Click **Help Topics** to see the list of Help topics.

Configuring Applications to Use DCOM

You can use distributed component object model (DCOM) to integrate distributed applications in a network. A distributed application consists of multiple processes that cooperate to accomplish a single task.

The DCOM Configuration tool can be used to configure 32-bit COM and DCOM applications. To run this tool, click **Start**, click **Run**, and then type **dcomcnfg**.

Note
- Before you can use an application with DCOM, you must use DCOM Configuration to set application properties, such as security and location. On the computer running the <u>client application</u>, you must specify the location of the server application that will be accessed or started. For the <u>server application</u>, you must specify the user account that will have permission to access or start the application, and the user accounts that will be used to run the application.

To set the location of a DCOM application

1 Click here to open DCOM Configuration.

2 Click the application you want to configure, and then click **Properties**.

3 Click the **Location** tab, and specify the location of the application.

Note

▪ In most client-application configurations, you need to specify only the server-application.

To set permissions for a DCOM application

1 Click here [image] to open DCOM Configuration.

2 Click the application you want to configure, and then click **Properties**.

3 Click the **Security** tab.

4 Select **Use custom permissions** for launch, access, or configuration, and then click **Edit**.

5 If needed, click **Add** to add other user or group accounts to the **Name** box.

6 In **Name**, select the user or group whose permissions you want to set.

7 In **Type of Access**, select an access type for the selected user or group.

Notes and Tips
- To customize configuration permissions, in **Type of Access** select **Special Access**.
- To grant access, launch, or configuration permissions that apply to all applications installed on the computer, click the **Default Security** tab.

{button ,AL("a_add_perm_dcom;a_set_defperm;a_specacc_dcom")} <u>Related Topics</u>

To set the user account that will be used to run a DCOM application

1 Click here [icon] to open DCOM Configuration.

2 Click the application you want to configure, and then click **Properties**.

3 Click the **Identity** tab, and click the user account that will be used to run the application.

The application uses this account to start processes and access resources on other computers in the domain.

Note
- If the application is installed as a service, you can run the application using the built-in System account or a service account that you create.

To disable DCOM

1 Click here   to open DCOM Configuration.

2 Click the **Default Properties** tab.

3 Click to clear the **Enable Distributed COM on this computer** check box.

Note

      You can disable DCOM for a specific application by denying access or launch permissions to the built-in Network user account. To do this, click the **Applications** tab, select the application, click **Properties**, click the **Security** tab, and then click **Use custom access permissions**.

The application that initiates a request to a server application. Typically, client and server applications are on different computers.

The application that responds to requests from a client application. Typically, server and client applications are on different computers.

To add a user or group to the DCOM permissions list

1 In the **Registry Permissions** dialog box, click **Add**.

2 Select the users and groups in **Names**, and then click **Add**.

3 If needed, select a permission in **Type of Access**.

4 If necessary, use **Names** to add accounts to the permissions list:

   To add an entire group, click it and click **Add**.

   To see all the users on a selected computer or domain, click **Show Users**.

   To see the contents of a selected group, click **Members**.

   To add only some members of a group, select them in the **Group Membership** dialog box, and click **Add**.

Notes and Tips

   To add users and groups to the default permissions list for all applications, in DCOM Configuration click the **Default Security** tab and then click **Edit Default**.

   To add users and groups to the permissions list for one application, in DCOM Configuration select the application, click **Properties**, and then click the **Security** tab.

   If you don't know the domain of the user or group, click **Search**.

   Local groups are shown in **Names** for the computer or domain name that is followed by an asterisk (*). You can click another domain.

   Domains appear only if your computer belongs to a network domain that uses Windows NT Server. The domains shown have a trust relationship.

To set default permissions for all DCOM applications

1 Click here   🔲   to open DCOM Configuration.

2   Click the **Default Security** tab.

3 Click the **Edit Default** button for **Default Access Permissions**, **Default Launch Permissions**, or **Default Configuration Permissions**.

4 If needed, click **Add** to add other user accounts to the **Name** box.

5 In **Name**, select the user or group whose default permissions you want to change.

6 In **Type of Access**, select an access type for the selected user or group.

Tip

🔲   To customize configuration permissions, in **Type of Access** select **Special Access**.

{button ,AL("a_specacc_dcom;a_add_perm_dcom")} <u>Related Topics</u>

To set Special Access configuration permissions for DCOM

1 In DCOM Configuration, use the **Default Security** tab to set default permissions for all applications, or the **Applications** tab to edit permissions for one application (using **Properties** and **Security**).

