uses the migration accounts to migrate the objects that you identify. Because ADMT requires only a limited set of credentials, creating separate migration accounts enables you to simplify administration. If the migration tasks for your organization are distributed across more than one group, it is helpful to create a migration account for each group involved in performing the migration.

To simplify administration, create a single account in the source domain and a single account in the target domain for all objects. Include the credentials that are required to modify the objects that the account will migrate. These objects include users, global groups, and local profiles. For example, suppose you have a migration account that you use to migrate the following:

- User accounts with SID history
- Global groups with SID history
- Computers
- User profiles

This account must have the following credentials:

- Local administrator or domain administrator credentials in the source domain
- Delegated permission on the user, group, and computer OUs in the target domain, with the extended right to migrate SID history on the user OU
• Local administrator on the computer in the target domain on which ADMT is installed

A migration account that you use to migrate workstations and domain controllers must have local administrator or domain administrator credentials on the workstations in the source domain. Otherwise, the account must have domain administrator credentials on the domain controller, or both.

In the target domain, it is necessary to use an account that has delegated permission on the computer OU and the user OU. You might want to use a separate account for the migration of workstations, if this migration process is delegated to administrators that are in the same location as the workstations.

The following table lists the credentials that are required in the source and target domains for different migration objects.

<table>
<thead>
<tr>
<th>Migration Object</th>
<th>Credentials Necessary in Source Domain</th>
<th>Credentials Necessary in Target Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>User/Group with SID history</td>
<td>Local administrator or domain administrator</td>
<td>Delegated permission on the user OU or the group OU, extended permission to migrate SID history, and local administrator on the computer on which ADMT is installed.</td>
</tr>
<tr>
<td>Computer</td>
<td>Domain administrator or local administrator in the source domain and local administrator on each computer</td>
<td>Delegated permission on the computer OU and local administrator on the computer on which ADMT is installed.</td>
</tr>
<tr>
<td>Profile</td>
<td>Local administrator or domain administrator</td>
<td>Delegated permission on the user OU and local administrator on the computer on which ADMT is installed.</td>
</tr>
</tbody>
</table>

The following procedures provide examples for creating groups or accounts to migrate accounts and resources. Procedures differ according to whether a one-way trust or a two-way trust exists. The procedure for creating migration groups when a one-way trust exists is more complex than the procedure for when a two-way trust exists. This is
because, with a one-way trust, you must add the migration group to the local Administrators group on local workstations.

The sample procedure for creating migration groups when a one-way trust exists involves creating separate groups for migrating accounts and resources; however, you can combine `acct_migrators` and `res_migrators` into one group, if you do not need to separate them to delegate different sets of permissions.

To create an account migration group when a one-way trust exists in which the source domain trusts the target domain

1. In the target domain, create a global group called `acct_migrators`.
2. In the target domain, add the `acct_migrators` group to the Domain Admins group, or delegate administration of OUs that are targets for account migration to this group.
3. If you are migrating SID history, and you did not place the `acct_migrators` group in the Domain Admins group, grant the `acct_migrators` group the Migrate SID History extended permission on the target domain object. To do this:
   a. Start Active Directory Users and Computers, right-click the domain object, and then click Properties.
   b. Click the Security tab, click Add, and then select `acct_migrators`.
      If the Security tab does not appear, in Active Directory Users and Computers, click View, and then click Advanced Features.
   c. In the Permissions for `acct_migrators` box, click Allow for the Migrate SID History permission.
4. In the source domain, add the `acct_migrators` group to the Administrators group.
5. On each computer on which you plan to translate local profiles, add the `acct_migrators` group to the local Administrators group.

To create a resource migration group when a one-way trust exists in which the source domain trusts the target domain

1. In the target domain, create a global group called `res_migrators`.
2. In the target domain, add the `res_migrators` group to the Domain Admins group, or delegate administration of OUs that are targets for resource migration to this group.
3. In the source domain, add the `res_migrators` group to the Administrators group.
4. On each computer that you plan to migrate or on which you plan to perform security translation, add the `res_migrators` group to the local Administrators group.
To create a resource migration account when a two-way trust exists between the source and target domains

1. In the source domain, create an account called res_migrator.
2. In the source domain, add the res_migrator account to the Domain Admins group. (The Domain Admins group is a member of the local Administrators group on every computer in the domain by default; therefore, you do not need to add it to the local Administrators group on every computer.)
3. In the target domain, delegate permissions on OUs that are targets for resource migration to the res_migrator account.

ADMT v3 also includes database administration roles that you can use to assign a subset of database permissions to users who perform specific migration tasks. The database administration roles and the migration tasks that they can perform are listed in the following table.

<table>
<thead>
<tr>
<th>Role</th>
<th>Migration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account migrators</td>
<td>Account migration tasks, such as user and group migration.</td>
</tr>
<tr>
<td>Resource migrators</td>
<td>Resource migration tasks, such as computer migration and security translation. Account migrators also hold the role of resource migrators.</td>
</tr>
<tr>
<td>Data readers</td>
<td>Queries against that database. Account migrators and resource migrators also hold the role of data readers.</td>
</tr>
</tbody>
</table>

Users who are assigned the role of SQL Server sysadmin hold all ADMT database administration roles. They have permissions to do the following:
- Display database roles and users who hold those roles
- Add groups or users to roles
- Remove groups or users from roles

By default, the local Administrators group is assigned the role of sysadmin and can perform all ADMT database functions.

For more information about using database administrator roles, see "Configure Database Administration Roles" in ADMT v3 Help.
Configuring the Source and Target Domains to Migrate SID History

You can manually configure the source and target domains to migrate SID history before you begin the migration, or you can allow ADMT to configure them automatically the first time that it runs.

To configure the source and target domains manually, complete the following procedures, so that the source and target domains are configured to migrate SID history from a Windows NT 4.0 domain:

- Create a local group in the Windows NT 4.0 source domain to support auditing.
- Enable TCP/IP client support on the source domain PDC.
- Enable auditing in the Active Directory target domain.
- Enable auditing in the Windows NT 4.0 source domain.

To create a local group in the Windows NT 4.0 source domain to support auditing

- On the source domain primary domain controller (PDC), create a local group called SourceDomain$$$, where SourceDomain is the name of your source domain. For example, in a domain named Boston, create a local group called Boston$$.  

To enable TCP/IP client support on the source domain PDC

1. While you are logged on to the PDC in the source domain, click Start, and then click Run.
2. In Open, type regedit, and then click OK.
   
   Caution
   Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after you make changes.

3. In Registry Editor, navigate to the following registry subkey:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

4. On the Edit menu, point to New, and then click DWORD Value.
5. Type TcpipClientSupport in the name field, and then press ENTER.
6. Double-click TcpipClientSupport.
7. In **Value data**, type 1, and then click **OK**.
8. Close Registry Editor, and then restart the computer.

▶ **To enable auditing in the Active Directory target domain**
1. Log on as an administrator to any computer in the target domain.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, double-click the domain, right-click the **Domain Controllers OU**, and then click **Properties**.
4. On the **Group Policy** tab, click **Default Domain Controllers Policy**, and then click **Edit**.
5. Double-click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then click **Audit Policy**.
6. Double-click **Audit account management**, and then select both the **Success** and **Failure** check boxes.
7. Click **Apply**, and then click **OK**.

▶ **To enable auditing in the Windows NT 4.0 source domain**
1. Log on as an administrator to any computer in the source domain.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **User Manager for Domains**.
3. On the **Policies** menu, click **Audit**.
4. Click **Audit These Events**, and then, next to **User and Group Management**, select both the **Success** and **Failure** check boxes.

---

**Configure the Target Domain OU Structure for Administration**

The Active Directory design team designs the OU structure for the target domain. They also define the groups that are responsible for the administration of each OU and the memberships of each group. You can use that information and the following procedure to configure the target domain for administration.
To configure the target domain OU structure for administration

1. Log on as an administrator to any domain controller in the target domain.
2. Start Active Directory Users and Computers, and then create the OU structure specified by your design team.
3. Create administrative groups, and assign users to these groups.
4. Delegate the administration of the OU structure to groups as defined by your design team.

Installing ADMT

When you install ADMT v3, it also installs Windows SQL Server 2000 Desktop Engine (Windows) (WMSDE) by default to use as its data store. Optionally, you can configure ADMT v3 to use a SQL Server 2000 with SP4 Standard or Enterprise Edition database installation that you have previously created.

Prerequisites for Installing ADMT

Before you install ADMT v3, complete the following prerequisites:

- Install Windows Server 2003. Although you can migrate accounts and resources from Windows NT 4.0 and Active Directory environments using ADMT v3, you can only install ADMT v3 on a server running Windows Server 2003.
- Remove all previous versions of ADMT by using Add or Remove Programs from Control Panel. If you attempt to install ADMT v3 on a server that has a previous version of ADMT installed, you receive an error, and the installation does not proceed. If necessary, you can import the database from the previous version of ADMT (protar.mdb) into ADMT v3 during the installation.
- If you do not plan to use the local default database installation, ensure that another SQL Server 2000 database installation is configured with an ADMT instance. For more information about creating an ADMT instance on a SQL Server 2000 database, see Installing ADMT Using a Preconfigured SQL Database.
Installing ADMT Using the Default Database Store

You can use the default database store or a preconfigured SQL database to install ADMT. The most common and recommended installation method is to use the default database store, which the Active Directory Migration Tool Installation Wizard configures automatically.

▶ To install ADMT using the default database store
- From the download location (http://go.microsoft.com/fwlink/?LinkId=75627), double-click admsetup.exe, which opens the installation wizard.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome to the Active Directory Migration Tool Installation</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Configuring Components</td>
<td>The ADMT database instance (MS_ADMT) is created on the local computer. Although WMSDE is installed locally by default whether ADMT uses it or not, ADMT disables WMSDE if you specify another database instance on the next wizard page.</td>
</tr>
</tbody>
</table>
| Database Selection | Specify the database instance you want to connect to. The recommended selection is **Use Microsoft SQL Server Desktop Engine (Windows)**, which configures ADMT v3 to use the locally installed database instance. If you are using multiple ADMT v3 consoles or have a dedicated database server where you want to centralize your ADMT database, select the **Use an existing Microsoft SQL Server** option. Specify the server to connect to in the form of `Server\Instance`. If you select this option, see [Installing ADMT Using a Preconfigured SQL Database](#).

You should configure the SQL Server database instance before you select this option. Although the ADMT v3 installation proceeds if the database cannot be contacted, you cannot use ADMT to migrate accounts or resources until the database instance is created and available. |
Active Directory Migration Tool v2
Database Import

Although you cannot upgrade an ADMT v2 installation to ADMT v3, you can import data to an ADMT v3 database from an ADMT v2 database. If you do not want to import data from an ADMT v2 database, select **No, do not import data from an ADMT v2 database (Default)**.

If you want to import data from ADMT v2 into the new ADMT v3 database, select **Yes, please import data from an ADMT v2 database**.

If you choose to import data, specify the path to the ADMT v2 database file. The ADMT v2 database file has the file name protar.mdb, and should be located in the directory formerly used for your ADMT v2 installation.

Summary

This page summarizes the options you selected. To complete the ADMT v3 installation, click **Finish**.

### Installing ADMT Using a Preconfigured SQL Database

If you plan to use multiple ADMT consoles or if you have a dedicated database server where you want to centralize your ADMT database, you can create another SQL Server database instance for ADMT instead of using the default local database. If you choose to install ADMT in an instance of SQL Server 2000, install SQL Server 2000 with SP4. To create the ADMT instance on the SQL Server, use the command-line syntax in the following table from any server that can target the SQL Server.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admtdb create /s</td>
<td>server:Server\Instance</td>
</tr>
</tbody>
</table>
Syntax | Description
---|---
`admtdb create /[i]import: "v2 database path"` | Specifies the fully qualified path to the protar.mdb database file that was used with a previous ADMT v2 installation. The `/server` parameter must be specified with this option. ADMT v2 data can be imported at the time of creation, or later into an empty database using the `admtdb import` command.

For all `admtdb.exe` command-line options, type `admtdb /?` at a command prompt.

After the database has been configured, navigate to the folder where you downloaded ADMT v3 and double-click `admtsetup.exe`.

In the Active Directory Migration Tool Installation Wizard, on the Database Selection page, select the **Use an existing Microsoft SQL Server** option and specify the server to connect to in the form of `Server\Instance`.

If you decide to use the local database after configuring a remote instance of a SQL Server database, use the following procedure.

**To use the default local database after configuring a remote instance of a SQL Server database**

1. On the local computer, click **Start**, point to **Administrative Tools**, and then click **Services**.
2. In the right pane, navigate to **MSSQL$MS_ADMT**, verify that the **Status** column displays **Started**, and that the **Startup Type** is set to **Automatic**. If the **MSSQL$MS_ADMT** service is not Started, right-click **MSSQL$MS_ADMT**, and then click **Properties**.
3. On the **General** tab, in the **Startup Type** drop-down list, click **Automatic**.
4. Under **Service Status**, click the **Start** button, and then click **OK**.
5. Close **Services**.
6. Open a command prompt, and then type:

   `admt config /setdatabase:Server\Instance`. You can now use the default local database.
Enabling Password Migration

Use the Password Export Server (PES) service to migrate passwords when you perform an interforest migration. The PES service can be installed on any domain controller in the source domain that supports 128-bit encryption.

Before you install the PES service for ADMT v3, remove the PES service installation from any previous versions of ADMT by using **Add or Remove Programs** in Control Panel. The PES service will be listed in **Add or Remove Programs** as **ADMT Password Migration DLL**.

The PES service installation in the source domain requires an encryption key. However, you must create the encryption key on the computer running ADMT in the target domain. When you create the key, save it to either a shared folder on your network or onto removable media. This way, you can store it in a secure location and reformat it after the migration is complete.

**To create an encryption key**

- At a command line, type the following:

  ```
  admtpwkey /option:create
  /sourcedomain:SourceDomain/keyfile:KeyFilePath/keypassword:{password*}
  ```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sourcedomain</strong></td>
<td>Specifies the name of the source domain in which the PES service is being installed. Can be specified as either the Domain Name System (DNS) or NetBIOS name.</td>
</tr>
<tr>
<td><strong>KeyFilePath</strong></td>
<td>Specifies the path to the location where the encrypted key is stored.</td>
</tr>
<tr>
<td><em><em>{password</em>}</em>*</td>
<td>A password, which provides key encryption, is optional. To protect the shared key, type either the password or an asterisk on the command line. The asterisk causes you to be prompted for a password that is not displayed on the screen.</td>
</tr>
</tbody>
</table>
After you create the encryption key, configure the PES service on a domain controller in the source domain. ADMT provides the option to run the PES service under the Local System account or by using the credentials of an authenticated user in the target domain. It is recommended that you run the PES service as an authenticated user in the target domain. This way, you do not need to add the Everyone group and the Anonymous Logon group to the Pre-Windows 2000 Compatible Access group.

**Note**

If you run the PES service under the Local System account, ensure that the Pre-Windows 2000 Compatible Access group in the target domain contains the Everyone group and the Anonymous Logon group.

**To configure the PES service in the source domain**

1. On the domain controller that runs the PES service in the source domain, insert the encryption key disk.
2. In the `%systemroot%\Windows\ADMT\PES` folder, run `Pwdmig.msi`. If you set a password during the key generation process on the domain controller in the target domain, provide the password that was given when the key was created, and then click **Next**.
3. If you plan to run the PES service as an authenticated user account, specify the account in the format `domain\user_name`.
4. After installation completes, restart the domain controller.
5. After the domain controller restarts, to start the PES service, point to **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Services**.
6. In the details pane, right-click **Password Export Server Service**, and then click **Start**.

**Note**

Run the PES service only when you migrate passwords. Stop the PES service after you complete the password migration.

---

**Initializing ADMT**

Initialize ADMT by running a test migration of a global group, and select the option named **Migrate Group SIDs to target domain**. If you did not previously configure the
source and target domains to migrate SID history, you will receive an error and a prompt for each item that has not yet been configured. When you accept each prompt, ADMT automatically completes the following tasks, which are required to enable SID history migration:

- Creates a local group, source_domain$$$, in the source domain, which is used to audit SID history operations. Do not add members to this group; if you do, SID history migration will fail.
- Enables TCP/IP client support on the source domain PDC by setting the value of the registry entry TcpipClientSupport to 1. This entry is located in the following subkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
  Setting TcpipClientSupport to 1 enables remote procedure calls (RPCs) over the TCP transport, while preserving the security of the system.
- Enables audit policies in the source and target domains.

For more information about configuring the source and target domains to migrate SID history, see Configuring the Source and Target Domains to Migrate SID History, earlier in this guide.

Use the following procedure to initialize ADMT.

To initialize ADMT by running a test migration of a global group

1. In the ADMT console, use the Group Account Migration Wizard by following the steps provided in the following table. Accept default settings when no information is specified.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>

- In the ADMT console, use the Group Account Migration Wizard by following the steps provided in the following table. Accept default settings when no information is specified.
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| Group Selection | Click **Select groups from domain**, and then click **Next**. On the **Group Selection** page, click **Add** to select the groups in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Type the name of the OU, or click **Browse**.

In the **Browse for Container** dialog box, find the container in the target domain that you want to move the global groups into, and then click **OK**. |
| Group Options | Select the **Migrate Group SIDs to target domain** check box.

Make sure that all other options are not selected. |
User Account | Type the user name, password, and domain of an account that has administrative rights in the source domain.
Conflict Management | Click Do not migrate source object if a conflict is detected in the target domain.

2. When the wizard has finished running, click View Log, and then review the migration log for any errors.
3. Verify that the test migration configured ADMT properly by ensuring that:
   - A new local group source_domain$$ exists in the source domain. This account supports ADMT auditing of SID history migration.
   - The registry entry TcpipClientSupport is created, and its value is set to 1, in the following subkey on the source domain PDC:
     HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
   - The audit policy for account management is enabled on the source and target domains.

Service Account Identification

Identify the member servers and domain controllers in the source domain that run applications in the context of a service account. A service account is a user account that provides a security context for applications and that is granted permission to log on as a service. ADMT does not migrate services that run in the context of the Local System account because they are migrated when the computer is migrated; however, services that run in the context of a user account must be updated on the computer after you have completed the account migration process. ADMT also cannot migrate the Local Service or Network Service accounts because they are well-known accounts that always exist in Windows Server 2003.

The process of identifying, migrating, and updating services that run in the context of user accounts involves three steps. First, the administrator starts ADMT from the target Active Directory domain controller and runs the Service Account Migration Wizard. For the second step, the Service Account Migration Wizard sends an agent to a specified computer and identifies (but does not migrate) all services on the computer that are
running in the context of a user account. The last step, which can occur later in the migration process, is to migrate the accounts when other user accounts are migrated with the User Account Migration Wizard.

The Service Account Migration Wizard scans an administrator-defined list of servers for services that are configured to use a domain account to authenticate. The accounts are then flagged as service accounts in the ADMT database. The password is never migrated when a service account is migrated. Instead, ADMT uses a clear-text representation of the password to configure the services after the service account migration. An encrypted version of the password is then stored in the password.txt file in the ADMT installation folder.

An administrator of a workstation or server can install any service and configure the service to use any domain account. If the administrator cannot configure the service to authenticate with the correct password, the service will not start. After the service account is migrated, ADMT configures the service on the workstation or the server to use the new password, and the service will now start under the user account.

Include in the Service Account Migration Wizard only those servers that trusted administrators manage. Do not use the wizard to detect service accounts on computers that trusted administrators do not manage, such as workstations.

Dispatch agents to all servers that trusted administrators manage in the domain to ensure that you do not overlook any service accounts. If you miss a service account that shares an account with a service that has already been migrated, it is not possible for ADMT to synchronize them. You must manually change the password for the service account and then reset the service account password on each server that is running that service.

When the accounts that the Service Account Migration Wizard identifies in the ADMT database as running in the context of a user account are migrated to the target domain, ADMT grants each account the right to log on as a service. If the service account is assigned rights by means of its membership in a group, the Security Translation Wizard updates the account to assign those rights. For more information about running the Security Translation Wizard, see Transitioning Service Accounts, later in this guide.

You can identify service accounts by using the ADMT console, the ADMT command-line option, or a script.

To identify service accounts by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. In the ADMT console, log on by using the ADMT account migration account and then use the Service Account Migration Wizard by following the steps provided in the following table.
<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>
| Domain Selection            | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.  
Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| Update Information          | Click **Yes, update the information**.                                                                                                                                                           |
| Computer Selection Option   | Click **Select computers from domain**, and then click **Next**. On the **Service Account Selection** page, click **Add** to select the accounts in the source domain that you want to migrate, click **OK**, and then click **Next**.  
- or -  
Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**.                                                                 |
| Agent Dialog                | In **Agent Actions**, select **Run pre-check and agent operation**, and then click **Start**. A message will appear in the Agent Summary when the agent operations are complete. After the agent operations finish, click **Close**. |
Service Account Information

Select any user accounts that do not need to be marked as service accounts in the ADMT database, and then click Skip/Include to mark the accounts as Skip.

The wizard connects to the selected computers, and then sends an agent to check every service on the remote computers. The Service Account Information page lists the services that are running in the context of a user account and the name of that user account. ADMT notes in its database that these user accounts need to be migrated as service accounts. If you do not want a user account to be migrated as a service account, select the account, and then click Skip/Include to change the status from Include to Skip.

You use Update SCM to update the Service Control Manager with the new information. Unless you have a failure in reaching a computer to update the service, the Update SCM button is not available. If you have a problem updating a service account after the account was identified and migrated, ensure that the computer that you are trying to reach is available, and then restart the Service Account Migration Wizard.

In the wizard, click Update SCM to try to update the service. If you ran the Service Account Migration Wizard previously and the Update SCM button is not available, examine the ADMT log files to determine the cause of the problem. After you correct the problem and the agent can connect successfully, the Update SCM button becomes available.

To identify service accounts by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type:

```
ADMT SERVICE /N "computer_name1" "computer_name2" /SD:"source_domain" /TD:"target_domain"
```

Computer_name1 and computer_name2 are the names of computers in the source domain that run service accounts.

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT SERVICE /N "computer_name1" "computer_name2" /o:"option_file.txt"
```

The following table lists the common parameters used for the identification of service accounts, along with the command-line parameter and option file.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.

➤ To identify service accounts by using a script

- Create a script that incorporates ADMT commands and options for identifying service accounts by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```vbscript
Option Explicit

Dim objMigration
Dim objServiceAccountEnumeration

'Create instance of ADMT migration objects.'

Set objMigration = CreateObject("ADMT.Migration")
Set objServiceAccountEnumeration = objMigration.CreateServiceAccountEnumeration

'Specify general migration options.'

objMigration.SourceDomain = "source_domain"

'Enumerate service accounts on specified computers.'

objServiceAccountEnumeration.Enumerate admtdata, _
Array("computer name1","computer name2")

Set objServiceAccountEnumeration = Nothing
Set objMigration = Nothing
```

```xml
<Job id="IdentifyingServiceAccounts" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
  Option Explicit

  Dim objMigration
  Dim objServiceAccountEnumeration

  'Create instance of ADMT migration objects.'

  Set objMigration = CreateObject("ADMT.Migration")
  Set objServiceAccountEnumeration = objMigration.CreateServiceAccountEnumeration

  'Specify general migration options.'

  objMigration.SourceDomain = "source_domain"

  'Enumerate service accounts on specified computers.'

  objServiceAccountEnumeration.Enumerate admtdata, _
  Array("computer name1","computer name2")

  Set objServiceAccountEnumeration = Nothing
  Set objMigration = Nothing
</Script>
```
Restructuring Account Domains

Restructuring Windows NT 4.0 account domains involves migrating the user, group, and service accounts that exist in the Windows NT 4.0 domain into an Active Directory domain. If account domains include resources, you must also migrate those resources. The Active Directory target domain owner is responsible for the migration of all Windows NT 4.0 accounts. The migration process must be completed for every Windows NT 4.0 source account domain.

The following figure shows the process for restructuring Windows NT 4.0 account domains.
Transitioning Service Accounts

Begin the process of migrating objects by transitioning the service accounts that you selected when you identified service accounts. For more information about identifying service accounts, see Service Account Identification, earlier in this guide.

To transition service accounts, use ADMT to complete the following tasks:

- Migrate the service accounts from the Windows NT 4.0 source account domain to the target domain.
- Modify the services on each server in the source domain to use the service account in the target domain in place of the service account in the Windows NT 4.0 source account domain.

Note

This process only updates the Log on as a service right. If a service account has local rights based on its membership in a local group, you must update these rights by running the Security Translation Wizard.

You can transition service accounts by using the ADMT console, the ADMT command-line option, or a script.

To transition service accounts by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. Use the User Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>


| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| User Selection | Click **Select users from domain**, and then click **Next**. On the **User Selection** page, click **Add** to select the accounts in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Click **Browse**.

In the **Browse for Container** dialog box, locate the source domain, select the container for the service accounts, and then click **OK**. |
| Password Options | Click **Generate complex passwords**. |
| Account Transition Options | Click **Enable target accounts**.

Select the **Migrate user SIDs to target domains** check box. |
### User Account
Type the user name, password, and domain of a user account that has administrative credentials.

### User Options
Select the **Update user rights** check box.
Ensure that no other settings are selected, including **Migrate associated user groups**.

### Conflict Management
Click **Do not migrate source object if a conflict is detected in the target domain**.

### Service Account Information
Click **Migrate all service accounts and update SCM for items marked include**. If you are also migrating other user accounts that are not service accounts, this wizard page tells you that you have selected some accounts that are marked as service accounts in the ADMT database. By default, the accounts are marked as Include. To change the status of the account, select the account, and then click **Skip/Include**. Click **Next** to migrate the accounts.

3. When the wizard has finished running, click **View Log**, and review the migration log for any errors.
4. Start Active Directory Users and Computers, navigate to the OU that you created for service accounts, and then verify that the service accounts exist in the target domain OU.
5. Confirm that each application for which the service account was relocated continues to function correctly.

---

**To transition service accounts by using the ADMT command-line option**

1. On a member server in the target domain on which ADMT is installed, log on as a member of the ADMT account migration group.
2. At the command line, type:
Server_name1 and Server_name2 are the names of servers in the source domain that run service accounts. Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT USER /N "server_name1" "server_name2" /O: "option_file.txt"
```

The following table lists the common parameters used for transitioning service accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD: &quot;source_domain&quot;</td>
<td>SourceDomain= &quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD: &quot;target_domain&quot;</td>
<td>TargetDomain= &quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO: &quot;target_OU&quot;</td>
<td>TargetOU= &quot;target_OU&quot;</td>
</tr>
<tr>
<td>Disable accounts</td>
<td>/DOT: ENABLETARGET</td>
<td>DisableOption= ENABLETARGET</td>
</tr>
<tr>
<td></td>
<td>(default)</td>
<td>(default)</td>
</tr>
<tr>
<td>Migrate password</td>
<td>/PO: COMPLEX</td>
<td>PasswordOption= COMPLEX</td>
</tr>
<tr>
<td></td>
<td>(default)</td>
<td></td>
</tr>
<tr>
<td>Migrate user SIDs</td>
<td>/MSS: YES</td>
<td>MigrateSIDs= YES</td>
</tr>
<tr>
<td>Update user rights</td>
<td>/UUR: YES</td>
<td>UpdateUserRights= YES</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO: IGNORE</td>
<td>ConflictOptions= IGNORE</td>
</tr>
<tr>
<td></td>
<td>(default)</td>
<td>(default)</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers, and locate the target service account OU. Verify that the service accounts exist in the target domain OU.

**To transition service accounts by using a script**

- Prepare a script that incorporates ADMT commands and options for transitioning service accounts by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the
same folder as the AdmtConstants.vbs file.

```vbscript
<Job id="TransitioningServiceAccountsNTSource" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
  Option Explicit
  Dim objMigration
  Dim objUserMigration

  'Create instance of ADMT migration objects.
  Set objMigration = CreateObject("ADMT.Migration")
  Set objUserMigration = objMigration.CreateUserMigration

  'Specify general migration options.
  objMigration.SourceDomain = "source domain"
  objMigration.TargetDomain = "target domain"
  objMigration.TargetOu = "target container"
  objMigration.ConflictOptions = admtIgnoreConflicting

  'Specify user migration specific options.
  objUserMigration.DisableOption = admtEnableTarget
  objUserMigration.MigrateSIDs = True
  objUserMigration.UpdateUserRights = True
  objUserMigration.MigrateServiceAccounts = True

  'Migrate specified service accounts.
  objUserMigration.Migrate admtData, Array("service account name1", "service account name2")
  Set objUserMigration = Nothing
  Set objMigration = Nothing
</Script>
</Job>
```

### Migrating Global Groups

To preserve the user memberships of global groups, you must migrate global groups before you migrate users.
**Note**

Do not migrate global groups during peak work hours. The global group migration process can consume a large amount of network resources and resources on the domain controller in the target domain.

Global group migration involves the following steps:

1. The administrator selects the global group objects in the source domain. ADMT reads the objects in the source domain.
2. A new global group object is created in the target domain, and a new primary SID is created for the object in the target domain.
3. To preserve resource access if you are migrating SID history, ADMT adds the SID of the global group in the source domain to the SID history attribute of the new global group in the target domain.

Following the migration, audit events are logged in both the source and the target domain.

**Note**

If the user account migration process takes place over an extended period of time, you might need to remigrate global groups from the source to the target domain. The objective is to propagate membership changes that are made in the source domain before the migration process is complete. For more information about remigrating global groups, see Remigrating Global Groups, later in this guide.

For a worksheet to assist you in completing your initial global group migration, see "User and Group Object Assignment Table — Windows NT 4.0 Source" (DSSRENT_1.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink?LinkId=14384).

You can migrate global groups by using the ADMT console, the ADMT command-line option, or a script.

**To migrate global groups from a Windows NT 4.0 source domain by using the ADMT console**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. Use the Group Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| --- | --- |
| Group Selection | Click **Select groups from domain**, and then click **Next**. On the **Group Selection** page, click **Add** to select the groups in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Type the name of the OU, or click **Browse**.

In the **Browse for Container** dialog box, find the container in the target domain that you want to move the global groups into, and then click **OK**. |
| Group Options | Click **Migrate Group SIDs to target domain**.

Make sure that all other options are not selected. |
Type the user name, password, and domain of an account that has administrative rights in the source
domain.

Click **Do not migrate source object if a conflict is detected in the target domain.**

3. When the wizard has finished running, click **View Log**, and then review the migration log for any errors.

4. Start Active Directory Users and Computers, and then navigate to the target OU. Verify that the global groups exist in the target domain OU.

**To migrate global groups from a Windows NT 4.0 source domain by using the ADMT command-line option**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT Group command with the appropriate parameters. For example:

   ```
   ADMT GROUP /N "group_name1" "group_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /MSS:YES
   ```

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT GROUP /N "group_name1" "group_name2" /O: "option_file.txt"
   ```

   The following table lists the parameters required for migrating global groups, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors.
4. Start Active Directory Users and Computers, and then navigate to the target OU. Verify that the global groups exist in the target domain OU.

