

Microsoft® Virtual Labs

Windows 7: UAC Data Redirection: .Net Framework

Table of Contents

Windows 7: UAC Data Redirection: .Net Framework	1
Exercise 1 Exploring User Account Control Virtualization	2
Exercise 2 Exploring User Account Control Virtualization	10

Windows 7: UAC Data Redirection: .Net Framework

Objectives

After completing this lab, you will be better able to:

- Troubleshoot a file redirection issue
- Use Process Monitor to find the root cause of the issue

Scenario

Many applications are still designed to write files to the Program Files, Windows® directories, or system root (typically the C drive) folders. Some applications are designed to update Microsoft® Windows registry values, specifically values in HKLM/Software. But there is one problem: the files or registry values are not created or updated. In this lab, you will experience first hand the effects of UAC virtualization and will walk through the steps to solve the problem.

Estimated Time to Complete This Lab

90 Minutes

Computer used in this Lab



Win7Devs

The username for the Administrator account on this computer is **Win7User** and the password is: **pass@word1**


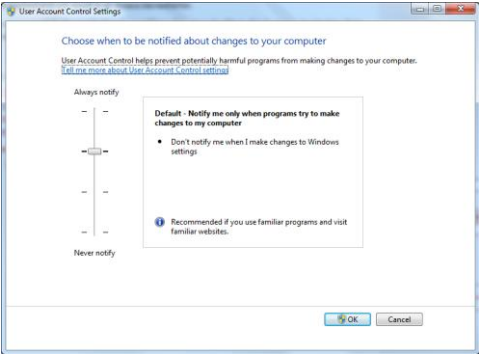
Exercise 1


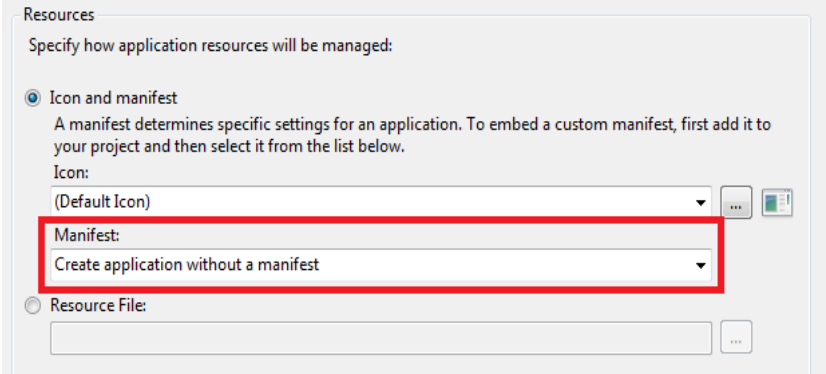
Exploring User Account Control Virtualization

Scenario

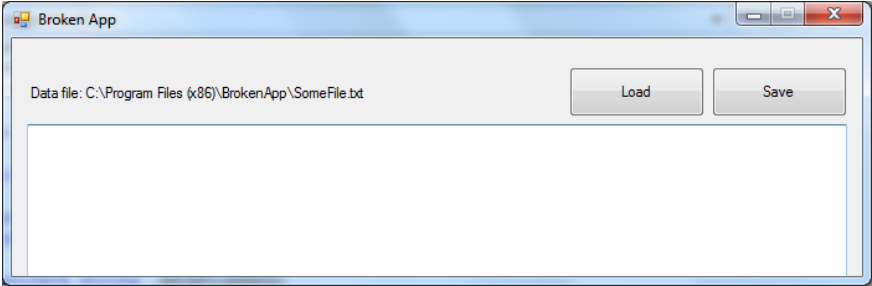
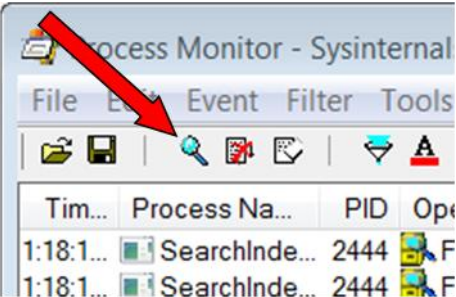
In this exercise, you will diagnose a managed (.NET Framework) application that is incompatible with Windows 7 and exhibits User Account Control (UAC) virtualization, specifically, file redirection, to the VirtualStore folder.

You will start by identifying the problem through a series of tests. Next, you will add a UAC manifest section and compile the application, thereby marking it as UAC-aware. As you run the application, you will notice that UAC does not virtualize your files when writing to any of the protected folders, such as Program Files; rather, the operation is blocked and results in an "access denied" error. Finally, you will fix the application by modifying it to store the file to the Application Data (ProgramData) folder.

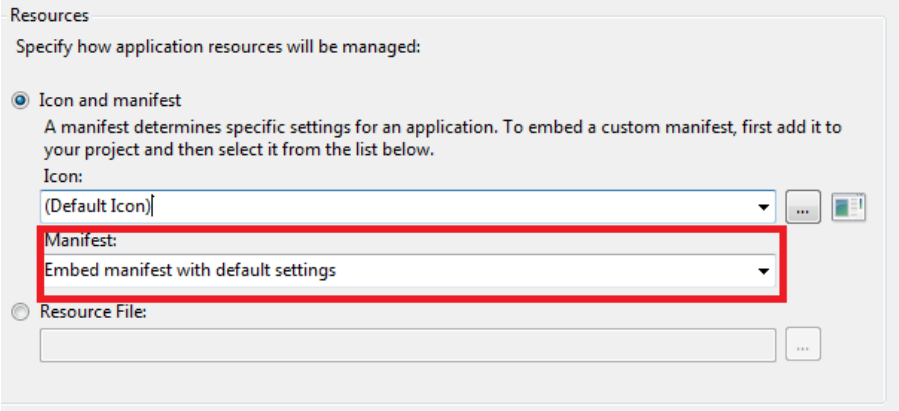
Tasks	Detailed Steps
<p>Complete the following task on:</p>  <p>Win7Devs</p> <p>1. Run the Application without a Manifest</p>	<p>Note: In this task, you will run the application without a manifest, which simulates an older application and triggers the UAC virtualization mechanism. New applications created with Visual Studio 2008 automatically embed a manifest containing a UAC section by default.</p> <ol style="list-style-type: none"> Make sure UAC is enabled. From the Start menu: Open Search Type "UAC" Click "Change User Account Control settings" in the search results list. The User Account Control Settings dialog box appears. To ensure UAC is NOT disabled: Set the UAC slider at the default level (as pictured) Click OK.  <ol style="list-style-type: none"> Open Windows Explorer and navigate to the folder containing the solution (C:\Labs\Managed\UAC Redirection\Begin)