2 In the **Registry Key Permissions** or **Registry Application Permissions** dialog box, respectively, in **Type of Access** select **Special Access**.

3 In the **Special Access** dialog box, select the type of control you want to assign to the selected user or group:

   To assign full control, click **Full Control (All)**.

   Or, to customize special access, click **Other**, and then select the types of access that you want to assign:
   - **Query Value** enables the user to read a value entry from the registry key.
   - **Set Value** enables the user to set value entries in the registry key.
   - **Create Subkey** enables a user to create subkeys on the registry key.
   - **Enumerate Subkeys** enables a user to identify the subkeys of the registry key .

   Notify enables a user to audit notification events from the key.

   Create Link enables a user to create a symbolic link in the key.

   Delete enables a user to delete the key.

   Write DAC enables a user to gain access to the key for the purpose of writing a discretionary ACL to the key.

   Write Owner enables a user to gain access to the key for the purpose of taking ownership of it.

   Read Control enables a user to gain access to the security information on the key.

Note

   Special Access is available only when assigning configuration permissions.

For information about using Registry Editor, see Registry Editor Help.

{button ,AL("a_set_defperm;a_dcom_perm")} Related Topics

Allows some users to connect to a resource or perform an action while preventing other users from doing so.

Identifies applications installed on this computer that support DCOM. The applications and services shown may be located on the local computer or on other computers (and are called remote server applications).

Click this to view or configure properties for the selected application.

Enables DCOM for all applications installed on this computer. Click to clear this if you want to disable DCOM for all applications. When DCOM is disabled, applications on this computer can't send or receive requests to or from applications on other computers.

Note

 You can disable DCOM for a specific application by denying access and launch permissions to the built-in Network user account. To do this, click the **Applications** tab, select the application, click **Properties**, click the **Security** tab, and then click **Use custom access permissions**. The application can send requests using DCOM but can't receive them from other computers.

Sets packet-level security on communications between applications. This system-wide default applies to all applications installed on the computer.

The settings, from lowest to greatest security, are as follows:

 None. No security-checking occurs on communications between applications.

Use **None** when **Anonymous** is selected in **Default Impersonation Level**.

 Default. The level of security is set to the default for the installed Authentication service. The default for the Windows NT Server Authentication service is **Connect**.

 Connect. Security-checking occurs for only the initial connection.

 Call. Security checking occurs on every call for the duration of the connection.

 Packet. The sender's identity is encrypted to ensure the authenticity of the sender.

 Packet integrity. The sender's identity and signature are encrypted to ensure the authenticity of the sender and to ensure that packets have not been changed during transit.

 Packet Privacy. The entire packet, including the data, and the sender's identity and signature, are encrypted for maximum security.

The level of permissions a client application grants to a server application to perform processing tasks on its behalf.

This system-wide default applies to all applications installed on the computer and should be set only if it has not already been set by the client application.

The settings, from lowest to greatest security, are as follows:

Anonymous. The server application performs processing tasks for the client without knowing the identity of the client application.

Identity. The server application can verify the identity of the client application.

Impersonate. The server application can impersonate the client application only by performing processing tasks as the client application. The server application can impersonate the client application only on the computer running the server application.

Delegate. The server application can perform processing tasks on another computer as the client application. The server application can act as the client application on the computer running the server application or other computers.

The Windows NT Server authentication service does not support **Delegate**.

Sets the server application to track the connected client applications. This may use more computer memory, but it ensures that a client application can't kill server processes by artificially forcing the reference-tracking number to 0.

Used to set the user accounts that you will allow or deny to access applications on this computer. This is a system-wide default that applies to all applications installed on the computer. **Default Security** settings determine whether or not you can override this option for individual applications.

Used to set the user accounts that you will allow or deny to start applications on this computer. This is a system-wide default that applies to all applications installed on the computer. **Default Security** settings determine whether or not you can override this option for individual applications.

Default Configuration Permissions defines those groups and users who are permitted to read or modify registry configuration information for DCOM applications. **Default Security** settings determine whether or not you can override this option for individual applications.

Indicates the name of the selected application.

If the application is to be run on a remote computer, indicates the name of that computer.

Indicates the type of application, including whether the application is on the local computer or on another computer in the network.

Indicates the path of the application.

Indicates that the application will run on the computer where the data is located. This is useful only if the client application provides a data file for the server application.

Indicates that the application will run on the local computer.

