Sandbox

USER MANUAL

Overview

The sandbox is a windows GUI application. It has Program setup tab and permission setup tab. This current Sandbox version contains thirteen (13) permissions options.

Execution permission is set active at default. This means that any application called through the Sandbox should be executed except where other permissions are required to be set. Although, this execute permission can be disabled on the Sandbox permission tab view.

Features of the Sandbox GUI

Application Menus

There are two (2) menus on the Sandbox application:

1. File Menu
   This comprises of the following Menu Items:
   a. New: This can be used to refresh the input / text fields on the Program Call Tab.
   b. Open: This can be used to run the application whose path is provided in the Program Path field.
   c. Close: This can be used to close the Sandbox application.
2. Help Menu
   This is made up of the following Menu Items:
   a. View Help: This displays a dialog page which contains the full user manual for the Sandbox application.
   b. Author: This provides details of the author of this Sandbox version.

Sandbox Program Call Tab

This tab holds all the necessary fields and command for running an application through the Sandbox application. Program Call Tab holds the following controls:

1. Program Path Field: This displays the full folder path of the application to be called through the sandbox application.
2. Browse button: This is used to launch a folder dialog that can be used to locate the application folder.
3. Class Path field/textbox: This should hold the class path / package path where the method / entry point is. E.g. Bird.Flamingo
4. Entry Point field/textbox: This field optional and it is where the main method to run is provided on the Sandbox. E.g. Main. If not provided by user on the GUI, the EntryPoint will be picked from the Assembly
5. Arguments field/textbox: This is field that holds any argument(s) required by the untrusted application.
6. File path: This is used to provide the path to the file that requires read, write or append permission on the untrusted application interface.
7. Clear Buttons: All the clear buttons are used to clear any input / text field beside it.

8. Run Button: The Run button is used to call / run the application whose path has been provided in the Program path field and all other fields have been well populated accordingly.

Permission Set Tab

There are thirteen (13) permissions made available on this Sandbox version. They include:

1. Read Environment
2. Execute
3. UI Permission
4. File Read
5. File Write
6. File Append
7. File Dialog Open
8. File Dialog Save
9. Web / Internet
10. Web Browser
11. Socket
12. DNS
13. Printing

1. Read Environment: This uses the DotNet framework 4.8 EnvironmentPermission class to create permission. Environment variable names are designated by one or more case-insensitive name lists separated by semicolons, with separate lists for read and write access to the named variables. However, only the read access is accessible with this option.
2. Execute: This uses the SecurityPermission class to create execution permission. This permission uses the SecurityPermissionFlag enumeration to provide the Execution permission as an argument.
3. UIPermission: This uses the UIPermission class to create permission to access a GUI interface, window. However this controls the permissions related to user interfaces and the Clipboard.
4. File Read: This uses the FileIOPermission to create the read permission. This permission gives read access to the contents of the file or access to information about the file, such as its length or last modification time. Only the file granted file read permission can be read.
5. File Write: This uses the FileIOPermission to create the write permission. This permission gives write access to the contents of the file or access to change information about the file, such as its name. Also allows for deletion and overwriting. Only the file granted file write permission can utilize it.
6. File Append: This uses the FileIOPermission to create the read permission. This permission gives the ability to write to the end of a file only. No ability to read. Only the file granted file append permission can utilize it.

7. File Dialog Open: This uses the FileDialogPermission class to create file dialog open permission. This controls the ability to access files or folders through a File dialog box.
8. File Dialog Save: This uses the FileDialogPermission class to create file dialog save permission. This controls the ability to access files or folders through a File dialog box.
9. Web / Internet: This uses the WebPermission Class to create permission. WebPermission provides a set of methods and properties to control access to Internet resources. You can use a WebPermission to provide either restricted or unrestricted access to your resource, based on the PermissionState that is set when the WebPermission is created.
10. Web Browser: This uses the WebBrowserPermission class to create permission. The Web browser permission enables frames to navigate HTML. This permission uses the values of the WebBrowserPermission enumerations.
11. Socket: This uses the SocketPermission class to create socket permission. This permission controls rights to make or accept connections on a transport address.
12. DNS: This uses the DNSPermission class to create DNS permission. This creates a new instance of the DnsPermission class that either allows unrestricted DNS access or disallows DNS access.
13. Printing: This uses the dotnet-plat-ext-7.0 PrintingPermission class to create permission. This permission controls access to printers on the system where the Sandbox is running.

How to Launch Sandbox GUI

There are three ways to launch this Sandbox version:

A. Launch Sandbox Executable

1. Enter the application folder
2. Double the executable Sandbox.exe or right click Sandbox.exe and click open.

B. Launch Sandbox GUI from Command Prompt

1. Launch the Command Console application on your computer
2. Change directory to the Sandbox application folder
3. Type Sandbox
4. Click enter key.

C. Launch and Execute Sandbox to run Untrusted Application from Command Line

To execute the Sandbox application on command line/prompt, provide the Sandbox name and all arguments in the following format and order:

Sandbox name**<SPACE>**Untrusted Application Folder Path**<SPACE>**Class Path **<SPACE>**Arguments**<SPACE>**Permission**<SPACE>**File Path

NB: When using command line / Prompt to call the Untrusted Application through Sandbox, the EntryPoint will be automatically picked from the Untrusted Application Assembly.

- Sandbox name – This is mandatory. E.g. Sandbox
- Untrusted Application Folder Path– This is mandatory. E.g. C:/
- Class Path– This is mandatory. e.g. Fruit.Apple

- Arguments – This arguments must be in bracket e.g (0,1,2,3). This bracket can be empty if this extra arguments are not required.
- Permission – The required permissions must be listed in bracket in number representation. e.g (0,1,2,3,4,5,6,7,8,9,10,11,12)
  Following are the available permissions and their number representation:
  0. Read Environment
  1. Execute
  2. UI Permission
  3. File Read
  4. File Write
  5. File Append
  6. File Dialog Open
  7. File Dialog Save
  8. Web / Internet
  9. Web Browser
  10. Socket
  11. DNS
  12. Printing

- File Path – This is optional. e.g C:/temp.txt

Example of sample command:

Sandbox C:\Users\Cends\source\repos\TestApp\TestApp\bin\Debug TestApp.Program () (1,2)

How to Use Sandbox GUI to Run an Untrusted Application

Steps:

1. Program Path Field: Provide the application folder path by using the browse button to browse to the application folder path or copy and paste the path in the Program Path textbox.
2. Class Path field/textbox: Provide the Class path by pasting it in the Class Path textbox. E.g. Bird.Flamingo
3. Entry Point field/textbox: This field is optional. User can specify the Entry Point of the Untrusted application by providing the method to be called which exists in the Class Path provided. E.g. Main. If not provided by the user, the Sandbox will automatically pick the EntryPoint from the Untrusted Application Assembly.
4. Arguments field/textbox: Argument(s) required by the untrusted application should be provided in the arguments textbox. This field is optional. It can be left blank if no argument is required.
5. File path: This can be used to provide the path to the file and the Untrusted application wants to read, write or append to. This textbox can be left blank as it is optional.

6. Clear Buttons: Use the clear buttons beside the textboxes to clear the textbox content.
7. Permissions: Go to the permission tab and check all required permissions to run the Untrusted application.
8. Click the Run button to call / run the application whose path has been provided in the Program path field/textbox and all other necessary fields/textboxes found under Program Call Tab have been well populated accordingly.