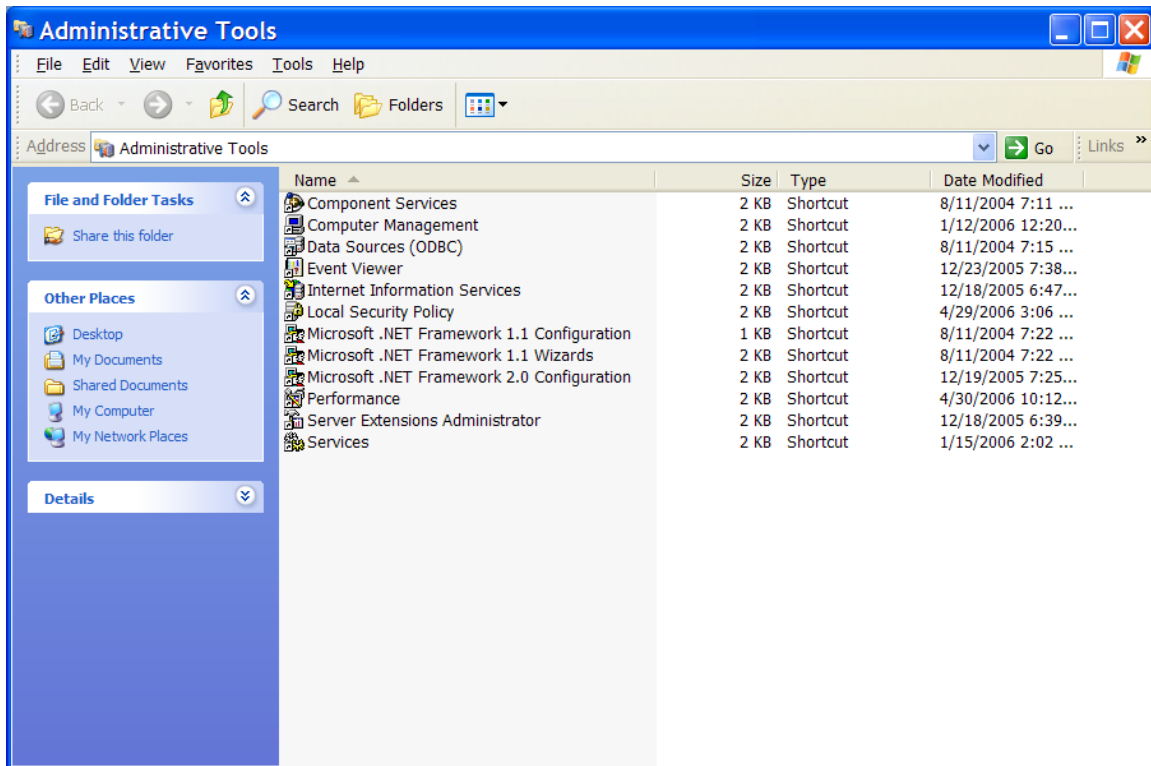


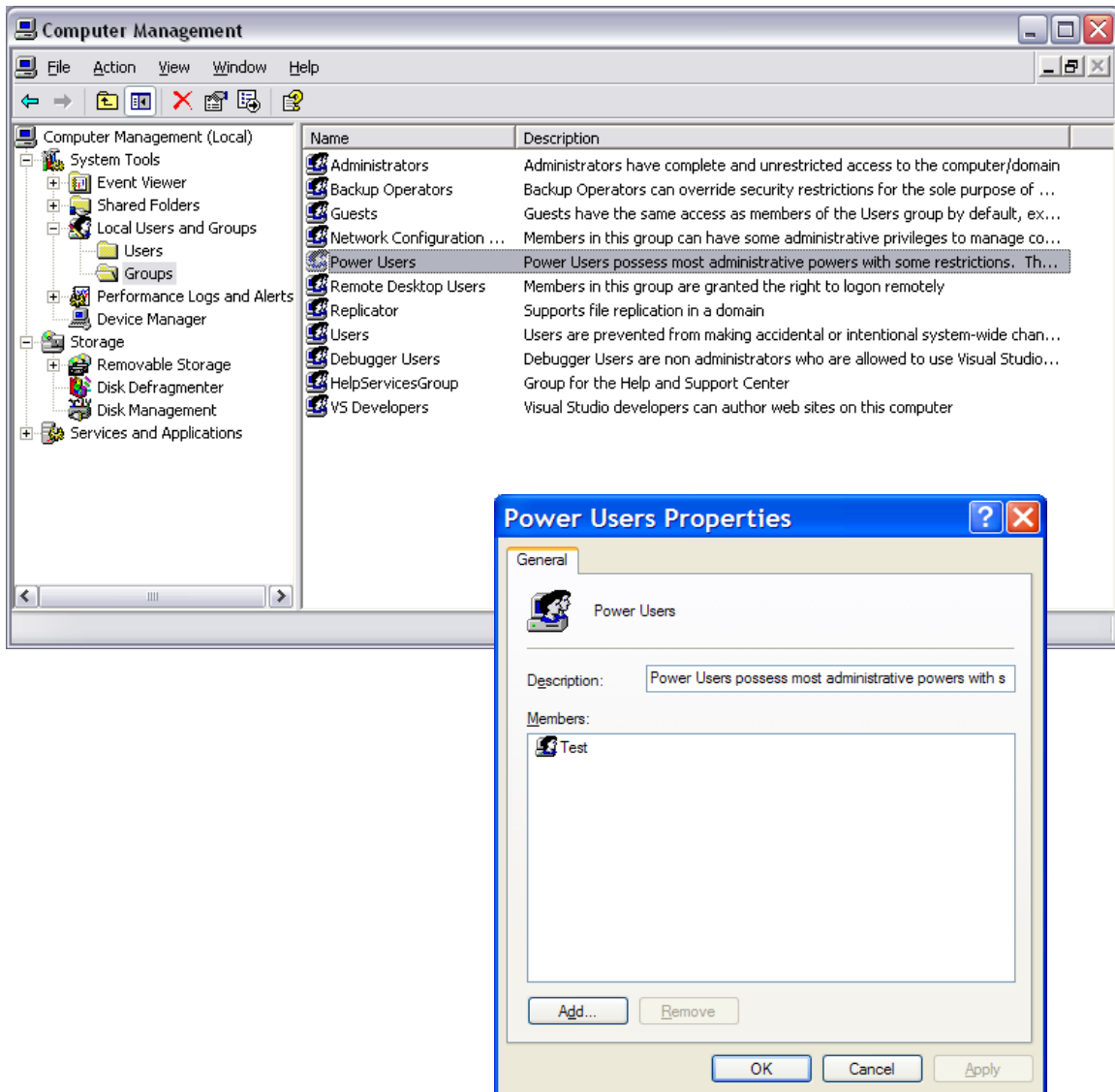
# ***Windows and .Net Security Tools***

Jim Fawcett  
CSE686 – Internet Programming  
Summer 2006

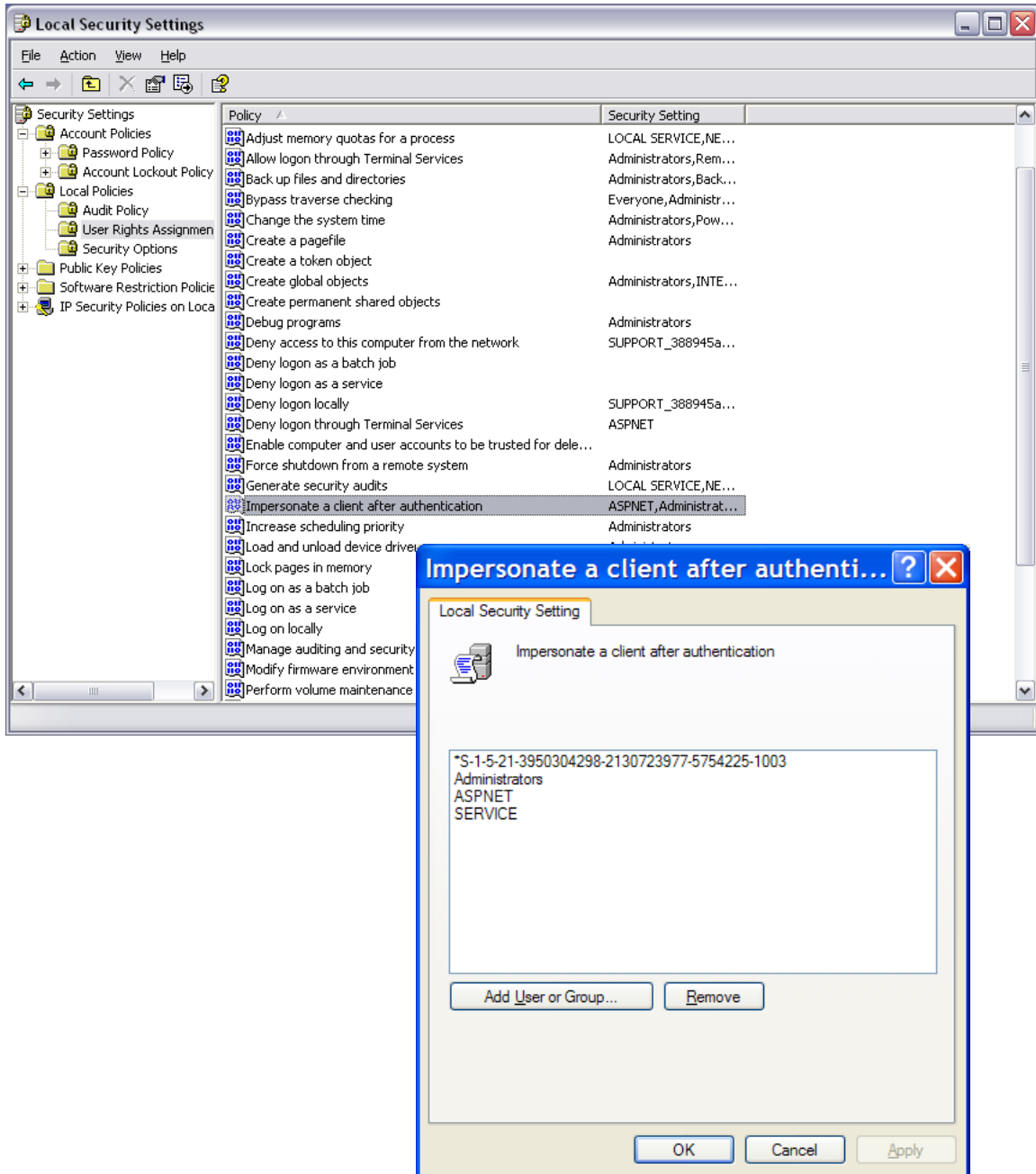
# Windows and .Net Security Tools



# Windows User and Group Management



# Windows Local Policy Management



# Access Control for Secured Objects

The screenshot shows the Windows XP Help and Support Center interface. The search bar at the top contains the text "view permissions". Below the search bar, there are navigation options: "Back", "Index", "Favorites", "History", "Support", and "Options". The search results are displayed in a list on the left side of the window, with 15 results found for "view permis...". The top result is "Glossary", followed by "Schtasks", "Access control overview", "Bootcfg", and "Set, view, change, or remove special permissions for files and folders". The right side of the window displays the "Access control overview" article, which explains the process of authorizing users, groups, and computers to access objects on the network. It defines "Permissions" and lists common permissions such as Read, Modify, Change owner, and Delete.

**Help and Support Center**

Search

Set search options Windows XP Professional

Search only Protecting your PC: security basics  
 Search within previous results

**Search Results** Tips

15 results found for **view permis...** Stop

Suggested Topics (0 results)

Full-text Search Matches (15 results)

1. [Glossary](#)
2. [Schtasks](#)
3. [Access control overview](#)
4. [Bootcfg](#)
5. [Set, view, change, or remove special permissions for files and folders](#)
6. [Set, view, change, or remove file and folder permissions](#)
7. [Permissions](#)
8. [Set or remove permissions for a printer](#)
9. [Changing inherited permissions](#)
10. [File and Folder permissions](#)
11. [View effective permissions for files and folders](#)
12. [Effective permissions](#)
13. [Accessing Windows 2000 Server Help remotely](#)
14. [Eventtriggers](#)
15. [Setting permissions](#)

Microsoft Knowledge Base (0 results)

## Access control overview

Access control is the process of authorizing users, groups, and computers to access objects on the network. Key concepts that make up access control are:

### Permissions

**Permissions** define the type of access granted to a user or group for an object or object property. For example, the Finance group can be granted Read and Write **permissions** for the file *payroll.dat*.

**Permissions** are applied to any secured objects such as files, Active directory objects, or registry objects. **Permissions** can be granted to any user, group, or computer. It is a good practice to assign to groups.

You can assign **permissions** for objects to:

- Groups, users, and [special identities](#) in the domain.
- Groups and users in that domain and any trusted domains.
- Local groups and users on the computer where the object resides.

The **permissions** attached to an object depend on the type of object. For example, the **permissions** that can be attached to a file are different from those that can be attached to a registry key. Some **permissions**, however, are common to most types of objects. These common **permissions** are:

- Read **permissions**
- Modify **permissions**
- Change owner
- Delete

When you set up **permissions**, you specify the level of access for groups and users. For example, you can let one user read the contents of a file, let another user make changes to the file, and prevent all other users from accessing the file. You can set similar

# Access Control for Secured Objects

The screenshot shows the Windows XP Help and Support Center interface. The search bar contains the text "view permissions". The search results are displayed in a list on the left side of the window. The main content area on the right displays the article "Security identifiers" with a sub-section for "Well-known security identifiers (special identities)". This section contains a table with two columns: "Well-known SID" and "Description".

**Search Results**

15 results found for **view permis...** [Stop](#)

Suggested Topics (0 results)

Full-text Search Matches (15 results)

1. [Glossary](#)
2. [Schtasks](#)
3. [Access control overview](#)
4. [Bootcfg](#)
5. [Set, view, change, or remove special permissions for files and folders](#)
6. [Set, view, change, or remove file and folder permissions](#)
7. [Permissions](#)
8. [Set or remove permissions for a printer](#)
9. [Changing inherited permissions](#)
10. [File and Folder permissions](#)
11. [View effective permissions for files and folders](#)
12. [Effective permissions](#)
13. [Accessing Windows 2000 Server Help remotely](#)
14. [Eventtriggers](#)
15. [Setting permissions](#)

Microsoft Knowledge Base (0 results)

## Security identifiers

Security identifiers (SIDs) are numeric values that identify a user or group. For each access control entry (ACE), there exists a SID that identifies the user or group for whom access is allowed, denied, or audited.