To migrate global groups by using a script

- Prepare a script that incorporates ADMT commands and options for migrating global groups by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmConstants.vbs file.

```xml
<Job id="MigratingGlobalGroupsNTSource" >
  <Script language="VBScript" src="AdmConstants.vbs" />
  <Script language="VBScript" >
    Option Explicit
    Dim objMigration
    Dim objGroupMigration
    'Create instance of ADMT migration objects.
    Set objMigration = CreateObject("ADMT.Migration")
    Set objGroupMigration = objMigration.CreateGroupMigration
    'Specify general migration options.
    objMigration.SourceDomain = "source domain"
    objMigration.TargetDomain = "target domain"
    objMigration.TargetOu = "target container"
    'Specify group migration specific options.
    objGroupMigration.MigrateSIDs = True
    'Migrate specified group objects.
    objGroupMigration.Migrate admtData, Array("group name1","group name2")
  </Script>
</Job>
```
Migrating Users in Batches

To begin migrating users, first migrate a small number of users as a pilot, and test whether they are able to access resources after the migration. Then migrate the remaining users in the source account domain in small batches of up to 100 users per batch. This helps to keep the migration process manageable.

Complete the following steps to migrate user accounts to the target domain:

1. Create test accounts that you can use to verify the success of each batch.
2. Migrate a single batch of users.
3. Translate any local user profiles for user accounts that are included in the batch.
4. Migrate workstations for users that are included in the batch.
5. Remigrate all global groups to update any group membership changes.
6. Notify users in the batch to log on to the target domain.
7. Repeat the steps for the next batch of users, until you have migrated all user accounts.

Until you migrate all user and group accounts, continue to administer global group membership in the Windows NT 4.0 source account domain. To support a rollback strategy, manually synchronize any changes you make to users in the target domain with the existing user accounts in the Windows NT 4.0 source account domain.

The following figure shows the steps you must complete for each batch of user accounts.
Migrating User Accounts

The ADMT user account migration process includes the following steps:

1. The administrator selects the source user objects to be migrated.
2. ADMT reads attributes from the source user objects.
3. ADMT creates a new user object in the target domain and a new primary SID for the new user account.
4. If you are migrating SID history, ADMT adds the original SID of the user account to the SID history attribute of the new user account.
5. ADMT migrates the password for the user account.

You cannot migrate every user property when you migrate user accounts. For example, Protected Storage (Pstore) contents for Windows NT 4.0 workstations, including Encrypting File System (EFS) private keys, are not migrated by ADMT when you migrate user accounts. To migrate Pstore contents, you must export and import keys during the migration process.

For clients that are running Windows 2000 Server or later, data that is protected by the Data Protection API (DPAPI) is also not migrated. DPAPI helps protect the following items:

- Web page credentials (for example, passwords)
• File share credentials
• Private keys associated with EFS, S/MIME, and other certificates
• Program data that is protected by using the CryptProtectData() function

For this reason, it is important to test user migrations. Use your test migration account to identify any properties that did not migrate, and update user configurations in the target domain accordingly.

After the migration, audit events are logged in both the source and the target domains if you are migrating SID history.

Using ADMT to migrate user accounts preserves group memberships. Because global groups can contain only members from the domain in which the group is located, when users are migrated to a new domain, the user accounts in the target domain cannot be members of the global groups in the source domain.

As part of the migration process, ADMT identifies the global groups in the source domain that the user account belongs to, and then determines whether the global groups have been migrated. If ADMT identifies global groups in the target domain that the users belonged to in the source domain, the tool adds the users to the appropriate groups in the target domain.

Using ADMT to migrate user accounts also preserves user passwords. After the user accounts are migrated to, and enabled, in the target domain, the users can log on to the target domain by using their original passwords. After they log on, they are prompted to change the password.

If the user account migration is successful but the password migration process fails, ADMT creates a new complex password for the user account in the target domain. By default, ADMT stores new complex passwords that are created in the default drive, in Program Files\Active Directory Migration Tool\Logs\Password.txt file.

If you have a Group Policy setting on the target domain that does not allow blank passwords (the Default Domain Policy/Computer Configuration/Security Settings/Account Policies/Password Policy/Minimum password length setting is set to any number other than zero), password migration will fail for any user who has a blank password. ADMT generates a complex password for that user, and writes an error to the error log.

Establish a method for notifying users who have been assigned new passwords. For example, you can create a script to send an e-mail message to users to notify them of their new passwords.

Important

Because only a hash of a user password exists in the source domain, the password filter cannot verify whether the password meets complexity or length
requirements. The target domain controller used to set the password can verify the password history because it compares the hash of the password against previous hashes.

You can migrate user accounts by using the AD MT console, the AD MT command-line option, or a script.

**To migrate the current batch of users by using the AD MT console**

1. On the computer in the target domain on which AD MT is installed, log on by using the AD MT account migration account.
2. Use the User Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
User Selection  
Click **Select users from domain**, and then click **Next**. On the User Selection page, click **Add** to select the users in the source domain that you want to migrate in the current batch, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**.

Organizational Unit Selection  
Ensure that ADMT lists the correct target OU. If it is not correct, type the correct OU, or click **Browse**.

In the **Browse for Container** dialog box, locate the target domain and OU, and then click **OK**.

Password Options  
Select **Migrate Passwords**.

Account Transition Options  
In **Target Account State**; click **Disable target accounts**.

In **Source Account Disabling Options**; click **Days until source accounts expire**; and then type the numbers of days you want to keep the source account. A value of 7 is commonly used.

Select the **Migrate user SIDs to target domains** check box.

User Account  
Type the user name, password, and domain of a user account that has administrative credentials in the source domain.
User Options

Select the Translate roaming profiles check box.
Select the Update user rights check box.
Clear the Migrate associated user groups check box.
Select the Fix users’ group memberships check box.

Object Property Exclusion

Clear the Exclude specific object properties from migration check box.

Conflict Management

Click Do not migrate source object if a conflict is detected in the target domain.

3. When the wizard has finished running, click View Log and review the migration log for any errors.
4. Start Active Directory Users and Computers, and then verify that the user accounts exist in the appropriate OU in the target domain.

To migrate the current batch of users by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. At the command line, type the ADMT User command with the appropriate parameters. For example:

```
ADMT USER /N "user_name1" "user_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /MSS:YES /TRP:YES /UUR:YES
```

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT USER /N "user_name1" "user_name2" /O:"option_file.txt"
```

The following table lists the parameters required for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Options</td>
<td>Select the Translate roaming profiles check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select the Update user rights check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clear the Migrate associated user groups check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select the Fix users’ group memberships check box.</td>
<td></td>
</tr>
</tbody>
</table>
### ADMT Parameters

<table>
<thead>
<tr>
<th>Source domain</th>
<th><code>&lt;SD: &quot;source_domain&quot;&gt;</code></th>
<th>SourceDomain= &quot;source_domain&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target domain</td>
<td><code>&lt;TD: &quot;target_domain&quot;&gt;</code></td>
<td>TargetDomain= &quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td><code>&lt;TO: &quot;target_OU&quot;&gt;</code></td>
<td>TargetOU= &quot;target_OU&quot;</td>
</tr>
<tr>
<td>Migrate SIDs</td>
<td>MSS: YES</td>
<td>MigrateSIDs= YES</td>
</tr>
<tr>
<td>Password options</td>
<td>PO: COPY</td>
<td>PasswordOption= COPY</td>
</tr>
<tr>
<td></td>
<td>PS: &quot;server name&quot;</td>
<td>PasswordServer= &quot;server name&quot;</td>
</tr>
<tr>
<td>Conflict management</td>
<td>CO: IGNORE</td>
<td>ConflictOptions= IGNORE</td>
</tr>
<tr>
<td>Translate Roaming Profile</td>
<td>TRP: YES (default)</td>
<td>TranslateRoamingProfile= YES</td>
</tr>
<tr>
<td>Update User Rights</td>
<td>UUR: YES</td>
<td>UpdateUserRights= NO</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.

4. Start Active Directory Users and Computers, and then navigate to the target OU. Verify that the users exist in the target domain OU.

#### To migrate the current batch of users by using a script

- Prepare a script that incorporates ADMT commands and options for migrating users by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```vbscript
<Job id="MigratingUserAccountsNTSource" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >

Option Explicit

Dim objMigration
Dim objUserMigration

'Create instance of ADMT migration objects.
Set objMigration = CreateObject("ADMT.Migration")
Set objUserMigration = objMigration.CreateUserMigration
```
Translating Local User Profiles

Local profiles contain the desktop state and user data for users in the source account domain. ADMT can migrate local profiles only for workstations running Windows NT 4.0, Windows 2000 Server, and Windows XP. Migrate local user profiles for a batch of users immediately after migrating the batch of users, and before the users log on to the target domain.

It is important to verify that user profile translation succeeded for each user before that user is allowed to log on. If it failed, that user must not log on to the target domain. Roll the user back manually, by disabling the user account in the target domain, and enabling the account in the source domain.

You can migrate roaming user profiles during the user account migration process. However, you still need to translate the local copy of the profile.
Note

The night before you notify the users to log on by using their new accounts in the target domain, translate the local user profiles. Migrating profiles the night before ensures that the new user profile reflects the most current user settings.

Before you migrate local user profiles, create a list of the workstations in the source domain. You can migrate local user profiles by running the ADMT console, the ADMT command-line option, or a script.

To translate local user profiles by using the ADMT console

1. For each workstation in the source domain that is running Windows NT 4.0, verify that the ADMT account migration account was added as a member of the local Administrators group.

2. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

3. Use the Security Translation Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Translation Options</td>
<td>Select <em>Previously migrated objects</em>.</td>
</tr>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
After migrating local user profiles, you must verify that the migration process was successful. Complete the following steps to verify that the user profile migration was successful:

1. Review the status message for each computer for which you migrated the user profile.
2. For computers for which the status is not Success, review the message to identify the cause of the failure. For more details about the cause of the failure, click View Migration Log and review the log for any errors that occurred during the local profile migration process. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#.ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.
3. For any computers for which the agent failed to migrate the local profile, fix the cause of the problem, and then perform the local profile migration again on those computers.

To migrate local user profiles by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by
using the ADMT account migration account.

2. At the command line, type the ADMT Security command with the appropriate parameters. For example:

```
ADMT SECURITY /N "computer_name1" "computer_name2"
/SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /TOT:Replace
/TUP:YES
```

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT SECURITY /N "computer_name1" "computer_name2" /o "option_file.txt"
```

The following table lists the parameters required for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Security translation options</td>
<td>/TOT:REPLACE</td>
<td>TranslateOption=REPLACE</td>
</tr>
<tr>
<td>Modify local user profile security</td>
<td>/TUP:YES</td>
<td>TranslateUserProfiles=YES</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.
4. Review the migration log for errors related to local profiles on workstations.
5. For computers to which the agent failed to be dispatched, fix the cause of the problem, click Run pre-check and agent operation, and then click Start again.
6. For any computers for which the agent failed to migrate the local profile, fix the cause of the problem, and then perform the local profile migration again on those computers.

It is important to verify the success of the local profile migration before users attempt to log on to the target domain.

If a user logs on to the target domain by using their new target account and their local profile did not migrate successfully, you must do the following:

7. On the computer of the user, delete the following registry subkey, where SID is
the SID of the user account in the target domain:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\SID

8. Remigrate the local user profile for that computer.

To migrate local user profiles by using a script

- Prepare a script that incorporates ADMT commands and options for migrating local profiles by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="MigratingLocalProfilesNTSource" >
  <Script language="VBScript" src="AdmtConstants.vbs" />
  <Script language="VBScript" >
    Option Explicit
    Dim objMigration
    Dim objSecurityTranslation

    'Create instance of ADMT migration objects.
    Set objMigration = CreateObject("ADMT.Migration")
    Set objSecurityTranslation = objMigration.CreateSecurityTranslation

    'Specify general migration options.
    objMigration.SourceDomain = "source domain"
    objMigration.TargetDomain = "target domain"
    objMigration.TargetOu = "Computers"

    'Specify security translation specific options.
    objSecurityTranslation.TranslationOption = admtTranslateReplace
    objSecurityTranslation.TranslateUserProfiles = True

    'Perform security translation on specified computer objects.
    objSecurityTranslation.Translate admtData, Array("computer name1", "computer name2")

    Set objSecurityTranslation = Nothing
    Set objMigration = Nothing
  </Script>
</Job>
```
Migrating User Workstations

For each batch of user accounts that you migrate, migrate a batch containing those users’ workstations, so that the user account and the workstation exist in the target domain when the user logs on. When you migrate a workstation, the SAM database is migrated along with the computer. Accounts located in the local SAM database (such as local groups) that are used to enable access to resources always move with the computer, and therefore do not need to be migrated.

Note

Restart workstations immediately after joining them to the target domain, by selecting a low number (such as 1) for the RestartDelay parameter. Resources that are not restarted following migration are in an indeterminate state.

You can migrate workstations by using the ADMT console, the ADMT command-line option, or a script.

To migrate workstations by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT resource migration account.
2. Use the Computer Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| Computer Selection | Click **Select computers from domain**, and then click **Next**. On the **Computer Selection** page, click **Add** to select the computers in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Click **Browse**.

In the **Browse for Container** dialog box, locate the target domain **Computers** container or the appropriate OU, and then click **OK**. |
| Translate Objects | Ensure that no boxes are selected. |
| Computer Options | In the **Minutes before computer restart after wizard completion** box, accept the default value of 5 minutes or type a different value. |
Object Property Exclusion | To exclude certain object properties from the migration, select the **Exclude specific object properties from migration** check box, select the object properties that you want to exclude and move them to the **Excluded Properties** box, and then click **Next**.

Conflict Management | Click **Do not migrate source object if a conflict is detected in the target domain**.

ADMT Agent Dialog | Select **Run pre-check and agent operation**, and then click **Start**.

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click **View Migration Log** to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

4. Start Active Directory Users and Computers, and then verify that the workstations exist in the appropriate OU in the target domain.

To migrate workstations by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT resource migration account.

2. At the command line, type the ADMT Computer command with the appropriate parameters. For example, type:

```
ADMT COMPUTER /N "computer_name1" "computer_name2"
/SD: "source_domain" /TD: "target_domain" /TO: "target_OU" /RDL: 5
```

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT COMPUTER /N "computer_name1" "computer_name2"
/o: "option_file.txt"
```

The following table lists the parameters required for migrating workstations, along
with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Restart Delay (minutes)</td>
<td>/RDL:5</td>
<td>RestartDelay=5</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO:IGNORE (default)</td>
<td>ConflictOptions=IGNORE</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click **View Migration Log** to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

4. Start Active Directory Users and Computers, and then navigate to the target OU. Verify that the workstations exist in the target OU.

To migrate workstations by using a script

- Prepare a script that incorporates ADMT commands and options for migrating workstations by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```vbscript
<Job id="MigratingWorkstationsMemberServersNTSource" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
   Option Explicit
   Dim objMigration
   Dim objComputerMigration
   'Create instance of ADMT migration objects.
   Set objMigration = CreateObject("ADMT.Migration")
```
Remigrating Global Groups

A large user account migration might take place over an extended period of time. For this reason, you might need to remigrate global groups from the source to the target domain to reflect changes made to the groups in the source domain after the initial global group migration occurred. This procedure updates global group membership without overwriting previously migrated user accounts.

Note

Do not migrate global groups during peak work hours. The global group migration process consumes a large amount of network resources as well as resources on the domain controller in the target domain.

You can migrate global groups by using the ADMT console, the ADMT command-line option, or a script.
To remigrate global groups from a Windows NT 4.0 source domain by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. Use the Group Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td><strong>Under Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Group Selection</td>
<td>Click <strong>Select groups from domain</strong>, and then click <strong>Next</strong>. On the Group Selection page, click <strong>Add</strong> to select the groups in the source domain that you want to migrate, click <strong>OK</strong>, and then click <strong>Next</strong>. - or - Click <strong>Read objects from an include file</strong>, and then click <strong>Next</strong>. Type the location of the include file, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
| Organizational Unit Selection | Type the name of the OU, or click **Browse**.  
In the **Browse for Container** dialog box, find the container in the target domain that you want to move the global groups into, and then click **OK**. |
| Group Options | Select **Update user rights**.  
Ensure that **Copy group members** is not selected.  
Ensure that **Update previously migrated objects** is not selected.  
Select **Fix membership of group**.  
Select **Migrate Group SIDs to target domain**. |
| User Account | Type the user name, password, and domain of an account that has administrative rights in the source domain. |
| Object Property Exclusion | Clear the **Exclude specific object properties from migration** check box. |
| Conflict Management | Select **Migrate and merge conflicting accounts**.  
Select **Before merging remove existing user rights for existing target accounts**  
Select **Before merging remove members from existing target group accounts**.  
Ensure that **Move merged objects to the specified target Organizational Unit** is not selected. |

3. When the wizard has finished running, click **View Log**, and then review the migration log for any errors.

4. Start Active Directory Users and Computers, and then navigate to the target OU.
Verify that the global groups exist in the target domain OU.

To remigrate global groups from a Windows NT 4.0 source domain by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. At the command line, type the ADMT Group command with the appropriate parameters. For example:

   ADMT GROUP /N "group_name1" "group_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target OU" /MSS:YES /UGR:YES /MMS:NO /CO:REPLACE+REMOVEMEMBERS

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ADMT GROUP /N "group_name1" "group_name2" /O: "option_file.txt"

The following table lists the parameters required for remigrating global groups, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target OU&quot;</td>
<td>TargetOU=&quot;target OU&quot;</td>
</tr>
<tr>
<td>Migrate GG SIDs</td>
<td>/MSS:YES</td>
<td>MigrateSIDs=YES</td>
</tr>
<tr>
<td>Update group rights</td>
<td>/UGR:YES</td>
<td>UpdateGroupRights=YES</td>
</tr>
<tr>
<td>Copy group members</td>
<td>/MMS:NO</td>
<td>MigrateMembers=NO</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors.
4. Start Active Directory Users and Computers, and then navigate to the target OU. Verify that the global groups exist in the target domain OU.

To remigrate global groups by using a script

- Prepare a script that incorporates ADMT commands and options for remigrating global groups by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmConstants.vbs file.

```xml
<Job id="RemigratingGlobalGroupsNTSource" >
<Script language="VBScript" src="AdmConstants.vbs" />;
<Script language="VBScript" >
    Option Explicit
    Dim objMigration
    Dim objGroupMigration

    'Create instance of ADMT migration objects.
    Set objMigration = CreateObject("ADMT.Migration")
    Set objGroupMigration = objMigration.CreateGroupMigration

    'Specify general migration options.
    objMigration.SourceDomain = "source domain"
    objMigration.TargetDomain = "target domain"
    objMigration.TargetOu = "target container"
    objMigration.ConflictOptions = admtReplaceConflicting + admtRemoveExistingUserRights + admtRemoveExistingMembers

    'Specify group migration specific options.
    objGroupMigration.MigrateSIDs = True
    objGroupMigration.UpdateGroupRights = True
    objGroupMigration.UpdatePreviouslyMigratedObjects = False
    objGroupMigration.FixGroupMembership = True
    objGroupMigration.MigrateMembers = False
```
Completing the Account Migration

After you migrate all batches of accounts from the source to the target domain, you can complete the account migration process. This involves the following steps:

- Transferring user and group administration to the target domain by doing the following:
  - Freezing user and group administration in the source domain.
  - Maintaining at least two operational domain controllers in the source domain until the account migration process is complete.
  - Backing up the two domain controllers in the source domain.
  - Beginning administration of user and group accounts in the target domain.
- Decommissioning the Windows NT 4.0 source account domain by doing the following:

  Note

  Ensure that you retain a full system backup of the PDC for each account domain. This enables you to bring the account domain back online.

- Removing all trust relationships involving the Windows NT 4.0 source account domain.
- Repurposing any remaining account domain controllers in the source account domain that you did not migrate to the target domain.
- Disabling all accounts that you created during the migration process, including those accounts to which you assigned administrative credentials.

When you decommission the source account domain, shared local groups and local groups in resource domains that you have not translated by using the Security Translation Wizard display group members as account unknown. This is because
Restructuring Resource Domains

Restructuring Windows NT 4.0 resource domains into an Active Directory domain involves migrating resources, such as workstation and server computer accounts, and the associated shared local groups to the new environment. The target domain owner is responsible for the migration of all Windows NT 4.0 resources. The migration process must be completed for every Windows NT 4.0 source resource domain.

The following figure shows the process for restructuring Windows NT 4.0 resource domains.
Migrating Workstations and Member Servers

Migrate remaining workstations that you did not migrate during the user account migration process, along with member servers, in small batches of up to 100 computers. Workstation account and member server migration is a straightforward process. Workstations and member servers have their own SAM account database. When you move workstations and member servers between domains, the database moves with them. Accounts located in the local SAM database (such as local groups) that are used to enable access to resources always move with the computer, and therefore do not need to be migrated.

Note

Restart member workstations and servers immediately after joining them to the target domain, by selecting a low number for the RestartDelay parameter. Resources that are not restarted following migration are in an indeterminate state.

You can migrate workstations and member servers by running the ADMT console, the ADMT command-line option, or a script.

To migrate Windows NT 4.0 workstations and member servers by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT resource migration account.
2. Use the Computer Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>
### Domain Selection

Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**.

### Computer Selection

Click **Select computers from domain**, and then click **Next**. On the Computer Selection page, click **Add** to select the computers in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**.

### Organizational Unit Selection

Click **Browse**.

In the **Browse for Container** dialog box, locate the target domain **Computers** container or the appropriate OU, and then click **OK**.

### Translate Objects

Ensure that no check boxes are selected.
<table>
<thead>
<tr>
<th>Computer Options</th>
<th>In the <strong>Minutes before computer restart after wizard completion</strong> box, accept the default value of 5 minutes, or type a different value.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Property Exclusion</td>
<td>To exclude certain object properties from the migration, select the <strong>Exclude specific object properties from migration</strong> check box, select the object properties that you want to exclude and move them to the <strong>Excluded Properties</strong> box, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Conflict Management</td>
<td>Click <strong>Do not migrate source object if a conflict is detected in the target domain</strong>.</td>
</tr>
<tr>
<td>ADMT Agent Dialog</td>
<td>Select <strong>Run pre-check and agent operation</strong>, and then click <strong>Start</strong>.</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click **View Migration Log** to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

4. Start Active Directory Users and Computers, and then verify that the workstations and member servers exist in the appropriate OU in the target domain.

**To migrate workstations and member servers by using the ADMT command-line option**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT resource migration account.

