

The ArcFM Solution & Windows 7/Windows Server 2008

The following document is meant to outline issues that may be encountered when using certain ArcFM Solution components and Windows or Windows Server 2008. These can include issues with *UAC* (*User Account Control*) or the *User Interface (GUI)*. To learn about some of these issues and what can be done by users to avoid them, please continue reading. Sections include:

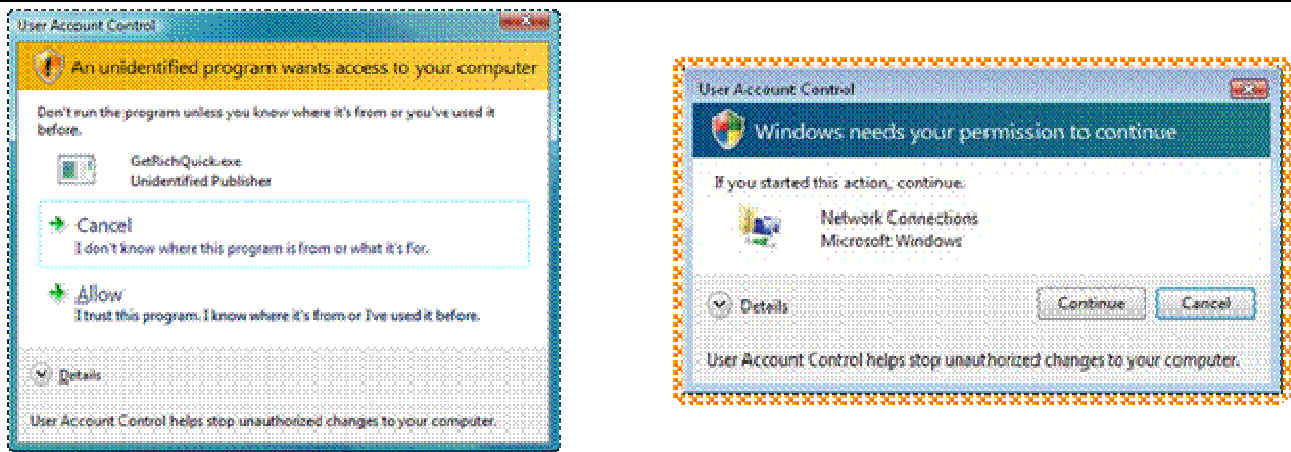
<i>User Account Control Basics</i>	1
<i>ArcFM 9.3.1</i>	3
<i>User Account Control and the ArcFM Solution 9.3.1 Release</i>	3
<i>License Manager and User Account Control</i>	3
<i>Geodatabase Manager and User Account Control</i>	7
<i>ArcFM 9.3.1 SP1</i>	10
<i>User Account Control and the ArcFM Solution 9.3.1 SP1 Release</i>	10
<i>Responder 9.3.1 SP1</i>	10
<i>Responder 9.3.1 SP1 and User Account Control</i>	10
<i>Windows 7 User Interface Issues</i>	11

User Account Control Basics

With Windows Vista and Windows Server 2008 SP2, Microsoft introduced a new security feature called **User Account Control (UAC)**. UAC was designed with the philosophy that even if a user on a computer had administrative rights, not all applications that user launched should have administrative privileges by default. When the user or application requests administrative access, a dialog box prompting the user for elevation will appear, and the user can decide to allow or deny administrator-level elevation.

The images below show two examples of User Account Control windows. When the user or application requests administrative access, a dialog box prompting the user for elevation will appear, and the user can decide to allow or deny administrator-level elevation.

Figure 1: User Account Control Dialog Examples



These dialog boxes will appear if a user or application requests administrative access to your system on a computer with UAC enabled.

Knowing the difference between administrator-level privileges and standard user privileges is important. Applications running with administrator privileges have access to all system settings and

critical system files. Applications running with standard user privileges are 'fenced off' from these sensitive parts of a system, unless given explicit permission to leave the 'fenced off' area.

This is where many third party applications have experienced problems. Before UAC, if a user had administrative privileges on a computer, all applications they launched had complete access to a system. When these same applications were run on Windows Vista (and later) with UAC enabled, they may have **expected** to have complete access to the system and appear to not work correctly (or at all) with standard user permissions. Types of items that UAC-incompatible applications might have expected access to are the **registry**, **windows services**, and **access to system folders**. Note that this is not an inclusive list.

User Access Control **may** be disabled by administrators so users will not need to worry about applications not working with UAC, but it is strongly advised against to maintain a more secure computing environment in your organization.