### Well-known security identifiers (special identities)

Well-known SID	Description
Anonymous Logon (S-1-5-7)	A user who has connected to the computer without supplying a user name and password.
Authenticated Users (S-1-5-11)	Includes all users and computers whose identities have been authenticated. Authenticated Users does not include Guest even if the Guest account has a password.
Batch (S-1-5-3)	Includes all users who have logged on through a batch queue facility such as task scheduler jobs.
Creator Owner (S-1-3-0)	A placeholder in an inheritable access control entry (ACE). When the ACE is inherited, the system replaces this SID with the SID for the object's current owner.
Creator Group (S-1-3-1)	A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's current owner.
Dialup (S-1-5-1)	Includes all users who are logged on to the system through a dial-up connection.
Everyone (S-1-1-0)	On computers running Windows XP Professional, Everyone includes Authenticated Users and Guest. On computers running earlier versions of the operating system, Everyone includes Authenticated Users and Guest plus Anonymous Logon.

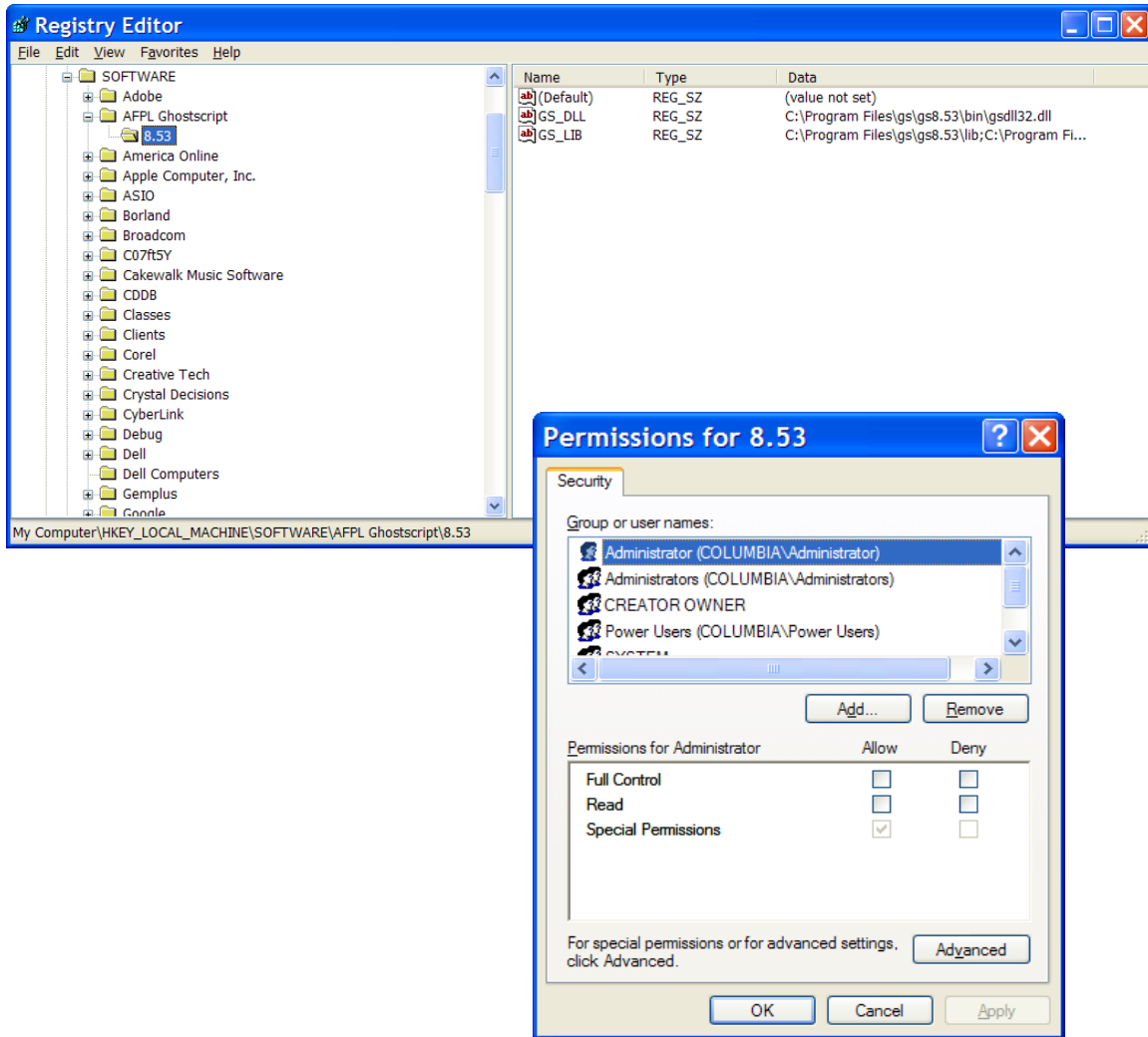
# Access Control for Secured Objects

The image shows a Windows Explorer window displaying the contents of the folder `C:\SU\CSE686\code\DataWizardDemos\CommandWizard`. The file `CoverSheet.doc` is selected. A 'CoverSheet.doc Properties' dialog box is open, showing the 'Security' tab. The 'Group or user names' list includes 'Administrators (COLUMBIA\Administrators)' and 'Everyone'. The permissions for 'Administrators' are:

Permissions for Administrators	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modify	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read & Execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Special Permissions	<input type="checkbox"/>	<input type="checkbox"/>

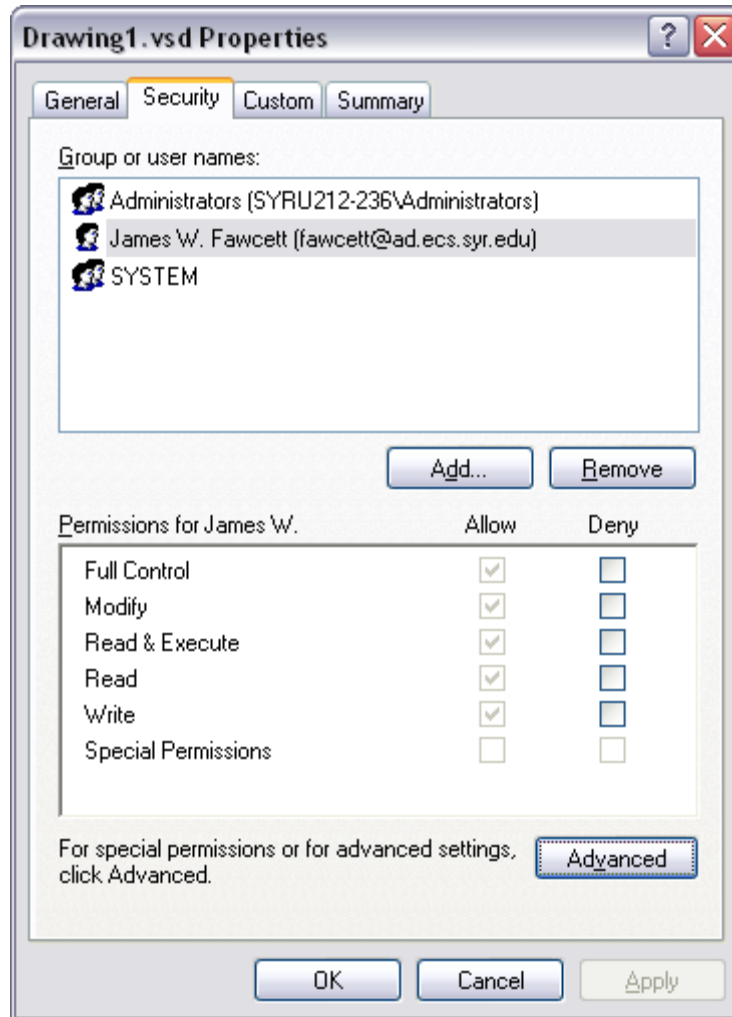
Buttons for 'Add...', 'Remove', 'Advanced', 'OK', 'Cancel', and 'Apply' are also visible.

