

Installation Considerations

*An extract from the Focal*Point User's Guide*

Preparing to Install the Program

In most cases, the installation and setup of Focal*Point is quite simple. Usually the only consideration is that the installation and first-run of the program be performed with local Administrative rights. This will ensure proper installation, configuration and licensing. Also note that day-to-day users may also need read/write/modify privileges for LAN drives (shares) to ensure that the Focal*Point program has proper access to the machine NC program files. This is especially true when configuring Focal*Point in a Multi-User environment that uses a "shared" database, which is generally located on a LAN drive.

Depending upon your network and related Group Policies, as well as the local PC operating system, it is not always easy to confirm full administrative read/write/modify permissions. Consult your IT manager for assistance if corporate Group Policies prevent successful installation and licensing.

Installations targeted for Windows Vista and above may have additional concerns. These operating systems do not provide full runtime privileges even when logged-in as an administrative user. As such, and before starting the installation process, it is best to right-click the setup program and select the "Run as Administrator" option. After completing the installation program you should have a program launch icon located on your desktop and also in the Focal*Point program group located in the Start>Programs list. Right-click either (or both) of these icons and again select the "Run as Administrator" option to run the program for the first time. This is an important first-step as the program is still in the configuration and licensing stage. Complete the initial configuration and licensing as directed.

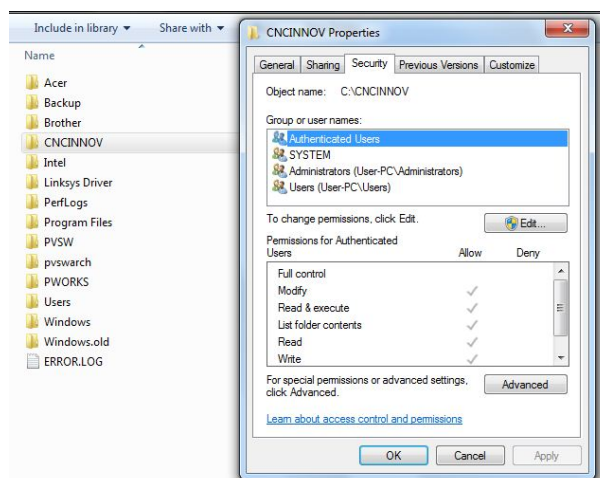
If multiple users will have login and startup rights for Focal*Point, it is best to provide on-going Administrative privileges to all users. This is done by right-clicking the shortcut and selecting the Properties option. From the Properties page, view the Shortcut tab and click the Advanced button. Ensure that the Run as Administrator option is checked. Next click to view the Compatibility tab and if available select the option to "Change settings for all users." It may also be helpful to set compatibility mode to run as Windows XP (Service Pack 3).

System Permissions

This section provides information for advanced operating system considerations. Please consult your IT manager when attempting to modify these settings.

*Also Note that although Focal*Point's installation program adds the necessary "Everyone" user group to its main working folder, named CNCINNOV, the following information is provided for IT professionals that may wish to add their own groups and privileges as required by company policies and procedures.*

In the event that several Standard Users (PC users with limited rights) will have login ability, it is easier to grant read/write/modify access to such users with Windows Security options as shown below.



As seen in this "Windows 7" example, all Authenticated Users (Users with a login name and password) have been given full read/write/modify permissions for the Focal*Point installation folder and all sub-folders. To access these settings open the Windows Explorer, right-click the CNCINNOV folder and select the Properties option. Note that permissions can only be changed by an administrative user.

As a side note this setting may also solve the problem displayed as "Error Updating Local Database / Error Number = 1" when Standard Users start Focal*Point for the first time.

It should also be understood that Focal*Point saves setup and user configuration information in the system registry. By default these registry locations allow proper access rights, but the locations are provided here for informational purposes. NOTE THAT CNC INNOVATIONS TAKES NO RESPONSIBILITY FOR CHANGES MADE TO THE SYSTEM REGISTRY.

Although changes are not likely required, the two areas of interest are:

HKEY_CURRENT_USER\Software\CNCInnovations
and
HKEY_LOCAL_MACHINE\Software\CNCInnovations

These two keys and all sub-keys may require the permissions discussed above.

Important Performance Considerations

- Be sure to check Power Saving settings for local harddrives and monitors, as well as, screen savers before attempting Drip-Feed operations.
- Avoid Buffer Over-flow errors during Drip-Feed operations by setting COMM Port hardware properties to disable FIFO buffers. See your hardware manufacturer for specific instructions. To change the native COMM port settings (COM 1) follow these general procedures

Right-Click the My Computer icon and select Manage
Select Device Manager from the Computer Management page
Expand the Ports (COM & LPT) section
Double-click COM 1 to display its Properties
Click Advanced on the Port Settings tab
Set the Buffer sliders to their lowest setting or Disable the Buffers .
Reboot the PC

