

---

# Module 3: Managing Groups

## Contents

Overview	1
Lesson: Creating Groups	2
Lesson: Managing Group Membership	19
Lesson: Strategies for Using Groups	26
Lesson: Modifying Groups	37
Lesson: Using Default Groups	47
Best Practices for Managing Groups	60
Lab A: Creating and Managing Groups	61



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, IntelliMirror, MSDN, PowerPoint, Visual Basic, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Overview

- 
- Creating Groups
  - Managing Group Membership
  - Strategies for Using Groups
  - Modifying Groups
  - Using Default Groups
  - Best Practices for Managing Groups

## Introduction

A group is a collection of user accounts. You can use groups to efficiently manage access to domain resources, which helps simplify network maintenance and administration. You can use groups separately, or you can place one group within another to further simplify administration.

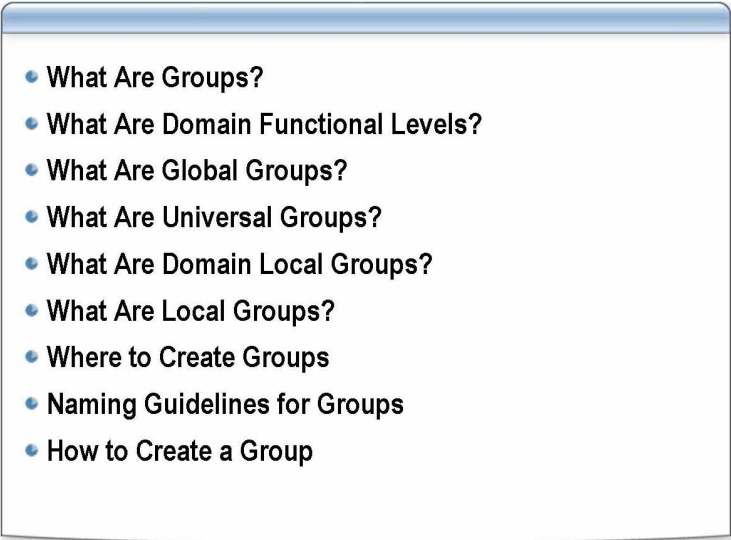
Before you can effectively use groups, you must understand the function of groups and the types of groups that you can create. The Active Directory® directory service supports different types of groups and also provides options to determine the group's scope, which is how the group can be used in multiple domains.

## Objectives

After completing this module, you will be able to:

- Create groups.
- Manage group membership.
- Apply strategies for using groups.
- Modify groups.
- Manage default groups.

# Lesson: Creating Groups

- 
- What Are Groups?
  - What Are Domain Functional Levels?
  - What Are Global Groups?
  - What Are Universal Groups?
  - What Are Domain Local Groups?
  - What Are Local Groups?
  - Where to Create Groups
  - Naming Guidelines for Groups
  - How to Create a Group

---

## Introduction

The information in this lesson presents the skills and knowledge that you need to create groups.


## Lesson objectives

After completing this lesson, you will be able to:

- Explain the purpose of groups, group types, and group scopes.
- Identify the domain functional levels.
- Describe global groups.
- Describe universal groups.
- Describe domain local groups.
- Describe local groups.
- Decide whether to create groups in a domain or organizational unit.
- Determine naming guidelines for groups.
- Create a group.

## What Are Groups?

**Groups simplify administration by enabling you to assign permissions for resources**



**Groups are characterized by scope and type**

- The group scope determines whether the group spans multiple domains or is limited to a single domain
- The three group scopes are global, domain local, and universal

Group Type	Description
Security	Used to assign user rights and permissions Can be used as an e-mail distribution list
Distribution	Can be used only with e-mail applications Cannot be used to assign permissions

### Definition

Groups are a collection of user and computer accounts that you can manage as a single unit. Groups:

- Simplify administration by enabling you to grant permissions for resources, once to a group rather than to each user account individually.
- Can be based on Active Directory or local to an individual computer.
- Are characterized by scope and type.
- Can be nested, which means that you can add a group to another group.

### Group scopes

The group scope determines whether the group spans multiple domains or is limited to a single domain. Group scopes enable you to use groups to grant permissions. The group scope determines:

- The domains from which you can add members to the group.
- The domains in which you can use the group to grant permissions.
- The domains in which you can nest the group within other groups.

The group scope determines who the members of the group are. Membership rules govern the members that a group can contain and the groups of which a group can be a member. Group members consist of user accounts and other groups.

To assign the correct members to groups and to use nesting, it is important to understand the characteristics of the group scope. There are the following group scopes:

- Global
- Domain local
- Universal

**Group types**

You use groups to organize user accounts, computer accounts, and other group accounts into manageable units. Working with groups instead of individual users helps simplify network maintenance and administration. There are the following types of groups in Active Directory:

- **Security groups**

You use security groups to assign user rights and permissions to groups of users and computers. Rights determine what members of a security group can do in a domain or forest, and permissions determine what resources a member of a group can access on the network.

You can also use security groups to send e-mail messages to multiple users. Sending an e-mail message to the group sends the message to all members of the group. Therefore, security groups have the capabilities of distribution groups.

- **Distribution groups**

You use distribution groups with e-mail applications, such as Microsoft® Exchange, to send e-mail messages to collections of users. The primary purpose of this type of group is to gather related objects, not to grant permissions.

Distribution groups are not security-enabled, meaning that they cannot be used to assign permissions. If you need a group for controlling access to shared resources, create a security group.

Even though security groups have all the capabilities of distribution groups, distribution groups are still required, because some applications can use only distribution groups.

Both distribution and security groups support one of the three group scopes.

## What Are Domain Functional Levels?

	Windows 2000 mixed (default)	Windows 2000 native	Windows Server 2003
Domain controllers Supported	Windows NT® Server 4.0, Windows 2000, Windows Server 2003	Windows 2000, Windows Server 2003	Windows Server 2003
Group scopes supported	Global, domain local	Global, domain local, universal	Global, domain local, universal

---

### Definition

The characteristics of groups in Active Directory depend on the domain functional level. Domain functionality enables features that will affect the entire domain and that domain only. Three domain functional levels are available: Microsoft Windows® 2000 mixed, Windows 2000 native, and Microsoft Windows Server 2003. By default, domains operate at the Windows 2000 mixed functional level. You can raise the domain functional level to either Windows 2000 native or Windows Server 2003.

The table above lists the domain functional levels and the domain controllers and group scopes they each support.

---

**Note** You can convert a group from a security group to a distribution group, and vice versa, at any time, but only if the domain functional level is set to Windows 2000 native or higher.


---

### Additional Reading

For more information on raising functional levels see KB Article How To: Raise the Domain Functional Level in Windows Server 2003.

## What Are Global Groups?

Global group rules	
Members	<ul style="list-style-type: none"> <li>• <b>Mixed mode:</b> User accounts from same domain</li> <li>• <b>Native mode:</b> User accounts and global groups from same domain</li> </ul>
Can be a member of	<ul style="list-style-type: none"> <li>• <b>Mixed mode:</b> Domain local groups</li> <li>• <b>Native mode:</b> Universal and domain local groups in any domain and global groups in the same domain</li> </ul>
Scope	Visible in its own domain and all trusted domains
Permissions	All domains in the forest



### Definition

A global group is a security or distribution group that can contain users, groups, and computers that are from the same domain as the global group. You can use global security groups to assign user rights and permissions to resources in any domain in the forest.

### Characteristics of global groups

The following summarizes the characteristics of global groups:

- **Members**
  - In domain mixed functional level, global groups can contain user and computer accounts that are from the same domain as the global group.
  - In native functional level, global groups can contain user accounts and global groups that are from the same domain as the global group.
- **Can be a member of**
  - In mixed mode, a global group can be a member of only domain local groups.
  - In native mode, a global group can be a member of universal and domain local groups in any domain and global groups that are from the same domain as the global group.
- **Scope**

A global group is visible within its domain and all trusted domains, which include all of the domains in the forest.
- **Permissions**

You can grant permissions to a global group for all domains in the forest.


### When to use global groups

Because global groups have a forest-wide visibility, do not create them for domain-specific resource access. Use a global group to organize users who share the same job tasks and have similar network access requirements. A different group type is more appropriate for controlling access to resources within a domain.



## What Are Universal Groups?

Universal group rules	
Members	<ul style="list-style-type: none"> <li>• <b>Mixed mode:</b> Not applicable</li> <li>• <b>Native mode:</b> User accounts, global groups, and other universal groups from any domain in the forest</li> </ul>
Can be a member of	<ul style="list-style-type: none"> <li>• <b>Mixed mode:</b> Not applicable</li> <li>• <b>Native mode:</b> Domain local and universal groups in any domain</li> </ul>
Scope	Visible in all domains in a forest
Permissions	All domains in a forest



### Definition

A universal group is a security or distribution group that can contain users, groups, and computers from any domain in its forest. You can use universal security groups to assign user rights and permissions to resources in any domain in the forest.

### Characteristics of universal groups

The following summarizes the characteristics of universal groups:

- **Members**
  - You cannot create universal groups in mixed mode.
  - In native mode, universal groups can contain user accounts, global groups, and other universal groups from any domain in the forest.
- **Can be a member of**
  - The universal group is not applicable in mixed mode.
  - In native mode, the universal group can be a member of domain local and universal groups in any domain.

#### ■ Scope

Universal groups are visible in all domains in the forest.

#### ■ Permissions


You can grant permissions to universal groups for all domains in the forest.

### When to use universal groups

Use universal groups to nest global groups so that you can assign permissions to related resources in multiple domains. A Windows Server 2003 domain must be in Windows 2000 native mode or higher to use universal groups.

## What Are Domain Local Groups?

Domain local group rules	
Members	<ul style="list-style-type: none"> <li>• <b>Mixed mode:</b> User accounts and global groups from any domain</li> <li>• <b>Native mode:</b> User accounts, global groups, and universal groups from any domain in the forest, and domain local groups from the same domain</li> </ul>
Can be a member of	<ul style="list-style-type: none"> <li>• <b>Mixed mode:</b> None</li> <li>• <b>Native mode:</b> Domain local groups in the same domain</li> </ul>
Scope	Visible only in its own domain
Permissions	Domain to which the domain local group belongs



### Definition

A domain local group is a security or distribution group that can contain universal groups, global groups, other domain local groups that are from its own domain, and accounts from any domain in the forest. You can use domain local security groups to assign user rights and permissions to resources only in the same domain where the domain local group is located.

### Characteristics of domain local groups

The following summarizes the characteristics of domain local groups:

- **Members**
  - In mixed mode, domain local groups can contain user accounts and global groups from any domain. Member servers cannot use domain local group in mixed mode.
  - In native mode, domain local groups can contain user accounts, global groups, and universal groups from any domain in the forest, and domain local groups that are from the same domain as the domain local group.
- **Can be a member of**
  - In mixed mode, a domain local group cannot be a member of any group.
  - In native mode, a domain local group can be a member of domain local groups that are from the same domain as the domain local group.
- **Scope**

A domain local group is visible only in the domain that the domain local group belongs to.
- **Permissions**


You can assign permissions to a domain local group for the domain that the domain local group belongs to.

### When to use domain local groups

Use a domain local group to assign permissions to resources that are located in the same domain as the domain local group. You can place all global groups that need to share the same resources into the appropriate domain local group.

## What Are Local Groups?

Local group rules	
Member	Local user accounts from the computer
Can be a member of	None



### Definition

A local group is a collection of user accounts or domain groups created on a member server or a stand-alone server. You can create local groups to grant permissions for resources residing on the local computer. Windows 2000 or Windows Server 2003 creates local groups in the local security database. Local groups can contain users, computers, global groups, universal groups, and other domain local groups.

Because groups with a domain local scope are sometimes referred to as local groups, it is important to distinguish between a local group and a group with domain local scope. Local groups are sometimes referred to as machine local groups to distinguish them from domain local groups.

### Characteristics of local groups

The following summarizes the characteristics of local groups:

- Local groups can contain local user accounts from the computer where you create the local group.
- Local groups cannot be members of any other group.

### When to use local groups

The following are guidelines for using local groups:

- You can use local groups only on the computer where you create the local groups. Local group permissions provide access to resources only on the computer where you created the local group.
- You can use local groups on computers running currently supported Microsoft client operating systems and member servers running Windows Server 2003. You cannot create local groups on domain controllers, because domain controllers cannot have a security database that is independent of the database in Active Directory.
- Create local groups to limit the ability of local users and groups to access network resources when you do not want to create domain groups.