Detailed Information for User Account Control can be found below:

- General UAC information: <http://windows.microsoft.com/en-us/windows-vista/What-is-User-Account-Control>
- UAC on Windows Server 2008: [http://technet.microsoft.com/en-us/library/cc709628\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc709628(W.S.10).aspx)
- UAC on Windows 7: [http://technet.microsoft.com/en-us/library/dd560669\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/dd560669(W.S.10).aspx)

ArcFM 9.3.1

User Account Control and the ArcFM Solution 9.3.1 Release

This section will show how User Account Control affects the 9.3.1 release products in detail with two examples: Geodatabase Manager and License Manager.

This guide assumes basic knowledge of License Manager, Geodatabase Manager, and certain Windows components such as services and background processes.

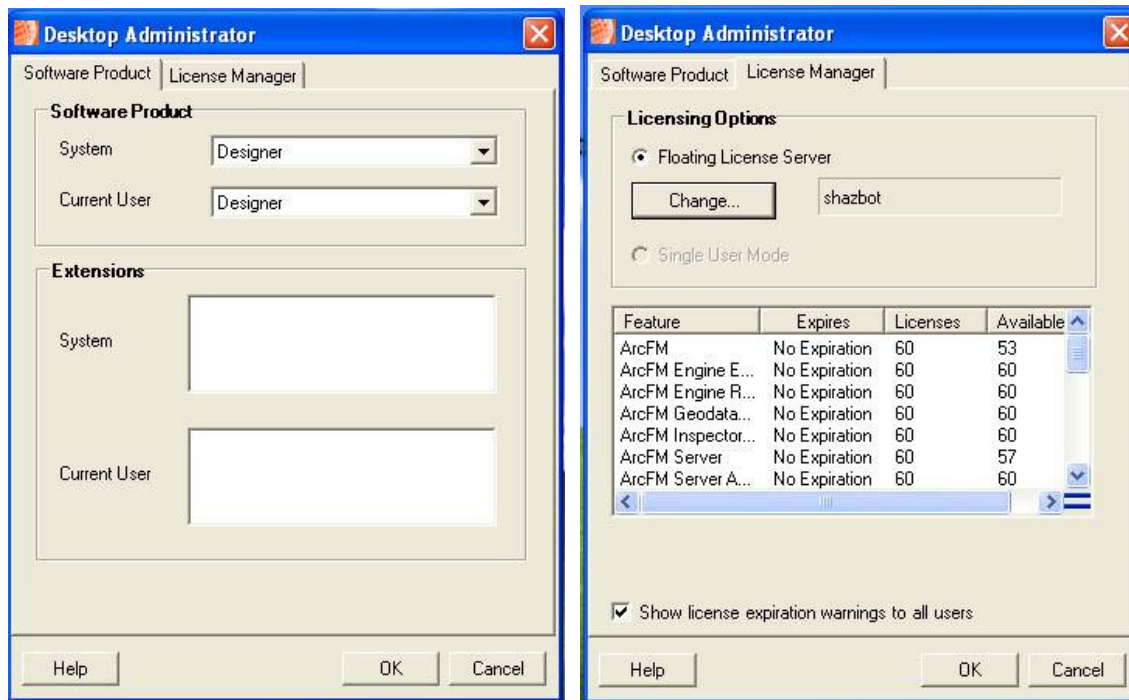
NOTE: Users should be aware that the ArcFM Solution 9.3.1 release was not designed to specifically work with Microsoft's User Account Control feature. Internal testing has shown product functionality has only been minimally affected, but users running in environments with UAC enabled should be aware that unexpected application behavior could be attributed to UAC. The first step to troubleshoot is to run the application as administrator and perform the same steps.

License Manager and User Account Control

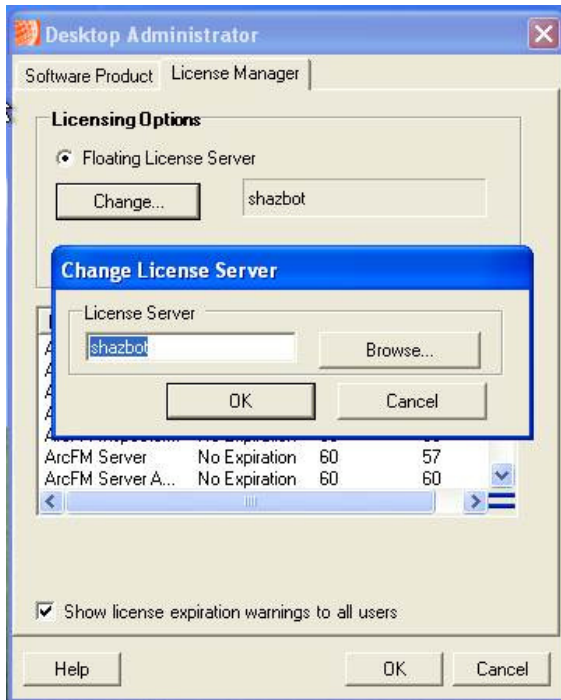
License Manager is affected by UAC in a way that is clearly visible to the end user.

