OpenFox™

Desktop Administrator Manual

Version   3.00
Revised   8/23/2013

CPI — The OpenFox Company

Computer Projects of Illinois, Inc.
475 Quadrangle Drive, Suite A
Bolingbrook, IL 60440
(630) 754-8820

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Chapter 1 – Introduction and Overview

OpenFox™ Desktop is an application framework which provides a secure and reliable connection to the OpenFox™ Message Switching system. Through the message switching system, users may communicate with remote data sources to obtain or manage information critical to fulfilling the mission of law enforcement, public safety, and affiliated agencies. Such data sources may include the FBI's National Crime Information Center (NCIC), state Department/Bureau of Motor Vehicles, state warrant/wanted/property files, criminal history databases, sexual offender registries, Department of Corrections, and many more.

The message switching system is typically governed by an agency such as State Police, Highway Patrol, Department of Public Safety, State Radio, etc. This agency is responsible for maintaining and enforcing a set of rules and regulations that govern system access, and this agency is referred to as the "governing agency" throughout the rest of this manual. Many of the rules and regulations set in place by this agency are the direct result of maintaining compliance with the FBI Criminal Justice Information Services (CJIS) Security Policy. As such, please understand that the governing agency may not have complete control over the rules and regulations that govern system access.

Desktop integrates OpenFox™ user applications into a unified and secure environment with a consistent look and feel. The OpenFox™ user applications that plug into Desktop are known as Modules, and this manual contains information that is appropriate for users of any OpenFox™ user application. Some commonly integrated Modules are listed below:

- OpenFox™ Messenger
- OpenFox™ Mobile Messenger
- OpenFox™ Criminal History Administrative Client
- OpenFox™ Sexual Offender Administrative Client
- OpenFox™ Archive Retrieval
- OpenFox™ Configurator (version 7)
- OpenFox™ Form Configurator
- OpenFox™ Interceptor

1.1 – Who Is This Manual For?

This manual is intended for use by personnel who are involved in installation and support of OpenFox™ Desktop end users. This includes the support and administrative staff of the governing agency as well as information technology support staff. This manual assumes a level of familiarity with information technology terms and concepts that may not be held by every OpenFox™ Desktop end user.

1.2 – Minimum System Requirements

Desktop is most commonly installed on Windows computers, and the system requirements for different versions of Windows are listed below. If a computer system does not meet or exceed the following specifications, then the performance of OpenFox™ Desktop may not be sufficient for a satisfactory user experience.

Several of the versions of Microsoft® Windows™ listed below are no longer officially supported by Microsoft®. While CPI remains committed to supporting its customers and user base to the best of its ability, it may not be possible to provide complete support for OpenFox™ Desktop if it runs on an operating system that is no longer officially supported by Microsoft®. To resolve issues, it may be necessary to upgrade the device to a version of Windows™ that is supported. For more information regarding the Windows™ product lifecycle, please consult the following resource available from Microsoft®:

http://windows.microsoft.com/en-us/windows/products/lifecycle

Common Requirements for All Windows Systems

- Microsoft® Internet Explorer 5.5 (and higher) , Mozilla 1.4 (and higher), or Firefox 1.0 (and higher)
- The Windows™ user profile must have write access to the directory paths as explained in the "Local Directory Structure" section

Windows 2000 or earlier

- Intel® Pentium® II Processor or equivalent (800 MHz or faster)
- Microsoft® Windows 98 Second Edition, Microsoft® Windows ME, Microsoft® Windows 2000,
- 256 MB of System RAM – 512 MB is preferred
- 20 GB Hard Drive, with 100 MB Available

Windows XP

- Intel® Pentium® III Processor or equivalent (1 GHz or faster) – 1.5 GHz is preferred
- Microsoft® Windows XP (Professional or Home), or Microsoft® Windows Server 2003 (Web, Standard, Enterprise, or Data Center Edition)
- 512 MB of System RAM – 1 GB is preferred
- 40 GB Hard Drive, with 100 MB Available

Windows Vista

- Intel® Pentium® IV Processor or equivalent (1.5 GHz or faster) – 2 GHz is preferred
- Microsoft® Windows Vista (Basic, Home Premium, Business, or Ultimate)
- 1 GB of System RAM – 2 GB is preferred
- 80 GB Hard Drive, with 100 MB Available
- Support for DirectX 9 graphics with:
    - WDDM Driver
    - 128 MB of graphics memory (minimum)
    - 256 MB of graphics memory (preferred)
    - Pixel Shader 2.0 support in hardware
    - 32 bits per pixel

Windows 7

- Same requirements as for Windows Vista plus the following:
- Microsoft® Windows 7 (Basic, Home Premium, Business, or Ultimate)
- 2 GB of System RAM – 4 GB is preferred

Windows 8

- Same requirements as for Windows 7 plus the following:
- Microsoft® Windows 8, Windows 8 Pro, or Windows 8 Enterprise
    - Windows 8 RT is *not* supported

1.3 – Java

OpenFox™ Desktop is a Java application, and thus Java must be installed and properly operating in order for Desktop to run. OpenFox™ Desktop supports any version of Java equal to or later than Java version 1.5. At the time of this writing, the current release is Java 7, and CPI recommends installing this version to have the latest updates, patches, and resolutions to any security vulnerabilities.

OpenFox™ Desktop requires the Standard Edition of Java. In addition to the Standard Edition, Oracle publishes Java Mirco Edition (for mobile devices) and Enterprise Edition (for servers). Desktop will not operate correctly under either the Micro Edition or the Enterprise Edition. Please be sure to install the Java Standard Edition on any device which will be running Desktop.

You may also see references to the Java Development Kit (JDK) in addition to the Java Runtime Environment (JRE). The Java Development Kit contains the Java Runtime Environment, but it also includes many tools and features which are only applicable to software developers. Although Desktop will operate correctly if the JDK is installed, it

only requires the JRE. Because the JDK is a much larger download and a more involved install, CPI recommends that the JRE is installed on end user devices.

When downloading and installing Java, you may also have the choice of installing either the 32 bit or 64 bit version. Please install the Java applicable for the operating system on your device. For example, if the device has a 32 bit version of Windows, you must install the 32 bit version of Java. If the device has a 64 bit version of Windows, then you should install the 64 bit version of Java.

The latest release version of the Standard Edition Java Runtime Environment may be downloaded from the following site:

<p style="text-align:center">http://www.java.com</p>

If you are looking for more options, then the following site allows you to download specific versions of the Java platform:

<p style="text-align:center">http://www.oracle.com/technetwork/java/javase/downloads/index.html</p>

1.4 – The CPI Folder

OpenFox™ Desktop requires full permissions to specific locations on the local hard drive of the device. If this access is not available due to security policies or computer configurations, then Desktop will not be able to launch or run. The user must have full access to CPI folder and to the Java Web Start™ cache folder. This section explains the requirements of the CPI folder. The Java Web Start™ cache folder is described in the following section.

<p style="text-align:center"><code>%SystemDrive%\CPI</code>
Default location of the CPI folder</p>

Please note that some governing agencies have chosen to change this folder to a different location. Please check with your governing agency if this is the case.