Windows 7 & 8 Security Considerations

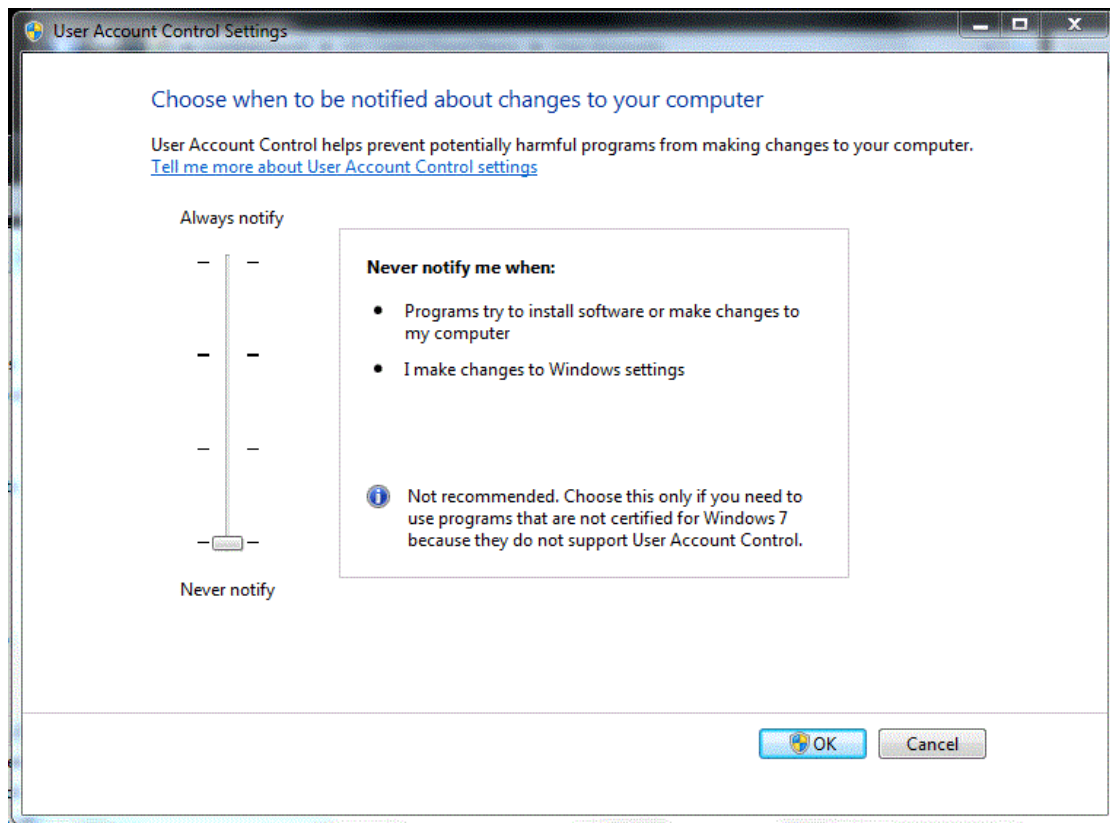
Important

Windows 7 & 8, as well as Vista, contains several new security enhancements that impact the way programs interact with the user and the operating system. To avoid complications while configuring and testing Focal*Point, CNC Innovations highly recommends that first-time users run Focal*Point with an Administrator account and that User Account Control (UAC) be set for the Never Notify option. By default, the first account created on Windows 7 & 8 will be an Administrator account. You can either use this account for setup and testing or create a new Administrator account. Do not attempt initial testing with a Standard User account.

Please keep in mind that Windows security features are an on-going project with Microsoft and are subject to change. The information discussed below is relative to the first release of Windows 7 and may very well change as operating systems mature.

Before proceeding, make certain that system permissions have been changed to allow the logged in user (Authenticated Users or specific user accounts) complete read./write/modify permissions as shown in the previous Installation Considerations section. Warning: do not assume that the Administrator account will provide the necessary permissions because even Administrators operate with Standard User permissions when running most applications. In fact, that is the purpose of the new security enhancements--to restrict full access to files and the operating system.

The User Account Control settings are located in the Control Panel > User Accounts section. At the User Accounts home screen click the option to Change User Account Control Settings and set the option for Never Notify as shown below.



How User Account Control (UAC) Limits Focal*Point Operation

- When UAC is active it will prompt the user for an acknowledgement each time Focal*Point is started. If Standard Users start Focal*Point it may also require an Administrator's password in order to proceed.
- Unlike earlier versions of Windows, UAC will stop Focal*Point from running automatically when placed in the system Startup menu. Only by setting UAC to Never Notify will this important function be possible. Search Windows help for instructions to add Focal*Point to the Startup menu.
- As of this writing Windows 7 support to run Focal*Point as a service is restricted to background operation only. Since it will not allow interaction with the desktop, running as service is not recommended.
- Access to file server mapped drives must be configured with Administrator rights. This is true even when changing an existing drive's UNC path location.
- Mapped network drives will not be available without some form of user intervention. This problem may NOT be evident to casual observers since mapped drives do appear connected when viewed from the My Computer application. The problem is that links to these drives remain inaccessible when software applications attempt to use them. Although Focal*Point will warn of connection problems at startup, the situation and solution are none-the-less quite annoying. This is especially true when you consider that Focal*Point's Multi-User Administration, DNC Program Library, the Received File Administrator, Automatic Library Transfer, and File Archiving may all refer to mapped drive locations.