2. At the command line, type the ADMT Computer command with the appropriate parameters. For example, type:

```
ADMT COMPUTER /N "computer_name1" "computer_name2"
/SD: "source_domain" /TD: "target_domain" /TO: "target_OU" /RDL: 5
```
Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT COMPUTER /N "computer_name1" "computer_name2" /O:"option_file.txt"
```

The following table lists the parameters required for migrating workstations and member servers, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Restart Delay</td>
<td>/RDL:1</td>
<td>RestartDelay=1</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO:IGNORE (default)</td>
<td>ConflictOptions=IGNORE</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.
4. Start Active Directory Users and Computers, and then navigate to the target OUs. Verify that the workstations and member servers exist in the target OUs.

To migrate workstations and member servers by using a script

- Prepare a script that incorporates ADMT commands and options for migrating workstations and member servers.

For a sample script file to assist you in migrating workstations and member servers, see Migrating User Workstations, earlier in this guide.

**Migrating Domain Controllers**

In some domains, domain controllers are dedicated servers used for authentication only. In other domains, resources are located on domain controllers. Shared local groups provide resource permissions to all domain controllers that support a resource.
Migrating domain controllers is a more complicated process than migrating member servers for the following reasons:

- Windows NT 4.0 backup domain controllers (BDCs) cannot be returned to member server status or moved between domains.
- All domain controller access rights are based on shared local groups that must also be migrated.

For this reason, only migrate domain controllers running Windows NT 4.0 when shared resources are located on the domain controller. Decommission any domain controllers that do not have shared resources.

When deciding the order in which to migrate resource domains, consider the following:

- Migrate resource domains that use domain controllers as dedicated domain controllers first. Then migrate resource domains that use domain controllers hosting resources.
- Migrate all the backup domain controllers in a domain first, and then migrate the PDC.

## Migrating Shared Local Groups

Migrate the shared local groups from the source domain to the target domain before you upgrade the Windows NT 4.0 domain controllers to Windows 2000 Server or Windows Server 2003, and move them to the target domain. It is not necessary to change any access control lists (ACLs) as part of this process. The ACLs continue to reference the shared local groups in the source resource domain. Because the shared local groups were migrated to the target domain as domain local groups (and have the original SID in the SID history), users are able to access the resources as before. ADMT retains the membership of the local group during the migration.

### To migrate shared local groups by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT resource migration account.
2. Use the Group Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>


| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.  
Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| Group Selection | Click **Select groups from domain**, and then click **Next**. On the **Group Selection** page, click **Add** to select the groups in the source domain that you want to migrate, click **OK**, and then click **Next**.  
- or -  
Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Type the name of the OU, or click **Browse**.  
In the **Browse for Container** dialog box, find the container in the target domain that you want to move the global groups into, and then click **OK**. |
| Group Options | Select **Fix membership of group**.  
Select **Migrate Group SIDs to target domain**.  
Ensure that all other options are not selected. |
User Account | Type the user name, password, and domain of an account that has administrative rights in the source domain.
Conflict Management | Click Do not migrate source object if a conflict is detected in the target domain.

3. When the wizard has finished running, click View Log. Review the migration log for any errors.
4. Start Active Directory Users and Computers, and then navigate to the target OU. Verify that the shared local groups exist in the target domain OU.

**Migrating Backup Domain Controllers**

Use the following steps to migrate Windows NT 4.0 BDCs from the source resource domain to the target domain.

- **To migrate backup domain controllers**
  1. Take the BDC offline.
  2. Use Server Manager to promote it to a PDC.
  4. Return the domain controller to stand-alone server status by running the Active Directory Installation Wizard (also known as dcpromo). If you are removing Active Directory from the last domain controller in the domain, select Domain controller is the last controller in the domain.
  5. Join the stand-alone server to the target domain.

**Completing the Resource Migration**

After you migrate all the resources from the source to the target domain, complete the restructuring process by doing the following:

- Transfer the administration of user and group accounts from the source to the target domain.
• Ensure that at least two domain controllers are operational in the source resource domain, until the resource migration process is complete.

• Back up the two domain controllers in the source resource domain.

After completing these steps, you can translate security on the member servers in the target domain and decommission the source resource domain.

Translating Security on Member Servers

Translate security on member servers to clean up access control lists (ACLs). After users and groups are migrated to the target domain, ACLs still contain SIDs from the source domain. The SIDs from the source domain remain in the ACLs, and users can access resources by using SID history while the migration is in progress. However, after the migration is complete, the SIDs from the source domain must be translated to SIDs in the target domain. Use the Security Translation Wizard in ADMT to translate the source domain SIDs to the target domain SIDs that are contained in the ACLs.

You can translate security on member servers by using the ADMT console.

➤ To translate security on member servers

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT resource migration account.

2. Use the Security Translation Wizard in ADMT by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Translation Options</td>
<td>Select <strong>Previously migrated objects</strong>.</td>
</tr>
</tbody>
</table>
### Domain Selection

Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**.

### Computer Selection

Click **Select computers from domain**, and then click **Next**. On the **Computer Selection** page, click **Add** to select the computers in the source domain for which you want to translate security, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**.

### Translate Objects

Clear the **User Profiles** check box. Select all other options.

### Security Translation Options

Select **Add**.

### ADMT Agent Dialog

Select **Run pre-check and agent operation**, and then click **Start**.

---

3. Review the status message for each computer for which you translated security.

4. For computers for which the status is not **Success**, review the message to identify the cause of the failure. For more details about the cause of the failure, click **View Migration Log**, and review the log for any errors that occurred during
the local profile migration process. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

5. For any computers for which the agent failed, fix the cause of the problem, and then perform security translation again on those computers.

---

**Decommissioning the Source Resource Domain**

After you complete the resource migration, decommission the Windows NT 4.0 source resource domains.

**Note**

Ensure that you retain a full system backup of the PDC for each resource domain. This enables you to bring the resource domain back online.

**To decommission the Windows NT 4.0 source resource domain**

1. Remove all trust relationships between the Windows NT 4.0 source resource domain and the Active Directory target domain.

2. Remove any remaining domain controllers in the source resource domain that you did not migrate to the target domain.

3. Disable all accounts that you created during the migration process, including those accounts to which you assigned administrative permissions.

---

**Interforest Active Directory Domain Restructure**

Restructuring Active Directory domains between forests involves relocating objects from source domains in one forest to target domains in another forest. You might need to restructure Active Directory domains between forests for the following reasons:

- Migrating a pilot domain into your production environment.
• Merging with another organization and consolidating the two IT infrastructures.
• Consolidating resource and account domains that you upgraded in-place from a Windows NT 4.0 environment.

However, if your Active Directory environment consists of multiple forests, you might also move objects between forests on a regular basis.

Overview of Restructuring Active Directory Domains Between Forests

Restructuring domains between forests enables you to reduce the number of domains in your organization and therefore the administrative complexity and associated overhead costs of your Active Directory environment. Restructuring domains involves copying accounts and resources from a Windows 2000 or Windows Server 2003 Active Directory source domain to a target domain in a different Active Directory forest. The target domain must be at the Windows 2000 native or Windows Server 2003 domain functional level.

If you completed an in-place upgrade of more than one domain from Windows NT 4.0 to multiple Windows 2000 or Windows Server 2003 forests, you might need to restructure your domains between forests to consolidate the objects because the Windows NT 4.0 Security Accounts Manager (SAM) size limits that restrict the number of objects in a domain do not apply to an Active Directory environment. If your organization has recently merged with another organization or IT infrastructure, then restructuring enables you to consolidate accounts and resources between the two infrastructures.

Process for Restructuring Active Directory Domains Between Forests

Restructuring Active Directory domains between forests involves planning and preparing for the domain restructure for your organization. It also entails successfully migrating accounts and resources to an Active Directory domain in another forest. The following figure shows the process for restructuring Active Directory domains between forests.
Background Information for Restructuring Active Directory Domains Between Forests

The migration process between forests is considered to be non-destructive because the migration objects continue to exist in the source domain until the source domain is decommissioned. Because the source and target domain environments exist simultaneously during the migration, you have the option to roll back to the source environment if necessary. ADMT enables you to migrate accounts and resources between domains while preserving user and object permissions. During the interforest restructure process, users have continuous access to required resources; furthermore, users, groups, and resources can be moved independently of each other.

Before you begin to restructure Active Directory domains between forests, you must be familiar with the account and resource migration process, Windows Server 2003 functional levels, and ADMT.
Account Migration Process

Restructuring accounts between Active Directory forests involves the copying of users, groups, and local profiles from the source domain to the target domain, while preserving the access rights and attributes of those objects.

When user accounts are migrated between Active Directory domains in different forests, the original account remains in place in the source domain and a new account is created in the target domain. Because the security identifier (SID) of a security principal (user or group) always contains an identifier for the domain in which the security principal is located, a new SID is created for the user in the target domain. Because ADMT can migrate the SID of the original security principal to the security principal in the target domain, you do not need to perform additional tasks to ensure resource access, unless you are using SID filtering between the forests.

If you are using Microsoft Exchange Server version 5.5, use the ADMT Exchange Server Migration Wizard to translate security on the mailboxes for migrated users. If you are using Exchange 2000 servers, ADMT does not provide tools for mailbox migration. In this case, plan to migrate mailboxes first by using the Exchange 2000 mailbox migration tool and then migrate user accounts.

If you are using Group Policy to manage folder redirection or software distribution, you need to ensure that these policies continue to apply when you migrate user accounts to a new forest. Also, if you are using a Group Policy object (GPO) to grant or deny remote access in the source domain and not the target domain, then ADMT cannot determine which remote access to assign to the user.

If you are using Group Policy to manage folder redirection, then Offline Files does not work after the user account is migrated to a new forest. Offline Files stores the SID of the user as owner; the SID changes when the user account is migrated. To restore ownership of Offline Files, use the ADMT Security Translation Wizard to replace the permissions on the files and folders on the client computer containing the offline files cache.

To ensure that users continue to have access to Offline Files after you migrate user accounts to the target domain, you can do the following:

1. Translate security on client computers to update the Offline Files.
2. If the SID history of the user account was not migrated to the target domain, translate security on the server that hosts redirected folders.

If you are using folder redirection, one of the following occurs:

- If the folder redirection path is different in the new environment, then users can access the folder if the SID history of the user account was migrated to the target domain. The folder redirection extension copies the files from the original location in
the source domain to the new location in the target domain. SID history enables the user account to access the source folders.

- If the folder redirection path is the same in the new environment, then users cannot access the redirected folder because folder redirection will check ownership of the redirected folder and will fail. You must then translate security on the redirected folder on the server.

If you are using Group Policy to manage software installation and the Windows Installer package requires access to the original source for operations such as repair and remove, then you need to translate security on the software distribution point after you migrate users to ensure that software installation continues to function properly in the target domain.

**Resource Migration Process**

Active Directory domains include three types of resources:

- Workstation accounts
- Member server accounts
- Resources on member servers

The migration of workstations and member servers is a straightforward process. The local groups that you create to assign permissions to users are located in the local SAM database and are moved when you move the server. You do not have to reconfigure access control lists (ACLs) to enable users to access resources after the migration.

In Active Directory, domain controllers can be migrated between domains. To do this, you must remove Active Directory from the domain controller, migrate it as a member server to the target domain, and then reinstall Active Directory. If you have deployed any domain controllers in the target domain that are running Windows Server 2003, then you can only reinstall Active Directory on the migrated server if the server is running Windows Server 2003 or if the forest and domain are operating at the Windows 2000 functional level.

**Functional Levels**

The functional level of a domain or forest defines the set of Windows operating systems that can run on the domain controllers in that domain or forest. The functional level of a domain or forest also defines the additional Windows Server 2003 Active Directory features that are available in that domain or forest.

All target domains must be operating at the Windows 2000 native or Windows Server 2003 functional level.
Planning to Restructure Active Directory Domains Between Forests

Completing the necessary planning tasks before you begin your migration helps ensure that users can continue to log on to the network and access resources during the migration. Planning your domain restructure involves:

- Determining your account migration process.
- Assigning object locations and roles.
- Creating a test plan.
- Creating a rollback plan for use if the migration fails.
- Managing users, groups, and user profiles.
- Creating an end-user communication plan.

To prepare for the restructuring process, the Active Directory deployment team must be sure to obtain the necessary design information from the Active Directory design team.

The following figure shows the steps involved in planning to restructure Active Directory domains between forests.
Determining Your Account Migration Process

With ADMT, you can use SID history to maintain resource permissions when you migrate accounts. However, if SID filtering is enabled between your source and target domains, and you do not trust the administrators in the source domain, you cannot disable SID filtering. Nor can you use SID history to enable access to resources in the source domain. In this case, you must use a different migration process.

You can choose one of the following three methods to migrate accounts between forests while maintaining user rights to access resources in the source domain:

- Migrate user accounts while using SID history for resource access. With this method, you remove SID filtering on the trusts between the domains to enable users to access resources in the source domain by means of their SID history credentials.
- If you have a forest trust in place, you remove SID filtering on the forest trust. (You can also override the forest trust by creating an external trust so that the domain that holds the resources trusts the target domain, and then removing SID filtering on the external trust.)
- If you do not have a forest trust in place, you establish external trusts between the source and target domains. You then need to remove SID filtering on the external trusts if the domain controller used to create the trust is running Windows Server 2003 or Windows 2000 Service Pack 4 (SP4) or later.

For more information about this process, see Migrating Accounts While Using SID History, later in this guide.

- Migrate all users, groups, and resources to the target domain in one step. For more information about this process, see Migrating Accounts While Using SID History, later in this guide.
- Migrate user accounts without using SID history for resource access, but translate security for all resources before the migration process to ensure resource access. For more information about migrating accounts without using SID history, see Migrating Accounts Without Using SID History, later in this guide.

To determine which account migration process is best for your organization, you must first determine if you can disable SID filtering and migrate accounts while using SID history for resource access. You can safely do this if the administrators of the source domain fully trust the administrators of the target domain. You might choose to disable SID filtering if one of the following conditions applies:

- The administrators of the trusting domain are the administrators of the trusted domain.
The administrators of the trusting domain trust the administrators of the trusted domain and are confident that they have secured the domain appropriately. If you disable SID filtering, you remove the security boundary between forests, which otherwise provides data and service isolation between the forests. For example, an administrator in the target domain who has service administrator rights or an individual who has physical access to a domain controller can modify the SID history of an account to include the SID of a domain administrator in the source domain. When the user account for which the SID history has been modified logs on to the target domain, it presents valid domain administrator credentials for, and can obtain access to, resources in the source domain.

For this reason, if you do not trust the administrators in the target domain or do not believe that the domain controllers in the target domain are physically secure, enable SID filtering between your source and target domains, and migrate user accounts without using SID history for resource access.

The following figure shows the decision process involved in determining which migration process is appropriate for your organization.
The best practice for granting access to resources is to use global groups to arrange users, and domain local groups to protect resources. Place global groups into a domain local group to grant the members of the global group access to the resource. A global group can only contain members from its own domain. When a user is migrated between domains, any global groups to which the user belongs must also be migrated. This ensures that users can continue to access resources that are protected by discretionary access control lists (DACLs) referring to global groups. After migrating an account and maintaining the SID history of the source domain account, when a user logs on to the target domain, both the new SID and the original SID from the SID history attribute are
added to the access token of the user. These SIDs determine the local group memberships of the user. The SIDs of the groups of which the user is a member are then added to the access token, together with the SID history of those groups.

Resources within the source and target domains resolve their ACLs to SIDs and then check for matches between their ACLs and the access token when granting or denying access. If the SID or the SID history matches, access to the resource is granted or denied, according to the access specified in the ACL. If the resource is in the source domain and you have not run security translation, it uses the SID history of the user account to grant access.

You can also preserve the original SID for global groups and universal groups in the SID history of the global group or universal group in the target domain. Because local group memberships are based on SIDs, when you migrate the SID to the SID history of the global group or universal group in the target domain, the local group memberships of the global group or universal group are preserved automatically.

SID history is used for:

- Roaming user profile access
- Certification authority access
- Software installation access
- Resource access

If you are not using SID history for resource access, you still need to migrate SID history to facilitate access to those items.

**Using SID Filtering When Migrating User Accounts**

SID filtering does not allow for the use of SIDs from outside the forest to enable access to any resource within the forest. You can enable the SID of a user in a different forest to access a resource within a forest that has SID filtering enabled by translating security on the resource to include the user SID in the permission list. Because SID filtering does not apply to authentication within a domain, it is also possible to allow access to resources by means of SID history, if the resource and the account are in the same domain.

To allow users or groups to access a resource by using SID history, the forest in which the resource is located must trust the forest in which the account is located. SID filtering is applied by default when a forest trust is established between two forest root domains. Also, SID filtering is enabled by default when external trusts are established between
domain controllers running Windows Server 2003 or Windows 2000 SP4 or later. This prevents potential security attacks by an administrator in a different forest.

For more information about SID history–based attacks and SID filtering, see Configuring SID Filtering Settings (http://go.microsoft.com/fwlink/?LinkId=73446).

**Assigning Object Locations and Roles**

Create an object assignment table that lists the roles and locations for all of the objects that you are migrating. Create one table for account objects, such as users, groups, and service accounts, and one table for resource objects, such as workstations, profiles, and domain controllers. In your tables, list the source and target locations for all objects to be migrated.

Before you create your account object assignment table, determine whether the domain organizational unit (OU) structures for the source and target domains are the same. If they are not the same, you must identify the source and target OU in your object assignment tables.

For a worksheet to assist you in creating an account object assignment table, see "User and Group Object Assignment Table" (DSSREER_1.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink?LinkId=14384).

The following figure shows an example of an object assignment table for users and groups.
To create a resource object assignment table, identify the source and target OU for each object and note the physical location and role in the target domain. For a worksheet to assist you in creating a resource object assignment table, see "Resource Object Assignment Table" (DSSREER_2.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink?LinkId=14384).

The following figure shows an example of a resource object assignment table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Source Location</th>
<th>Target Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Group</td>
<td>Asia\Groups OU</td>
<td>EMEA\Groups OU</td>
</tr>
<tr>
<td>Accounting</td>
<td>Group</td>
<td>Asia\Groups OU</td>
<td>EMEA\Groups OU</td>
</tr>
<tr>
<td>JBrown</td>
<td>User</td>
<td>Asia\Users OU</td>
<td>EMEA\Users OU</td>
</tr>
<tr>
<td>NVuyen</td>
<td>User</td>
<td>Asia\Users OU</td>
<td>EMEA\Users OU</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Service Account</td>
<td>Asia\Users OU</td>
<td>EMEA\Service Accounts OU</td>
</tr>
</tbody>
</table>
Developing a Test Plan for Your Migration

ADMT v3 does not include a test migration option which was available in previous versions of ADMT. Develop a test plan to assist you in systematically testing each object after it is migrated to the new environment, and identifying and correcting any problems that might occur. Testing to verify that your migration is successful helps ensure that users who are migrated from the source to the target domain are able to log on, to access resources based on group membership, and to access resources based on user credentials. Testing also helps ensure that users are able to access the resources that you migrate.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Source OU</th>
<th>Target OU</th>
<th>Physical Location</th>
<th>Role in Target Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS01</td>
<td>Member server (file server)</td>
<td>Computers</td>
<td>Member Servers</td>
<td>Hong Kong SAR</td>
<td>Member Server</td>
</tr>
<tr>
<td>User01</td>
<td>Computer account</td>
<td>Default</td>
<td>Wck</td>
<td>Hong Kong SAR</td>
<td>Computer account</td>
</tr>
<tr>
<td>User02</td>
<td>Computer account</td>
<td>Wck</td>
<td>Wck</td>
<td>Boston</td>
<td>Computer account</td>
</tr>
<tr>
<td>DC01</td>
<td>Domain Controller</td>
<td>Domain Controllers</td>
<td>Domain Controllers</td>
<td>Boston</td>
<td>Domain controller</td>
</tr>
<tr>
<td>DC02</td>
<td>Domain Controller</td>
<td>Domain Controllers</td>
<td>Member Servers</td>
<td>Hong Kong SAR</td>
<td>Member server</td>
</tr>
</tbody>
</table>

Resource Assignment Table

Prepared By: Trecorp.treyresearch.net
Target Forest Name: Contcorp.contoso.com
Source Domain Name: Asia.trecorp.treyresearch.net
Target Domain Name: Asia.contcorp.contoso.com

Date: 01/01/03
After your testing is complete, you can proceed with migrating small pilot groups and then gradually increase the size of each batch of migration objects in your production environment.

Use the following process to test the migration of your account object and resource objects:

1. Create a test user in the source domain. Include this test user with your migrations.
2. Join that user to the appropriate global groups to enable resource access.
3. Log on to the source domain as the test user, and verify that you can access resources as appropriate.
4. After you migrate the user account, translate the user profile, and migrate the workstation of the user, log on to the target domain as the test user, and verify that the user has retained all necessary access and functionality. For example, you might test to verify that:
   - The user can log on successfully.
   - The user has access to all appropriate resources, such as file and print shares; access to services such as messaging; and access to line-of-business applications. It is especially important to test access to internally developed applications that access database servers.
   - The user profile was successfully translated, and the user retains desktop settings, desktop appearance, shortcuts, and access to the My Documents folder. Also, verify that applications appear in and start from the Start menu.

You cannot migrate every user property when you migrate user accounts. For more information about user properties that cannot be migrated, see *Migrate User Accounts*, later in this guide.

After you migrate resources, log on as the test user in the target domain, and verify that you can access resources as appropriate.

If any steps in the test process fail, identify the source of the problem, and determine whether you can correct the problem before the object needs to be accessible in the target domain. If you cannot correct the problem before access to the object is required, roll back to your original configuration to ensure access to the user or resource object. For more information about creating a rollback plan, see *Creating a Rollback Plan*, later in this guide.

As part of your test plan, create a migration test matrix. Complete a test matrix for each step that you complete in the migration process. For example, if you migrate 10 batches of users, complete the test matrix 10 times, once for each batch that you migrate. If you migrate 10 member servers, complete the test matrix for each of the 10 servers.
For a worksheet to assist you in creating a test matrix, see Migration Test Matrix (DSSREER_3.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink?LinkId=14384).

The following figure shows an example of a completed migration test matrix.

<table>
<thead>
<tr>
<th>Migration Test Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepared By</strong></td>
</tr>
<tr>
<td>Source Forest Name</td>
</tr>
<tr>
<td>Target Forest Name</td>
</tr>
<tr>
<td>Source Domain Name</td>
</tr>
<tr>
<td>Target Domain Name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Performed Before Migration</th>
<th>Result After Migration</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create test user for users in Sales department “batch”</td>
<td>Yes</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Join user to sales group</td>
<td>Yes</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Log on to source domain and verify access to required resources</td>
<td>Yes</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Log on to target domain</td>
<td>No</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Verify access to file and print shares</td>
<td>No</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Verify access to customer management application</td>
<td>No</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Verify user desktop settings and access to My Documents Folder</td>
<td>No</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Verify that applications appear and start from the Start menu</td>
<td>No</td>
<td>Success</td>
<td></td>
</tr>
</tbody>
</table>
Creating a Rollback Plan

Reduce the risk of disrupting end users in your organization by establishing a rollback plan. In general, it is possible to isolate and resolve any problems that occur during each phase of the migration. However, it is important to analyze potential risks and identify the levels of user impact and downtime that might necessitate rolling back the migration. You might be required to roll back your migration if any of the following occur:

- Users cannot log on to their accounts after migration.
- Users cannot access resources after migration.
- User migration is incomplete; for example, passwords did not migrate.
- User migration was successful, but user workstation migration or local profile translation failed.

If user impact or downtime reaches a level that you have defined as unacceptable in your organization, you can implement your rollback plan and continue to operate in your premigration environment. Because the source domain remains intact during the restructure, you can restore the original environment by completing a few key steps.

To roll back to the premigration environment after migrating account objects:

1. Enable the user accounts in the source domain (if you disabled the accounts during the migration process).
2. Notify the users to log off from the target domain.
3. Notify the users to log on to the source domain.
4. Verify that users are able to access resources.
5. Verify that the logon scripts and user profiles for users work as configured in the source domain.

The rollback process for resource objects is similar to that for account objects. To roll back to the premigration environment after migrating resource objects:

1. Change the domain membership for the server or workstation to the source domain.
2. Restart the server or workstation.
3. Log on as a user and verify that you can access the resource.

**Note**

If you need to modify objects such as member servers or domain controllers in order to migrate them to the target domain, back up all the data before making the modifications and performing the migration.
Managing Users, Groups, and User Profiles

You must define how the objects that you are migrating are to be administered during the interforest restructure process. By establishing administrative procedures for migration objects, you can preserve the objects both in the source and the target domains. Consequently, you can fall back to the premigration environment, if the restructure process is not successful.

Plan for the administration and management of the following types of account migration objects:
- User accounts, including SIDs
- Global group membership
- User profiles

Administering User Accounts

During the migration process, user accounts exist in both the source and the target domains. Administer changes to user accounts in the domain in which the user object is active. Continue to administer changes to group memberships in the source domain while the migration is taking place. Use the Migrate and merge conflicting objects option in ADMT to remigrate user accounts as often as necessary during the migration process. This ensures that changes made to the account in the source domain are propagated to the account in the target domain. This operation merges the existing account and the new account, so that administration of the object can continue in the source domain for the duration of the migration process.

The Migrate and merge conflicting objects option applies the following guidelines when an account is migrated:
- If you change an attribute in the target domain and it is not used in the source domain, it is not overwritten with the NULL value from the source domain.
- If you change an attribute in the target domain and it is used in the source domain, it is overwritten with the value from the source domain.
- If the user has group memberships, the memberships are merged from the source memberships and the target memberships.

If this is not the desired behavior, you can configure ADMT to exclude attributes from being migrated, so that attributes in the target domain are retained.

For example, suppose that after migrating a user, you set attributes on the new user object in the target domain, such as a telephone number or office number. You remigrate
the user by using the **Migrate and merge conflicting objects** option in ADMT, and the new information is retained in the target domain. If you changed the group memberships for the user in the source domain, the changes are propagated to the target domain when you perform the remigration.

Some attributes are excluded from the migration. These include:

- Attributes that are always excluded by the system.
- Attributes that are in the system attribute exclusion list.
- Attributes that are configured by the administrator to be excluded.

### Attributes That Are Always Excluded by the System

Some attributes are always excluded from the migration by ADMT and cannot be configured to be migrated. This protects system-owned attributes. These attributes include:

- Object globally unique identifier (GUID)
- SIDs (although SIDs can be added to the SID history of the object in the target domain)
- LegacyExchangeDN

### System Attribute Exclusion List

The first time that you run an ADMT user migration, ADMT generates a system attribute exclusion list, which it stores in its database. The system attribute exclusion list contains two attributes by default: **mail** and **proxyAddresses**. ADMT also reads the schema in the target domain, and adds any attributes to the list that are not part of the base schema. Attributes in this list are excluded from migration operations even if the attribute is not specified in the attribute exclusion list. An administrator can change the system attribute exclusion list only by using a script. This protects attributes that are important in order for server-based applications, such as Microsoft Exchange, to work. If the target domain schema is further extended after ADMT has generated the list, administrators must manually add the new attributes to the list, unless they are certain that copying the values of these attributes from the source domain will not interfere with server-based applications.

### Attribute Exclusion List

Administrators can define a list of attributes that are excluded from each migration. This is called an attribute exclusion list. By default, when using the ADMT console, state information for attributes that are configured to be excluded is stored in the UI and included in the exclusion list for the next migration. Scripting and command-line attributes
do not have state information and therefore are not stored in the UI. These attributes must be added to the attribute exclusion list for each migration operation, either by means of the attribute name or by means of an option file.

Administering Global Groups

Continue to administer the groups in the source domain during the migration process. Remigrate groups as often as necessary by using the **Migrate and merge conflicting objects** option in ADMT. This ensures that changes made to group memberships in the source domain are propagated to the groups in the target domain.

Planning for a User Profile Migration

User profiles store user data and information about the desktop settings of the user. User profiles can either be roaming or local. The migration process is different for local and for roaming profiles.

Profile translation is one type of security translation, and profiles are translated during the migration process. If you perform security translation in add mode, the SIDs in the target and the source domains both have access to the profile. Therefore, if you need to roll back to the source environment, the SID in the source domain can use the profile. If you perform security translation in replace mode, you must retranslate the profile by using a SID mapping file (undoing the security translation) to roll back to the source environment.

**Important**

If you need to roll back to your original configuration, notify users that profile changes made in the target domain are not reflected in the source domain.

Some organizations might choose not to migrate user profiles. Other organizations might choose to replace users’ workstations during the user account migration process, and use a tool such as the User State Migration Tool (USMT) to migrate user data and settings to the users’ new computers. The following table summarizes the migration requirements for user profiles.
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Migration Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roaming profiles</td>
<td>User profiles are stored centrally on servers. Profiles are available to the user, regardless of the workstation in use.</td>
<td>Select the Translate roaming profiles option on the User Options page in the User Account Migration Wizard. Then, translate local user profiles for a batch of users immediately after you migrate those users.</td>
</tr>
<tr>
<td>Local profiles</td>
<td>User profiles are stored locally on the workstation. When a user logs on to another workstation, a unique local user profile is created.</td>
<td>Translate local profiles as a separate step from the user account migration process. Select the User profiles option on the Translate Objects page of the Security Translation Wizard. Translate local user profiles for a batch of users immediately after migrating those users.</td>
</tr>
<tr>
<td>Profiles not managed</td>
<td>Same as local profiles.</td>
<td>Users lose their existing profiles when their user accounts are migrated.</td>
</tr>
<tr>
<td>Hardware refresh</td>
<td>User state information is stored locally on the workstation.</td>
<td>Migrate as a separate step from the user account migration. Migrate the profiles to the user’s new computer by means of a tool such as USMT.</td>
</tr>
</tbody>
</table>
Creating the End-User Communication Plan

Develop a plan to inform all affected users about the upcoming account migration, to ensure that they understand their responsibilities, the impact of the migration, and who to contact for help and support.

Before you begin the user migration process, send a notice to all users who are scheduled to be migrated. Because you typically migrate users in batches of approximately one hundred users at a time, it is also helpful to send a final notice to the users in each batch two to three days before their batch is scheduled. If your organization maintains an intranet, publish the account migration schedule and the information contained in the user mail on an easily accessible Web page.

Include the following information in your end-user communication.

General Information
Alert users to the fact that their user accounts are scheduled to be migrated to a new domain. Point users to a Web page or internal resource where they can find additional information and view a migration schedule.

Inform users of their new domain name. Be sure to let them know that their account passwords will not change. Let users know that the original domain account will be disabled immediately following the migration, and the disabled account will be deleted after a specified period of time. This is not needed if they log on with user principal names (UPNs).

Impact
Make sure that users understand that when their account is migrated, they might be unable to access some resources, such as Web sites, shared folders, or resources that individuals in their group or division do not widely use.

Provide information to users about whom to contact for assistance in regaining access to required resources.

Logon Status During Migration
Make sure that users understand that during the migration process, they will be unable to log on to the domain or access e-mail or other resources. Be sure to specify the period of time for which they will be unable to log on.
Premigration Steps
Alert users to any steps that they need to complete before the migration process begins. For example, they must decrypt files encrypted by means of Encrypting File System (EFS). Failure to decrypt encrypted files will result in loss of access to encrypted files following the migration.
Users must also ensure that their computers are connected to the network when their account is scheduled to be migrated.

Expected Changes
Describe other changes that users can expect to experience following the migration, such as changes in use of smart cards, secure e-mail, or instant messaging if applicable.

Scheduling and Support Information
Provide information about where users can go to find more information, for example, an internal Web site where you post information about the migration. Also, provide information about whom to contact if a user has a conflict with the date scheduled for the migration.

Preparing the Source and Target Domains
Before you begin to migrate your accounts from the source to the target domains, you need to prepare the source and target domains for the migration. The following figure shows the tasks required to prepare them for the interforest domain restructure process.
Installing 128-Bit High Encryption Software

The computer on which ADMT is installed requires 128-bit high encryption. This encryption is standard on computers running Windows Server 2003 and Windows 2000 Server SP3 or later. If you plan to install ADMT on a computer that does not support 128-bit high encryption by default, you must install the 128-bit high encryption pack.

You can download the encryption pack from Windows 2000 High Encryption Pack (http://go.microsoft.com/fwlink/?LinkId=76037).
Establishing Required Trusts for Your Migration

Before you can migrate accounts and resources from a source domain to a target domain in a different Active Directory forest, you must ensure that the appropriate trusts exist between the forests. Trust relationships between the forests that you are restructuring enables ADMT to migrate users and service accounts and translate local user profiles from the source to the target domains. In addition, depending on how trust relationships are configured, users in the source domains can access resources in the target domains. Moreover, users in the target domains can access resources in the source domains that have not yet been migrated.

To migrate users and global groups, you must establish a one-way trust between the source domain and the target domain, so that the source domain trusts the target domain.

To migrate resources or translate local profiles, you must do one of the following:

- Create a one-way trust between the source domain and the target domain.
- Create a two-way trust between source and target domains.

For more information about creating trusts, see Creating Domain and Forest Trusts (http://go.microsoft.com/fwlink/?LinkId=77381).

Establishing Migration Accounts for Your Migration

To migrate accounts and resources between forests, you must establish migration accounts and assign the appropriate credentials to those accounts. ADMT uses the migration accounts to migrate the objects that you identify. Because ADMT requires only a limited set of credentials, creating separate migration accounts enables you to simplify administration. If the migration tasks for your organization are distributed across more than one group, it is helpful to create a migration account for each group involved in performing the migration.

To simplify administration, create a single account in the source domain and a single account in the target domain for all objects, with the required credentials to modify the objects, such as users, global groups, and local profiles, to be migrated by that account. For example, a migration account that you use to migrate user accounts along with SID history, global groups along with SID history, computers, and user profiles has local administrator or domain administrator credentials in the source domain, and delegated
permission on the user, group, and computer OUs in the target domain, with the extended right to migrate SID history on the user OU. The user needs to be a local administrator on the computer in the target domain on which ADMT is installed. A migration account that you use to migrate workstations and domain controllers must have local administrator or source domain administrator credentials on the workstations or the account must have source domain administrator credentials on the domain controller, or both.

In the target domain, it is necessary to use an account that has delegated permissions on the computer OU and the user OU. You might want to use a separate account for the migration of workstations if this migration process is delegated to administrators that are in the same location as the workstations.

The following table lists the credentials that are required in the source and target domains for different migration objects.

<table>
<thead>
<tr>
<th>Migration Object</th>
<th>Credentials Necessary in Source Domain</th>
<th>Credentials Necessary in Target Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>User/Group without SID history</td>
<td>Delegated <strong>Read all user information</strong> permission on the user OU or group OU and domain administrator credential.</td>
<td>Delegated <strong>Create, delete, and manage user accounts, Create, delete, and manage groups</strong>, and <strong>Modify the membership of a group</strong> for the user OU or the group OU and local administrator on the computer where ADMT is installed.</td>
</tr>
<tr>
<td>User/Group with SID history</td>
<td>Delegated <strong>Read all user information</strong> permission on the user OU or group OU and domain administrator credential.</td>
<td>Delegated permission on the user OU or the group OU, extended permission to migrate SID history, and local administrator on the computer on which ADMT is installed.</td>
</tr>
<tr>
<td>Computer</td>
<td>Domain administrator or administrator in the source domain and on each computer</td>
<td>Delegated permission on the computer OU and local administrator on the computer on which ADMT is installed.</td>
</tr>
</tbody>
</table>
The following procedures provide examples for creating groups or accounts to migrate accounts and resources. Procedures differ according to whether a one-way trust or a two-way trust exists. The procedure for creating migration groups when a one-way trust exists is more complex than the procedure for when a two-way trust exists. This is because, with a one-way trust, you must add the migration group to the local Administrators group on local workstations.

The sample procedure for creating migration groups when a one-way trust exists involves creating separate groups for migrating accounts and resources; however, you can combine acct_migrators and res_migrators into one group, if you do not need to separate them to delegate different sets of permissions.

To create an account migration group when a one-way trust exists in which the source domain trusts the target domain

1. In the target domain, create a global group called acct_migrators.
2. In the target domain, add the acct_migrators group to the Domain Admins group, or delegate administration of OUs that are targets for account migration to this group.
3. If you are migrating SID history, and you did not place the acct_migrators group in the Domain Admins group, grant the acct_migrators group the Migrate SID History extended permission on the target domain object. To do this:
   a. Start Active Directory Users and Computers, right-click the domain object, and then click Properties.
   b. Click the Security tab, click Add, and then select acct_migrators.
      If the Security tab does not appear, in Active Directory Users and Computers, click View, and then click Advanced Features.
   c. In the Permissions for acct_migrators box, click Allow for the Migrate SID History permission.
4. In the source domain, add the acct_migrators group to the Administrators group.
5. On each computer on which you plan to translate local profiles, add the

<table>
<thead>
<tr>
<th>Migration Object</th>
<th>Credentials Necessary in Source Domain</th>
<th>Credentials Necessary in Target Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>Local administrator or domain administrator</td>
<td>Delegated permission on the user OU and local administrator on the computer on which ADMT is installed.</td>
</tr>
</tbody>
</table>

The sample procedure for creating migration groups when a one-way trust exists involves creating separate groups for migrating accounts and resources; however, you can combine acct_migrators and res_migrators into one group, if you do not need to separate them to delegate different sets of permissions.
acct_migrators group to the local Administrators group.

To create a resource migration group when a one-way trust exists in which the source domain trusts the target domain

1. In the target domain, create a global group called res_migrators.
2. In the target domain, add the res_migrators group to the Domain Admins group, or delegate administration of OUs that are targets for resource migration to this group.
3. In the source domain, add the res_migrators group to the Administrators group.
4. On each computer that you plan to migrate or on which you plan to perform security translation, add the res_migrators group to the local Administrators group.

To create a resource migration account when a two-way trust exists between the source and target domains

1. In the source domain, create an account called res_migrator.
2. In the source domain, add the res_migrator account to the Domain Admins group. (The Domain Admins group is a member of the local Administrators group on every computer in the domain by default; therefore, you do not need to add it to the local Administrators group on every computer.)
3. In the target domain, delegate permissions on OUs that are targets for resource migration to the res_migrator account.

ADMT v3 also includes database administration roles that you can use to assign a subset of database permissions to users who perform specific migration tasks. The database administration roles and the migration tasks that they can perform are listed in the following table.

<table>
<thead>
<tr>
<th>Role</th>
<th>Migration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account migrators</td>
<td>Account migrations tasks, such as user and group migration.</td>
</tr>
<tr>
<td>Resource migrators</td>
<td>Resource migration tasks, such as computer migrations and security translation. Account migrators also hold the role of resource migrators.</td>
</tr>
<tr>
<td>Role</td>
<td>Migration task</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data readers</td>
<td>Queries against that database. Account migrators and resource migrators also hold the role of data readers.</td>
</tr>
</tbody>
</table>

Users who are assigned the role of SQL Server sysadmin hold all ADMT database administration roles. They have permissions to do the following:

- Display database roles and users who hold those roles
- Add groups or users to roles
- Remove groups or users from roles

By default, the local Administrators group is assigned the role of sysadmin and can perform all ADMT database functions.

For more information about using database administrator roles, see “Configure Database Administration Roles” in ADMT v3 Help.

---

**Configuring the Source and Target Domains for SID History Migration**

You can manually configure the source and target domains to migrate SID history before you begin an interforest migration, or you can allow ADMT to configure them automatically the first time that it runs.

To configure the source and target domains manually, complete the following procedures:

- Create a local group in the source domain to support auditing.
- Enable TCP/IP client support on the source domain PDC emulator.
- Enable auditing in the Windows Server 2003 source and target domains.

**To create a local group in the source domain to support auditing**

- In the source domain, create a local group called `SourceDomain$$`, where `SourceDomain` is the NetBIOS name of your source domain, for example, Boston$$. Do not add members to this group; if you do, SID history migration will fail.
To enable TCP/IP client support on the source domain PDC emulator

1. On the domain controller in the source domain that holds the PDC emulator operations master role, click Start, and then click Run.

2. In Open, type regedit, and then click OK.

   **Caution**
   Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after you make changes.

3. In Registry Editor, navigate to the following registry subkey:
   
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

4. Modify the registry entry TcpipClientSupport, of data type REG_DWORD, by setting the value to 1.

5. Close Registry Editor, and then restart the computer.

   **Note**
   If you are migrating from a Windows Server 2003 domain to another Windows Server 2003 domain, the TcpipClientSupport registry entry does not have to be modified.

To enable auditing in Windows Server 2003 domains

1. Log on as an administrator to any domain controller in the target domain.

2. Click Start, point to All Programs, point to Administrative Tools, and then click Active Directory Users and Computers.

3. In the console tree, expand the domain, right-click the Domain Controllers OU, and then click Properties.

4. On the Group Policy tab, click Default Domain Controllers Policy, and then click Edit.

5. Double-click Computer Configuration, double-click Windows Settings, double-click Security Settings, double-click Local Policies, and then click Audit Policy.

6. Double-click Audit account management, and then select both the Success and Failure check boxes.

7. Click Apply, and then click OK.

8. Repeat steps 1 through 7 in the source domain.
Configuring the Target Domain OU Structure for Administration

The Active Directory design team creates the OU structure for the target domain. They also define the groups responsible for the administration of each OU and the membership of each group. You can use that information and the following procedure to configure the target domain for administration.

To configure the target domain OU structure for administration

1. Log on as an administrator to any domain controller in the target domain.
2. Start Active Directory Users and Computers, and then create the OU structure specified by your design team.
3. Create administrative groups, and assign users to these groups.
4. Delegate the administration of the OU structure to groups as defined by your design team.

Installing ADMT in the Target Domain

When you install ADMT v3, it also installs Windows SQL Server 2000 Desktop Edition (Windows) (WMSDE) by default to use as its data store. Optionally, you can configure ADMT v3 to use a SQL Server 2000 with SP4 Standard or Enterprise Edition database installation that you have previously created.

Prerequisites for Installing ADMT

Before you install ADMT v3, complete the following prerequisites:

- Install Windows Server 2003. Although you can migrate accounts and resources from Windows NT 4.0 and Active Directory environments using ADMT v3, you can only install ADMT v3 on a server running Windows Server 2003.

- Remove all previous versions of ADMT by using Add or Remove Programs from Control Panel. If you attempt to install ADMT v3 on a server that has a previous version of ADMT installed, you receive an error, and the installation does not proceed. If necessary, you can import the database from the previous version of ADMT (protar.mdb) into ADMT v3 during the installation.
• If you do not plan to use the default local database installation, ensure that another SQL Server 2000 database installation is configured with an ADMT instance. For more information about creating an ADMT instance on a SQL Server 2000 database, see Installing ADMT Using a Preconfigured SQL Database.

Installing ADMT Using the Default Database Store

You can use the default database store or a preconfigured SQL database to install ADMT. The most common and recommended installation method is to use the default database store, which the Active Directory Migration Tool Installation Wizard configures automatically.

To install ADMT using the default database store

• From the download location (http://go.microsoft.com/fwlink/?LinkId=75627), double-click admsetup.exe, which opens the installation wizard.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome to the Active Directory Migration Tool Installation</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Configuring Components</td>
<td>The ADMT database instance (MS_ADMT) is created on the local computer. Although WMSDE is installed locally by default whether ADMT uses it or not, ADMT disables WMSDE if you specify another database instance on the next wizard page.</td>
</tr>
<tr>
<td>Database Selection</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td></td>
</tr>
</tbody>
</table>
| Specify the database instance you want to connect to. The recommended selection is **Use Microsoft SQL Server Desktop Edition (Windows)**, which configures ADMT v3 to use the locally installed database instance. If you are using multiple ADMT v3 consoles or have a dedicated database server where you want to centralize your ADMT database, select the **Use an existing Microsoft SQL Server** option. Specify the server to connect to in the form of `Server\Instance`. If you select this option, see [Installing ADMT Using a Preconfigured SQL Database](#).

You should configure the SQL Server database instance before you select this option. Although the ADMT v3 installation proceeds if the database cannot be contacted, you cannot use ADMT to migrate accounts or resources until the database instance is created and available. |
Although you cannot upgrade an ADMT v2 installation to ADMT v3, you can import data to an ADMT v3 database from an ADMT v2 database. If you do not want to import data from an ADMT v2 database, select **No, do not import data from an ADMT v2 database (Default)**. If you want to import data from ADMT v2 into the new ADMT v3 database, select **Yes, please import data from an ADMT v2 database**. If you choose to import data, specify the path to the ADMT v2 database file. The ADMT v2 database file has the file name protar.mdb, and should be located in the directory formerly used for your ADMT v2 installation.

**Summary**

This page summarizes the options you selected. To complete the ADMT v3 installation, click **Finish**.

### Installing ADMT Using a Preconfigured SQL Database

If you plan to use multiple ADMT consoles or if you have a dedicated database server where you want to centralize your ADMT database, you can create another SQL Server database instance for ADMT instead of using the default local database. If you choose to install ADMT in an instance of SQL Server 2000, install SQL Server 2000 with SP4. To create the ADMT instance on the SQL Server, use the command-line syntax in the following table from any server that can target the SQL Server.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admtdb create /s</td>
<td><strong>server</strong>:</td>
</tr>
</tbody>
</table>
Syntax | Description
---|---
`admtdb create [/(i|j|import): "v2 database path"]` | Specifies the fully qualified path to the protar.mdb database file that was used with a previous ADMT v2 installation. Required `/server` parameter must be specified with this option. ADMT v2 data can be imported at the time of creation, or later into an empty database using the `admtdb import` command.

For all `admtdb.exe` command-line options, type `admtdb /?` at a command prompt.

After the database has been configured, navigate to the folder where you downloaded ADMT v3 and double-click `admtsetup.exe`.

In the Active Directory Migration Tool Installation Wizard, on the Database Selection page, select the **Use an existing Microsoft SQL Server** option and specify the server to connect to in the form of `Server\Instance`.

If you decide to use the local database after configuring a remote instance of a SQL Server database, use the following procedure.

**To use the default local database after configuring a remote instance of a SQL Server database**

1. On the local computer, click **Start**, point to **Administrative Tools**, and then click **Services**.
2. In the right pane, navigate to `MSSQL$MS_ADMT`, verify that the **Status** column displays **Started**, and that the **Startup Type** is set to **Automatic**. If the `MSSQL$MS_ADMT` service is not **Started**, right-click `MSSQL$MS_ADMT`, and then click **Properties**.
3. On the **General** tab, in the **Startup Type** drop-down list, click **Automatic**.
4. Under **Service Status**, click the **Start** button, and then click **OK**.
5. Close **Services**.
6. Open a command prompt, and then type:

   `admt config /setdatabase: Server\Instance`. You can now use the default local database.
Enabling Migration of Passwords

Use the Password Export Server (PES) service to migrate passwords when you perform an interforest migration. The PES service can be installed on any domain controller in the source domain that supports 128-bit encryption.

The PES service installation in the source domain requires an encryption key. However, you must create the encryption key on the computer running the ADMT in the target domain. When you create the key, save it to a shared folder on your network or onto removable media. This way, you can store it in a secure location and reformat it after the migration is complete.

To create an encryption key

- At a command line, type the following:

  admn key /option:create
  /sourcedomain:SourceDomain/keyfile:KeyFilePath/keypassword:{password*}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SourceDomain</td>
<td>Specifies the name of the source domain in which the PES service is being installed. Can be specified as either the Domain Name System (DNS) or NetBIOS name.</td>
</tr>
<tr>
<td>KeyFilePath</td>
<td>Specifies the path to the location where the encrypted key is stored.</td>
</tr>
<tr>
<td>{password*}</td>
<td>A password, which provides key encryption, is optional. To protect the shared key, type either the password or an asterisk on the command line. The asterisk causes you to be prompted for a password that is not displayed on the screen.</td>
</tr>
</tbody>
</table>

After you create the encryption key, configure the PES service on a domain controller in the source domain.

ADMT provides the option to run the PES service under the Local System account or by using the credentials of an authenticated user in the target domain. It is recommended that you run the PES service as an authenticated user in the target domain. This way,
you do not need to add the Everyone group and the Anonymous Logon group to the Pre-Windows 2000 Compatible Access group.

Note

If you run the PES service under the Local System account, ensure that the Pre-Windows 2000 Compatible Access group in the target domain contains the Everyone group and the Anonymous Logon group.

To configure the PES service in the source domain

1. On the domain controller that runs the PES service in the source domain, insert the encryption key disk.
2. In the %systemroot%\Windows\ADMT\PES folder, run Pwdmig.msi. If you set a password during the key generation process on the domain controller in the target domain, provide the password that was given when the key was created, and then click Next.
3. If you plan to run the PES service as an authenticated user account, specify the account in the format domain\user_name.
4. After installation completes, restart the domain controller.
5. After the domain controller restarts, to start the PES service, point to Start, point to All Programs, point to Administrative Tools, and then click Services.
6. In the details pane, right-click Password Export Server Service, and then click Start.

Note

Run the PES service only when you migrate passwords. Stop the PES service after you complete the password migration.

Initializing ADMT by Running a Test Migration

Initialize ADMT by running a test migration of a global group, and select the option named Migrate Group SIDs to target domain. If you did not previously configure the source and target domains to migrate SID history, you will receive an error and a prompt for each item that has not yet been configured. When you accept each prompt, ADMT automatically completes the following tasks, which are required to enable SID history migration:
• Creates a local group, source_domain$$$, in the source domain, which is used to audit SID history operations. Do not add members to this group; if you do, SID history migration will fail.

• Enables TCP/IP client support on the source domain PDC by setting the value of the registry entry TcpipClientSupport to 1. This entry is located in the following subkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

  Setting TcpipClientSupport to 1 enables remote procedure calls (RPCs) over the TCP transport, while preserving the security of the system.

• Enables audit policies in the source and target domains.

For more information about configuring the source and target domains to migrate SID history, see Configuring the Source and Target Domains to Migrate SID History, earlier in this guide.

Use the following procedure to initialize ADMT.

➢ To initialize ADMT by running a test migration of a global group

1. In the ADMT console, use the Group Account Migration Wizard by following the steps provided in the following table. Accept default settings when no information is specified.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under Source, in the Domain drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the Domain controller drop-down list, type or select the name of the domain controller, or select Any domain controller. Under Target, in the Domain drop-down list, type or select the NetBIOS or DNS name of the target domain. In the Domain controller drop-down list, type or select the name of the domain controller, or select Any domain controller, and then click Next.</td>
</tr>
</tbody>
</table>
| Group Selection | Click Select groups from domain, and then click Next. On the Group Selection page, click Add to select the groups in the source domain that you want to migrate, click OK, and then click Next. 
- or - 
Click Read objects from an include file, and then click Next. Type the location of the include file, and then click Next. |
|-----------------|---------------------------------------------------------------------------------------------------------------|
| Organizational Unit Selection | Type the name of the OU, or click Browse. 
In the Browse for Container dialog box, find the container in the target domain that you want to move the global groups into, and then click OK. |
| Group Options | Select the Migrate Group SIDs to target domain check box. Make sure that all other options are not selected. |
| User Account | Type the user name, password, and domain of an account that has administrative rights in the source domain. |
| Conflict Management | Click Do not migrate source object if a conflict is detected in the target domain. |

2. When the wizard has finished running, click View Log, and then review the migration log for any errors.

3. Verify that the test migration configured ADMT properly by ensuring that:
   - A new local group source_domain$$$ exists in the source domain. This account supports ADMT auditing of SID history migration.
   - The registry entry TcpipClientSupport is created, and its value is set to 1, in the following subkey on the source domain PDC:
Identifying Service Accounts for Your Migration

Identify the member servers and domain controllers in the source domain that run applications in the context of a service account. A service account is a user account that provides a security context for applications and that is granted permission to log on as a service. ADMT does not migrate services that run in the context of the Local System account because they are migrated when the computer is migrated; however, services that run in the context of a user account must be updated on the computer after you have completed the account migration process. ADMT also cannot migrate the Local Service or Network Service accounts because they are well-known accounts that always exist in Windows Server 2003.

The process of identifying, migrating, and updating services that run in the context of user accounts involves three steps. First, the administrator starts ADMT from the target Active Directory domain controller and runs the Service Account Migration Wizard. For the second step, the Service Account Migration Wizard sends an agent to a specified computer and identifies (but does not migrate) all services on the computer that are running in the context of a user account. The last step, which can occur later in the migration process, is to migrate the accounts when other user accounts are migrated with the User Account Migration Wizard.

The Service Account Migration Wizard scans an administrator-defined list of servers for services that are configured to use a domain account to authenticate. The accounts are then flagged as service accounts in the ADMT database. The password is never migrated when a service account is migrated. Instead, ADMT uses a clear-text representation of the password to configure the services after the service account migration. An encrypted version of the password is then stored in the password.txt file in the ADMT installation folder.

An administrator of a workstation or server can install any service and configure the service to use any domain account. If the administrator cannot configure the service to authenticate with the correct password, the service will not start. After the service account is migrated, ADMT configures the service on the workstation or the server to use the new password, and the service will now start under the user account.
Include in the Service Account Migration Wizard only those servers that trusted administrators manage. Do not use the wizard to detect service accounts on computers that trusted administrators do not manage, such as workstations.

Dispatch agents to all servers that trusted administrators manage in the domain to ensure that you do not overlook any service accounts. If you miss a service account that shares an account with a service that has already been migrated, it is not possible for ADMT to synchronize them. You must manually change the password for the service account and then reset the service account password on each server that is running that service.

When the accounts that the Service Account Migration Wizard identifies in the ADMT database as running in the context of a user account are migrated to the target domain, ADMT grants each account the right to log on as a service. If the service account is assigned rights by means of its membership in a group, the Security Translation Wizard updates the account to assign those rights. For more information about running the Security Translation Wizard, see Transitioning Service Accounts, later in this guide.

You can identify service accounts by using the ADMT console, the ADMT command-line option, or a script.

To identify service accounts by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. In the ADMT console, log on by using the ADMT account migration account and then use the Service Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Domain Selection**

Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**.

**Update Information**

Click **Yes, update the information**.

**Computer Selection Option**

Click **Select computers from domain**, and then click **Next**. On the **Service Account Selection** page, click **Add** to select the accounts in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**.

**Agent Dialog**

In **Agent Actions**, select **Run pre-check and agent operation**, and then click **Start**. A message will appear in the Agent Summary when the agent operations are complete. After the agent operations finish, click **Close**.
Service Account Information | Select any user accounts that do not need to be marked as service accounts in the ADMT database, and then click **Skip/Include** to mark the accounts as **Skip**.

The wizard connects to the selected computers, and then sends an agent to check every service on the remote computers. The Service Account Information page lists the services that are running in the context of a user account and the name of that user account. ADMT notes in its database that these user accounts need to be migrated as service accounts. If you do not want a user account to be migrated as a service account, select the account, and then click **Skip/Include** to change the status from **Include** to **Skip**.

You use **Update SCM** to update the Service Control Manager with the new information. Unless you have a failure in reaching a computer to update the service, the **Update SCM** button is not available. If you have a problem updating a service account after the account was identified and migrated, ensure that the computer that you are trying to reach is available, and then restart the Service Account Migration Wizard.

In the wizard, click **Update SCM** to try to update the service. If you ran the Service Account Migration Wizard previously and the **Update SCM** button is not available, examine the ADMT log files to determine the cause of the problem. After you correct the problem and the agent can connect successfully, the **Update SCM** button becomes available.

To identify service accounts by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. At the command line, type:

   ```
   ADMT SERVICE /N "computer_name1" "computer_name2" /SD:"source_domain" /TD:"target_domain"
   ```

   *Computer_name1* and *computer_name2* are the names of computers in the source domain that run service accounts.

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT SERVICE /N "computer_name1" "computer_name2" /O:"option_file.txt"
   ```

