Installing Alarm Data Interface on Microsoft Windows Vista and on Microsoft Windows 7

Last updated: 04/17/2011

Because of security enhancements Microsoft has made on its newer operating systems, additional steps are now required to install ADI on Windows Vista and Windows 7. Additionally, ADI is no longer able to be run as a Windows Service like it was on Windows 2000 and Windows XP. Instead, ADI should be installed on a computer that is usually only logged in to one account.

Installation Considerations

In most cases, you will want to run ADI from a Standard user type account as opposed to an Administrator type account. This will prevent users from being able to tamper with this and other applications on the computer. However, ADI will also run under an Administrator type account with no problem.

Another consideration that needs to be made is whether you will be running the computer with User Account Control (UAC) enabled or not. UAC was designed to keep third-party applications from making unauthorized changes on your computer without your knowledge. With UAC enabled, almost all manual actions that could potentially change or delete a file on your computer are interrupted with a prompt. You will have to authorize the action each time before a change is processed. Many users opt to disable this feature due to the high annoyance factor. You may consider disabling it also if your computer is not accessible to your general membership.

Starting with version 9.00 of ADI, the default installation location is now **C:\FDCMS\Alarm Data Interface**. We have changed this default from the *Program Files* folder because Windows would like to hide some of ADI's folders in the User area of the file structure. In our opinion, this practice caused more problems than it helped so the decision to relocate ADI out of the *Program Files* folders was an easy one. We recommend installation scenario #4 below.

User Account Control

The UAC feature in Windows Vista and Windows 7 was designed to decrease the amount of malicious file tampering caused by both applications and users. Because of this, Microsoft recommends that you run programs only when UAC is enabled. The following links will give you step-by-step instructions on changing the state of the UAC controls:

For Windows Vista, use the following link:
http://windows.microsoft.com/en-US/windows-vista/Turn-User-Account-Control-on-or-off

For Windows 7, use the following link:
http://windows.microsoft.com/en-US/Windows7/Turn-User-Account-Control-on-or-off

Installation Scenarios

In all of the following scenarios, ADI must always be run from the same Windows account. Running from multiple accounts will have unpredictable results depending on the installation scenario. All scenarios apply to both Windows Vista and Windows 7 unless noted otherwise.

1. Scenario #1 – Account Type: **Administrator** User Account Control: **Off**

   Pros
   - Easy installation.
   - Recommended for agencies that have this computer located in a locked closet or area where only administrators can physically access it.

Cons

- If unauthorized users were to gain physical access to this machine, they would have full administrator rights to it.

Installation Sequence

- Install ADI as you would any other application. After it is first run, ADI will properly create and maintain its \Logs, \Local and \Export data folders in its own default installation folder.

2. Scenario #2 - Account Type: **Administrator** User Account Control: **On**

Pros

- Easy installation.
- Recommended for agencies that have this computer located in a locked closet or area where only administrators can physically access it.

Cons

- If unauthorized users were to gain physical access to this machine, they would have full administrator rights to it.
- With UAC on at the time of installation, Windows will not allow ADI's \Logs, \Local or \Export folders to be created in the Program Files folder. Instead, Windows will create these files in an alternate folder. If other applications will need access to these folders, you will have to locate them and create a network share.

Installation Sequence

- Install ADI as you would any other application. If ADI is installed in the Program Files folder then Windows will relocate ADI's \Logs, \Local and \Export data folders to *C:\Users\[Account name]\AppData\Local\VirtualStore\Program Files\FDCMS\Alarm Data Interface*.
- If other FDCMS applications located on other network computers require access to these hidden folders, then you will need to navigate to the above path and share the *Alarm Data Interface* folder accordingly.
- The path in each FireHouse Definition File (if used) will need to be updated to reflect the location of the relocated \Export folder.

3. Scenario #3 - Account Type: **Standard user** User Account Control: **On**

Pros

- Computer can be located in an area accessible to the general membership.
- Chance of file tampering is minimal.

Cons

- With UAC on at the time of installation, Windows will not allow ADI's \Logs, \Local or \Export folders to be created in the Program Files folder. Instead, Windows will create these files in an alternate folder. If other applications will need access to these folders, you will have to locate them and create a network share.

Installation Sequence

- Install ADI as you would any other application. Windows will prompt you for an Administrator's password before continuing.

- If ADI is installed in the Program Files folder then Windows will relocate ADI's \Logs, \Local and \Export data folders to *C:\Users\[Account name]\AppData\Local\VirtualStore\Program Files\FDCMS\Alarm Data Interface*.
- If other FDCMS applications located on other network computers require access to these hidden folders, then you will need to navigate to the above path and share the *Alarm Data Interface* folder accordingly.
- The path in each FireHouse Definition File (if used) will need to be updated to reflect the location of the relocated \Export folder.

4. Scenario #4 – Account Type: **Standard user** User Account Control: **Off (initially)**

Pros

- **This is the recommended method of installing ADI to achieve the best security while maintaining the original design of the application.**
- The ADI computer can be located in an area where your general membership has access to it

Cons

- Complex Installation and setup.

Installation Sequence

- Log on to the ADI computer in to an existing Administrator account.
- Create a new Administrator type Windows account. This will be the account that ADI will always run under.
- Log in to the new account.
- Insure that UAC is Off. If it is not then turn it off and restart the computer. When the computer restarts, log back into the new account.
- Install ADI as you would any other application. After it is first run, ADI will properly create and maintain its \Logs, \Local and \Export data folders in its own default installation folder.
- Open the Windows Explorer and navigate to ADI's default installation folder: *C:\FDCMS\Alarm Data Interface*.
- Right-click on the Alarm Data Interface folder and then select *Properties*.
- Click on the *Security* tab.
- Click on the *Edit…* button.
- On the Permissions for Alarm Data Interface form, click on the *Users* group.
- Place a check mark next to the *Modify* permission in the *Allow* column.
- Click on the *OK* button.
- Click on the *OK* button again.
- Close Windows Explorer.
- Turn the UAC control ON.
- Change the Account Type from Administrator to Standard user.
- Restart the computer.
- Log back in to the new account and start ADI.