The CPI folder contains Desktop and Module application data. This includes the Desktop registered license file, the local cache of Desktop resources, and any Module application data. In order to operate correctly, the Windows™ user profile that is running Desktop must have full write access to the CPI folder, including the following permissions:

- Create and delete subfolders
- Create, delete, and write to all files under all subfolders

Under the CPI folder is a subfolder named Desktop. This directory contains the registered license file, the Desktop log file, and the cache directory. If a particular Module requires disk access to store application data (i.e. the Messenger mail file), then this application data is stored in a subfolder under the CPI folder. For example, OpenFox™ Messenger saves its data under the **CPI\Messenger** folder. For more information on the disk access required by a specific Desktop Module, please consult

the User Guide for that Module. You can determine the exact location of the CPI folder from within Desktop by opening the About OpenFox™ Desktop item from the Help menu.
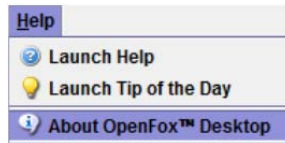
Access the about window

Select the Desktop item on the left hand side of the window and select the General tab. Scroll down to find the Desktop Information group and you will find the exact location of the CPI folder, the cache directory, and the registered license file as shown below.
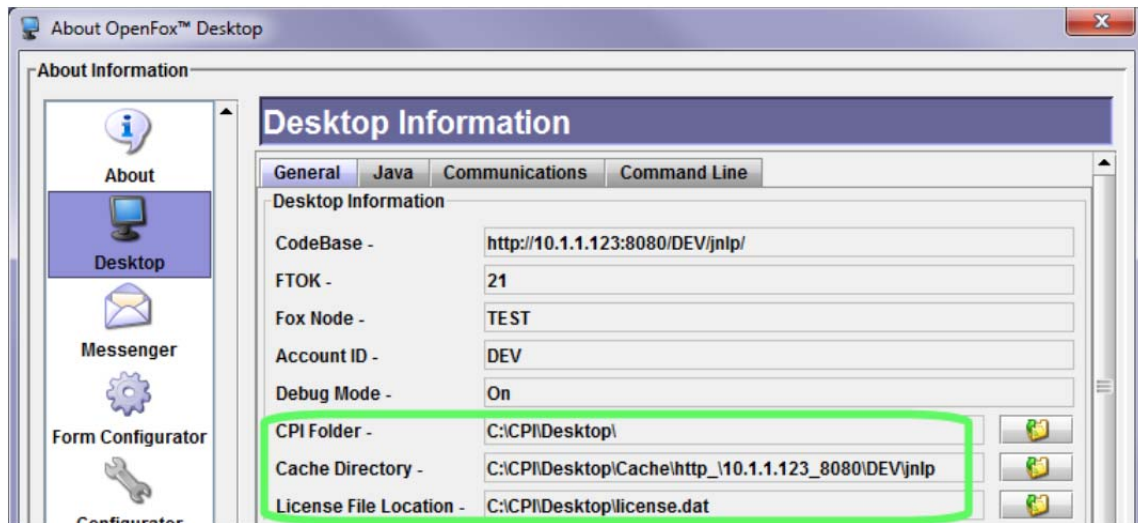
Desktop General information with the CPI folder, cache directory, and license file locations highlighted

1.4.1 – Registered License File

When OpenFox™ Desktop is registered on a device, the registered license file is created on the local disk. This file is stored under the **CPI\Desktop** folder and is named **license.dat**. This file is encrypted and contains information that identifies this particular copy of the Desktop software. If this file is moved or deleted, then the user will be asked to register Desktop the next time the software is launched.
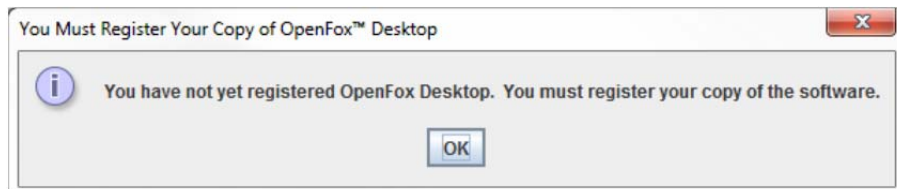
Notification that the registered license file is missing or corrupted

1.4.2 – Desktop Log
The Desktop log maintains a record of routine and exceptional events that occur during operation of the software. This information can be helpful in troubleshooting and diagnosing issues that the end user may encounter. The Desktop log is comprised of two files on the local device disk. They are **index.log** and **desktop.log**, and these files are saved under the **/CPI/Desktop** folder.

```
%SystemDrive%\CPI\Desktop\index.log
%SystemDrive%\CPI\Desktop\desktop.log
```
The files which comprise the Desktop log

1.4.3 – Cache
The cache subfolder holds local copies of application resource files. These resource files are stored locally to reduce bandwidth requirements while the application runs. For example, you will find copies of the NCIC vehicle manufacturer and gun manufacturer code lists in the cache. When these resources are updated on the message switching system, new versions are downloaded and stored in the local cache.

```
%SystemDrive%\CPI\Desktop\Cache
```
The local cache directory

1.4.4 – Test and Development Systems
When running OpenFox™ Desktop against a non-production system (i.e. the test or development system), the CPI folder is located in a different location. This feature allows you to run a copy of Desktop against the production system and a copy of Desktop against the test system. Because both copies write to a different location for the CPI folder, they will not conflict with each other. When running against such a system, the location of the CPI folder is determined as follows:

```
%SystemDrive%\CPI\Desktop\TestAndDev\
http_\%HOST%_%PORT%\%CONTEXT%\jnlp\CPI
```
Location of the CPI folder for non-production systems

The %HOST%, %PORT%, and %CONTEXT% values are determined from the URL address of the OpenFox™ Desktop launch page.

1.5 – Web Start Cache

In addition to the CPI folder (as described in the previous section), the Windows™ profile running Desktop must have write access to the Java Web Start™ Temporary Internet Files cache. When the application is launched for the first time, the application code is downloaded and saved in the Web Start cache. The user must have full write access to this location in order to run Desktop. For more information on the Java Web Start cache, please see the following section [3.1.3 – Java Web Start Cache].

1.6 – Hardware Fingerprint

Certain OpenFox™ Desktop installs are configured to require a hardware fingerprint. The fingerprint is constructed from forensic identification information gathered from the device which is launching Desktop. This feature enables Desktop to provide advanced identification of the physical device.

When the software is first registered, the fingerprint is stored and associated with the product key used to register the device. Each subsequent time that Desktop is launched, the fingerprint is constructed and compared to the fingerprint on file. If the fingerprints do not match, then Desktop does not launch.

Because the fingerprint is constructed from forensic identification information of the device, changing hardware components in the device may alter its fingerprint. If this situation occurs, the Desktop license will need to be unregistered, and then the software will need to be registered from the device once more. Marking the license as unregistered is typically performed by the administrative or support staff at the governing agency. For more information on license management, please see [4.4 – License Administration].

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 2 - Installation

This chapter describes the process of installing OpenFox™ Desktop on a computer. Prior to installing the software, please make sure that the device is capable of running Desktop and that it has been correctly configured. Please see the previous chapter for more information on this topic.