Reproduction Steps:

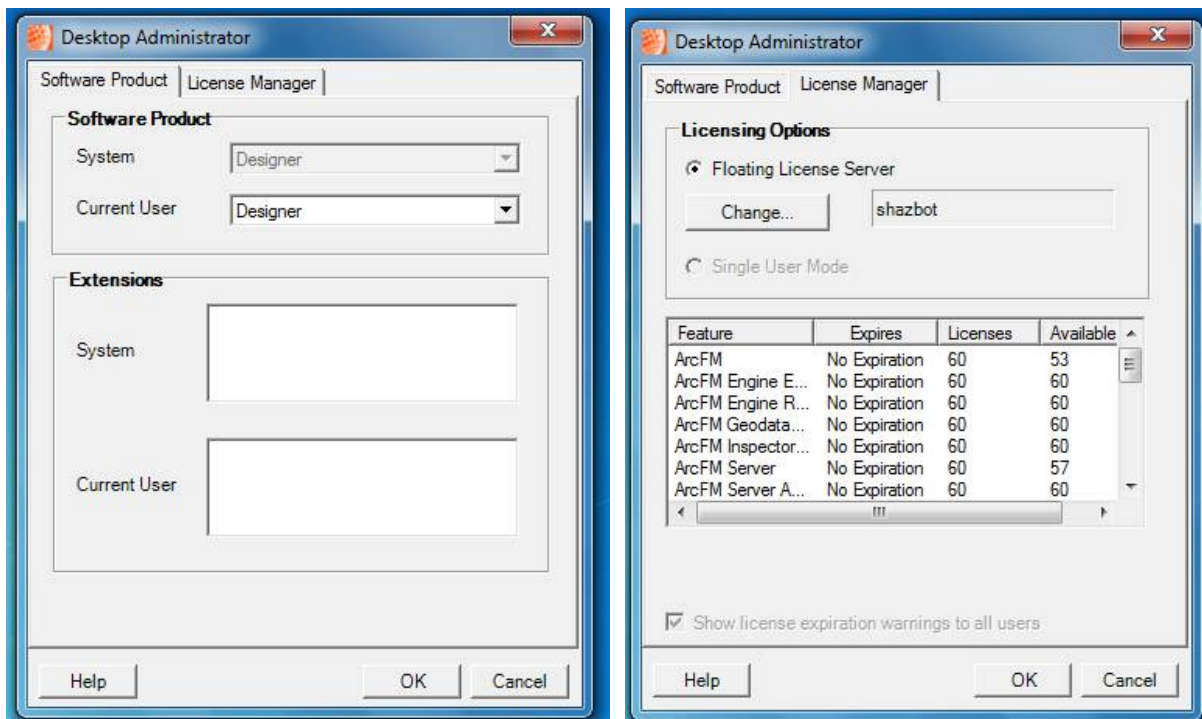
1. First, the images below show how License Manager behaves on Windows XP running under an account with administrative privileges:



Notice that windows appear as expected. Click on the 'Change...' button:



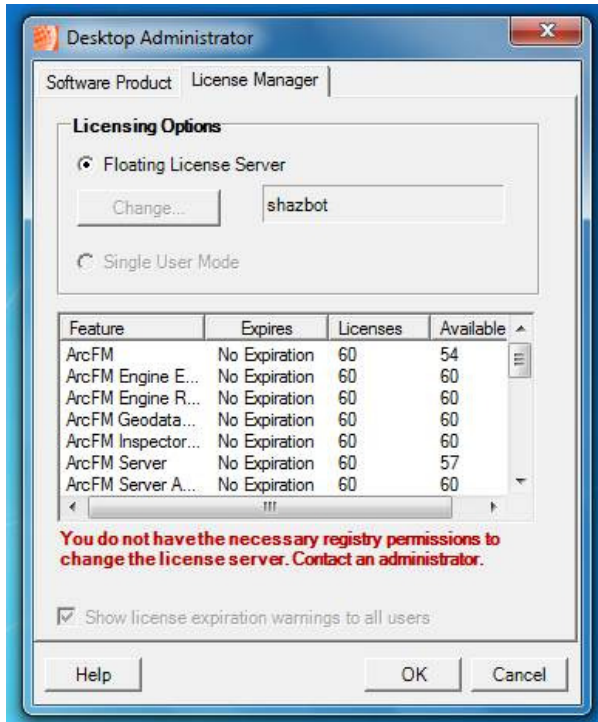
2. Now, these images demonstrate how License Manager appears on Windows 7, with UAC enabled.