The following table lists the common parameters used for the identification of service accounts, along with the command-line parameter and option file.
equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.

**To identify service accounts by using a script**

- Create a script that incorporates ADMT commands and options for identifying service accounts by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="IdentifyingServiceAccounts" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
    Option Explicit

    Dim objMigration
    Dim objServiceAccountEnumeration

    'Create instance of ADMT migration objects.
    Set objMigration = CreateObject("ADMT.Migration")
    Set objServiceAccountEnumeration = objMigration.CreateServiceAccountEnumeration

    'Specify general migration options.

    objMigration.SourceDomain = "source domain"

    'Enumerate service accounts on specified computers.

    objServiceAccountEnumeration.Enumerate admtData, _
    Array("computer name1", "computer name2")

    Set objServiceAccountEnumeration = Nothing
    Set objMigration = Nothing
</Script>
```
Migrating Accounts

The process of migrating account objects from a source domain to a target domain in another Active Directory forest involves first migrating service accounts, and then migrating global groups. After the groups are in place in the target domain, you can migrate users according to the process that you selected, either while using SID history for resource access, or without using SID history for resource access. When the account object migration process is complete, you can instruct users from the source domain to log on to the target domain. The following figure shows the process for migrating accounts between domains in different forests.
Transitioning Service Accounts in Your Migration

Begin the process of migrating objects by migrating service accounts. For information about identifying service accounts for migration, see Identifying Service Accounts for Your Migration, earlier in this guide.

To transition service accounts, use ADMT to complete the following tasks:

- Migrate the service accounts from the source domain to the target domain.
- Modify the services on each server in the source domain, so that they use the service account in the target domain instead of in the source domain.

You can transition service accounts by using the ADMT console, the ADMT command-line option, or a script.

To transition service accounts by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. Use the User Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
| **User Selection** | Click **Select users from domain**, and then click **Next**. On the **User Selection** page, click **Add** to select the accounts in the source domain that you want to migrate, click **OK**, and then click **Next**.  
- or -  
Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| **Organizational Unit Selection** | Click **Browse**.  
In the **Browse for Container** dialog box, locate the source domain, select the container for the service accounts, and then click **OK**. |
| **Password Options** | Click **Generate complex passwords**. |
| **Account Transition Options** | Click **Enable target accounts**.  
Select the **Migrate user SIDs to target domains** check box. |
| **User Account** | Type the user name, password, and domain of a user account that has administrative credentials. |
| **User Options** | Select the **Update user rights** check box.  
Ensure that no other settings are selected, including **Migrate associated user groups**. |
| **Conflict Management** | Click **Do not migrate source object if a conflict is detected in the target domain**. |
Service Account Information | Click **Migrate all service accounts and update SCM for items marked include**. If you are also migrating other user accounts that are not service accounts, this wizard page tells you that you have selected some accounts that are marked as service accounts in the ADMT database. By default, the accounts are marked as Include. To change the status of the account, select the account, and then click **Skip/Include**. Click **Next** to migrate the accounts.

3. When the wizard has finished running, click **View Log**, and review the migration log for any errors.

4. Start Active Directory Users and Computers, navigate to the OU that you created for service accounts, and then verify that the service accounts exist in the target domain OU.

5. Confirm that each application for which the service account was relocated continues to function correctly.

To transition service accounts by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type:

   \[
   \text{ADMT USER /N "server_name1" "server_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /MSS:YES}
   \]

   \[
   \text{ADMT USER /N "server_name1" "server_name2" /O: "option_file.txt"}
   \]

   Server\_name1 and Server\_name2 are the names of servers in the source domain that run service accounts. Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   \[
   \text{ADMT USER /N "server_name1" "server_name2" /o: "option_file.txt"}
   \]

   The following table lists the common parameters used for transitioning service accounts, along with the command-line parameter and option file equivalents.
3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers and locate the target service account OU. Verify that the service accounts exist in the target domain OU.

To transition service accounts by using a script

- Prepare a script that incorporates ADMT commands and options for transitioning service accounts by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmConstants.vbs file.

```vbscript
Option Explicit
Dim objMigration
Dim objUserMigration

Set objMigration = CreateObject("ADMT.Migration")
Set objUserMigration = objMigration.CreateUserMigration
```
Migration of Global Groups

To preserve the memberships of global groups, you must migrate global groups before you migrate users.

**Note**

Do not migrate global groups during peak work hours. The global group migration process can consume a large amount of network resources and resources on the domain controller in the target domain.

Global group migration involves the following steps:
1. The administrator selects global group objects in the source domain.
2. A new global group object is created in the target domain, and a new primary SID is created for the object in the target domain.
3. To preserve resource access, ADMT adds the SID of the global group in the source domain to the SID history attribute of the new global group in the target domain.

Following the migration, events are logged in both the source and the target domain.

**Note**

If the user account migration process takes place over an extended period of time, you might need to remigrate global groups from the source to the target domain. The objective is to propagate membership changes that are made in the source domain before the migration process is complete. For more information about remigrating global groups, see [Remigrating All Global Groups After All Batches Are Migrated](#), later in this guide.

You can migrate global groups by using the ADMT console, the ADMT command-line option, or a script.

➤ To migrate global groups by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. Use the Group Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
| Group Selection               | Click **Select groups from domain**, and then click **Next**. On the **Group Selection** page, click **Add** to select the groups in the source domain that you want to migrate, click **OK**, and then click **Next**.  
- or -  
Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Type the name of the OU, or click **Browse**.  
In the **Browse for Container** dialog box, find the container in the target domain that you want to move the global groups into, and then click **OK**. |
| Group Options                | Click **Migrate Group SIDs to target domain**.  
Make sure that all other options are not selected. |
| User Account                 | Type the user name, password, and domain of an account that has administrative rights in the source domain. |
| Conflict Management          | Click **Do not migrate source object if a conflict is detected in the target domain**. |

3. When the wizard has finished running, click **View Log**, and review the migration log for any errors.

4. Open the Active Directory Users and Computers console, and then locate the target OU. Verify that the global groups exist in the target domain OU.

**To migrate global groups by using the ADMT command line option**

1. On the computer in the target domain on which ADMT is installed, log on by
using the ADMT account migration account.

2. At the command line, type the ADMT Group command with the appropriate parameters. For example:

```
ADMT GROUP /N "group_name1" "group_name2" /SD:"source_domain"
/TO:"target OU" /MSS:YES
```

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT GROUP /N "group_name1" "group_name2" /o: "option_file.txt"
```

The following table lists the common parameters used for migrating global groups, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Migrate GG SIDs</td>
<td>/MSS:YES</td>
<td>MigrateSIDs=YES</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO:IGNORE (default)</td>
<td>ConflictOptions=IGNORE</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.

4. Open the Active Directory Users and Computers console and locate the target OU. Verify that the global groups exist in the target domain OU.

To migrate global groups by using a script

- Prepare a script that incorporates ADMT commands and options for migrating global groups by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```
<Job id="MigratingGlobalGroupsBetweenForests" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
  Option Explicit
</Script>
```
Migrating Accounts While Using SID History

To migrate accounts while using SID history, first migrate all user accounts, but do not enable them in the target domain, to prepopulate the target domain and allow migration of user profiles. After all user accounts are successfully migrated, begin migrating users in batches by migrating first the user profile, then the workstation, then the user account.
Before migrating all user accounts, ensure that you have created test accounts that you can include in each batch to verify the success of the migration for that batch.

You cannot migrate every user property when you migrate user accounts. For example, Protected Storage (Pstore) contents for Windows NT 4.0 workstations, including Encrypting File System (EFS) private keys, are not migrated by ADMT when you migrate user accounts. To migrate Pstore contents, you must export and import keys during the migration process.

For clients that are running Windows 2000 Server or later, data that is protected by the Data Protection API (DPAPI) is also not migrated. DPAPI helps protect the following items:

- Web page credentials (for example, passwords)
- File share credentials
- Private keys associated with EFS, S/MIME, and other certificates
- Program data that is protected by using the CryptProtectData() function

For this reason, it is important to test user migrations. Use your test migration account to identify any properties that did not migrate, and update user configurations in the target domain accordingly.

Complete the following steps to migrate user accounts to the target domain:

1. Migrate all user accounts with the account enabled in the source domain, disabled in the target domain, with complex password selected, and with no attributes migrated.
2. Translate local user profiles for a batch of users.
3. Migrate workstations in batches that correspond to the user account batches.
4. Before migrating the batch of user accounts, verify that local profile and workstation migration succeeded for all users in the batch. Do not migrate any user account for which profile or workstation migration failed. This will result in users overwriting their existing profiles when they log on to the target domain.
5. Remigrate user accounts in batches with the account set to expire in the source domain in seven days, the target account enabled, with password migration selected, and all attributes migrated.
6. After each batch, remigrate all global groups to update any group membership changes.
7. Notify users in the batch to log on to the target domain.
8. After all users are migrated, run a final global group migration to update any group membership changes.

Migrating user accounts in batches enables you to track the accounts that have been migrated and to test the success of each migration step. If the OU structure for the target domain is the same as the OU structure for the source domain, migrate groups of users
based on OU. If the OU structures are not the same, select an alternate way to group users based on the structure of your organization. For example, you might migrate users by business unit or by floor to enable you to consolidate help desk resources.

If you plan to retain your source domain OU structure, migrate the OU along with the users that they contain. For example, if your source domain is a Windows Server 2003 Active Directory environment that has a functional OU structure, and the target domain does not have an OU structure, migrate OUs from the source domain.

If you created a new OU structure in the target domain, migrate batches of users without the OUs. For example, if your source environment was a Windows NT 4.0 domain that you upgraded to a Windows Server 2003 domain, the source domain might not have an existing OU structure; therefore, you can migrate users without migrating OUs.

For more information about creating an OU structure, see Designing Organizational Units for Delegation of Administration (http://go.microsoft.com/fwlink/?LinkId=76628).

Until you migrate all user and group accounts, continue to administer global group membership in the source domain. To support a rollback strategy, manually synchronize any changes you make to users in the target domain with the existing user accounts in the source domain. For more information about administering users and groups during the interforest restructure process, see Managing Users, Groups, and User Profiles, earlier in this guide.

If you are migrating OUs when you migrate user accounts, migrate the groups that belong to those OUs to the target domain OU during the user account migration process. When you migrate global groups by using the global group migration process, they are placed in the target OU in the target domain. If you migrate OUs from the source to the target domain, select the option to move the global groups to the target domain at the same time. This way, the groups are moved from the target OU that they were placed in during the initial global group migration to the OU in which they belong.

Using ADMT to migrate user accounts preserves group memberships. Because global groups can contain only members from the domain in which the group is located, when users are migrated to a new domain, the user accounts in the target domain cannot be members of the global groups in the source domain. As part of the migration process, ADMT identifies the global groups in the source domain that the user accounts belong to, and then determines whether the global groups have been migrated. If ADMT identifies global groups in the target domain that the migrated users belonged to in the source domain, the tool adds the users to the appropriate global groups in the target domain.

Using ADMT to migrate user accounts also preserves user passwords. After the user accounts are migrated to and enabled in the target domain, the users can log on to the target domain by using their original passwords. After they log on, the users are prompted to change the password.
If the user account migration process is successful but the password migration process fails, ADMT creates a new complex password for the user account in the target domain. By default, ADMT stores new complex passwords in the C:\Program Files\Active Directory Migration Tool\Logs\Password.txt file.

If you have a Group Policy setting on the target domain that does not allow blank passwords (the Default Domain Policy/Computer Configuration/Security Settings/Account Policies/Password Policy/Minimum password length setting is set to any number other than zero), password migration will fail for any user who has a blank password. ADMT generates a complex password for that user, and writes an error to the error log.

Establish a method for notifying users who have been assigned new passwords. For example, you can create a script to send an e-mail message to users to notify them of their new passwords.

The following figure shows the steps involved in migrating accounts if you are using SID history for resource access.
Migrating All User Accounts

Begin the user account migration process by migrating all users. This enables you to translate local profiles and ensure that users continue to have the appropriate resource access following the migration.

**Note**

Built-in accounts (such as Administrators, Users, and Power Users) cannot be ADMT migration objects. Because built-in account SIDs are identical in every domain, migrating these accounts to a target domain results in duplicate SIDs in a single domain. Every SID in a domain must be unique. Well-known accounts (such as Domain Admins and Domain Users) also cannot be ADMT migration objects.

The ADMT user account migration process includes the following steps:

1. ADMT reads the attributes of the source user objects.
2. ADMT creates a new user object in the target domain and a new primary SID for the new user account.
3. ADMT adds the original SID of the user account to the SID history attribute of the new user account.
4. ADMT migrates the password for the user account.
5. If ADMT identifies global groups in the target domain that the migrated users belonged to in the source domain, the tool adds the users to the appropriate global groups in the target domain.

During the migration, audit events are logged in both the source and the target domains.

You can migrate user accounts by using the ADMT console, by using the ADMT command-line option, or by using a script.

**To migrate the current batch of users by using the ADMT console**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. Use the User Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>

...
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| User Selection | Click **Select users from domain**, and then click **Next**. On the **User Selection** page, click **Add** to select the users in the source domain that you want to migrate in the current batch, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Ensure that ADMT lists the correct target OU. If it is not correct, type the correct OU, or click **Browse**.

In the **Browse for Container** dialog box, locate the target domain and OU, and then click **OK**. |
| Password Options | Click **Do not update passwords for existing users**.

Click **Generate complex passwords**. |
| Account Transition Options | In **Target Account State**: click **Disable target accounts**.  
In **Source Account Disabling Options**: click **Days until source accounts expire**; and then type the numbers of days you want to keep the source account. A value of 7 is commonly used.  
Select the **Migrate user SIDs to target domains** check box. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account</td>
<td>Type the user name, password, and domain of a user account that has administrative credentials in the source domain.</td>
</tr>
</tbody>
</table>
| User Options                | Select the **Translate roaming profiles** check box.  
Clear the **Update user rights** check box.  
Clear the **Migrate associated user groups** check box.  
Select the **Fix users’ group memberships** check box. |
| Object Property Exclusion   | Clear the **Exclude specific object properties from migration** check box. |
| Conflict Management         | Click **Do not migrate source object if a conflict is detected in the target domain**.  
Ensure that the **Before merging remove user rights for existing target accounts** and **Move merged objects to specified target Organizational Unit** check boxes are not selected. |

3. When the wizard has finished running, click **View Log**, and then review the migration log for any errors.
4. Start Active Directory Users and Computers, and then verify that the user accounts exist in the appropriate OU in the target domain.

To migrate user accounts by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT User command with the appropriate parameters. For example:

   ```
   ADMT USER /N "user_name1" "user_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /MSS:YES /TRP:YES /UUR:NO
   ```

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT USER /N "user_name1" "user_name2" /O "option_file.txt"
   ```

   The following table lists the common parameters used for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Migrate SIDs</td>
<td>/MSS:YES</td>
<td>MigrateSIDs=YES</td>
</tr>
<tr>
<td>Disable Option</td>
<td>/DOT:DISABLETARGET</td>
<td>DISABLEOPTION=DISABLETARGET</td>
</tr>
<tr>
<td>Source Expiration</td>
<td>/SEP:7</td>
<td>SOURCEEXPIRATION=7</td>
</tr>
<tr>
<td>Conflict Management</td>
<td>/CO:IGNORE (default)</td>
<td>ConflictOptions=IGNORE</td>
</tr>
<tr>
<td>Translate Roaming Profile</td>
<td>/TRP:YES (default)</td>
<td>TranslateRoamingProfile=YES</td>
</tr>
<tr>
<td>Update User Rights</td>
<td>/UUR:NO</td>
<td>UpdateUserRights=NO</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers and locate the target OU. Verify that the users exist in the target OU.

