

## Article : Code Access Security Part – 2 (.Net Framework Tools Series)

**Source:**

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet.mobile/2004-11/0019.html>

---

**From:** Namratha Shah \Nasha\ (*namratha1\_at\_gmail.com*)

**Date:** 11/06/04

Date: Sun, 7 Nov 2004 00:20:55 +0530

Hey Guys,

Before we start with our sample app we need to view the security configuration files on the machine. You will find them under

<drive>\WinNT\Microsoft.NET\Framework\<version>\Config

Enterprise Level Security configuration file is :- enterprise.config

Machine Level Security configuration file is :- security.config

You will find the user security configuration file in

<drive>:\Documents and Settings\<userprofile>\Application

Data\Microsoft\CLR Security Config\v1.1.4322\security.config

Let us now create our sample app. In this we will create a Windows Forms application which will try and read and write to the local disk.

- 1) Go to VS.NET create a new Win App.
- 2) On the Form Place one text box And one button Make the multiline property of the text box true.
- 3) In the click event of the button write the following piece of code which writes to a file whatever is written in the text box.

```
StreamWriter sWriter = new StreamWriter("C://MyTextFile.txt");
```

```
sWriter.Write(textBox1.Text);
```

```
sWriter.Flush();
```

```
sWriter.Close();
```

4) If you run this from your machine you will be able to create the file and write the textbox contents in it.

Well Currently this code is executing on the local machine cause in the local machine policy MyComputer Zone has Full trust permission set.

Check it out by typing `caspol -m -lg`

Suppose if we were to run this same app from a local network share then the Intranet code access group does not have the permission to write to the local hard disk.

5) Place the exe on a network share and execute it. It should give you a Security Permission Exception.

6) Modify your code to catch the exception and give a user friendly message. Run the file again from the network share.

Suppose that we wanted this application to run from the network share. For that we will need to change the Intranet Permission set.

```
caspol.exe -chggroup 1.2 FullTrust. // This command tells to fully trust all the intranet applications
```

Note : Please be extremely careful to change the permission sets as this can cause a lot of viruses and other spy wares to come in. Change the permission sets only if you have not made any custom changes to your PC. After changing the permission set use

```
caspol.exe -reset command this resets the .NET default permission sets for all code groups
```

Thus in this way we can prevent malicious code to access our resources.

Lets now explore the other options of `caspol.exe`

### Turning the Security On/Off

It is possible to turn the .Net Security Off if so for any reason. By

default it is On.

```
caspol.exe -security off // to turn off the .Net security
```

To reset the security to .Net default security use

```
caspol.exe -reset
```

To create a new code group

```
caspol.exe –addgroup 1.3 –site www. <name of the site> /// this will add full trust for any content from this site.
```

To create a code group under intranet with fulltrust to a particular share on the network

```
caspol.exe –addgroup 1.2 –url file:///\\<machinename>/<foldername>/* FullTrust
```

To remove a code group give the codegroup number (as shown in the list groups) with –remgroup option

```
caspol.exe –remgroup 1.3.2
```

To change the code group's permission( we just sw above when we changed the permission for our intranet code group)

```
caspol.exe –chggroup 1.2 FullTrust
```

You can add code group for a particular strong name E.g. If you have an application MyApp.exe and you want any version of this application have FullTrust you can achieve that by using the a similar command

```
caspol.exe –addgroup 1 –strong –file \bin\debug\MyApp.exe –noname –noversion FullTrust
```

This command will a new strong Name code group. You can view it by giving caspol –lg command.

You will see that are already 2 strong name code groups installed by default. They belong to Microsoft and ECMA.

— Please post your queries and comments for my articles in the usergroup for the benefit of all. I hope this step from my end is helpful to all of us.

Regards,

Namratha (Nasha)