Indicates that the application will run on the specified computer.

Specifies the name of the computer where the application will run. You can type here or use **Browse** to specify a computer.

Click this to select a domain and then browse for a computer.

Indicates that the application will use the default access permissions, as set in **Default Security**. The application may override these settings.

Indicates that the application will use the access permissions that you set. Click **Edit** to change the access permissions.

Click this to give or deny user accounts permissions to access this application.

Indicates that the application will use the default permissions (as set in **Default Security**) to start the application.

Indicates that the application will use the launch permissions that you set. Click **Edit** to change the launch permissions.

Click this to give or deny user accounts permission to start this application.

Indicates that the application will use the default registry configuration permissions (as set in **Default Security**).

Indicates that the application will use the registry configuration permissions that you set. Click **Edit** to change the configuration permissions.

Click this to give or deny user accounts permission to read or modify registry configuration information for this application.

Specifies that the application will run using the security context of the user who is currently logged onto the computer (the interactive user). The application runs as this user in order to be authenticated in the domain. The interactive user may be the same as the launching user.

Note

If this is selected and a user is not logged on, the application will not start.

Specifies that the application will run using the security context of the user who started the application (the launching user). The application runs as this user in order to be authenticated in the domain. The launching user may be the same as the interactive user.

Note

The Windows NT Server authentication service does not allow an identity that is passed from another computer over the network to be used to access network resources.

Specifies that the application will run using the security context of the specified user account. The application runs as this user in order to be authenticated in the domain.

Specifies the user account that will be used to run the server application. The user account can be a user account or a service account you create to run services. You can type here or use **Browse** to specify an account name.

Click this to choose a user account from a list.

The logon password for the specified user account.

Type the logon password for the specified user account again to confirm it.

The server application will run using the security context of the built-in System account. This is available only for applications that are installed as a service.

Registry Value Permissions

Used to set and change permissions for groups and users. You can specify which users can access and launch the application.

Click the following for information about this dialog box:

Registry value

Owner

Name

Type of Access

Add

Remove

Registry value

Displays the value of HKEY_CLASSES_ROOT for which you are assigning permissions.

Owner

Identifies the administrator of this computer.

Name

Displays the names of groups and users and their current permissions. You can change permissions for selected accounts using **Type of Access**.

Type of Access

Select one of the types of access listed in **Type of Access**.

Allow Access permits the user to access applications that do not provide their own settings.

Allow Launch permits the user to launch applications that do not provide their own settings.

Deny Access prevents the user from accessing applications that do not provide their own settings.

Deny Launch prevents the user from launching applications that do not provide their own settings.

Add

Used to add selected groups or users to the permissions list.

Remove

Used to remove selected groups or users from the permission list.

Registry Key Permissions

Used to set and change permissions for groups and users. You can specify which users can read or modify the HKEY_CLASSES_ROOT registry key, or you can customize the type of user access.

Click the following for information about this dialog box:

Registry Key
Owner
Name
Type of Access
Add
Remove

Registry Key

Displays the name of the key that you are permitting access to.

Name

Lists the groups who currently have permission to access HKEY_CLASSES_ROOT.

Type of Access

Select one of the types of access listed in **Type of Access**.

Read enables the user to read the key but not to save any changes to the key.

Full Control enables the user to access, edit, and to take ownership of the key.

Special Access enables you to customize permissions for the selected users or groups.

Special Access

Used to set default access permissions for users to read or change HKEY_CLASSES_ROOT and its subkeys.

Click the following for more information about this dialog box.
Registry Key
Name
Full Control (All)
Other

{button ,AL("a_specacc_dcom")} Related Topics

Registry Key

Identifies the registry key you are setting special access permissions for.

Name

Identifies the group or user to whom you are assigning special access permissions.

Other

Click to specify the access you want to assign for HKEY_CLASSES_ROOT.

Query Value enables the user to read a value entry from the registry key.

Set Value enables the user to set value entries in the registry key.

Create Subkey enables a user to create subkeys on the registry key.

Enumerate Subkeys enables a user to identify the subkeys of the registry key .

Notify enables a user to audit notification events from the key.

Create Link enables a user to create a symbolic link in the key.

Delete enables a user to delete the key.

Write DAC enables a user to gain access to the key for the purpose of writing a discretionary ACL to the key.

Write Owner enables a user to gain access to the key for the purpose of taking ownership of it.

Read Control enables a user to gain access to the security information on the key.

Full Control (All)

Assigns full control of the registry key to the selected user or group.