Symptoms and Solutions for Inaccessible Drives due to activated User Account Controls

If Multi-User Administration (Settings menu) is enabled and points to a mapped drive location, Focal*Point may report an error activating the form during startup. Focal*Point's error log will contain the following entries.

```
Error Location 174 Err = 76  
Error Location 172 Err = 3044
```

This error can be resolved in several ways. The first is a quick work-around. During startup when Focal*Point displays the message that you appear to be using the shared location for the first time, simply click the Cancel button to run Focal*Point in local mode. If you then open the File menu and select Send (browse), you will be shown a listing of all drives. Inaccessible drives display with a large red X through them. If you click the shared drive it will open normally and will remain accessible for the remainder of your windows session. If you exit Focal*Point and restart, it will run as normal.

A better and more permanent way to solve this problem is to set the Multi-User shared location with a Universal Naming Convention (UNC) path rather than the usual mapped drive location. The first step is to establish a connection as described above and then use the Multi-User Advanced button to enter the UNC path. UNC paths are specific to your network but typically take the following form, \\ServerName\FolderName. This method works well because network shares are not affected by UAC settings, to date Microsoft only restricts mapped drives.

UNC paths work very well when you simply need to designate a shared folder location for Focal*Point's working database. However, there may still be additional considerations. If your Local Area Network uses mapped drives versus local folders for the storage of NC programs, you may still have a problem accessing these files from within the DNC program library. Note that this restriction impacts Sending, Receiving, Remote Program Requests and Editing. To test this condition, simply double-click the DNC ID for an established library entry. If the editor fails to open the file it is an indication that the link to mapping drive has not been established. Again a simple correction is to click the Send button and attempt to browse the inaccessible drive. The drive will then be accessible for the remainder of your Windows session.

As shown by the discussions above, User Account Control impacts Focal*Point's operation in several ways. It is for this reason that CNC Innovations warns against using UAC during the initial setup and execution of Focal*Point.

However, recognizing that some companies will want to take advantage of the increased security that UAC offers, and the possibility of running Standard User accounts, we offer the following for informational purposes only. Note that it is not the intent of CNC Innovations to provide help for Windows operating systems. For additional information please refer to the Windows Help program, newsgroups, blogs, and Microsoft support.

Since the release of Windows Vista, Microsoft has acknowledged and defended the reason for restricting mapped drives as discussed above. To that end Microsoft has issued a knowledge base article discussing the situation. Please refer to <http://support.microsoft.com/kb/937624>

As stated by Microsoft:

"The article briefly describes the drive mapping situation when UAC controls are enabled and provides the following work-around. Use the net use command together with a UNC name to access the network location. For example, at a command prompt, type the following command, and then press Enter:"

```
net use \\<computername>\<sharename> /user:<username>
```

If you are particularly ambitious and rushed off to try the above example you found that it did not work as listed. The Microsoft article provides a very generalized example that should be modified to account for mapped network drives not being available, which is the case for Focal*Point and other programs that rely on mapped network shares. For example, suppose that your Focal*Point multi-user share location and NC programs are contained on a network drive share such as \\Companyshare\DNC, which is mapped to drive H:.

First open notepad and create a desktop file named Enablemaps.cmd, and enter the following command.

```
net use H: \\Companyshare\DNC [user Password] /user:<username> /Persistent:YES
```

Pause

- You must substitute Companyshare\DNC with the server and location used by your network.
- [user Password] should be the password of the user with rights to the share location
- <username> is the name of the user with rights to access the shared location.
- Persistent merely keeps the share active and Pause keeps the command window open until the Enter key is pressed. In other words you can verify that the command was successful.

Here is how the command line might look:

```
net use H: \\Companyshare\DNC 1234 /user:Joe /Persistent:YES  
(If the share location contains spaces add quotes - "\\Company Share\DNC Programs" )
```

Points to remember before starting Focal*Point:

- If the local user is part of the administrator group, it is important to right-click the file and select the "Run as Administrator" option.
- If the user is standard simply double-click the file to run it.
- The mapped drive will remain active for the entire Windows session, but it will be necessary to run the program every time Windows is re-started.

As an alternative to the above work-around, Microsoft has a technet article showing a registry change to accomplish the same results without having to run a separate command file.

A more permanent solution which used to be included in the KB article is now described in the following Microsoft Technet article :

<http://technet.microsoft.com/en-us/library/ee844140%28v=ws.10%29.aspx>

The solution requires a small change to the Windows' registry to Enable Linked Connections. Note that CNC Innovations has successfully tested this workaround using a Windows 7 administrator account.

To configure the **EnableLinkedConnections** registry value, follow these steps:

Click Start, type regedit in the Start Search box, and then press ENTER.
Locate and then right-click the following registry subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Point to New, and then click DWORD Value.
Type EnableLinkedConnections, and then press ENTER.
Right-click EnableLinkedConnections, and then click Modify.
In the Value data box, type 1, and then click OK.
Exit Registry Editor, and then restart the computer.