ADMT v3.1 Guide: Migrating and Restructuring Active Directory Domains

Microsoft Corporation

Published: July 2008

Authors: Moon Majumdar, Brad Mahugh

Editors: Jim Becker, Fran Tooke

Abstract

This guide explains how to use the Active Directory® Migration Tool version 3.1 (ADMT v3.1) to migrate users, groups, and computers between Active Directory domains in different forests (interforest migration) or between Active Directory domains in the same forest (intraforest migration). It also shows how to use ADMT v3.1 to perform security translation between different Active Directory forests.

Microsoft

Contents

ADMT v3.1 Guide: Migrating and Restructuring Active Directory Domains

As part of deploying the Active Directory® directory service or Active Directory Domain Services (AD DS), you might choose to restructure your environment for the following reasons:

- To optimize the arrangement of elements within the logical Active Directory structure
- To assist in completing a business merger, acquisition, or divestiture

Restructuring involves the migration of resources between Active Directory domains in either the same forest or in different forests. After you deploy Active Directory or AD DS, 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 3.1 (ADMT v3.1) to perform object migrations and security translation as necessary so that users can maintain access to network resources during the migration process. To download ADMT v3.1, see Active Directory Migration Tool v3.1 (http://go.microsoft.com/fwlink/?LinkId=121732).

In this guide

The following sections explain the main migration scenarios for using ADMT v3.1. After you determine the appropriate scenario for your environment, follow the steps later in this guide for that scenario.

Interforest Active Directory domain restructure

You might perform an interforest restructure for business changes, such as mergers or acquisitions or divestitures, in which your organizations have to combine or divide resources. As part of the restructuring process, when you migrate objects between forests both the source and target domain environments exist simultaneously. This makes it possible for you to roll back to the source environment during the migration, if necessary.

Splitting or cloning forests—for example, to accommodate divestiture of an organization—is not supported. For more information, see the section "Restructuring Limitations" in Determining the Number of Forests Required (http://go.microsoft.com/fwlink/?LinkId=121736).

Important

All target domains must be operating at either the Windows 2000 native functional level, the Windows Server 2003 functional level, or the Windows Server 2008 functional level.

Intraforest Active Directory domain restructure

When you restructure Windows Server 2008 domains in a Windows Server 2008 forest, you can consolidate your domain structure and reduce administrative complexity and overhead. Unlike the process for restructuring Windows Server 2008 domains *between* forests, when you restructure domains *in* a forest, the migrated accounts no longer exist in the source domain. Therefore, rollback of the migration can only occur when you carry out the migration process again in reverse order from the previous target domain to the previous source domain.

Important

All target domains must be operating at either the Windows 2000 native functional level, the Windows Server 2003 functional level, or the Windows Server 2008 functional level.

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

Migration consideration	Interforest restructure	Intraforest restructure
Object preservation	Objects are cloned rather than migrated. The original object remains in the source location to maintain access to resources for users.	Objects are migrated and no longer exist in the source location.
Security identifier (SID) history maintenance	Maintaining SID history is optional.	SID history is required.
Password retention	Password retention is optional.	Passwords are always retained.
Local profile migration	You must use tools such as ADMT to migrate local profiles.	For workstations that run the Microsoft® Windows®°2000 Server operating system, local profiles are migrated automatically because the user's globally unique identifier (GUID) is preserved.
Closed sets	You do not have to migrate accounts in closed sets. For more information, see Background	You must migrate accounts in closed sets.

Migration consideration	Interforest restructure	Intraforest restructure
	Information for Restructuring Active Directory Domains Within a Forest (http://go.microsoft.com/fwlink/?LinkId=122123).	

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 it 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 you restructure 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 SIDs are identical in every domain. Therefore, built-in accounts cannot be migration objects.

Active Directory Migration Tool

You can use ADMT to migrate objects in Active Directory forests. This tool 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 you run 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 in the following example 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. You can comment out items 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
;UpdatePreviouslyMigratedObjects=No
;FixGroupMembership=Yes
```

```
;UpdateGroupRights=No

;MigrateMembers=No

;DisableOption=EnableTarget

;SourceExpiration=None

;TranslateRoamingProfile=No

;MigrateServiceAccounts=No


[Security]

;TranslationOption=Add

;TranslateFilesAndFolders=No

;TranslateLocalGroups=No

;TranslatePrinters=No

;TranslateRegistry=No

;TranslateShares=No

;TranslateUserProfiles=No

;TranslateUserRights=No

;SidMappingFile="SidMappingFile.txt"
```

When you run ADMT at the command line, you do not have 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 options for which 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"
```

Where <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 if you want 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:

```
ADMT COMPUTER /F "<includefile_name>" /IF:YES /SD:"<source_domain>" /TD:"<target_domain>"
/TO:"<target_OU>"
```

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 dollar sign ($) to the computer name. For example, to specify a computer with the name Workstation01, use Workstation01$.
- 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. You can specify the canonical name 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 field:

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 a relative distinguished name.

SourceName

name

CN=*name*

TargetName field

You can use the *TargetName* field 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 that are described later in this section.

Note

The target UPN is generated only for user objects, and only a UPN prefix is generated. A UPN suffix is appended using an algorithm that depends on whether a UPN suffix is defined for the target OU or the 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*

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 that are provided in this guide refer to the symbolic constants that are defined in a file named AdmtConstants.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.

```
Option Explicit


'--------------------------------------------------------------------------
' ADMT Scripting Constants
'--------------------------------------------------------------------------


' PasswordOption constants


Const admtComplexPassword                  = &H0001
Const admtCopyPassword                     = &H0002


' Note that the following constant cannot be specified alone.
' It must be specified along with admtComplexPassword or admtCopyPassword.
Const admtDoNotUpdatePasswordsForExisting   = &H0010


' ConflictOptions constants
```

```
Const admtIgnoreConflicting           = &H0000
Const admtMergeConflicting            = &H0001
Const admtRemoveExistingUserRights    = &H0010
Const admtRemoveExistingMembers       = &H0020
Const admtMoveMergedAccounts          = &H0040

' DisableOption constants

Const admtLeaveSource        = &H0000
Const admtDisableSource      = &H0001
Const admtTargetSameAsSource = &H0000
Const admtDisableTarget      = &H0010
Const admtEnableTarget       = &H0020

' SourceExpiration constant

Const admtNoExpiration = -1

' Translation Option

Const admtTranslateReplace = 0
Const admtTranslateAdd     = 1
Const admtTranslateRemove  = 2

' Report Type

Const admtReportMigratedAccounts  = 0
Const admtReportMigratedComputers = 1
Const admtReportExpiredComputers  = 2
Const admtReportAccountReferences = 3
Const admtReportNameConflicts     = 4

' Option constants
```

```
Const admtNone     = 0
Const admtData     = 1
Const admtFile     = 2
Const admtDomain   = 3
Const admtRecurse           = &H0100
Const admtFlattenHierarchy  = &H0000
Const admtMaintainHierarchy = &H0200
```

Best Practices for Active Directory Migration

To ensure that your migration process is as seamless as possible, follow these best practice recommendations:

- Best Practices for Using the Active Directory Migration Tool
- Best Practices for Performing User and Group Account Migrations
- Best Practices for Performing Computer Migrations
- Best Practices for Rolling Back a Migration

Best Practices for Using the Active Directory Migration Tool

- Perform regular backups of domain controllers in both the source and target domains throughout the course of the migrations. If you are migrating computers that contain file shares to perform security translation, we recommend that you also back up those computers throughout migrations.
- Before you begin a migration, perform a test migration by creating a test user, adding the test user to the appropriate global groups, and then verifying resource access before and after migration.
- Test your migration scenarios in a test environment before migrating objects in the production environment.
- Have a recovery plan, and ensure that your recovery plan works during the test phase of your migration.
- Decrypt files that have been encrypted by means of Encrypting File System (EFS). Failure to decrypt encrypted files will result in loss of access to encrypted files after migration. Be sure to communicate to end users that they must decrypt any encrypted files or they will lose access to those files.

- Ensure that the system time is synchronized in each domain from which objects are migrated. Kerberos authentication fails if time is skewed.

Best Practices for Performing User and Group Account Migrations

- Perform regular backups of domain controllers in both the source and target domains throughout the course of the migrations. If you are migrating computers that contain file shares to perform security translation, we recommend that you also back up those computers throughout migrations.
- We recommend that you migrate users in batches. A batch size of 100 users helps to keep the migration process manageable.
- Always administer changes to user accounts and group accounts in the source domain during the migration process.
- Use the **Migrate and merge conflicting objects** option on the **Conflict Management** page of the User Account Migration Wizard and the Group Account Migration Wizard to remigrate users and groups as often as necessary throughout the migration. Administering changes in the source domain and then using the **Migrate and merge conflicting objects** option during migration ensures that all changes that are made to an object in the source domain are reflected after it has been migrated to the target domain.
- To maintain access to resources, ensure that group membership adheres to the following guidelines:
  - Use global groups to group users.
  - Use local groups to protect resources.
  - Place global groups into local groups to grant members of the global groups access to a resource.
- Adhere to the guidelines in the following table when you translate user profiles.

Profile type	Translation guidelines
Roaming profiles	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.
Local profiles	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 you migrate those users.
Unmanaged profiles	Users lose their existing profiles when their user accounts are migrated.

Important

It is important to verify that local profile translation has succeeded before users attempt to log on to the target domain. If users log on to the target domain by using their new target accounts and their profiles have not translated successfully, those users must be migrated again from the source domain to the target domain. For more information about the steps to follow if local profile translation fails, see Troubleshooting Security Translation Issues.

Best Practices for Performing Computer Migrations

- Perform regular backups of domain controllers in both the source and target domains throughout the course of the migrations. If you are migrating computers that contain file shares to perform security translation, we recommend that you also back up those computers throughout the migration.
- Verify that workstations and member servers have restarted immediately after you join them to the target domain. The Active Directory Migration Tool (ADMT) automates the restart of workstations and member servers, but you use the **Minutes before computers restart after wizard completion** option in the Computer Migration Wizard to select the amount of time that passes before the computer is restarted. Computers that do not restart after migration are in an indeterminate state.
- Communicate to end users that their computers must be connected to the network at the time that their computer is scheduled to be migrated.

Best Practices for Rolling Back a Migration

- Roll back user and group accounts that have been migrated between forests by enabling the accounts in the source domain (if they were disabled during the migration), verifying that the accounts have access to resources in the source domain, and then verifying that logon scripts and user profiles work as configured in the source domain.
- Roll back resources that have been migrated between forests by changing the domain membership of servers and workstations and then restarting them. Log on to the resources in the source domain to ensure that the resources are accessible.
- Roll back accounts and resources that have been migrated within a forest by migrating the objects back from the target domain to the source domain. Accounts and resources that are migrated within a forest are moved and not copied. Therefore, they do not continue to exist in the source domain.

  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.

  Note

  When you perform an intraforest migration, if the functional level of the source domain is Windows 2000 mixed, you will not be able to migrate the objects back from the target domain to the source domain to undo migration changes. A remigration requires that the source domain become the target domain, and the functional level of the target domain must be Windows 2000 native or Windows Server 2003.

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 have to restructure Active Directory domains between forests to:

- Migrate a pilot domain into your production environment.
- Merge users and resources with another organization because of a corporate merger and the need to consolidate the two information technology (IT) infrastructures.
- Relocate users and resources on a regular basis because of a planned multiforest deployment.
- Remove objects from your forest because of a divestiture to another organization or to merge later into a new or existing forest for that organization.

In this section

Checklist: Performing an Interforest Migration

Migrating Active Directory domains between forests (interforest migration) involves relocating objects from source domains in one forest to target domains in another forest. You might have to restructure Active Directory domains between forests for the following reasons:

- To migrate a pilot domain into your production environment
- To merge your Active Directory forest with the forest of another organization and consolidate the two information technology (IT) infrastructures

Task	Reference
Review Active Directory Migration Tool version 3 (ADMT v3.1) preinstallation instructions.	Install ADMT v3.1
To migrate computers running Windows 2000, Windows XP, and Windows Server 2003 to a target domain with domain controllers running Windows Server 2008, first set the following registry key on the target domain controllers: Registry path: **HKLM\System\CurrentControlSet\Services\Netlogon\Parameters** Registry value: **AllowNT4Crypto** Type: **REG_DWORD** Data: **1** **Note** If you are running Group Policy with target Windows Server 2008 domain controllers, make this change using Group Policy administration.	For more information about making this change using Group Policy, see Known Issues for Installing and Removing AD DS (http://go.microsoft.com/fwlink/?LinkId=119321).

Task	Reference
This registry setting corresponds to the **Allow cryptography algorithms compatible with Windows NT 4.0** setting in Group Policy.	
For any migration tasks that use agent deployment and where Windows Firewall is in use, enable the File and Printer Sharing exception. This can include migration for the following situations: • Migrating workstation computers and member servers that are running under Windows Vista® or Windows Server 2008 • Migrating security settings or performing security translation	For more information about making this change in Windows Firewall, see Enable or Disable the File and Printer Sharing Exception (http://go.microsoft.com/fwlink/?LinkID=119315).
Prepare to restructure Active Directory domains within a forest. This task has the following subtasks: • Determine your account migration process. • Assign object roles and locations. • Develop a test plan for your migration. • Create a rollback plan. • Manage users, groups, and user profiles. • Create a user communication plan.	Install ADMT v3.1 Planning to Restructure Active Directory Domains Between Forests
Prepare the source and target domains. This task has the following subtasks: • Install 128-bit encryption software. • Establish trusts that are required for migration. • Establish migration accounts for your migration. • Configure the source and target domains for security identifier (SID) history migration. • Configure the target domain organizational unit (OU) structure. • Install ADMT in the target domain. • Specify service accounts for your migration.	Install ADMT v3.1 Planning to Restructure Active Directory Domains Between Forests
Specify and transition service accounts using either the Service Account Migration Wizard or ADMT command-line tools. You can use the **admt service** command-line tool to specify service accounts in the source domain. You can use the **admt user** command-line tool to	Transitioning Service Accounts in Your Migration

Task	Reference
transition service accounts that you specify.	
Migrate global groups using either the Group Account Migration Wizard or the **admt group** command-line tool.	Migrating Global Groups
Migrate user accounts and workstation accounts with their SID histories in batches. You can use either the User Account Migration Wizard or the **admt user** command-line tool to migrate user accounts.	Migrating Accounts While Using SID History
Migrate resources, such as member servers and domain controllers, and domain local groups. You can use either the Computer Account Migration Wizard or the **admt computer** command-line tool to migrate computer accounts. You can use the Group Account Migration Wizard or the **admt group** command-line tool to migrate groups.	Migrating All User Accounts Migrating All User Accounts
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. You can use either the Security Translation Wizard or the **admt security** command-line tool.	Translating Security in Add Mode
Repeat a migration of user accounts, workstation computers, and member servers, including translating local user profiles to user and computer objects that you migrated earlier.	Migrating Workstations and Member Servers
Migrate domain local groups using either the Group Account Migration Wizard or the **admt group** command-line tool.	Migrating Domain and Shared Local Groups
Migrate domain controllers.	Migrating Domain Controllers
Complete postmigration tasks. This task has the following subtasks: • Translate security on member servers. • Decommission the source domains.	Translating Security on Your Member Servers Decommissioning the Source Domain

Overview of Restructuring Active Directory Domains Between Forests

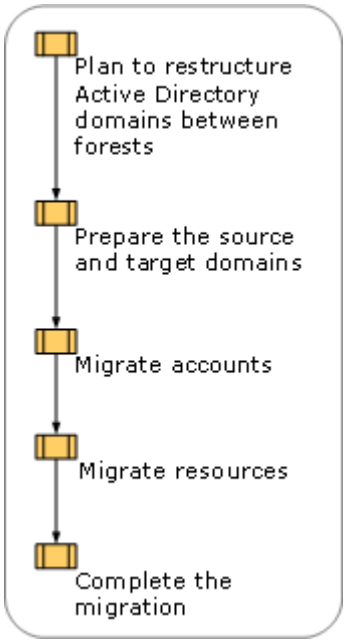
When you restructure domains between forests, you can reduce the number of domains in your organization, which helps reduce the administrative complexity and associated overhead costs of your Active Directory environment. Restructuring domains involves copying accounts and resources from a Windows 2000, Windows Server 2003, or Windows Server 2008 Active Directory source domain to a target domain in a different Active Directory forest. The target domain must be at the Windows 2000 native, Windows Server 2003, or Windows Server 2008 domain functional level.

If your organization has recently merged with another organization or information technology (IT) infrastructure, you can restructure domains to consolidate accounts and resources between the two infrastructures.

In this section

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 not considered to be 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 migration fails for any reason, for example, if a particular object does not migrate or access is not maintained or preserved in the target domain after you perform the migration. You can use the Active Directory Migration Tool (ADMT) 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, you can move users, groups, and resources 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, domain and forest 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 have 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, 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, ADMT cannot determine which remote access to assign to the user.

If you are using Group Policy to manage folder redirection, 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 that contains 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, 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, users cannot access the redirected folder because folder redirection will check ownership of the redirected folder and 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, you must 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 Security Accounts Manager (SAM) database, and they are moved when you move the server. You do not have to reconfigure access control lists (ACLs) so that users can access resources after the migration.

In Active Directory, domain controllers can be migrated between domains. To migrate domain controllers between domains, you must remove Active Directory or Active Directory Domain Services (AD DS) from the domain controller, migrate it as a member server to the target domain, and then reinstall Active Directory or AD DS.