Notice the differences between Windows XP and Windows 7 with UAC enabled:

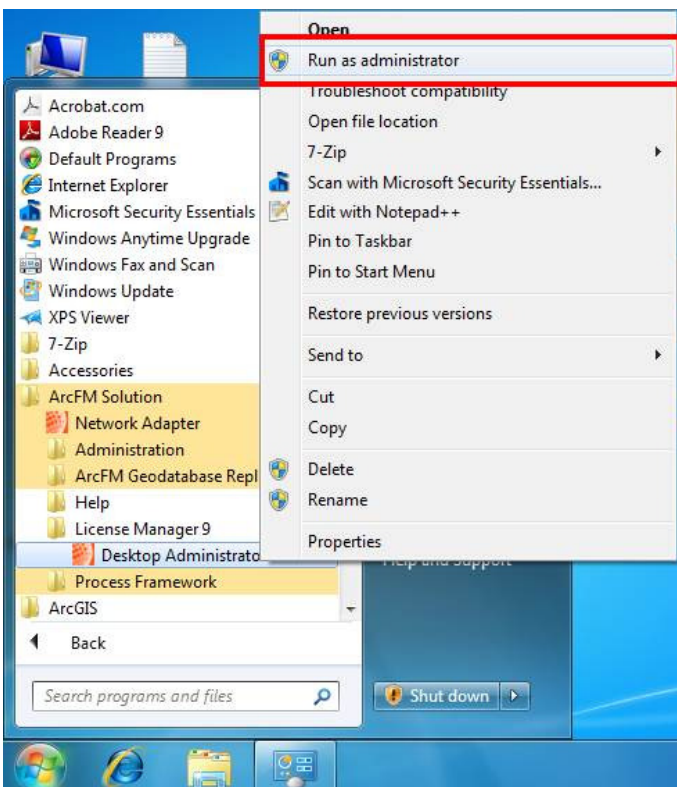
- The 'System' license level control is disabled and cannot be changed by the user.
- The 'Show license expiration warnings to all users' checkbox control is disabled.

Clicking the 'Change...' button on the License Manager tab results in:



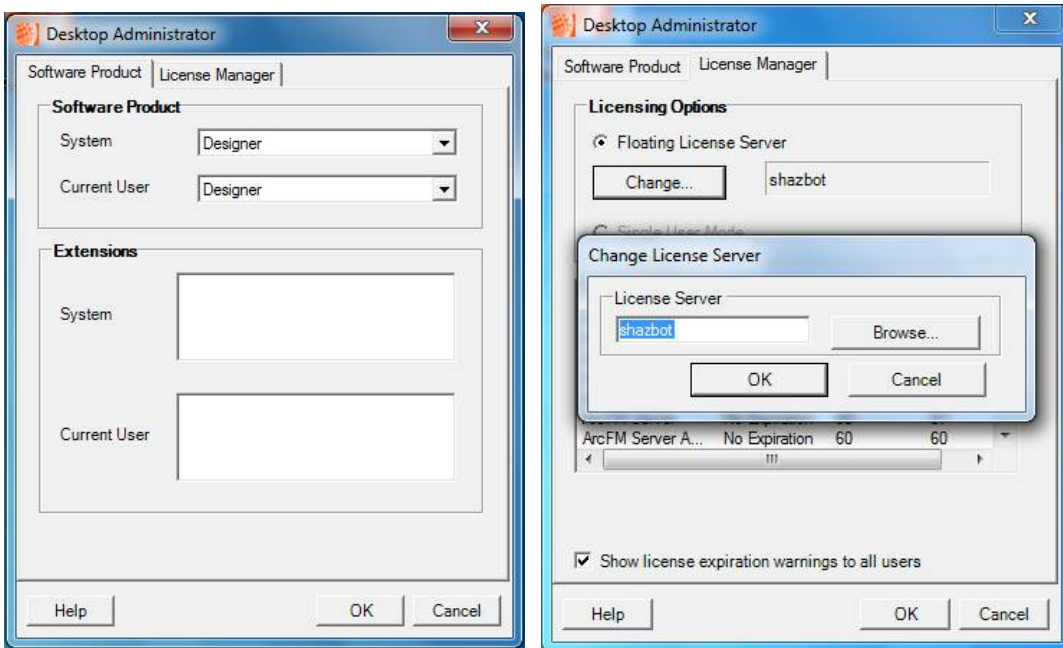
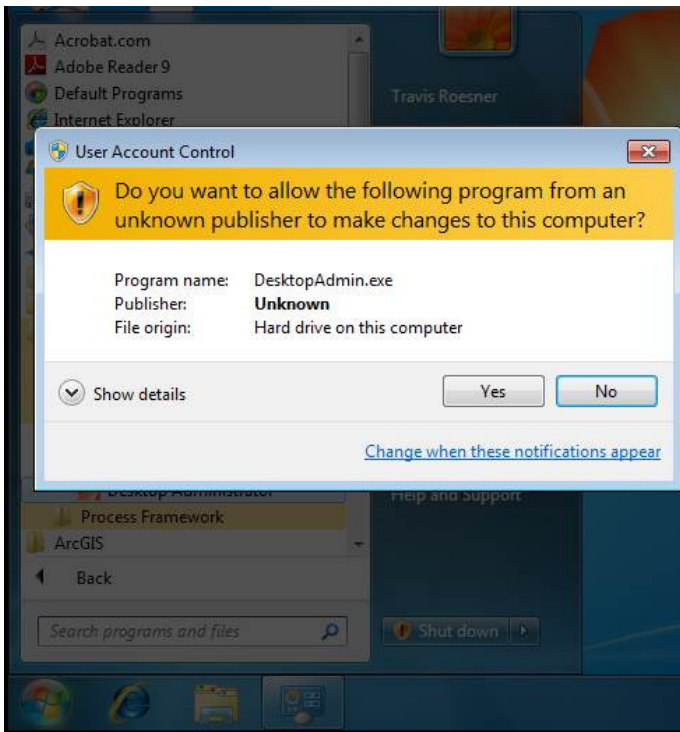
Notice that the application informs you that additional privileges are needed. This is due to UAC. Starting the application with standard user privileges, even though your user account is able to use those privileges, results in additional steps required.

3. To inform UAC that License Manager should have administrator-level access to the whole system, navigate to 'Desktop Administrator' in your start menu and then, right click.
 - Click 'Run as administrator'



Notice that the screen dims and a noticeable dialog box appears. This is UAC asking if this application should have access to the system at an administrator-level.

- Click the 'Yes' button.



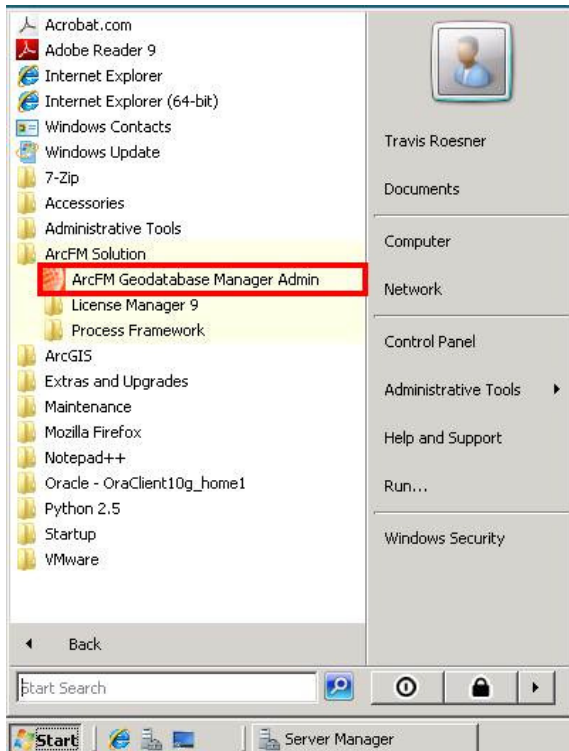
The Desktop Administrator will now behave as it did on Windows XP.