## Where to Create Groups

- You can create groups in the root domain of the forest, any other domain in the forest, or an organizational unit
- Choose the domain or organizational unit where you create a group based on the administration requirements for the group
  - For example:  
If your directory has multiple organizational units, each of which has a different administrator, you can create global groups in those organizational units

---

### Introduction

In Active Directory, groups are created in domains. You use Active Directory Users and Computers to create groups. If you have the necessary permissions, and by correctly associating users and computers with groups, you can create groups in any other domain in the forest, or an organizational unit.

Besides the domain in which it is created, a group is also characterized by its scope. The scope of a group determines:

- The domain from which members can be added.
- The domain in which the user rights and permissions assigned to the group are valid.

### Choosing a domain or organizational unit

Choose the particular domain or organizational unit where you create a group based on the administration requirements for the group.

For example, suppose your directory has multiple organizational units, each of which has a different administrator. You may want to create global groups in those organizational units so that those administrators can manage group membership for users in their respective organizational units.

If groups are required to control access outside the organizational unit, you can nest the groups within the organizational unit into universal groups (or other groups with global scope) that can be used elsewhere in the forest. It may be more efficient to nest global groups if the domain functional level is set to Windows 2000 native or higher, the domain contains a hierarchy of organizational units, and administration is delegated to administrators at each organizational unit.

## Naming Guidelines for Groups

### For security groups:

- Incorporate the scope in the naming convention of the group name
- The name should reflect the ownership (division or team name)
- Place domain names or abbreviations at the beginning of the group name
- Use a descriptor to identify the maximum permissions a group can have, such as DL IT London OU Admins

### For distribution groups:

- Use a short alias name
- Do not include a user's alias name as part of a display name
- Allow a maximum of five co-owners of a single distribution group

### Introduction

In Active Directory, there are many security and distribution groups. The following naming conventions help you manage these groups. Organizations develop their own naming conventions for their security and distribution groups. A group name should identify the scope, type, who the group was created for, and what permissions the group can have.

### Security group

Consider the following in defining a naming convention for security groups:

#### ■ Scope of security groups

Although the group type and scope are displayed as the group type in Active Directory Users and Computers, organizations often incorporate the scope in the naming convention of the group name.

For example, Northwind Traders identifies the scope of security groups by adding a first letter to the group name:

- **G** IT Admins  
G for global groups
- **U** All IT Admins  
U for universal groups
- **DL** IT Admins Full Control  
DL for domain local groups

- Ownership of the security group

The name for any domain-level security group, whether universal, global, or domain local, should clearly identify ownership by including the name of the division or team that owns the group.

The following is an example of a naming convention that Northwind Traders might use to identify group ownership:

- G **Marketing** Managers
- DL **IT Admins** Full Control

- Domain name

Upon client request, the domain name or abbreviation is placed at the beginning of the group name. For example:

- G **NWTraders** Marketing
- DL **S.N.MSFT** IT Admins Read

- Purpose of the security group

Finally, in a name, you can include the business purpose of the group and maximum permissions the group should ever have on the network. This naming convention is more applicable to domain local or local groups.

The following is an example of a naming convention that Northwind Traders might use to identify the purpose of the security group. Northwind Traders uses a descriptor to identify the maximum permissions a group should ever have on the network. For example:

- DL IT London **OU Admins**
- DL IT Admins **Full Control**

## Distribution groups

Because security groups are mostly used for network administration, only the personnel administering the network must use the naming convention. End users use distribution groups, so the naming convention must be relevant to an end user.

When defining a naming convention for distribution groups consider the following:

- E-mail names

- *Length.* Use a short alias name. To conform to current downstream data standards, the minimum length of this field is three characters, and the maximum length is eight characters.
- *Offensive words.* Do not create distribution groups with words that may be considered offensive. If in doubt, do not use the word.
- *Allowed characters.* You can use all ASCII characters. The only allowed special characters are the hyphen (-) and underscore (\_).
- *Special designations.* Do not use the following character combinations for distributions groups:
  - An underscore (\_) as the beginning character of the group name or the alias name
  - A first name or combination of first name and last name that may easily be confused with a user account name

### ■ Display names

- *User alias names.* For standardization purposes, do not include a user's alias name as part of a display name (for example, Sfine Direct Reports). Include the full name (for example, Suzan Fine's Direct Reports).
- *Offensive words.* Do not create distribution groups with words that may be considered offensive.
- *Social discussions.* Distribution groups for social discussions should not be allowed, because public folders are a more efficient means of transmitting and storing high-volume communications associated with social discussions. Because a post is visible to multiple users, both network traffic and data storage are minimized if you use public folders instead of corporate distribution groups.
- *Length.* The maximum length of this field is 40 characters. Abbreviations are acceptable as long as the meaning is clear.
- *Style.* Do not capitalize the entire description, but capitalize the first letter in the display name. Use proper punctuation and spelling.
- *Top of the address book.* Do not use the word *A*, numbers, special characters (especially quotes), or a space to begin a description. This makes it appear at the top of the address book. The address book should begin with individual user names starting with *A*.
- *Special characters.* Slashes (/) are acceptable in display names, but do not use them in front of server names. Do not use more than one apostrophe (') and do not use the following special characters: " \* @ # \$ % | [ ] ; < > =

### ■ Ownership

There can be a maximum of five co-owners of a single distribution group.

### Local groups

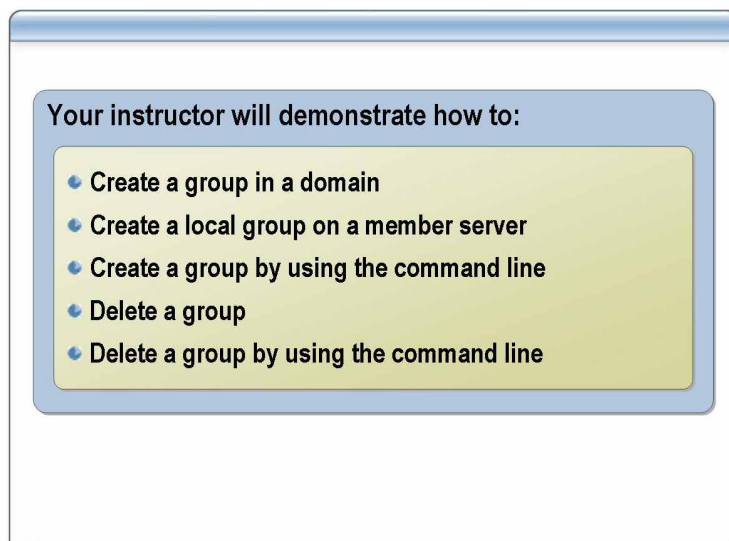
A local group name cannot be identical to any other group or user name on the local computer being administered. A local group name cannot consist solely of periods (.) or spaces. It can contain up to 256 uppercase or lowercase characters, except the following: " /\ [ ] : ; | = , + \* ? < >

---

**Note** Your environment may not use these guidelines but will most likely use some group naming conventions.

---

## How to Create a Group



---

### Introduction

In most corporate environments, you will create groups in domains. Active Directory has security and tracking features that limit the addition of users to groups. Active Directory also gives corporations the flexibility to use groups on member servers. Corporations often have servers that are exposed to the Internet and want to use local groups on member servers rather than domain local groups to limit the exposure of internal groups and group members.

### Procedure for creating a group in a domain

To create a group in an Active Directory domain:

1. In Active Directory Users and Computers, in the console tree, right-click the folder to which you want to add the group, point to **New**, and then click **Group**.
2. In the **New Object – Group** dialog box, in the **Group name** box, type the name of the new group.
3. Under **Group scope**, click the group scope for the new group.
4. Under **Group type**, click the group type for the new group.

---

**Note** To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or the Enterprise Admins group in Active Directory, or you must be delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.

---

---

**Important** If the domain in which you are creating the group is set to the domain functional level of Windows 2000 mixed, you can select only security groups with domain local or global scope.

---



Procedure for creating a local group on a member server

To create a local group on a member server:

- 1. In Computer Management, in the console tree, click **Groups**.
- 2. On the **Action** menu, click **New Group**.
- 3. In the **New Group** dialog box, in the **Group name** box, type a name for the new group.
- 4. In the **Description** box, type a description for the new group.
- 5. To add one or more users to a new group, click **Add**.
- 6. Click **Create**, and then click **Close**.

**Note** To perform this procedure, you must be a member of the Power Users group or the Administrators group on the local computer, or you must be delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure. As a security best practice, consider using **Run as** to perform this procedure.

Using a command line

To create a group in an Active Directory domain by using **dsadd**:

- 1. Open a command prompt.
- 2. Type **dsadd group GroupDN -samid SAMName -secgrp yes | no -scope l | g | u**

Value	Description
<i>GroupDN</i>	Specifies the distinguished name of the group object that you want to add
<i>SAMName</i>	Specifies the Security Accounts Manager (SAM) name as the unique SAM account name for this group (for example, operators)
<i>yes   no</i>	Specifies whether the group you want to add is a security group (yes) or a distribution group (no)
<i>l   g   u</i>	Specifies whether the scope of the group you want to add is domain local (l), global (g), or universal (u)

**Note** To view the complete syntax for this command, at a command prompt, type **dsadd group /?**

**Procedure for deleting a group**

To delete a group:

1. In Active Directory Users and Computers, in the console tree, click the folder that contains the group.
2. In the details pane, right-click the group, and then click **Delete**.

---

**Note** To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or the Enterprise Admins group in Active Directory, or you must be delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.

---

**Using a command line**

To delete a group by using **dsrm**:

1. Open a command prompt.
2. Type **dsrm GroupDN**

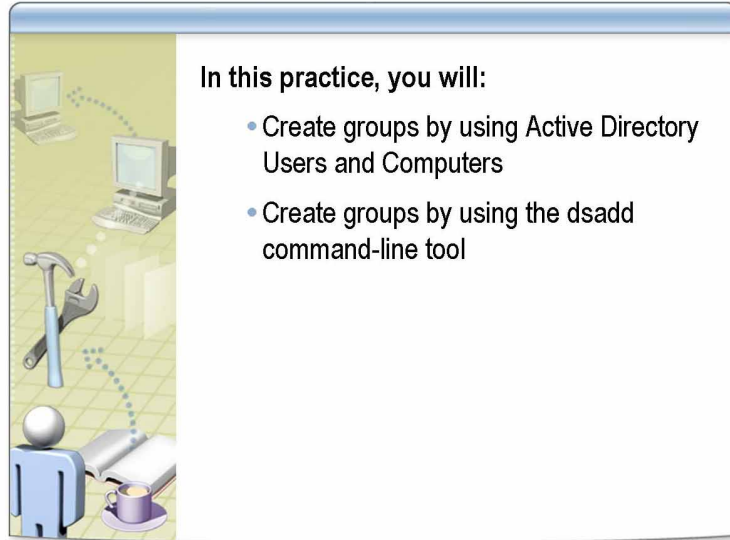
Value	Description
<i>GroupDN</i>	Specifies the distinguished name of the group object to be deleted.

---

**Note** To view the complete syntax for this command, at a command prompt, type **dsrm /?**

---

## Practice: Creating Groups



### Objective

In this practice, you will create global and local groups by using Active Directory Users and Computers. You will also create global groups by using the **dsadd** command-line tool.

### Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerNameUser* account.
- Open CustomMMC with the **Run as** command.  
Use the user account *Nwtraders\ComputerNameAdmin* (Example: *LondonAdmin*).
- Ensure that CustomMMC contains Active Directory Users and Computers.
- Review the procedures in this lesson that describe how to perform this task.

### Scenario

As a systems administrator, you must create multiple groups for the Accounting department. These groups will eventually be used for grouping accounts and assigning groups to resources.