Tasks	Detailed Steps
	<p>j. Double-click the “DataRedirection” solution file to open the solution.</p> <p>Note: Make sure you don’t start Visual Studio with Administrator privileges. If Visual Studio is started with elevated privileges, then “Visual Studio (Administrator)” will display in the title bar</p> <p>k. In the toolbar, set the target architecture to x86:</p>  <p>l. Right-click the BrokenAppManaged project and select Properties.</p> <p>Note: Configure the project to build the application without a manifest (the default manifest contains a UAC section)</p> <p>m. In the Application tab, under Manifest, verify “Create application without a manifest” is selected.</p>  <p>n. Close the Properties window.</p> <p>o. In the Solution Explorer pane, double-click on FileIO.cs to open it.</p> <p>p. Navigate to the FileIO class.</p> <p>q. Inspect the Save and Load functions and the static constructor and observe how the data file path is constructed as a file under Program Files\BrokenApp.</p> <p>r. Build the project and run it by pressing the F5 key.</p> <p>s. Open Task Manager and click the Processes tab.</p> <p>t. From the View menu, choose Select Columns</p> <p>u. The Select Process Page Columns dialog box appears</p> <p>v. Check the User Account Control (UAC) Virtualization check box</p> <p>w. Click OK</p>

Tasks	Detailed Steps																																																												
	<div data-bbox="604 191 1240 821" data-label="Image"> </div> <p data-bbox="505 877 1317 909">x. Notice that the UAC Virtualization column is enabled for your process.</p> <div data-bbox="604 926 1276 1675" data-label="Image"> <table border="1" data-bbox="656 1079 1230 1541"> <thead> <tr> <th>Image Name</th> <th>UAC Virtualization</th> <th>PID</th> <th>U</th> </tr> </thead> <tbody> <tr> <td>BrokenAppManaged.exe *32</td> <td>Enabled</td> <td>1740</td> <td>D</td> </tr> <tr> <td>csrss.exe</td> <td></td> <td>404</td> <td></td> </tr> <tr> <td>devenv.exe *32</td> <td>Disabled</td> <td>2820</td> <td>D</td> </tr> <tr> <td>dwm.exe</td> <td>Disabled</td> <td>2640</td> <td>D</td> </tr> <tr> <td>explorer.exe</td> <td>Disabled</td> <td>2724</td> <td>D</td> </tr> <tr> <td>Moe.exe *32</td> <td>Enabled</td> <td>2296</td> <td>D</td> </tr> <tr> <td>MoeMonitor.exe</td> <td>Disabled</td> <td>2944</td> <td>D</td> </tr> <tr> <td>msnmgr.exe *32</td> <td>Disabled</td> <td>4380</td> <td>D</td> </tr> <tr> <td>mspaint.exe</td> <td>Disabled</td> <td>740</td> <td>D</td> </tr> <tr> <td>OUTLOOK.EXE *32</td> <td>Disabled</td> <td>1600</td> <td>D</td> </tr> <tr> <td>procexp.exe *32</td> <td></td> <td>3300</td> <td>D</td> </tr> <tr> <td>procexp64.exe</td> <td></td> <td>3304</td> <td>D</td> </tr> <tr> <td>splwow64.exe</td> <td>Disabled</td> <td>3380</td> <td>D</td> </tr> <tr> <td>taskhost.exe</td> <td>Disabled</td> <td>2564</td> <td>D</td> </tr> </tbody> </table> </div> <p data-bbox="505 1730 1365 1797">y. Type some text into the edit box and then click Save. The operation should succeed (that is, you won't receive any error).</p>	Image Name	UAC Virtualization	PID	U	BrokenAppManaged.exe *32	Enabled	1740	D	csrss.exe		404		devenv.exe *32	Disabled	2820	D	dwm.exe	Disabled	2640	D	explorer.exe	Disabled	2724	D	Moe.exe *32	Enabled	2296	D	MoeMonitor.exe	Disabled	2944	D	msnmgr.exe *32	Disabled	4380	D	mspaint.exe	Disabled	740	D	OUTLOOK.EXE *32	Disabled	1600	D	procexp.exe *32		3300	D	procexp64.exe		3304	D	splwow64.exe	Disabled	3380	D	taskhost.exe	Disabled	2564	D
Image Name	UAC Virtualization	PID	U																																																										
BrokenAppManaged.exe *32	Enabled	1740	D																																																										
csrss.exe		404																																																											
devenv.exe *32	Disabled	2820	D																																																										
dwm.exe	Disabled	2640	D																																																										
explorer.exe	Disabled	2724	D																																																										
Moe.exe *32	Enabled	2296	D																																																										
MoeMonitor.exe	Disabled	2944	D																																																										
msnmgr.exe *32	Disabled	4380	D																																																										
mspaint.exe	Disabled	740	D																																																										
OUTLOOK.EXE *32	Disabled	1600	D																																																										
procexp.exe *32		3300	D																																																										
procexp64.exe		3304	D																																																										
splwow64.exe	Disabled	3380	D																																																										
taskhost.exe	Disabled	2564	D																																																										

Tasks	Detailed Steps
	 <p data-bbox="506 554 1287 583">z. Try to navigate to the path indicated (C:\Program Files\BrokenApp).</p> <p data-bbox="506 606 1422 667">Note: You won't find BrokenApp under Program Files because the write file operation was redirected to the VirtualStore folder</p>
<p data-bbox="186 688 428 718">2. Find the Problem</p>	<p data-bbox="506 688 1427 749">Note: In this task, you will walk through the different steps that will confirm that your application is experiencing UAC virtualization.</p> <p data-bbox="506 762 1430 854">Note: In this task, we will use the Process Monitor application. This utility is available for download from Microsoft TechNet (http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx).</p> <ol data-bbox="506 867 1422 1129" style="list-style-type: none"> From the Start menu, launch Process Monitor. Click Yes for the User Account Control dialog box. Click Cancel in the Process Monitor Filter dialog box. In the menu bar, click Filter -> Reset Filter. Ensure Process Monitor is capturing events by verifying the third toolbar button is not crossed out. You can also toggle capturing on/off by pressing CTRL-E.  <ol data-bbox="506 1503 1406 1709" style="list-style-type: none"> In the BrokenAppManaged application, click Save again. Stop capturing in Process Monitor by clicking the third toolbar button (or by pressing CTRL-E). In Process Monitor, from the Tools menu, click Process Tree. The Process Tree dialog box appears.