To migrate user accounts by using a script

- Prepare a script that incorporates ADMT commands and options for migrating users by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmConstants.vbs file.

In your script, specify the source and target container names in the relative canonical format. For example, if the container is a child OU named Sales and its parent OU is named West, then specify West/Sales as the container name. For more information, see TemplateScripts.vbs in the ADMT installation folder.

```vbscript
Option Explicit

Dim objMigration
Dim objUserMigration

'Create instance of ADMT migration objects.

Set objMigration = CreateObject("ADMT.Migration")
Set objUserMigration = objMigration.CreateUserMigration

'Specify general migration options.

objMigration.SourceDomain = "source domain"
objMigration.SourceOu = "source container"
objMigration.TargetDomain = "target domain"
objMigration.TargetOu = "target container"
objMigration.PasswordOption = admtComplexPassword
objMigration.ConflictOptions = admtIgnoreConflicting

'Specify user migration specific options.
```
Remigrating User Accounts and Workstations in Batches

Remigrating user accounts and workstations in batches helps you track the migration process. For each batch of users, first translate local user profiles, and then migrate workstations. Verify that the profile and workstation migration succeeded, and then migrate the user accounts. Remigrate global groups after each batch. For more information, see Remigrating All Global Groups After All Batches Are Migrated, later in this guide.

Translating Local User Profiles


User profiles are stored locally on the workstation. When a user logs on to another workstation, he or she must create a new, unique local user profile. Translate the local user profiles for the first batch of users immediately after migrating all user accounts.

Local profiles are translated in replace mode because if you perform the profile translation in add mode, certain aspects of software installation that use Group Policy software deployment might not work. Any application that is packaged with Windows Installer version 2.0 (which is included on workstations running Windows 2000 Server
SP3 or later and Windows XP SP1 or later, as well as in many common software packages) might not function after the profile is translated. For example, the application executable files might not be removed after the last user removed the application. When the ADMT Security Translation Wizard is translating local profiles in replace mode, it reverts to add mode if a profile is locked. This might result in a successful profile translation; however, application installations might not function after the profile is translated.

Note

The night before you notify the users to log on by using their new accounts in the target domain, translate the local user profiles. Translating profiles the night before ensures that the new user profile reflects the most current user settings.

You can translate local user profiles by using the ADMT console, the ADMT command-line option, or a script.

To translate local user profiles by using the ADMT console

1. For each workstation in the source domain that is running Windows NT 4.0, Windows 2000 Server, or Windows XP, add the ADMT resource migration account to the local Administrators group.

2. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

3. Use the Security Translation Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Translation Options</td>
<td>Click <strong>Previously migrated objects</strong>.</td>
</tr>
</tbody>
</table>
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| Computer Selection Option | Click **Select computers from domain**, and then click **Next**. On the **Computer Selection** page, click **Add** to select the computers in the source domain for which you want to translate security, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Translate Objects | Click **User Profiles**. |
| Security Translation Options | Click **Replace**. |
| ADMT Agent Dialog | Select **Run pre-check and agent operation**, and then click **Start**. |

4. Review the results that are displayed on the screen for any errors. After the wizard completes, click **View Migration Log** to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named
MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

To translate local user profiles by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT Security command with the appropriate parameters. For example:

   ADMT SECURITY /N "computer_name1" "computer_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /TOT:Replace /TUP:YES

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ADMT SECURITY /N "computer_name1" "computer_name2" /o "option_file.txt"

   The following table lists the common parameters used for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Security translation options</td>
<td>/TOT:REPLACE</td>
<td>TranslateOption=REPLACE</td>
</tr>
<tr>
<td>Modify local user profile security</td>
<td>/TUP:YES</td>
<td>TranslateUserProfiles=YES</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click View Migration Log to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.
To translate local user profiles by using a script

- Prepare a script that incorporates ADMT commands and options for translating local user profiles by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```vb
Option Explicit
Dim objMigration
Dim objSecurityTranslation

'Create instance of ADMT migration objects.

Set objMigration = CreateObject("ADMT.Migration")
Set objSecurityTranslation = objMigration.CreateSecurityTranslation

'Specify general migration options.

objMigration.SourceDomain = "source domain"
objMigration.TargetDomain = "target domain"
objMigration.TargetOu = "Computers"

'Specify security translation specific options.

objSecurityTranslation.TranslationOption = admtTranslateReplace
objSecurityTranslation.TranslateUserProfiles = True

'Perform security translation on specified computer objects.

objSecurityTranslation.Translate admData, _
Array("computer name1", "computer name2")

Set objSecurityTranslation = Nothing
Set objMigration = Nothing
</Script>
</Job>
```
Migrating Workstations in Batches

After you migrate a batch of local user profiles, migrate the corresponding batch of user workstations. When you migrate a workstation between domains, the SAM database is migrated along with the computer. Accounts located in the local SAM database (such as local groups) that are used to enable access to resources always move with the computer, and therefore do not need to be migrated.

**Note**

Use a low value for the `RestartDelay` parameter to restart workstations immediately after joining them to the target domain, or as soon as possible thereafter. Resources that are not restarted following migration are in an indeterminate state.

You can migrate workstations and member servers by using the AMDT console, ADMT command-line option, or a script.

**To migrate workstations by using the ADMT console**

1. On the computer in the target domain on which you installed ADMT, log on by using the ADMT resource migration account.
2. Use the Computer Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click Next.</td>
</tr>
</tbody>
</table>
| Computer Selection | Click **Select computers from domain**, and then click **Next**. On the **Computer Selection** page, click **Add** to select the computers in the source domain that you want to migrate, click **OK**, and then click **Next**.  
- or -  
Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Click **Browse**. In the **Browse for Container** dialog box, locate the target domain **Computers** container or the appropriate OU, and then click **OK**. |
| Translate Objects | Select the **Local groups** check box. Select the **User rights** check box. |
| Security Translation Options | Click **Add**. |
| Computer Options | In the **Minutes before computer restart after wizard completion** box, accept the default value of 5 minutes or type a different value. |
| Object Property Exclusion | To exclude certain object properties from the migration, select the **Exclude specific object properties from migration** check box, select the object properties that you want to exclude and move them to the **Excluded Properties** box, and then click **Next**. |
| Conflict Management | Click **Do not migrate source object if a conflict is detected in the target domain**. |
3. Review the results that are displayed on the screen for any errors. After the wizard completes, click View Migration Log to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#.ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

4. Open Active Directory Users and Computers and verify that the workstations exist in the appropriate OU in the target domain.

To migrate workstations by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT resource migration account.

2. At the command line, type the ADMT Computer command with the appropriate parameters. For example, type:

   ```
   ADMT COMPUTER /N "computer_name1" "computer_name2"
   /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /RDL:5
   ```

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT COMPUTER /N "computer_name1" "computer_name2"
   /O:"option_file.txt"
   ```

The following table lists the common parameters used for workstation migration, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors. The migration log lists computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file for that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

4. Open Active Directory Users and Computers and locate the target OU. Verify that the workstations and member servers exist in the target OU.

To migrate workstations by using a script

- Prepare a script that incorporates ADMT commands and options for migrating workstations by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="MigratingWorkstationsBetweenForest">
  <Script language="VBScript" src="AdmtConstants.vbs" />
  <Script language="VBScript">
    Option Explicit

    Dim objMigration
    Dim objComputerMigration

    ' Create instance of ADMT migration objects.

    Set objMigration = CreateObject("ADMT.Migration")
    Set objComputerMigration = objMigration.CreateComputerMigration

    ' Specify general migration options.
  </Script>
</Job>
```
Remigrating User Accounts in Batches

After you have verified the success of local user profile and user workstation migration for the user batch, migrate the user accounts for that batch. You can migrate user accounts in batches by using the ADMT console, the ADMT command-line option, or a script.

To migrate the current batch of user accounts by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. Complete the User Account Migration Wizard by following the steps in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.  
  **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| --- | --- |
| User Selection | Click **Select users from domain**, and then click **Next**. On the **User Selection** page, click **Add** to select the users in the source domain that you want to migrate in the current batch, click **OK**, and then click **Next**.  
- or -  
Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Ensure that ADMT lists the correct target OU. If it is not correct, type the correct OU, or click **Browse**.  
In the **Browse for Container** dialog box, locate the target domain and OU, and then click **OK**. |
| Password Options | Click **Migrate Passwords**.  
In **Password migration source DC:** type the name of the password export server or accept the default value. |
3. When the wizard has finished, click **View Log**, and review the migration log for any errors.

4. Open Active Directory Users and Computers and verify that the user accounts
exist in the appropriate OU in the target domain.

To migrate the current batch of users by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT User command with the appropriate parameters. For example:

   ADMT USER /N "user_name1" "user_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /MSS:YES /TRP:YES /UUR:YES

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ADMT USER /N "user_name1" "user_name2" /O "option_file.txt"

The following table lists the common parameters used for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Migrate SIDs</td>
<td>/MSS:YES</td>
<td>MigrateSIDs=YES</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO:REPLACE</td>
<td>ConflictOptions=REPLACE</td>
</tr>
<tr>
<td>Translate Roaming Profile</td>
<td>/TRP:YES (default)</td>
<td>TranslateRoamingProfile=YES</td>
</tr>
<tr>
<td>Update User Rights</td>
<td>/UUR:YES</td>
<td>UpdateUserRights=YES</td>
</tr>
<tr>
<td>Password Options</td>
<td>/PO:COPY /PS:&lt;name of PES server&gt;</td>
<td>PasswordOption=COPY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PasswordServer=:&lt;name of PES server&gt;</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers and locate the target OU. Verify that the users exist in the target OU.

➤ To migrate the current batch of user accounts by using a script

- Prepare a script that incorporates ADMT commands and options for migrating users by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmConstants.vbs file.

```vbnet
<Job id="MigratingUserAccountsInBatchesBetweenForests" /> <Script language="VBScript" src="AdmConstants.vbs" /> <Script language="VBScript" >
Option Explicit
Dim objMigration
Dim objUserMigration

' Create instance of ADMT migration objects.

Set objMigration = CreateObject("ADMT.Migration")
Set objUserMigration = objMigration.CreateUserMigration

' Specify general migration options.

objMigration.SourceDomain = "source domain"
objMigration.SourceOu = "source container"
objMigration.TargetDomain = "target domain"
objMigration.TargetOu = "target container"
objMigration.PasswordOption = admtCopyPassword
objMigration.PasswordServer = "password export server name"
objMigration.ConflictOptions = admtReplaceConflicting

' Specify user migration specific options.

objUserMigration.SourceExpiration = 7
objUserMigration.MigrateSIDs = True
objUserMigration.TranslateRoamingProfile = True
objUserMigration.UpdateUserRights = True
objUserMigration.FixGroupMembership = True
```
Remigrating All Global Groups Following User Account Migration

A large user account migration might take place over an extended period of time. For this reason, you might need to remigrate global groups from the source to the target domain after you migrate each batch of users, to reflect changes made to the membership of groups in the source domain after the initial global group migration occurred. For more information about, and procedures, for remigrating global groups, see Remigrating All Global Groups After All Batches Are Migrated, later in this guide.

Remigrating All Global Groups After All Batches Are Migrated

After all batches have been migrated, perform a final global group remigration to ensure that any late changes made to global group membership in the source domain are reflected in the target domain. You can remigrate global groups by using the ADMT console, the ADMT command-line option, or a script.

To remigrate global groups by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. Use the Group Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
|---|---|
| Group Selection | Click **Select groups from domain**, and then click **Next**. On the **Group Selection** page, click **Add** to select the groups in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Type the name of the OU, or click **Browse**.

In the **Browse for Container** dialog box, find the container in the target domain that you want to move the global groups into, and then click **OK**. |
Group Options

| Group Options | Click **Update user rights.**
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ensure that <strong>Copy group members</strong> is not selected.</td>
</tr>
<tr>
<td></td>
<td>Ensure that <strong>Update previously migrated objects</strong> is not selected.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Fix membership of group.</strong></td>
</tr>
<tr>
<td></td>
<td>Click <strong>Migrate Group SIDs to target domain.</strong></td>
</tr>
</tbody>
</table>

User Account

| User Account | Type the user name, password, and domain of an account that has administrative rights in the source domain. |

Object Property Exclusion

| Object Property Exclusion | Clear the **Exclude specific object properties from migration** check box. |

Conflict Management

| Conflict Management | Select the **Migrate and merge conflicting objects** check box (all other options are cleared). |

3. When the wizard has finished running, click **View Log**, and review the migration log for any errors.

4. Open Active Directory Users and Computers and locate the target OU. Verify that the global groups exist in the target domain OU.

**To remigrate global groups by using the ADMT command-line option**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT Group command with the appropriate parameters. For example:

   ```
   ADMT GROUP /N "group_name1" "group_name2" /SD:"source_domain" /TD:"target domain" /TO:"target OU" /MSS:YES /CO:REPLACE
   ```

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT GROUP /N "group_name1" "group_name2" /O: "option_file.txt"
   ```

The following table lists the common parameters used for migrating global
groups, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Migrate GG SIDs</td>
<td>/MSS:YES</td>
<td>MigrateSIDs=YES</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO:REPLACE</td>
<td>ConflictOptions=REPLACE</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers and locate the target OU. Verify that the global groups exist in the target domain OU.

To remigrate global groups by using a script

- Prepare a script that incorporates ADMT commands and options for migrating global groups by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="RemigratingGlobalGroupsBetweenForests" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
    Option Explicit
    Dim objMigration
    Dim objGroupMigration
    
    'Create instance of ADMT migration objects.
    
    Set objMigration = CreateObject("ADMT.Migration")
    Set objGroupMigration = objMigration.CreateGroupMigration
    
    'Specify general migration options.
```
Migrating Accounts Without Using SID History

If you are not using SID history for resource access because SID filtering is in place between your forests, your migration process involves first migrating all user accounts, but not enabling them in the target domain, to prepopulate the target domain and allow migration of user profiles. Then you run security translation on all resources that the users access across forests. The next step is to migrate users in batches by migrating first the user profile, then the workstation, then the user account. Finally, you must remigrate the global groups to apply any changes made to the global groups in the source domain, and translate security in remove mode.

It is still important to migrate SID history although user accounts will not use SID history for resource access. This ensures that operations such as Offline Files continue to function within the forest. Migrating SID history does not present a security risk because SID filtering is in place between the source and target forests. Before migrating all user
accounts, ensure that you have created test accounts that you can use to verify the success of each batch.

Complete the following steps to migrate user accounts to the target domain:

1. Migrate all users. Use the **Fix users’ group membership** option both to have ADMT identify global groups in the target domain that the user belonged to in the source domain and to add the user to the appropriate global group in the target domain. For this initial user migration, leave the user account enabled in source domain, and disabled in the target domain.

2. Translate security in add mode for files, shares, printers, local groups, and domain local groups.

3. Translate local user profiles for a batch of users.

4. Migrate workstations in batches that correspond to the user account batches.

5. Before migrating the batch of user accounts, verify that local profile and workstation migration succeeded for all users in the batch. Do not migrate any user account for which profile or workstation migration failed, because this will result in users overwriting their existing profiles when they log onto the target domain.

6. Remigrate user accounts in small batches with the accounts in the source domain set to expire in seven days, the target accounts enabled, password migration selected, and all attributes selected for migration.

7. After each batch, remigrate all global groups to update any group membership changes.

8. After all users are migrated, run a final global group migration to update any group membership changes.

9. Translate security in remove mode for files, shared folders, printers, local groups, and domain local groups.

10. Notify users in the batch to log on to the target domain.

Until you migrate all user and group accounts, continue to administer global group membership in the source domain.

The following figure shows the steps involved in migrating accounts that are not using SID history for resource access.
Migration of All User Accounts

Begin the user account migration process by migrating all users. You can then translate security on all files, printers, shared folders, local groups, and domain local groups. This ensures that users continue to have the appropriate resource access following the migration.

**Note**

Built-in accounts (such as Administrators, Users, and Power Users) cannot be ADMT migration objects. Because built-in account SIDs are identical in every domain, migrating these accounts to a target domain results in duplicate SIDs in a single domain. Every SID in a domain must be unique. Well-known accounts (such as Domain Admins and Domain Users) also cannot be ADMT migration objects.

The ADMT user account migration process includes the following steps:

1. ADMT reads the attributes of the source user objects.
2. ADMT creates a new user object in the target domain and a new primary SID for the new user account.
3. ADMT adds the original SID of the user account to the SID history attribute of the new user account.
4. ADMT migrates the password for the user account.
5. If ADMT identifies global groups in the target domain that the migrated users belonged to in the source domain, the tool adds the users to the appropriate global groups in the target domain.

During the migration, audit events are logged in both the source and the target domains.

You can migrate user accounts by using the ADMT console, the ADMT command-line option, or a script.

#### To migrate user accounts by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. Use the User Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Section</td>
<td>Instructions</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| User Selection               | Click Select users from domain, and then click Next. On the User Selection page, click Add to select the users in the source domain that you want to migrate in the current batch, click OK, and then click Next.  
- or -  
On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account. |
| Organizational Unit Selection| Ensure that ADMT lists the correct target OU. If it is not correct, type the correct OU, or click Browse.  
In the Browse for Container dialog box, locate the target domain and OU, and then click OK. |
| Password Options             | Click Do not update passwords for existing users.  
Click Generate complex passwords. |
| Account Transition Options   | In Target Account State:, click Disable target accounts.  
In Source Account Disabling Options:, click Days until source accounts expire:, and then type the numbers of days you want to keep the source account. A value of 7 is commonly used.  
Select the Migrate user SIDs to target domains check box. |
| User Account                 | Type the user name, password, and domain of a user account that has administrative credentials in the source domain. |
### User Options

| Select the **Translate roaming profiles** check box. |
| Select the **Update user rights** check box. |
| Clear the **Migrate associated user groups** check box. |
| Select **Fix users’ group memberships**. |

### Object Property Exclusion

Clear the **Exclude specific object properties from migration** check box.

### Conflict Management

Select the **Do not migrate source object if a conflict is detected in the target domain** check box.  
Ensure that the **Before merging remove user rights for existing target accounts** and **Move merged objects to specified target Organizational Unit** check boxes are not selected.

3. When the wizard finishes, click **View Log**, and review the migration log for any errors.

4. Open Active Directory Users and Computers, and verify that the user accounts exist in the appropriate OU in the target domain.

---

**To migrate user accounts by using the ADMT command-line option**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT User command with the appropriate parameters. For example:

```
ADMT USER /N "user_name1" "user_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /MSS:YES /TRP:YES /UUR:YES
```

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT USER /N "user_name1" "user_name2" /O "option_file.txt"
```
The following table lists the common parameters used for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD: &quot;source_domain&quot;</td>
<td>SourceDomain= &quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO: &quot;source_OU&quot;</td>
<td>SourceOU= &quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD: &quot;target_domain&quot;</td>
<td>TargetDomain= &quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO: &quot;target_OU&quot;</td>
<td>TargetOU= &quot;target_OU&quot;</td>
</tr>
<tr>
<td>Migrate SIDs</td>
<td>/MSS:YES</td>
<td>MigrateSIDs=YES</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO:IGNORE (default)</td>
<td>ConflictOptions=IGNORE</td>
</tr>
<tr>
<td>Translate Roaming Profile</td>
<td>/TRP:YES (default)</td>
<td>TranslateRoamingProfile=YES</td>
</tr>
<tr>
<td>Update User Rights</td>
<td>/UUR:YES</td>
<td>UpdateUserRights=YES</td>
</tr>
<tr>
<td>Password Options</td>
<td>/PO:COMPLEX (default)</td>
<td>PasswordOption=COMPLEX</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers and locate the target OU. Verify that the users exist in the target OU.

**To migrate user accounts by using a script**

- Prepare a script that incorporates ADMT commands and options for migrating users by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="MigratingAllUserAccountsBetweenForests">
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript">
  Option Explicit
</Script>
</Job>
```
Dim objMigration
Dim objUserMigration

'Create instance of ADMT migration objects."

Set objMigration = CreateObject("ADMT.Migration")
Set objUserMigration = objMigration.CreateUserMigration

'Specify general migration options."

objMigration.SourceDomain = "source domain"
objMigration.SourceOu = "source container"
objMigration.TargetDomain = "target domain"
objMigration.TargetOu = "target container"
objMigration.PasswordOption = admtComplexPassword
objMigration.ConflictOptions = admtIgnoreConflicting

'Specify user migration specific options."

objUserMigration.MigrateSIDs = True
objUserMigration.TranslateRoamingProfile = True
objUserMigration.UpdateUserRights = True
objUserMigration.FixGroupMembership = True
objUserMigration.MigrateServiceAccounts = False

'Migrate specified user objects."

objUserMigration.Migrate admtData, Array("user name1", "user name2")

Set objUserMigration = Nothing
Set objMigration = Nothing
</Script>
</Job>

Translating Security in Add Mode

Translate security on servers to add the SIDs of the user and group accounts in the target domain to the access control lists (ACLs) of the resources. After objects are
migrated to the target domain, the objects contain the ACL entries from both the source and the target domains. Use the Security Translation Wizard in ADMT to add the target domain SIDs from the migrated objects. Run the Security Translation Wizard on all files, shares, printers, local groups, and at least one domain controller (to translate security on shared local groups).

You can translate security in add mode on objects by using the ADMT console, the ADMT command-line option, or a script.

To translate security in add mode on objects by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. Use the Security Translation Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Translation Options</td>
<td>Click <strong>Previously migrated objects.</strong></td>
</tr>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
Computer Selection

Click **Select computers from domain**, and then click **Next**. On the **Computer Selection page**, click **Add** to select the computers for which you want to translate security, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**.

---

Translate Objects

Clear the **User Profiles** check box. Select all other check boxes.

Security Translation Options

Click **Add**.

ADMT Agent Dialog

Select **Run pre-check and agent operation**, and then click **Start**.

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click **View Migration Log** to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

To translate security in add mode on objects by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT Security command with the appropriate parameters. For example:

   ```
   ADMT SECURITY /N "computer_name1" "computer_name2"
   /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /TOT:Add
   ```

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT SECURITY /N "computer_name1" "computer_name2" /o
   ```
The following table lists the common parameters used for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD: &quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD: &quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Security translation</td>
<td>/TOT: Add</td>
<td>TranslateOption=ADD</td>
</tr>
<tr>
<td>options</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click View Migration Log to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

To translate security in add mode on objects by using a script

- Prepare a script that incorporates ADMT commands and options for translating security in add mode on objects by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmConstants.vbs file.

```vbscript
<Job id="TranslatingSecurityInAddModeOnObjectsBetweenForests">
<Script language="VBScript" src="AdmConstants.vbs" />
<Script language="VBScript" >
    Option Explicit
    Dim objMigration
    Dim objSecurityTranslation

    'Create instance of ADMT migration objects.

    Set objMigration = CreateObject("ADMT.Migration")
    Set objSecurityTranslation = objMigration.CreateSecurityTranslation
```
'Specify general migration options.

objMigration.SourceDomain = "source domain"
objMigration.TargetDomain = "target domain"
objMigration.TargetOu = "Computers"

' Specify security translation specific options.

objSecurityTranslation.TranslationOption = admtTranslateAdd
objSecurityTranslation.TranslateFilesAndFolders = True
objSecurityTranslation.TranslateLocalGroups = True
objSecurityTranslation.TranslatePrinters = True
objSecurityTranslation.TranslateRegistry = True
objSecurityTranslation.TranslateShares = True
objSecurityTranslation.TranslateUserProfiles = False
objSecurityTranslation.TranslateUserRights = True

' Perform security translation on specified computer objects.

objSecurityTranslation.Translate admtData, _
Array("computer name1" ,"computer name2" )

Set objSecurityTranslation = Nothing
Set objMigration = Nothing
</Script>
</Job>

Remigration of User Accounts and Workstations in Batches

Remigrating user accounts and workstations in batches helps you track the migration process. For each batch of users, first translate local user profiles, and then migrate workstations. Verify that the profile and workstation migration succeeded, and then migrate the user accounts. Remigrate global groups after each batch. For more information, see Remigrating All Global Groups After All Batches Are Migrated, later in this guide.
Translating Local User Profiles


Local profiles are translated in replace mode because if you perform the profile translation in add mode, software installation by means of Group Policy software deployment might not work. Any application that is packaged with Windows Installer version 2.0 (which is used on workstations running Windows 2000 Server SP3 or later, Windows XP SP1 or later, and in many common software packages) might not function after the profile is translated. When the ADMT Security Translation Wizard is translating local profiles in replace mode, it reverts to add mode if a profile is locked. This might result in a successful profile translation; however, application installations might not function after the profile is translated.

Before you start the local user profile translation, allow enough time for the workstations to restart after you move them to the target domain. Allow for the ADMT time delay factor (five minutes by default) plus the time required for a restart cycle for your workstations.

Note

The night before you notify the users to log on by using their new accounts in the target domain, translate the local user profiles. Translating profiles the night before ensures that the new user profile reflects the most current user settings.

You can translate local user profiles by using the ADMT console, the ADMT command-line option, or a script.

To translate local user profiles by using the ADMT console

1. For each workstation in the source domain that is running Windows NT 4.0, Windows 2000 Server, or Windows XP, add the ADMT resource migration account to the local Administrators group.

2. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

3. Use the Security Translation Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Translation Options</td>
<td>Click <strong>Previously migrated objects</strong></td>
</tr>
</tbody>
</table>
Domain Selection

Under Source, in the Domain drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the Domain controller drop-down list, type or select the name of the domain controller, or select Any domain controller.

Under Target, in the Domain drop-down list, type or select the NetBIOS or DNS name of the target domain. In the Domain controller drop-down list, type or select the name of the domain controller, or select Any domain controller, and then click Next.

Computer Selection

Click Select computers from domain, and then click Next. On the Computer Selection page, click Add to select the computers in the source domain for which you want to translate security, click OK, and then click Next.

- or -

Click Read objects from an include file, and then click Next. Type the location of the include file, and then click Next.

Translate Objects

Click User Profiles.

Security Translation Options

Click Replace.

ADMT Agent Dialog

Select Run pre-check and agent operation, and then click Start.

4. Review the results that are displayed on the screen for any errors. After the wizard completes, click View Migration Log to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named
To translate local user profiles by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT Security command with the appropriate parameters. For example:

```
ADMT SECURITY /N "computer_name1" "computer_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /TOT:Replace /TUP:YES
```

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT SECURITY /N " computer_name1" " computer_name2" /o "option_file.txt"
```

The following table lists the common parameters used for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Security translation options</td>
<td>/TOT:REPLACE</td>
<td>TranslateOption=REPLACE</td>
</tr>
<tr>
<td>Modify local user profile security</td>
<td>/TUP:YES</td>
<td>TranslateUserProfiles=YES</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click View Migration Log to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.
To translate local user profiles by using a script

- Prepare a script that incorporates ADMT commands and options for translating local user profiles by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```vbs
<Job id="TranslatingLocalProfilesBetweenForests" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
  Option Explicit

  Dim objMigration
  Dim objSecurityTranslation

  'Create instance of ADMT migration objects.

  Set objMigration = CreateObject("ADMT.Migration")
  Set objSecurityTranslation = objMigration.CreateSecurityTranslation

  'Specify general migration options.

  objMigration.SourceDomain = "source domain"
  objMigration.TargetDomain = "target domain"
  objMigration.TargetOu = "Computers"

  'Specify security translation specific options.

  objSecurityTranslation.TranslationOption = admtTranslateReplace
  objSecurityTranslation.TranslateUserProfiles = True

  'Perform security translation on specified computer objects.

  objSecurityTranslation.Translate admtdata, _
  Array("computer name1", "computer name2")

  Set objSecurityTranslation = Nothing
  Set objMigration = Nothing
</Script>
</Job>
```
Migrating Workstations in Batches

After you migrate a batch of local user profiles, migrate the corresponding batch of user workstations. When you migrate a workstation between domains, the SAM database is migrated along with the computer. Accounts located in the local SAM database (such as local groups) that are used to enable access to resources always move with the computer, and therefore do not need to be migrated.

**Note**

To restart workstations immediately after joining them to the target domain, or as soon as possible thereafter, use a low value for the ADMT `RestartDelay` parameter. Resources that are not restarted following migration are in an indeterminate state.

You can migrate workstations by using the ADMT console, the ADMT command-line option, or a script.

▶ **To migrate workstations by using the ADMT console**

1. On the computer in the target domain on which you installed ADMT, log on by using the ADMT resource migration account.
2. Use the Computer Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
| Computer Selection | Click **Select computers from domain**, and then click **Next**. On the **Computer Selection** page, click **Add** to select the computers in the source domain that you want to migrate, click **OK**, and then click **Next**.  
- or -  
Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Click **Browse**.  
In the **Browse for Container** dialog box, locate the target domain **Computers** container or the appropriate OU, and then click **OK**. |
| Translate Objects | Select the **Local groups** check box.  
Select the **User rights** check box. |
| Security Translation Options | Click **Add**. |
| Computer Options | In the **Minutes before computer restart after wizard completion** box, accept the default value of 5 minutes or type a different value. |
| Object Property Exclusion | To exclude certain object properties from the migration, select the **Exclude specific object properties from migration** check box, select the object properties that you want to exclude and move them to the **Excluded Properties** box, and then click **Next**. |
| Conflict Management | Click **Do not migrate source object if a conflict is detected in the target domain**. |
ADMT Agent Dialog

Select Run pre-check and agent operation, and then click Start.

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click View Migration Log to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#.ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

4. Open Active Directory Users and Computers, and verify that the workstations exist in the appropriate OU in the target domain.

To migrate workstations by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT resource migration account.

2. At the command line, type the ADMT Computer command with the appropriate parameters. For example, type:

   `ADMT COMPUTER /N "computer_name1" "computer_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" RDL:5`

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   `ADMT COMPUTER /N "computer_name1" "computer_name2" /O:"option_file.txt"`

The following table lists the common parameters used for workstation migration, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors. The migration log lists computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file for that computer to review any problems with local groups. The log file for each computer is named `MigrationTask#_ComputerName.log` and is stored in the `Windows\ADMT\Logs\Agents` folder.