**Practice****► Create groups by using Active Directory Users and Computers**

1. Create the following global groups in the organizational unit Locations/*ComputerName*/Groups:
  - G *ComputerName* Accounting Managers
  - G *ComputerName* Accounting Personnel
2. Create the following domain local groups in the organizational unit Locations/*ComputerName*/Groups:
  - DL *ComputerName* Accounting Managers Full Control
  - DL *ComputerName* Accounting Managers Read
  - DL *ComputerName* Accounting Personnel Full Control
  - DL *ComputerName* Accounting Personnel Read

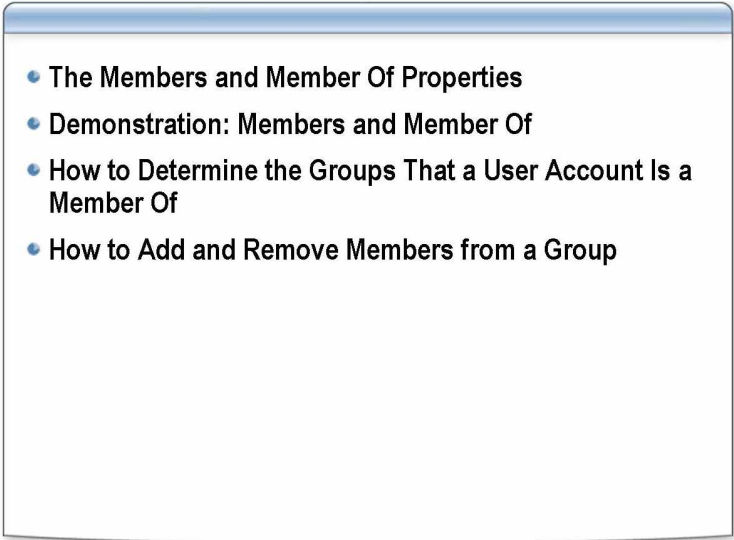
**Practice: Using the command line****► Create groups by using the dsadd command-line tool**

1. Create the following global group in the IT Test organizational unit:
  - G *ComputerName*Test

Example: C:\>dsadd group "cn=G London Test,ou=it test,dc=nwtraders,dc=msft" -secgrp yes -scope g -samid "G London Test"
2. Create the following domain local group in the IT Test organizational unit:
  - DL *ComputerName*Test

Example: C:\>dsadd group "cn=DL London Test,ou=it test,dc=nwtraders,dc=msft" -secgrp yes -scope L -samid "DL London Test"

## Lesson: Managing Group Membership

- 
- The Members and Member Of Properties
  - Demonstration: Members and Member Of
  - How to Determine the Groups That a User Account Is a Member Of
  - How to Add and Remove Members from a Group

---

### Introduction

Because many users often require access to different resources throughout an organization, administrators may have to grant membership to groups that reside in Active Directory or on local computers.

When adding members to or removing members from groups in Active Directory, an administrator can open Active Directory Users and Computers, click on a user account, drag it to the desired group, and drop the user account onto the group. This action quickly adds the user account to the group.

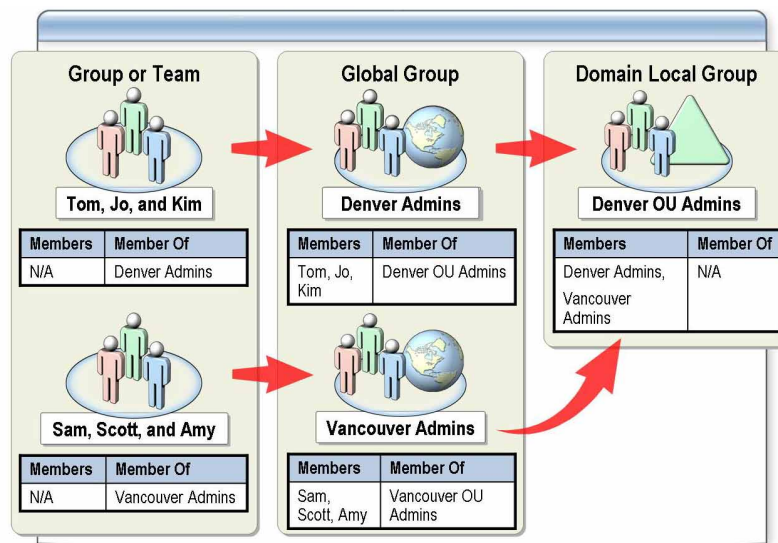
When adding members to or removing members from groups on a local computer, an administrator can use Computer Management to change group membership on the local computer.

### Lesson objectives

After completing this lesson, you will be able to:

- Distinguish between the **Members** and **Member Of** properties.
- Use the **Members** and **Member Of** properties by using the interface.
- Determine the groups that a user account is a member of.
- Add members to and remove members from a group.

## The Members and Member Of Properties



### Introduction

The illustration in the slide describes the **Members** and **Member Of** properties.

### Definition of Members and Member Of

Tom, Jo, and Kim are *members of* the Denver Admins global group. The global group Denver Admins is a *member of* the domain local group Denver OU Admins.

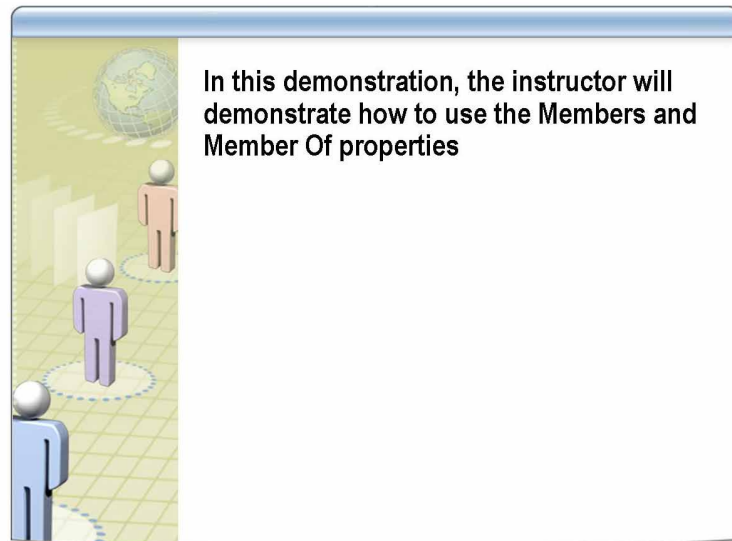
Sam, Scott, and Amy are *members of* the Vancouver Admins global group. The global group Vancouver Admins is a *member of* the domain local group Denver OU Admins.

The following table summarizes the information in the slide.

User or Group	Members	Members Of
Tom, Jo, Kim		Denver Admins
Denver Admins	Tom, Jo, Kim	Denver OU Admins
Sam, Scott, Amy		Vancouver Admins
Vancouver Admins	Sam, Scott, Amy	Denver OU Admins
Denver OU Admins	Denver Admins Vancouver Admins	

By using the **Members** and **Member Of** properties, you can determine groups that the user belongs to and what groups that group belongs to.

## Demonstration: Members and Member Of



### Objective

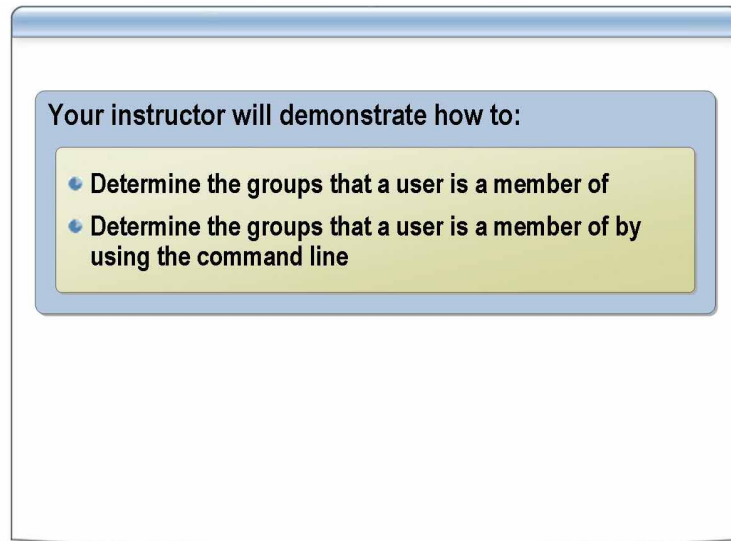
In this demonstration, the instructor will demonstrate how to use the **Members** and **Member Of** properties.

### Demonstration

To demonstrate how to use **Members** and **Member Of**:

1. Open Active Directory Users and Computers.
2. In the console tree, expand **NWTraders.msft**, and then expand the **IT Admin** organizational unit.
3. Click the **IT Users** organizational unit.
4. In the details pane double-click the **AcapulcoAdmin** user account.
5. In the **Properties** dialog box, on the **Member Of** tab, notice that the AcapulcoAdmin user account is a member of the following groups:
  - Domain Users
  - G Acapulco Admins
  - G IT Admins
6. Double-click the **G IT Admins** group.
7. In the **Properties** dialog box, on the **Members** tab, notice that the G IT Admins group has many members.
8. On the **Member Of** tab, notice the G IT Admins group is a member of the DL IT OU Administrators group.
9. Double-click the **DL IT OU Administrators** group.
10. In the **Properties** dialog box, on the **Members** tab, notice that the G IT Admins group is a member.

## How to Determine the Groups That a User Account Is a Member Of



### Introduction

After you add users to groups, Active Directory updates the **Member Of** property of their user accounts.

### Procedure

To determine the groups that a user is a member of:

1. In Active Directory Users and Computers, in the console tree, click **Users** or click the folder that contains the user account.
2. In the details pane, right-click a user account, and then click **Properties**.
3. In the **Properties** dialog box, click the **Member Of** tab.

**Note** You do not need administrative credentials to perform this task. Therefore, as a security best practice, consider performing this task as a user without administrative credentials.

### Using a command line

To determine the groups a user is a member of by using **dsget**:

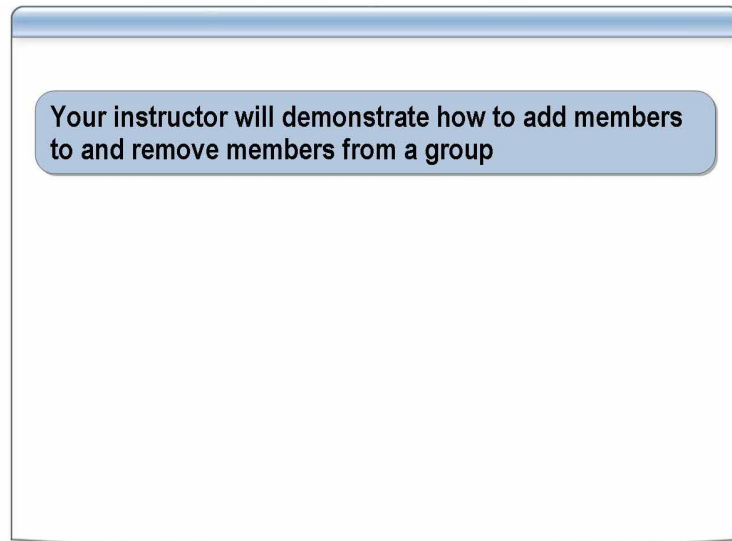
1. Open a command prompt.
2. Type **dsget user *UserDN* -memberof**

Value	Description
<i>UserDN</i>	Specifies the distinguished name of the user object for which you want to display group membership

**Note** To view the complete syntax for this command, at the command prompt, type **dsget user /?**



## How to Add and Remove Members from a Group



---

### Introduction

After creating a group, you add members by using Active Directory Users and Computers. Members of groups can include user accounts, other groups, and computers.

### Procedure

To add members to or remove members from a group:

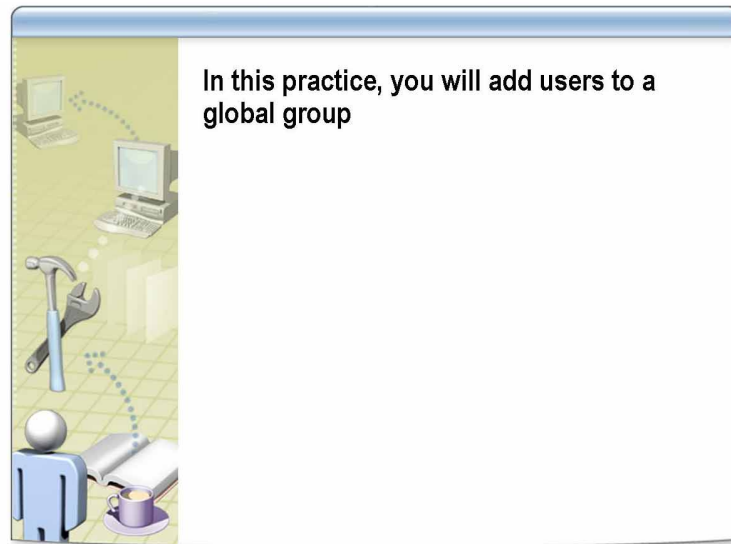
1. In Active Directory Users and Computers, in the console tree, click the folder that contains the group to which you want to add a member.
2. In the details pane, right-click the group, and then click **Properties**.
3. In the **Properties** dialog box, on the **Members** tab, click **Add**.  
If you want to remove a member from the group, click the member, and then click **Remove**.
4. In the **Select Users, Contact, Computers, or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user, group, or computer that you want to add to the group, and then click **OK**.

