Group Accounts

On This Page

Types of Group Accounts

Group accounts are used to manage privileges for multiple users. Global group accounts, for domain use, are created in **Active Directory Users And Computers,** while local group accounts, for local system use, are created in **Local Users And Groups**. Generally, group accounts are created to facilitate the management of similar types of users. The types of groups that can be created include the following:

- **Groups for departments within the organization:** Generally, users who work in the same department need access to similar resources. Because of this, groups can be created that are organized by department, such as Business Development, Sales, Marketing, or Engineering.
- **Groups for users of specific applications:** Often, users will need access to an application and resources related to the application. Application-specific groups can be created so that users get proper access to the necessary resources and application files.
- **Groups for roles within the organization:** Groups could also be organized by the user's role within the organization. For example, executives probably need access to different resources than supervisors and general users. Thus, by creating groups based on roles within the organization, proper access is given to the users that need it.

Top Of Page

Group Scope and Group Type

Each security and distribution group has a scope that identifies the extent to which the group is applied in the domain tree or forest. There are three different scopes: universal, global, and domain local.

- Groups with universal scope can have as their members groups and accounts from any Windows 2000 domain in the domain tree or forest and can be granted permissions in any domain in the domain tree or forest. Groups with universal scope are referred to as universal groups.
- Groups with global scope can have as their members groups and accounts only from the domain in which the group is defined and can be granted permissions in any domain in the forest. Groups with a global scope are referred to as global groups.

- Groups with domain local scope can have as their members groups and accounts from a Windows 2000 or Windows NT domain and can be used to grant permissions only within a domain. Groups with a domain local scope are referred to as domain local groups.

In the case of multiple forests, users defined in only one forest cannot be placed into groups defined in another forest, and groups defined in only one forest cannot be assigned permissions in another forest.

The following table summarizes the behaviors of the different group scopes.

Universal scope	**Global scope**	**Domain local scope**
In native-mode domains, can have as their members accounts from any domain, global groups from any domain and universal groups from any domain.	In native-mode domains, can have as their members accounts from the same domain and global groups from the same domain.	In native-mode domains, can have as their members accounts, global groups, and universal groups from any domain, as well as domain local groups from the same domain.
In native-mode domains, security groups with universal scope cannot be created.	In native-mode domains, can have as their members accounts from the same domain.	In native-mode domains, can have as their members accounts and global groups from any domain.
Groups can be put into other groups (when the domain is in native-mode) and assigned permissions in any domain.	Groups can be put into other groups and assigned permissions in any domain.	Groups can be put into other domain local groups and assigned permissions only in the same domain.
Cannot be converted to any other group scope.	Can be converted to universal scope, as long as it is not a member of any other group having global scope.	Can be converted to universal scope, as long as it does not have as its member another group having domain local scope.

Changing group scope

When creating a new group, by default, the new group is configured as a security group with global scope regardless of the current domain mode. Changing a group scope can be accomplished by the following allowed conversions:

- **Global to universal**. This is only allowed if the group is not a member of another group having global scope.
- **Domain local to universal**. The group being converted cannot have as its member another group having domain local scope.

Note: Changing a group scope is not allowed in mixed-mode domains. Note that mixed-mode

domains are not part of the evaluated configuration.

Group types

There are two types of groups in Windows 2000:

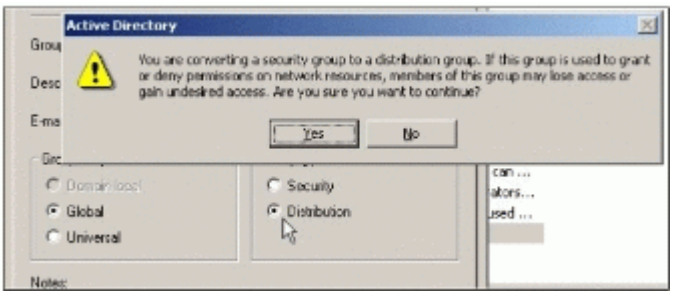
- **Security groups**. Security groups are listed in discretionary access control lists (DACLs) that define permissions on resources and objects. Security groups can also be used as an e-mail entity. Sending an e-mail message to the group sends the message to all the members of the group.
- **Distribution groups**. Distribution groups are not security-enabled. They cannot be listed in DACLs. Distribution groups can be used only with e-mail applications (such as Exchange), to send e-mail to collections of users.

Note: Although a contact can be added to a security group as well as to a distribution group, contacts cannot be assigned rights and permissions. Contacts in a group can be sent e-mail.