To install Java on the computer, you will need to have administrator privileges on the system. To install Desktop on the computer, you only need the disk access rights as described in sections [1.4 – The CPI Folder] and [1.5 – Web Start Cache].

Please note that if you are running Windows Vista or a later version of Windows, then the Desktop application will only be installed for the Windows™ user who is currently logged into the computer. If multiple Windows™ users will be running Desktop, then the application should be installed for each Windows™ user. Please note that this does not apply to Java; when Java is installed on the computer, it is installed for all users. For more information on this topic, please see section [1.3 – Java].

2.1 – Installing from CD

This section assumes that you have been provided with an OpenFox™ Desktop install CD. If you are installing from the launch page, please see the following section.

The first step to install Desktop is to insert the CD into your computer CD or DVD drive. After inserting the disc, the install program should automatically open. If the application does not come up, then you may need to follow the below procedure:

- Double click the My Computer icon
- Double click the CD/DVD drive. This is typically the D: drive
- Double click the file named **autorun.exe**

The Desktop install window

If the Install Java Runtime button is greyed out, you already have a compatible version of Java installed on this computer. You may skip the following section and jump directly to the section titled Installing Desktop.

2.1.1 – Installing Java Runtime Environment from CD
To install the Java Runtime Environment from the CD, simply click on the Install Java Runtime button. Please wait as the Java installer loads. When the installation has completed, please refer to section [2.3 – Installing the Java Runtime Environment] for specific instructions on installing Java.

After Java has been successfully installed on the device, you are directed back to the Desktop install window. It may take a few moments for the install window to detect that Java has been installed. Please wait while it does this. After the install window has detected Java, the screen should update so you can click the button to install Desktop.

The Desktop install window after Java has been installed

2.1.2 – Installing Desktop from CD
To install OpenFox™ Desktop from the CD, click the Install OpenFox Desktop button. This should be the second button on the screen. If this button is greyed out, and nothing happens when you click on it, then you must first install the Java Runtime Environment. Please see the previous section for instructions on this topic.

When you click the button, Java Web Start™ launches and loads the Desktop application code from the CD. Please wait until Java Web Start™ has finished loading all the Desktop application files.
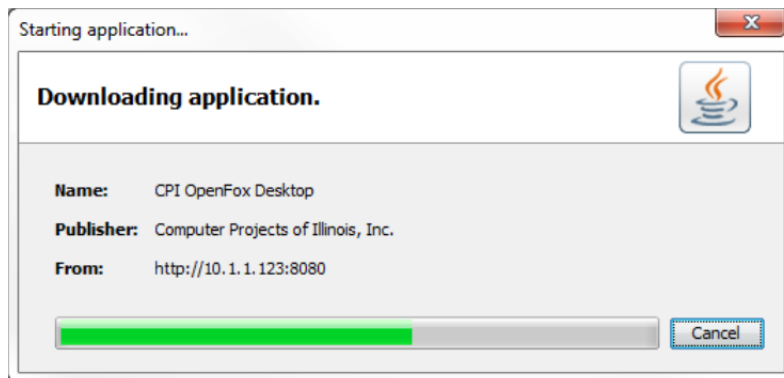
Java Web Start installing the application files from CD

When all files have been loaded, you will see the following confirmation window.
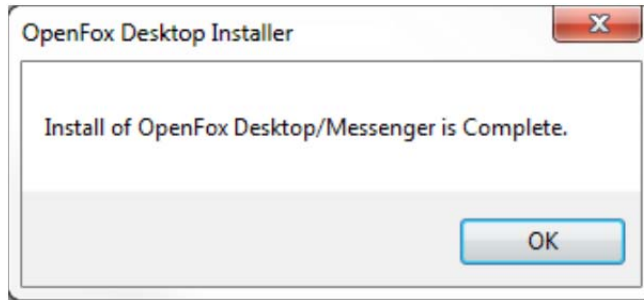
Confirmation that Desktop has been installed

After Desktop has been installed, click the button to go to the web portal, and then jump ahead to section [2.5 – Desktop Registration] for further instructions.

2.2 – Installing from the Web Portal

This section describes the process of installing the application from the web portal directly from your Internet browser. If you have been provided with an install CD, please refer back to the previous section.

The first step to installing Desktop from the web portal is to open the web portal in your Internet browser. You should have been provided with the address of the Desktop web portal. If you do not have the address, please contact your governing agency for this information. When you navigate to the web portal in your Internet browser, you will see a display similar to the following.


The Desktop web portal screen

You should bookmark the web portal address or create a shortcut to it from your Windows™ Desktop so that you may easily access the page in the future.

If the Java Runtime Environment has not been installed on this computer, then you should first click the Download Java Runtime Environment link. If you do not have a compatible version of Java installed on the computer and you attempt to launch the application, you will see one of the following messages.
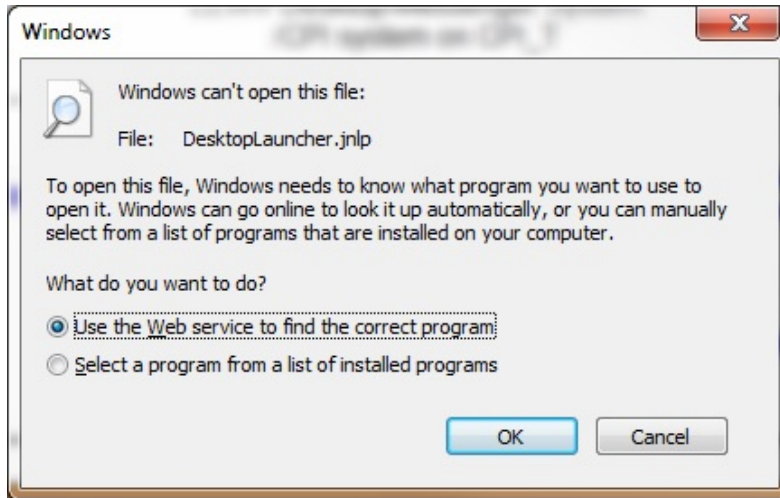
Attempt to launch without Java installed
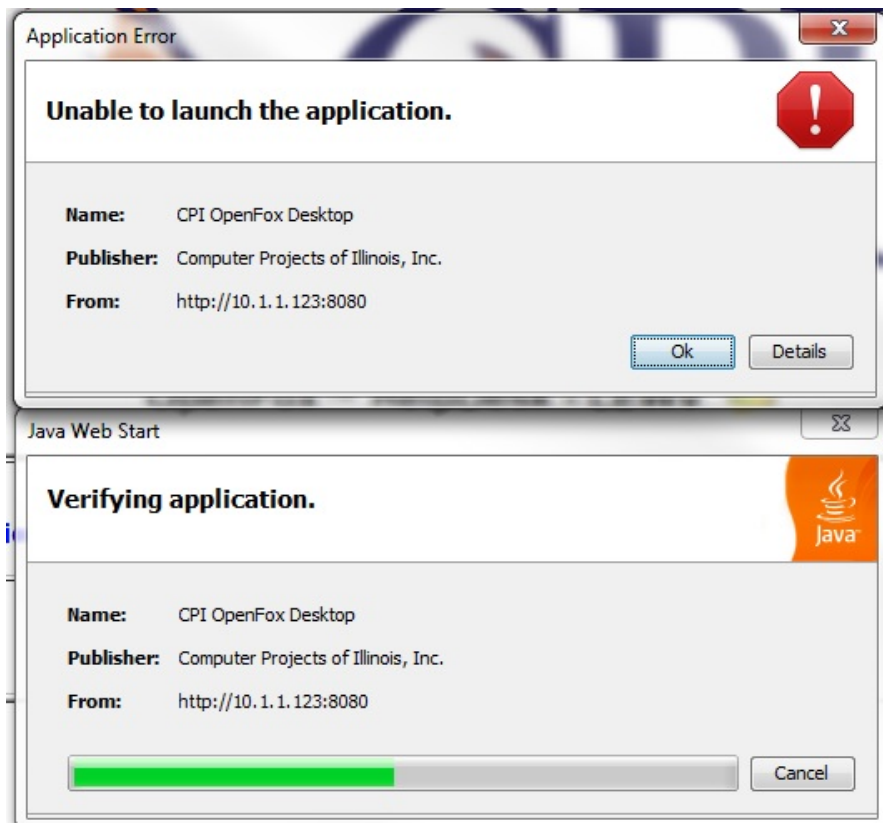
Attempt to launch with an incompatible version of Java installed