---

**Tip** You can also add a user account or group by using the **Member Of** tab in the **Properties** dialog box for that user account or group. Use this method to quickly add the same user or group to multiple groups.

---

## Practice: Managing Group Membership



---

### Objectives

In this practice, you will add users to a global group.

### Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.  
Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Ensure that CustomMMC contains Active Directory Users and Computers.
- Ensure that the following groups are in the *Locations/ComputerName/Groups* organizational unit:
  - Global groups:
    - G *ComputerName* Accounting Managers
    - G *ComputerName* Accounting Personnel
- Review the procedures in this lesson that describe how to perform this task.

**Scenario**

Northwind Traders is starting to implement global groups. You will need to find all Accounting personnel in your city organizational unit and add them to the G *ComputerName* Accounting Personnel group.

**Practice****► Perform a custom search for Accounting personnel**

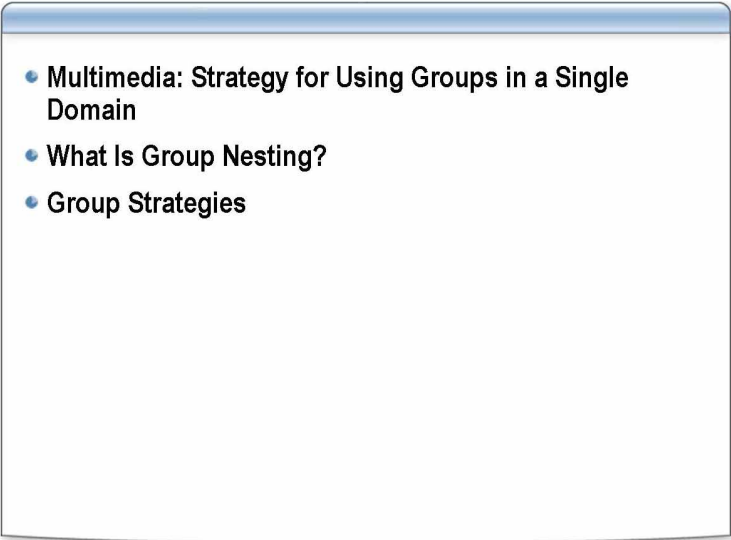
- Search for users with the City search attribute of *ComputerName* (Example: London) and the Department search attribute of Accounting.

This search should produce approximately 10 users. One of the users is the Accounting manager.

**► Add the users to G *ComputerName* Accounting Personnel**

1. Select all users produced by the preceding search.
2. Right-click the selection, and then click **Add to a group**.
3. Add the users to G *ComputerName* Accounting Personnel.

## Lesson: Strategies for Using Groups

- 
- Multimedia: Strategy for Using Groups in a Single Domain
  - What Is Group Nesting?
  - Group Strategies

---

### Introduction

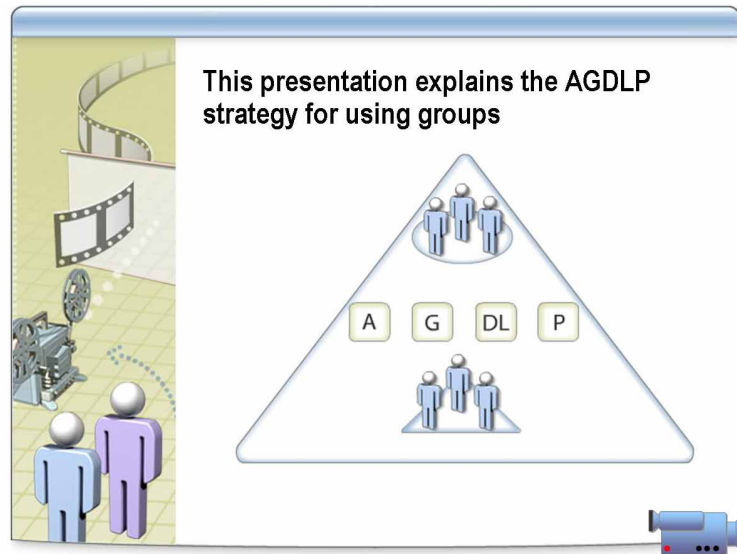
To use groups effectively, you need strategies for applying different group scopes. This lesson covers skills and knowledge that you need to use groups optimally by employing different strategies with groups.

### Lesson objectives

After completing this lesson, you will be able to:

- Explain the AGDLP strategy for using groups in a single domain.
- Describe group nesting.
- Describe the following strategies for using groups:
  - A G P
  - A DL P
  - A G DL P
  - A G U DL P
  - A G L P

## Multimedia: Strategy for Using Groups in a Single Domain



### File location

To view the *Strategy for Using Groups in a Single Domain* presentation, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation. Do not open this presentation unless the instructor tells you to.

### Key points

User accounts → Global groups → Domain Local groups ← Permissions

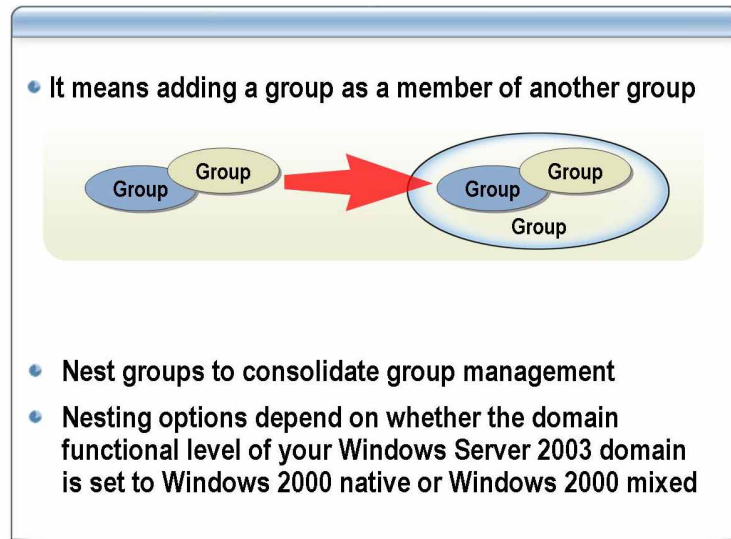
(A)

(G)

(DL)

(P)

## What Is Group Nesting?



---

### Introduction

Using nesting, you can add a group as a member of another group. You can nest groups to consolidate group management. Nesting increases the member accounts that are affected by a single action and reduces replication traffic caused by the replication of changes in group membership.

### Nesting options

Your nesting options depend on whether the domain functional level of your Windows Server 2003 domain is set to Windows 2000 native or Windows 2000 mixed. In domains where the domain functional level is set to Windows 2000 native, group membership is determined as follows:

- Universal groups can have as their members: user accounts, computer accounts, universal groups, and global groups from any domain.
- Global groups can have as their members: user accounts from the same domain and global groups from the same domain.
- Domain local groups can have as their members: user accounts, universal groups, and global groups, all from any domain. They can also have as members domain local groups from within the same domain.

You cannot create security groups with universal scope in domains where the domain functional level is set to Windows 2000 mixed. Universal scope is supported only in domains where the domain functional level is set to Windows 2000 native or Windows Server 2003.

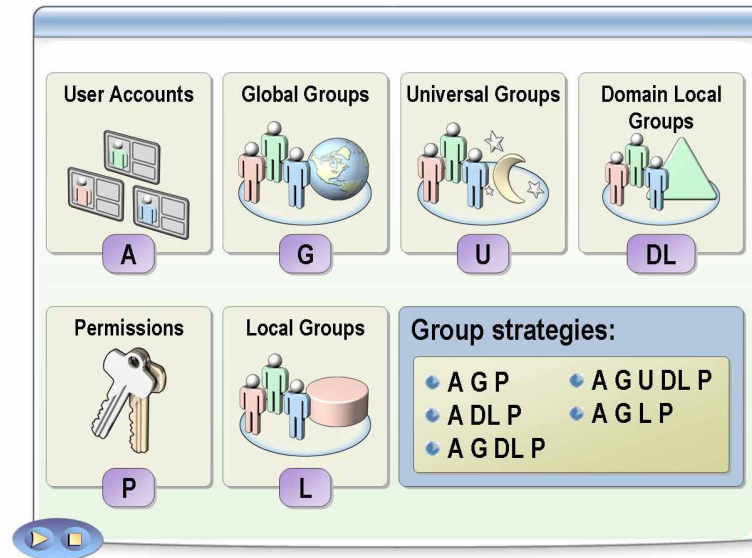
---

**Note** Minimize the levels of nesting. A single level of nesting is the most effective method, because tracking permissions is more complex with multiple levels.

Also, troubleshooting becomes difficult if you must trace permissions through multiple levels of nesting. Therefore, document group membership to keep track of permissions.

---

## Group Strategies



### Introduction

To use groups effectively, you need strategies for applying the different group scopes. The strategy you choose depends on the Windows network environment of your organization. In a single domain, the common practice is to use global and domain local groups to grant permissions for network resources. In a network with multiple domains, you can incorporate global and universal groups into your strategy.

### A G P

With A G P, you place user accounts (A) in global groups (G), and you grant permissions (P) to the global groups. The limitation of this strategy is that it complicates administration when you use multiple domains. If global groups from multiple domains require the same permissions, you must grant permissions to each global group individually.

### When to use the A G P strategy

Use A G P for forests with one domain and very few users and to which you will never add other domains.

A G P has the following advantages:

- Groups are not nested and therefore troubleshooting may be easier.
- Accounts belong to a single group scope.

A G P has the following disadvantages:

- Every time a user authenticates with a resource, the server must check the global group membership to determine if the user is still a member of the group.
- Performance degrades, because a global group is not cached.

### A DL P

With A DL P, you place user accounts (A) in domain local groups (DL), and you grant permissions (P) to the domain local groups. One limitation of this strategy is that it does not allow you to grant permissions for resources outside of the domain. Therefore, it reduces flexibility as your network grows.

**When to use the A DL P strategy**

Use A DL P for a forest where all of the following are true:

- The forest has only one domain and very few users.
- You will never add other domains to the forest.
- There are no Microsoft Windows NT 4.0 member servers in the domain.

A DL P has the following advantages:

- Accounts belong only to a single group scope.
- Groups are not nested, and therefore troubleshooting may be easier.

A DL P has the following disadvantage:

- Performance degrades, because each domain local group has many members that must be authenticated.

**A G DL P**

With A G DL P, you place user accounts (A) in global groups (G), place the global groups in domain local groups (DL), and then grant permissions (P) to the domain local groups. This strategy creates flexibility for network growth and reduces the number of times you must set permissions.

**When to use the A G DL P strategy**

Use A G DL P for a forest consisting of one or more domains and to which you might have to add future domains.

A G DL P has the following advantages:

- Domains are flexible.
- Resource owners require less access to Active Directory to flexibly secure their resources.

A G DL P has the following disadvantage:

- A tiered management structure is more complex to set up initially, but easier to manage over time.

**A G U DL P**

With A G U DL P, you place user accounts (A) in global groups (G), place the global groups in universal groups (U), place the universal groups in domain local groups (DL), and then grant permissions (P) to the domain local groups.



**When to use the A G U DL P strategy**

Use A G U DL P for a forest with more than one domain where administrators require centralized administration for many global groups.

A G U DL P has the following advantages:

- There is flexibility across the forest.
- It enables centralized administration.

---

**Note** Domain Local groups should not be used to assign Active Directory object permissions in a Forest with more than one Domain. For more information see Microsoft Knowledge Base Article 231273, Group Type and Scope Usage in Windows at <http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B231273>.

---

A G U DL P has the following disadvantage:

- The membership of universal groups is stored in the global catalog.

---

**Note** The global catalog is a domain controller that stores a copy of all Active Directory objects in a forest. The global catalog stores a full copy of all objects in Active Directory for its host domain and a partial copy of all objects for all other domains in the forest.

---

- It may be necessary to add more global catalog servers.
- There may be global catalog replication latency. When referring to the global catalog, *latency* is the time it takes to replicate a change to each global catalog server in the forest.

There is a disadvantage to using universal groups only if the universal groups have a very dynamic membership with a lot of global catalog replication traffic as the membership changes) in a multidomain forest. With A G U DL P, this is less of an issue, because the membership of universal groups is relatively static (that is, the universal group has global groups, not individual users, as members).

**A G L P**

Use the A G L P strategy to place user accounts in a global group and grant permissions to the local group. One limitation of this strategy is that you cannot grant permissions for resources outside the local computer.

Therefore, place user accounts in a global group, add the global group to the local group, and then grant permissions to the local group. With this strategy, you can use the same global group on multiple local computers.