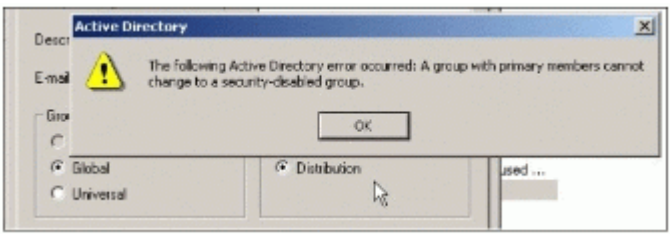
Converting between security and distribution groups

A group can be converted from a security group to a distribution group, and vice versa, at any time, but only if the domain is in native-mode. No groups can be converted while a domain is in mixed-mode.

- When attempting to a group type from convert from a security group to a distribution group the following warning will be presented:



- Any attempt to change a security group that is also the primary group of a user, to a distribution group will not be allowed. The attempt will result in the following message:



- Changes to group type will affect users once they log off and log back on to the network. Since distribution groups are not security enabled and are only for e-mail, any member of a group that is changed from security to distribution type would not be allowed to log on and would receive the following message:

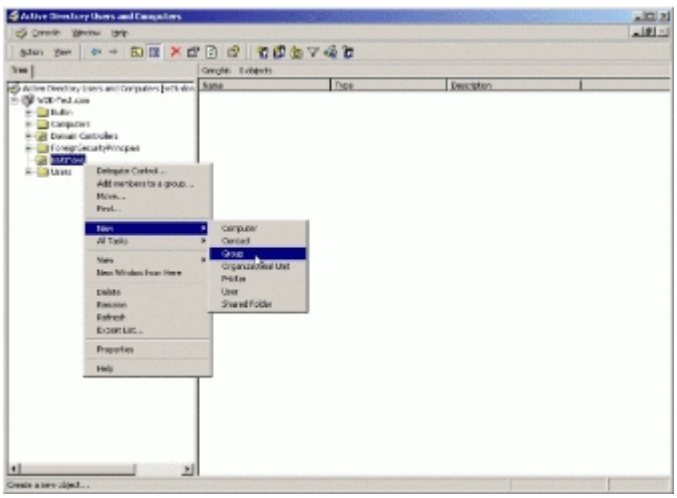
- Conversely, care must be taken to evaluate permissions, privileges, and group memberships associated with any group that is changed from a distribution group to a security group. Any user that is originally a member of a distribution group and then gets changed to a security group would gain any new privileges and access rights associated with the newly converted security group.

Top Of Page

Creating Group Accounts

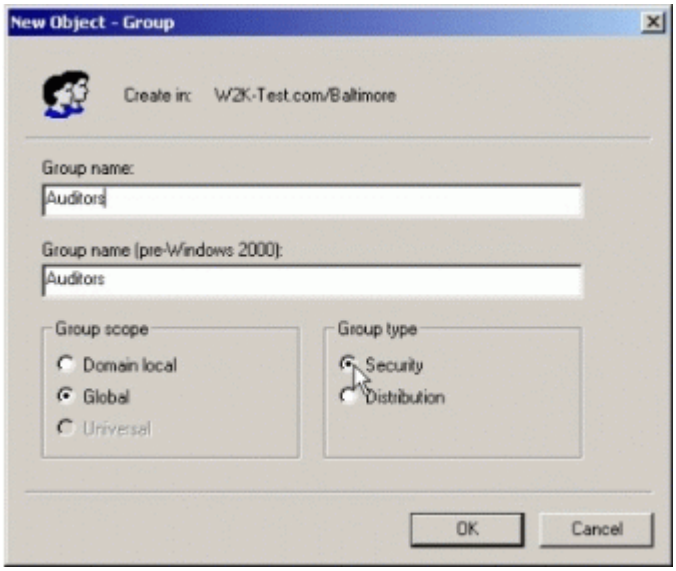
Add a group account as follows:

1. Open **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click the domain node.
3. Right-click the folder in which the group is to be added, point to **New**, and then click **Group**.



4. Type the name of the new group. By default, the name that is typed is also entered as the pre-Windows 2000 name of the new group.
5. Select the desired **Group scope**.

6. Select the desired **Group type**.



7. Click **OK**. The new group will appear in the details pane of the Active **Directory Users and Computers**.

8. Modify logon rights and privileges for the new group as explained in the "Configuring User Rights" subsection of this document. These procedures may be used by authorized administrators to modify user logon rights and privileges at any time by assigning or removing logon rights and privileges as required.