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 Active Directory features that are available in that domain or forest.

All target domains must be operating at either the Windows 2000 native, Windows Server 2003, or Windows Server 2008 functional level.

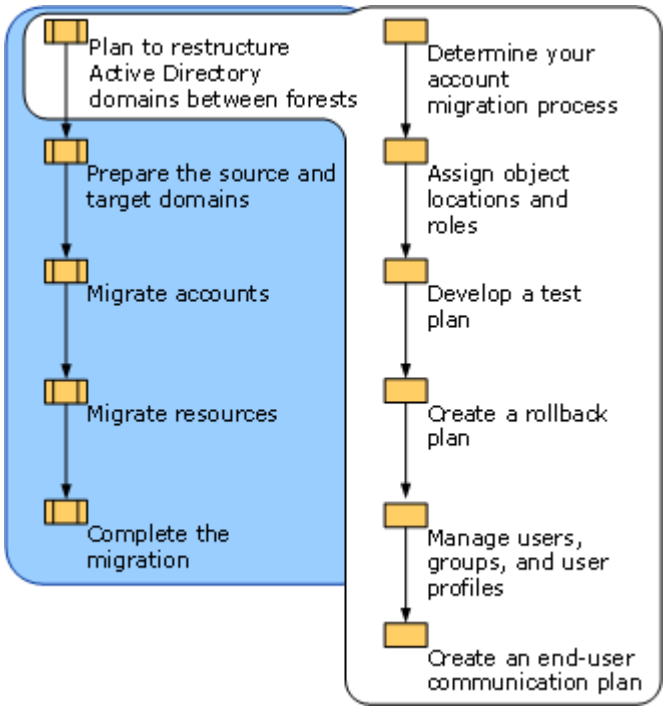
Planning to Restructure Active Directory Domains Between Forests

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 the following:

- Determining your account migration process
- Assigning object locations and roles
- Developing 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 obtain the necessary design information from the Active Directory design team.

The following illustration shows the steps involved in planning to restructure Active Directory domains between forests.



Determining Your Account Migration Process

With the Active Directory Migration Tool (ADMT), you can use security identifier (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 have to remove SID filtering on the external trusts if the domain controller that is used to create the trust is running Windows Server 2008, 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.

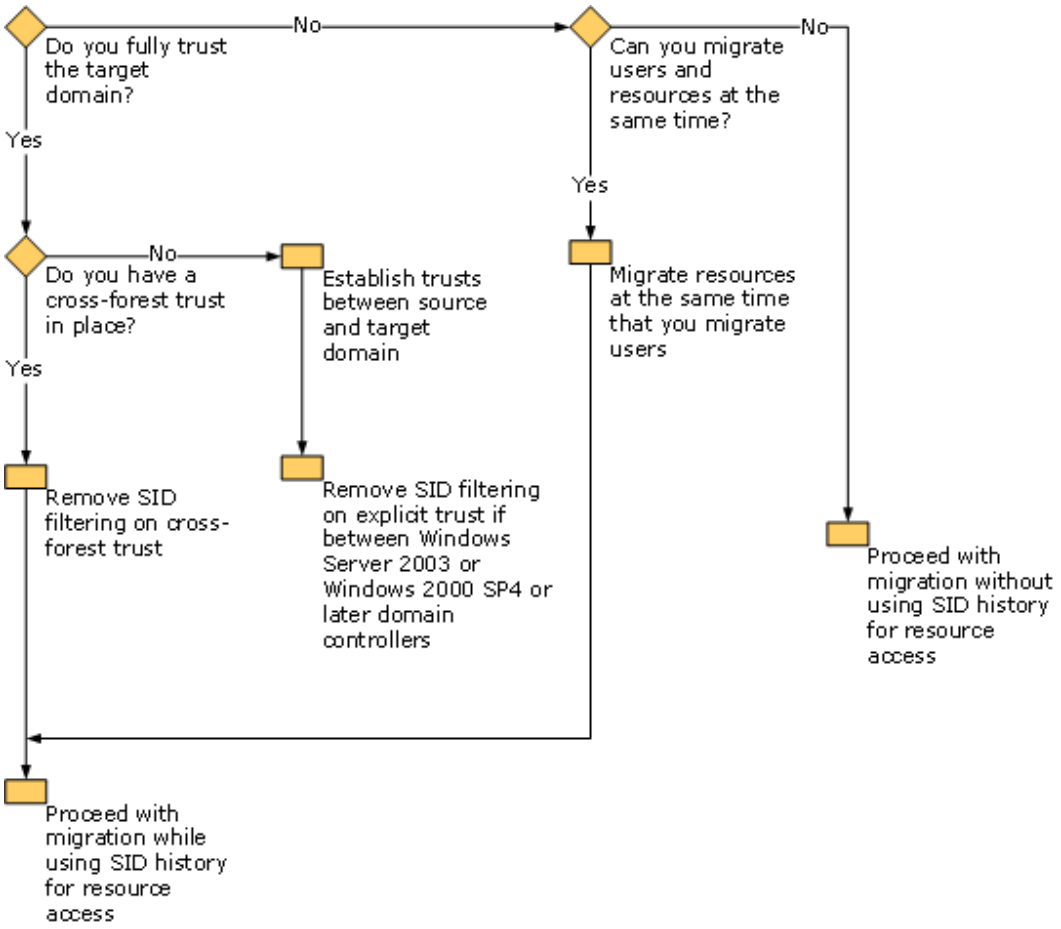
To determine which account migration process is best for your organization, you must first determine if you can disable SID filtering and migrate accounts while using SID history for resource access. You can safely do this if the administrators of the source domain fully trust the administrators of the target domain. You might 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 illustration shows the decision process involved in determining which migration process is appropriate for your organization.



Using SID History to Preserve Resource Access

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 security identifier (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 access control lists (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 the following:

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

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

Using SID Filtering When Migrating User Accounts

Security identifier (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.

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 that are running Windows 2000 Service Pack 4 (SP4), Windows Server 2003, or Windows Server 2008. This prevents potential security attacks by an administrator in a different forest.

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.

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 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 illustration shows an example of an object assignment table for users and groups.

User and Group Object Assignment Table

Prepared By	Active Directory Deployment Team	Date	01/01/03
Source Forest Name	Trccorp.treyresearch.net		
Target Forest Name	Concorp.contoso.com		
Source Domain Name	Asia.trccorp.treyresearch.net		
Target Domain Name	Emea.concorp.contoso.com		

Name	Type	Source Location	Target Location
Finance	Group	Asia\Groups OU	EMEA\Groups OU
Accounting	Group	Asia\Groups OU	EMEA\Groups OU
JBrown	User	Asia\Users OU	EMEA\Users OU
MNguyen	User	Asia\Users OU	EMEA\Users OU
!Scheduler	Service Account	Asia\Users OU	EMEA\Service Accounts OU

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 illustration shows an example of a resource object assignment table.

Resource Assignment Table					
Prepared By	Active Directory Deployment Team		Date	01/01/03	
Source Forest Name	Trccorp.treyresearch.net				
Target Forest Name	Concorp.contoso.com				
Source Domain Name	Asia.trccorp.treyresearch.net				
Target Domain Name	Emea.concorp.contoso.com				
Name	Type	Source OU	Target OU	Physical Location	Role in Target Domain
FS01	Member server (file server)	Computers	Member Servers	Hong Kong SAR	Member Server
UserWrk01	Computer account	Default	Wrk	Hong Kong SAR	Computer account
UserWrk02	Computer account	Wrk	Wrk	Boston	Computer account
DC01	Domain Controller	Domain Controllers	Domain Controllers	Boston	Domain controller
DC02	Domain Controller	Domain Controllers	Member Servers	Hong Kong SAR	Member server

Developing a Test Plan for Your Migration

The Active Directory Migration Tool version 3.1 (ADMT v3.1) does not include a test migration option, which was available in previous versions of ADMT. However, you can develop a test plan to systematically test each object after it is migrated to the new environment and identify and correct 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, access resources based on group membership, and 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 (LOB) 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 has 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 illustration shows an example of a completed migration test matrix.

Migration Test Matrix			
Prepared By	Active Directory Deployment Team	Date	01/01/03
Source Forest Name	Trccorp.treyresearch.net		
Target Forest Name	Concorp.contoso.com		
Source Domain Name	Asia.trccorp.treyresearch.net		
Target Domain Name	Emea.concorp.contoso.com		

Test Name	Performed Before Migration	Result After Migration	Notes
Create test user for users in Sales department "batch1"	Yes	Success	
Join user to sales group	Yes	Success	
Log on to source domain and verify access to required resources	Yes	Success	
Log on to target domain	No	Success	
Verify access to file and print shares	No	Success	
Verify access to customer management application	No	Success	
Verify user desktop settings and access to My Documents folder	No	Success	
Verify that applications appear and start from the Start menu	No	Success	

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 can 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 have to modify objects, such as member servers or domain controllers, to migrate them to the target domain, back up all the data before you make the modifications and perform 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 domain and the target domain. 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 security identifiers (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 the Active Directory Migration Tool (ADMT) to remigrate user accounts as often as necessary during the migration process. This ensures that changes that are 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 attributes include the following:

- 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 the following:

- 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 user interface (UI) and included in the exclusion list for the next migration. Scripting and command-line attributes do not have state information. Therefore, they 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 have 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 have 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.

Type	Description	Migration Requirements
Roaming profiles	User profiles are stored centrally on servers. Profiles are available to the user, regardless of the workstation in use.	Select **Translate roaming profiles** 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.
Local profiles	User profiles are stored locally on the workstation. When a user logs on to another workstation, a unique local user profile is created.	Translate local profiles as a separate step from the user account migration process. Select **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.
Profiles not managed	Same as local profiles.	Users lose their existing profiles when their user accounts are migrated.
Hardware refresh	User state information is stored locally on the workstation.	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.

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 100 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 contain ned 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 necessary if the users 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 must 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

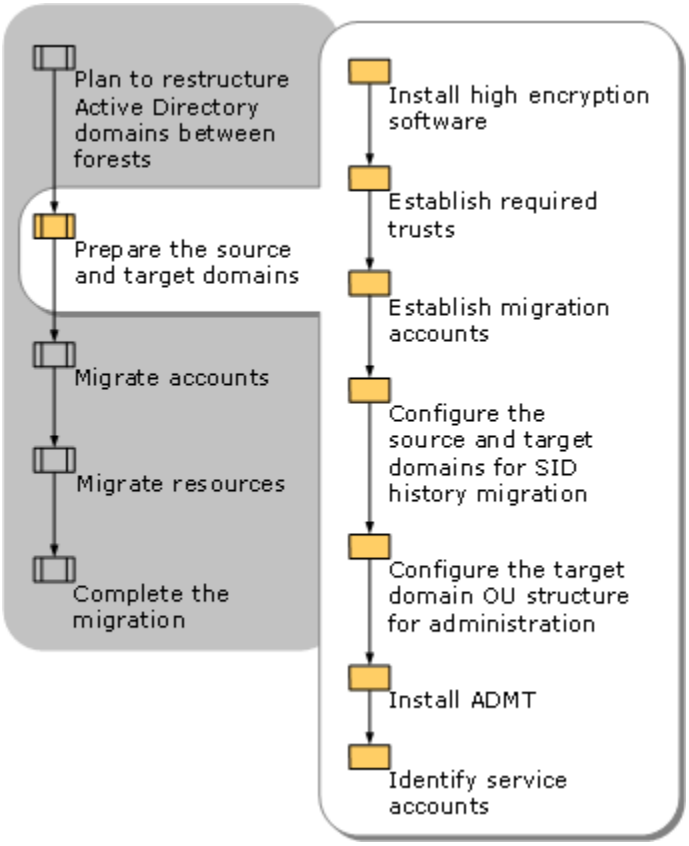
Describe other changes that users can expect to experience after the migration, such as changes in use of smart cards, secure e-mail, or instant messaging, if applicable.

Scheduling and support information

Provide information about where users can go to find more information For example, they can visit 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 domain to the target domain, you have to prepare the source and target domains for the migration. The following illustration shows the tasks that are required to prepare the domains for the interforest domain restructure process.



Installing 128-Bit High Encryption Software

The computer on which the Active Directory Migration Tool (ADMT) is installed requires 128-bit high encryption. This encryption is standard on computers that are running Windows 2000 Server Service Pack 3 (SP3) or Service Pack 4 (SP4), Windows Server 2003, or Windows Server 2008. 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 makes it possible for the

Active Directory Migration Tool (ADMT) to migrate users and service accounts and translate local user profiles from the source domains to the target domains. In addition, depending on how trust relationships are configured, users in the source domain can access resources in the target domain. Moreover, users in the target domains can access resources in the source domain 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. The Active Directory Migration Tool (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 helps 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 the security identifier (SID) history, global groups along with SID history, computers, and user profiles has local administrator or domain administrator credentials in the source domain. The migration account also has delegated permission on the user, group, and computer organizational units (OUs) in the target domain, with the extended right to migrate SID history on the user OU. The user must 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.

Migration object	Credentials necessary in source domain	Credentials necessary in target domain
User/group without SID history	Delegated **Read all user information** permission on the user OU or group OU and domain administrator credential	Delegated **Create, delete, and manage user accounts**, **Create, delete, and manage groups**, and **Modify the membership of a group** for the user OU or the group OU and local administrator on the computer where ADMT is installed
User/group with SID history	Delegated **Read all user information** permission on the user OU or group OU and domain administrator credential	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
Computer	Domain administrator or administrator in the source domain and on each computer	Delegated permission on the computer OU and local administrator on the computer on which ADMT is installed
Profile	Local administrator or domain administrator	Delegated permission on the user OU and local administrator on the computer on which ADMT is installed.

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, follow these steps:
   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 **Permissions for acct_migrators**, 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 have 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 version 3.1 (v3.1) 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.

Role	Migration task
Account migrators	Account migrations tasks, such as user and group migration.
Resource migrators	Resource migration tasks, such as computer migrations and security translation. Account migrators also hold the role of resource migrators.
Data readers	Queries against that database. Account migrators and resource migrators also hold the role of data readers.

Users who are assigned the role of SQL Server sysadmin hold all ADMT database administration roles. They have the credentials 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.

Configuring the Source and Target Domains for SID History Migration

You can manually configure the source and target domains to migrate the security identifier (SID) history before you begin an interforest migration, or you can allow the Active Directory Migration Tool (ADMT) to configure the domains 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 primary domain controller (PDC) emulator.
- Enable auditing in the Windows Server 2008 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 (also known as flexible single master operations or FSMO) 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 2008 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 organizational unit (OU) structure for the target domain. This team also defines the groups that are 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 that your design team specified.
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 the Active Directory Migration Tool version 3.1 (ADMT v3.1), it also installs SQL Server 2005 Express Edition by default to use as its data store. As an option, you can configure ADMT v3.1 to use a SQL Server 2000 with a Service Pack 4 (SP4) Standard or Enterprise Edition database or SQL Server 2005 Standard or Enterprise Edition installation that you have previously created.

Prerequisites for installing ADMT

Before you install ADMT v3.1, complete the following prerequisites:

- Install Windows Server 2008.
- Remove all previous versions of ADMT by using **Add or Remove Programs** from Control Panel. If you attempt to install ADMT v3.1 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 (such as ADMT v2.0 or ADMT v3.0) into ADMT v3.1 during the installation.
- If you do not plan to use the default local database installation, ensure that another SQL Server 2000 or SQL Server 2005 database installation is configured with an ADMT instance. For more information about creating an ADMT instance on a SQL Server database, see Installing ADMT Using a Preconfigured SQL Database.

Installing ADMT using the default database store

You can use the default database store based on SQL Server 2005 Express Edition 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 by using the default database store

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

Wizard Page	Action
Welcome to the Active Directory Migration Tool Installation	Click **Next**.
Configuring Components	The ADMT database instance (MS_ADMT) is created on the local computer. Although SQL Server 2005 Express Edition is installed locally by default whether ADMT uses it or not, ADMT disables SQL Server 2005 Express Edition if you specify another database instance on the next wizard page.
Database Selection	Specify the database instance you want to connect to. The recommended selection is **Use Microsoft SQL Server Express Edition**, which configures ADMT v3.1 to use the locally installed database instance. If you are using multiple ADMT v3.1 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 v3.1 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 v3 Database Import	Although you cannot upgrade an ADMT v3.0 installation to ADMT v3.1, you can import data to an ADMT v3.1 database from an ADMT v3.0 database. If you do not want to import data from an ADMT v3.0 database, select **No, do not import data from an existing database (Default)**. If you want to import data from ADMT v3.0 into the new ADMT v3.1 database, select **Yes, please import data from an ADMT v3 database**. If you choose to import data, specify the path to the ADMT v3.0 database file.
Active Directory Migration Tool v2 Database Import	Although you cannot upgrade an ADMT v2.0 installation to ADMT v3.1, you can import data to an ADMT v3.1 database from an ADMT v2.0 database. If you do not want to import data from an ADMT v2.0 database, select **No, do not import data from an ADMT v2 database**. If you want to import data from ADMT v2.0 into the new ADMT v3.1 database, select **Yes, please import data from an ADMT v2 database**. If you choose to import data, specify the path to the ADMT v2.0 database file. The ADMT v2.0 database has the filename protar.mdb, and should be located in the directory formerly used for your ADMT v2.0 installation.
Summary	This page summarizes the options you selected. To complete the ADMT v3.1 installation, click **Finish**.

Installing ADMT by 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. You can also choose to install ADMT in an instance of SQL Server 2005.

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.