---

**Note** Use domain local groups whenever possible. Use local groups only when a domain local group has not been created for this purpose.

---

**When to use the A G L P strategy**

Use the A G L P strategy when your domain has the following characteristics:

- Upgrade from Windows NT 4.0 to Windows Server 2003
- Contain one domain
- Have few users
- Will never add other domains
- To maintain a Windows NT 4.0 group strategy
- To maintain centralized user management and decentralized resource management

It is recommended that you use A G L P with Windows Server 2003 Active Directory and Windows NT 4.0 member servers.

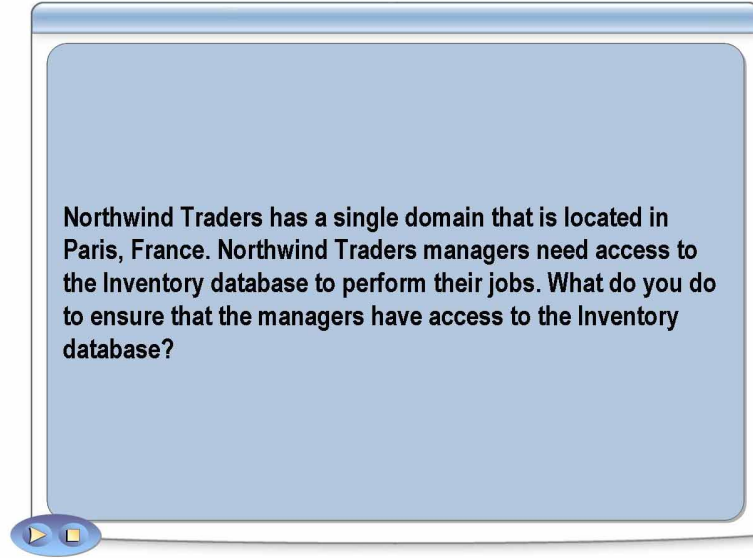
A G L P has the following advantages:

- It maintains the Windows NT 4.0 group strategy.
- Resource owners own membership to every group that needs access.

A G L P has the following disadvantages:

- Active Directory does not control access.
- You must create redundant groups across member servers.
- It does not enable centralized administration.

## Class Discussion: Using Groups in a Single Domain



### Example 1

Northwind Traders has a single domain that is located in Paris, France. Northwind Traders managers need access to the Inventory database to perform their jobs.

What do you do to ensure that the managers have access to the Inventory database?

---

---

---

---

**Example 2**

Northwind Traders wants to react more quickly to market demands. It is determined that the accounting data must be available to all Accounting personnel. Northwind Traders wants to create the group structure for the entire Accounting division, which includes the Accounts Payable and Accounts Receivable departments.

What do you do to ensure that the managers have the required access and that there is a minimum of administration?

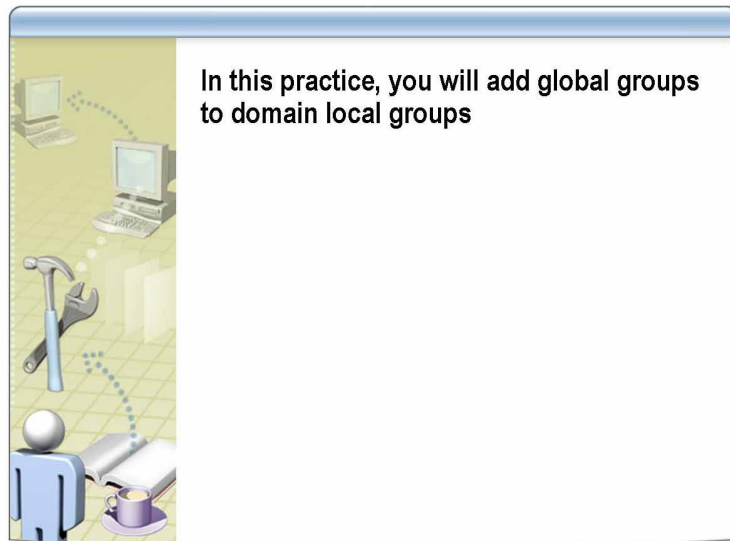
---

---

---

---

## Practice: Adding Global Groups to Domain Local Groups



### Objective

In this exercise, you will add a global group to a domain local group.

### Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.  
Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Ensure that CustomMMC contains Active Directory Users and Computers.
- Ensure that the following groups are in the *Locations/ComputerName/Groups* organizational unit:
  - Global groups:
    - G *ComputerName* Accounting Managers
    - G *ComputerName* Accounting Personnel
  - Domain local groups:
    - DL *ComputerName* Accounting Managers Full Control
    - DL *ComputerName* Accounting Managers Read
    - DL *ComputerName* Accounting Personnel Full Control
    - DL *ComputerName* Accounting Personnel Read
- Review the procedures in this lesson that describe how to perform this task.

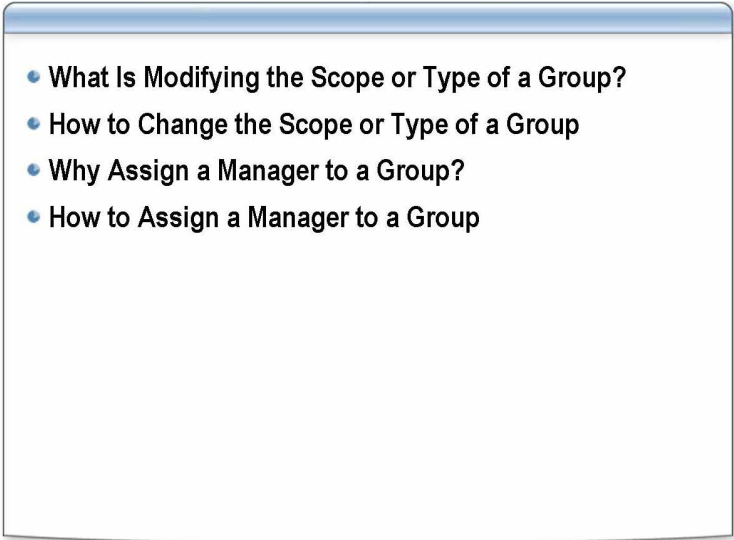
**Scenario**

Northwind Traders is implementing A G DL P and needs you to add global groups to domain local groups.

**Practice****► Add global groups to domain local groups**

1. Add the G *ComputerName* Accounting Managers global group to DL *ComputerName* Accounting Managers Full Control.
2. Add the G *ComputerName* Accounting Managers global group to DL *ComputerName* Accounting Managers Read.
3. Add the G *ComputerName* Accounting Personnel global group to DL *ComputerName* Accounting Personnel Full Control.
4. Add the G *ComputerName* Accounting Personnel global group to DL *ComputerName* Accounting Personnel Read.

## Lesson: Modifying Groups

- 
- What Is Modifying the Scope or Type of a Group?
  - How to Change the Scope or Type of a Group
  - Why Assign a Manager to a Group?
  - How to Assign a Manager to a Group

---

### Introduction

This lesson introduces you to the skills and knowledge that you need to modify groups.

### Lesson objectives

After completing this lesson, you will be able to:

- Explain what it means to modify the scope or type of a group.
- Change the scope or type of a group.
- Explain why you assign a manager to a group.
- Assign a manager to a group.

## What Is Modifying the Scope or Type of a Group?



---

### Introduction

When creating a new group, by default, the new group is configured as a security group with global scope, regardless of the current domain functional level.

### Changing group scope

Although you cannot change group scope in domains with a domain functional level set to Windows 2000 mixed, you can make the following scope changes in domains with the domain functional level set to Windows 2000 native or Windows Server 2003:

- *Global to universal.* This is allowed only if the group you want to change is not a member of another global group.

---

**Note** You cannot change a group's scope from global to domain local directly. To do that, you must change the group's scope from global to universal and then from universal to domain local.

---

- *Domain local to universal.* This is allowed only if the group you want to change does not have another domain local group as a member.
- *Universal to global.* This is allowed only if the group you want to change does not have another universal group as a member.
- *Universal to domain local.* There are no restrictions for this change.



---

**Changing group type**

You can convert a group from a security group to a distribution group, and vice versa, at any time, but only if the domain functional level is set to Windows 2000 native or higher. You cannot convert a group while the domain functional level is set to Windows 2000 mixed.

You may convert groups from one type to the other in the following scenarios:

- **Security to distribution**

A company splits into two companies. Users migrate from one domain to another domain, but they keep their old e-mail addresses. You want to send them e-mail messages by using old security groups, but you want to remove security context from the group.

- **Distribution to security**

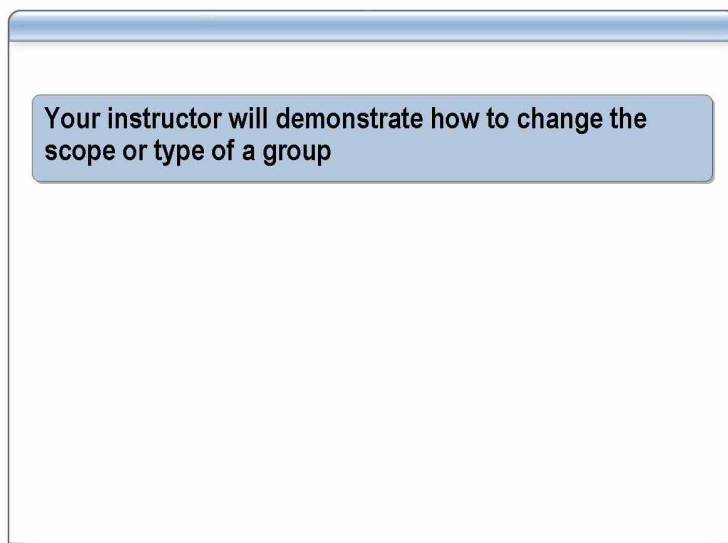
A distribution group gets very large, and the users want to use this group for security-related tasks. However, they still want to use the group for e-mail.

---

**Note** Although you can add a contact to a security group and to a distribution group, you cannot grant permissions to contacts. You can send contacts e-mail messages.

---

## How to Change the Scope or Type of a Group



---

### Introduction

To change the scope or type of a group, the domain functional level must be set to Windows 2000 native or higher. You cannot change the scope or type of groups if the domain functional level is set to Windows 2000 mixed.

### Procedure

To change the scope or type of a group:

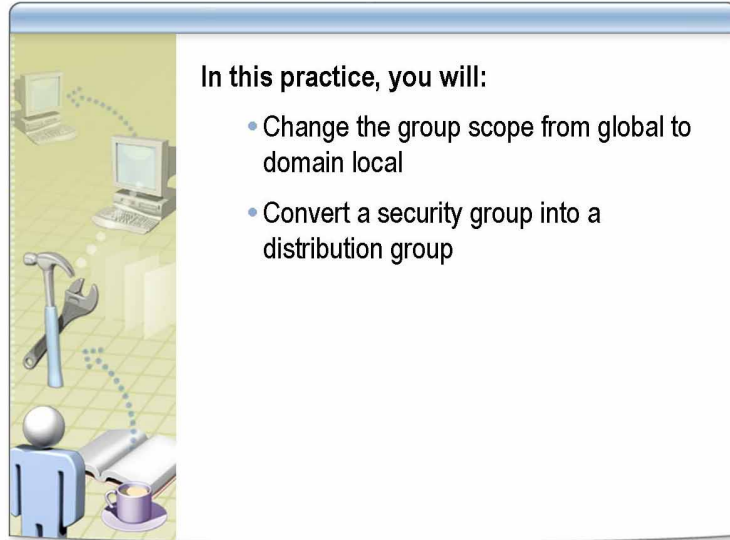
1. In Active Directory Users and Computers, in the console tree, click the folder that contains the group.
2. In the details pane, right-click the group, and then click **Properties**.
3. In the **Properties** dialog box, on the **General** tab, under **Group type**, click the group type to change it.
4. Under **Group scope**, click the group scope to change it.

---

**Note** To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in Active Directory, or you must be delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.

---

## Practice: Changing the Scope and Type of a Group



### Objective

In this practice, you will:

- Change the group scope from global to a domain local.
- Convert a security group into a distribution group.

### Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.  
Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Ensure that CustomMMC contains Active Directory Users and Computers.

### Scenario

The IT managers at Northwind Traders want you to write a procedure for changing the scope of a security group from global to domain local. You must create all test groups in the IT Test organizational unit.

### Practice: Changing group scope

#### ► Create a global security group

- In the IT Test organizational unit, create a global security group named *ComputerName* Group Scope Test.

