Lists the users and groups to whom permissions have been assigned for this object.

Click to open the **Select Users, Groups, or Computers** dialog box, where you can select the users and groups to whom you want to assign permissions.

Removes the selected user or group and its associated permissions from this object.

Lists the standard permissions that you can allow or deny for each user or group.

Click to view and set special permissions, auditing information, and owner information for this object.

Lists the current permission entries for this object, including the users and groups who have permissions for this object, a description of the permissions, and where the permissions are applied.

Click to open the **Select User, Group, or Computer** dialog box, where you can select the users and groups to whom you want to assign permissions.

Removes the selected user or group and its associated permissions from this object.

Click to display and edit permissions for the selected user or group for this object.

Specifies whether permissions for this object will be affected by inheritance. By default, when you create or change permissions for a parent object, such as a folder, all existing child objects, such as files or subfolders, inherit those permissions. However, if you clear this check box, this object will not inherit any permissions from the parent object. In addition, by clearing this check box you can change or remove any permissions already inherited.

Lists the auditing entries currently assigned to this object, including the users and groups who are audited, the type of auditing, and where the auditing takes place.

Click to open the **Select User, Group, or Computer** dialog box, where you can select the users and groups whose actions you want to audit.

Removes the selected user or group and its associated auditing entries for this object.

Click to display and edit the access attempts that will be audited for the selected user or group.

Specifies whether auditing entries for this object will be affected by inheritance. By default, when you create or change auditing entries for a parent object, such as a folder, all existing child objects, such as files or subfolders, inherit those auditing entries. If you clear this check box, this object will not inherit auditing entries from parent objects. In addition, by clearing this check box you can change or remove any auditing entries already inherited.

Click to choose a user or group account to add to the **Permission Entries** list for this object.

Specifies where the permissions are applied.

Lists the special permissions you can allow or deny for each user and group.

Specifies whether you want to apply permissions to the selection in **Apply onto** and all applicable child objects within the tree.

Click to choose a user or group account to add to the **Auditing Entries** list.

Clears the check boxes that are selected. Inherited auditing entries (shaded check boxes) are not cleared unless you close this dialog box and clear **Allow inheritable auditing entries from parent to propagate to this object**.

Specifies where objects are audited.

Lists the types of access to audit. You can audit both successful and failed access to objects. Successful access means that a user was able to successfully access the object. Failed access means that a user attempted to access the object but did not have the necessary permissions to do so.

Specifies whether you want to apply auditing to the selection in **Apply onto** and all applicable child objects within the tree.

Clears the check boxes that are selected. Inherited permissions (shaded check boxes) are not cleared unless you close this dialog box and clear **Allow inheritable permissions from parent to propagate to this object**.

Specifies the current owner of this object. The owner is the person who controls how permissions are set on every object on an NTFS volume and can grant permissions to others.

Lists the users to whom you can assign ownership of this object.

Specifies whether to replace the owner on all objects and subcontainers within the selected container.

Specifies the user or group to whom the auditing entries are assigned for this object

Specifies the user or group to whom the permissions are assigned for this object.