4. Open Active Directory Users and Computers, and locate the target OU. Verify that the workstations exist in the target OU.

To migrate workstations by using a script

- Prepare a script that incorporates ADMT commands and options for migrating workstations by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a `.wsf` file name extension in the same folder as the `AdmtConstants.vbs` file.

```vbscript
<Job id="MigratingWorkstationsBetweenForest">
  <Script language="VBScript" src="AdmtConstants.vbs"/>
  <Script language="VBScript">
    Option Explicit

    Dim objMigration
    Dim objComputerMigration

    'Create instance of ADMT migration objects.

    Set objMigration = CreateObject("ADMT.Migration")
    Set objComputerMigration = objMigration.CreateComputerMigration

    'Specify general migration options.
```
Remigrating User Accounts in Batches

After you have verified the success of migrating local user profiles and user workstations for the user batch, migrate the user accounts for that batch.

You can migrate user accounts in batches by using the ADMT console, the ADMT command-line option, or a script.

To remigrate the current batch of user accounts by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. Use the User Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| User Selection | Click **Select users from domain**, and then click **Next**. On the **User Selection** page, click **Add** to select the users in the source domain that you want to migrate in the current batch, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Ensure that ADMT lists the correct target OU. If it is not correct, type the correct OU, or click **Browse**.

In the **Browse for Container** dialog box, locate the target domain and OU, and then click **OK**. |
| Password Options | Click **Migrate Passwords**.

In **Password migration source DC:** type the name of the password export server or accept the default value. |
| Account Transition Options | In **Target Account State**: click **Enable target accounts**.  
In **Source Account Disabling Options**: click **Days until source accounts expire**; and then type the numbers of days you want to keep the source account. A value of 7 is commonly used.  
Select the **Migrate user SIDs to target domains** check box. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account</td>
<td>Type the user name, password, and domain of a user account that has administrative credentials.</td>
</tr>
</tbody>
</table>
| User Options               | Select the **Translate roaming profiles** check box.  
Select the **Update user rights** check box.  
Select the **Migrate associated user groups** check box.  
Select **Fix users’ group memberships** check box. |
| Object Property Exclusion  | Clear the **Exclude specific object properties from migration** check box. |
| Conflict Management        | Click **Migrate and merge conflicting objects**.  
Clear the **Before merging remove user rights for existing target accounts** check box.  
Clear the **Move merged objects to specified target Organizational Unit** check box. |

3. When the wizard finishes, click **View Log**, and review the migration log for any errors.  
4. Open Active Directory Users and Computers and verify that the user accounts
exist in the appropriate OU in the target domain.

To remigrate the current batch of users by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. At the command line, type the ADMT User command with the appropriate parameters. For example:

   ADMT USER /N "user_name1" "user_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /MSS:YES /TRP:YES /UUR:YES

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ADMT USER /N "user_name1" "user_name2" /O "option_file.txt"

The following table lists the common parameters used for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Migrate SIDs</td>
<td>/MSS:YES</td>
<td>MigrateSIDs=YES</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO:REPLACE</td>
<td>ConflictOptions=REPLACE</td>
</tr>
<tr>
<td>Translate Roaming Profile</td>
<td>/TRP:YES (default)</td>
<td>TranslateRoamingProfile=YES</td>
</tr>
<tr>
<td>Update User Rights</td>
<td>/UUR:YES</td>
<td>UpdateUserRights=YES</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors.

4. Open Active Directory Users and Computers, and locate the target OU. Verify that the users exist in the target OU.

**To remigrate the current batch of user accounts by using a script**

- Prepare a script that incorporates ADMT commands and options for migrating users by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="MigratingUserAccountsInBatchesBetweenForests" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
  Option Explicit
  Dim objMigration
  Dim objUserMigration
  ,
  'Create instance of ADMT migration objects.
  ,
  Set objMigration = CreateObject("ADMT.Migration")
  Set objUserMigration = objMigration.CreateUserMigration
  ,
  'Specify general migration options.
  ,
  objMigration.SourceDomain = "source domain"
  objMigration.SourceOu = "source container"
  objMigration.TargetDomain = "target domain"
  objMigration.TargetOu = "target container"
  objMigration.PasswordOption = admtCopyPassword
  objMigration.PasswordServer = "password export server name"
  objMigration.ConflictOptions = admtReplaceConflicting
  ,
  'Specify user migration specific options.
  ,
```
Remigrating All Global Groups Following User Account Migration

A large user account migration might take place over an extended period of time. For this reason, you might need to remigrate global groups from the source to the target domain after you migrate each batch of users. The objective is to reflect changes made to group membership in the source domain after the initial global group migration has occurred. For more information about, and procedures for, remigrating global groups, see Remigration of All Global Groups After All Batches Are Migrated, later in this guide.

Remigration of All Global Groups After All Batches Are Migrated

After all batches have been migrated, perform a final global group remigration to ensure that any late changes made to global group membership in the source domain are reflected in the target domain.

You can remigrate global groups by using the ADMT console, the ADMT command-line option, or a script.

To remigrate global groups by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. Use the Group Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Group Selection</td>
<td>Click <strong>Select groups from domain</strong>, and then click <strong>Next</strong>. On the <strong>Group Selection</strong> page, click <strong>Add</strong> to select the groups in the source domain that you want to migrate, click <strong>OK</strong>, and then click <strong>Next</strong>. - or - Click <strong>Read objects from an include file</strong>, and then click <strong>Next</strong>. Type the location of the include file, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Organizational Unit Selection</td>
<td>Type the name of the OU, or click <strong>Browse</strong>. In the <strong>Browse for Container</strong> dialog box, find the container in the target domain that you want to move the global groups into, and then click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
3. When the wizard has finished running, click View Log, and review the migration log for any errors.

4. Open Active Directory Users and Computers, and locate the target OU. Verify that the global groups exist in the target domain OU.

To remigrate global groups by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT Group command with the appropriate parameters. For example:

   ```
   ADMT GROUP /N "group_name1" "group_name2" /SD:"source_domain"
   /TD:"target domain" /TO:"target OU" /MSS:YES /CO:REPLACE
   ```

   Alternatively, you can include parameters in an option file that is specified at the
command line as follows:

```
ADMT GROUP /N "group_name1" "group_name2" /O: "option_file.txt"
```

The following table lists the common parameters used for migrating global
groups, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD: &quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO: &quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD: &quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO: &quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Migrate GG SIDs</td>
<td>/MSS: YES</td>
<td>MigrateSIDs=YES</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO: REPLACE</td>
<td>ConflictOptions=REPLACE</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers, and locate the target OU. Verify
that the global groups exist in the target domain OU.

**To remigrate global groups by using a script**

- Prepare a script that incorporates ADMT commands and options for migrating
global groups by using the sample script shown in the following listing. Copy the
script to Notepad, and save the file with a .wsf file name extension in the same
folder as the AdmtConstants.vbs file.

```vbscript
<Job id="RemigratingGlobalGroupsBetweenForests" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
    Option Explicit
    Dim objMigration
    Dim objGroupMigration

    'Create instance of ADMT migration objects.

    Set objMigration = CreateObject("ADMT.Migration")
```
Translating Security in Remove Mode

Translate security on objects to remove the SIDs of the accounts in the source domain from the ACLs of the migrated objects. Do this only after all of the source accounts are disabled. Run the Security Translation Wizard on all files, shared folders, printers, and local groups, and at least one domain controller (to translate security on shared local groups).

You can translate security in remove mode on objects by using the ADMT console, the ADMT command-line option, or a script.

To translate security in remove mode on objects by using the ADMT console
1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

```vbscript
Set objGroupMigration = objMigration.CreateGroupMigration

' Specify general migration options.

objMigration.SourceDomain = "source domain"
objMigration.SourceOu = "source container"
objMigration.TargetDomain = "target domain"
objMigration.TargetOu = "target container"
objMigration.ConflictOptions = admtReplaceConflicting

' Specify group migration specific options.

objGroupMigration.MigrateSIDs = True

'Migrate specified group objects.

objGroupMigration.Migrate admtData, Array("group name1", "group name2")

Set objGroupMigration = Nothing
Set objMigration = Nothing
</Script>
</Job>
```
2. Use the Security Translation Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Translation Options</td>
<td>Click <strong>Previously migrated objects.</strong></td>
</tr>
</tbody>
</table>
| Domain Selection                 | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.  
Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| Computer Selection               | Click **Select computers from domain**, and then click **Next**. On the **Computer Selection** page, click **Add** to select the computers for which you want to translate security, click **OK**, and then click **Next**.  
- or -  
Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Translate Objects                | Clear the **User Profiles** check box.  
Select all the other check boxes.                                                                                                                                                                   |
| Security Translation Options     | Click **Remove**.                                                                                                                       |
To translate security in remove mode on objects by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT Security command with the appropriate parameters. For example:

   ```
   ADMT SECURITY /N "computer_name1" "computer_name2"
   /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /TOT:Remove
   ```

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT SECURITY /N "computer_name1" "computer_name2" /o "option_file.txt"
   ```

   The following table lists the common parameters used for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Security translation options</td>
<td>/TOT:Remove</td>
<td>TranslateOption=REMOVE</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click **View Migration Log** to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

To translate security in remove mode on objects by using a script

- Prepare a script that incorporates ADMT commands and options for translating security in remove mode on objects by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.
Option Explicit

Dim objMigration
Dim objSecurityTranslation

'Create instance of ADMT migration objects.

Set objMigration = CreateObject("ADMT.Migration")
Set objSecurityTranslation = objMigration.CreateSecurityTranslation

'Specify general migration options.

objMigration.SourceDomain = "source domain"
objMigration.TargetDomain = "target domain"
objMigration.TargetOu = "Computers"

'Specify security translation specific options.

objSecurityTranslation.TranslationOption = admtTranslateRemove
objSecurityTranslation.TranslateFilesAndFolders = True
objSecurityTranslation.TranslateLocalGroups = True
objSecurityTranslation.TranslatePrinters = True
objSecurityTranslation.TranslateRegistry = True
objSecurityTranslation.TranslateShares = True
objSecurityTranslation.TranslateUserProfiles = False
objSecurityTranslation.TranslateUserRights = True

'Perform security translation on specified computer objects.

objSecurityTranslation.Translate admtData, _
Array("computer name1", "computer name2")

Set objSecurityTranslation = Nothing
Set objMigration = Nothing
Migrating Resources

The process of migrating resources between Active Directory domains in different forests involves completing the migration of the following:

- Workstation accounts and member servers
- Domain and shared local groups
- Domain controllers

When you have successfully migrated all resource objects to the target domain, you can decommission the source domain.

The following figure shows the process for migrating resource objects between Active Directory domains in different forests.

---

Migration of Workstations and Member Servers

Migrate remaining workstations that you did not migrate during the user account migration process, along with member servers, in small batches of up to 100 computers. Workstation account and member server migration is a straightforward process.
Workstations and member servers have their own SAM account database. When you migrate a workstation between domains, the SAM database is migrated along with the computer. Accounts located in the local SAM database (such as local groups) that are used to enable access to resources always move with the computer, and therefore do not need to be migrated. Because the migration requires that workstations and member servers restart, it is important to schedule the migration for a time when the server is not servicing requests.

**Note**

Restart workstations immediately after joining them to the target domain, by selecting a low number (such as 1) for the RestartDelay parameter. Resources that are not restarted following migration are in an indeterminate state.

You can migrate workstations and member servers by using the ADMT console, the ADMT command-line option, or a script.

**To migrate workstations and member servers by using the ADMT console**

1. On the computer in the target domain on which you installed ADMT, log on by using the ADMT resource migration account.
2. Use the Computer Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
Computer Selection | Click Select computers from domain, and then click Next. On the Computer Selection page, click Add to select the computers in the source domain that you want to migrate, click OK, and then click Next.
- or -
Click Read objects from an include file, and then click Next. Type the location of the include file, and then click Next.

Organizational Unit Selection | Click Browse. In the Browse for Container dialog box, locate the target domain Computers container or the appropriate OU, and then click OK.

Security Translation Options | Select the Local groups check box. Select the User rights check box.

Translate Objects | Click Add.

Computer Options | In the Minutes before computer restart after wizard completion box, accept the default value of 5 minutes, or type a different value.

Object Property Exclusion | To exclude certain object properties from the migration, select the Exclude specific object properties from migration check box, select the object properties that you want to exclude and move them to the Excluded Properties box, and then click Next.

Conflict Management | Click Do not migrate source object if a conflict is detected in the target domain.
ADMT Agent Dialog

Select Run pre-check and agent operation and then click Start.

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click View Migration Log to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#.ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

4. Open Active Directory Users and Computers, and verify that the workstations exist in the appropriate OU in the target domain.

To migrate workstations and member servers by using the ADMT command-line option

1. On the computer in the target domain on which ADMT installed, log on by using the ADMT resource migration account.

2. At the command line, type the ADMT Computer command with the appropriate parameters. For example, type:

   ```
   ADMT COMPUTER /N "computer_name1\computer_name2" /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /RDL:5
   ```

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT COMPUTER /N "computer_name1\computer_name2" /O:"option_file.txt"
   ```

   The following table lists the common parameters used for workstation migration, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
</tbody>
</table>
### ADMT Commands and Options

<table>
<thead>
<tr>
<th><strong>Target OU location</strong></th>
<th>TargetOU=&quot;target_OU&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restart Delay (minutes)</strong></td>
<td>RestartDelay=5</td>
</tr>
<tr>
<td><strong>Security Translation Option</strong></td>
<td>TranslationOption=ADD</td>
</tr>
<tr>
<td><strong>Translate User rights</strong></td>
<td>TranslateUserRights=YES</td>
</tr>
<tr>
<td><strong>Translate Local Groups</strong></td>
<td>TranslateLocalGroups=YES</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors. The migration log lists computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file for that computer to review any problems with local groups. The log file for each computer is named `MigrationTask#_ComputerName.log` and is stored in the `Windows\ADMT\Logs\Agents` folder.

4. Open Active Directory Users and Computers and locate the target OU. Verify that the workstations exist in the target OU.

▶ **To migrate workstations and member servers by using a script**

- Prepare a script that incorporates ADMT commands and options for migrating workstations and member servers by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a `.wsf` file name extension in the same folder as the `AdmtConstants.vbs` file.

```xml
<Job id="MigratingWorkstationsMemberServersBetweenForests" >
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
  Option Explicit

  Dim objMigration
  Dim objComputerMigration

  'Create instance of ADMT migration objects.

  Set objMigration = CreateObject("ADMT.Migration")
```
Migrating Domain and Shared Local Groups

Shared local groups are local groups in Windows NT 4.0 and Active Directory domains that can be used in ACLs on domain controllers. When a domain is configured to operate either in Windows 2000 native mode or at the Windows Server 2003 domain functional level, shared local groups are automatically changed to domain local groups. These groups can then be used in ACLs on member servers and workstations. If domain local groups or shared local groups are used in ACLs on either domain controllers or member servers, you need to migrate them to the target domain before the server is migrated.
It is not necessary to change any ACLs as part of the migration process. The ACLs continue to reference the domain local groups or shared local groups in the source domain. Because the domain local groups or shared local groups can be migrated to the target domain while using SID history, users maintain access to the resources. ADMT retains the membership of the local group during the migration.

You can migrate domain or shared local groups by using the ADMT console or a script.

**To migrate domain and shared local groups by using the ADMT console**

1. On the computer in the target domain on which you installed ADMT, log on by using the ADMT resource migration account.
2. Use the Group Account Migration Wizard by following the steps in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
| Group Selection | Click **Select groups from domain**, and then click **Next**. On the **Group Selection** page, click **Add** to select the groups in the source domain that you want to migrate, click **OK**, and then click **Next**.
- or -
  Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Type the name of the OU, or click **Browse**.
  In the **Browse for Container** dialog box, find the container in the target domain that you want to move the global groups into, and then click **OK**. |
| Group Options | Select the **Migrate Group SIDs to target domain** check box.
  Ensure that all other options are not selected. |
| User Account | Type the user name, password, and domain of an account that has administrative rights in the source domain. |
| Object Property Exclusion | Clear the **Exclude specific object properties from migration** check box. |
| Conflict Management | Select the **Migrate and merge conflicting objects** check box (all other options are cleared). |

3. When the wizard has finished running, click **View Log**. Review the migration log for any errors.

4. Open Active Directory Users and Computers, locate the target OU, and then verify that the shared local groups exist in the target domain OU.
To migrate domain and shared local groups by using a script

- Prepare a script that incorporates ADMT commands and options for migrating domain and shared local groups by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="MigratingDomainAndSharedLocalGroupsBetweenForests">
<Script language="VBScript" src="AdmtConstants.vbs"/>
<Script language="VBScript">
  Option Explicit
  Dim objMigration
  Dim objGroupMigration

  'Create instance of ADMT migration objects.

  Set objMigration = CreateObject("ADMT.Migration")
  Set objGroupMigration = objMigration.CreateGroupMigration

  'Specify general migration options.

  objMigration.SourceDomain = "source domain"
  objMigration.SourceOu = "source container"
  objMigration.TargetDomain = "target domain"
  objMigration.TargetOu = "target container"

  'Specify group migration specific options.

  objGroupMigration.MigrateSIDs = True

  'Migrate specified group objects.

  objGroupMigration.Migrate admData, _
  Array("local group name1", "local group name2")

  Set objGroupMigration = Nothing
  Set objMigration = Nothing
</Script>
</Job>
```
Migration of Domain Controllers

In Active Directory, you can migrate domain controllers between domains. To do this, you must:

- Remove Active Directory from the domain controller
- Migrate it as a member server to the target domain
- Reinstall Active Directory

If the server is running Windows 2000 Server, you cannot install Active Directory in the target domain if the target domain is already at the Windows Server 2003 functional level. In this case, you must upgrade the server to Windows Server 2003 before installing Active Directory.

Completing the Migration

After you migrate all accounts and resources from the source to the target domain, perform the following tasks to complete the restructuring process:

- Transfer the administration of user and group accounts from the source to the target domain.
- Ensure that at least two domain controllers continue to operate in the source domain until the resource migration process is complete.
- Back up the two domain controllers in the source domain.

After completing these steps, you can translate security on the member servers in the target domain and decommission the source domain. The following figure shows the process for completing the migration of Active Directory domains between forests.
Translating Security on Your Member Servers

Translate security on member servers to clean up the ACLs of the resources. After objects are migrated to the target domain, resources contain the ACL entries of the source domain objects. If you are using SID history to provide access to resources during the migration, the SIDs from the source domain remain in the ACLs, so that users can access resources while the migration is in progress. After the migration is complete, the SIDs from the source domain are no longer needed. Use the Security Translation Wizard in ADMT to replace the source domain SIDs with the target domain SIDs.

You do not need to perform this procedure if you are not using SID history for resource access because you should have already run security translation in remove mode after the user migration.

You can translate security on member servers by using the ADMT console, the ADMT command-line option, or a script.
To translate security on member servers by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. Use the Security Translation Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Translation Options</td>
<td>Click Previously migrated objects.</td>
</tr>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select Any domain controller. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select Any domain controller, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Computer Selection</td>
<td>Click <strong>Select computers from domain</strong>, and then click <strong>Next</strong>. On the <strong>Computer Selection</strong> page, click <strong>Add</strong> to select the computers for which you want to translate security, click <strong>OK</strong>, and then click <strong>Next</strong>. - or - Click <strong>Read objects from an include file</strong>, and then click <strong>Next</strong>. Type the location of the include file, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Translate Objects</td>
<td>Clear the <strong>User Profiles</strong> check box. Select all other options.</td>
</tr>
</tbody>
</table>
To translate security on member servers by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT Security command with the appropriate parameters. For example:

   ```
   ADMT SECURITY /N "computer_name1" "computer_name2"
   /SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /TOT:Replace
   ```

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT SECURITY /N " computer_name1" " computer_name2" /o 
   "option_file.txt"
   ```

   The following table lists the common parameters used for migrating user accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Security translation options</td>
<td>/TOT:Replace</td>
<td>TranslateOption=REPLACE</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click View Migration Log to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named MigrationTask#.ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

To translate security on member servers by using a script

- Prepare a script that incorporates ADMT commands and options for translating security on member servers by using the sample script shown in the following
Listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="TranslatingSecurityOnMemberServersBetweenForests">
  <Script language="VBScript" src="AdmtConstants.vbs" />
  <Script language="VBScript">
    Option Explicit
    Dim objMigration
    Dim objSecurityTranslation
    
    'Create instance of ADMT migration objects.'
    Set objMigration = CreateObject("ADMT.Migration")
    Set objSecurityTranslation = objMigration.CreateSecurityTranslation
    
    'Specify general migration options.'
    objMigration.SourceDomain = "source domain"
    objMigration.TargetDomain = "target domain"
    objMigration.TargetOu = "Computers"
    
    'Specify security translation specific options.'
    objSecurityTranslation.TranslationOption = admtTranslateReplace
    objSecurityTranslation.TranslateFilesAndFolders = True
    objSecurityTranslation.TranslateLocalGroups = True
    objSecurityTranslation.TranslatePrinters = True
    objSecurityTranslation.TranslateRegistry = True
    objSecurityTranslation.TranslateShares = True
    objSecurityTranslation.TranslateUserProfiles = False
    objSecurityTranslation.TranslateUserRights = True
    
    'Perform security translation on specified computer objects.'
    
    objSecurityTranslation.Translate admtData, Array("computer name1", "computer name2")
    
    Set objSecurityTranslation = Nothing
    Set objMigration = Nothing
  </Script>
</Job>
```
Decommissioning the Source Domain

After you complete the migration of the accounts and resources in your source domain, decommission the source domain. Ensure that you retain a full system state backup of a domain controller, so that you can bring the domain back online at any time.

To decommission the source domain

1. Remove all trust relationships between the source domain and the target domain.
2. Repurpose any remaining domain controllers in the source domain that you did not migrate to the target domain.
3. Disable all accounts that you created during the migration process, including those accounts to which you assigned administrative permissions.

Note

When you decommission the source domain, shared local groups and local groups that you have not translated by using the Security Translation Wizard display group members as "account unknown." This is because member names from the source domain do not resolve. Those group memberships still exist, however, and it does not affect users. Do not delete "account unknown" entries because this disables the access facilitated by SID history. Run the Security Translation Wizard to remove these entries.

Intraforest Active Directory Domain Restructure

Reducing the number of Active Directory domains in your forest in turn reduces or simplifies:

- Administration requirements for your organization.
- Replication traffic.
- User and group administration.
- Implementation of Group Policy.

If users are frequently reassigned to locations that are part of different domains, you might also migrate objects between domains on a regular basis. The process for
Restructuring Active Directory domains within a forest differs from that used between forests and requires careful planning and testing.

**Overview of Restructuring Active Directory Domains Within a Forest Using ADMT v3**

The most efficient Active Directory design includes the smallest possible number of domains. By minimizing the number of domains in your forest, you can reduce administrative costs and increase the efficiency of your organization.

You might need to restructure domains in your forest if, for example, your organization closes a regional office location, and the regional domain for that location is no longer needed. In the following cases, to simplify your Active Directory logical structure, you might also restructure domains in your forest:

- If you have upgraded your network infrastructure
- If you have increased network bandwidth and replication capacity

The process of restructuring Active Directory domains in a forest is similar to the process of migrating accounts between domains. When you migrate accounts and resources between domains, you migrate objects from the source domain to the target domain without decommissioning the source domain. When you restructure Active Directory domains, you eliminate the source domain from the forest after you complete the migration of all domain objects.

Before you begin the process for restructuring Active Directory domains in a forest, ensure that the source and target domains are operating at the Windows 2000 native or Windows Server 2003 domain functional level. Restructuring source domains that are operating at the Windows 2000 mixed domain functional level, which can include domain controllers that are running Microsoft Windows NT 4.0, is not recommended.

After you complete the process for restructuring Active Directory domains in a forest, you can decommission the source domain to help reduce overhead and simplify administration in your organization.

**Note**

For job aids that are available to assist you in restructuring Active Directory domains in a forest, see Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?Linkid=14384). This package includes worksheets and sample scripts that you can customize to use for your own migration.
Process for Restructuring Active Directory Domains Within a Forest Using ADMT v3

To maintain user access to resources during the process of restructuring domains, you must perform the migration steps in a specific order. The following figure shows the process for restructuring Active Directory domains in a forest.

Background Information for Restructuring Active Directory Domains Within a Forest Using ADMT v3

Restructuring Active Directory domains within a forest involves migrating accounts and resources from the source domains to the target domains. Unlike the process for restructuring Active Directory domains between forests, when you restructure domains in a forest, the migrated objects no longer exist in the source domain.

Note

For intraforest migration, computer accounts are treated differently than user and group accounts. To facilitate rollback, a new computer account is created in the target domain, but the source computer account is disabled instead of deleted after the migration.
Additionally, migrating user accounts, resources, and groups requires special consideration when you restructure Active Directory domains within a forest because of the containment rules that apply to Active Directory groups. For these reasons, the challenge when you restructure Active Directory domains in a forest is to ensure that users have continuous access to resources during the migration process.

**Closed Sets and Open Sets**

When you restructure Active Directory domains within a forest, you must be concerned with two types of closed sets:

- Users and groups
- Resources and local groups

**Users and Groups**

The first type of closed set includes the following:

- User accounts
- All the global groups to which the users belong
- All the other members of the global groups

Global groups are limited to members of the domain where the global group exists. Therefore, if you migrate a user account to a new domain but do not migrate the global groups to which the user belongs, the user is no longer a valid member of those global groups and cannot access resources that are based on membership in those global groups. Therefore, when you are moving accounts between domains in a forest, it is necessary to move closed sets so that users retain access to their resources.

Although built-in accounts (such as Administrators, Users, and Power Users) and well-known accounts (such as Domain Admins and Domain Users) cannot be ADMT migration objects, migrating these groups in closed sets is not a common problem. Using them in access control lists (ACLs) or membership in domain local groups is not an effective way to assign resource permissions.

When you migrate users, ADMT makes the user a member of the domain users group in the target domain. However, it does not maintain permissions for other built-in groups (such as Server Operators and Backup Operators) or well-known groups (such as Domain Admins). If you have used built-in or well-known groups to assign resource permissions, you must reassign those permissions to a new domain local group before you begin the migration. Reassigning permissions includes the following steps:

1. Create a new domain local group in the source domain.
2. Create a new global group in the source domain that contains users who need access to the resource.
3. Add the new global group to the domain local group.
4. Run security translation by using a SID mapping file that maps the well-known group to the new domain local group (created in the first step) on all resources that assign permissions using well-known groups. For information about performing a security translation by using a SID mapping file, see Translate Security by Using a SID Mapping File, later in this guide.

In small domain environments that have few global groups, you might be able to identify closed sets of users and groups. If you can identify closed sets, you can migrate users and groups at the same time. In a large domain environment, a user can belong to a number of global groups; therefore, it is difficult to identify and migrate only closed sets of users and groups. For this reason, it is best to migrate groups before you migrate user accounts.

For example, User 1 belongs to global groups Global A and Global B and is a member of Domain 1. If an administrator moves User 1 and Global A to Domain 2 in the same forest, these accounts no longer exist in Domain 1; they exist only in Domain 2 in the same forest. Global B group remains in Domain 1. This creates an open set, or a set that includes users and groups in more than one domain. Because global groups can only contain members from the domain where the global group exists, the membership of User 1 in Global B is no longer valid, and User 1 can no longer access resources based on membership in Global B. Therefore, it is best to migrate both global groups before you migrate User 1.

If you are migrating an open set of objects in an environment where the functional level for both the source domain and the target domain is Windows 2000 native or higher, ADMT transforms the global group into a universal group so that it can contain users from other domains and retain the group membership. When the set becomes a closed set, ADMT changes the group back to a global group. The benefit of this process is that ADMT ensures that all closed set problems are resolved. However, replication of the global catalog is increased while the groups are universal groups because membership is copied to the global catalog.

**Note**

If the functional level of the source domain is Windows 2000 mixed, ADMT cannot transform the global group into a universal group because universal groups cannot exist at that functional level. Even if the target domain is in native mode, however, users in mixed mode domains would not get the SIDs of universal groups in their access tokens, if the groups are from outside the domain. Therefore, ADMT creates a copy of the global group in the target
domain and adds all migrated users to the copy of that group. This group has a new security identifier (SID) and no SID history. This method does not preserve access to resources unless you run the ADMT Security Translation Wizard in Add mode to update permissions, which delays and complicates the migration process. For this reason, it is not recommended that you restructure domains that are operating at the Windows 2000 mixed domain functional level or the Windows Server 2003 interim domain functional level.

Resources and Local Groups
The second type of closed set is resources and local groups. In most cases, resources have permissions assigned to computer local groups or domain local groups. Because computer local groups are migrated when you migrate the computer, these groups are a natural closed set. However, domain local groups can be used on multiple computers to assign permissions.

In this case, you can either migrate all the computers that use the domain local group at the same time the domain local group is migrated to the target domain. Or you can manually change the domain local group to a universal group and then migrate the universal group. Changing the domain local group to a universal group is a manual process because ADMT does not automatically perform this task. Although this change can increase the size of your global catalog, over a limited time period, it is an effective way to migrate resources and domain local groups as a closed set.

SID History
SID history enables you to maintain user access to resources during the process of restructuring Active Directory domains. When you migrate an object to another domain, the object is assigned a new SID. Because you assign permissions to objects based on SIDs, when the SID changes, the user loses access to that resource until you can reassign permissions. When you use ADMT to migrate objects between domains in the same forest, the SID history is automatically retained. In this way, the SID from the source domain remains as an attribute of the object after the object is migrated to the target domain.

For example, an organization that is restructuring its Active Directory domains moves universal and global groups from a source domain to the target domain before moving user accounts. Because this is a migration within a forest and the functional level of the source domain is Windows 2000 native, these groups cease to exist in the source domain and exist only in the target domain. Because the SID history of both users and groups is migrated, the users continue to have access to resources in the source domain based on their membership in a group that exists in the target domain.
Assigning Resource Access to Groups

The most effective way to assign permissions to resources is to:

1. Assign users to global groups
2. Place global groups within domain local groups
3. Assign permissions to the domain local groups

Assigning permissions to resources in this way simplifies the migration process.

Preparing to Restructure Active Directory Domains Within a Forest

By carefully preparing before you restructure Active Directory domains, you can reduce the effect that migrating objects from source to target domains has on users. The following figure shows the steps that are involved in preparing to restructure Active Directory domains within a forest.
Evaluate the New Active Directory Forest Structure

Evaluate the domain structure of your existing Active Directory forest, and then identify the domains that you want to restructure by consolidating them with other domains. You will also need to:

- Identify the source domains from which you will migrate objects.
• Identify and evaluate the organizational unit (OU) structure of the target domain where you will place those objects.

Identify the Source Domains

The source domains are the domains that you want to migrate objects from and that you plan to decommission. When you restructure Active Directory domains, it is best to migrate the smallest possible number of objects. When you select source domains, identify the domains that have the fewest objects to migrate.