Geodatabase Manager and User Account Control

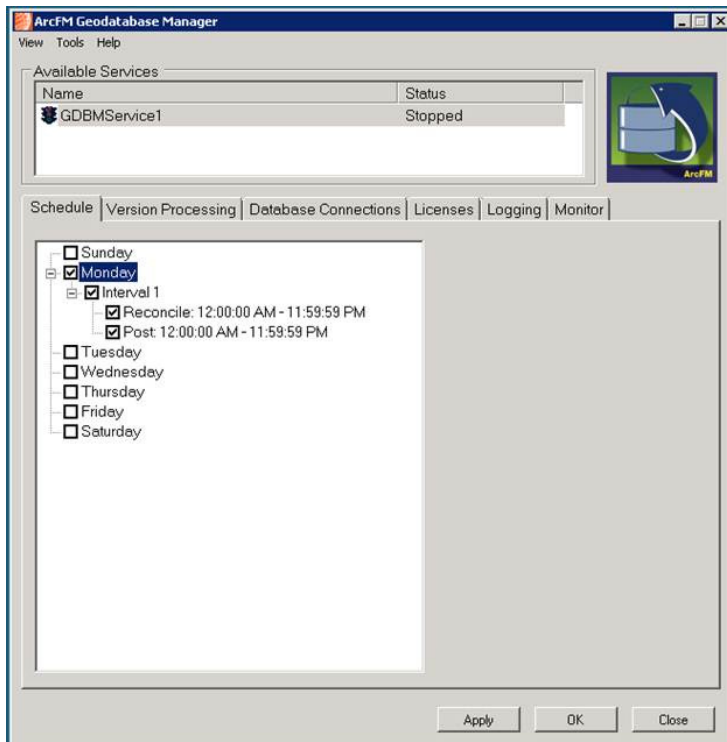
Geodatabase Manager utilizes Windows Services and requires access to multiple system-level folders. This application will not work correctly without administrator-level privileges.

Reproduction Steps:

1. Launch the ArcFM Geodatabase Manager Admin.

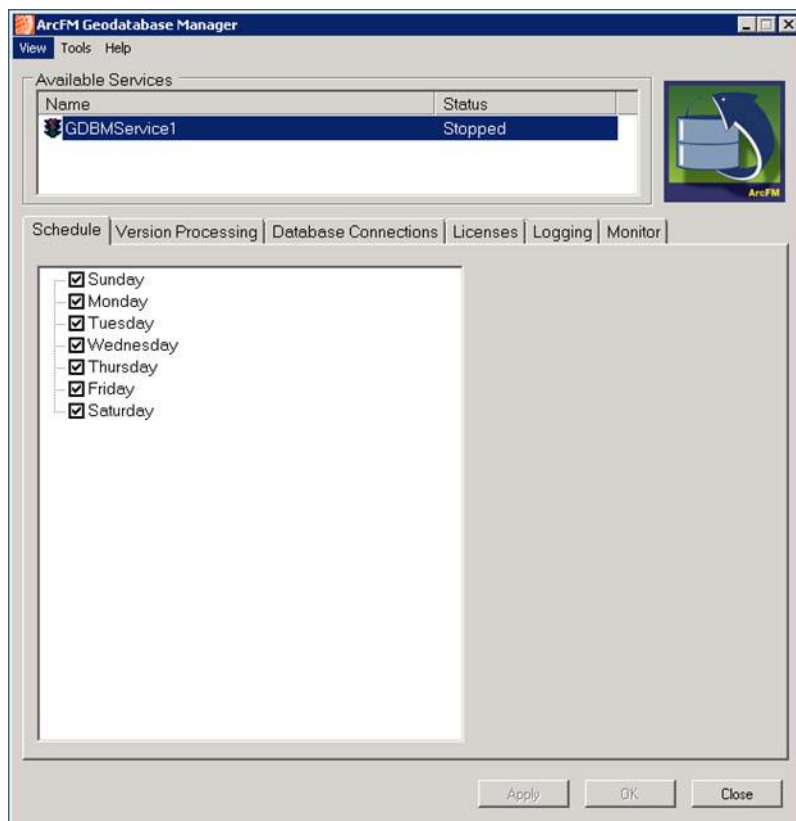


2. Create an interval on any of the days of the week in GDBM:



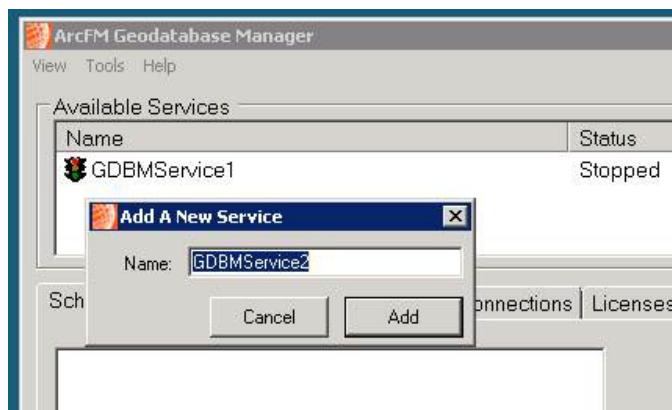
Notice how the application behaves normally. Click 'OK' to close the application.