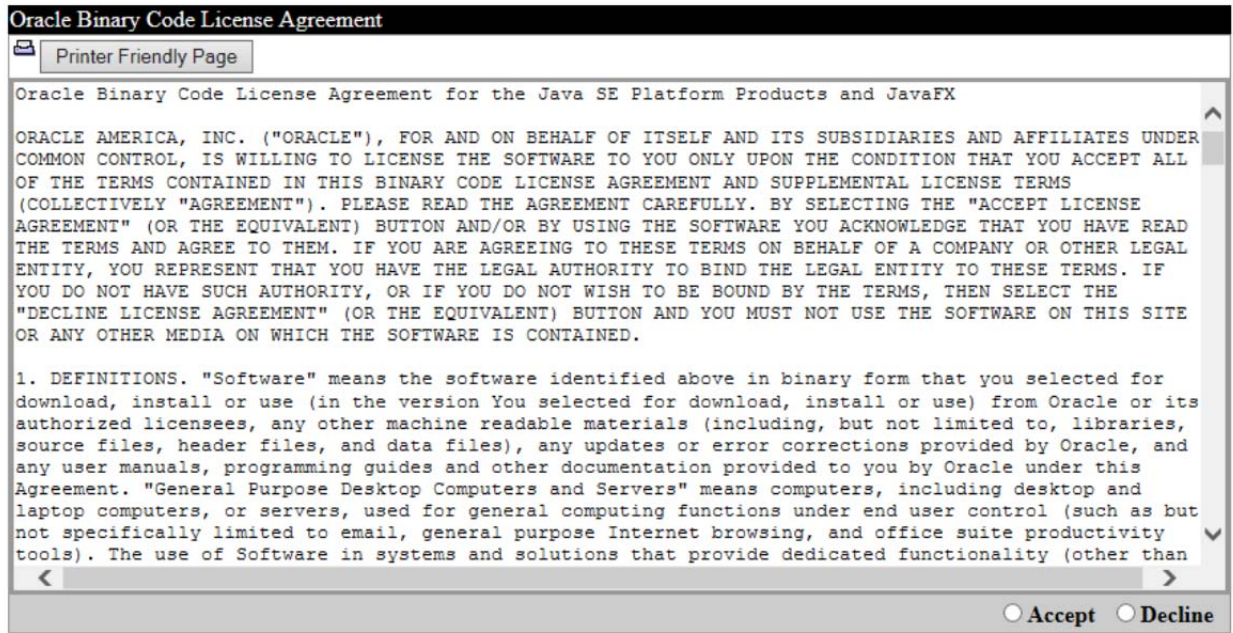## 2.2.1 – Installing Java Runtime Environment from Web Portal

To install the Java Runtime Environment from the web portal, click the Download Java Runtime Environment link. This directs you to the Oracle Binary Code License Agreement for the Java SE Platform. Please read through the license agreement. If you agree to the terms, choose the Accept item and click Continue. If you do not agree, you will not be able to download Java.

The Oracle Binary Code License Agreement for the Java SE Platform
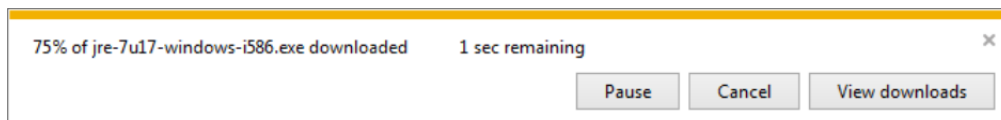
When you are prompted to download the Java installation file, click on the Run button.
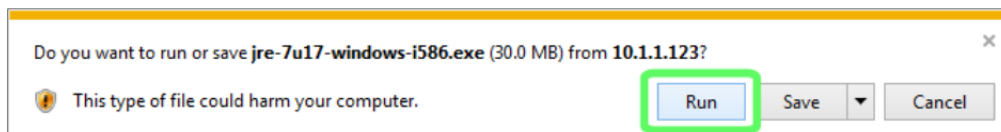
Run the file to install Java

Please wait while the file is downloaded to your computer.

The Java install file is being downloaded

When the download completes, the Java Runtime Environment will be installed. At this point, please refer to the following section [2.3 – Installing the Java Runtime Environment] for further instructions.

2.2.2 – Installing Desktop from Web Portal
To install OpenFox™ Desktop from the web portal, click the link to Launch the OpenFox™ Desktop. Java Web Start will launch and it will download and install the application on the computer. Please refer to section [2.4 – Installing OpenFox™ Desktop] for instructions on installing Desktop. After installing Desktop, please go to section [2.5 – Desktop Registration] to complete the install.

2.3 – Installing the Java Runtime Environment

This section contains information about running the Java Runtime Environment Installation program. These instructions are the same whether you are installing from a provided CD-ROM or directly from OpenFox™ Desktop Web Portal. Please refer to those sections for instructions specific to your situation.

When you first run the Java Runtime Environment Installer, you may see the following security warning. Click on the "Run" button to continue.
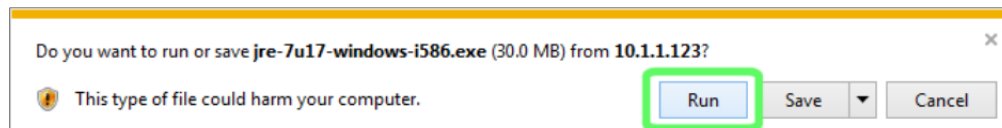
Internet Explorer security warning

At this time, you should make sure that all other applications running on your computer are closed. This is especially important for any anti-virus applications that you may be running. You *must* disable your anti-virus program and close any other applications running on your computer before continuing.