Tasks	Detailed Steps																																																																																							
	<div data-bbox="607 191 1198 810" data-label="Image"> <p>The screenshot shows the 'Process Tree' dialog box with a table of running processes. The process 'BrokenAppManaged.exe (4852)' is highlighted in blue. Below the table, the description and path for this process are shown.</p> <table border="1"> <thead> <tr> <th>Process</th> <th>Description</th> <th>Image</th> </tr> </thead> <tbody> <tr> <td>Explorer.EXE (5056)</td> <td>Windows Explorer</td> <td>C:\W...</td> </tr> <tr> <td>mspaint.exe (6940)</td> <td>Paint</td> <td>C:\W...</td> </tr> <tr> <td>taskmgr.exe (3208)</td> <td>Windows Task M...</td> <td>C:\W...</td> </tr> <tr> <td>devenv.exe (2964)</td> <td>Microsoft Visual St...</td> <td>C:\Pr...</td> </tr> <tr> <td>BrokenAppManaged.exe (4852)</td> <td>BrokenAppManag...</td> <td>C:\U...</td> </tr> <tr> <td>mspdbsrv.exe (5524)</td> <td>Microsoft® Progra...</td> <td>C:\Pr...</td> </tr> </tbody> </table> <p>Description: BrokenAppManaged Company: Microsoft Path: C:\Users\Dima\Desktop\HOL\BrokenAppManaged\bin\x8 Command: "C:\Users\Dima\Desktop\HOL\BrokenAppManaged\bin\x8 User: WIN7\Dima PID: 4852 Started: 22 23:09:12 2009 אפריל</p> </div> <p data-bbox="505 863 1312 1052"> h. Look for BrokenAppManaged.exe in the tree and double-click it. i. Click Close to close the Process Tree dialog box. j. Right-click the process name BrokenAppManaged in Process Monitor. k. Select Include -> Process Name. This will filter out all other events. </p> <div data-bbox="537 1079 1409 1591" data-label="Image"> <p>The screenshot shows the Process Monitor window with a filtered list of events for 'BrokenAppManaged.exe'. The 'Result' column shows a sequence of operations: FAST IO DISALLOWED, REPARSE, FAST IO DISALLOWED, SUCCESS, SUCCESS, SUCCESS, REPARSE, SUCCESS, SUCCESS, SUCCESS.</p> <table border="1"> <thead> <tr> <th>Time</th> <th>Process Name</th> <th>PID</th> <th>Operation</th> <th>Path</th> <th>Result</th> </tr> </thead> <tbody> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>QueryOpen</td> <td>C:\Program Files (x86)\BrokenApp</td> <td>FAST IO DISALLOWED</td> </tr> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>CreateFile</td> <td>C:\Program Files (x86)\BrokenApp</td> <td>REPARSE</td> </tr> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>QueryOpen</td> <td>C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp</td> <td>FAST IO DISALLOWED</td> </tr> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>CreateFile</td> <td>C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp</td> <td>SUCCESS</td> </tr> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>QueryNetwor...</td> <td>C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp</td> <td>SUCCESS</td> </tr> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>CloseFile</td> <td>C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp</td> <td>SUCCESS</td> </tr> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>CreateFile</td> <td>C:\Program Files (x86)\BrokenApp\SomeFile.txt</td> <td>REPARSE</td> </tr> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>CreateFile</td> <td>C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp\SomeFile.txt</td> <td>SUCCESS</td> </tr> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>WriteFile</td> <td>C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp\SomeFile.txt</td> <td>SUCCESS</td> </tr> <tr> <td>23:27...</td> <td>BrokenAppMan...</td> <td>5624</td> <td>CloseFile</td> <td>C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp\SomeFile.txt</td> <td>SUCCESS</td> </tr> </tbody> </table> </div> <p data-bbox="505 1654 1409 1745"> Note: You can see that BrokenAppManaged is trying to create the file C:\ProgramFiles \BrokenApp\SomeFile.txt. This file is redirected to the VirtualStore folder, where the actual data file ends up. </p> <p data-bbox="505 1759 1409 1822"> Notice the Result column. The line where the result is "REPARSE" is the original operation. The next line with the result "SUCCESS" is the redirected operation. </p> <p data-bbox="505 1835 1110 1864"> l. Close the running BrokenAppManaged application. </p>	Process	Description	Image	Explorer.EXE (5056)	Windows Explorer	C:\W...	mspaint.exe (6940)	Paint	C:\W...	taskmgr.exe (3208)	Windows Task M...	C:\W...	devenv.exe (2964)	Microsoft Visual St...	C:\Pr...	BrokenAppManaged.exe (4852)	BrokenAppManag...	C:\U...	mspdbsrv.exe (5524)	Microsoft® Progra...	C:\Pr...	Time	Process Name	PID	Operation	Path	Result	23:27...	BrokenAppMan...	5624	QueryOpen	C:\Program Files (x86)\BrokenApp	FAST IO DISALLOWED	23:27...	BrokenAppMan...	5624	CreateFile	C:\Program Files (x86)\BrokenApp	REPARSE	23:27...	BrokenAppMan...	5624	QueryOpen	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp	FAST IO DISALLOWED	23:27...	BrokenAppMan...	5624	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp	SUCCESS	23:27...	BrokenAppMan...	5624	QueryNetwor...	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp	SUCCESS	23:27...	BrokenAppMan...	5624	CloseFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp	SUCCESS	23:27...	BrokenAppMan...	5624	CreateFile	C:\Program Files (x86)\BrokenApp\SomeFile.txt	REPARSE	23:27...	BrokenAppMan...	5624	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp\SomeFile.txt	SUCCESS	23:27...	BrokenAppMan...	5624	WriteFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp\SomeFile.txt	SUCCESS	23:27...	BrokenAppMan...	5624	CloseFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp\SomeFile.txt	SUCCESS
Process	Description	Image																																																																																						
Explorer.EXE (5056)	Windows Explorer	C:\W...																																																																																						
mspaint.exe (6940)	Paint	C:\W...																																																																																						
taskmgr.exe (3208)	Windows Task M...	C:\W...																																																																																						
devenv.exe (2964)	Microsoft Visual St...	C:\Pr...																																																																																						
BrokenAppManaged.exe (4852)	BrokenAppManag...	C:\U...																																																																																						
mspdbsrv.exe (5524)	Microsoft® Progra...	C:\Pr...																																																																																						
Time	Process Name	PID	Operation	Path	Result																																																																																			
23:27...	BrokenAppMan...	5624	QueryOpen	C:\Program Files (x86)\BrokenApp	FAST IO DISALLOWED																																																																																			
23:27...	BrokenAppMan...	5624	CreateFile	C:\Program Files (x86)\BrokenApp	REPARSE																																																																																			
23:27...	BrokenAppMan...	5624	QueryOpen	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp	FAST IO DISALLOWED																																																																																			
23:27...	BrokenAppMan...	5624	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp	SUCCESS																																																																																			
23:27...	BrokenAppMan...	5624	QueryNetwor...	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp	SUCCESS																																																																																			
23:27...	BrokenAppMan...	5624	CloseFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp	SUCCESS																																																																																			
23:27...	BrokenAppMan...	5624	CreateFile	C:\Program Files (x86)\BrokenApp\SomeFile.txt	REPARSE																																																																																			
23:27...	BrokenAppMan...	5624	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp\SomeFile.txt	SUCCESS																																																																																			
23:27...	BrokenAppMan...	5624	WriteFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp\SomeFile.txt	SUCCESS																																																																																			
23:27...	BrokenAppMan...	5624	CloseFile	C:\Users\User\AppData\Local\VirtualStore\Program Files (x86)\BrokenApp\SomeFile.txt	SUCCESS																																																																																			