- **Document the procedure for converting the global group into a domain local group**

---

---

---

---

---

---

---

---

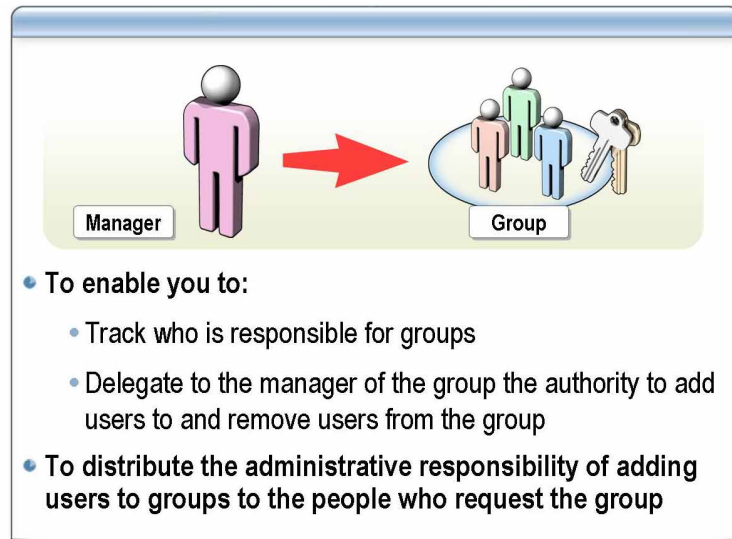
**Scenario**

The IT managers at Northwind Traders want you to test the Active Directory feature that enables you to convert a security group into a distribution group. They want you to convert the security group you created into a distribution group.

**Practice: Changing group type**

- **Convert a global security group into a distribution group**
  - Change the *ComputerName* Group Scope group from a security group to a distribution group.

## Why Assign a Manager to a Group?



### Advantages of assigning a manager to a group

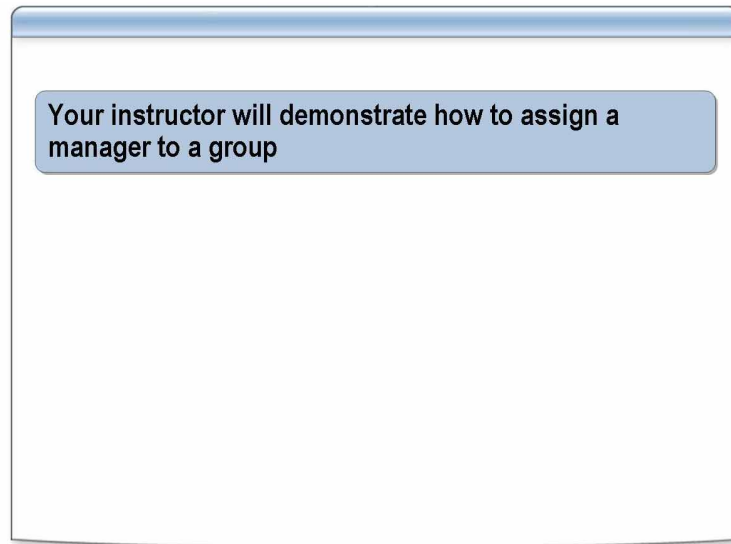
Active Directory in Windows Server 2003 allows you to assign a manager to a group as a property of the group. This enables you to:

- Track who is responsible for groups.
- Delegate to the manager of the group the authority to add users to and remove users from the group.

Because people in large organizations are added to and removed from groups so often, some organizations distribute the administrative responsibility of adding users to groups to the people who request the group.

If you document who the manager of the group is, the contact information for that user account is recorded. If the group ever needs to be migrated to another domain or needs to be deleted, the network administrator has a record of who owns the group and their contact information. Therefore, the network administrator can call or send an e-mail message to the manager to notify the manager about the change that needs to be made to the group.

## How to Assign a Manager to a Group



---

### Introduction

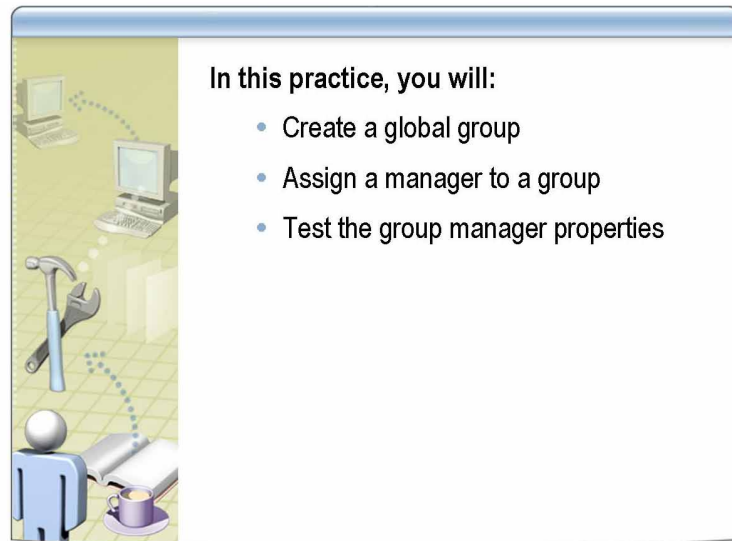
Use the following procedure to assign a manager to a group.

### Procedure

To assign a manager to a group:

1. In Active Directory Users and Computers, in the console tree, double-click the group that needs a manager.
2. In the **Properties** dialog box, on the **Managed By** tab, click **Change** to add a manager to a group or to change the manager of a group.
3. In the **Select User or Contact** dialog box, in the **Enter the object name to select** box, type the user name of the user who you want to manage the group, and then click **OK**.
4. Select the **Manager can update membership list** check box if you want the manager to add and remove users and groups.
5. In the **Properties** dialog box, click **OK**.

## Practice: Assigning a Manager to a Group



### In this practice, you will:

- Create a global group
- Assign a manager to a group
- Test the group manager properties

### Objective

In this practice, you will:

- Create a global group.
- Assign a manager to the group who can modify group membership.
- Test the group manager properties.

### Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.  
Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Ensure that CustomMMC contains Active Directory Users and Computers.

### Scenario

You have been asked to create a group for the Sales department called G *ComputerName* Sales Strategy. The owner of the group will be the Sales manager for your city organizational unit.

### Practice

#### ► Create a global group in your city organizational unit

1. Create a global group called G *ComputerName* Sales Strategy in the organizational unit *Locations/ComputerName*
2. Log off.

► **Test the group manager properties**

1. Log on by using the *ComputerNameUser* account.
2. Open CustomMMC and try to add a user to G *ComputerName Sales Strategy*.  
You should not be able to add any users to this group.
3. Close CustomMMC.
4. Open CustomMMC (do not use the **Run as** command).
5. In Active Directory Users and Computers, navigate to your city organizational unit, and then double-click **G *ComputerNameSales Strategy***.
6. In the **Properties** dialog box, click the **Members** tab, and notice that you cannot add any users, because the **Add** button is unavailable.
7. Close CustomMMC.

► **Make *ComputerNameUser* a manager of G *ComputerName Sales Strategy***

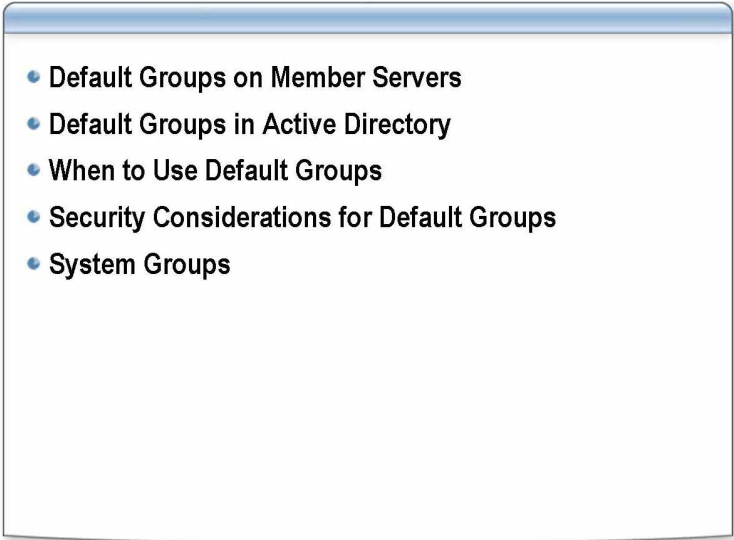
1. Open CustomMMC with the **Run as** command.  
Use the *Nwtraders\ComputerNameAdmin* account.
2. In Active Directory Users and Computers, navigate to your city organizational unit, and then double-click **G *ComputerName Sales Strategy***.
3. In the **Properties** dialog box, on the **Managed By** tab, add the *ComputerNameUser* user account.
4. Select the **Manager can update membership list** check box.
5. Close CustomMMC.

► **Test the group manager properties**

1. In Active Directory Users and Computers, navigate to your city organizational unit, and then double-click **G *ComputerName Sales Strategy***.
2. In the **Properties** dialog box, on the **Members** tab, add the *User0001* user account.
3. Close all windows and CustomMMC.



## Lesson: Using Default Groups

- 
- Default Groups on Member Servers
  - Default Groups in Active Directory
  - When to Use Default Groups
  - Security Considerations for Default Groups
  - System Groups

---

### Introduction

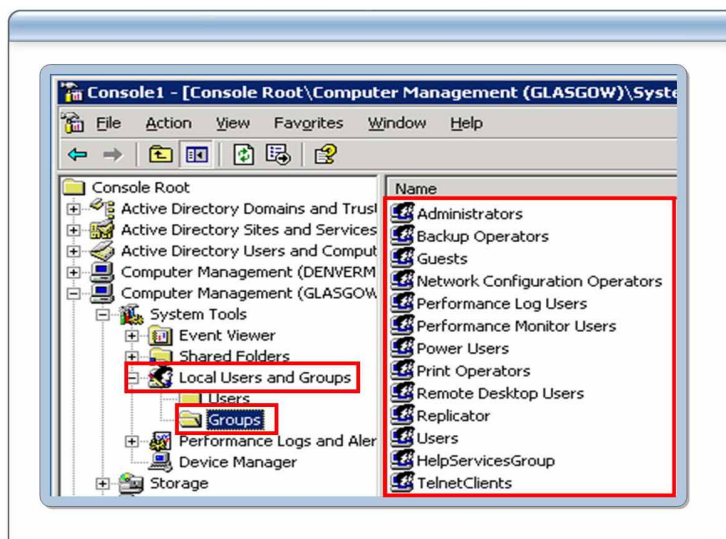
This lesson introduces how default groups are used.

### Lesson objectives

After completing this lesson, you will be able to:

- Explain how default groups are used on member servers.
- Explain how default groups are used in Active Directory.
- Identify when to use default groups.
- Identify the security considerations for default groups.
- Explain how system groups are used.

## Default Groups on Member Servers



### Definition

The Groups folder is located on a member server in the Local Users and Groups console, which displays all built-in default local groups and any local groups you create. The default local groups are created automatically when you install Windows Server 2003. The local groups can contain local user accounts, domain user accounts, computer accounts, and global groups.

### Default local groups on member server

The following table describes some of the default local groups on a member or stand-alone server running Windows Server 2003.

Group	Description
Administrators	<ul style="list-style-type: none"> <li>Members have full control of the server and can assign user rights and access control permissions to users as necessary.</li> <li>Administrators is a default member account and has full control of the server.</li> <li>Users should be added with caution.</li> <li>When joined to a domain, the Domain Admins group is automatically added to this group.</li> </ul>
Guests	<ul style="list-style-type: none"> <li>A temporary profile is created for a member when the member logs on.</li> <li>When the guest member logs off, the profile is deleted.</li> <li>The Guest account is disabled by default.</li> </ul>
Performance Log Users	<ul style="list-style-type: none"> <li>Members can manage performance counters, logs, and alerts on the server locally and from remote clients without being a member of the Administrators group.</li> </ul>

*(continued)*

Group	Description
Performance Monitor Users	<ul style="list-style-type: none"> <li>Members can monitor performance counters on the server locally and from remote clients without being a member of the Administrators or Performance Log Users groups.</li> </ul>
Power Users	<ul style="list-style-type: none"> <li>Members can create user accounts and then modify and delete the accounts they have created.</li> <li>Members can create local groups and then add or remove users from the local groups they have created.</li> <li>Members can add or remove users from the Power Users, Users, and Guests groups.</li> <li>Members can create shared resources and administer the shared resources they have created.</li> <li>Members cannot take ownership of files, back up or restore directories, load or unload device drivers, or manage security and auditing logs.</li> </ul>
Print Operators Users	<ul style="list-style-type: none"> <li>Members can manage printers and print queues.</li> <li>Members perform common tasks, such as running applications, using local and network printers, and locking the server.</li> <li>Users cannot share directories or create local printers.</li> <li>The Domain Users, Authenticated Users, and Interactive groups are members of this group. Therefore, any user account created in the domain becomes a member of this group.</li> </ul>

The following additional groups are also default groups on a member server which are not commonly used.