Top Of Page

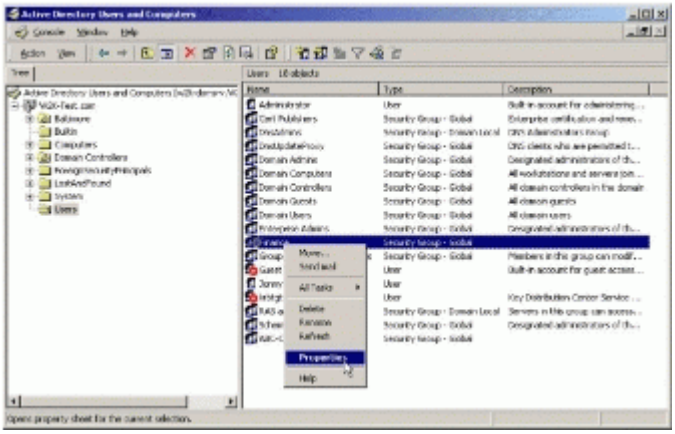
Adding group members

Add members to a group as follows:

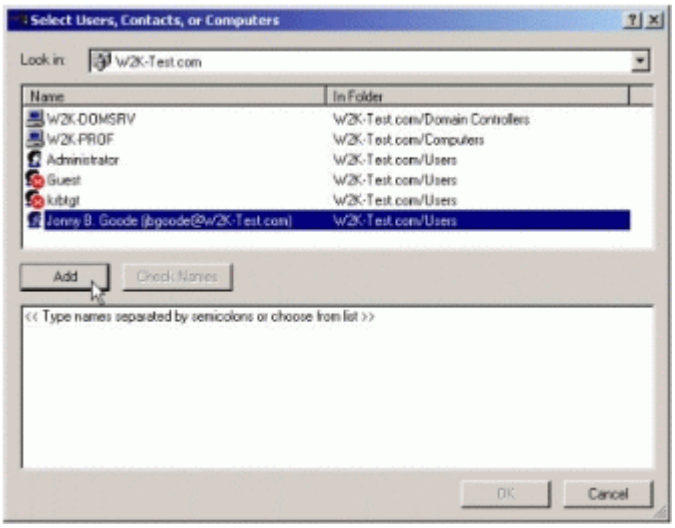
1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

2. In the console tree, click the folder that contains the desired group account.

3. In the details pane, double-click the desired group account, or right-click the group and select **Properties** from the menu.



4. In the **Properties** window, click the **Members** tab.
5. Click **Add**. The **Select Users, Contacts, or Computers** dialog box appears.
6. From the **Look in** drop list select the domain from which to add accounts. From the list of users, select the user/users to add to the group and click **Add**.



7. Click **OK** in the **Select Users, Contacts, or Computers** dialog box, then click the **Apply** button in the **Properties** window. When there are no more users to add, click **OK** in the **Properties** window.

Top Of Page

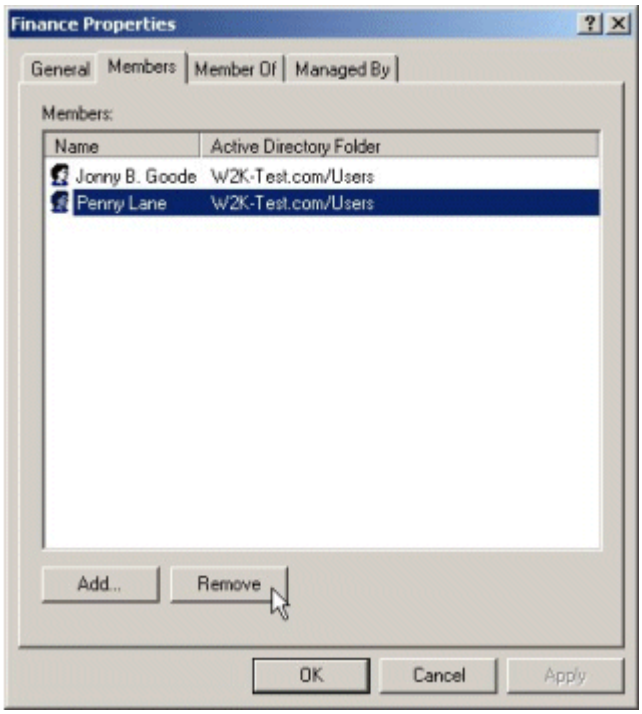
Removing group members

Remove members to a group as follows:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, click the folder that contains the desired group account.
3. In the details pane, double-click the desired group account, or right-click the group and select Properties from the menu.

4. In the **Properties** window, click the **Members** tab.

5. From the list of group members, select the member to be removed and click the **Remove** button.



6. An **Active Directory** confirmation message will appear. Click the **Yes** button to remove the member from the group.