The Java Runtime Environment Installer then launches. The initial screen provides links to additional information regarding the Java install. You may also choose to view the license agreement you accept by installing Java. To accept the license agreement and install Java, click the Install button.
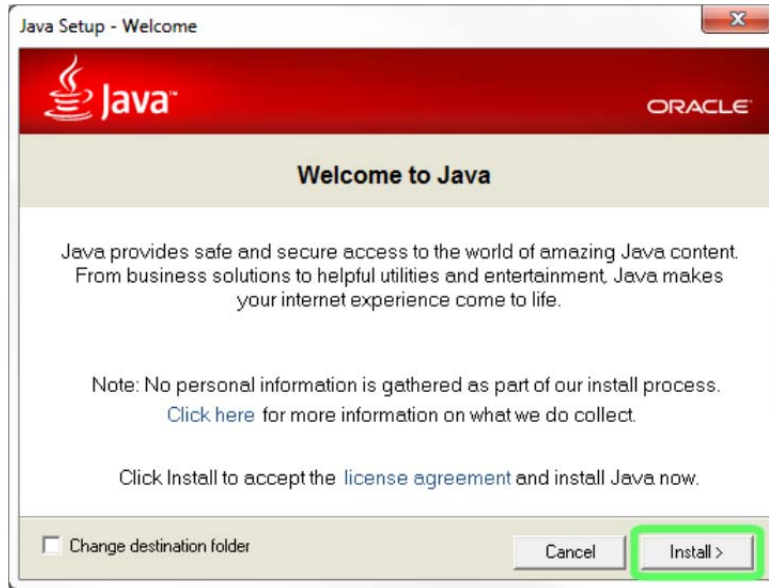
Initial Java install screen

Java is now installed on your machine. Please be patient as the software is installed and configured. This process may take several minutes.

Java is being installed

After the install is complete, you are directed to a confirmation screen. This screen provides a link to instructions regarding how to change the automatic update behavior for Java. Please consult the Java update guidelines recommended by your governing agency for more information.

Java has been installed

You may have to restart your computer to finish the installation. After your computer has rebooted, you can launch OpenFox™ Desktop and resume working in your other applications.   Please go back to the proper section of this chapter for further instructions.

2.4 – Installing OpenFox™ Desktop

This section contains information about installing the OpenFox™ Desktop application. These instructions are the same whether you are installing from a provided CD-ROM or directly from the web portal. Please refer to those section for instructions specific to your situation.

OpenFox™ Desktop is a Java Web Start application, and the installation is performed via Web Start. You are presented with a progress screen as the application is installed. Please wait while the application files are loaded.
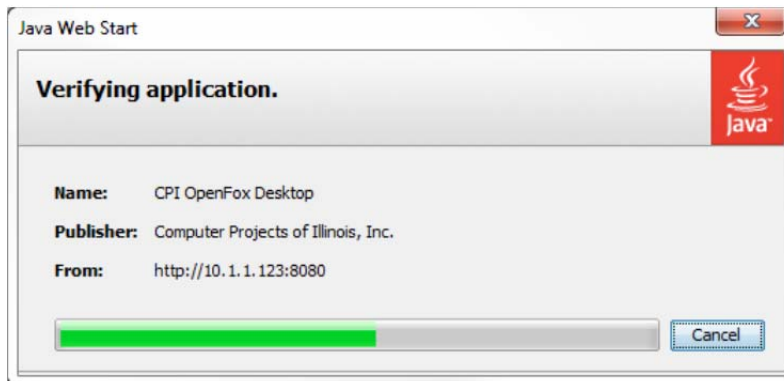
Desktop is being installed

When the installation is complete, please refer back to the proper section of this chapter for further instructions.
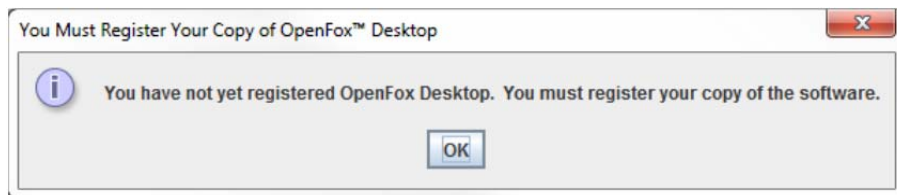
2.5 – Desktop Registration

This section contains information on registering your copy of OpenFox™ Desktop. It assumes that you have already installed the Java Runtime Environment and Desktop. If you have not completed those steps, please refer back to one of the earlier sections in this chapter.

To register OpenFox™ Desktop, you need the following information:

- Desktop Product Key
- Your OpenFox™ Agency ID
- The terminal mnemonic (or station name) of your workstation   *--or--*
- The name of the LIST class station if registering a pool or restricted use license

This information should have been provided to you by your supervisor or by your governing agency. If you do not have this information, please contact your governing agency to obtain this information before proceeding.

Access the Desktop web portal and click the link to Launch the OpenFox™ Desktop. You will receive a message that you have not registered. Click the OK button to continue.

You must register

The registration application is now downloaded to your computer. Please wait while the file is downloaded.
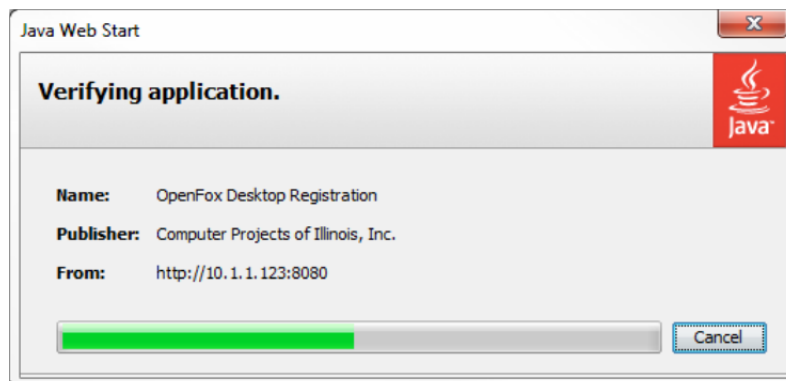
The registration application is being downloaded

After the download has completed, you are presented with the registration screen. Enter the information that has been provided to you into this screen. This includes:

- Product Key – enter the Desktop product key
- Agency – enter the ID of your OpenFox™ Agency
- Default Station – enter the terminal mnemonic of your workstation –or—
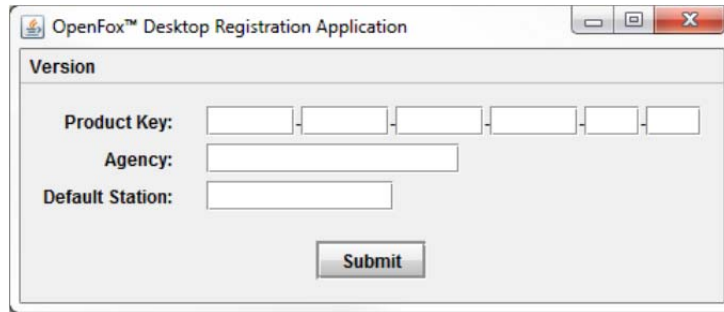- Default Station – enter the name of the LIST station if registering a pool or restricted use license