Tasks	Detailed Steps
<p>3. Add a UAC Manifest</p>	<p>Note: <i>In this task, you will add a manifest to the application to mark the application as UAC-aware. By marking your application as UAC aware, you declare that the application does not require write access to protected locations. UAC virtualization will not apply to your application.</i></p> <ol style="list-style-type: none"> In Visual Studio, right-click the project in Project Explorer and select Properties. Right-click the BrokenAppManaged project and select Properties. Configure the project to build the application with a manifest. Under Manifest, select “Embed manifest with default settings” <p>Note: <i>The default manifest will contain a UAC section</i></p>  <p>The screenshot shows the 'Resources' section of the Visual Studio Properties window. It is titled 'Specify how application resources will be managed:'. There are two radio buttons: 'Icon and manifest' (which is selected) and 'Resource File'. Under 'Icon and manifest', there is a text box for 'Icon:' containing '(Default Icon)' and a dropdown menu for 'Manifest:' containing 'Embed manifest with default settings'. The 'Manifest:' dropdown is highlighted with a red rectangle. Below 'Resource File' is an empty text box.</p> <ol style="list-style-type: none"> Save the change and close the Properties window. Press the F5 key to run the application. Look at Task Manager again, and you will notice that virtualization is now disabled for the process:

Tasks	Detailed Steps
	<div data-bbox="607 195 1346 1018" data-label="Image"> </div> <p data-bbox="505 1083 1357 1150">h. Type some text into the edit box and click Save in the BrokenAppManaged application. You should receive an error dialog box.</p> <p data-bbox="505 1171 1409 1234">Note: Because UAC virtualization is turned off, writing to protected locations results in an error.</p> <p data-bbox="505 1247 1110 1276">i. Close the running BrokenAppManaged application.</p>
<p data-bbox="188 1310 441 1369">4. Correct the Access Denied Error</p>	<p data-bbox="505 1310 1367 1436">Note: By embedding the manifest containing a UAC section, you declare to Windows 7 that your application is UAC-aware; therefore the application will be unable to write to any protected storage area. In this task, you will change the location to which the text file will be saved and fix the access denied error.</p> <p data-bbox="505 1449 1419 1904"> a. Return to Visual Studio. b. In the static constructor of the FileIO class in FileIO.cs: c. Comment out the line to save to Environment.SpecialFolders.ProgramFiles (Line 49) d. Uncomment the line to save to Environment.SpecialFolders.CommonApplicationData (Line 50) e. This will save the file to the common program data folder (C:\ProgramData, by default), which is accessible by all users. f. Press the F5 key to rebuild and run the application. g. Type some text into the edit box and then click Save. The operation should </p>

Tasks	Detailed Steps
	<p>succeed.</p> <p>h. Make sure the data file is now saved to the correct folder: C:\ProgramData\BrokenApp.</p> <p>Note: You now have fixed the redirection issue and saved your data file to the correct location.</p> <p><i>In order for redirection to work in Visual Studio 2008, you must turn off UAC in the manifest generation. To do so:</i></p> <p><i>For C# projects In Visual Studio:</i></p> <ul style="list-style-type: none">• Click the Project menu.• Click the Properties for that project.• On the Application tab, in the Resources area, select the Icon and manifest button.• Select Create application without a manifest.• Click OK. <p><i>UAC is turned off here only for demonstration purposes. All executables should contain a UAC section in the manifest. If a UAC section is present in the manifest, Windows will not consider the application a legacy application and does not enable redirection. Writing to Program Files would return an access denied error.</i></p>

Exercise 2


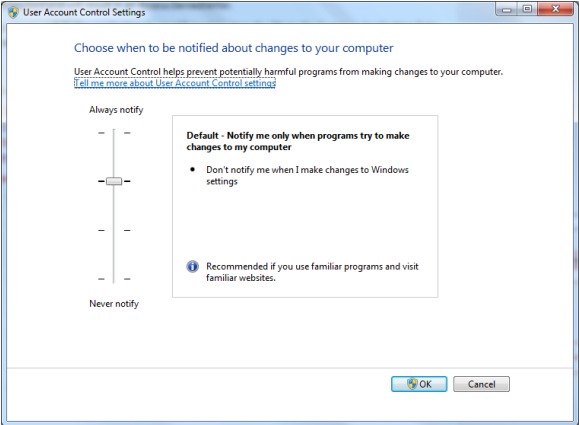
Exploring User Account Control Virtualization