Special Access

Used to set access permissions for users to read or change the AppID key for this application as well as all associated CLSID keys and their subkeys.

Click the following for more information about this dialog box.

Registry Application

Name

Full Control (All)

Other

{button ,AL("a_specacc_dcom")} Related Topics

Registry Application

The application whose registry configuration permissions you are setting.

Select Domain

Used to select a domain and then browse for a computer.

 Domain

 Select Domain

Domain

If you know the name of the domain you want, you can type it in **Domain**. Or, if you select a domain in **Select Domain**, that domain appears in **Domain**.

Select Domain

 Double-click a domain to see the computers in the domain, and then select a computer to use for the location to run the DCOM-configured application.

Registry Key Permissions

Used to set and change permissions for groups and users. You can specify which users can change registry configuration for the application.

Click the following for information about this dialog box:

Registry Application
Owner
Name
Type of Access
Add
Remove

{button ,AL("a_add_perm_dcom;a_specacc_dcom")} Related Topics

Type of Access

Select one of the types of access listed in **Type of Access**.

Read enables the user to read the application but not to save any changes.

Full Control enables the user to access, edit, and to take ownership of the application.

Special Access enables you to customize permissions for the selected users or groups.

Add Users and Groups

Used to add a group or user to the permissions list for a DCOM application.

Click the following for information about this dialog box:

List Names From
Names
Add
Show Users
Members
Search
Add Names
Type of Access

{button ,AL("a_add_perm_dcom")} Related Topics

List Names From

Displays the domain or computer of the groups shown in **Names**. Local groups are shown in **Names** for the computer or domain name that is followed by an asterisk (*).

You can see the display for another domain or computer by selecting it in **List Names From**.

Names

Displays the groups (and users, if you clicked **Show Users**) for the current domain or computer. By default, only groups are listed.

You can select a user in **Names** and click **Add** to add it to **Add Names**.

Add

Adds selected groups or users to **Add Names**.

Show Users

When selected, lists the user accounts belonging to the domain or computer in **List Names From**. By default, only groups are listed.

Members

Displays the contents of the selected group.

Search

Used to find the domain to which a group or user belongs.

You must know the domain for an account in order to add it to the permissions list.

Add Names

Displays the names of groups and users you are adding to the permissions list. You can add groups and users to this list by selecting them in **Names** and clicking **Add**. When you click **OK**, the accounts in **Add Names** are added to the DCOM permissions list.

Type of Access

Displays a list of available permissions. The permission you select here applies to the groups and users in **Add Names**.

Local Group Membership

Displays the members of the local group selected in the **Add Users and Groups** dialog box.

You can add the entire group to **Add Names** by clicking **Add**. Or, you can select only the members you want, and then click **Add**.

On a Windows NT Server network, global groups that are members of a local group appear in the list. To see the members of a global group, select it and click **Members**.

Global Group Membership

Displays the members of the global group selected in either the **Add Users and Groups** or the **Local Group Membership** dialog box. You can add the entire group to **Add Names** by clicking **Add**. Or, you can select only the members you want, and then click **Add**.

Find Account

Used to locate the domain of an account on a Windows NT Server network.

Click the following for information about the dialog box:

Find User or Group
Search All
Search Only In
Search
Add

Find User or Group

Used to enter the group or user name for the account you want to find.

Search All

Sets a search to look in all listed domains.

Search Only In

Restricts a search to the selected domains.

Search

Starts the search for the specified group or user account.

Add

Closes the **Find Account** dialog box and adds the users and groups selected in **Search Results** to **Add Names** in the **Users and Groups** dialog box.

Find Account

Used to locate the domain of an account on a Windows NT Server network.

Click the following for information about the dialog box:

 Find User or Group
 Search All
 Search Only In
 Search
 Add

Find User or Group

Used to enter the user name for the account you want to find.

Add

Closes the **Find Account** dialog box and adds the user selected in **Search Results** to **Add Name** in the **Browse for Users** dialog box.

Browse for Users

Used to find a user account to run the application being configured for distributed use.

Click the following for information about the dialog box:

List Names From
Names
Add
Members
Search
Add Name

Names

Enables you to select the Windows NT domain from which to select a user or group.

Add

Enables you to add the selected user or group to the **Add Name** box.

Members

Enables you to select from the members of a group.

Search

Enables you to search in one or more domains for the user or group.

Add Name

Shows the user account to be permitted to run the application. You can type a user name or select one from **Names**.