Syntax	Description
`admtdb create /s|server:  <Server\Instance>`	Specifies the name of the SQL Server and instance to connect to for the purpose of database creation. This is a required parameter.
`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 by using the **admtdb import** command.
`admtdb create [/{a|attach}: "<v3 database path>"`	Specifies the fully qualified path to the database file that was used with a previous ADMT v3.0 installation. Required **/server** parameter must be specified with this option. ADMT v3.0 data can be imported at the time of creation, or later into an empty database by 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 **Start**, and then click **OK**.
5. Close **Services**.
6. Open a command prompt, type the following command and then press ENTER:

   ```
   admt config /setdatabase: <Server\Instance>
   ```

   You can now use the default local database.

Enabling Migration of Passwords

The Active Directory Migration Tool version 3.1 (ADMT v3.1) uses the Password Export Server (PES) service version 3.1 to help you migrate passwords when you perform an interforest migration. The PES service can be installed on any fully writable domain controller in the source domain that supports 128-bit encryption.

Note

The PES service cannot be installed on read-only domain controllers (RODCs).

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.

You can install the PES service before or after you install ADMT v3.1. The following procedures explain how to install and use the PES service on computers running Windows Server 2008.

Membership in **Administrators**, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at http://go.microsoft.com/fwlink/?LinkId=83477.

To create an encryption key

- At a command line, type the following command, and then press ENTER:

```
admt key /option:create /sourcedomain:<SourceDomain> /keyfile:<KeyFilePath>
/keypassword:{<password>|*}
```

Value	Description
<SourceDomain>	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.
<KeyFilePath>	Specifies the path to the location where the encrypted key is stored.
{<password>|*}	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.

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. We recommend that you run the PES service as an authenticated user in the target domain. This way, you do not have 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**.

Wizard page	Action

Welcome to the ADMT Password Migration DLL Installation Wizard	Click **Next**.
Encryption File	To install the ADMT Password Migration dynamic-link library (DLL), you must specify a file that contains a valid password encryption key for this source domain. The key file must be located on a local drive. You use the **admt key** command to generate the key files. For more information, see the previous procedure "To create an encryption key."
Run the service as	Specify the account that you want the PES service to run under. You can specify either of the following accounts: • The local System account • A specified user account **Note** If you plan to run the PES service as an authenticated user account, specify the account in the format *domain\user_name*.
Summary	Click **Finish** to complete the PES service installation. **Note** To use the password migration of ADMT, you must restart the server where you installed the PES service.

3. After installation completes, restart the domain controller.
4. 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**.
5. 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

Start the Active Directory Migration Tool (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 the security idenditifer (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 primary domain controller (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.

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 comleting the steps in the following table. Accept default settings when no information is specified.

Wizard page	Action
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.

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. The Active Directory Migration Tool (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. Second, the Service Account Migration Wizard sends an agent to a specified computer and identifies (but does not migrate) all of the services on the computer that are running in the context of a user account. Third, which can occur later in the migration process, the accounts are migrated 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, ADMT cannot synchronize the service accounts. 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 in Your Migration, later in this guide.

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

To identify service accounts by using the ADMT snap-in

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 snap-in, click **Action**, and then click **Service Account Migration Wizard**.
3. Complete the Service Account Migration Wizard by using the information in the following table.

Wizard page	Action
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 have to be marked as service accounts in the ADMT database, and then click **Skip/Include** to mark the accounts as **Skip**.
Completing the Service Account Migration Wizard	Review your selections, and then click **Finish**.

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 have 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 the following command, and then press ENTER:

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

   Where `<computer_name1>` and `<computer_name2>` are the names of computers in the source domain that run service accounts.

   As an alternative, 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 that are used for the identification of

service accounts, along with the command-line parameter and option file equivalents.

Values	Command-line syntax	Option file syntax
<Source domain>	/SD:"*source_domain*"	SourceDomain="*source_domain*"
<Target domain>	/TD:"*target_domain*"	TargetDomain="*target_domain*"

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 following sample script. 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="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"

   '
```

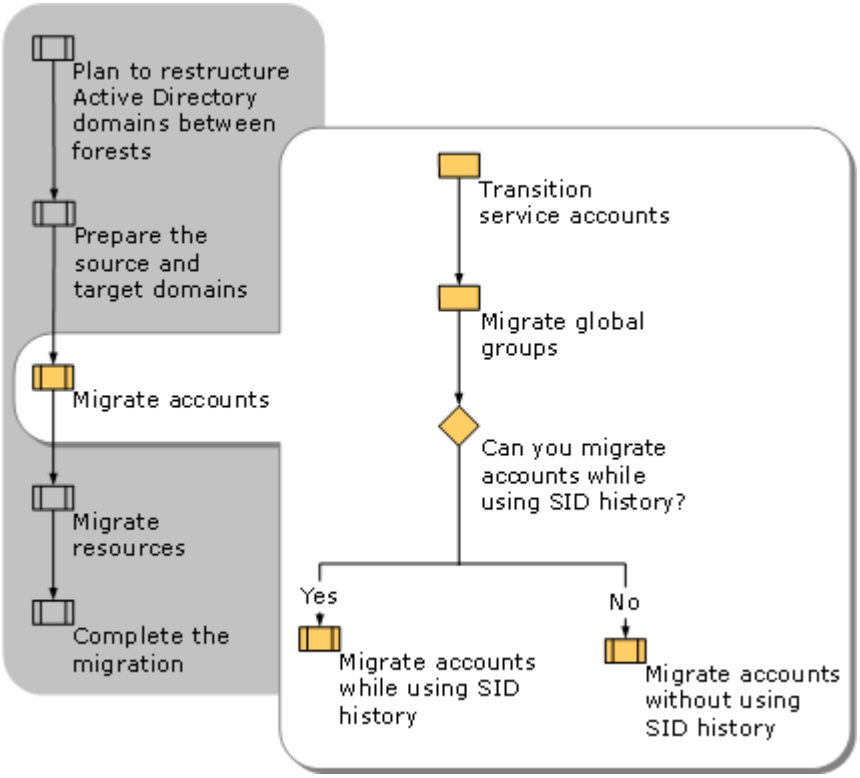
```
    'Enumerate service accounts on specified computers.
    '


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


    Set objServiceAccountEnumeration = Nothing
    Set objMigration = Nothing
</Script>
</Job>
```

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 the security identifier (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 illustration 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 Transitioning Service Accounts in Your Migration, earlier in this guide.

To transition service accounts, use the Active Directory Migration Tool (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 the services use the service account in the target domain instead of in the source domain.

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

To transition service accounts by using the ADMT snap-in

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 snap-in, click **Action**, and then click **User Account Migration Wizard**.

3. Complete the User Account Migration Wizard by using the information in the following table.

Wizard page	Action
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 **Browse for Container**, locate the source domain, select the container for the service accounts, and then click **OK**.
Password Options	Click **Generate complex passwords**. **Note** When you transition service accounts by using the User Account Migration Wizard, a complex password is generated automatically, regardless of the option that is

	selected on this wizard page. Even if **Do not update passwords for existing users** is selected, a complex password is generated.
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.

4. When the wizard has finished running, click **View Log**, and review the migration log for any errors.
5. Start Active Directory Users and Computers, navigate to the organizational unit (OU) that you created for service accounts, and then verify that the service accounts exist in the target domain OU.
6. 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 the following command, and then press ENTER:

   ```
   ADMT USER /N "<server_name1>" "<server_name2>" /SD:" <source_domain>" /TD:" <target_domain>" /TO:" <target_OU>" /MSS:YES
   ```

   Where *Server_name1* and *Server_name2* are the names of servers in the source domain that run service accounts. As an alternative, 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 that are used for transitioning service accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Disable accounts	`/DOT:ENABLETARGET` (default)	`DisableOption=ENABLETARGET` (default)
Migrate password	`/PO:COMPLEX` (default)	`PasswordOption=COMPLEX`
Migrate user SIDs = YES	`/MSS:YES`	`MigrateSIDs=YES`
Update user rights=YES	`/UUR:YES`	`UpdateUserRights=YES`
Conflict management	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE` (default)

3. Review the results that appear 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 following sample script. 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=" TransitioningServiceAccountsBetweenForests" >
<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.ConflictOptions = admtIgnoreConflicting

   '
   'Specify user migration specific options.
   '

   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 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 performing 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 security identifier (SID) is created for the object in the target domain.
3. To preserve resource access, the Active Directory Migration Tool (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.

After 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 have 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 snap-in, the ADMT command-line option, or a script.

To migrate global groups by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
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 organizational unit (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 snap-in, 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, and then press ENTER:

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

   As an alternative, 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 that are used for migrating global groups, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Migrate GG SIDs	`/MSS:YES`	`MigrateSIDs=YES`
Conflict	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE`

management		

3. Review the results that appear on the screen for any errors.
4. Open the Active Directory Users and Computers snap-in 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 following sample script. 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

   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 admtData, Array("group name1" ,"group name2" )

    Set objGroupMigration = Nothing
    Set objMigration = Nothing
</Script>
</Job>
```

Migrating Accounts While Using SID History

To migrate accounts while using the security identifier (SID) history, first migrate all the user accounts—but do not enable them in the target domain—to prepopulate the target domain and allow migration of user profiles. After all the user accounts are successfully migrated, begin migrating users in batches by migrating first the user profile, then the workstation, and then the user account. Before you migrate 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 the Active Directory Migration Tool (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 that are associated with EFS, Secure/Multipurpose Internet Mail Extensions (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 the 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 you migrate 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 helps you to track the accounts that have been migrated and to test the success of each migration step. If the organizational unit (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 alternative 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 OUs 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 that 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.

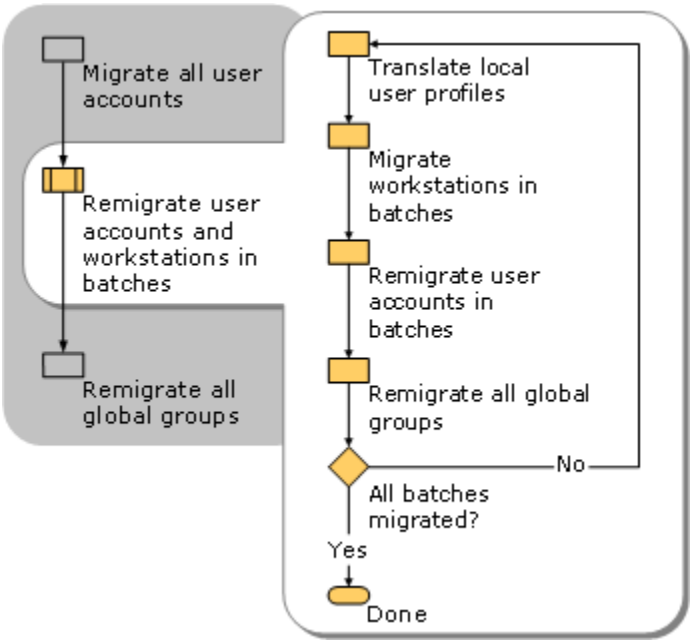
Using ADMT to migrate user accounts also preserves user passwords. After the user accounts are migrated to and enabled in the target domain, the users can log on to the target domain by using their original passwords. After they log on, the users are prompted to change the password.

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 illustration 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 helps you translate local profiles and ensure that users continue to have the appropriate resource access after the migration.

Note

Built-in accounts (such as Administrators, Users, and Power Users) cannot be Active Directory Migration Tool (ADMT) migration objects. Because built-in account security identifiers (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 snap-in, by using the ADMT command-line option, or by using a script.

To migrate the current batch of users by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
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 **Generatecomplex 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 seven 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. 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, and then press ENTER.

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

   As an alternative, 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 that are used for migrating user accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Migrate SIDs	`/MSS:YES`	`MigrateSIDs=YES`
Disable option	`/DOT:DISABLETARGET`	`DISABLEOPTION=DISABLETARGET`
Source expiration	`/SEP:7`	`SOURCEEXPIRATION=7`
Conflict management	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE`
Translate roaming profile	`/TRP:YES` (default)	`TranslateRoamingProfile=YES`
Update user rights	`/UUR:NO`	`UpdateUserRights=NO`
Password options	`/PO:COMPLEX`	`PasswordOption=COMPLEX`

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 following sample script. Copy the script to Notepad, and save the file with a .wsf file name extension in the same folder as the AdmtConstants.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, specify West/Sales as the container name. For more information, see TemplateScripts.vbs in the ADMT installation folder.

```
   <Job id=" MigratingAllUserAccountsBetweenForests" >
<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 = admtComplexPassword
   objMigration.ConflictOptions = admtIgnoreConflicting

   '
```

```
    'Specify user migration specific options.
    '

    objUserMigration.MigrateSIDs = True
    objUserMigration.TranslateRoamingProfile = True
    objUserMigration.UpdateUserRights = False
    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>
```

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

The Active Directory Migration Tool (ADMT) only translates profiles for computers running Windows NT 4.0, Windows 2000 Server, Windows XP, or Windows Server 2003.

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 Service Pack 3 (SP3) or Service Pack 4 (SP4) and Windows XP Service Pack 1 (SP1) or Service Pack 2 (SP2), 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 snap-in, the ADMT command-line option, or a script.

To translate local user profiles by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
Security Translation Options	Click **Previously migrated objects**.
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 have 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, and then press ENTER.

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

   As an alternative, 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 that are used for migrating user accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:"`*source_domain*`"`	`SourceDomain="`*source_domain*`"`
<Target domain>	`/TD:"`*target_domain*`"`	`TargetDomain="`*target_domain*`"`
Security translation options	`/TOT:REPLACE`	`TranslateOption=REPLACE`
Modify local user profile security	`/TUP:YES`	`TranslateUserProfiles=YES`

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 have 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 following sample script. 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=" 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 Security Accounts Manager (SAM) database is migrated along with the computer. Accounts in the local SAM database (such as local groups) that are used to enable access to resources always move with the computer. Therefore, these accounts do not have 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 after migration are in an indeterminate state.

You can migrate workstations and member servers by using the AMDT snap-in, ADMT command-line option, or a script.

To migrate workstations by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
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	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 **Excluded Properties**, 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 have 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, and then press ENTER.

```
ADMT COMPUTER /N "<computer_name1>" "<computer_name2>" /SD:" <source_domain>"
```

```
/TD:" <target_domain>" /TO:"<target_OU>" /RDL:5
```

As an alternative, 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 that are used for workstation migration, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Restart delay (minutes)	`/RDL:5`	`RestartDelay=5`
Security translation option	`/TOT:ADD`	`TranslationOption=ADD`
Translate user rights	`/TUR:YES`	`TranslateUserRights=YES`
Translate local groups	`/TLG:YES`	`TranslateLocalGroups=YES`

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 have 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 following sample script 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="MigratingWorkstationsBwtweenForest" >
```

```
<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.SourceDomain = "source domain"
   objMigration.SourceOu = "Computers"
   objMigration.TargetDomain = "target domain"
   objMigration.TargetOu = "Computers"

   '
   'Specify computer migration specific options.
   '

   objComputerMigration.RestartDelay = 1
   objComputerMigration.TranslationOption = admtTranslateAdd
   objComputerMigration.TranslateLocalGroups = True
   objComputerMigration.TranslateUserRights = True
```

```
    '
    'Migrate computer objects on specified computer objects.
    '


    objComputerMigration.Migrate admtData, _
   Array("computer name1" ,"computer name2" )


    Set objComputerMigration = Nothing
    Set objMigration = Nothing
</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 snap-in, the ADMT command-line option, or a script.

To migrate the current batch of user accounts by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
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 seven 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.
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	Select the **Migrate and merge conflicting objects** check box. 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 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, and then press ENTER.

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

   As an alternative, 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 that are used for migrating user accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"

<Target OU> location	/TO:"*target_OU*"	TargetOU="*target_OU*"
Migrate SIDs	/MSS:YES	MigrateSIDs=YES
Conflict management	/CO:REPLACE	ConflictOptions=REPLACE
Translate roaming profile	/TRP:YES (default)	TranslateRoamingProfile=YES
Update user rights	/UUR:YES	UpdateUserRights=YES
Password options	/PO:COPY /PS:*<name of PES server>*	PasswordOption=COPY PasswordServer=:*<name of PES server>*
Source expiration	/SEP:7	SourceExpiration=7

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 following sample script. 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="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.
    '
    objUserMigration.SourceExpiration = 7
    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>
```

Remigrating all global groups after user account migration

A large user account migration might take place over an extended period of time. For this reason, you might have 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 that are made to global group membership in the source domain are reflected in the target domain. You can remigrate global groups by using the Active Directory Migration Tool ADMT snap-in, the ADMT command-line option, or a script.

To remigrate global groups by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
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 organization unit (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 **Update user rights**. Ensure that **Copy group members** is not selected. Ensure that **Update previously migrated objects** is not selected. Click **Fix membership of group**. Click **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 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, and then press ENTER.

   ```
   ADMT GROUP /N "<group_name1>" "<group_name2>" /SD:" <source_domain>" /TD:" <target domain>" /TO:" <target OU>" /MSS:YES /CO:REPLACE
   ```

   As an alternative, 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 that are used for migrating global groups, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Migrate GG SIDs	`/MSS:YES`	`MigrateSIDs=YES`
Conflict management	`/CO:REPLACE`	`ConflictOptions=REPLACE`

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 following sample script. 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=" 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.
    '

    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>
```

Migrating Accounts Without Using SID History

If you are not using security identifier (SID) history for resource access because SID filtering is in place between your forests, your migration process involves performing the following steps. First, you migrate all the user accounts—but do not enable 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, and then the user account. Finally, you must remigrate the global groups to apply any changes that are 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 you migrate all user accounts, ensure that you have created test accounts that you can use to verify the success of each batch.