The registration application

Click the Submit button after filling in the information. This registers your copy of OpenFox™ Desktop and identifies your device as the terminal identified by the mnemonic that you entered. After a short delay, you are presented with the following confirmation screen.
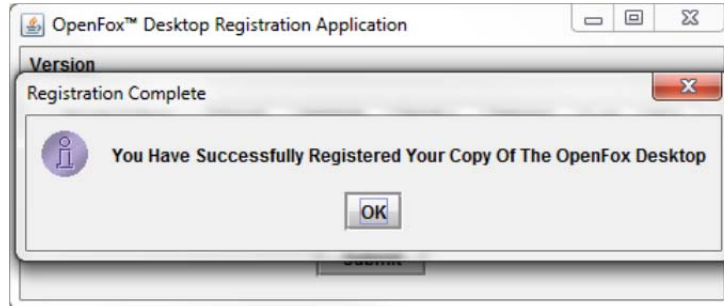
Registration success

If you receive an error notification, please double check that the information you have entered matches the information provided to you by your governing agency. If the information is correct and you continue to receive the error, please contact your governing agency support personnel.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 3 – Device Administration

This chapter includes information on performing device administration for terminals running OpenFox™ Desktop. This chapter is intended for use by information technology administrative or support personnel.

3.1 – Java Control Panel

The Java control panel window provides several options for managing the Java Standard Edition Platform that is installed on the device. To access the control panel under Windows™, open the Windows control panel, locate the Java item, and double click on it. Please note, you may need to switch the control panel to "classic" mode to find the Java item.
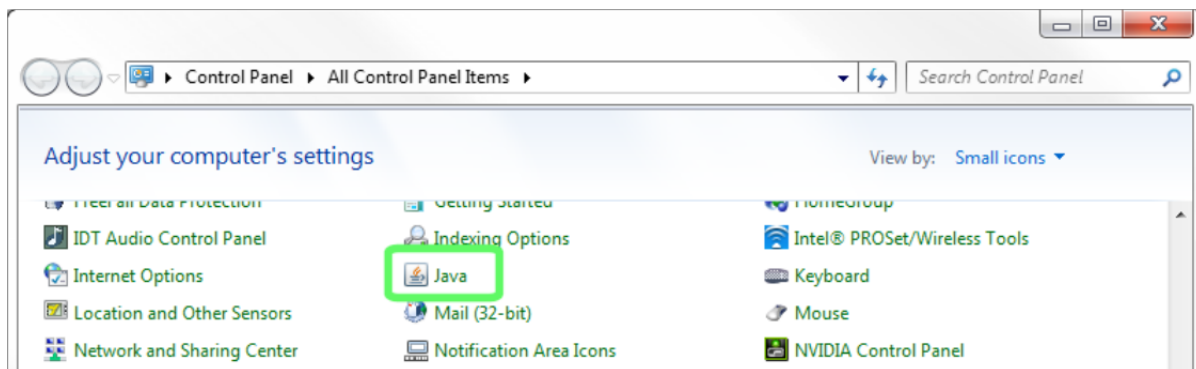
Java item under the Windows Control Panel

After opening the Java control panel, you are presented with the following display.
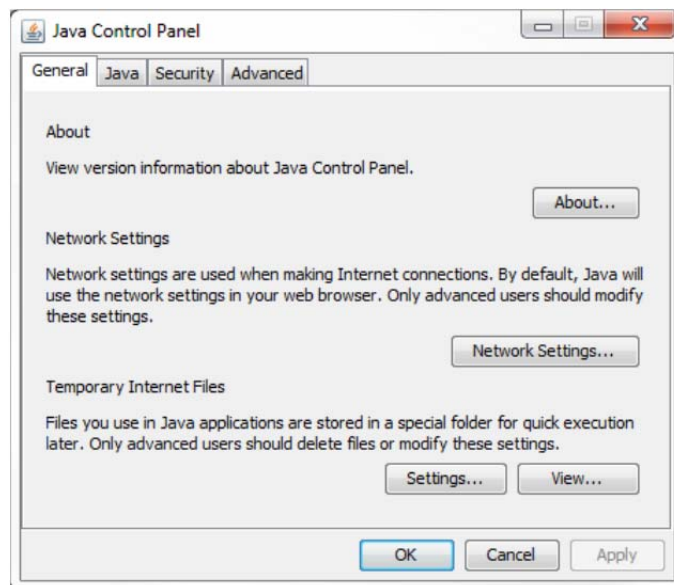
Java Control Panel

3.1.1 – Java Versions

For compatibility or performance issues, it may be necessary to specify which version of Java is used with OpenFox™ Desktop. There have been occurances of bugs in Java versions which adversely affect the operation of Desktop. Although these bugs are typically fixed in a timely release of a new Java version, it may be necessary to downgrade Java when running Desktop.

Please note that any changes made to these settings do not take effect until the next time that Desktop is launched. Changes made to these settings have no effect on Desktop if it is currently running. From the Java Control Panel, select the Java tab and click the View button
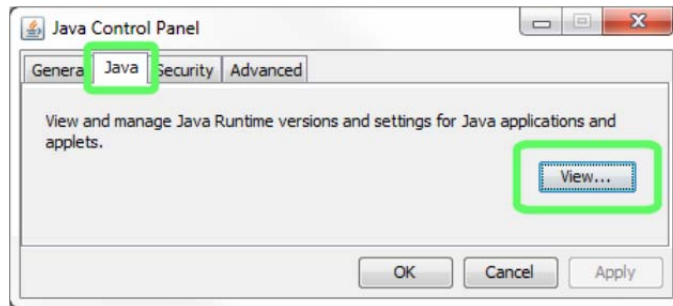

Access to Java Runtime Versions

The next window lists every version of Java that is installed on the device. You can check or uncheck the boxes under the Enabled column to enable or disable specific versions of Java. Desktop typically runs under the most recent Java version that is enabled on the device. For example, the below window shows that there are two versions of Java installed on this device, 1.7.0_06 and 1.6.0_31. Notice that version 1.7.0_06 is disabled. This means that when Desktop launches, it will run under version 1.6.0_31, since that is the most recent enabled version on this device.
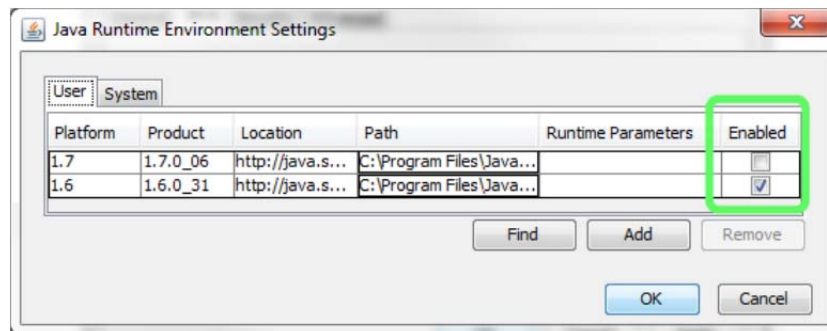
Use the Enabled column to enable or disable specific Java versions

3.1.2 – Java Console
Desktop sends diagnostic information to the Java Console window; however this window does not open by default. You have to adjust a setting in the Java Control Panel to request that this window opens when Desktop launches.