3. Re-open the ArcFM Geodatabase Manager application. Notice how the changes were lost:



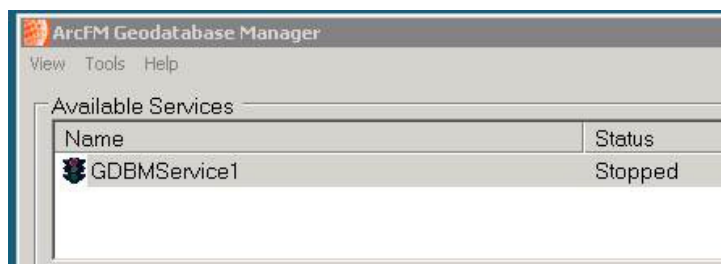
This is an example of how UAC is preventing an application from performing its usual actions. Since Geodatabase Manager was not designed for use with UAC, there are currently no prompts to tell you this fact.

4. Try to add a GDBM Service:



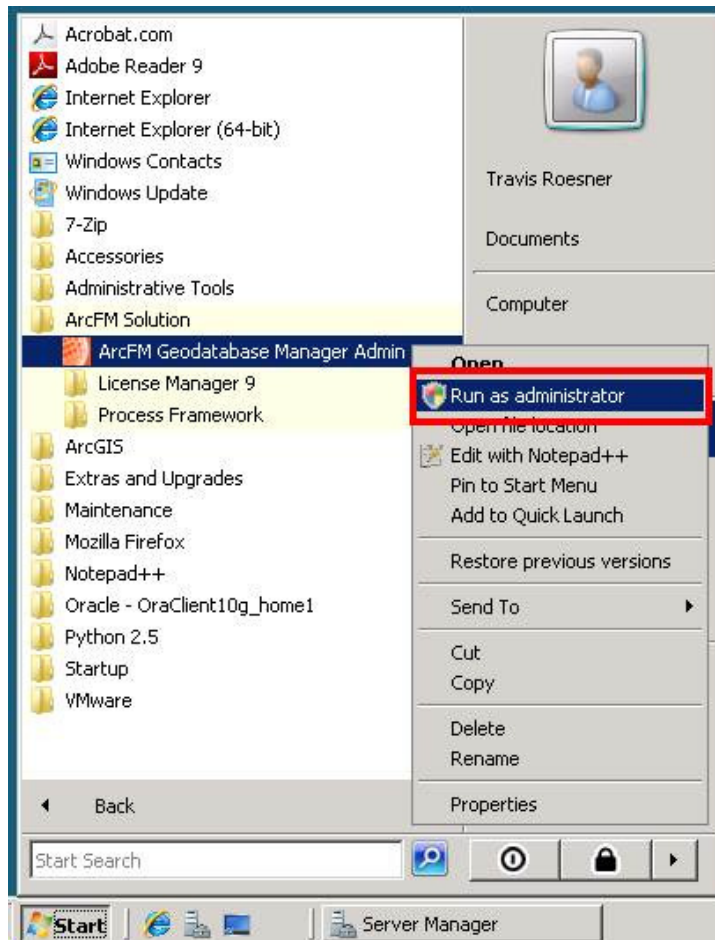
Notice that the application seems to behave normally. Click 'Add'.