- Network Configuration Operators
- Remote Desktop Users
- Replicator
- HelpServicesGroup
- Terminal Server Users

---

**Note** For more information about default groups on member servers, search for “default local groups” in Windows Server 2003 Help.

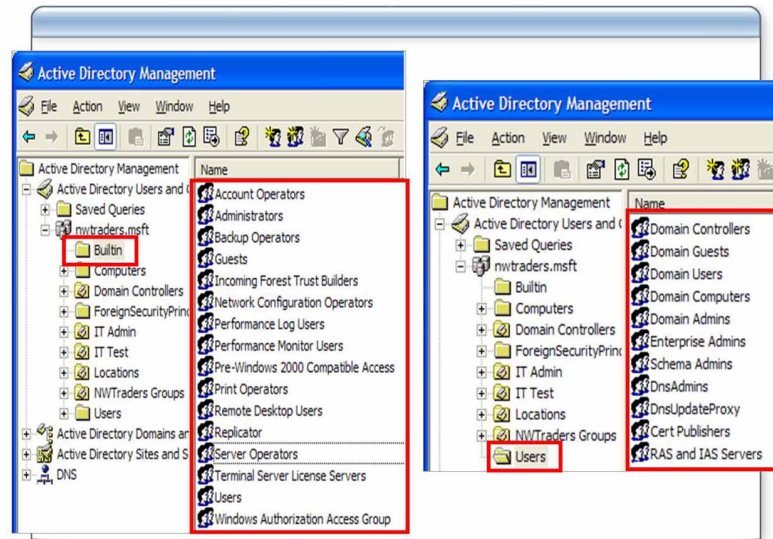
---

**Default groups used by network services**

The following table describes the default groups used by network services and installed only with the Dynamic Host Configuration Protocol (DHCP) service.

Group	Membership
DHCP Administrators	<ul style="list-style-type: none"><li>• Members have administrative access to the DHCP service.</li><li>• The DHCP Administrators group provides security to assign limited administrative access to the DHCP server only, while not providing full access to the server.</li><li>• Members can administer DHCP on a server by using the DHCP console or the <b>Netsh</b> command, but they cannot perform other administrative actions on the server.</li></ul>
DHCP Users	<ul style="list-style-type: none"><li>• Members have read-only access to the DHCP service.</li><li>• Members can view information and properties stored at a specified DHCP server. This information is useful to support staff when they need to obtain DHCP status reports.</li></ul>
WINS Users	<ul style="list-style-type: none"><li>• Members are permitted read-only access to the Windows Internet Name Service (WINS).</li><li>• Members can view information and properties stored at a specified WINS server. This information is useful to support staff when they need to obtain WINS status reports.</li></ul>

## Default Groups in Active Directory



### Definition

Default groups are security groups automatically created when you install an Active Directory domain. You can use these predefined groups to manage shared resources and delegate specific domain-wide administrative roles.

Many default groups are automatically assigned a set of user rights that determine what each group and their members can do within the scope of a domain or forest. User rights authorize members of a group to perform specific actions, such as log on to a local system or back up files and folders. For example, a member of the Backup Operators group has the right to perform backup operations for all domain controllers in the domain.

Several default groups are available in the Users and Builtin containers of Active Directory. The Builtin container contains domain local groups. The Users container contains global groups and domain local groups. You can move groups in the Users and Builtin containers to other group or organizational unit folders in the domain, but you cannot move them to other domains.

**Groups in the Builtin container**

The following table describes each default group in the Builtin container that is added to the default groups on a stand-alone or member server when Active Directory is installed. All of these default groups are added along with the user rights assigned to each group.

Group	Description
Account Operators	<ul style="list-style-type: none"><li>• Members can create, modify, and delete accounts for users, groups, and computers located in the Users or Computers containers and organizational units in the domain, except the Domain Controllers organizational unit.</li><li>• Members do not have permission to modify the Administrators or the Domain Admins groups or accounts for members of those groups.</li><li>• Members can log on locally to domain controllers in the domain and shut them down.</li><li>• Because this group has significant power in the domain, add users with caution.</li></ul>
Incoming Forest Trust Builders	<ul style="list-style-type: none"><li>• Members can create one-way, incoming forest trusts to the forest root domain.</li><li>• This group has no default members.</li></ul>
Pre-Windows 2000 Compatible Access	<ul style="list-style-type: none"><li>• Members have read access on all users and groups in the domain.</li><li>• This group is provided for backward compatibility for computers running Windows NT 4.0 and earlier.</li><li>• Add users to this group only if they are using Remote Access Service (RAS) on a computer running Windows NT 4.0 or earlier.</li></ul>
Server Operators	<ul style="list-style-type: none"><li>• Members can log on interactively, create and delete shared resources, start and stop some services, back up and restore files, format the hard disk, and shut down the computer.</li><li>• This group has no default members.</li><li>• Because this group has significant power on domain controllers, add users with caution.</li></ul>

**Groups in the Users container**

The following table describes each default group in the Users container and the user rights assigned to each group.

Group	Description
Domain Controllers	<ul style="list-style-type: none"> <li>This group contains all domain controllers in the domain.</li> </ul>
Domain Guests	<ul style="list-style-type: none"> <li>This group contains all domain guests.</li> </ul>
Domain Users	<ul style="list-style-type: none"> <li>This group contains all domain users.</li> <li>Any user account created in the domain is a member of this group automatically.</li> </ul>
Domain Computers	<ul style="list-style-type: none"> <li>This group contains all workstations and servers joined to the domain.</li> <li>Any computer account created becomes a member of this group automatically.</li> </ul>
Domain Admins	<ul style="list-style-type: none"> <li>Members have full control of the domain.</li> <li>This group is a member of the Administrators group on all domain controllers, all domain workstations, and all domain member servers at the time they are joined to the domain.</li> <li>The Administrator account is a member of this group. Because the group has full power in the domain, add users with caution.</li> </ul>
Enterprise Admins	<ul style="list-style-type: none"> <li>Members have full control of all domains in the forest.</li> <li>This group is a member of the Administrators group on all domain controllers in the forest.</li> <li>The Administrator account is a member of this group. Because this group has full control of all domains in the forest, add users with caution.</li> </ul>
Group Policy Creator Owners	<ul style="list-style-type: none"> <li>Members can modify Group Policy in the domain.</li> <li>The Administrator account is a member of this group. Because this group has significant power in the domain, add users with caution.</li> </ul>

The following list contains the additional Default groups that Systems Engineers would use to manage groups:

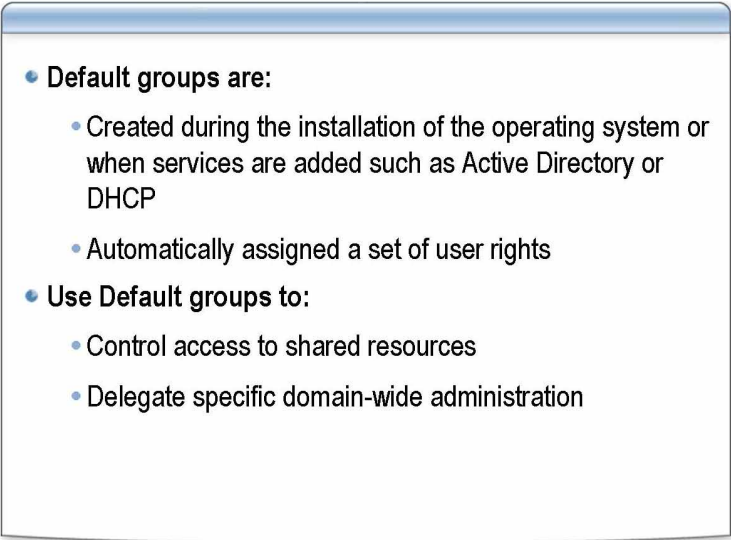
- Schema Admins
- DnsAdmins
- DnsUpdateProxy
- Cert Publishers
- RAS and IAS Servers

---

**Note** For more information about other groups in the Users container, search for “Active Directory default groups” in Windows Server 2003 Help.

---

## When to Use Default Groups

- 
- **Default groups are:**
    - Created during the installation of the operating system or when services are added such as Active Directory or DHCP
    - Automatically assigned a set of user rights
  - **Use Default groups to:**
    - Control access to shared resources
    - Delegate specific domain-wide administration

---

### Using default groups

Predefined groups help you to control access to shared resources and delegate specific domain-wide administrative roles. Many default groups are automatically assigned a set of user rights that authorize members of the group to perform specific actions in a domain, such as log on to a local system or back up files and folders.

When you add a user to a group, the user receives all the user rights assigned to the group and all the permissions assigned to the group for any shared resources.

As a security best practice, it is recommended that members of default groups with broad administrative access use **Run as** to perform administrative tasks.



## Security Considerations for Default Groups

- Place a user in a default group only when you are sure you want to give the user all the user rights and permissions assigned to that group in Active Directory; otherwise, create a new security group
- As a security best practice, members of default groups should use Run as

---

### Security considerations for default groups

Only place a user in a default group when you are sure you want to give the user:

- All the user rights assigned to that group in Active Directory.
- All of the permissions assigned to that group for any shared resources associated with that default group.

Otherwise, create a new security group and assign the group only those user rights or permissions that the user absolutely requires.

As a security best practice, members of default groups that have broad administrative access should not perform an interactive logon by using administrative credentials. Instead, users with this level of access should use **Run as**.

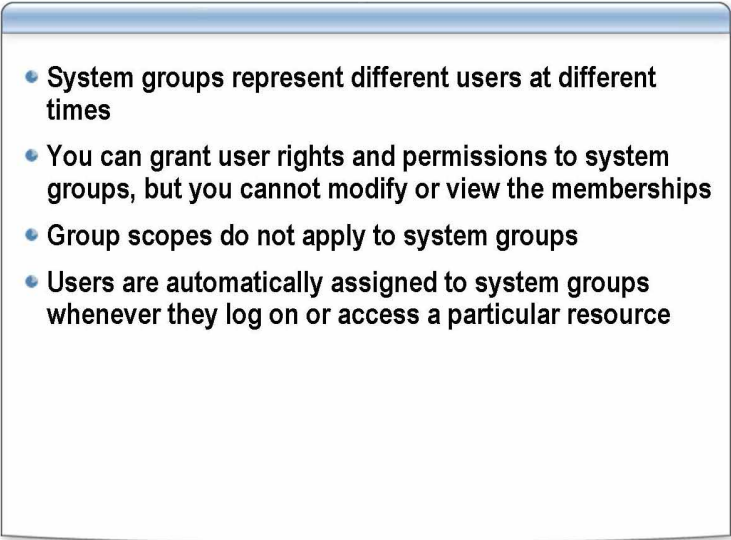
---

**Warning** Only add members to default groups when members need all rights associated with the group. For example, if you need to add a service account to back up and restore files on a member server, you add the service account to the Backup Operators group. The Backup Operators group has the user rights to back up and restore files on the computer.

However, if your service account only needs to back up files and not restore them, it is better to create a new group. You can then grant the group the user right to back up files and not grant the group the right to restore files.

---

## System Groups

- 
- System groups represent different users at different times
  - You can grant user rights and permissions to system groups, but you cannot modify or view the memberships
  - Group scopes do not apply to system groups
  - Users are automatically assigned to system groups whenever they log on or access a particular resource

---

### Introduction

You cannot change the membership of system groups. The operating system creates them, and you cannot change or manage them. It is important to understand the system groups, because you can use them for security purposes.

### Definition

Servers running Windows Server 2003 include several special identities in addition to the groups in the Users and Builtin containers. For convenience, these identities are generally referred to as system groups.

System groups represent different users at different times, depending on the circumstances. Although you can grant user rights and permissions to the system groups, you cannot modify or view their memberships.