Please note that any changes made to this setting does not take effect until the next time that Desktop is launched. Changes made to this setting have no effect on Desktop if it is currently running. From the Java Control Panel, select the Advanced tab.
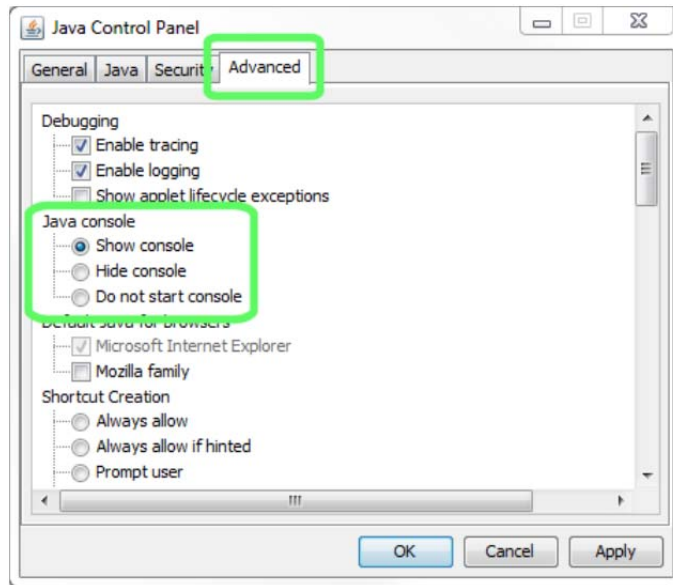
Java Console options listed under the Advanced tab

There are three options under the Java console category. You can choose to show console, hide console, or do not start console. If you select show console, then the Java Console window opens when Desktop is launched. If you select either of the other options, then the console window is not displayed. For systems at or near the minimum system requirements, choosing do not start console may result in better performance.

When the show console option is selected, the Java Console Window opens when Desktop is launched. This window typically appears in the upper left hand corner of the screen. Desktop reports diagnostic information to this window as the software runs. To change what information is reported to this window, you can adjust the parameters passed to Desktop, and for more information on this topic, please see the following section [3.2.3 – Desktop Parameters].
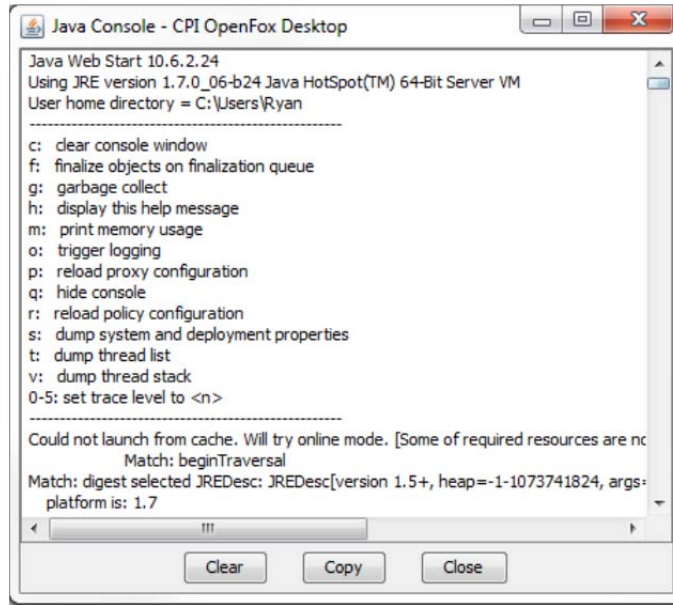
Example of the Java Console window

3.1.3 – Java Web Start Cache
The Java Web Start cache contains a local copy of the application code for Java Web Start applications. Because OpenFox™ Desktop is a Java Web Start application, the Desktop application code is saved in this location. When Desktop is installed or updated, the application is saved into the cache, and you can delete the application from the cache via the Java Control Panel.

As of Windows Vista and later versions of Windows, the location of the Web Start cache may not be changed. This means that the cache location is forced to be located under the user's Windows profile "AppData" folder. While a user should have write access to this folder by default, this also means that each user has a different copy of the Web Start cache. Thus application updates will be downloaded separately for each Windows™ user that launches Desktop.

You can determine the location of the Web Start cache by clicking the "Settings…" button under the General tab.
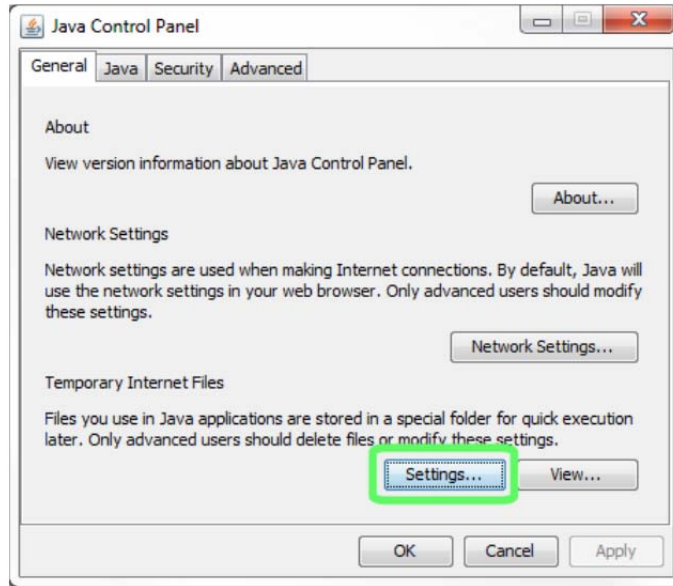
Temporary Internet Files Settings button

The Temporary Files Settings screen displays the location of the cache directory. You can also configure how much disk space is allocated for cache storage, as well as to delete the contents of the cache. Please note that if you choose to delete the cache files, then the entire Desktop application will be downloaded the next time the application is launched.
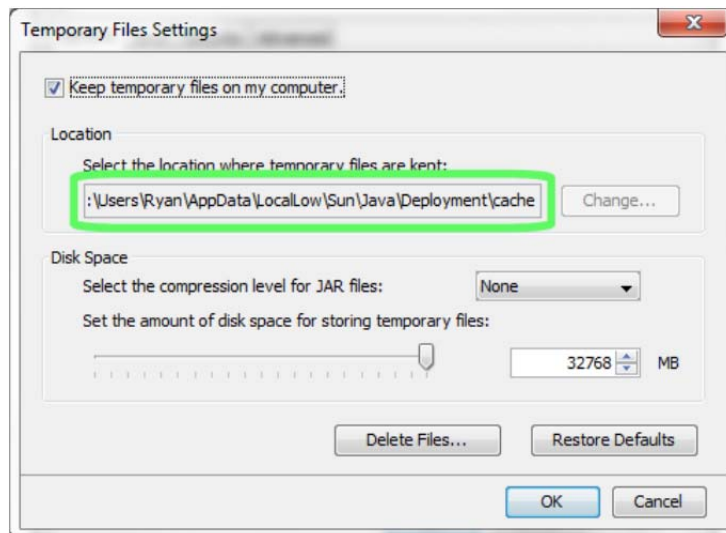
Temporary Files Settings screen, showing the location of the Web Start™ cache

3.2 – Initialization Parameters

OpenFox™ Desktop allows you to change several parameters that affect the environment in which Desktop executes. These parameters can be adjusted to resolve or assist in diagnosing technical support issues. Changes to these parameters affect the operation of OpenFox™ Desktop on a particular device for all users. If you make changes to these parameters while Desktop is running, they will not take effect until Desktop is closed and re-launched.
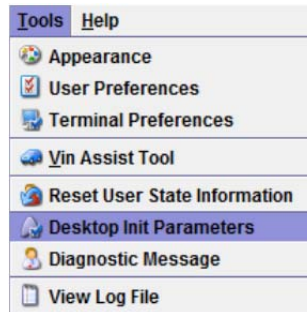
You can adjust these parameters from within Desktop by choosing the Desktop Init Parameters item from the Tools pull down menu.