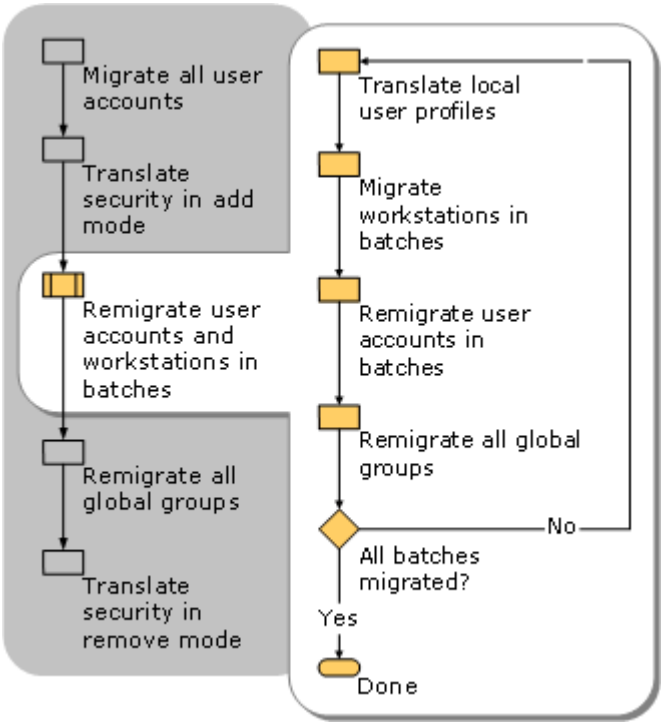
Complete the following steps to migrate user accounts to the target domain:

1. Migrate all users. Use the **Fix users' group membership** option both to have the Active Directory Migration Tool (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 you migrate 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 that are set to expire in seven days with 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 illustration shows the steps involved in migrating accounts that are not using SID history for resource access.



Migrating 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 after the migration.

Note

Built-in accounts (such as Administrators, Users, and Power Users) cannot be Active Directory Migration Tools (ADMT) migration objects. Because built-in account security identifiers (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 snap-in, the ADMT command-line option, or a script.

To migrate user accounts by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
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 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 organizational unit (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, and then press ENTER:

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

   As an alternative, 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 that are used for migrating user accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Migrate SIDs	`/MSS:YES`	`MigrateSIDs=YES`
Conflict management	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE`
Translate roaming profile	`/TRP:YES` (default)	`TranslateRoamingProfile=YES`
Update user rights	`/UUR:YES`	`UpdateUserRights=YES`
Password options	`/PO:COMPLEX` (default)	`PasswordOption=COMPLEX`

3. Review the results that appear 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 following sample script. 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=" MigratingAllUserAccountsBetweenForests" >
<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 = 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 security identifiers (SIDs) of the user accounts 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 the Active Directory Migration Tool (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 snap-in, the ADMT command-line option, or a script.

To translate security in Add mode on objects by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
Security Translation Options	Click **Previously migrated objects**.
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 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 have 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 it 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, and then press ENTER::

   ```
   ADMT SECURITY /N "<computer_name1>" "<computer_name2>"  /SD:" <source_domain>"
   /TD:" <target_domain>" /TO:" <target_OU>" /TOT:Add
   ```

   As an alternative, 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 that are used for migrating user accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
Security translation options	`/TOT:Add`	`TranslateOption=ADD`

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 have 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 it 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 following sample script. 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=" TranslatingSecurityInAddModeOnObjectsBetweenForests" >
<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 = 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>
```

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

The Active Directory Migration Tool (ADMT) only translates profiles for computers that are running Windows NT 4.0, Windows 2000 Server, Windows XP, or Windows Server 2003.

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 that are running Windows 2000 Server Service Pack 3 (SP3) or Service Pack 4 (SP4), Windows XP Service Pack 1 (SP1) or Service Pack 2 (SP2), 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 snap-in, the ADMT command-line option, or a script.

To translate local user profiles by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
Security Translation Options	Click **Previously migrated objects**.
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 have 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 it 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, and then press ENTER:

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

   As an alternative, 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 that are used for migrating user accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
Security translation options	`/TOT:REPLACE`	`TranslateOption=REPLACE`
Modify local user profile security	`/TUP:YES`	`TranslateUserProfiles=YES`

3. Review the results that appear 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 have 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 following sample script. 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=" 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 Security Accounts Manager (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. Therefore, they do not have 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 after migration are in an indeterminate state.

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

To migrate workstations by using the ADMT snap-in

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 in the following table.

Wizard page	Action
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 organizational unit (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 have 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 it 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, and then press ENTER:

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

   As an alternative, 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 that are used for workstation migration, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Restart delay	`/RDL:5`	`RestartDelay=5`

(minutes)		
Security translation option	`/TOT:ADD`	`TranslationOption=ADD`
Translate user rights	`/TUR:YES`	`TranslateUserRights=YES`
Translate local groups	`/TLG:YES`	`TranslateLocalGroups=YES`

3. Review the results that appear 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 have 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 it 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 following sample script. 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="MigratingWorkstationsBwtweenForest" >
<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.SourceDomain = "source domain"
    objMigration.SourceOu = "Computers"
    objMigration.TargetDomain = "target domain"
    objMigration.TargetOu = "Computers"

    '
    'Specify computer migration specific options.
    '

    objComputerMigration.RestartDelay = 1
    objComputerMigration.TranslationOption = admtTranslateAdd
    objComputerMigration.TranslateLocalGroups = True
    objComputerMigration.TranslateUserRights = True




    '
    'Migrate computer objects on specified computer objects.
    '

    objComputerMigration.Migrate admtData, _
   Array("computer name1" ,"computer name2" )

    Set objComputerMigration = Nothing
    Set objMigration = Nothing
</Script>
```

Remigrating user accounts in batches

After you have verified the success of your migration of 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 snap-in, the ADMT command-line option, or a script.

To remigrate the current batch of user accounts by using the ADMT snap-in

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 in the following table.

Wizard page	Action
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 number of days that 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.
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, and then press ENTER:

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

   As an alternative, 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 that are used for migrating user accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Migrate SIDs	`/MSS:YES`	`MigrateSIDs=YES`
Conflict management	`/CO:REPLACE`	`ConflictOptions=REPLACE`
Translate roaming profile	`/TRP:YES` (default)	`TranslateRoamingProfile=YES`
Update user rights	`/UUR:YES`	`UpdateUserRights=YES`
Password options	`/PO:COPY /PS:`*<name of PES server>*	`PasswordOption=COPY` `PasswordServer=:`*<name of PES server>*
Source expiration	`/SEP:30`	`SourceExpiration=30`

3. Review the results that appear 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 following sample script. 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="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.
   '
   objUserMigration.SourceExpiration = 7
```

```
    objUserMigration.MigrateSIDs = True
    objUserMigration.TranslateRoamingProfile = True
    objUserMigration.UpdateUserRights = False
    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>
```

Remigrating all global groups after user account migration

A large user account migration might take place over an extended period of time. For this reason, you may have to remigrate global groups from the source to the target domain after you migrate each batch of users. The objective is to reflect changes that are 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 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 that are made to global group membership in the source domain are reflected in the target domain.

You can remigrate global groups by using the Active Directory Migration Tool (ADMT)snap-in, the ADMT command-line option, or a script.

To remigrate global groups by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
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 organizational unit (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 **Update user rights** check box. Ensure that the **Copy group members** check box is not selected. Ensure that the **Update previously**

	migrated objects check box is not selected. Select the **Fix membership of group** check box. Select the **Migrate Group SIDs to target domain** check box.
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** (all other options are cleared) check box.

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, and then press ENTER:

   ```
   ADMT GROUP /N "<group_name1>" "<group_name2>" /SD:" <source_domain>" /TD:" <target domain>" /TO:" <target OU>" /MSS:YES /CO:REPLACE
   ```

   As an alternative, 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 that are used for migrating global groups, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"

<Target domain>	/TD:"*target_domain*"	TargetDomain="*target_domain*"
<Target OU> location	/TO:"*target_OU*"	TargetOU="*target_OU*"
Migrate GG SIDs	/MSS:YES	MigrateSIDs=YES
Conflict management	/CO:REPLACE	ConflictOptions=REPLACE

3. Review the results that appear 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 following sample script. 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=" 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.
   '

   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>
```

Translating Security in Remove Mode

Translate security on objects to remove the security identifiers (SIDs) of the accounts in the source domain from the access control lists (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).

When you translate security in Remove mode, the SIDs in the source domain for the user are no longer present or available if the target user account has been migrated successfully and the SIDs are added there. This process enables administrative cleanup, and it ensures that users use their "new" target domain account and stop using the "old" source domain account.

You can translate security in Remove mode on objects by using the Active Directory Migration Tool (ADMT) snap-in, the ADMT command-line option, or a script.

To translate security in Remove mode on objects by using the ADMT snap-in

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 in the following table.

Wizard page	Action
Security Translation Options	Click **Previously migrated objects**.
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, and then press ENTER:

   ```
   ADMT SECURITY /N "<computer_name1>" "<computer_name2>"  /SD:" <source_domain>"
   /TD:" <target_domain>" /TO:" <target_OU>" /TOT:Remove
   ```

   As an alternative, 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 that are used for migrating user accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
Security translation options	`/TOT:Remove`	`TranslateOption=REMOVE`

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 have 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 it 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 following sample script. 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=" TranslatingSecurityInRemoveModeOnObjectsBetweenForests" >
<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 = 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
</Script>
</Job>
```

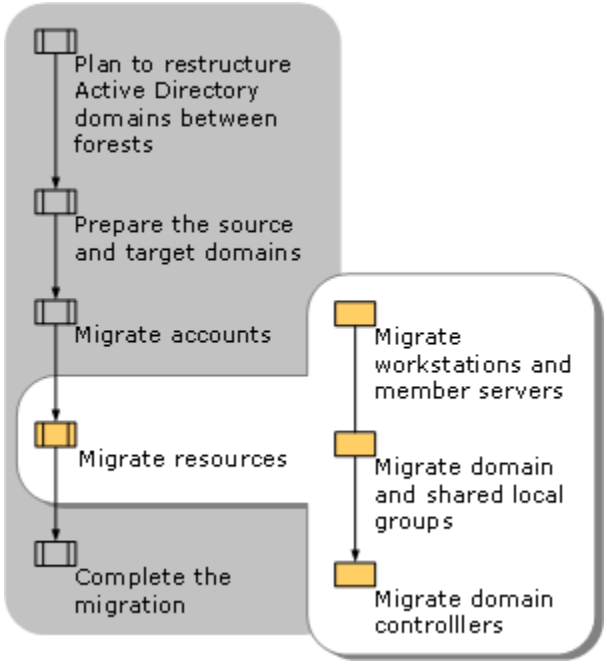
Migrating Resources

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 illustration shows the process for migrating resource objects between Active Directory domains in different forests.



Migrating Workstations and Member Servers

Migrate the 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 Security Accounts Manager (SAM) account database. When you migrate a workstation between domains, the SAM database is migrated along with the computer. Accounts in the local SAM database (such as local groups) that are used to enable access to resources always move with the computer. Therefore, they do not have 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 you join them to the target domain, by selecting a low number (such as 1) for the *RestartDelay* parameter. Resources that are not restarted after migration are in an indeterminate state.

You can migrate workstations and member servers by using the Active Directory Migration Tool (ADMT)snap-in, the ADMT command-line option, or a script.

To migrate workstations and member servers by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
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 organizational unit (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 **Minutes before computer restart after wizard completion** , 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 **Excluded Properties**, 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 have 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 it 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, and then press ENTER:

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

   As an alternative, 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 that are used for workstation migration, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Restart delay (minutes)	`/RDL:5`	`RestartDelay=5`
Security translation option	`/TOT:ADD`	`TranslationOption=ADD`
Translate user rights	`/TUR:YES`	`TranslateUserRights=YES`
Translate local groups	`/TLG:YES`	`TranslateLocalGroups=YES`

3. Review the results that appear 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 have 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 it 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 following sample script. 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="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" )
   Set objComputerMigration = objMigration.CreateComputerMigration

   '
   'Specify general migration options.
   '

   objMigration.SourceDomain = "source domain"
   objMigration.SourceOu = "Computers"
   objMigration.TargetDomain = "target domain"
   objMigration.TargetOu = "Computers"

   '
```

```
    'Specify computer migration specific options.
    '

    objComputerMigration.RestartDelay = 1
    objComputerMigration.TranslationOption = admtTranslateAdd
    objComputerMigration.TranslateLocalGroups = True
    objComputerMigration.TranslateUserRights = True




    '
    'Migrate computer objects on specified computer objects.
    '

    objComputerMigration.Migrate admtData, _
   Array("computer name1" ,"computer name2" )

    Set objComputerMigration = Nothing
    Set objMigration = Nothing
</Script>
</Job>
```

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 the access control lists (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 have 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

security identifier (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 Active Directory Migration Tool (ADMT) snap-in or a script.

To migrate domain and shared local groups by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
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 organizational unit (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 organizational unit (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 following sample script. 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=" 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 admtData, _
   Array("local group name1" ,"local group name2" )