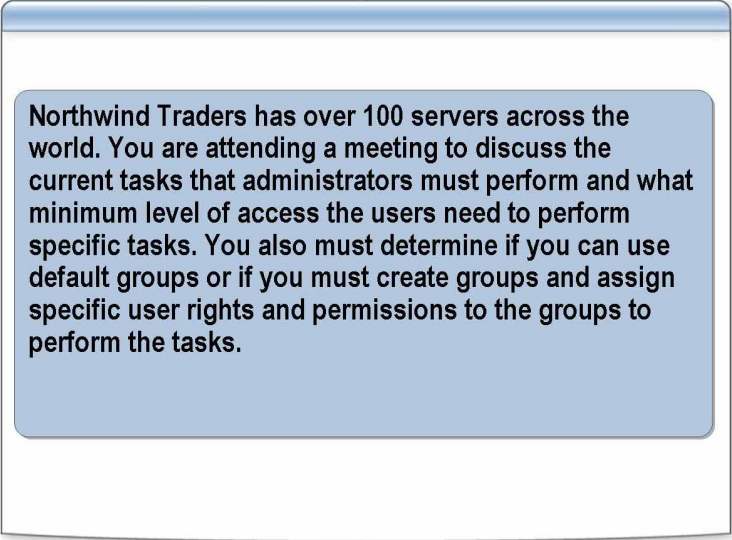
Group scopes do not apply to system groups. Users are automatically assigned to system groups whenever they log on or access a particular resource.

**System groups**

The following table describes the system groups.

<b>System group</b>	<b>Description</b>
Anonymous Logon	<p>The Anonymous Logon system group represents users and services that access a computer and its resources through the network without using an account name, password, or domain name.</p> <p>On computers running Windows NT and earlier, the Anonymous Logon group is a member of the Everyone group by default.</p> <p>On computers running a member of the Windows Server 2003 family, the Anonymous Logon group is not a member of the Everyone group by default. If you want to create a file share for an anonymous user, you grant permissions to the Anonymous Logon group.</p>
Everyone	<p>The Everyone system group represents all current network users, including guests and users from other domains. Whenever a user logs on to the network, the user is automatically added to the Everyone group.</p> <p>If security is not a concern for a specific group in your domain, you can grant permissions to the Everyone group. However, because the Anonymous Logon group can become a member of the Everyone group, it is not recommended that you use this group for permissions above read-only.</p>
Network	<p>The Network system group represents users currently accessing a given resource over the network, as opposed to users who access a resource by logging on locally at the computer where the resource is located. Whenever a user accesses a given resource over the network, the user is automatically added to the Network group.</p>
Interactive	<p>The Interactive system group represents all users currently logged on to a particular computer and accessing a given resource located on that computer, as opposed to users who access the resource over the network. Whenever a user accesses a resource on the computer to which they are currently logged on, the user is automatically added to the Interactive group.</p>
Authenticated Users	<p>The Authenticated Users system group represents all users within Active Directory. Always use the Authenticated Users group when granting permissions for a resource instead of using the Everyone group to prevent guests from accessing resources.</p>
Creator Owner	<p>The Creator Owner system group includes the user account for the user who created or took ownership of a resource. If a member of the Administrators group creates a resource, the Administrators group is the owner of the resource.</p>

## Class Discussion: Using Default Groups vs. Creating New Groups



Northwind Traders has over 100 servers across the world. You are attending a meeting to discuss the current tasks that administrators must perform and what minimum level of access the users need to perform specific tasks. You also must determine if you can use default groups or if you must create groups and assign specific user rights and permissions to the groups to perform the tasks.

---

**Scenario**

Northwind Traders has over 100 servers across the world. You are attending a meeting to discuss the current tasks that administrators must perform and what minimum level of access the users need to perform specific tasks. You also must determine if you can use default groups or if you must create groups and assign specific user rights and permissions to the groups to perform the tasks.

**Discussion**

You must assign default groups or create new groups for the following tasks. List the group that has the most restrictive user rights for performing the following actions or determine if you must create a new group.

1. Backing up and restoring domain controllers

---

---

---

2. Backing up member servers

---

---

---

3. Creating groups in the NWTraders Groups organizational unit

---

---

---

- 
4. Logging on to the domain

---

---

---

5. Determining who needs read-only access to the DHCP servers

---

---

---

6. Determining what help desk employees need access to control the desktop remotely

---

---

---

7. Determining who needs administrative access to all computers in the entire domain

---

---

---

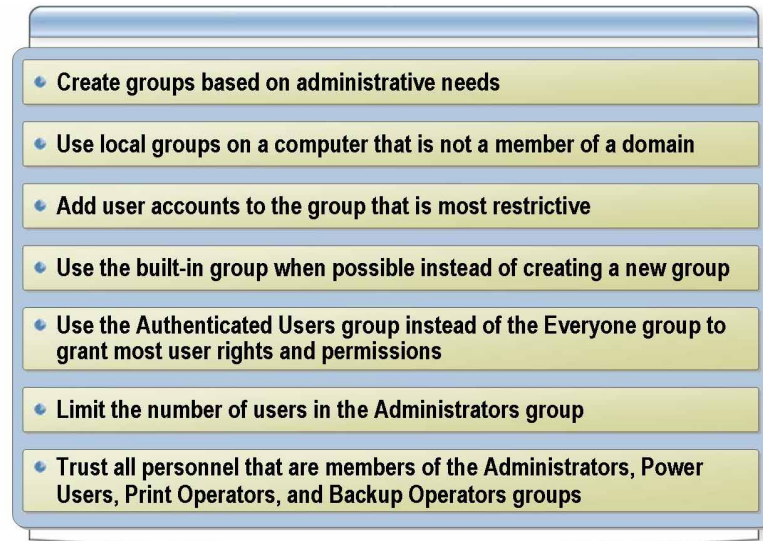
8. Determining who need access to a shared folder called Sales on a server called LonSrv2

---

---

---

## Best Practices for Managing Groups



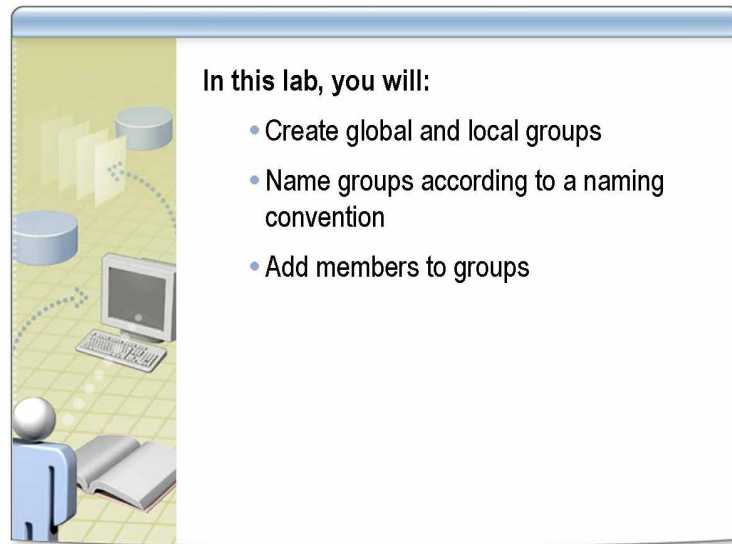
---

### Best practices

Consider the following best practices for managing groups:

- Create groups based on administrative needs. When you create a group based on a job function and another person takes over that job, you only need to change the group membership. You do not need to change all permissions that are granted to the individual user account. Because of this, it is sometimes advantageous to create a group that has only one member.
- Use local groups to give users access to resources on local computers when the computer is not a member of a domain.
- If you have multiple groups to which you can add user accounts, add user accounts to the group that is most restrictive. However, ensure that you grant the appropriate user rights and permissions so that users can accomplish any required task.
- Whenever a default group enables users to accomplish a task, use the default group instead of creating a new group. Create groups only when there are no default groups that provide the required user rights and permissions.
- Use the Authenticated Users group instead of the Everyone group to grant most user rights and permissions. Using this group minimizes the risk of unauthorized access, because Windows Server 2003 adds only valid user accounts to members of the Authenticated Users system group.
- Limit the number of users in the Administrators group. Members of the Administrators group on a local computer have Full Control permissions for that computer. Add a user to the Administrators group if the user will perform only administrative tasks.
- Your organization must equally trust all personnel that are members of the Administrators, Power Users, Print Operators, and Backup Operators groups. Some default user rights assigned to specific default local groups may allow members of those groups to gain additional rights on your computer, including administrative rights.

## Lab A: Creating and Managing Groups



### Objectives

After completing this lab, you will be able to:

- Create global and domain local groups.
- Name groups according to a naming convention.
- Add members to groups.

### Prerequisites

Before working on this lab, you must have knowledge of Active Directory, organizational units, organizational unit hierarchy, and accounts in Active Directory.

Before you begin this lab:

- Log on to the domain by using the *ComputerNameUser* account.
- Open CustomMMC with the **Run as** command.  
Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Ensure that CustomMMC contains Active Directory Users and Computers.

**Estimated time to  
complete this lab:  
60 minutes**

## Exercise 1

### Creating and Managing Groups

In this exercise, you will create domain local and global groups, add members to groups, and nest groups.

#### Scenario

The Active Directory designers have just finished creating the group naming convention. They have given you a list of teams in Northwind Traders that you must create groups for. Some groups have already been created in your city organizational unit, so you must determine if the existing groups meet the naming convention and contain the appropriate users and groups. You then must add the appropriate user to the appropriate global groups. Finally, you must add the appropriate global groups to the appropriate domain local groups. All groups should be created in the *Locations/ComputerName/Groups* organizational unit.

The following teams in Northwind Traders need groups:

- Marketing Managers
- Marketing Personnel
- HR Managers
- HR Personnel

The Active Directory designers have created the following naming convention for groups:

- The first part of the group name defines the scope of the group (Example: **G** for global group and **DL** for domain local group).
- The second part of the group name defines the city organizational unit that the group belongs to (Example: London).
- The third part of the group name defines who the group is created for (Example: Sales Managers or Sales Personnel).
- If the group is a domain local group, the last part of the group name defines the maximum permissions the group will be used for (Example: Read or Full Control).



Tasks	Specific instructions
1. Create global groups for the following teams in the Locations/ <i>ComputerName</i> /Groups organizational unit.	<ol style="list-style-type: none"> <li>Marketing Managers (Example: G London Marketing Managers)</li> <li>Marketing Personnel</li> <li>HR Managers</li> <li>HR Personnel</li> </ol>
2. Search for users who are managers and add them to the manager global groups.	<ol style="list-style-type: none"> <li>Search for all Marketing Managers in the city called <i>ComputerName</i> and add them to the G <i>ComputerName</i> Marketing Managers group.</li> <li>Do the preceding step for the following groups: <ul style="list-style-type: none"> <li>G <i>ComputerName</i> Marketing Personnel</li> <li>G <i>ComputerName</i> HR Managers</li> <li>G <i>ComputerName</i> HR Personnel</li> </ul> </li> </ol>
3. Search for users who are personnel and add them to the personnel global groups.	<ol style="list-style-type: none"> <li>Search for all users in the city called <i>ComputerName</i> and in the Marketing department and add them to the G Marketing Personnel group.</li> <li>Do the preceding step for each global personnel group.</li> </ol>
4. Create domain local groups that will be used for Read and Modify permissions for the following teams in the Locations/ <i>ComputerName</i> /Groups organizational unit.	<ul style="list-style-type: none"> <li>Create the following Domain Local groups: <ul style="list-style-type: none"> <li>DL <i>ComputerName</i> Marketing Managers Read</li> <li>DL <i>ComputerName</i> Marketing Personnel Read</li> <li>DL <i>ComputerName</i> HR Managers Read</li> <li>DL <i>ComputerName</i> HR Personnel Read</li> <li>DL <i>ComputerName</i> Marketing Managers Modify</li> <li>DL <i>ComputerName</i> Marketing Personnel Modify</li> <li>DL <i>ComputerName</i> HR Managers Modify</li> <li>DL <i>ComputerName</i> HR Personnel Modify</li> </ul> </li> </ul>
5. Add members to the domain local groups for managers.	<ol style="list-style-type: none"> <li>For each manager domain local group that was created, add the appropriate managers global group. For example: add G <i>ComputerName</i> Marketing Managers to DL <i>ComputerName</i> Marketing Managers Read and DL <i>ComputerName</i> Marketing Managers Modify.</li> <li>Do the preceding step for every manager's domain local group.</li> </ol>
6. Add members to the domain local groups for personnel.	<ol style="list-style-type: none"> <li>For each personnel domain local group that was created, add the appropriate global group for personnel. For example: add G <i>ComputerName</i> Marketing Personnel to DL <i>ComputerName</i> Marketing Personnel Read and DL <i>ComputerName</i> Marketing Personnel Modify.</li> <li>Do the preceding step for every personnel's domain local group.</li> </ol>