5. Notice that the service was not actually added once you click the 'Add' button:

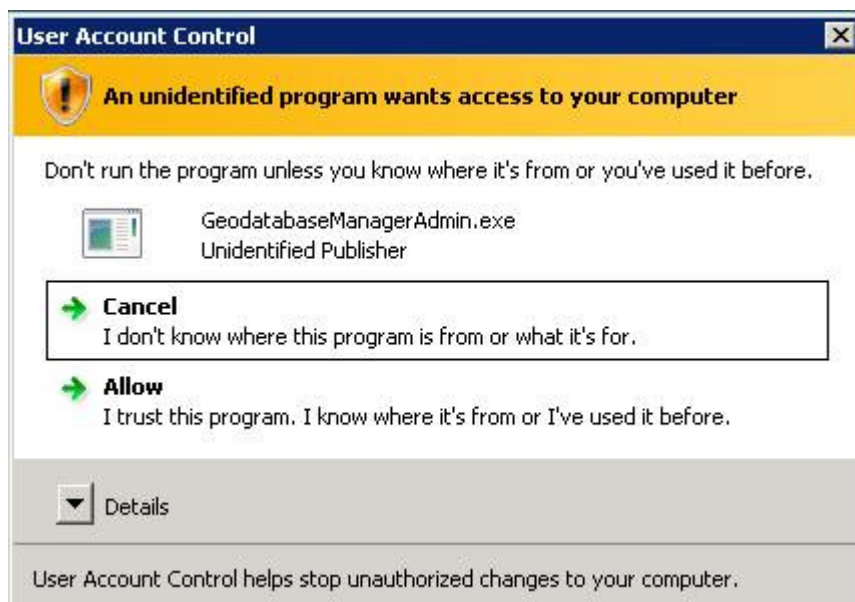


This is another example of how UAC is blocking an application from interacting with core system features; in this case, Windows services. Even if you try to **start** GDBMService1, it will fail. UAC is preventing interaction with all aspects of Windows services.

6. To work around this issue, launch GDBM as administrator:



Click 'Allow' to let GDBM run with administrator-level privileges.



Repeat steps 2 through 5 and notice that the application behaves normally.

ArcFM 9.3.1 SP1

User Account Control and the ArcFM Solution 9.3.1 SP1 Release

For the 9.3.1 SP1 release of the ArcFM Solution, both Geodatabase Manager and License Manager were updated to auto-elevate permissions. This means that the steps required to edit settings in these programs in the 9.3.1 release are no longer required if the user has administrative privileges.

Responder 9.3.1 SP1

Responder 9.3.1 SP1 and User Account Control

Responder 9.3.1 SP1 is affected by User Account Control in the following ways:

- **Starting and Stopping Responder Services:** The 'Start/Stop Responder Windows Service' entries under the Responder application on the Start menu will not work unless run as administrator.
 - 1) Click on the Start menu and locate the 'Start/Stop Responder Windows Service' entries.
 - 2) Right click on the desired action, and select 'Run as Administrator.' A small shield icon appears next to this option to denote UAC.
- **Modifying Responder configuration files:** Responder configuration files are located in the 'Program Files' directory on your computer, which is protected by UAC. Users must have 'modify' privileges assigned to edit these files. In addition, if you are running XUpdate batch files, you must run them as an administrator because they access and edit these configuration files.
 - 1) Open Windows Explorer.
 - 2) Navigate to the Responder installation directory. (Default: C:\Program Files\Miner and Miner)
 - 3) Find a .config file you wish to edit.
 - 4) Right click on the file, and select 'Properties.'
 - 5) Click on the 'Security' tab.
 - 6) Click the 'Edit' button.
 - 7) Add the user account(s) or group(s) you wish to allow to modify this file if necessary.
 - 8) Select the user you wish to give permissions to. Click the 'Allow' button next to 'Modify.'
 - 9) Click 'OK' to both dialog boxes.
- **Responder Client Installation:** There is an XUpdate that modifies the ArcMap.exe.config file during Responder Client installation. This installer must therefore be run as Administrator or else it will fail with Error 1721: A program required for this install to complete could not be run.
- **Build TroubleMaker Database Tool:** The TroubleMaker database tool in ArcMap is unable to write to the default TroubleMaker database when User Account Control is enabled. This is due to the fact that default database is installed in the application folder, to which User Account

Control restricts access. As a workaround, users can manually copy the TroubleMaker.mdb from the application folder to a different location such as their Desktop or their user's personal Application data folder. Then, when running TroubleMaker, be sure to change the path to the database to point to the location of this new database.

- **Replication Initializer Tool:** The Replication Initializer tool must be run by right-clicking and selecting "Run as administrator." Otherwise, you will see an error saying that the access to the path where the log is saved is denied. This log is located in the Program Files folders and therefore is inaccessible to non-admin users under the UAC rules.

Windows 7 User Interface Issues

In Windows 7, users have the option to change the "theme" of their desktop. Two of these themes, "Aero" and "Windows 7 Basic" will cause issues with the Responder Explorer user interface. These include:

- Certain forms appear blank until they are moved.
- The user can not manually edit time controls in forms such as "Create Incident" or "Edit Incident." The only way to change the time is to click the "Current Time" button next to the control.
- Some pop-ups (for example, a confirmation pop-up before submitting an incident in a region outside of a dispatcher's assigned regions) appeared behind other dialogs and could not be seen unless the user pressed the ALT key.
- Some required fields are not appearing highlighted in yellow as they should be (e.g. the "Executed By" field in the Restore dialog).

To avoid these issues, the "Windows Classic" theme must be used.

These will be present in the 9.3.1 SP1 release but will be fixed in the Responder release which will follow the 10.0 Compatibility Release of the ArcFM Solution.