    Set objGroupMigration = Nothing
    Set objMigration = Nothing
</Script>
</Job>
```

Migrating Domain Controllers

In Active Directory or Active Directory Domain Services (AD DS), you can migrate domain controllers between domains. To do this, you must perform the following actions:

- Remove Active Directory or AD DS from the domain controller.
- Migrate the domain controller as a member server to the target domain.
- Reinstall Active Directory or AD DS.

If the server is running Windows 2000 Server, you cannot install Active Directory or AD DS 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 or AD DS.

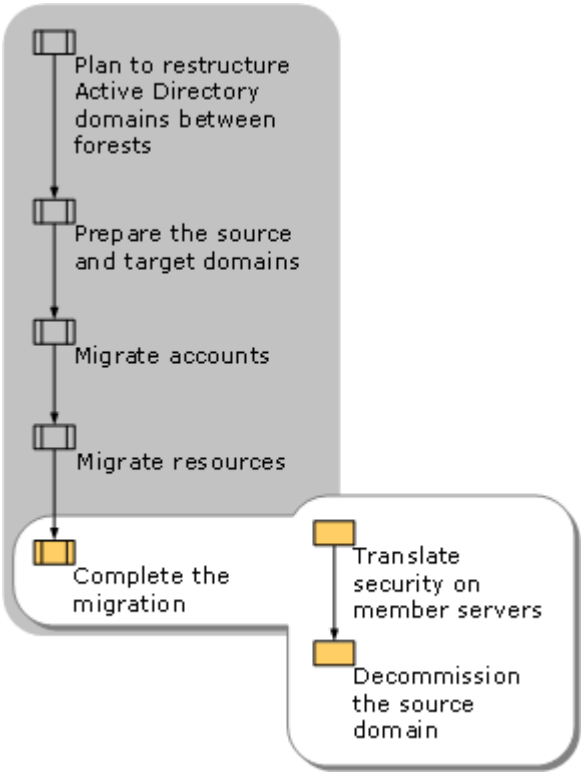
For read-only domain controllers (RODCs) that are deployed on servers running Windows Server 2008, the same steps are required to migrate an RODC as are required for writeable domain controllers.

Completing the Migration

After you migrate all the accounts and resources from the source domain to the target domain, perform the following tasks to complete the restructuring process:

- Transfer the administration of user accounts and group accounts from the source domain 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 you complete these steps, you can translate security on the member servers in the target domain and decommission the source domain. The following illustration 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 access control lists (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 security identifier (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 the Active Directory Migration Tool (ADMT) to replace the source domain SIDs with the target domain SIDs.

You do not have 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 snap-in, the ADMT command-line option, or a script.

To translate security on member servers by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action
Security Translation Options	Click **Previously migrated objects**.
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 other options.
Security Translation Options	Click **Replace**.

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, and then press ENTER:

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

   As an alternative, 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 that are used for migrating user accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
Security translation options	`/TOT:Replace`	`TranslateOption=REPLACE`

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 have 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 it 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 following sample script. 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=" 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 this does not affect users. Do not delete "account unknown" entries because this disables the access that is facilitated by security identifier (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 the following:

- 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 the process for restructuring Active Directory domains between forests. This process requires careful planning and testing.

Checklist: Performing an Intraforest Migration

Reducing the number of Active Directory domains in your forest simplifies the following tasks or reduces the time that is required to complete them:

- Managing administration requirements for your organization
- Handling replication traffic
- Administering users and groups
- Implementing Group Policy

If you frequently reassign users to different domains, you might also migrate objects between domains on a regular basis. Restructuring Active Directory domains within a forest differs from migration between forests, and it requires careful planning and testing.

Task	Reference
Review Active Directory Migration Tool version 3.1 (ADMT v3.1) installation instructions.	Install ADMT v3.1
To migrate computers that are running Windows 2000, Windows XP, and Windows Server 2003 to a target domain with domain controllers running Windows Server 2008, first set the following registry key on the target domain controllers: Registry path: **HKLM\System\CurrentControlSet\Services\Netlogon\Parameters** Registry value: **AllowNT4Crypto** Type: **REG_DWORD** Data: **1** **Note** If you are running Group Policy with target Windows Server 2008 domain controllers, make this change using Group Policy administration. This registry setting corresponds to the **Allow cryptography algorithms compatible with Windows NT 4.0** setting in Group Policy.	For more information about making this change using Group Policy, see Known Issues for Installing and Removing AD DS (http://go.microsoft.com/fwlink/?LinkId=119321).
For any migration tasks that use agent deployment and where Windows Firewall is in use, enable the File and Printer Sharing exception. This can include migration for	For more information, see Enable or Disable the File and Printer Sharing Exception (http://go.microsoft.com/fwlink/?LinkID=

Task	Reference
the following situations: • Migrating workstation computers and member servers that are running under Windows Vista or Windows Server 2008 • Migrating security settings or performing security translation	119315).
Prepare to restructure Active Directory domains within a forest. This task has the following subtasks: • Evaluate the new Active Directory domain structure. • Assign domain object roles and locations. • Plan for group and text migration. • Create a rollback plan and a user communication plan. • Create migration account groups. • Install ADMT. • Plan to transition service accounts.	Install ADMT v3.1 Preparing to Restructure Active Directory Domains Within a Forest
Migrate universal and global groups using either the Group Account Migration Wizard or the **admt group** command-line tool.	Migrate Groups
Migrate service accounts using either the Service Account Migration Wizard or ADMT command-line tools, such as **admt service** to identify service accounts in the source domain and **admt user** to migrate service accounts that you specify.	Migrate Service Accounts
Migrate user accounts using either the User Account Migration Wizard or the **admt user** command-line tool.	Migrate User Accounts
Translate local user profiles using either the Security Translation Wizard or the **admt security** command-line tool.	Translate Local User Profiles
Migrate workstation computers and member servers using either the Computer Migration Wizard or the **admt computer** command-line tool.	Migrate Workstations and Member Servers
Migrate domain local groups using either the Group Account Migration Wizard or the **admt group** command-line tool.	Migrate Domain Local Groups
Complete post-migration tasks. This task has the	• Examine Migration Logs for Errors

Task	Reference
following subtasks: • Examine migration logs for errors. • Verify group types. • Translate security on member servers. • Decommission the source domains.	• Verify Group Types • Translate Security on Member Servers • Decommission the Source Domain

Overview of Restructuring Active Directory Domains Within a Forest Using ADMT v3.1

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 have 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. To simplify your Active Directory logical structure, in the following cases, you might also restructure domains in your forest:

- If you have upgraded your network infrastructure.
- If you have increased network bandwidth and replication capacity.

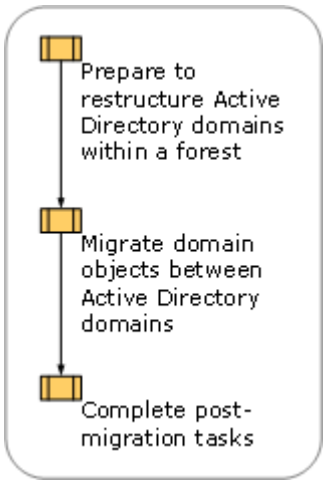
The process of restructuring Active Directory domains in a forest is similar to the process of migrating accounts between domains. When you migrate accounts and resources between domains, you migrate objects from the source domain to the target domain without decommissioning the source domain. When you 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, Windows Server 2003, or Windows Server 2008 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 domain functional level administration in your organization.

Restructuring Active Directory Domains Within a Forest Using ADMT v3.1

To maintain user access to resources during the process of restructuring domains, you must perform the migration steps in a specific order. The following illustration shows the process for restructuring Active Directory domains in a forest.



Background Information for Restructuring Active Directory Domains Within a Forest Using ADMT v3.1

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.

In addition, 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 you do not migrate the global groups to which the user belongs, the user is no longer a valid member of those global groups and the user 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 Active Directory Migration Tool (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 performing 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 security identifier (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 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, we do not recommend 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 that 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 helps 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

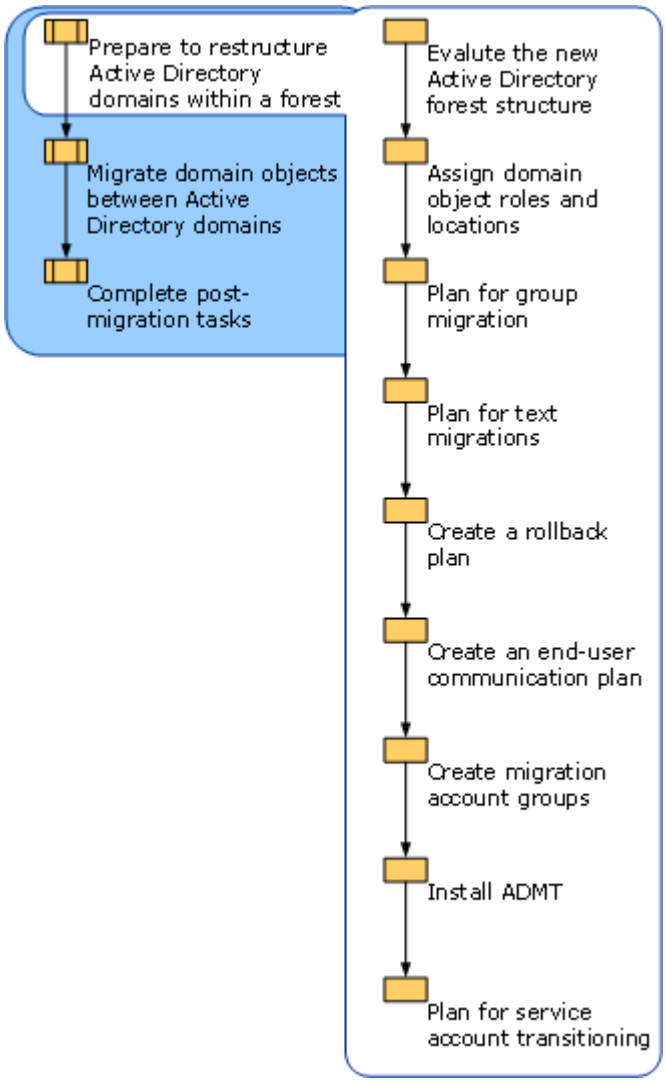
The most effective way to assign permissions to resources is to perform the following actions:

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 illustration 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 have to create new OUs in the target domain.

If you are using the Active Directory Migration Tool (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 they 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/?LinkID=76628).

Assign Domain Object Roles and Locations

Create an object assignment table that lists the roles and locations for all 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 illustration shows an example of an object assignment table for users and groups.

User and Group Object Assignment Table			
Prepared By	Active Directory Deployment Team	Date	01/01/03
Source Forest Name	Trccorp.treyresearch.net		
Target Forest Name	Concorp.contoso.com		
Source Domain Name	Asia.trccorp.treyresearch.net		
Target Domain Name	Emea.concorp.contoso.com		

Name	Type	Source Location	Target Location
Finance	Group	Asia\Groups OU	EMEA\Groups OU
Accounting	Group	Asia\Groups OU	EMEA\Groups OU
JBrown	User	Asia\Users OU	EMEA\Users OU
MNguyen	User	Asia\Users OU	EMEA\Users OU
!Scheduler	Service Account	Asia\Users OU	EMEA\Service Accounts OU

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 illustration shows an example of a resource object assignment table.

Resource Assignment Table			
Prepared By	Active Directory Deployment Team	Date	01/01/03

Source Forest Name	Trccorp.treyresearch.net
Target Forest Name	Concorp.contoso.com
Source Domain Name	Asia.trccorp.treyresearch.net
Target Domain Name	Emea.concorp.contoso.com

Name	Type	Source OU	Target OU	Physical Location	Role in Target Domain
FS01	Member server (file server)	Computers	Member Servers	Hong Kong SAR	Member Server
UserWrk01	Computer account	Default	Wrk	Hong Kong SAR	Computer account
UserWrk02	Computer account	Wrk	Wrk	Boston	Computer account
DC01	Domain Controller	Domain Controllers	Domain Controllers	Boston	Domain controller
DC02	Domain Controller	Domain Controllers	Member Servers	Hong Kong SAR	Member server

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.

Group type	Location
Global group	Active Directory
Universal group	Active Directory
Domain local group	Active Directory
Computer local group	Database of the local computer

Each type of group is migrated differently based on the group's physical location and its rules for group membership. You can migrate universal groups and global groups by using the Active Directory Migration Tool (ADMT). You can transform them 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 each group type 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.

Group type	Rules and membership
Universal groups	Universal groups can contain members from any domain in the forest, and they can replicate group membership to the global catalog. Therefore, you can use them for administrative groups. When you restructure domains, migrate universal groups first.
Global groups	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.
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

The Active Directory Migration Tool version 3.1 (ADMT v3.1) 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 can log on, access resources based on group membership, and access resources based on user credentials. Testing also helps ensure that users can 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 (LOB) 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 has 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 illustration shows an example of a completed migration test matrix.

Migration Test Matrix			
Prepared By	Active Directory Deployment Team	Date	01/01/03
Source Forest Name	Trccorp.treyresearch.net		
Target Forest Name	Concorp.contoso.com		
Source Domain Name	Asia.trccorp.treyresearch.net		
Target Domain Name	Emea.concorp.contoso.com		

Test Name	Performed Before Migration	Result After Migration	Notes
Create test user for users in Sales department "batch1"	Yes	Success	
Join user to sales group	Yes	Success	
Log on to source domain and verify access to required resources	Yes	Success	
Log on to target domain	No	Success	
Verify access to file and print shares	No	Success	
Verify access to customer management application	No	Success	
Verify user desktop settings and access to My Documents folder	No	Success	
Verify that applications appear and start from the Start menu	No	Success	

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 have 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 the Active Directory Migration Tool (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 security identifiers (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 or Windows Server 2008. 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 100 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 not be able 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 that is 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 Active Directory Migration Tool (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 makes it possible for 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 following table. 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 organizational unit (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.

Migration object	Credentials necessary in the source domain	Credentials necessary in the target domain
User/group	Local administrator, domain administrator, and delegated **Read all user information** for	Delegated **Create, delete, and manage user accounts**, **Create, delete, and manage groups**, and **Modify the**

Migration object	Credentials necessary in the source domain	Credentials necessary in the target domain
	the source OU	**membership of a group** for the user OU or the group OU and local administrator on the computer where ADMT is installed
Computer	Domain administrator or delegated rights to delete the objects in the source OU and member of Administrators group on each computer	Delegated permission on the computer OU and local administrator on the computer on which ADMT is installed
Profile (for Windows NT 4.0 computers only)	Local administrator or domain administrator; for roaming profiles, Administrator of the computer that hosts the roaming profile shared folder	Delegated **Create, delete, and manage user accounts** for the computer OU and local administrator on the computer where ADMT is installed

ADMT v3.1 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.

Role	Migration task
Account migrators	Account migration tasks, such as user and group migration
Resource migrators	Resource migration tasks, such as computer migration and security translation; account migrators also hold the role of resource migrators
Data readers	Queries against that database; account migrators and resource migrators also hold the role of data readers

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. This group can perform all ADMT database functions.

Install ADMT v3.1

The Active Directory Migration Tool version 3.1 (ADMT v3.1) uses SQL Server 2005 Express Edition as its default, underlying data store. You can use ADMT with the default local database installation, or you can use another SQL Server database installation that you have previously configured.

Prerequisites for installing ADMT

Before you install ADMT v3.1, complete the following prerequisite tasks:

- In Control Panel, select **Add or Remove Programs** to remove all versions of ADMT that are earlier than ADMT v3.1.

  ADMT v3.1 does not support an upgrade from a previous version of ADMT.
- Install or upgrade a server computer (preferably a member server) in either your source or target domain environment as necessary to run Windows Server 2008.

  Although you can use ADMT v3.1 to migrate accounts and resources from Active Directory environments earlier than Windows Server 2008, you can install ADMT v3.1 only on a server running Windows Server 2008.

  In addition to running Windows Server 2008, the server computer that you use to install ADMT v3.1 must not be installed under the Server Core installation option for Windows Server 2008 or be running as a read-only domain controller (RODC).
- If you do not plan to use the local database installation, configure another SQL Server database installation with an ADMT instance. For more information about creating an ADMT instance on a SQL Server database, see Installing ADMT Using a Preconfigured SQL Database.

Installing ADMT by using the default database store

You can use the default database store or a preconfigured SQL Server database to install ADMT v3.1. The most common and recommended installation method is to use the default database store that the Active Directory Migration Tool Installation Wizard configures automatically.

Note

The following procedure describes setup options for configuring how to install ADMT v3.1 with the default database store on a computer that is running Windows Server 2008. Membership in **Administrators**, or equivalent, is the minimum required to complete this

procedure. Review details about using the appropriate accounts and group memberships at http://go.microsoft.com/fwlink/?LinkId=83477.

To install ADMT by using the default database store

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

Wizard page	Action
Welcome to the Active Directory Migration Tool Installation	Click **Next**.
Configuring Components	The ADMT instance (MS_ADMT) is created on the local computer. **Note** ADMT v3.1 setup installs SQL Server 2005 Express Edition locally by default, whether it uses the software or not. However, ADMT v3.1 setup disables SQL Server 2005 Express Edition if you specify another database instance on the **Database Selection** page.
Database Selection	Specify the database instance to which you want to connect. We recommend **Use Microsoft SQL Server 2005 Express Edition**, which configures ADMT v3.1 to use the locally installed database instance. If you are using multiple ADMT v3.1 consoles or have a dedicated database server where you want to centralize your ADMT database, click **Use an existing Microsoft SQL Server**. 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. Configure the SQL Server database instance before you select this option. Although the ADMT v3.1 installation proceeds if the database cannot be

	contacted, you cannot use ADMT v3.1 to migrate accounts or resources until the database instance is created and available.
Database Import	Although you cannot upgrade an ADMT v3.0 installation to ADMT v3.1, you can import data to an ADMT v3.1 database from an ADMT v3.0 database. If you do not want to import data from an ADMT database, click **No, do not import data from an ADMT database (Default)**. If you want to import data from a database that you created by using ADMT v2.0 into the new ADMT v3.1 database, click **Yes, please import data from an ADMT v2.0 database**. If you want to import data, specify the path to the ADMT v2.0 database file.  **Note** The ADMT v2.0 database file is named Protar.mdb. Place this file in the directory that you used formerly for your ADMT v3.0 database file. If you want to import data from a database that you created by using ADMT v3.0 into the new ADMT v3.1 database, click **Yes, please import data from an ADMT v3.0 database**. If you choose to import data using this option, you might have to specify the path to the ADMT v3.0 database file.  **Note** This option appears only if an ADMT v3.0 database is not discovered during setup. ADMT v3.1 setup attempts to locate and attach to the ADMT v3.0 database files in their default location—the \MSSQL$MS\Data subfolder under the directory where ADMT v3.0 was installed. The

	ADMT v3.0 database files are named Admt.mdf and Admt.ldf. You have to browse and select the location only if you are importing from a database that is not discovered. If the database was not discovered by ADMT v3.1 setup, it might have to be detached from the previous ADMT v3.0 and SQL Server Desktop Edition (Windows) instance by using SQL commands. For more information about detaching a SQL database, see SQL Server Books Online. If you are importing or reusing a prior ADMT v3.1 database, the database file can be copied and reused locally. You have to perform the file copy before you install ADMT v3.1 so that the file can be discovered during ADMT v3.1 setup.
Summary	Click **Finish** to complete the ADMT v3.1 installation. This page summarizes the options that you selected.

Install ADMT by using a preconfigured SQL Server 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 want to install ADMT in an instance of SQL Server 2005, install SQL Server 2005, and then use the ADMT database command-line tool (Admtdb.exe). The command-line syntax for this tool is in the following table.

You can run this tool from any server that can target the server computer that is running SQL Server to create the ADMT instance on that server computer.

Syntax	Description
admtdb create /{s|server}: " <Server\Instance>" [/{i|import}:"<v2 database path>"]	Installs a new ADMT database or prepares an empty database.

Syntax	Description
	The **/server** parameter specifies the name of the SQL Server and instance to connect to for the purpose of creating the database. This is a required parameter. The **/import** parameter, which is optional, specifies the path to the Protar.mdb file from a previous ADMT v2 installation. ADMT v1 database files are not suitable for use in an import operation.
admtdb import /{s|server}: "<Server\instance>"/{if|importfile}: "<path to v2 database file>"	Imports an existing ADMT v2 database into an empty database. The **/server** parameter, which is required, specifies the name of the SQL Server and instance to connect to for the purpose of importing the ADMT v2 database. The **/importfile** parameter, which is required, specifies the path to the Protar.mdb file from a previous ADMT v2 installation. ADMT v1 database files are not suitable for use in an import operation.
admtdb upgrade /{s|server}: <Server\instance>	Upgrades a previous version of an ADMT database. The **/server** parameter, which is required, specifies the name of the computer running SQL Server and the instance to connect to for the purpose of upgrading the ADMT v3.0 database. **Note** Before you upgrade the ADMT database, first verify compatibility between the database and the ADMT console by opening the ADMT console.
admtdb attach /{a|attach}: "<v3 database path>"	Attaches an existing ADMT v3.0 database to the local SQL Express 2005 instance. The **/attach** parameter, which is required, specifies the path to the Admt.mdf file that was used in a previous ADMT v3.0 installation.

To see Help for all Admtdb.exe command-line options, type **admtdb /?** at a command prompt.

After you configure the SQL Server database, you can resume ADMT setup and specify the database that you configured in this procedure.

In the Active Directory Migration Tool Installation Wizard, on the **Database Selection** page, select **Use an existing Microsoft SQL Server**, and then specify the server to connect to that you configured in this procedure.

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

Membership in **Administrators**, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at http://go.microsoft.com/fwlink/?LinkId=83477.

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 details pane, navigate to **MSSQL$MS_ADMT**, and then verify that the **Status** column displays **Started**, and that the **Startup Type** is set to **Automatic**. If the **MSSQL$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 **Start**, and then click **OK**.
5. Close **Services**.
6. At the command prompt, type the following command:

   ```
   admt config setdatabase s: Server\Instance
   ```

   You can now use the default local database.

Reuse an existing ADMT v3 database from a previous installation

If you want to use an existing (detached) database from an earlier ADMT v3.0 or ADMT v3.1 installation with the local SQL Express instance, you can complete the following procedure.

Note

Membership in **Administrators**, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at http://go.microsoft.com/fwlink/?LinkId=83477.

To use an existing (detached) ADMT v3 database with the local SQL Server instance

1. On the local computer, click **Start**, point to **Administrative Tools**, and then click

Services.

2. In the details pane, navigate to **MSSQL$MS_ADMT**, and then verify that the **Status** column displays **Started** and that the **Startup Type** is set to **Automatic**.

   If the **MSSQL$MS_ADMT** service is not started or if it is not set to start automatically at system startup, click **Started**, right-click **MSSQL$MS_ADMT**, and then click **Properties**.
3. On the **General** tab, in the **Startup Type** list, click **Automatic**.
4. Under **Service Status**, click **Start**, and then click **OK**.
5. Close **Services**.
6. At the command prompt, type the following command, and then press ENTER:

   ```
   admt attach /a:<v3 database file path>
   ```

   You can now use the existing ADMT v3 database with the local SQL Server Express Edition instance that is installed with ADMT v3.1

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. First, the administrator starts the Active Directory Migration Tool (ADMT) from the target Active Directory domain controller and runs the Service Account Migration Wizard. Second, the Service Account Migration Wizard sends an agent to a specified computer and identifies (but does not migrate) all the services on the computer that are running in the context of a user account. The third 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. You can 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 have to manually set the new password that ADMT creates. 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 performing the steps in the following table.

Wizard page	Action
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**.
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 have 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 have 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 the following command, and then press ENTER:

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

   Where <*computer_name1*>and<*computer_name2*> are the names of computers in the source domain that run service accounts.

As an alternative, 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 that are used for the identification of service accounts, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	`/SD:"`*source_domain*"	`SourceDomain="`*source_domain*"
<Target domain>	`/TD:"`*target_domain*"	`TargetDomain="`*target_domain*"

3. Review the results that appear 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 following sample script. 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="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>
</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 its Africa domain into its EMEA domain.

The Africa domain is the source domain, and the EMEA domain is the target domain for the migration. The organization has to migrate a total of 1,800 users from the Africa domain to the EMEA domain. In addition to the user accounts, the organization must also migrate resources, such as workstations, servers, and groups.

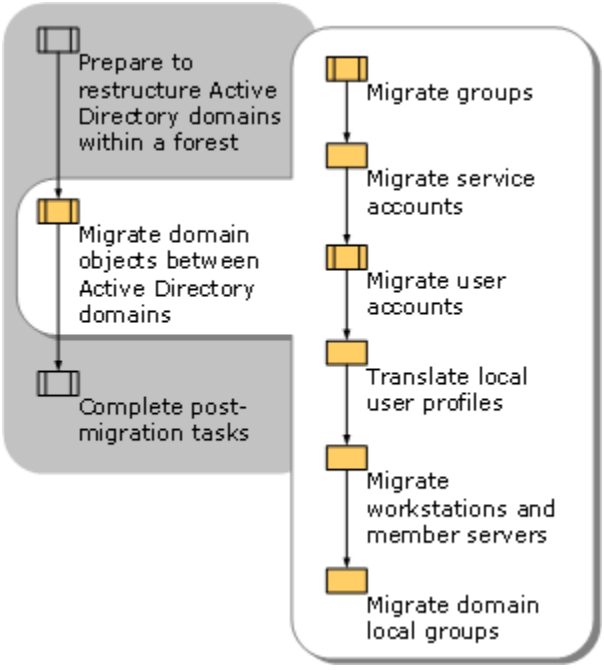
Because Contoso Corporation is a large organization with many global groups, closed sets are difficult to identify. Therefore, the company decided to migrate global groups as universal groups. The company can do this because the infrastructure of the corporation can handle the increased replication of the universal groups and because both the Africa and EMEA domains are operating at the Windows 2000 native functional level. The company created identical organizational unit (OU) structures in the Africa and EMEA domains. Therefore, they do not have 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 decided to use Active Directory Migration Tool (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. The company assigns high-level permissions to the first group and then adds the appropriate deployment team members to that group. The centralized deployment team will use this account to migrate users. The company assigns 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 illustration 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 simultaneously with migrating users, you might not migrate nested groups, which creates 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. The security identifier (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.

Note

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 Active Directory Migration Tool (ADMT) snap-in, the ADMT command-line option, or a script.

To migrate universal groups by using the ADMT snap-in

- 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 performing the steps in the following table.

Wizard page	Action
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 (also known as flexible single master operations or FSMO) 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**.
Organizational Unit Selection	Type the name of the organizational unit (OU), or click **Browse**. In the **Browse for Container** dialog box, find the container in the target domain that you want to move the universal 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**.

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.

   Note

   When you start a group migration with sIDHistory migration from the command line, the command must be run on a domain controller in the target domain.

2. At a command line, type the `ADMT Group` command with the appropriate parameters, and then press ENTER:

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

   As an alternative, 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 universal groups, the command-line parameters, and option file equivalents. For a complete list of all available parameters, see ADMT v3.1 Help.

Parameters	Command-line syntax	Option file syntax
Intra-forest	`/IF:YES`	`IntraForest=YES`
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Conflict management	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE`

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 sample 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 AdmtConstants.vbs file.

  Note

  When you start a group migration with sIDHistory migration from a script, you must run the script on a domain controller in the target domain.