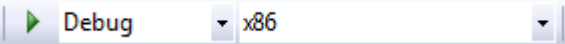
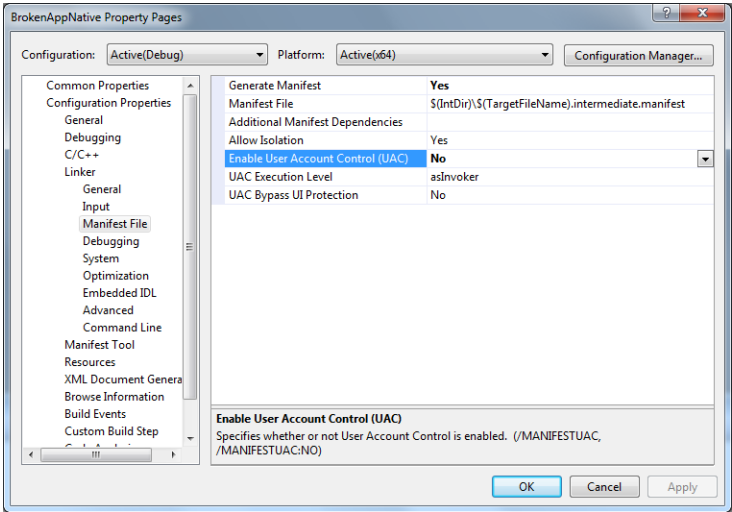
Scenario

In this exercise, you will diagnose a broken native (Win32) C++ application that exhibits file redirection to the VirtualStore folder.

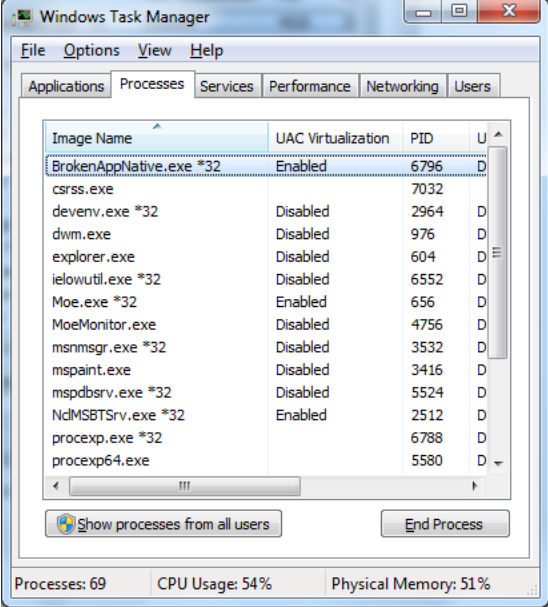
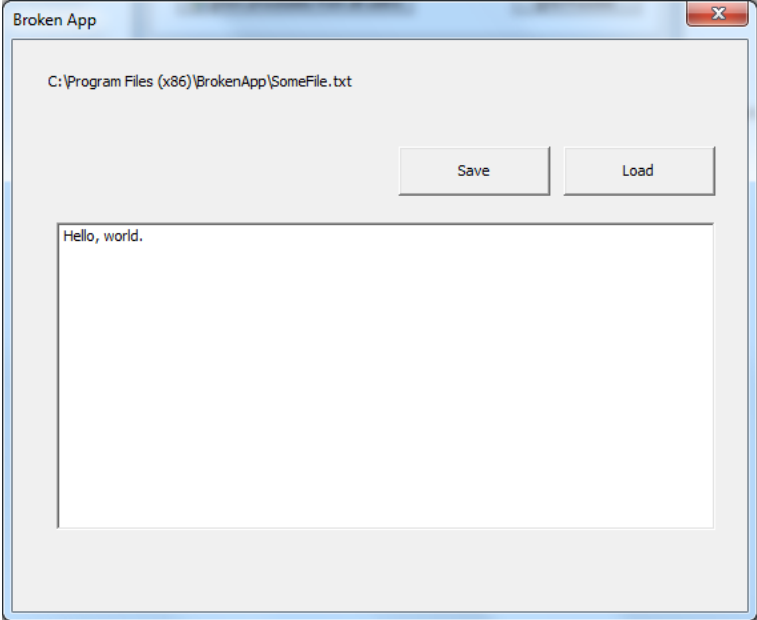
You will then add a UAC manifest section and compile the application, thereby marking it as UAC-aware. You will observe that instead of being redirected, write operations to the Program Files folder will be blocked resulting in an “access denied” error.

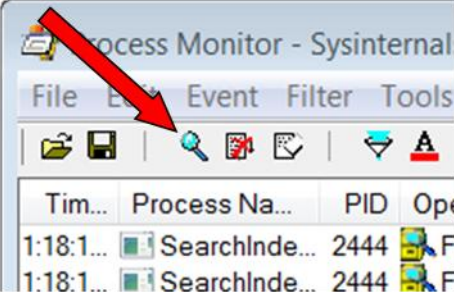
Finally, you will fix the application by modifying it to store the file to the Application Data (ProgramData) folder.