# Access Control for Secured Objects

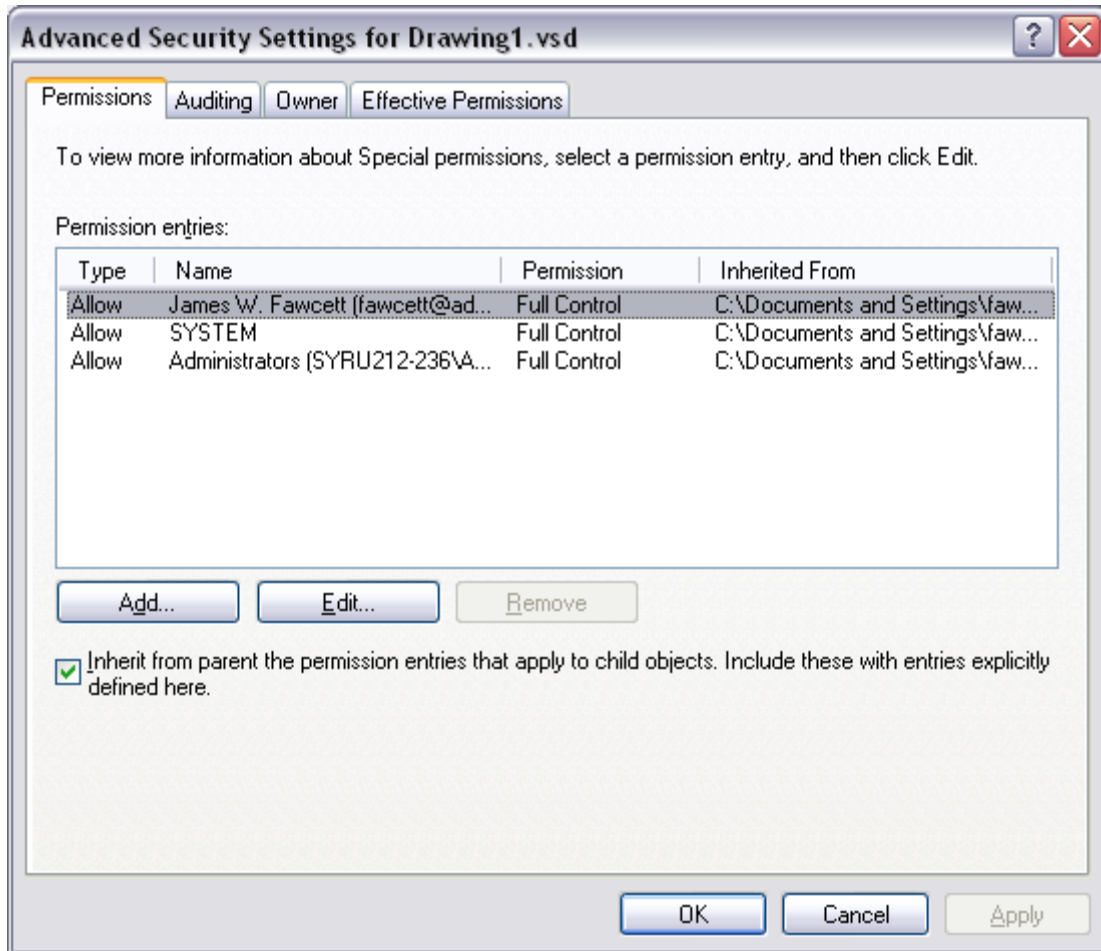




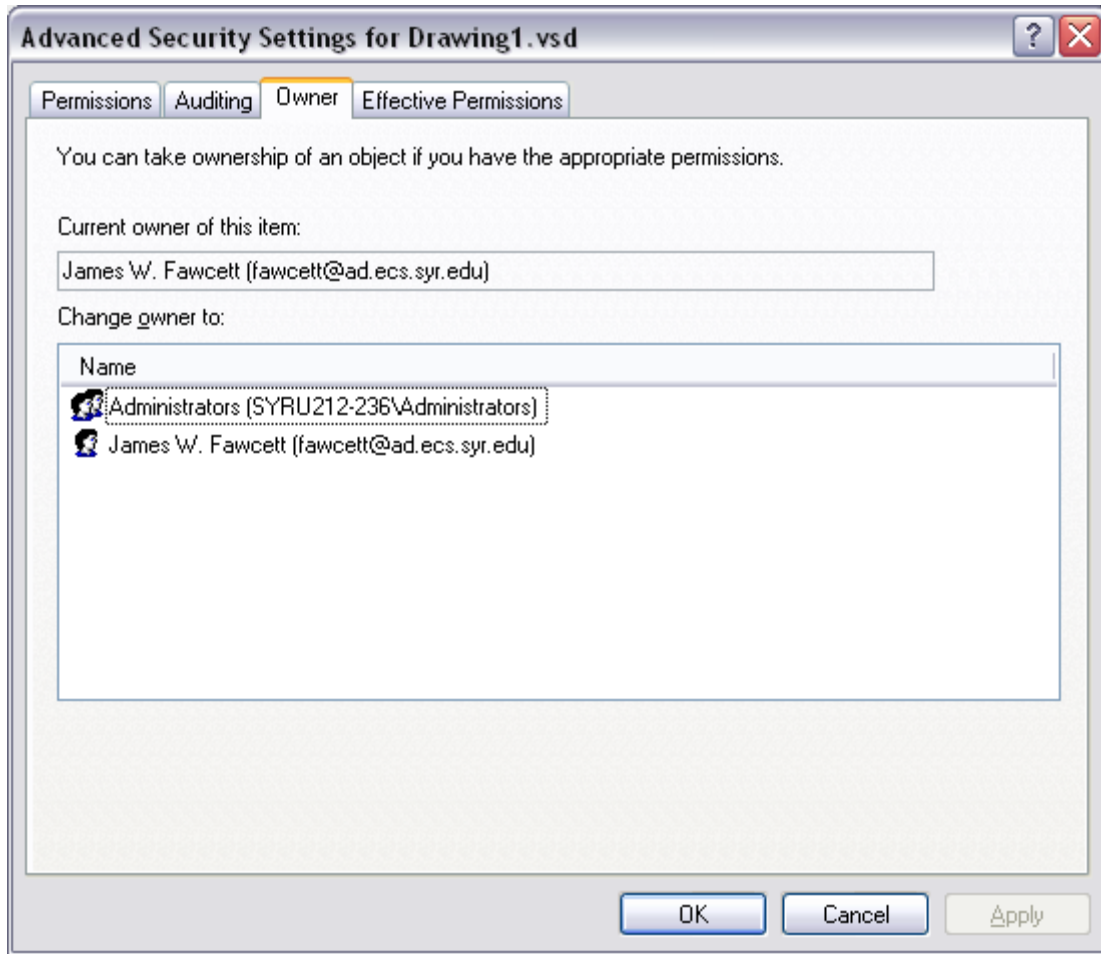
# Access Control for Secured Objects



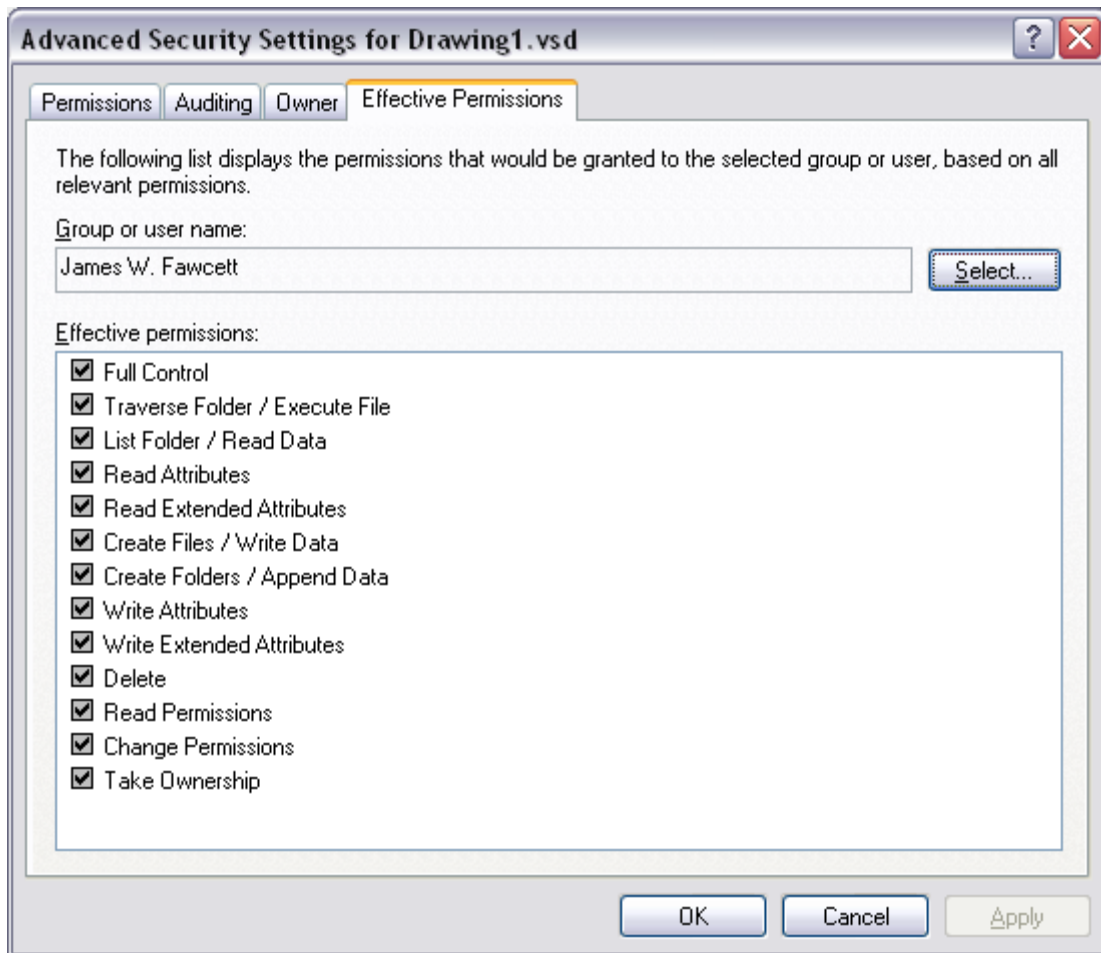
# Access Control for Secured Objects



# Access Control for Secured Objects



## ***Access Control for Secured Objects***





# .Net Security Administration

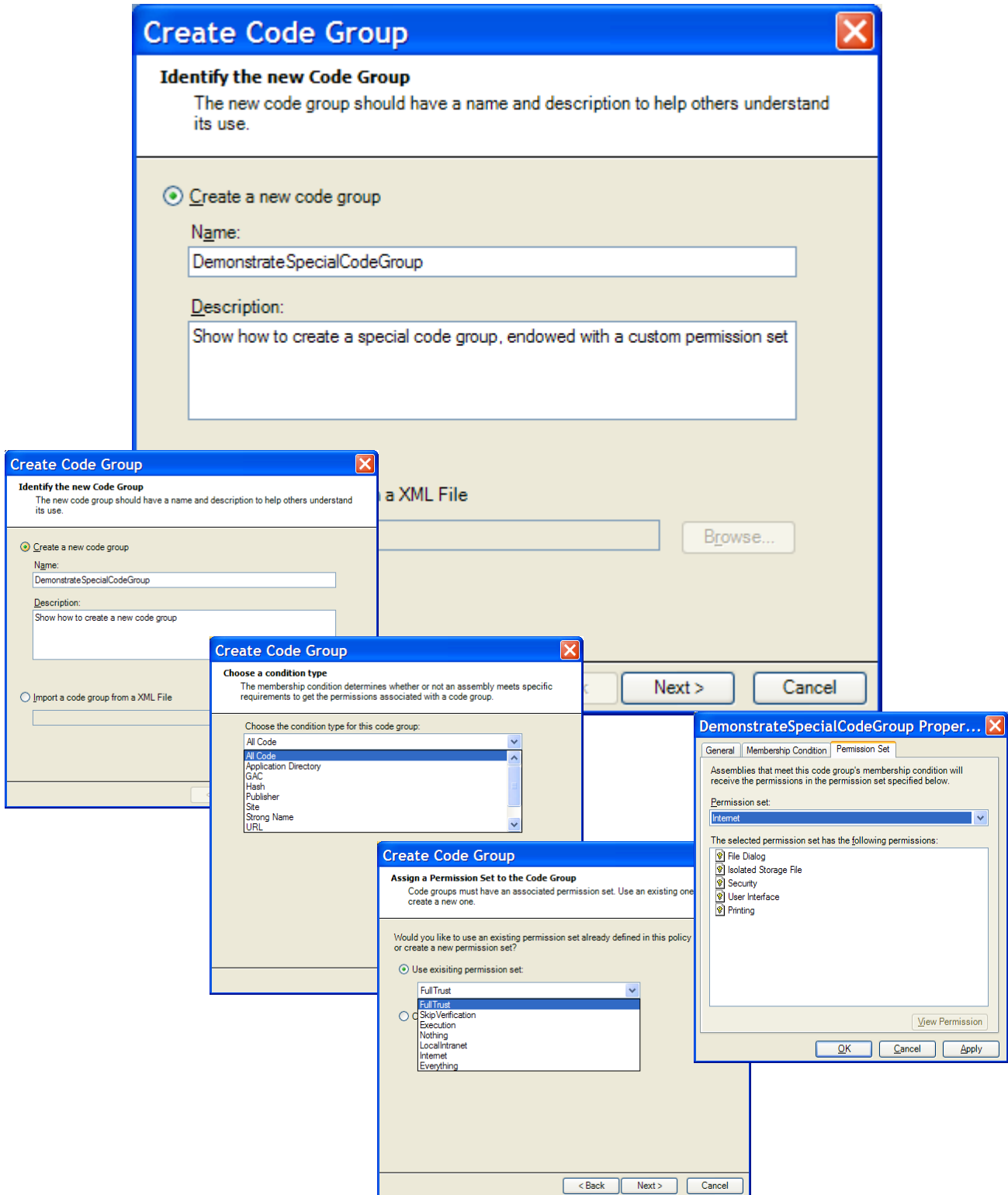
The screenshot displays the .NET Framework 2.0 Configuration console. The left pane shows a tree view of the configuration hierarchy, with the 'Internet' zone selected under the 'Machine' code group. The right pane lists the permissions for this zone, including 'SQL Client'. Two dialog boxes are overlaid on the console:

- SQL Client Properties**: Shows 'Permission Settings' with two radio buttons: 'Grant assemblies no access to Microsoft SQL Servers' (unselected) and 'Grant assemblies unrestricted access to Microsoft SQL Servers' (selected). Buttons for 'OK', 'Cancel', and 'Apply' are at the bottom.
- Web Access Properties**: Shows 'Permission Settings' with two radio buttons: 'Grant assemblies access to the following Web sites:' (unselected) and 'Grant assemblies unrestricted access to Web sites' (selected). The first option includes a table for specifying host access:

Host	Accept	Connect
	<input type="checkbox"/>	<input type="checkbox"/>

Buttons for 'Delete Entry', 'OK', 'Cancel', and 'Apply' are at the bottom of the dialog.

# .Net Security Administration



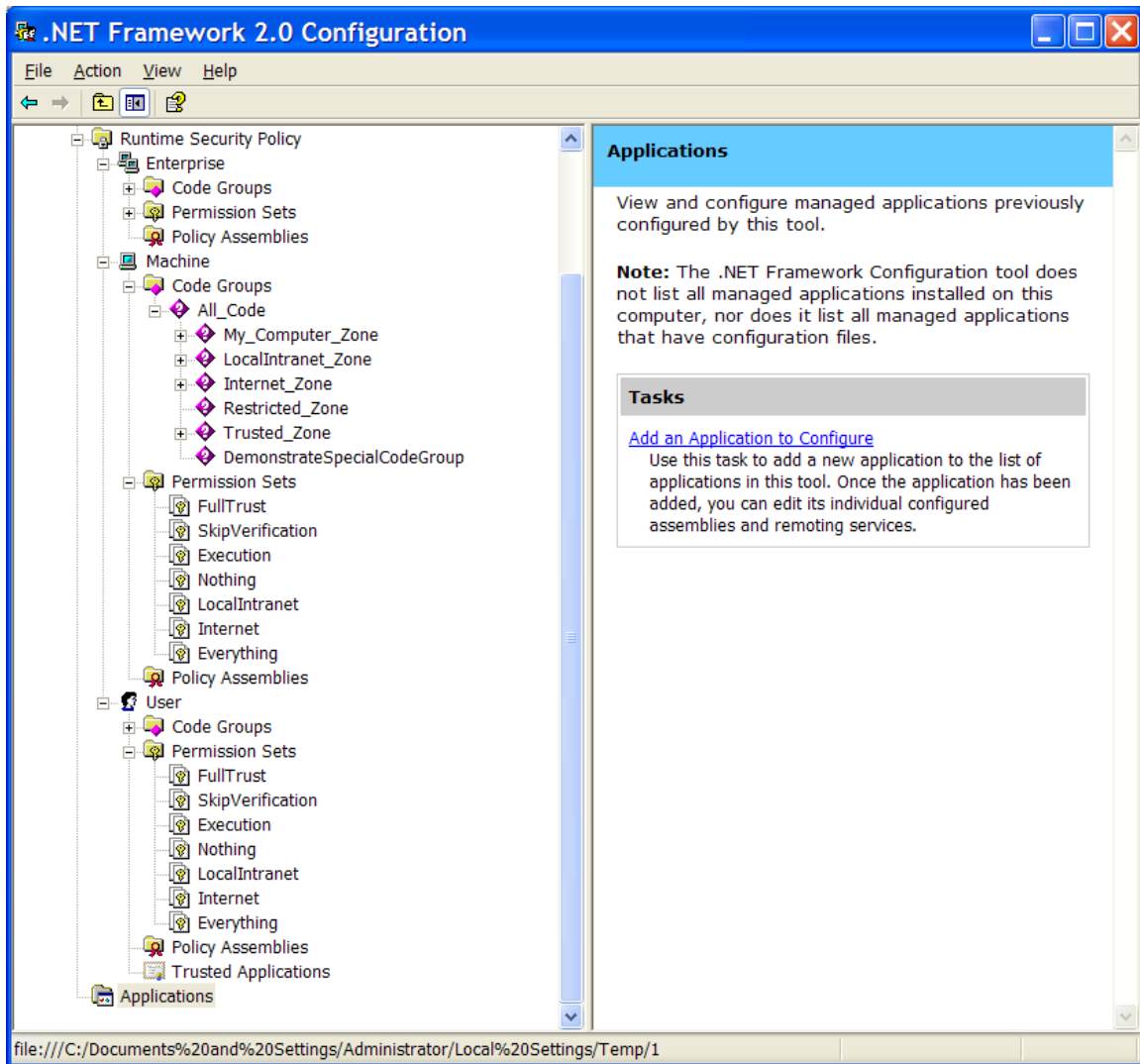
# .Net Security Administration

The screenshot displays the .NET Framework 2.0 Configuration console. The left pane shows a tree view of the Runtime Security Policy configuration. The right pane shows a list of assemblies and their public keys.

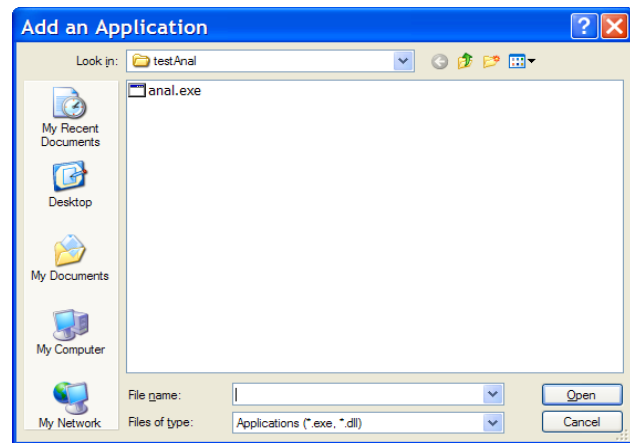
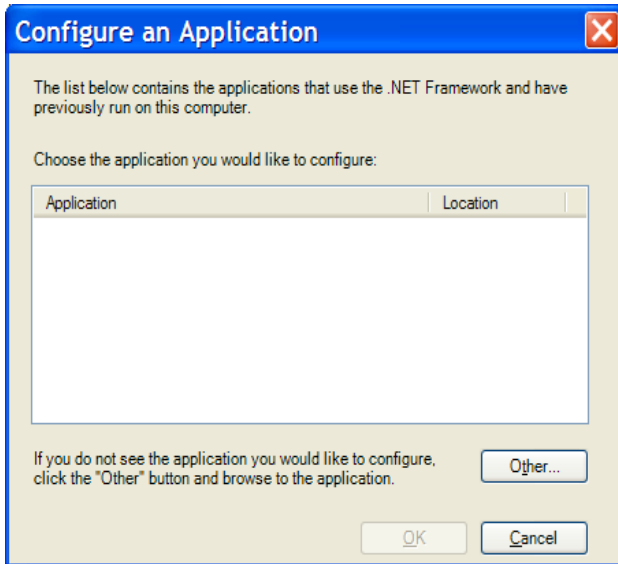
Assembly Name	Public Key
mscorlib.resources	b77a5c56
System	b77a5c56
System.resources	b77a5c56
System.Xml	b77a5c56
System.Xml.resources	b77a5c56
System.Windows.Forms	b77a5c56
System.Windows.Forms.resources	b77a5c56
System.Data	b77a5c56
System.Data.resources	b77a5c56
System.Security	b03f5f7f1
System.Security.resources	b03f5f7f1
System.Drawing	b03f5f7f1
System.Drawing.resources	b03f5f7f1
System.Messaging	b03f5f7f1
System.Messaging.resources	b03f5f7f1
System.ServiceProcess	b03f5f7f1
System.ServiceProcess.resources	b03f5f7f1
System.DirectoryServices	b03f5f7f1
System.DirectoryServices.resources	b03f5f7f1
System.Deployment	b03f5f7f1
System.Deployment.resources	b03f5f7f1