Identify and Evaluate the OU Structure of the Target Domain

Identify the OUs from the source domain that you need in the target domain, and then determine whether you need to create new OUs in the target domain.

If you are using ADMT in command-line or scripting mode, you can migrate the OU structure when you migrate users, groups, or computers. The OUs are always copied between the domains and are not deleted in the source domain. To successfully migrate an OU, you must specify a source OU and a target OU in ADMT, and the target OU must exist. All objects in the source OU and all subordinate OUs are migrated to the target OU. The specified source OU itself is not migrated.

For more information about creating an OU structure, see Designing Organizational Units for Delegation of Administration (http://go.microsoft.com/fwlink).

Assign Domain Object Roles and Locations

Create an object assignment table that lists the roles and locations for all of the objects that you are migrating. Create one table for account objects, such as users, groups, and service accounts, and one table for resource objects, such as workstations, profiles, and domain controllers. In your tables, list the source and target locations for all objects to be migrated.

Before you create your account object assignment table, determine whether the domain organizational unit (OU) structures for the source and target domains are the same. If they are not the same, you must identify the source and target OU in your object assignment tables.
For a worksheet to assist you in creating an account object assignment table, see "User and Group Object Assignment Table" (DSSREER_1.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?LinkId=14384).

The following figure shows an example of an object assignment table for users and groups.

<table>
<thead>
<tr>
<th>Source Forest Name</th>
<th>Target Forest Name</th>
<th>Source Domain Name</th>
<th>Target Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tccorp.treyresearch.net</td>
<td>Contcorp.contoso.com</td>
<td>Asia.tccorp.treyresearch.net</td>
<td>Enea.contcorp.contoso.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Source Location</th>
<th>Target Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Group</td>
<td>Asia\Groups OU</td>
<td>Enea\Groups OU</td>
</tr>
<tr>
<td>Accounting</td>
<td>Group</td>
<td>Asia\Groups OU</td>
<td>Enea\Groups OU</td>
</tr>
<tr>
<td>JBrown</td>
<td>User</td>
<td>Asia\Users OU</td>
<td>Enea\Users OU</td>
</tr>
<tr>
<td>MNguyen</td>
<td>User</td>
<td>Asia\Users OU</td>
<td>Enea\Users OU</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Service Account</td>
<td>Asia\Users OU</td>
<td>Enea\Service Accounts OU</td>
</tr>
</tbody>
</table>

To create a resource object assignment table, identify the source and target OU for each object and note the physical location and role in the target domain. For a worksheet to assist you in creating a resource object assignment table, see Resource Object Assignment Table (DSSREER_2.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?LinkId=14384).

The following figure shows an example of a resource object assignment table.
Plan for Group Migration

Unless you can identify closed sets when you are restructuring Active Directory domains within a forest, you should migrate groups and users separately. This ensures that users continue to have access to required resources.

The following table lists each type of group and where the group is physically located.

<table>
<thead>
<tr>
<th>Group Type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Group</td>
<td>Active Directory</td>
</tr>
<tr>
<td>Universal Group</td>
<td>Active Directory</td>
</tr>
</tbody>
</table>
Each type of group is migrated differently based on the group’s physical location and its rules for group membership. Universal and global groups are migrated by using ADMT; they can be transformed into universal groups for the duration of the migration, if you are not migrating closed sets. You can update computer local group membership by using the Security Translation Wizard.

Each group type has different rules for membership and serves a different purpose. This affects the order that the groups are migrated from the source to the target domains. The following table summarizes the groups and their membership rules.

<table>
<thead>
<tr>
<th>Type of Group</th>
<th>Rules and Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal groups</td>
<td>Universal groups can contain members from any domain in the forest and replicate group membership to the global catalog. For this reason, you can use them for administrative groups. When you restructure domains, migrate universal groups first.</td>
</tr>
<tr>
<td>Global groups</td>
<td>Global groups can include only members from the domain to which they belong. ADMT automatically changes the global group in the source domain to a universal group when it is migrated to the target domain, if the functional level of both domains is Windows 2000 native or higher. ADMT automatically changes universal groups back to global groups after all members of the group are migrated to the target domain.</td>
</tr>
</tbody>
</table>
Type of Group | Rules and Membership
---|---
Domain local groups | Domain local groups can contain users from any domain. They are used to assign permissions to resources. When you restructure domains, you must migrate domain local groups when you migrate the resources to which they provide access, or you must change the group type to universal group. This minimizes the disruption in user access to resources. ADMT does not automatically convert domain local groups to universal groups as it does for global groups.

Plan for Test Migrations

ADMT v3 does not include a test migration option which was available in previous versions of ADMT. Develop a test plan to assist you in systematically testing each object after it is migrated to the new environment, and identifying and correcting any problems that might occur. Testing to verify that your migration is successful helps ensure that users who are migrated from the source to the target domain are able to log on, to access resources based on group membership, and to access resources based on user credentials. Testing also helps ensure that users are able to access the resources that you migrate.

After your testing is complete, you can proceed with migrating small pilot groups and then gradually increase the size of each batch of migration objects in your production environment.

Use the following process to test the migration of your account object and resource objects:

1. Create a test user in the source domain. Include this test user with your migrations.
2. Join that user to the appropriate global groups to enable resource access.
3. Log on to the source domain as the test user, and verify that you can access resources as appropriate.
4. After you migrate the user account, translate the user profile, and migrate the workstation of the user, log on to the target domain as the test user, and verify that
the user has retained all necessary access and functionality. For example, you might test to verify that:

- The user can log on successfully.
- The user has access to all appropriate resources, such as file and print shares; access to services such as messaging; and access to line-of-business applications. It is especially important to test access to internally developed applications that access database servers.
- The user profile was successfully translated, and the user retains desktop settings, desktop appearance, shortcuts, and access to the My Documents folder. Also, verify that applications appear in and start from the Start menu.

You cannot migrate every user property when you migrate user accounts. For more information about user properties that cannot be migrated, see Migrate User Accounts, later in this guide.

After you migrate resources, log on as the test user in the target domain, and verify that you can access resources as appropriate.

If any steps in the test process fail, identify the source of the problem, and determine whether you can correct the problem before the object needs to be accessible in the target domain. If you cannot correct the problem before access to the object is required, roll back to your original configuration to ensure access to the user or resource object. For more information about creating a rollback plan, see Creating a Rollback Plan, later in this guide.

As part of your test plan, create a migration test matrix. Complete a test matrix for each step that you complete in the migration process. For example, if you migrate 10 batches of users, complete the test matrix 10 times, once for each batch that you migrate. If you migrate 10 member servers, complete the test matrix for each of the 10 servers.

For a worksheet to assist you in creating a test matrix, see Migration Test Matrix (DSSREER_3.doc) in the Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?LinkId=14384).

The following figure shows an example of a completed migration test matrix.
Create a Rollback Plan

After you begin the migration process, you cannot roll back the changes that you make to the Active Directory domains in your forest. Because accounts are moved and not copied from one domain to another when you restructure domains, the changes are not
reversible. If your plans change after you begin the migration process, the only way to return accounts to your source domain is to remigrate the accounts. Create a rollback plan in case you need to remigrate accounts after you have begun to restructure your domains. To create a rollback plan, select the method that you will use to remigrate accounts.

Note

To ensure a successful rollback of an intraforest migration, do not attempt to delete the objects in the target domain and then restore them in the source domain. You will not be able to recover the objects in the source domain because they are automatically deleted by the cross-domain move proxy if a restore is attempted.

You can use ADMT to remigrate accounts from the target domain back to the source domain. In this case, the original target domain becomes the new source domain, and the original source domain becomes the new target domain. Follow the same steps in the wizards that you used earlier to migrate the accounts. If you remigrate the accounts, the objects that have been migrated to the target domain and then remigrated to the source domain will have new SIDs. However, they will have the original SID in their SID history. Therefore, they will not be identical to the accounts before the migration, but they will have the same functionality.

If you want to reverse a service account migration, you must enumerate the services again, and then remigrate the service accounts by reversing the target and source domains.

If you use scripts to perform the original migration, using scripts to remigrate accounts is the fastest method to roll back the changes. Simply reverse the objects used for the source and target domains in the script to remigrate the objects.

Note

If the functional level of the original source domain is Windows 2000 mixed, you cannot use a rollback method to undo the changes and migrate the accounts back to the source domain. A remigration requires that the original source domain become the target domain, and the functional level of the target domain must be Windows 2000 native or Windows Server 2003. For this reason, you should not restructure domains that are operating at the Windows 2000 mixed functional level or the Windows Server 2003 interim domain functional level.

After you create your rollback plan, make sure to test it to identify and correct any problems before you begin to restructure your Active Directory domains.
Create an End-User Communication Plan

Develop a plan to inform all affected users about the upcoming account migration, to ensure that they understand their responsibilities, the impact of the migration, and who to contact for help and support.

Before you begin the user migration process, send a notice to all users who are scheduled to be migrated. Because you typically migrate users in batches of approximately one hundred users at a time, it is also helpful to send a final notice to the users in each batch two to three days before their batch is scheduled. If your organization maintains an intranet, publish the account migration schedule and the information contained in the user mail on an easily accessible Web page.

Include the following information in your end-user communication.

General Information
Alert users to the fact that their user accounts are scheduled to be migrated to a new domain. Point users to a Web page or internal resource where they can find additional information, and view a migration schedule.
Inform users of their new domain name. Be sure to let them know that their account passwords will not change. Let users know that the original domain account will be disabled immediately following the migration, and the disabled account will be deleted after a specified period of time. This is not needed if they log on with user principal names (UPNs).

Impact
Make sure that users understand that when their account is migrated, they might be unable to access some resources, such as Web sites, shared folders, or resources that individuals in their group or division do not widely use.
Provide information to users about whom to contact for assistance in regaining access to required resources.

Logon Status During Migration
Make sure that users understand that during the migration process, they will be unable to log on to the domain or access e-mail or other resources. Be sure to specify the period of time for which they will be unable to log on.
Premigration Steps
Alert users to any steps that they need to complete before the migration process begins. For example, they must decrypt files encrypted by means of Encrypting File System (EFS). Failure to decrypt encrypted files will result in loss of access to encrypted files following the migration.
Users must also ensure that their computers are connected to the network when their account is scheduled to be migrated.

Expected Changes
Describe other changes that users can expect to experience following the migration, such as changes in use of smart cards, secure e-mail, or instant messaging if applicable.

Scheduling and Support Information
Provide information about where users can go to find more information; for example, an internal Web site where you post information about the migration. Also, provide information about whom to contact if a user has a conflict with the date scheduled for the migration.

Create Migration Account Groups
To migrate accounts and resources within a forest, you can create an account migration group and a resource migration group with the appropriate credentials. You must then add the accounts that will be performing the ADMT migrations to the account migration and resource migration groups, as appropriate. Because ADMT requires only a limited set of permissions, creating separate migration groups allows you to simplify administration by creating the groups, assigning the appropriate permissions, and then adding the necessary administrators to those groups. If the migration tasks for your organization are distributed across more than one administrative group, create separate migration groups for each administrative group that performs the migration.
Assign the required permissions to modify objects such as users, global groups, and local profiles according to the table that follows. The user who is running ADMT must be an administrator on the computer where ADMT is installed.
In the target domain, use a group with delegated control of the computer OU and the user OU. You might want to use a separate group for the migration of workstations if this migration process is delegated to administrators who are in the same location as the workstations.
Use the information in the following table to determine the credentials that are required for your migration.

<table>
<thead>
<tr>
<th>Migration Object</th>
<th>Credentials Necessary in Source Domain</th>
<th>Credentials Necessary in Target Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>User/Group</td>
<td>Local administrator, domain administrator, and delegated <strong>Read all user information</strong> for the source OU.</td>
<td>Delegated <strong>Create, delete, and manage user accounts. Create, delete, and manage groups, and Modify the membership of a group</strong> for the user OU or the group OU and local administrator on the computer where ADMT is installed.</td>
</tr>
<tr>
<td>Computer</td>
<td>Domain administrator or delegated rights to delete the objects in the source OU; and member of Administrators group on each computer</td>
<td>Delegated permission on the computer OU and local administrator on the computer on which ADMT is installed.</td>
</tr>
<tr>
<td>Profile (needed for Windows NT 4.0 computers only)</td>
<td>Local administrator or domain administrator. For roaming profiles, Administrator of the computer that hosts the roaming profile shared folder.</td>
<td>Delegated <strong>Create, delete, and manage user accounts</strong> for the computer OU and local administrator on the computer where ADMT is installed.</td>
</tr>
</tbody>
</table>

ADMT v3 also includes database administration roles that you can use to assign a subset of database permissions to users who perform specific migration tasks. The database administration roles and the migration tasks that they can perform are listed in the following table.

<table>
<thead>
<tr>
<th>Role</th>
<th>Migration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account migrators</td>
<td>Account migration tasks, such as user and group migration.</td>
</tr>
<tr>
<td>Role</td>
<td>Migration task</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Resource migrators</td>
<td>Resource migration tasks, such as computer migration and security translation. Account migrators also hold the role of resource migrators.</td>
</tr>
<tr>
<td>Data readers</td>
<td>Queries against that database. Account migrators and resource migrators also hold the role of data readers.</td>
</tr>
</tbody>
</table>

Users who are assigned the role of SQL Server sysadmin hold all ADMT database administration roles. They have permissions to:

- Display database roles and users who hold those roles.
- Add groups or users to roles.
- Remove groups or users from roles.

By default, the local Administrators group is assigned the role of sysadmin and can perform all ADMT database functions.

For more information about using database administrator roles, see "Configure Database Administration Roles" in ADMT v3 Help.

**Install ADMT v3**

When you install ADMT v3, it also installs Windows SQL Server 2000 Desktop Engine (Windows) (WMSDE) by default to use as its data store. Optionally, you can configure ADMT v3 to use a SQL Server 2000 with SP4 Standard or Enterprise Edition database installation that you have previously created.

**Prerequisites for Installing ADMT**

Before you install ADMT v3, complete the following prerequisites:

- Install Windows Server 2003. Although you can migrate accounts and resources from Windows NT 4.0 and Active Directory environments using ADMT v3, you can only install ADMT v3 on a server running Windows Server 2003.
- Remove all previous versions of ADMT by using **Add or Remove Programs** from Control Panel. If you attempt to install ADMT v3 on a server that has a previous version of ADMT installed, you receive an error, and the installation does not
proceed. If necessary, you can import the database from the previous version of ADMT (protar.mdb) into ADMT v3 during the installation.

- If you do not plan to use the default local database installation, ensure that another SQL Server 2000 database installation is configured with an ADMT instance. For more information about creating an ADMT instance on a SQL Server 2000 database, see Installing ADMT Using a Preconfigured SQL Database.

Installing ADMT Using the Default Database Store

You can use the default database store or a preconfigured SQL database to install ADMT. The most common and recommended installation method is to use the default database store, which the Active Directory Migration Tool Installation Wizard configures automatically.

To install ADMT using the default database store

- From the download location (http://go.microsoft.com/fwlink/?LinkId=75627), double-click admsetup.exe, which opens the installation wizard.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome to the Active Directory Migration Tool Installation</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Configuring Components</td>
<td>The ADMT database instance (MS_ADMT) is created on the local computer. Although WMSDE is installed locally by default whether ADMT uses it or not, ADMT disables WMSDE if you specify another database instance on the next wizard page.</td>
</tr>
<tr>
<td>Database Selection</td>
<td>Specify the database instance you want to connect to. The recommended selection is <strong>Use Microsoft SQL Server Desktop Engine (Windows)</strong>, which configures ADMT v3 to use the locally installed database instance. If you are using multiple ADMT v3 consoles or have a dedicated database server where you want to centralize your ADMT database, select the <strong>Use an existing Microsoft SQL Server</strong> option. Specify the server to connect to in the form of <code>Server\Instance</code>. If you select this option, see <a href="#">Installing ADMT Using a Preconfigured SQL Database</a>. You should configure the SQL Server database instance before you select this option. Although the ADMT v3 installation proceeds if the database cannot be contacted, you cannot use ADMT to migrate accounts or resources until the database instance is created and available.</td>
</tr>
</tbody>
</table>
Active Directory Migration Tool v2
Database Import

Although you cannot upgrade an ADMT v2 installation to ADMT v3, you can import data to an ADMT v3 database from an ADMT v2 database. If you do not want to import data from an ADMT v2 database, select **No, do not import data from an ADMT v2 database (Default)**.

If you want to import data from ADMT v2 into the new ADMT v3 database, select **Yes, please import data from an ADMT v2 database**.

If you choose to import data, specify the path to the ADMT v2 database file. The ADMT v2 database file has the file name protar.mdb, and should be located in the directory formerly used for your ADMT v2 installation.

Summary
This page summarizes the options you selected. To complete the ADMT v3 installation, click **Finish**.

---

### Installing ADMT Using a Preconfigured SQL Database

If you plan to use multiple ADMT consoles or if you have a dedicated database server where you want to centralize your ADMT database, you can create another SQL Server database instance for ADMT instead of using the default local database. If you choose to install ADMT in an instance of SQL Server 2000, install SQL Server 2000 with SP4. To create the ADMT instance on the SQL Server, use the command-line syntax in the following table from any server that can target the SQL Server.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**admtdb create \s</td>
<td>server:Server\Instance**</td>
</tr>
</tbody>
</table>
Syntax | Description
--- | ---
**admtdb create /\{i\|import\} "v2 database path"** | Specifies the fully qualified path to the protar.mdb database file that was used with a previous ADMT v2 installation. Required /server parameter must be specified with this option. ADMT v2 data can be imported at the time of creation, or later into an empty database using the **admtdb import** command.

For all admtdb.exe command-line options, type **admtdb /?** at a command prompt.

After the database has been configured, navigate to the folder where you downloaded ADMT v3 and double-click admtdsetup.exe.

In the Active Directory Migration Tool Installation Wizard, on the Database Selection page, select the **Use an existing Microsoft SQL Server** option and specify the server to connect to in the form of Server/Instance.

If you decide to use the local database after configuring a remote instance of a SQL Server database, use the following procedure.

**To use the default local database after configuring a remote instance of a SQL Server database**

1. On the local computer, click Start, point to Administrative Tools, and then click Services.
2. In the right pane, navigate to MSSQL$MS_ADMT, verify that the Status column displays Started, and that the Startup Type is set to Automatic. If the MSSQL$MS_ADMT service is not Started, right-click MSSQL$MS_ADMT, and then click Properties.
3. On the General tab, in the Startup Type drop-down list, click Automatic.
4. Under Service Status, click the Start button, and then click OK.
6. Open a command prompt, and then type:
   ```
   admtd config /setdatabase:Server/Instance
   ```
   You can now use the default local database.
Plan for Service Account Transitioning

Most services run within the context of the Local System account. Consequently, they do not need any maintenance when they are migrated to a different domain. Some services, however, run in the context of a user account instead of the Local System account.

Service account transitioning refers to the process of identifying, migrating, and updating services that run in the context of user accounts. This process has three steps. In the first step, the administrator starts ADMT from the target Active Directory domain controller and runs the Service Account Migration Wizard. In the second step, the Service Account Migration Wizard sends an agent to a specified computer and identifies (but does not migrate) all services on the computer that are running in the context of a user account. The last step, which can occur later in the migration process, is to migrate the accounts when other user accounts are migrated with the User Account Migration Wizard.

The Service Account Migration Wizard checks every service on a computer to identify services that run in the context of a user account. It is possible to create a security hole during the migration of service accounts if someone who is not a service administrator enters an account with administrative permissions in the source domain but uses an invalid password on their computer to start the service. The service will not start before the account migration, because the password is not correct, but it will work after migration because ADMT resets the password of the service account and configures all services that are using that service account with the new password.

To eliminate this possible security problem, it is important to include in the Service Account Migration Wizard only those servers that are managed by trusted administrators. Do not use the Service Account Migration Wizard to detect service accounts on computers that are not managed by trusted administrators, such as workstations.

If you do not identify and transition a trusted computer that therefore does not get its service account updated, you will need to manually set the new password created by ADMT. To do this, obtain the password from the Password.txt file, and then manually enter that account and password information for the service on the computer that did not get transitioned.

When the accounts that the Service Account Migration Wizard identifies in the ADMT database as running in the context of a user account are migrated to the target domain, ADMT grants each account the right to log on as a service.

To run the Service Account Migration Wizard

1. In ADMT, start the Service Account Migration Wizard.
2. Use the wizard by following the steps provided in the following table.
<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master role is always used as the source domain controller regardless of your selection. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Update Information</td>
<td>Click <strong>Yes, update the information</strong>.</td>
</tr>
<tr>
<td>Computer Selection Option</td>
<td>Click <strong>Select computers from domain</strong>, and then click <strong>Next</strong>. On the <strong>Service Account Selection</strong> page, click <strong>Add</strong> to select the accounts in the source domain that you want to migrate, click <strong>OK</strong>, and then click <strong>Next</strong>. - or - Click <strong>Read objects from an include file</strong>, and then click <strong>Next</strong>. Type the location of the include file, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Agent Dialog</td>
<td>In <strong>Agent Actions</strong>, select <strong>Run pre-check and agent operation</strong>, and then click <strong>Start</strong>. A message will appear in the Agent Summary when the agent operations are complete. After the agent operations finish, click <strong>Close</strong>.</td>
</tr>
<tr>
<td>Service Account Information</td>
<td>Select any user accounts that do not need to be marked as service accounts in the ADMT database, and then click <strong>Skip/Include</strong> to mark the accounts as <strong>Skip</strong>.</td>
</tr>
</tbody>
</table>

The wizard connects to the selected computers, and then sends an agent to check every service on the remote computers. The Service Account Information page lists the services that are running in the context of a user account and the name of that user account. ADMT notes in its database that these user accounts need to be migrated as service accounts. If you do not want a user account to be migrated as a service account, select the account, and then click **Skip/Include** to change the status from **Include** to **Skip**.

3. You use **Update SCM** to update the Service Control Manager with the new information. Unless you have a failure in reaching a computer to update the service, the **Update SCM** button is not available. If you have a problem updating a service account after the account was identified and migrated, ensure that the computer that you are trying to reach is available, and then restart the Service Account Migration Wizard. In the wizard, click **Update SCM** to try to update the service. If you ran the Service Account Migration Wizard previously and the **Update SCM** button is not available, examine the ADMT log files to determine the cause of the problem. After you correct the problem and the agent can connect successfully, the **Update SCM** button becomes available.

**To identify service accounts by using the ADMT command-line option**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type:

   ```
   ADMT SERVICE /N "computer_name1" "computer_name2"
   /SD:"source_domain" /TD:"target_domain"
   ```

   *computer_name1* and *computer_name2* are the names of computers in the
source domain that run service accounts.

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT SERVICE /N "computer_name1" "computer_name2" /O:"option_file.txt"
```

The following table lists the common parameters used for the identification of service accounts, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.

**To identify service accounts by using a script**

- Create a script that incorporates ADMT commands and options for identifying service accounts by using the sample script shown in the following listing. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="IdentifyingServiceAccounts" >
  <Script language="VBScript" src="AdmtConstants.vbs" />
  <Script language="VBScript" >
    Option Explicit
    Dim objMigration
    Dim objServiceAccountEnumeration
    'Create instance of ADMT migration objects.
    Set objMigration = CreateObject("ADMT.Migration")
    Set objServiceAccountEnumeration = objMigration.CreateServiceAccountEnumeration
    'Specify general migration options.
    objMigration.SourceDomain = "source domain"
  </Script>
</Job>
```
Example: Preparing to Restructure Active Directory Domains

Contoso Corporation upgraded its hardware to increase its network bandwidth and the amount of replication traffic that it can support. As a result, the company is consolidating the Africa domain into the EMEA domain.

The Africa domain is the source domain, and the EMEA domain is the target domain for the migration. The organization needs to migrate a total of 1,800 users from the Africa domain to the EMEA domain. In addition to the user accounts, they must also migrate resources such as workstations, servers, and groups.

Because Contoso Corporation is a large organization with many global groups, closed sets are difficult to identify, so the company decided to migrate global groups as universal groups. They can do this because the infrastructure of the corporation can handle the increased replication of the universal groups and because both the Africa and EMEA domains are operating at the Windows 2000 native functional level. The company created identical OU structures in the Africa and EMEA domains; therefore, they do not need to create a new OU structure or migrate OUs.

Contoso Corporation created a list of computers that run service accounts, so that it can use the Service Account Migration Wizard to identify services that run in the context of user accounts. The company is most concerned about a set of accounts that access a SQL Server database. Access to this database is an important part of their business. The company decides to use ADMT as its migration tool and to use the wizards. The company installs ADMT and creates two account migration groups to use for the migration process. They assign high-level permissions to the first group, and then add the appropriate deployment team members to that group. The centralized deployment team will use this account to migrate users. They assign workstation and local resource...
permissions to the second group. The deployment team will use the second group to migrate resources at the remote locations.

Migrating Domain Objects Between Active Directory Domains

Restructuring Active Directory domains in a forest involves migrating domain objects in a specific order to ensure that users maintain access to resources. The following figure shows the process for migrating domain objects between Active Directory domains.

Migrate Groups

To protect your system against the problem of open sets when you restructure Active Directory domains within a forest, migrate groups before you migrate the user accounts that are members of those groups. If you migrate groups simultaneous with migrating users, you might not migrate nested groups, thereby creating an open set.

In addition, follow these guidelines for migrating groups:

- Migrate universal groups first, followed by global groups.
• Migrate domain local groups when you migrate the resources (domain controllers and member servers) on which they are used to assign permissions.
• You can choose to migrate computer local groups when you migrate the computer later in the restructure process.

Migrate Universal Groups

Migrate universal groups, without migrating users who are members of these groups at the same time, from the source domain to the target domain. Migrating universal groups without the users helps to protect against the problem of open sets. SID history allows group members to continue to have access to resources based on universal group membership. When you migrate universal groups to the target domain, they cease to exist in the source domain.

Important

If you are migrating a small number of universal groups, you can migrate universal groups at the same time that you migrate global groups.

You can migrate universal groups by using the ADMT console, the ADMT command-line option, or a script.

To migrate universal groups by using the ADMT console

• On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
• Use the Group Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
</table>
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master role is always used as the source domain controller regardless of your selection.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
|---|---|
| Group Selection Option | Click **Select groups from domain**, and then click **Next**. On the **Group Selection** page, click **Add** to select the groups in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
To migrate universal groups by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
2. At a command line, type the ADMT Group command with the appropriate parameters. For example:

```plaintext
ADMT GROUP /N "group_name1" "group_name2" /IF:YES /SD:"source_domain" /TD:"target_domain" /TO:"target_OU"
```

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```plaintext
ADMT GROUP /N "group_name1" "group_name2" /o: "option_file.txt"
```

The following table lists the parameters that are required for migrating universal groups, the command-line parameters, and option file equivalents. For a complete list of all available parameters, see ADMT v3 Help.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra-Forest</td>
<td>/IF:YES</td>
<td>IntraForest=YES</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers, and then locate the target domain OU. Verify that the universal groups exist in the target domain OU.

To migrate universal groups by using a script

- Use the following listing to prepare a script that incorporates ADMT commands and options for migrating groups within a forest. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmConstants.vbs file.

```xml
<Job id="MigratingGroupsWithinForest" />
<Script language="VBScript" src="AdmConstants.vbs" />
<Script language="VBScript" >
    Option Explicit
    Dim objMigration
    Dim objGroupMigration
    
    'Create instance of ADMT migration objects.
    Set objMigration = CreateObject("ADMT.Migration")
    Set objGroupMigration = objMigration.CreateGroupMigration
    
    'Specify general migration options.
    objMigration.IntraForest = True
    objMigration.SourceDomain = "source domain"
    objMigration.SourceOu = "source container"
    objMigration.TargetDomain = "target domain"
    objMigration.TargetOu = "target container"
    
    'Migrate specified group objects.
    objGroupMigration.Migrate admData, Array("groupName1", "groupName2")
```
Migrate Global Groups

Migrate global groups, without members, from the source domain to the target domain to protect against the problem of open sets. (For more information about open sets, see Background Information for Restructuring Active Directory Domains Within a Forest Using ADMT v3, earlier in this guide.) After global groups are migrated to the target domain, they cease to exist in the source domain if the source domain has a functional level of Windows 2000 native or higher.

Because global groups only contain members from their own domain, you cannot migrate them from one domain to another. ADMT changes global groups to universal groups when they are migrated. The universal group in the target domain retains the SID history of the global group in the source domain, which enables users to continue to access resources in the source domain after the global groups are migrated. ADMT changes the universal groups back to global groups after all members of the global group are migrated from the source domain to the target domain.

You do not need to include built-in and well-known global groups in your migration because these already exist in the target domain. If you select a built-in or well-known global group for migration, ADMT does not migrate it; instead, ADMT makes a note in the log and continues to migrate other global groups.

The procedure for using the Group Account Migration Wizard to migrate global groups is the same as that for migrating universal groups. For more information about the procedure for migrating global groups and universal groups, see Migrate Universal Groups, earlier in this guide.

After you complete the global group migration process, use Active Directory Users and Computers to verify that the global groups migrated successfully. Verify that the global groups no longer exist in the source domain and that the groups appear in the target domain in the OU that you specified during the migration process. The global groups are listed as universal groups in the target domain if they still have members in the source domain. To view a list of members of the universal group, right-click the group, click Properties, and then click the Members tab. The original members of the global group are listed. Note, however, that user accounts have not yet been migrated.
If you are migrating user accounts during the intraforest migration but are not
migrating the global groups in the source domain that the user accounts are members of,
ADMT updates the global groups in the source domain regardless. ADMT removes the
migrated user accounts from the membership of the global group in the source domain
because the global group can only include members from the source domain. As a result,
it is possible that users do not continue to access resources in the source domain after
the migration because they are no longer members of those groups.

You can migrate global groups by using the ADMT console, the ADMT command-line
option, or a script.

To migrate global groups by using the ADMT console

1. On the computer in the target domain on which ADMT is installed, log on by
   using the ADMT account migration account.
2. Use the Group Account Migration Wizard by following the steps provided in the
   following table.
| Domain Selection | Under **Source**, in the **Domain** drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**.

When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master role is always used as the source domain controller regardless of your selection.

Under **Target**, in the **Domain** drop-down list, type or select the NetBIOS or DNS name of the target domain. In the **Domain controller** drop-down list, type or select the name of the domain controller, or select **Any domain controller**, and then click **Next**. |
| Group Selection | Click **Select groups from domain**, and then click **Next**. On the **Group Selection** page, click **Add** to select the groups in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
Organizational Unit Selection

Type the name of the OU, or click **Browse**.

In the **Browse for Container** dialog box, find the container in the target domain that you want to move the global groups into, and then click **OK**.

Group Options

The **Migrate Group SIDs to target domain** and **Fix Group Membership** check boxes are selected and appear dimmed.

Ensure that no other options are selected.

Conflict Management

Select **Do not migrate source object if a conflict is detected in the target domain**.

3. After the wizard runs, click **View Log**, and review the migration log for any errors.

4. Open Active Directory Users and Computers, and then locate the target domain OU. Verify that the global groups exist in the target domain OU.

▶ **To migrate global groups by using the ADMT command-line option**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At a command line, type the ADMT Group command with the appropriate parameters. For example:

   ```
   ADMT GROUP /N "group_name1" "group_name2" /IF:YES
   /sd:"source_domain" /td:"target domain" /to:"target OU"
   ```

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT GROUP /N "group_name1" "group_name2" /o: "option_file.txt"
   ```

   The following table lists the parameters that are required for migrating global groups, the command-line parameters, and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra-Forest</td>
<td>/IF:YES</td>
<td>IntraForest=YES</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers, and then locate the target domain OU. Verify that the global groups exist in the target domain OU.