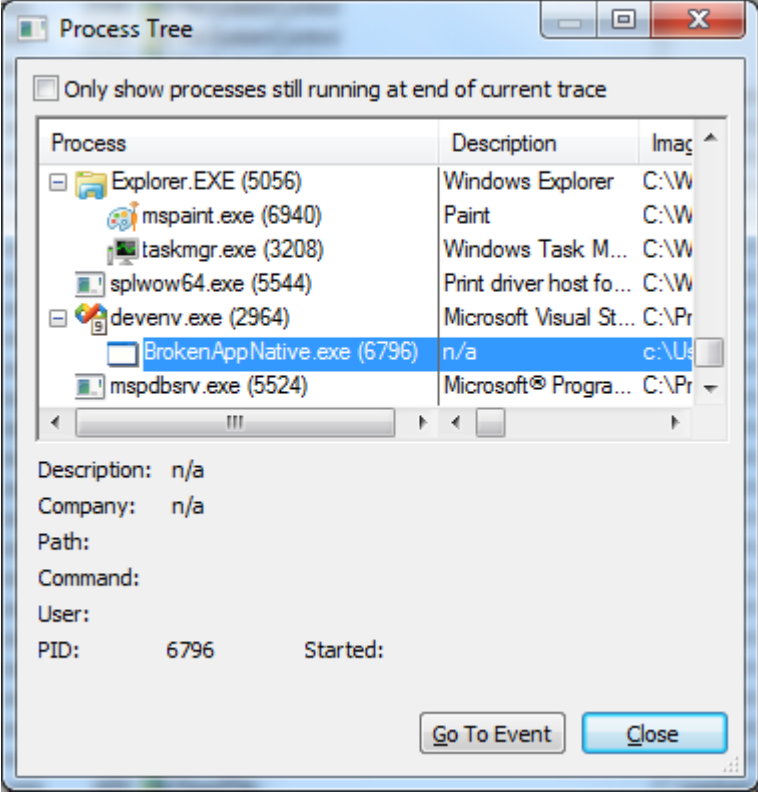
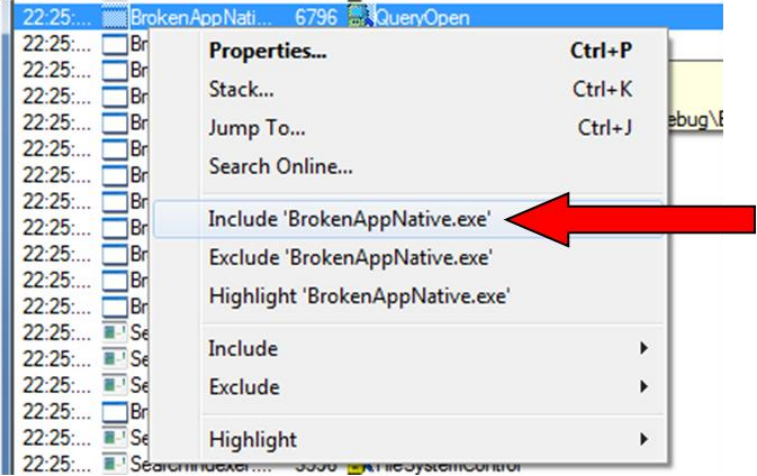
Tasks	Detailed Steps
<p>Complete the following task on:</p>  <p>Win7Devs</p> <p>1. Run the Application without a Manifest</p>	<p><i>Note: In this task, you will run the application without a manifest, which simulates an older application and triggers the UAC virtualization mechanism. New applications created with Visual Studio 2008 automatically embed a manifest containing a UAC section by default.</i></p> <ol style="list-style-type: none"> a. Make sure UAC is enabled b. From the Start menu <ul style="list-style-type: none"> • Open Search • Type UAC • Click “Change User Account Control settings” in the search results list c. The User Account Control Settings dialog box appears. To ensure UAC is NOT disabled: <ul style="list-style-type: none"> • Set the UAC slider at the default level (as pictured below) • Click OK 

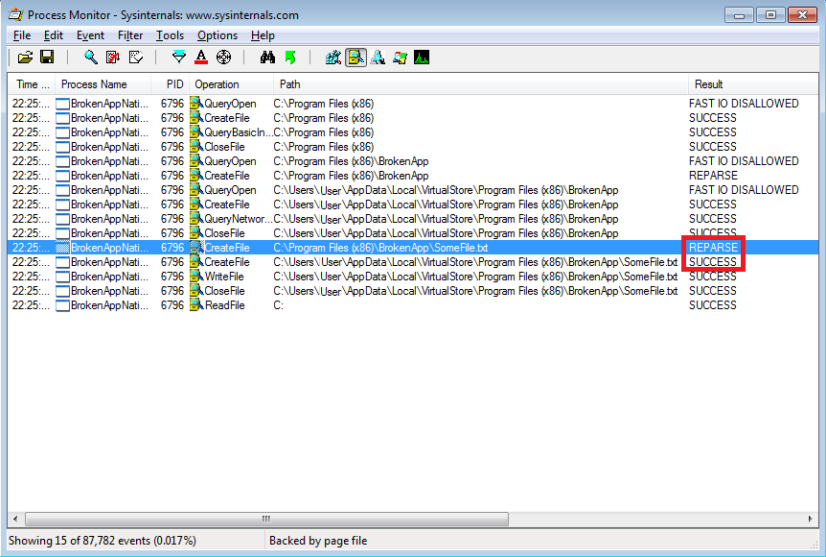
Tasks	Detailed Steps
	<p>d. Open Windows Explorer and navigate to the folder containing the solution (C:\Labs\Native\UAC Redirection\Begin)</p> <p>e. Double-click the “DataRedirection” solution file to open the solution.</p> <p>Note: Make sure you don’t start Visual Studio with Administrator privileges. If Visual Studio is started with elevated privileges, then “Visual Studio (Administrator)” will display in the title bar</p> <p>f. In the toolbar, set the build target to x86:</p>  <p>Note: The reason for this is that for x64 applications, virtualization is turned off regardless of a manifest.</p> <p>g. Right-click the BrokenAppNative project in Solution Explorer and select Properties:</p> <p>h. By default, Visual Studio 2008 configures projects to include a UAC section in the manifest; we will turn off this setting to illustrate how a legacy application would behave</p> <p>i. In Properties:</p> <p>j. Under Configuration Properties, expand the Linker node</p> <p>k. Select Manifest File</p> <p>l. Ensure the “Enable User Account Control (UAC)” selection is set to No</p> <p>m. Click OK</p>  <p>n. Close the Properties window.</p> <p>o. In Solution Explorer, double-click on the BrokenAppNative.cpp file to open it.</p> <p>p. Inspect the SaveFile and LoadFile functions</p> <p>q. Observe how the path is constructed in the MakeDataFilePath function:</p>