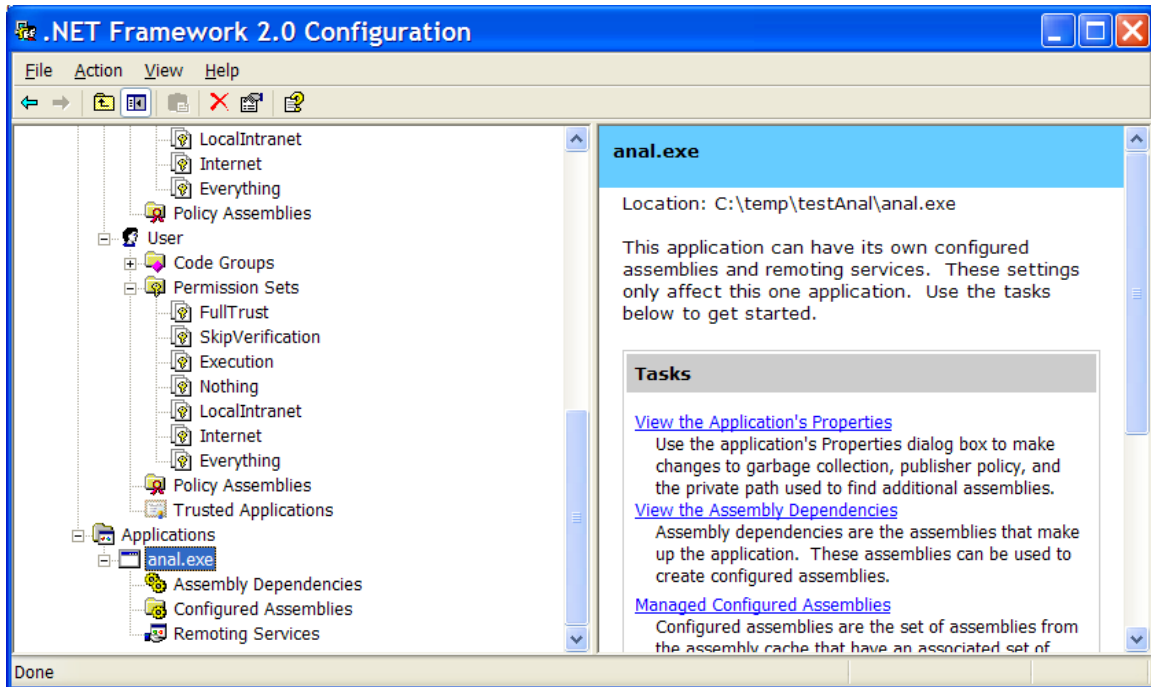
# .Net Security Administration



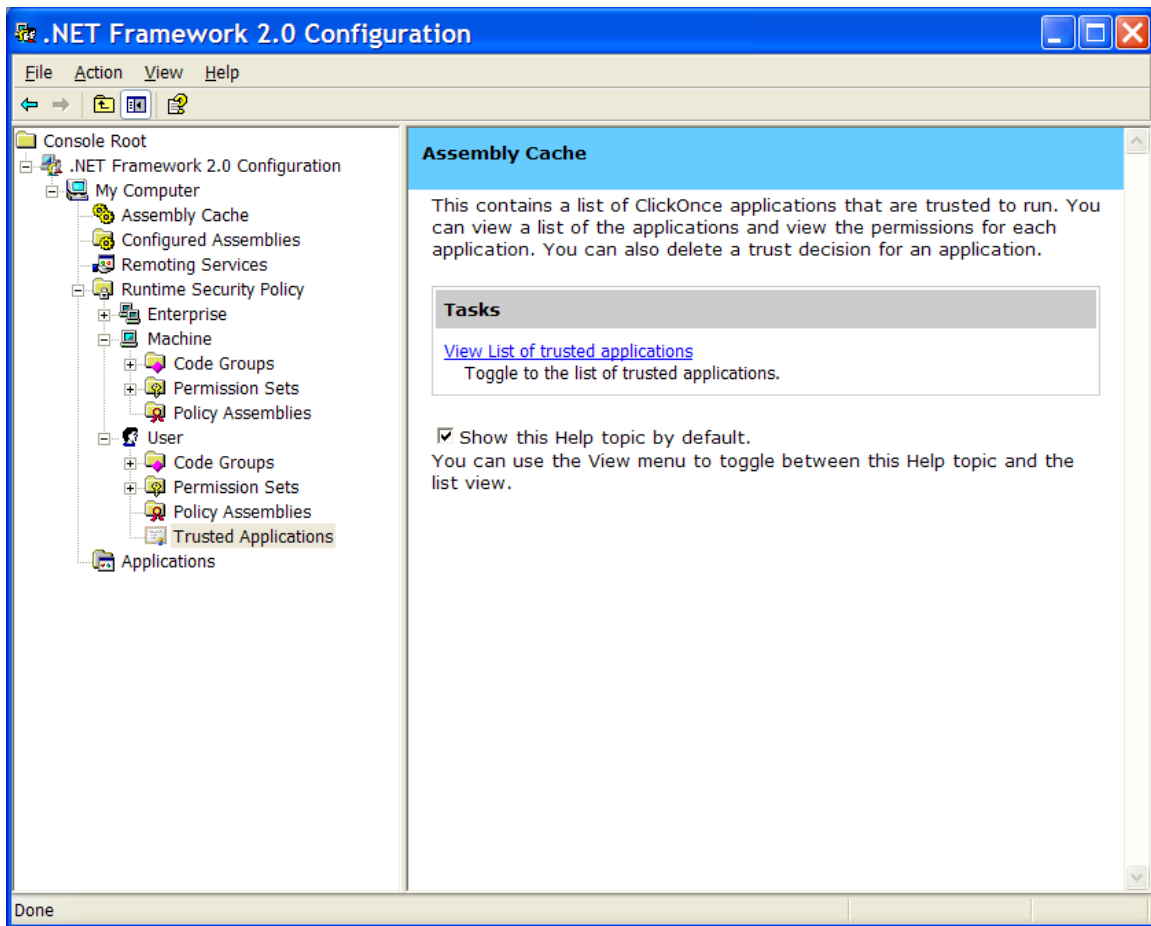
# *.Net Security Administration*



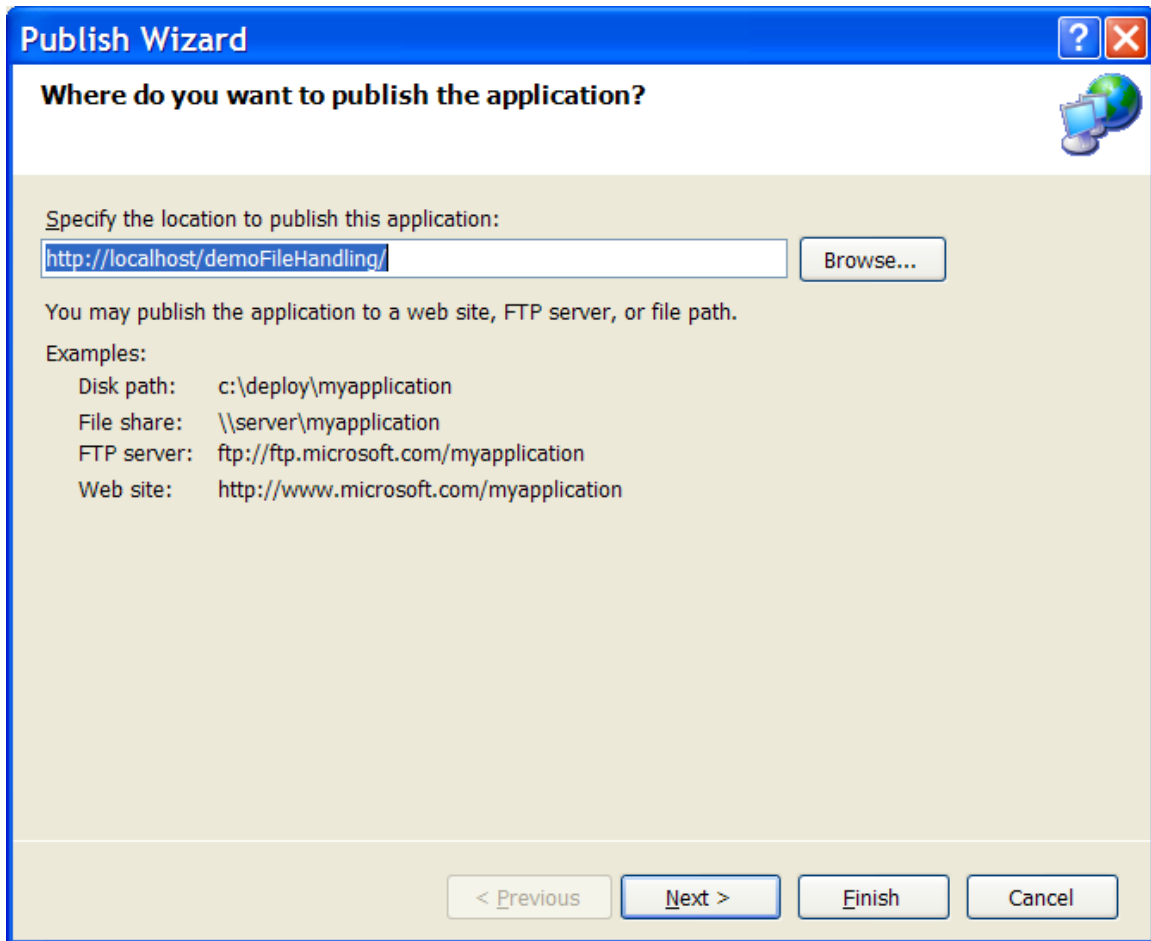