To migrate global groups by using a script

1. Use a script that incorporates ADMT commands and options for migrating universal groups. For more information about migrating universal groups, see Migrate Universal Groups, earlier in this guide.

2. After completing the global group migration by using a script, view the migration log. The migration.log file is stored in the folder where you installed ADMT, typically Windows\ADMT\Logs.

Note
Because universal groups are replicated to the global catalog, converting global groups to universal groups can affect replication traffic. When the forest is operating at the Windows Server 2003 functional level, this impact is reduced because only changes to the universal group membership are replicated. However, if the forest is not operating at the Windows Server 2003 functional level, the entire group membership replicates every time the universal group membership changes.

Migrate Service Accounts

Migrate the service accounts that you identified earlier in the intraforest restructure process by using the Service Account Migration Wizard. This wizard marked the accounts as service accounts in the ADMT database. For more information about using ADMT to identify service accounts that are running in the context of a user account, see Plan for Service Account Transitioning, earlier in this guide.
You can migrate service accounts by using the ADMT console, the ADMT command-line option, or a script.

To migrate service accounts by using the ADMT console

- On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
- Use the User Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master role is always used as the source domain controller regardless of your selection. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
| User Selection | Click **Select users from domain**, and then click **Next**. On the **User Selection** page, click **Add** to select the accounts in the source domain that you want to migrate, click **OK**, and then click **Next**.  
- or -  
Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |
| Organizational Unit Selection | Type the name of the OU, or click **Browse**.  
In the **Browse for Container** dialog box, find the container in the target domain that you want to move the accounts into, and then click **OK**. |
| User Options | Select the **Update user rights** check box.  
Ensure that no other settings are selected, including the **Migrate associated user groups** option. A warning box will appear to inform you that if the global groups to which the user accounts belong are not also migrated, users will lose access to resources. Select **OK** to continue with the migration. |
| Conflict Management | Select **Do not migrate source object if a conflict is detected in the target domain**. |
Service Account Information

Click **Migrate all service accounts and update SCM for items marked include**. The wizard will present you with a list of the service accounts that you are migrating (if you are migrating accounts that are not service accounts, they will be migrated but will not be listed). By default, the accounts are marked as **Include**. To change the status of the account, select the account, and then click the **Skip/Include** button.

Click **Next** to migrate the accounts.

A **Migration Progress** dialog box updates you on the status of the migration. During this time, ADMT moves the accounts to the target domain, generates a new password for the accounts, assigns the accounts the right to log on as a service, and provides this new information to the services that use the accounts. When the status is listed as **Completed** in the **Migration Progress** dialog box, you can continue with the rest of the intraforest migration.

Before the migration of the service accounts is completed, users might experience interruptions when they use the services. This is because, until the service is restarted, it still uses the account that has been migrated. For any services that continually use credentials, such as search services, manually restart the services to ensure optimal results.

▶ **To migrate service accounts by using the ADMT command-line option**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type:

```
ADMT USER /N "server_name1" "server_name2" /IF:YES
/SD:"source_domain" /TD:"target_domain" /TO:"target_OU" /MSA:YES
```

*Server_name1* and *Server_name2* are the names of servers in the source domain that run service accounts. Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT USER /N "server_name1" "server_name2" /O: "option_file.txt"
```
The following table lists the parameters that are required for migrating service accounts, the command-line syntax, and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra-Forest</td>
<td>/IF:YES</td>
<td>IntraForest=YES</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD: &quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO: &quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Migrate Service Accounts</td>
<td>/MSA:YES</td>
<td>MigrateServiceAccounts=YES</td>
</tr>
<tr>
<td>Update user rights</td>
<td>/UUR:YES</td>
<td>UpdateUserRights=YES</td>
</tr>
<tr>
<td>Ignore conflicting accounts</td>
<td>/CO:IGNORE (default)</td>
<td>ConflictOptions=IGNORE (default)</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers, and locate the target domain OU. Verify that the service accounts exist in the target domain OU.

To migrate service accounts by using a script
- Use the following listing to prepare a script that incorporates ADMT commands and options for migrating service accounts. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```xml
<Job id="MigratingServiceAccountsWithinForest">
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript">
  Option Explicit

  Dim objMigration
  Dim objUserMigration

  'Create instance of ADMT migration objects.

  Set objMigration = CreateObject("ADMT.Migration")
  Set objUserMigration = objMigration.CreateUserMigration
```
Migrate User Accounts

Domains can include a large number of user accounts. To make the migration of user accounts manageable, use a technique called \textit{phased transitioning}, by which you place your user accounts into smaller batches and migrate each of the smaller batches individually. You can group the users in any way that you prefer.

You cannot migrate every user property when you migrate user accounts. For example, Protected Storage (Pstore) contents for Windows NT 4.0 workstations, including Encrypting File System (EFS) private keys, are not migrated by ADMT when you migrate user accounts. To migrate Pstore contents, you must export and import keys during the migration process.

For clients that are running Windows 2000 Server or later, data that is protected by the Data Protection API (DPAPI) is also not migrated. DPAPI helps protect the following items:
- Web page credentials (for example, passwords)
- File share credentials
- Private keys associated with EFS, S/MIME, and other certificates
- Program data that is protected by using the CryptProtectData() function

For this reason, it is important to test user migrations. Use your test migration account to identify any properties that did not migrate and update user configurations in the target domain accordingly.

If you are using Group Policy objects to manage software installation, remember that some Windows Installer files require access to the original source for certain operations, such as repair and uninstall. The administrator must reassign permissions to the software distribution point to provide access to any account.

To retain software distribution access, perform these tasks:
1. Migrate users by using ADMT.
2. Run the Security Translation Wizard on the software distribution point.

**Migrating OUs and Subtrees of OUs**

If you want to copy OUs and subtrees of OUs to your target domain, you can use either the command-line or scripting option and substitute the appropriate parameters. You must specify a source OU and a target OU, and the target OU must exist. All objects in the source OU and all subordinate OUs are migrated to the target OU, but the specified source OU itself is not migrated.

If you are using the command-line option to migrate your accounts, groups, or computers, and you also want to migrate OUs, modify the command line to use the /D option. Instead of using the /N (/IncludeName) option, you must use the /D (/IncludeDomain) option with RECURSE and MAINTAIN as follows:

```
ADMT /D:RECURSE+MAINTAIN /O "option_file.txt"
```

If you are migrating accounts, groups, or computers by using the scripting option, and you also want to migrate OUs, modify your script to use the admtdomain option. Instead of using the admtdata or admmyfile option, you must use the admtdomain option with admtrecurse and admtdomainhierarchy as follows:

```vbnet
objUserMigration.Migrate admtdomain + admtrecurse + admtdomainhierarchy
```
Migrate Accounts

You can migrate each batch of user accounts by using the ADMT console, the ADMT command-line option, or a script.

To migrate user accounts by using the ADMT console

- On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
- Use the User Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master role is always used as the source domain controller regardless of your selection. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
Click **Select users from domain**, and then click **Next**. On the **Group Selection** page, click **Add** to select the users in the source domain that you want to migrate in the current batch, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**.

**Organizational Unit Selection**

Ensure that ADMT lists the correct target OU. If it is not correct, type the correct OU, or click **Browse**.

In the **Browse for Container** dialog box, locate the target domain and OU, and then click **OK**.

**User Options**

Select the **Translate roaming profiles** check box.

Select the **Update user rights** check box.

Clear the **Migrate associated user groups** check box. A warning box appears that states that if the global groups to which the user accounts belong are not also migrated, users will lose access to resources. Click **OK** to continue with the migration.

**Conflict Management**

Click **Do not migrate source object if a conflict is detected in the target domain**.

After you click **Finish** in the User Account Migration Wizard, the **Migration Progress** dialog box appears. After the status changes to **Completed**, view the migration log to determine whether any errors occurred in the migration process. In the **Migration Progress** dialog box, click **Close**.

The migrated user accounts can log on only to the target domain, and they are
prompted to change the password the first time they log on to the target domain.

To migrate the user accounts by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At a command line, type the ADMT User command with the appropriate parameters. For example:

   ```
   ADMT USER /N "user_name1, user_name2" /IF:YES /SD:"source_domain" /TD:"target_domain" /TO:"target OU" /TRP:YES /UUR:YES
   ```

   Alternatively, you can include parameters in an option file that is specified on the command line as follows:

   ```
   ADMT USER /N "user_name1, user_name2" /O "option_file.txt"
   ```

   The following table lists the parameters that are required for migrating user accounts, the command-line parameters, and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra-Forest</td>
<td>/IF:YES</td>
<td>IntraForest=YES</td>
</tr>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Source OU location</td>
<td>/SO:&quot;source_OU&quot;</td>
<td>SourceOU=&quot;source_OU&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Conflict Management</td>
<td>/CO:IGNORE (default)</td>
<td>ConflictOptions=IGNORE</td>
</tr>
<tr>
<td>Translate Roaming Profile</td>
<td>/TRP:YES (default)</td>
<td>TranslateRoamingProfile=YES</td>
</tr>
<tr>
<td>Update User Rights</td>
<td>/UUR:YES</td>
<td>UpdateUserRights=YES</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.

4. Open Active Directory Users and Computers, and then locate the target domain
OU. Verify that the users exist in the target domain OU.

To migrate user accounts by using a script

- Use the following listing to prepare a script that incorporates ADMT commands and options for migrating user accounts within a forest. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmConstants.vbs file.

```vbscript
Option Explicit

Dim objMigration
Dim objUserMigration

'Create instance of ADMT migration objects.
Set objMigration = CreateObject("ADMT.Migration")
Set objUserMigration = objMigration.CreateUserMigration

'Specify general migration options.
objMigration.IntraForest = True
objMigration.SourceDomain = "source domain"
objMigration.SourceOu = "source container"
objMigration.TargetDomain = "target domain"
objMigration.TargetOu = "target container"

'Specify user migration specific options.
objUserMigration.TranslateRoamingProfile = True
objUserMigration.UpdateUserRights = True
objUserMigration.FixGroupMembership = True
objUserMigration.MigrateServiceAccounts = False

'Migrate specified user objects.
objUserMigration.Migrate admtData, Array("user name1","user name2")

Set objUserMigration = Nothing
```
Translate Local User Profiles

Translate local user profiles after you migrate the user accounts. You only need to translate local user profiles for Windows NT 4.0 computers. To minimize the disruption to users, translate local user profiles immediately after you migrate a batch of users. If your source domain includes only a small number of pre-Active Directory clients, migrate them as a group, and then translate their user profiles before you migrate the next batch of users.

**Note**

Because roaming profiles are stored on a server, you do not need to translate them.

Local profiles are translated in replace mode because if you perform the profile translation in add mode, software installation by using software deployment Group Policy might not work. Any application that is packaged with Windows Installer version 2.0 (which is used on workstations with Windows 2000 Server SP3 or later, Windows XP SP1 or later, and in many common software packages) might not function after the profile is translated. When the Security Translation Wizard is translating local profiles in replace mode, it reverts to add mode if a profile is locked. This could result in a successful profile translation, but application installations might not function after the profile is translated.

No action is required to translate a local profile on Windows 2000 Server or Windows XP clients between domains in the same forest because the GUID of the user remains the same. The local profile can use the SID-to-GUID mapping that it preserves in the registry to reassign the profile of the user, and then reassociate it with the new SID.

For profile translations, if a user is using offline files on a client running Windows XP SP1, the user loses access to the files in the offline folder. Although the SID of the user changes, the owner in the ACLs of the files and folders does not change. On Windows XP SP1 clients, the user will not have access to content in offline folders unless he or she is the owner of the files and folders. Therefore, to give the user access to the offline file folder, you must run the Security Translation Wizard on the profile folder.

If you are migrating the user account to a domain within the forest, and the path for the local profile is different, the user profile is modified, and a new profile folder is created on the server with the correct ACLs. The administrator must make sure that the user has access to the profile folder.
You can translate local user profiles by using the ADMT console, the ADMT command-line option, or a script.

To translate local user profiles by using the ADMT console

- On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
- Use the Security Translation Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Translation Options</td>
<td>Click <strong>Previously migrated objects</strong>.</td>
</tr>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master role is always used as the source domain controller regardless of your selection. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
Computer Selection

Click **Select computers from domain**, and then click **Next**. On the **Computer Selection** page, click **Add** to select the computers in the source domain that have user profiles that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**.

Translate Objects

Click **User Profiles**.

Security Translation Options

Click **Replace**.

---

**To translate local user profiles by using the ADMT command-line option**

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type the ADMT /Security command with the appropriate parameters. For example, type:

   ```
   ADMT SECURITY /N "computer_name1" "computer_name2"
   /SD:"source_domain" /TD:"target_domain" /TOT:REPLACE /TUP:YES
   ```

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

``` ADMT SECURITY /N "computer_name1" "computer_name2" /o "option_file.txt" ```

The following table lists the parameters that are required for translating local user profiles, command-line parameters, and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntraForest</td>
<td>/IF:YES</td>
<td>IntraForest=YES</td>
</tr>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
</tbody>
</table>
To translate local user profiles by using a script

- Use the following listing to prepare a script that incorporates ADMT commands and options for translating local user profiles. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmConstants.vbs file.

```vbscript
Option Explicit

Dim objMigration
Dim objSecurityTranslation

'Create instance of ADMT migration objects.

Set objMigration = CreateObject("ADMT.Migration")
Set objSecurityTranslation = objMigration.CreateSecurityTranslation

'Specify general migration options.

objMigration.IntraForest = True
objMigration.SourceDomain = "source domain"
objMigration.TargetDomain = "target domain"

'Specify security translation specific options.

objSecurityTranslation.TranslationOption = admtTranslateReplace
objSecurityTranslation.TranslateUserProfiles = True

'Perform security translation on specified computer objects.
```
Migrate Workstations and Member Servers

Migrate workstations and member servers from the source domain to the target domain. When you migrate computers, the changes do not take effect until the computer is restarted. Restart the computers that you are migrating as soon as possible to complete the migration process.

Note

Restart member workstations and servers immediately after joining them to the target domain, by selecting a low number for the RestartDelay parameter. Resources that are not restarted following migration are in an indeterminate state.

Firewalls such as Windows Firewall in Windows XP SP 2 can prevent ADMT computer account migration from completing. Thoroughly test your computer migration in a lab environment to uncover any potential issues before you perform the migration in the production environment. For more information about configuring Windows Firewall, see Some programs seem to stop working after you install Windows XP Service Pack 2 (http://go.microsoft.com/fwlink/?LinkId=76705) and Service overview and network port requirements for the Windows Server system (http://go.microsoft.com/fwlink/?LinkId=58432).

Computer accounts are treated differently than user and group accounts during a migration between domains in an Active Directory forest. Where user and group accounts in the source domain are deleted during an intraforest migration, computer accounts in the source domain are instead disabled, and a new computer account is created in the target domain.
This allows you to roll back the computer migration if necessary. After the migration is complete and your testing verifies that the computer is functioning as expected, you can safely delete the computer account in the source domain.

You can migrate workstations and member servers by using the ADMT console, the ADMT command-line option, or a script.

**To migrate workstations and member servers by using the ADMT console**

1. On the computer in the target domain where ADMT installed, log on by using a user account that is a member of the ADMT resource migration group.

2. Use the Computer Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master role is always used as the source domain controller regardless of your selection. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
| **Computer Selection** | Click **Select computers from domain**, and then click **Next**. On the **Computer Selection** page, click **Add** to select the computers in the source domain that you want to migrate, click **OK**, and then click **Next**.

- or -

Click **Read objects from an include file**, and then click **Next**. Type the location of the include file, and then click **Next**. |

| **Organizational Unit Selection** | Click **Browse**.

In the **Browse for Container** dialog box, click the OU in the target domain to which the computers are migrating, and then click **OK**. |

| **Translate Objects** | Select the **Local groups** check box. 
Select the **User rights** check box. |

| **Security Translation Options** | Click **Replace**.

When you perform an intraforest migration, ADMT migrates the SID history and deletes the source object. Therefore, when you perform an intraforest migration, ADMT allows security translation only in **Replace** mode. |

| **Computer Options** | In the **Minutes before computer restart after wizard completion** box, accept the default value of 5 minutes or type a different value. |
Object Property Exclusion | To exclude certain object properties from the migration, select the **Exclude specific object properties from migration** check box, select the object properties that you want to exclude and move them to the **Excluded Properties** box, and then click **Next**.

Conflict Management | Click **Do not migrate source object if a conflict is detected in the target domain**.

ADMT Agent Dialog | Select **Run pre-check and agent operation**, and then click **Start**.

3. Review the results that are displayed on the screen for any errors. After the wizard completes, click **View log** to see the list of computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file on that computer to review any problems with local groups. The log file for each computer is named `MigrationTask#_ComputerName.log` and is stored in the `Windows\ADMT\Logs\Agents` folder.

**To migrate workstations and member servers by using the ADMT command-line option**

1. On the computer in the target domain where ADMT is installed, log on by using a user account that is a member of the ADMT resource migration group.

2. At the command line, type the ADMT Computer command with the appropriate parameters. For example, type:

   ```
   ADMT COMPUTER /N "computer_name1" "computer_name2" /IF:YES /SD:"source_domain" /TD:"target_domain" /to:"target_OU" /rdl:1
   ```

   Alternatively, you can include parameters in an option file that is specified at the command line as follows:

   ```
   ADMT COMPUTER /N "computer_name1" "computer_name2" /o:"option_file.txt"
   ```

   The following table lists the parameters that are required for workstation and member server migration, the command-line parameters, and option file
equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntraForest</td>
<td>/IF:YES</td>
<td>IntraForest=YES</td>
</tr>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Restart delay (minutes)</td>
<td>/RDL:5</td>
<td>RestartDelay=5</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO:IGNORE (default)</td>
<td>ConflictOptions=IGNORE</td>
</tr>
<tr>
<td>Security Translation Options</td>
<td>/TOT:ADD</td>
<td>TranslationOption=YES</td>
</tr>
<tr>
<td>Translate User Rights</td>
<td>/TUR:YES</td>
<td>TranslateUserRights=YES</td>
</tr>
<tr>
<td>Translate Local Groups</td>
<td>/TLG:YES</td>
<td>TranslateLocalGroups=YES</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors. The migration log lists computers, completion status, and the path to the log file for each computer. If an error is reported for a computer, you will need to refer to the log file for that computer to review any problems with local groups. The log file for each computer is named MigrationTask#_ComputerName.log and is stored in the Windows\ADMT\Logs\Agents folder.

4. Open Active Directory Users and Computers, and then locate the target domain OU. Verify that the workstations and member servers exist in the target domain OU.

To migrate workstations and member servers by using a script

- Use the following listing to prepare a script that incorporates ADMT commands and options for migrating workstations and member servers within a forest. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.
<Job id="MigratingWorkstationsMemberServersWithinForest">
  <Script language="VBScript" src="AdmtConstants.vbs" />
  <Script language="VBScript"/>
  Option Explicit

  Dim objMigration
  Dim objComputerMigration

  'Create instance of ADMT migration objects.
  Set objMigration = CreateObject("ADMT.Migration")
  Set objComputerMigration = objMigration.CreateComputerMigration

  'Specify general migration options.
  objMigration.IntraForest = True
  objMigration.SourceDomain = "source domain"
  objMigration.SourceOu = "Computers"
  objMigration.TargetDomain = "target domain"
  objMigration.TargetOu = "Computers"

  'Specify computer migration specific options.
  objComputerMigration.TranslationOption = admtTranslateAdd
  objComputerMigration.TranslateLocalGroups = True
  objComputerMigration.TranslateUserRights = True
  objComputerMigration.RestartDelay = 1

  'Migrate computer objects on specified computer objects.
  objComputerMigration.Migrate admtData, _
  Array("computer name1", "computer name2")

  Set objComputerMigration = Nothing
  Set objMigration = Nothing
</Script>
</Job>
Migrate Domain Local Groups

Migrate the domain local groups that exist in Active Directory. You can migrate domain local groups by using the ADMT console, the ADMT command-line option, or a script.

To migrate domain local groups by using the ADMT console

- On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
- Use the Group Account Migration Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master role is always used as the source domain controller regardless of your selection. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
To migrate domain local groups by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At a command line, type the ADMT Group command with the appropriate parameters. For example:

   ```
   ADMT GROUP /N "group_name1" "group_name2" /IF:YES /SD:"source_domain" /TD:"target_domain" /TO:"target_OU"
   ```

   Alternatively, you can include parameters in an option file that is specified at the
command line as follows:

```
ADMT GROUP /N "group_name1" "group_name2" /O: "option_file.txt"
```

The following table lists the parameters that are required for migrating domain local groups, the command-line parameters, and option file equivalents. For a complete list of all available parameters, see ADMT v3 Help.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra-Forest</td>
<td>/IF:YES</td>
<td>IntraForest=YES</td>
</tr>
<tr>
<td>Target domain</td>
<td>/TD:&quot;target_domain&quot;</td>
<td>TargetDomain=&quot;target_domain&quot;</td>
</tr>
<tr>
<td>Target OU location</td>
<td>/TO:&quot;target_OU&quot;</td>
<td>TargetOU=&quot;target_OU&quot;</td>
</tr>
<tr>
<td>Conflict management</td>
<td>/CO:IGNORE (default)</td>
<td>ConflictOptions=IGNORE</td>
</tr>
</tbody>
</table>

3. Review the results that are displayed on the screen for any errors.
4. Open Active Directory Users and Computers, and then locate the target domain OU. Verify that the domain local groups exist in the target domain OU.

To migrate domain local groups by using a script

- Use a script that incorporates ADMT commands and options for migrating domain local groups. You can use the same script that you used to migrate universal groups. For more information about migrating universal groups, see Migrate Universal Groups, earlier in this guide.

Example: Restructuring Active Directory Domains

Contoso Corporation wants to migrate the Africa domain objects to the EMEA domain. To minimize the impact on users and reduce the time that network traffic is affected, Contoso decided to complete the migration of domain objects in as little time as possible. During the migration, all global groups that are migrated become universal groups until each user who belongs to the group is migrated to the target domain. Because the forest
includes domains running at the Windows Server 2003 functional level, only incremental membership changes to the universal groups are replicated to the global catalog.

Contoso administrators set up an extensive test lab to test the migration process before proceeding. They determined by testing the procedures that they could complete the migration process in two weeks. Global and universal groups will be migrated on Monday and Tuesday of the first week. Service accounts will be migrated and services updated on Wednesday. Thursday, Friday, and Saturday are reserved for migrating user accounts. Servers will be migrated on Sunday of the first week. The second week is reserved for migrating servers and workstations. Domain local groups will be migrated at the end of the second week.

**Completing Post-Migration Tasks**

After you complete all the migration tasks that are required to restructure your Active Directory domains in a forest, you must verify that the migration occurred as planned and complete a few post-migration tasks. The following figure shows the process for completing post-migration tasks.
Examine Migration Logs for Errors

ADMT keeps a detailed log of every action that you perform when you migrate resources between Active Directory domains. Errors that occur during the migration process are noted in the migration log, although they might not produce a warning message in ADMT. Examining the migration log after a migration is a good way to verify that all tasks were completed successfully. Because it is important to complete the steps of the migration in a specific order, it is best to check the migration log after each step, so that you can discover any failures in time to fix them.

For more information about how to generate the migration log files, see ADMT v3 Help. The log files are created in the Windows\ADMT\Logs folder on the computer where ADMT is installed.

Verify Group Types

ADMT changes global groups to universal groups when you migrate them from the source domain to the target domain. The change occurs automatically because global groups can only contain members of their own domain. Therefore, they cannot continue to be global groups when they are migrated to another domain until the group members are migrated. ADMT changes the universal groups back to global groups when the last member of the group is migrated to the target domain. Because universal groups replicate their membership to the global catalog, it is important to verify that the universal groups correctly changed back to global groups.

Use Active Directory Users and Computers to verify that universal groups migrated successfully. If you manually changed domain local groups into universal groups, make sure that you switch them back to domain local groups when all resources have been migrated.

Translate Security on Member Servers

Translate security on member servers to clean up the ACLs of the resources. After objects are migrated to the target domain, resources contain the ACL entries of the source domain objects. Although SID history provides access to resources during the migration, ACLs should be cleaned up after the migration to contain the new primary SID of the migrated groups. Use the Security Translation Wizard in ADMT to replace the source domain SIDs with the target domain SIDs.
To translate security on member servers by using the ADMT console

- On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.
- Use the Security Translation Wizard by following the steps provided in the following table.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Translation Options</td>
<td>Click <strong>Previously migrated objects.</strong> If you plan to use a SID mapping file, click <strong>Other objects specified in a file</strong>, and then provide the location of the SID mapping file that you have created.</td>
</tr>
<tr>
<td>Domain Selection</td>
<td>Under <strong>Source</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or Domain Name System (DNS) name of the source domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>. When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master role is always used as the source domain controller regardless of your selection. Under <strong>Target</strong>, in the <strong>Domain</strong> drop-down list, type or select the NetBIOS or DNS name of the target domain. In the <strong>Domain controller</strong> drop-down list, type or select the name of the domain controller, or select <strong>Any domain controller</strong>, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
To translate security on member servers by using the ADMT command-line option

1. On the computer in the target domain on which ADMT is installed, log on by using the ADMT account migration account.

2. At the command line, type:

```
ADMT Security /N "computer_name1" "computer_name2"
/SD:"source_domain" /TD:"target_domain"
```

`Computer_name1` and `computer_name2` are the names of computers for which you want to translate security.

Alternatively, you can include parameters in an option file that is specified at the command line as follows:

```
ADMT Security /N "computer_name1" "computer_name2"
/O: "option_file.txt"
```

The following table lists the common parameters used to translate security on member servers, along with the command-line parameter and option file equivalents.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command-Line Syntax</th>
<th>Option File Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source domain</td>
<td>/SD:&quot;source_domain&quot;</td>
<td>SourceDomain=&quot;source_domain&quot;</td>
</tr>
</tbody>
</table>
3. Review the results that are displayed on the screen for any errors.

**To translate security on member servers by using a script**

- Use the following listing to prepare a script that incorporates ADMT commands and options to translate security on member servers. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.vbs file.

```vbscript
<Job id="TranslatingSecurityOnMemberServersWithinForest" />
<Script language="VBScript" src="AdmtConstants.vbs" />
<Script language="VBScript" >
  Option Explicit
  Dim objMigration
  Dim objSecurityTranslation
  
  'Create instance of ADMT migration objects.
  
  Set objMigration = CreateObject("ADMT.Migration")
  Set objSecurityTranslation = objMigration.CreateSecurityTranslation
  
  'Specify general migration options.
  
  objMigration.IntraForest = True
  objMigration.SourceDomain = "source domain"
  objMigration.TargetDomain = "target domain"
  objMigration.TargetOu = "Computers"
  
  'Specify security translation specific options.
  
  objSecurityTranslation.TranslationOption = admtTranslateReplace
  objSecurityTranslation.TranslateFilesAndFolders = True
  objSecurityTranslation.TranslateLocalGroups = True
  objSecurityTranslation.TranslatePrinters = True
  objSecurityTranslation.TranslateRegistry = True
  objSecurityTranslation.TranslateShares = True
  objSecurityTranslation.TranslateUserProfiles = False
  objSecurityTranslation.TranslateUserRights = True
```
'Perform security translation on specified computer objects.
'

objSecurityTranslation.Translate admtdData, Array("computer name1" ,"computer name2" )

Set objSecurityTranslation = Nothing
Set objMigration = Nothing
</Script>
</Job>

Translate Security by Using a SID Mapping File

If you need to translate security so that permissions that are granted to the source account or group are now granted to the target account or group, use a SID mapping file to associate the two accounts. The SID mapping file is a comma-separated values (CSV) formatted file that lists pairs of accounts, in either NT account name (domain\name) format or SID format. The account on the left is the source account and the account on the right is the target account. ADMT security translation translates security from the source account to the target account.

You can reference the SID mapping file in the Security Translation Wizard or from the command line. The option is /SMF so that the full command line looks similar to:

```
ADMT SECURITY /N "computer_name" /SMF:"sid_mapping_file_path"
```

Decommission the Source Domain

After you have migrated all the objects from the source domain to the target domain, including all the computers and member servers, only the domain controllers remain in the source domain. To decommission the source domain, run the Active Directory Installation Wizard to remove Active Directory from the domain controllers in the source domain.

Migrate the domain controllers from the source domain to the target domain as member servers. If necessary, depending on the new role that is planned for the servers in the target domain, use the Active Directory Installation Wizard to install Active Directory on the member servers to return them to domain controller status in the target domain. Run
security translation on domain controllers, if resources reside on the computer that will be used as the new domain controller.

Example: Completing Post-Migration Tasks

The post-migration team of Contoso Corporation starts the post-migration tasks during the first week of the migration. The team examines the migration log after the first group of migrations is completed on the first day. They analyze the migration log and define the action that is required to migrate any accounts for which they find errors. This way, the migration team can continue the migration without interruption.

During the second week of the migration process, the deployment team verifies that global groups have returned from universal group to global group status after the migration of users has completed. After the member servers are migrated, the deployment team runs the Security Translation Wizard to remove the source domain SIDs from the ACLs of the member servers. Finally, the deployment team decommissions the Africa domain at the end of the second week by removing Active Directory from the domain controllers in the Africa domain. They then migrate the domain controllers to the EMEA domain as member servers.

Additional Resources

These resources contain additional information, tools, and job aids related to this guide.

Related Information

- Designing and Deploying Directory and Security Services ([http://go.microsoft.com/fwlink/?Linkid=76005](http://go.microsoft.com/fwlink/?Linkid=76005))

  This content includes prescriptive guidance for deploying Active Directory and establishing security practices. These practices include creating an authorization strategy (based on security groups) to effectively manage users’ access to resources.

Related Tools

- ADMT v3

  You can use ADMT v3 to migrate accounts and restructure your Active Directory domains. ADMT v3 includes wizards that you can use to migrate objects such as
groups, users, computers, and service accounts. These wizards assist you in performing the appropriate migration for each object type.

- Article Q295758 in the Microsoft Knowledge Base: How to Use Visual Basic Script to Clear SidHistory (http://go.microsoft.com/fwlink/?LinkId=77553)

### Related Job Aids

- The Job_Aids_Designing_and_Deploying_Directory_and_Security_Services download of the Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?LinkId=14384)

  This package includes worksheets and sample scripts that you can customize to use for your own migration.