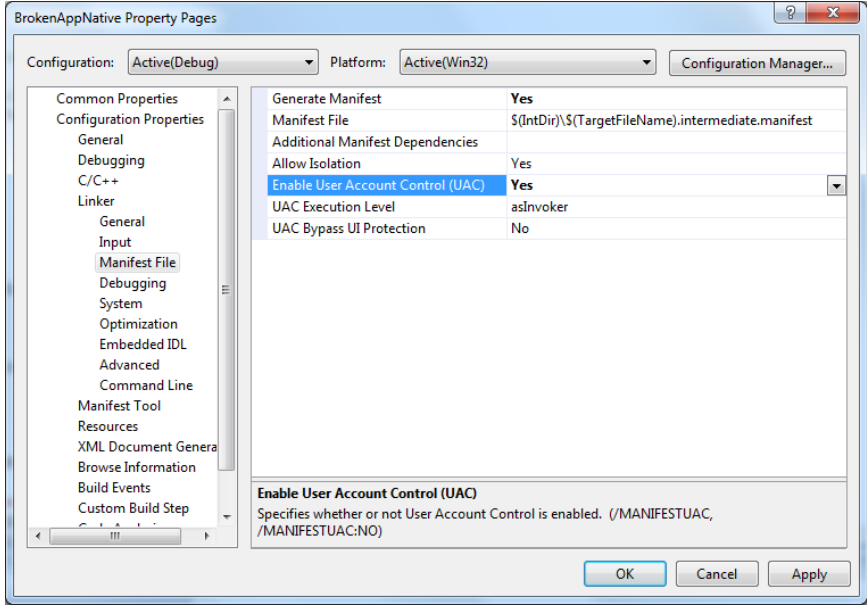
Tasks	Detailed Steps
	<p>r. The data file path saves to a folder under Program Files</p> <ul style="list-style-type: none"> • SHGetKnownFolderPath with the FOLDERID_ProgramFiles parameter retrieves the path of the Program Files folder • A subdirectory under Program Files is created first (BrokenApp), if it doesn't exist • Then a filename (SomeFile.txt) is created under that subdirectory <p>s. Build the project.</p> <p>t. Press the F5 key to run it.</p> <p>u. Open Task Manager and click the Processes tab.</p> <ul style="list-style-type: none"> • From the View menu, choose Select Columns • The Select Process Page Columns dialog box appears • Check the User Account Control (UAC) Virtualization check box • Click OK <div data-bbox="607 863 1162 1415" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Select Process Page Columns</p> <p>Select the columns that will appear on the Process page of Task Manager.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Handles <input type="checkbox"/> Threads <input type="checkbox"/> USER Objects <input type="checkbox"/> GDI Objects <input type="checkbox"/> I/O Reads <input type="checkbox"/> I/O Writes <input type="checkbox"/> I/O Other <input type="checkbox"/> I/O Read Bytes <input type="checkbox"/> I/O Write Bytes <input type="checkbox"/> I/O Other Bytes <input type="checkbox"/> Image Path Name <input type="checkbox"/> Command Line <input checked="" type="checkbox"/> User Account Control (UAC) Virtualization <input checked="" type="checkbox"/> Description <input type="checkbox"/> Data Execution Prevention <p style="text-align: right;">OK Cancel</p> </div> <p>v. Notice that the UAC Virtualization column is enabled for your process:</p>

Tasks	Detailed Steps
	 <p>w. Type some text into the edit box and then click Save. The operation should succeed; that is, you won't receive an error.</p>  <p>x. Try to navigate to the path indicated (C:\Program Files\BrokenApp).</p> <p>y. Close the running BrokenAppNative application.</p> <p><i>Note: You won't find BrokenApp under Program Files because the write file operation was redirected to the VirtualStore folder</i></p>
<p>2. Find the Problem</p>	<p><i>Note: In this task, you will walk through the different steps to confirm that your application is experiencing UAC virtualization.</i></p>

Tasks	Detailed Steps
	<p data-bbox="506 199 1398 289"><i>In this task, we will use the Process Monitor application. This utility is available for download from Microsoft TechNet (http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx).</i></p> <ol style="list-style-type: none"> <li data-bbox="506 304 1398 367">a. From the Start menu, launch Process Monitor. Click Yes for the User Account Control dialog box. <li data-bbox="506 394 1122 422">b. Click Cancel in the Process Monitor Filter dialog box. <li data-bbox="506 449 1013 476">c. In the menu bar, click Filter -> Reset Filter. <li data-bbox="506 504 1419 567">d. Ensure Process Monitor is capturing events by verifying the third toolbar button is not crossed out. You can also toggle capturing on/off by pressing CTRL-E.  <ol style="list-style-type: none"> <li data-bbox="506 947 1130 974">e. In the BrokenAppNative application, click Save again. <li data-bbox="506 1001 1377 1064">f. Stop capturing in Process Monitor by clicking the third toolbar button (or by pressing CTRL-E). <li data-bbox="506 1092 1403 1155">g. In Process Monitor, from the Tools menu, click Process Tree. The Process Tree dialog box appears:

Tasks	Detailed Steps
	 <p data-bbox="505 1045 1224 1075">h. Look for BrokenAppNative.exe in the tree and double-click it.</p> <p data-bbox="505 1098 1070 1127">i. Click Close to close the Process Tree dialog box.</p> <p data-bbox="505 1150 1284 1180">j. Right-click the process name BrokenAppNative in Process Monitor.</p> <p data-bbox="505 1203 1276 1232">k. Click Include BrokenAppNative. This will filter out all other events:</p> 

Tasks	Detailed Steps
	 <p>Note: You can see that BrokenAppNative is trying to create the file C:\ProgramFiles\BrokenApp\SomeFile.txt. This file is redirected to the VirtualStore folder, where the actual data file ends up.</p> <p>Notice the Result column. The line where the result is “REPARSE” is the original operation. The next line with the result “SUCCESS” is the redirected operation.</p> <ol style="list-style-type: none"> I. Close the running BrokenAppNative application.
<p>3. Add a UAC Manifest</p>	<p>Note: In this task, you will add a manifest to the application to mark the application as UAC-aware. By marking your application as UAC-aware, you declare that the application does not require write access to protected locations. UAC virtualization will not apply to your application.</p> <ol style="list-style-type: none"> a. In Visual Studio, right-click the BrokenAppNative project and select Properties. b. Under Configuration Properties, expand Linker. c. Select Manifest File. d. Change the “Enable User Account Control (UAC)” selection to Yes. e. Click OK.

Tasks	Detailed Steps														
	 <p>The screenshot shows the 'BrokenAppNative Property Pages' dialog box. The 'Configuration' is set to 'Active(Debug)' and the 'Platform' is 'Active(Win32)'. The 'Manifest File' section is expanded, showing the following properties:</p> <table border="1"><tr><td>Generate Manifest</td><td>Yes</td></tr><tr><td>Manifest File</td><td>\$(IntDir)\\$(TargetFileName).intermediate.manifest</td></tr><tr><td>Additional Manifest Dependencies</td><td></td></tr><tr><td>Allow Isolation</td><td>Yes</td></tr><tr><td>Enable User Account Control (UAC)</td><td>Yes</td></tr><tr><td>UAC Execution Level</td><td>asInvoker</td></tr><tr><td>UAC Bypass UI Protection</td><td>No</td></tr></table> <p>At the bottom of the dialog, there is a description for 'Enable User Account Control (UAC)':</p> <p>Enable User Account Control (UAC) Specifies whether or not User Account Control is enabled. (/MANIFESTUAC, /MANIFESTUAC:NO)</p> <p>Buttons: OK, Cancel, Apply</p>	Generate Manifest	Yes	Manifest File	\$(IntDir)\\$(TargetFileName).intermediate.manifest	Additional Manifest Dependencies		Allow Isolation	Yes	Enable User Account Control (UAC)	Yes	UAC Execution Level	asInvoker	UAC Bypass UI Protection	No
Generate Manifest	Yes														
Manifest File	\$(IntDir)\\$(TargetFileName).intermediate.manifest														
Additional Manifest Dependencies															
Allow Isolation	Yes														
Enable User Account Control (UAC)	Yes														
UAC Execution Level	asInvoker														
UAC Bypass UI Protection	No														
	<p>f. Re-build the application.</p> <p>g. Press the F5 key to run the application.</p> <p>h. Look at Task Manager again, and you will notice that virtualization is now disabled:</p>														