# *.Net Security Administration*



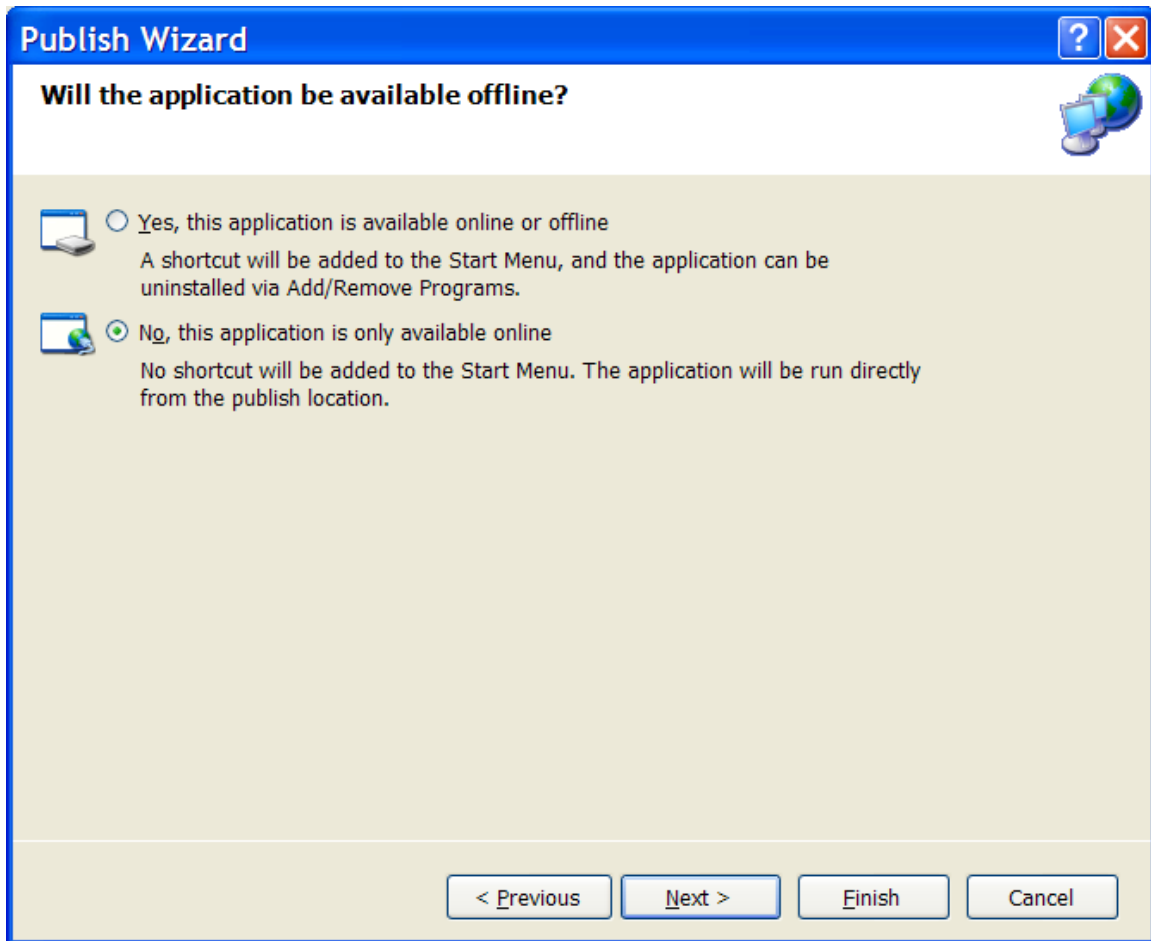
# *.Net Security Administration*



# *.Net Click Once Deployment*



# *.Net Click Once Deployment*



# .Net Click Once Deployment