7. In the **Properties** window, click **Apply** and click **OK**.

Top Of Page

Nesting Groups

Adding groups to other groups (nesting groups) can reduce the number of times permissions need to be assigned. Desired Groups can be nested to consolidate group management by increasing the affected member accounts and to reduce replication traffic caused by replication of group membership changes. Windows 2000 allows for unlimited levels of nesting in Native mode. However, tracking permissions becomes more complex with multiple levels of nesting, therefore it is important to keep the levels of nesting to a minimum. Nesting options depend on whether the domain is in native mode or mixed-mode. Groups in native-mode domains or distribution groups in mixed-mode domains have their membership determined as follows:

- Groups with universal scope can have as their members: accounts, computer accounts, other groups with universal scope, and groups with global scope from any domain.
- Groups with global scope can have as their members: accounts from the same domain and other groups with global scope from the same domain.
- Groups with domain local scope can have as their members: accounts, groups with universal scope, and groups with global scope, all from any domain. They can also have as members other groups with domain local scope from within the same domain.

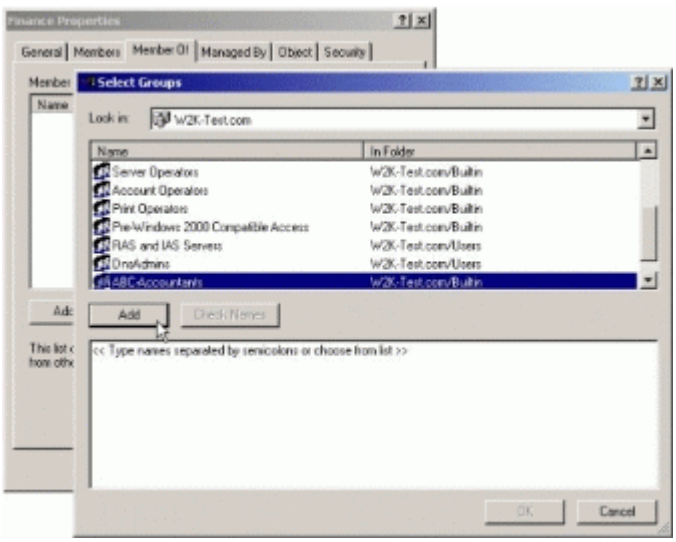
Security groups in a mixed-mode domain are restricted to the following types of membership:

- Groups with global scope can have as their members only accounts.
- Groups with domain local scope can have as their members other groups with global scope and accounts.

Security groups with universal scope cannot be created in mixed-mode domains because universal scope is supported only in Windows 2000 native-mode domains.

Add/modify group nesting as follows:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, click the folder that contains the desired group account.
3. In the details pane, double-click the desired group account, or right-click the group and select Properties from the menu.
4. In the **Properties** window, click the **Member of** tab.
5. Click **Add**. The Select Groups dialog box appears.
6. From the **Look in** drop list select the domain from to add accounts. From the list of users, select the group accounts to add to the group and click **Add**.



7. Click **OK** in the **Select Groups** dialog box, then click **Apply** in the **Properties** window. When there are no more group accounts to add, click **OK** in the **Properties** window.

Top Of Page

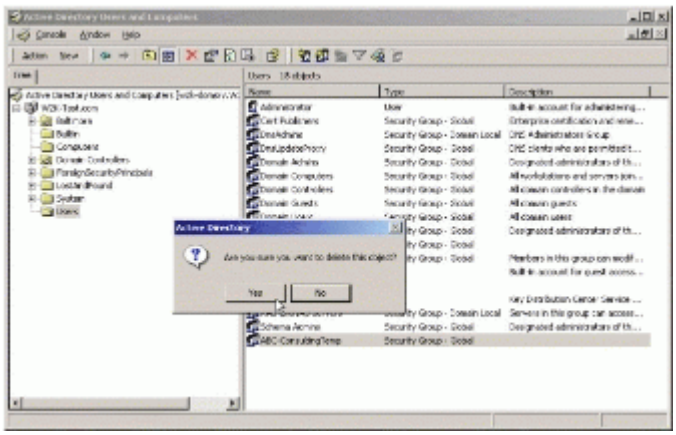
Deleting a group

Each group that is created has a unique, nonreusable security identifier (SID). Windows 2000 uses the SID to identify the group and the permissions that are assigned to it. When a group is deleted,

Windows 2000 does not use the SID again, even if a new group is created with the same name as the group that was deleted. Therefore, simply re-creating a deleted group cannot restore access to resources.

A group may be deleted as follows:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, click **Groups** or the folder that contains the desired group account.
3. In the details pane, right-click the group.
4. Click **Delete**. An **Active Directory** confirmation window will appear.



5. Click **Yes** to delete the group.

Top Of Page