```
   <Job id="MigratingGroupsWithinForest" >
<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.IntraForest = True
    objMigration.SourceDomain = "source domain"
    objMigration.SourceOu = "source container"
    objMigration.TargetDomain = "target domain"
    objMigration.TargetOu = "target container"

    '
    'Migrate specified group objects.
    '

    objGroupMigration.Migrate admtData, Array("group name1" ,"group name2" )

    Set objGroupMigration = Nothing
    Set objMigration = Nothing
</Script>
</Job>
```

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 v3.1, 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 mode or higher.

Because global groups only contain members from their own domain, you cannot migrate them from one domain to another. The Active Directory Migration Tool (ADMT) changes global groups to universal groups when they are migrated. The universal group in the target domain retains the security identifier (SID) history of the global group in the source domain, which makes it possible for 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 have to include built-in and well-known global groups in your migration because these groups already exist in the target domain. If you select a built-in group 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 organizational unit (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 you 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 snap-in, the ADMT command-line option, or a script.

To migrate global groups by using the ADMT snap-in

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 performing the steps in the following table.

Wizard page	Action

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 (also known as flexible single master operations or FSMO) role is always used as the source domain controller, no matter what your selection is. 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.

   Note

   When you start a group migration with sIDHistory migration from the command line, you must run the command on a domain controller in the target domain.

2. At a command line, type the `ADMT Group` command with the appropriate parameters, and then press ENTER:

   ```
   ADMT GROUP /N "<group_name1>" "<group_name2>" /IF:YES /SD:" <source_domain>" /TD:" <target domain>" /TO:" <target OU>"
   ```

   As an alternative, 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.

Parameters	Command-line syntax	Option file syntax
Intra-forest	`/IF:YES`	`IntraForest=YES`
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Conflict management	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE`

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.

Note

When you start a group migration with sIDHistory migration from a script, the script must be run on a domain controller in the target domain.

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 or Windows Server 2008 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 or Windows Server 2008 functional level, the entire group membership replicates every time that 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 Active Directory Migration Tool (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 snap-in, the ADMT command-line option, or a script.

To migrate service accounts by using the ADMT snap-in

- 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 performing the steps in the following table.

Wizard page	Action
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 (also known as flexible single master operations or FSMO) 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**.
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 organizational unit (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 presents 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 they 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 **Skip/Include**. 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 the following command, and then press ENTER:

   ```
   ADMT USER /N "<server_name1>" "<server_name2>" /IF:YES /SD:" <source_domain>" /TD:" <target_domain>" /TO:" <target_OU>" /MSA:YES
   ```

   Where `<Server_name1>` and `<Server_name2>` are the names of servers in the source domain that run service accounts. As an alternative, 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.

Parameters	Command-line syntax	Option file syntax
Intra-forest	`/IF:YES`	`IntraForest=YES`
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Migrate service accounts	`/MSA:YES`	`MigrateServiceAccounts=YES`
Update user rights	`/UUR:YES`	`UpdateUserRights=YES`
Ignore conflicting accounts	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE` (default)

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.

```
   <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
```

```
    '
    '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.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>
```

Migrate User Accounts

Domains can include a large number of user accounts. To make the migration of user accounts manageable, use a technique called *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, for clients that are running Windows 2000 Server, Windows Server 2003, or Windows Server 2008, data that is protected by the Data Protection API (DPAPI) is not migrated. DPAPI helps protect the following items:

- Web page credentials (for example, passwords)
- File share credentials
- Private keys that are associated with EFS, Secure/Multipurpose Internet Mail Extensions (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 the Active Directory Migration Tool (ADMT).
2. Run the Security Translation Wizard on the software distribution point.

Migrating OUs and Subtrees of OUs

If you want to copy organizational units (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 **admtFile** option, you must use the **admtDomain** option with **admtRecurse** and **admtMaintainHierarchy**, as follows:

```
objUserMigration.Migrate admtDomain + admtRecurse + admtMaintainHierarchy
```

Migrate Accounts

You can migrate each batch of user accounts by using the Active Directory Migration Tool (ADMT) snap-in, the ADMT command-line option, or a script.

To migrate user accounts by using the ADMT snap-in

- 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 performing the steps in the following table.

Wizard page	Action
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 (also known as flexible single master operations or FSMO) 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**.
User Selection	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 organizational unit (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 that 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.

   Note

   When you start a user migration with sIDHistory migration from the command line, you must run the command on a domain controller in the target domain.

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
```

As an alternative, 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.

Parameters	Command-line syntax	Option file syntax
Intraforest	`/IF:YES`	`IntraForest=YES`
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Source OU> location	`/SO:`"*source_OU*"	`SourceOU=`"*source_OU*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Conflict management	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE`
Translate roaming profile	`/TRP:YES` (default)	`TranslateRoamingProfile=YES`
Update user rights	`/UUR:YES`	`UpdateUserRights=YES`

3. Review the results that appear 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

-

Note

When you start a user migration with sIDHistory migration from a script, the script must be run on a domain controller in the target domain.

Use the following sample 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 AdmtConstants.vbs file.

```
<Job id=" MigratingUserAccountsWithinForest" >
<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.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
    Set objMigration = Nothing
</Script>
</Job>
```

Translate Local User Profiles

Translate local user profiles after you migrate the user accounts. 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.

Typically, no action is required to translate a local profile on 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 security identifier (SID).

For profile translations, if a user is using offline files on a client running Windows XP Service Pack 1 (SP1), the user loses access to the files in the offline folder. Although the SID of the user changes, the owner in the access control lists (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 Active Directory Migration Tool (ADMT) snap-in, the ADMT command-line option, or a script.

Caution

Verify that user profile translation succeeds for each user before that user is allowed to log on. If the user profile translation fails for a user, that user must not log on to the target domain. In this case, roll back the user account manually by disabling the user account in the target domain and enabling the user account in the source domain.

To translate local user profiles by using the ADMT snap-in

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 Active Directory Migration Tool (ADMT) snap-in, click **Action**, and then click **Security Translation Wizard**.
3. Complete the Security Translation Wizard by using the information in the following table.

Wizard page	Action
Security Translation Options	Click **Previously migrated objects**.
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 (also known as flexible single master operations or FSMO) 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**.
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 and then press ENTER.

   ```
   ADMT SECURITY /N "<computer_name1>" "<computer_name2>" /SD:" <source_domain>"
   /TD:" <target_domain>"  /TOT:REPLACE /TUP:YES
   ```

   As an alternative, 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.

Parameters	Command-line syntax	Option file syntax
Intraforest	`/IF:YES`	`IntraForest=YES`
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target domain>	`/TOT:REPLACE`	`TranslateOption=REPLACE`
Modify local user profile security	`/TUP:YES`	`TranslateUserProfiles=YES`

3. Review the results that appear in the migration log for any errors.

To translate local user profiles by using a script

- Use the following sample 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 AdmtConstants.vbs file.

```
   <Job id=" TranslatingLocalProfilesWithinForest" >
<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"



    '
    '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>
```

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 you join them to the target domain by selecting a low number for the *RestartDelay* parameter. Resources that are not restarted after migration are in an indeterminate state.

Firewalls, such as Windows Firewall in Windows XP Service Pack 2 (SP 2), can prevent the Active Directory Migration Tool (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 makes it possible for 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 snap-in, the ADMT command-line option, or a script.

To migrate workstations and member servers by using the ADMT snap-in

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. Use the Computer Account Migration Wizard by performing the steps in the following table.

Wizard page	Action
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 (also known as flexible single master operations or FSMO) 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**.
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 organizational unit (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 security identifier (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 **Excluded Properties**, 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 have 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 it 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, and then press ENTER.

   ```
   ADMT COMPUTER /N "<computer_name1>" "<computer_name2>" /IF:YES /SD:"
   <source_domain>" /TD:" <target_domain>" /TO:" <target_OU>" /RDL:1
   ```

   As an alternative, 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.

Parameters	Command-line syntax	Option file syntax
Intraforest	`/IF:YES`	`IntraForest=YES`
<Source domain>	`/SD:`"*source_domain*"	`SourceDomain=`"*source_domain*"
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Restart delay (minutes)	`/RDL:5`	`RestartDelay=5`
Conflict management	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE`
Security translation options	`/TOT:ADD`	`TranslationOption=YES`
Translate user rights	`/TUR:YES`	`TranslateUserRights=YES`
Translate local groups	`/TLG:YES`	`TranslateLocalGroups=YES`

3. Review the results that appear 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 have 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 it 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 the Active Directory domain. You can migrate domain local groups by using the Active Directory Migration Tool (ADMT) snap-in, the ADMT command-line option, or a script.

To migrate domain local groups by using the ADMT snap-in

- 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 in the following table.

Wizard page	Action
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 (also known as flexible single master operations or FSMO) 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 organizational unit (OU), or click **Browse**. In **Browse for Container**, locate the OU in the target domain to which the domain local groups are migrating, 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.
Naming Conflicts	Click **Ignore conflicting accounts and don't migrate**.

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, and then press ENTER:

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

   As an alternative, 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 v3.1 Help.

Parameters	Command-line syntax	Option file syntax
Intra-forest	`/IF:YES`	`IntraForest=YES`
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Conflict management	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE`

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

Migrate the domain local groups that exist in the Active Directory domain. You can migrate domain local groups by using the Active Directory Migration Tool (ADMT) snap-in, the ADMT command-line option, or a script.

To migrate domain local groups by using the ADMT snap-in

- 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 in the following table.

Wizard page	Action
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 (also known as flexible single master operations or FSMO) 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 organizational unit (OU), or click **Browse**. In the **Browse for Container** dialog box, locate the OU in the target domain to which the domain local groups are migrating, 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.
Naming Conflicts	Click **Ignore conflicting accounts and don't migrate**.

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, and then press ENTER:

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

   As an alternative, 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 v3.1 Help.

Parameters	Command-line syntax	Option file syntax
Intra-forest	`/IF:YES`	`IntraForest=YES`
<Target domain>	`/TD:`"*target_domain*"	`TargetDomain=`"*target_domain*"
<Target OU> location	`/TO:`"*target_OU*"	`TargetOU=`"*target_OU*"
Conflict management	`/CO:IGNORE` (default)	`ConflictOptions=IGNORE`

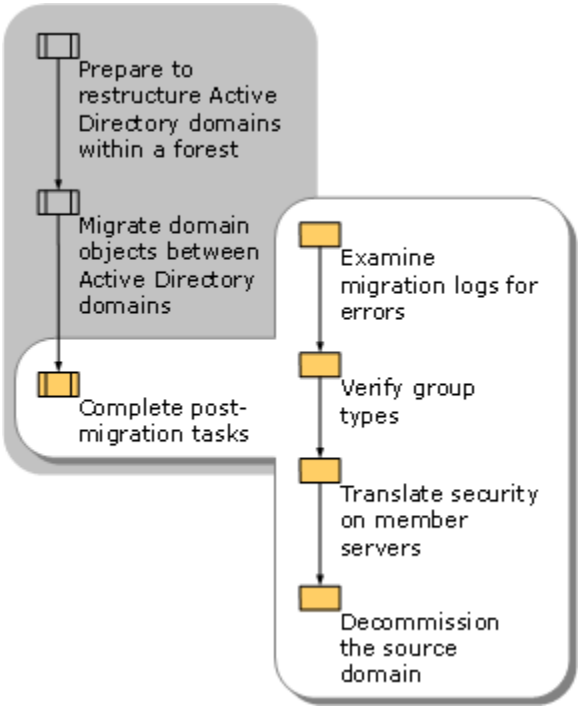
3. Review the results that appear on the screen for any errors.
4. Open Active Directory Users and Computers, and then locate the target domain OU. Verify that the domain local groups exist in the target domain OU.

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.

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 illustration shows the process for completing post-migration tasks.



Examine Migration Logs for Errors

The Active Directory Migration Tool (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 the 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.