Tasks	Detailed Steps																																																												
	<div data-bbox="604 191 1425 1104" data-label="Image"> <table border="1"> <thead> <tr> <th>Image Name</th> <th>UAC Virtualization</th> <th>PID</th> <th>U</th> </tr> </thead> <tbody> <tr> <td>BrokenAppNative.exe *32</td> <td>Disabled</td> <td>1060</td> <td>D</td> </tr> <tr> <td>csrss.exe</td> <td></td> <td>7032</td> <td></td> </tr> <tr> <td>devenv.exe *32</td> <td>Disabled</td> <td>2964</td> <td>D</td> </tr> <tr> <td>dwm.exe</td> <td>Disabled</td> <td>976</td> <td>D</td> </tr> <tr> <td>explorer.exe</td> <td>Disabled</td> <td>604</td> <td>D</td> </tr> <tr> <td>ielowutil.exe *32</td> <td>Disabled</td> <td>6552</td> <td>D</td> </tr> <tr> <td>Moe.exe *32</td> <td>Enabled</td> <td>656</td> <td>D</td> </tr> <tr> <td>MoeMonitor.exe</td> <td>Disabled</td> <td>4756</td> <td>D</td> </tr> <tr> <td>msnmsgr.exe *32</td> <td>Disabled</td> <td>3532</td> <td>D</td> </tr> <tr> <td>mspaint.exe</td> <td>Disabled</td> <td>3416</td> <td>D</td> </tr> <tr> <td>mspaint.exe</td> <td>Disabled</td> <td>4036</td> <td>D</td> </tr> <tr> <td>mspaint.exe</td> <td>Disabled</td> <td>4792</td> <td>D</td> </tr> <tr> <td>mspdbsrv.exe *32</td> <td>Disabled</td> <td>5524</td> <td>D</td> </tr> <tr> <td>NdMSBTSrv.exe *32</td> <td>Enabled</td> <td>2512</td> <td>D</td> </tr> </tbody> </table> </div> <p data-bbox="505 1171 1364 1234">Note: This is because the presence of the UAC section in the manifest marks the application as UAC-aware.</p> <p data-bbox="505 1245 1333 1308">i. Type some text into the edit box and click Save in the BrokenAppNative application. You should receive the following error:</p> <div data-bbox="604 1329 1357 1671" data-label="Image"> </div> <p data-bbox="505 1738 1409 1801">Note: Because UAC virtualization is turned off, writing to protected locations results in an error.</p> <p data-bbox="505 1812 1081 1843">j. Close the running BrokenAppNative application.</p>	Image Name	UAC Virtualization	PID	U	BrokenAppNative.exe *32	Disabled	1060	D	csrss.exe		7032		devenv.exe *32	Disabled	2964	D	dwm.exe	Disabled	976	D	explorer.exe	Disabled	604	D	ielowutil.exe *32	Disabled	6552	D	Moe.exe *32	Enabled	656	D	MoeMonitor.exe	Disabled	4756	D	msnmsgr.exe *32	Disabled	3532	D	mspaint.exe	Disabled	3416	D	mspaint.exe	Disabled	4036	D	mspaint.exe	Disabled	4792	D	mspdbsrv.exe *32	Disabled	5524	D	NdMSBTSrv.exe *32	Enabled	2512	D
Image Name	UAC Virtualization	PID	U																																																										
BrokenAppNative.exe *32	Disabled	1060	D																																																										
csrss.exe		7032																																																											
devenv.exe *32	Disabled	2964	D																																																										
dwm.exe	Disabled	976	D																																																										
explorer.exe	Disabled	604	D																																																										
ielowutil.exe *32	Disabled	6552	D																																																										
Moe.exe *32	Enabled	656	D																																																										
MoeMonitor.exe	Disabled	4756	D																																																										
msnmsgr.exe *32	Disabled	3532	D																																																										
mspaint.exe	Disabled	3416	D																																																										
mspaint.exe	Disabled	4036	D																																																										
mspaint.exe	Disabled	4792	D																																																										
mspdbsrv.exe *32	Disabled	5524	D																																																										
NdMSBTSrv.exe *32	Enabled	2512	D																																																										

Tasks	Detailed Steps
<p>4. Correct the Access Denied Error</p>	<p>Note: By embedding the manifest containing a UAC section, you declare to Windows 7 that your application is UAC-aware, and therefore will refrain from writing to any protected storage area. In this task, you will change the location to which the text file will be saved and fix the access denied error.</p> <ol style="list-style-type: none"> a. Return to Visual Studio. b. Navigate to the MakeDataFilePath function in BrokenAppNative.cpp. c. Comment out the line at the top of the function that includes FOLDERID_ProgramFiles (Line 63). d. Uncomment the line that includes FOLDERID_ProgramData (Line 62). e. Rebuild the application. f. Press the F5 key to run the application. g. Type some text into the edit box and then click Save. The operation should succeed. h. Make sure the data file is now saved to the correct folder: C:\ProgramData\BrokenApp. <p>Note: You now have fixed the redirection issue and saved your data file to the correct location.</p> <p>Note: In order for redirection to work in Visual Studio 2008, you must turn off UAC in the manifest generation. To do so:</p> <p>For C++ projects In Visual Studio:</p> <ol style="list-style-type: none"> 1. Click the Project menu. 2. Click the Properties for that project. 3. Expand Configuration Properties. 4. Expand Linker. 5. Select Manifest File. 5. Change the Enable User Account Control (UAC) selection to No. 6. Click OK. <p>UAC is turned off here only for demonstration purposes. All executables should contain a UAC section in the manifest. If a UAC section is present in the manifest, Windows will not consider the application a legacy application and does not enable redirection. Writing to Program Files would return an access denied error.</p>