Note

Log files are created in the Windows\ADMT\Logs folder on the computer where ADMT is installed.

Accessing ADMT log files

ADMT logs each migration task and stores the logs in the ADMT database. The logs for the last 20 migration tasks are stored on the local computer. You can view log information that is stored in the ADMT database from the ADMT snap-in, or you can use the **admt task** command to retrieve and store that information in a specified location.

When you perform interforest migrations, you can choose to log the attributes for each user, group, and computer object that is migrated. This is called verbose logging, and you do it with the **admt config logging** command.

For more information and examples of commands related to accessing ADMT log files, search for "admt config logging" or "admt task" in the ADMT v3.1 Help.

Verify Group Types

The Active Directory Migration Tool (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 contain only 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 the Active Directory Users and Computers snap-in to verify that universal groups migrated successfully. If you changed domain local groups into universal groups manually, 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 access control lists (ACLs) of the resources. After objects are migrated to the target domain, resources contain the ACL entries of the source domain objects. Although the security identifier (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 snap-in

- 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 performing the steps in the following table.

Wizard page	Action
Security Translation Options	Click **Previously migrated objects**. If you plan to use a SID mapping file, click **Other objects specified in a file**, and then provide the location of the SID

	mapping file that you have created.
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 (also known as flexible single master operations or FSMO) 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**.
Computer Selection	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**.
Translate Objects	Click **File and folders**, **Shares**, **Printers**, **User rights**, and **Registry**.
Security Translation Options	Click **Replace**.

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 following command, and then press ENTER:

   ```
   ADMT Security /N "<computer_name1>" "<computer_name2>" /SD:" <source_domain>"
   /TD:" <target_domain>"
   ```

   Where <Computer_name1> and <computer_name2> are the names of computers for which you want to translate security.

   As an alternative, 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 that are used to translate security on member servers, along with the command-line parameter and option file equivalents.

Parameters	Command-line syntax	Option file syntax
<Source domain>	/SD:"*source_domain*"	SourceDomain="*source_domain*"
<Target domain>	/TD:"*target_domain*"	TargetDomain="*target_domain*"

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 sample 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.

```
   <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 admtData, _
   Array("computer name1" ,"computer name2" )

    Set objSecurityTranslation = Nothing
    Set objMigration = Nothing
</Script>
</Job>
```

Translate Security by Using a SID Mapping File

If you have 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 security identifier (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 Windows 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. The Active Directory Migration Tool (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 the following:

```
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 or Active Directory Domain Services (AD DS) 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 or AD DS 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 members of the team examine 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 security identifiers (SIDs) from the access

control lists (ACLs) of the member servers. Finally, the members of the deployment team decommission the Africa domain at the end of the second week by removing Active Directory or AD DS from the domain controllers in the Africa domain. They then migrate the domain controllers to the EMEA domain as member servers.

Appendix: Advanced Procedures

The following are advanced procedures that you can use to perform various tasks that are helpful when you restructure domains using the Active Directory Migration Tool version 3.1 (ADMT v3.1).

- Configure a Preferred Domain Controller
- Rename Objects During Migration
- Use an Include File
- Use an Option File

Configure a Preferred Domain Controller

The Active Directory Migration Tool (ADMT) provides the option for you to select the source and target domain controller to be used for a migration instead of relying on the domain controller Locator (DC Locator) to select them.

The **Domain Selection** page, which all ADMT wizards contain, now provides a way for you to select an explicit source and target domain controller. As an alternative, you can select **Any domain controller** in the drop-down list. If you specify a domain controller, that domain controller will be used if it is available. If you select **Any domain controller**, ADMT queries for a preferred domain controller. If a preferred domain controller has not been configured, ADMT uses DC Locator to locate a domain controller in the specified domain.

To use a preferred domain controller, you must configure it by using the **admt config** command-line option. You must configure source and target domain controllers independently. After you configure a preferred domain controller, ADMT determines its validity and availability and uses it automatically every time that you run ADMT.

Note

When you perform an intraforest migration, the domain controller that holds the relative ID (RID) operations master (also known as flexible single master operations or FSMO) role is always used by default. If you select a domain controller other than the RID master as the preferred domain controller, ADMT overrides your selection and always uses the RID master.

To configure a preferred domain controller in the source domain

- At a command prompt, type the following command, and then press ENTER:

```
admt config setdomaincontroller /Domain:<DomainName> /sdc:<SourceDomainController>
```

Value	Description
DomainName	Specifies the name of an Active Directory domain.
SourceDomainController	Specifies the computer name of a domain controller in the source domain.

To configure a preferred domain controller in the target domain

- At a command prompt, type the following command, and then press ENTER:

```
admt config setdomaincontroller /Domain:<DomainName> /tdc:<TargetDomainController>
```

Value	Description
DomainName	Specifies the name of an Active Directory domain.
TargetDomainController	Specifies the computer name of a domain controller in the target domain.

You can also clear the preferred domain controller that you have configured in the source or target domain.

To clear preferred domain controllers in a specified domain

- At a command prompt, type the following command, and then press ENTER:

```
admt config cleardomaincontrollers /Domain:<DomainName>
```

Value	Description
DomainName	Specifies the name of an Active Directory domain.

You can also display the preferred domain controllers that you have configured in the source or target domain.

To display preferred domain controllers that you have configured

- At a command prompt, type the following command, and then press ENTER:

```
admt config getdomaincontrollers
```

Rename Objects During Migration

In the Active Directory Migration Tool version 3.1 (ADMT v3.1), you can use an include file to rename source domain objects so that they get a new name after they are migrated to the target domain.

For more information about how to use an include file during a migration, see Use an Include File.

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

To rename objects using an include file

- 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.

  Note

  If the target user principal name (UPN) for a user requires you to specify a domain name that is different from the target domain UPN, use this format to ensure that the user name is preserved and not altered by ADMT during migration.
- 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 organizational unit (OU).
- The **TargetRDN**, **TargetSAM**, and **TargetUPN** column headings are optional, and you can list them in any order.

  Note

  The **TargetUPN** column heading is only relevant during user account migrations because group and computer accounts do not have a UPN.

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 you did not specify in the include file, does 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 you use an RDN value.

Use 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 can list users, groups, and computers together in one file or you can create a separate file for each object type.

After you create the include file (or files), specify the name of the file during migration. The Active Directory Migration Tool (ADMT) accesses the file for the appropriate information.

To specify an include file

From an ADMT wizard

From the command line

To specify an include file from an ADMT wizard

- On the:
  - **Computer Selection Option** page of the Computer Migration Wizard
  - **User Selection Option** page of the User Account Migration Wizard
  - **Group Selection Option** page of the Group Account Migration Wizard

    Click **Read objects from an include file**. When the prompt appears, specify the location of the include file.

To specify an include file from the command line

- At a command prompt, type the following command, and then press ENTER:

  ```
  admt computer /sd:<SourceDomain> /td:<TargetDomain> /F:<IncludeFileName>
  ```

  Note

  For the appropriate command-line syntax for migrating users and groups, search for "admt user" and "admt group" in ADMT version 3.1 (v3.1) Help.

The following information describes the fields of an include file and provides examples of each field:

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 includes a header line indicating the *SourceName* field and 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

You can use the *TargetName* field to specify a base name which is used to generate a target relative distinguished name, a target Security Accounts Manager (SAM) account name and a target user principal name (UPN). The *TargetName* field cannot be combined with other target name fields that are discussed below.

Note

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

Given the following example input, the target relative distinguished name, target SAM account name, and target UPN generated are "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. The *TargetRDN* specifies the target relative distinguished name for the object.

The *TargetSAM* specifies the target SAM account name for the object. Note that for computers the name must include a "$" suffix in order to be a valid SAM account name for a computer.

The *TargetUPN* specifies the target user principal name (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 " "or "," characters, you must enclose the name in double quotation marks ("). In addition, a "," character must be preceded with a "\" escape character or the operation will fail and ADMT will record an invalid syntax error in the log file.

SourceName,TargetRDN

oldname, **CN=***newname*

SourceName,TargetRDN,TargetSAM

oldname, **"CN=***New RDN***"**, *newsamname*

SourceName,TargetRDN,TargetSAM,TargetUPN

oldname, **"CN=***last*, *first***"**, *newsamname*, *newupnname*

SourceName,TargetSAM,TargetUPN,TargetRDN

Note

Use this format when you are renaming user objects, for example, to accommodate specifying a target domain of a different domain for the target UPN. For more information, see Rename Objects During Migration.

oldname, *newsamname*, *newupnname@targetdomain.com*, **"CN=***New Name*"

Note

You can also rename objects during migration by using an include file. For more information about how to use an include file, see Rename Objects During Migration.

Use an Option File

You can use option files to specify one or more parameters for migration tasks. An option file eliminates the need to provide parameters each time that you run a task from the command line.

You have two options to create an option file. You can:

- Create a single option file that contains sections for each type of migration task.
- Create separate option files with unique settings for each type of migration task.

The Migration section in the option file specifies parameters that apply to all tasks. Subsequent sections specify parameters that are task specific.

Use the following option file as a reference to customize the option file for your migration.

[Migration]

IntraForest=No

SourceDomain=*SourceDomainName*

SourceOu=*SourceOuPath*

TargetDomain=*TargetDomainName*

TargetOu=*TargetOuPath*

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
UpdatePreviouslyMigratedObjects=No
FixGroupMembership=Yes
UpdateGroupRights=No
MigrateMembers=No
DisableOption=EnableTarget
SourceExpiration=None
TranslateRoamingProfile=No
MigrateServiceAccounts=No

[Security]
TranslationOption=Add
TranslateFilesAndFolders=No
TranslateLocalGroups=No
TranslatePrinters=No
TranslateRegistry=No
TranslateShares=No
TranslateUserProfiles=No
TranslateUserRights=No

SidMappingFile=*SidMappingFile*

You can comment out options by a adding a semicolon at the beginning of a line.

Note

When a parameter is not specified, the default setting is used.

Troubleshooting ADMT

To troubleshoot your migration process, follow these troubleshooting recommendations:

- Troubleshooting User Migration Issues
- Troubleshooting Group Migration Issues
- Troubleshooting Service Account Migration Issues
- Troubleshooting Computer Migration Issues
- Troubleshooting Password Migration Issues
- Troubleshooting Security Translation Issues
- Troubleshooting Intraforest Migration Issues
- Troubleshooting ADMT Log File Issues
- Troubleshooting ADMT Command-Line Issues
- Troubleshooting Agent Operations

Troubleshooting User Migration Issues

This topic describes known issues related to migrating users with this version of the Active Directory Migration Tool (ADMT version 3.1 (v3.1)).

Special characters are replaced when account names are migrated

ADMT replaces the following characters with an underscore character "_" in the pre–Windows 2000 name Security Accounts Manager (SAM) account name and user principal name (UPN):

"*+,/:;<=>?[\]|

The period character "." is replaced with an underscore character "_" if it is the last character of a name.

Group membership of target accounts is updated after subsequent user migrations

When you migrate a user who has been previously migrated, the **Migrate associated user groups** option in the User Account Migration Wizard updates the group membership of the migrated account. During subsequent user migrations, any new groups that the source user account is a member of are appended to the group membership of the user in the target account.

Example: Bob is a user in the domain HB-ACCT-WC. He is a member of the group HB-ACCT-WC \Writers and he is migrated, along with the Writers group, to the target domain hay-buv.tld (NetBIOS name HAY-BUV). After the first migration, Bob is a member of HAY-BUV\Writers. Bob is also added to the following groups in the source domain after this first migration:

1. HB-ACCT-WC\Bob is added to the group HB-ACCT-WC\Editors.
2. HAY-BUV\Bob is added to HAY-BUV\TechEditors.

When HB-ACCT-WC\Bob is migrated again to fix his group accounts, HAY-BUV\Bob will be a member of HAY-BUV\Writers, HAY-BUV\Editors, and HAY-BUV\TechEditors.

To reset the account to only the groups of the source user, you must delete the target account and then repeat the migration of the source account.

It is also possible to remigrate groups with the **Remove existing members** option.

Permissions on a user that is migrated from an Active Directory domain are reset to default values during migration

When you migrate a user from one Active Directory domain to another, the User Account Migration Wizard creates a new security descriptor on migrated user objects by using settings from the target domain. The **Security** tab is only visible if you select **View\Advanced Features**.

This is by design, because the target domain, not the source domain, dictates security settings on the migrated user account.

Incorrect error message is displayed during user group fix-up if a user account is deleted

After a migration, if you delete a user account in the target domain and a group that contained the user account in the source domain (as a member of another group), is migrated between the same domains, ADMT logs the following wrong error message:

```
<account> has not been migrated to the target domain.
```

If you receive this error message, remigrate the user account to the target domain.

Exclusion of the useraccountcontrol property is ignored

The user property **userAccountControl** is always copied when you migrate from Windows NT 4.0 domains. Even if you choose to exclude this property on the **Object Property Exclusion** wizard page, the exclusion is ignored and the property is migrated.

However, when you migrate from Active Directory domains, the exclusion of this property is honored and it is not be copied during user migration.

The Remove existing user rights option did not work

Cause: If the Group Policy template that is associated with a user whose user rights are being removed contains the non-domain-qualified name of the user (for example, if it contains User1 instead of DomainA\User1), the remove operation fails.

Solution: Correct the user name entry in the Group Policy template.

Troubleshooting Group Migration Issues

This topic describes known issues related to migrating groups with this version of the Active Directory Migration Tool (ADMT version 3.1 (v3.1)).

Local group contains both source and target accounts when that account is migrated after you migrate the local group

When you migrate a member of a previously migrated local group, the source account for that member is not removed when the target member is added. If the member is migrated before you migrate the local group, only the target account member is added.

This is by design and applies to interforest migrations only.

Group member list is not updated for a group that includes a migrated group from a third domain

If you migrate a group, any groups in a third domain that include that original group as a member still refer to the group in the source domain. When you perform an intraforest migration, group members retain access to resources because the security identifier (SID) history is migrated automatically. When you perform an interforest migration, group membership must be fixed unless SID history is migrated.

Use the group migration wizard to migrate users that belong to nested groups

If **Migrate associated user groups** is selected, the User Account Migration Wizard only migrates the groups that the user is directly a member of. It does not migrate groups that the user is a member of through group nesting.

When you migrate groups by using the Group Account Migration Wizard, if **Copy group members** is selected, the wizard recursively migrates all users and groups that are members of that group, including groups that are members through group nesting.

Where the source domain is running Windows 2000 or Windows Server 2003, with group nesting, we recommend that you migrate the objects that are affected by using the Group Account Migration Wizard, if you want to preserve group membership that is gained through such nesting.

Troubleshooting Service Account Migration Issues

This topic describes known issues related to migrating service accounts with this version of the Active Directory Migration Tool (ADMT version 3.1 (v3.1)).

You must have the appropriate rights to update a service account on a remote computer when you migrate an account

The user account that is running ADMT must have **Logon Locally** rights to any remote computer to which the tool dispatches an agent. This also applies to any remote computer whose Service Control Manager (SCM) is modified while a service account is migrated with the User Account Migration Wizard. If this account does not have the right to change the SCM, the service account

is still migrated to the target domain, but the service on the remote computer is not updated to use the target domain account. To update the service on the remote computer, run the Service Account Migration Wizard and select **No, use the previously collected information** on the **Update Information** page. Because the user's lack of access is not always flagged as an error in **Migration Progress**, it is a good practice to check the migration log file for any errors after you migrate service accounts.

Services must be identified on all computers before service accounts are migrated

If you identify services on servers using the Service Account Migration Wizard after user migration has taken place, the configuration of these services with the migrated account and password information will fail. To configure these services you have to rerun the user migration.

Service account migration on Windows Server 2008 and Windows Vista takes longer than expected

If you are running service account migration at a computer that is running Windows Server 2008 or Windows Vista and it is taking much longer than expected, you might increase performance by enabling a Windows Firewall exception for Remote Service Management on the computer that is being used. For more information, see the following procedure.

To add a Windows Firewall exception for Remote Service Management

1. Open **Control Panel** (Classic View), and then open **Windows Firewall**.
2. Click the **Exceptions** tab.
3. Make sure that the **Remote Service Management** check box is selected.
4. Click **OK**.

Troubleshooting Computer Migration Issues

This topic describes known issues related to migrating computers with this version of the Active Directory Migration Tool (ADMT version 3.1 (v3.1)).

Intraforest computer migration does not disable the computer account in the source domain

After an intraforest computer migration, the migrated computer account in the source domain is neither disabled nor deleted. This is by design.

To disable or delete the accounts of migrated computers in the source domain, write a simple Active Directory Service Interfaces (ADSI) script.

Computer account is created even if migration fails

If a computer migration fails as the result of an agent-related error, the computer account that is created for the computer in the target domain is not deleted.

Note

If you select **Migrate and merge conflicting objects** on the **Conflict Management** page of the Computer Account Migration Wizard, you do not have to delete the computer account that was created in the target domain before you attempt to migrate the computer again.

Migrate computers before any groups in an intraforest migration

When you perform an intraforest migration, if you have any computers that are members of groups (other than the Domain Computers group), you must migrate those computers before you migrate the groups to which they belong. This is a condition for intraforest migrations, and it prevents those computers from losing their group membership.

Intermittent failure of ADMT remote agent service

If a failure occurs when you deploy the ADMT remote agent service on a remote computer as part of a computer migration, security translation, service account identification, or account reference report, it is possible that the agent might fail to stop or uninstall itself. If this occurs, you receive the message “An instance of the agent is already running” with each subsequent agent deployment until either the ADMT agent process is closed or the remote computer is rebooted.

Computer migration may fail if a computer account with the same NetBios name already exists in the target domain

When you migrate a computer back and forth between two domains, the agent dispatch might fail if a computer account with the same NetBIOS name as the computer that is being migrated from the source domain already exists in the target domain.

ADMT could not change the domain affiliation of a particular computer. This failure caused the computer to lose affiliation with any domain.

Cause: This can be caused by an incorrect migration environment configuration or some malfunction with either the source computer or target computer.

Solution: Join the computer to a domain and create the computer account in the domain as described in the following procedures:

To change the domain membership of a computer that is running Windows 2000 or Windows Server 2003

1. Log on to the computer that is using an account with local administrator credentials.
2. On the desktop, right-click **My Computer**, and then click **Properties**.
3. On the **Computer Name** tab, click **Change**.
4. In **Computer Name Changes**, select **Domain:**, and then type the name of the domain that you want the computer to join.

Notes

- To join a domain, you must enter credentials of an account with administrative permissions on the domain that you want the computer to join. You must restart the computer to complete the joining of the computer to the domain.

Troubleshooting Password Migration Issues

This topic describes a known issue related to migrating passwords with this version of the Active Directory Migration Tool (ADMT version 3.1 (v3.1)).

Migrated passwords may not conform to the password policy of the target domain

Password migration in ADMT bypasses password policy checks. If a password policy is set, it is not enforced until the password is changed. For this reason, ADMT always requires migrated users to change their passwords the next time that they log on.

After an interforest migration, users cannot log on to their new domain.

Cause: When you perform an interforest migration, ADMT always sets the **User Must Change Password** option for migrated users. If the user account has the **User Cannot Change Password** option set, the target account cannot log on until one or both options have been changed.

Solution: Change the options by using one of the following procedures:

To enable the ability to change the user password

1. In Active Directory Users and Computers, on the **View** menu, click **Advanced Features**.
2. Right-click the user, and then click **Properties**.
3. On the **Security** tab, allow the **Change Password** permission for **Everyone** and for the user.

To remove the User Must Change Password flag

- In Active Directory Users and Computers, right-click the user, and then click **Reset Password**.

After an intraforest migration, users cannot log on to their new domain.

Cause: The user account passwords that were used in the old domain might violate the password restrictions in the new domain.

In an intraforest migration, user account passwords from the source domain are migrated to the target domain. If the source domain user accounts have passwords that violate password restrictions (such as minimum length) in the target domain, the affected migrated users cannot log on until their password has been set to a value that fits the target domain password policy.

If the users try to use the invalid passwords, their new user accounts might be locked. If you selected the Disable target accounts option in the User Account Migration Wizard, the new user accounts are disabled. As a result, the migrated users might not be able to log on until their accounts have been unlocked or marked as enabled.

Solution: Reset the user account passwords to a value that fits the new domain's password policy, and enable the user accounts if they were disabled as a result of repeated password failure.

Migrated users receive an error indicating that their user name or password is incorrect.

Cause: Migrated users cannot log on because of password policy, even though password policies appear to be disabled.

During a migration, some administrators may choose to disable their password policies on the target domain. If they try to accomplish this by turning off the minimum password length policy without setting the policy to zero, it is possible that the users cannot log on because a password policy is still in effect.

Solution: Set the minimum password length policy to zero. After the zero length policy is in effect, the minimum password length policy can be turned off.

Troubleshooting Security Translation Issues

This topic describes a known issue related to security translation using this version of the Active Directory Migration Tool (ADMT version 3.1 (v3.1)).

Security translation does not affect the Outlook profile

When you select **User Profiles** on the Translate Objects page of the Security Translation Wizard, security is not translated on Outlook profiles. To fix Outlook profiles for migrated accounts, use the Exchange Server Migration Wizard. The Exchange Server Migration Wizard ships with and is installed with Exchange Server 2003.

Security translation on native registry keys is not available when you are running 64-bit versions before Windows Vista

This is a known issue that occurs because of inconsistencies in how the Windows-on-Windows 64-bit (WoW64) subsystem handles registry redirection differently in Windows Vista and earlier versions of the Microsoft Windows operating system. This issue does not affect running security translation on native registry locations for 64-bit versions of Windows Vista or Windows Server 2008.

After migration, new user accounts in the target domain cannot access resources where the source domain accounts have permissions.

Cause: The settings that are necessary to run ADMT have not been correctly established.

Most migration problems are caused by an incorrectly configured migration environment.

Solution: Open the migration log file, and find the account that you migrated with the security identifier (SID) history. If SID history was added to the account, you should see an entry similar to the following:

2005-10-06 18:28:50-SID for *UserAccountName* added to the SID history of *UserAccountName*

If you receive an error message, it is almost certain that you have not configured the environment correctly, and you should review the configuration topics before you try the migration again.

SID history migration is not working.

Cause: There are a number of conditions that must be satisfied for SID history migration to work.

Solution: Configure the migration environment correctly before you run ADMT, and review the configuration topics before you proceed with the migration.

Note

When you migrate a previously migrated security principal to a new domain, the criteria for migrating SID history should be in place for all three domains.

For example, say that you have the following three domains: DomainA, DomainB, and DomainC. DomainA is a Windows NT 4.0 domain. DomainB and DomainC are Windows 2000 domains operating in native mode. User1 in DomainA (DomainA\User1) is migrated to DomainB as DomainB\User1 and SID history is translated. DomainB\User1 now has the primary SID for DomainB\User1 and the SID history value for DomainA\User1. If an administrator wants to migrate DomainB\User1 to DomainC\User1 and preserve all of DomainB\User1's SIDs, the proper configuration settings must be in place to allow migration from DomainA to DomainC and from DomainB to DomainC. If DomainA has been decommissioned, or if proper configuration cannot be satisfied between DomainA and DomainC, ADMT migrates the SID for DomainB\User1 to DomainC\User1 and logs the fact that it could not migrate the DomainA\User1 SID.

If DomainA does not exist, ADMT writes an error message to the log, but migration still succeeds. You can ignore this error message.

Permissions on a resource show "Account Unknown" for a migrated group or user.

Cause: When you migrate a group or user account, and domain controllers in the source domain are no longer available, computers in domains outside the target forest that are running Windows NT 4.0 or Windows 2000 (in a domain operating in mixed mode) might not be able to resolve the group or user object's SID history with the target domain's global catalog.

As long as the source domain is accessible, the group or user account name can be resolved. The inability to resolve the account name is an administrative problem only. The inability to resolve the group or user account name through SID history does not prevent that account from having the desired access to that resource. For example, if a user shows up as "Account

Unknown" in a group's membership list, that user is still a member of that group and has the rights associated with that group.

Solution: You can fix this SID history resolution problem by running the Security Translation Wizard to replace the source account SID with the new target account SID for all resources on all affected computers. This problem is much more prevalent if you decommission the source account domain before you migrate the source resource domain. Therefore, you should decommission all source domains together as the last step in the migration process.

After migration, new user accounts in the target domain cannot access resources where the source domain accounts have permissions.

Cause: The settings that are necessary to run ADMT have not been correctly established.

Most migration problems are caused by an incorrectly configured migration environment.

Solution: Open the migration log file, and find the account that you migrated with SID history. If SID history was added to the account, you should see an entry similar to the following:

2005-10-06 18:28:50-SID for *UserAccountName* added to the SID history of *UserAccountName*

If you receive an error message, it is almost certain that you have not configured the environment correctly, and you should review the configuration topics before you try the migration again.

I am receiving the following error: "The Recycle Bin on C:\ is corrupt or invalid. Do you want to empty the Recycle Bin for this drive?"

Cause: This is by design. For security reasons, each user who logs on to a Windows 2000 or Windows Server 2003 computer receives their own, user-specific Recycle Bin. The access control list (ACL) for each instance of the Recycle Bin can contain only one user-specific SID. When you migrate a user's profile using the **Add** option, the SID of the source domain user is added to the SID history of the Recycle Bin. This places two user-specific SIDs in the Recycle Bin's ACL. This problem does not occur if you migrate the profiles by using the **Replace** option.

Solution: On the error message, click **Yes**, and the Recycle Bin is emptied without a problem. If you click **No**, the error continues to appear until you empty the Recycle Bin.

Users in domains that are not trusted cannot access Distributed File System (DFS) shares in Active Directory domains.

Cause: This is by design.

Solution: If you plan to use DFS shares in your domain, migrate the computers that belong to users who access DFS shares first or migrate the computers and users in the same migration session.

SID history does not work for migrated Exchange service accounts.

Cause: ADMT correctly migrates the Exchange service accounts, but there is a special manual process for updating Exchange service accounts that must be completed while you run Exchange. Failure to follow this process could result in system failure or data loss on the Exchange system.

Solution: To review walkthrough material, scenarios, and other information about how to perform a domain migration, see Domain Upgrades & Active Directory at the Microsoft Web site (http://www.microsoft.com/). You can also contact Microsoft Product Support Services for details about how to change the service account that is used by Exchange services in a site.

Troubleshooting Intraforest Migration Issues

This topic describes known issues related to intraforest migrations using this version of the Active Directory Migration Tool (ADMT version 3.1 (v3.1)).

Domain-wide user and group rights are not migrated to the target domain

When you check **User Rights** in the User and Group Account Migration Wizards, you migrate only the local rights on the source domain controller. Domain-wide rights are not migrated.

Global Group migration and mixed mode source domains

When global groups are migrated between a mixed mode source domain and a native mode target domain and the groups are not empty, ADMT creates copies of the global groups in the target domain and does not add the security identifier (SID) of the source domain's global group to the SID history attribute. This is by design.

In this situation, ADMT cannot convert the global group to a universal group because mixed mode domains do not recognize universal groups and cannot add them to the access token of the user. Therefore, the users would lose access to resources.

Important

We strongly recommend that you migrate users and groups between native mode domains only.

Global Groups are copied without SID history for intraforest migrations if they are not migrated with group members and the source domain is in mixed mode

When you migrate a global group in a mixed mode domain for an intraforest migration by using the Group Account Migration Wizard, if you do not select the Copy Group Members option, that global group is copied—not migrated—without SID history, instead of being moved. This behavior is a result of the rules of global group membership.

If ADMT moves, rather than copies, the global group, the group members are "orphaned" from the group and lose any resource access that is granted through membership of the group because global groups cannot contain members from other domains.

When that global group's members are later migrated, the group membership is restored. However, because SID history is not migrated with the group, you must run the Security Translation Wizard to update the access control lists (ACLs), just as you would do in an interforest migration without SID history.

Important

We strongly recommend that you migrate users and groups only between native mode domains only.

Migrated objects table does not sync

If the administrator in the target domain deletes a migrated group after the migration, the entries for the migrated group are not removed from the migrated object table. If a group with the same name as the group that is deleted in the target domain is migrated from the source domain, an error can occur. This error occurs only if users are migrated with the group. The error message is as follows:

```
ERR2:7422 Failed to move object <object_RDN>, hr=80070057 The parameter is incorrect.
```

Troubleshooting ADMT Log File Issues

This section describes a known issue related to the Active Directory Migration Tool (ADMT) log files that occur with this version of ADMT (ADMT version 3 (v3.1).

I cannot find the ADMT log files.

Solution: All the ADMT log files are stored in the ADMT database. However, the last 20 migration logs are also stored in the Logs folder under the ADMT folder on the computer on which ADMT is installed. You can access all ADMT logs in the database by using the **admt task** command at a command line.

I cannot read the event log entries for the ADMT agent.

Cause: You are not on a computer on which ADMT has been installed.

Solution: The agent may write event log entries to the computer on which it runs. However, the agent software is removed when the agent's task is finished. You can view the event log entries on the computer to which the agent was dispatched by running Event Viewer from the computer on which ADMT is installed.

I need more information from the ADMT logs.

Cause: Incorrect logging level setting.

By default, ADMT writes summary information to its log files. You can increase the level of detail by changing the registry entry that controls the logging level.

Solution: On the computer on which ADMT is installed, set the value of the **HKEY_LOCAL_MACHINE\Software\Microsoft\ADMT\TranslationLogLevel** registry key to 7.

You can use verbose logging mode for problem diagnosis and troubleshooting. Verbose logging mode can create very large log files, particularly in cases where large numbers of files, or other objects whose access control lists (ACLs) must be updated, exist on the target computer. Because the agent logs are written to the folder that is specified by the %TEMP% environment variable, the volume to which that environment variable points should have ample disk space. When you log in with verbose mode, you may have to change the value of the %TEMP% environment variable before you dispatch an agent.

Generated reports do not show up in the ADMT.

Cause: When ADMT generates reports, it does not update the console automatically.

Solution: To view the reports, close and then reopen ADMT.

Running multiple instances of ADMT in multiple languages

When you run multiple instances of ADMT where different instances are using different languages, the log files are generated in the language that the instance is being run in. This does not affect the functionality of ADMT in any way. However, we recommend that you use a unified language when you run multiple instances of ADMT.

Troubleshooting ADMT Command-Line Issues

Note that the command-line tool uses the scripting component, and, therefore, scripting issues are also applicable to the command-line tool.

Windows NT 4.0 user migration from a command line

All the Active Directory Migration Tool (ADMT) migration operations can be performed by using a command-line or script with ADMT installed on a Windows Server 2003 member server, except for user migrations from a Windows NT 4.0 source domain with the security identifier (SID) history. However, all migration operations work when you perform them from the user interface (UI).

Duplicate command-line parameters override any previous occurrences

If a command-line parameter is specified more the once, the last value overrides the previous value. This is by design.

Extended characters are not displayed by command-line interface

The ADMT command-line interface does not convert Unicode. Therefore, extended characters such as the German "umlaut" do not display correctly.

Enable source account option not disabled in intraforest migrations

When you perform intraforest migrations, accounts are moved and not copied between domains. The source account is removed as part of the move. However, the option to enable a source account is available through the ADMT command-line interface. When you use this option, you will receive the following warning:

```
WRN1:  7362: <object_name> - Could not enable source account.  The parameter is wrong
```

Troubleshooting Agent Operations

I am receiving an error message that the Active Directory Migration Tool (ADMT) could not verify auditing and TcpipClientSupport on domains

Cause: The agent is dispatched with invalid credentials or the migration environment is not configured correctly.

Solution: An agent is dispatched to a remote computer that uses the credentials of the account that is used to run ADMT. After the agent is installed on the remote computer, it runs under the Local System account. The credentials that you provide to the wizard, before the agent is dispatched to the remote computer, are used to write results back to a share that is created on the computer on which ADMT is running. The agent must have the right to log on locally to the remote computer, and, if the agent is used to migrate computers, it must have administrative rights in the source domain and be a local administrator on all workstations.

To ensure that you have the correct credentials, create trusts so that the source and target domain trust each other. Add the Domain Admins group of the target domain (target\Domain Admins) to the built-in Administrators group of the source domain (source\Administrators). Log on by using the target\Domain Admins account, and supply a set of credentials for the source\Administrators account when you are prompted. This provides you with administrative permissions on both the source domain and target domain.

Agent dispatch operations fail with credentials conflict errors

Cause: You have an active connection, such as a mapped drive or a printer, to a computer on which an agent is being installed. The dispatch operation fails because the credentials of the agent installation conflict with the existing set of credentials.

Solution: Remove any active connections between the computer that is running ADMT and the computer to which the agent is being dispatched.

When I try to view the results of a remote agent operation, I receive the following error: "Cannot open the \\ComputerName\(%SystemRoot%)$\temp\dctlog.txt file."

Cause: The default administrative share for the system volume of the computer to which the agent was dispatched is not enabled.

Because the default share is not enabled, ADMT cannot read the log file.

Solution: Re-enable the default share of the system volume.

When generating reports, I receive IDispatch error 3107

Cause: This error may occur when the Agent Monitor is closed before all agents have finished writing their results back to the ADMT reporting database.

Solution: To prevent this problem, wait until all agents have completed their tasks before closing the Agent Monitor.

I need to know which protocols and ports ADMT uses to establish console communication with domain controllers and ADMT agents running on workstations

Cause: When you run ADMT in environments that have a firewall, you might have to make firewall port exceptions to support ADMT-related traffic on your network.

Solution: The ADMT console uses Lightweight Directory Access Protocol (LDAP) port 389 to communicate with domain controllers and Remote Procedure Call (RPC) to communicate with ADMT agents. For RPC communication, any available RPC port in the range between 1024 and 5000 might be used. For more information, see 836429 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=122010).

Why are files that ADMT generates for agent deployment not removed after use?

Files that are generated on client computers where the ADMT agent service was run for security translation of local groups are placed in the following locations:

- %windir%\onepointdomainagent (ADMT v3.0 and v3.1)
- %programfiles%\onepointdomainagent (ADMT v2.0)

Files at this location can remain after reboot for the following reasons:

- If the computer still has ADMT installed.
- If after you remove ADMT from the computer, you do not perform registry cleanup to remove any entries from the **HKLM\Software\Microsoft\ADMT** path.
- If you reboot the computer without waiting for ADMT agent processes to exit or complete. To verify that ADMT processes have been exited, you can use Task Manager to verify that ADMTAgnt.exe and DctAgentServices.exe are no longer listed on the **Processes** tab. If either of these processes is listed, use Task Manager to end them first before you perform a reboot.

Additional Resources

These resources contain additional information, tools, and job aids that are related to this guide.

Related information

- Designing and Deploying Directory and Security Services (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

- Article 295758 in the Microsoft Knowledge Base (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 for your own migration.