Menu access to initialization parameters

You can also adjust these parameters outside of Desktop by launching the Desktop diagnostic tool from the web portal. This can be helpful in resolving technical issues which prevent Desktop from launching.

Web portal access to initialization parameters

3.2.1 – Maximum Memory (heap)
This setting allows you to control how much system RAM is made available to the Desktop application. By default, the Override box is left unselected, which means that Desktop requests the default amount of memory (usually one gigabyte). However, you may change this setting by selecting the Override box and entering a specific amount of memory. Users that run many Module applications will benefit from increasing the amount of memory available to Desktop; however, if you specify too large a value, then Desktop will fail to launch and report the message "Failed to Create Virtual Machine."

It is possible that some incompatibilities between certain versions of Windows and certain versions of Java have resulted in Desktop failing to launch, even when very moderate amounts of memory are requested. In some scenarios, the only way to prevent this error may be to prevent Java from requesting a specific amount of memory. Checking the Disable Max Heap box causes Java to accept the standard amount of memory granted to it by the operating system, and this may resolve issues with launching Desktop.
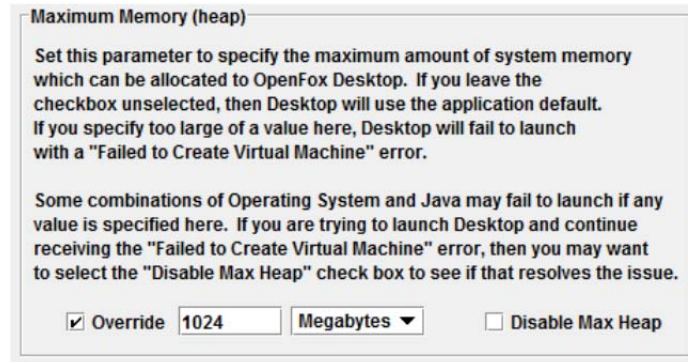
The maximum memory parameter screen

3.2.2 – Incremental Updates
When an update to Desktop is released to the message switch, users download the update the next time that Desktop is launched. To conserve bandwidth and to minimize the impact on users, this download typically only contains the parts of Desktop that have changed. This is called an incremental update. However, some incompatibilities between certain versions of Windows and certain versions of Java may cause these incremental updates to fail. In some scenarios, the only resolution to this issue may be to avoid the incremental updates.

If incremental updates are avoided, then the user downloads the entire Desktop application when any update is released, not just the portions that have changed. Obviously, this has a significant impact on the bandwidth and time required to download the update. Please exercise caution when considering whether to avoid incremental updates.
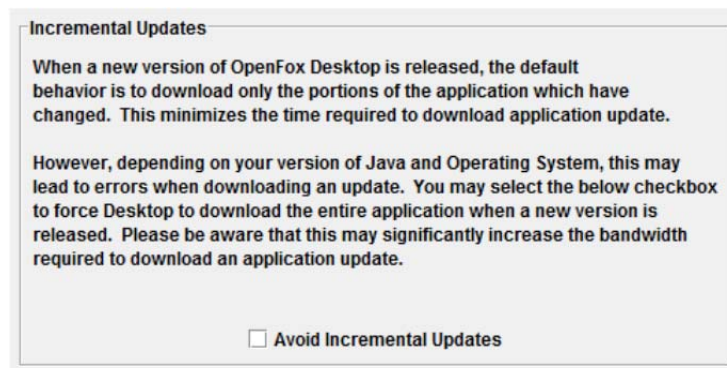
The incremental updates parameter screen

3.2.3 – Desktop Parameters
This parameter allows you to pass additional information to Desktop when the application launches. This parameter is most often used to report diagnostic information to the Java Console window. This information can prove helpful when diagnosing technical issues with the software.

You can request this diagnostic information by adding a "`-debug`" parameter to this field. The "`-debug`" parameter is followed by a comma separated list of debug modes that can be turned on. Each Module may support debug modes to help diagnose any issues with a particular application. Please refer to the user manual for a specific Module for more information on this topic. The debug modes supported by Desktop are listed below:

- **`all`** – enables all debug modes for Desktop and all Modules
- **`swing`** – reports thread violation errors in the graphical user interface support
- **`logon`** – reports fine grained diagnostic information regarding user log on and log off events
- **`comm`** – reports diagnostic information for all communications between Desktop and the message switch
- **`launch`** – reports fine grained diagnostic information as Desktop is launched
- **`rules`** – reports diagnostic information regarding the business rules on Messenger forms and other module screens (i.e. CCH, SOR, etc.)
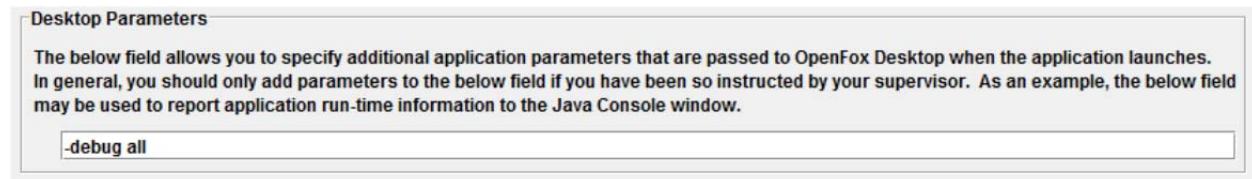
Example of turning on all debug modes
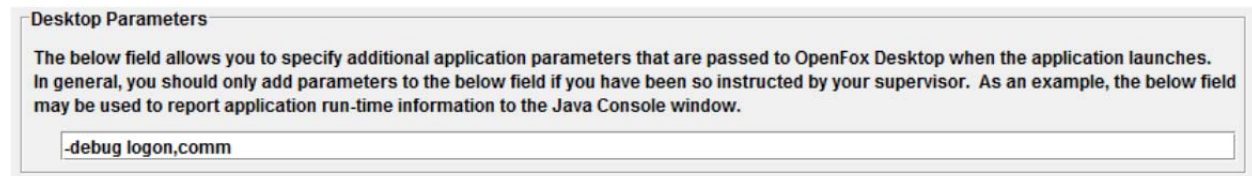
Example of turning on debug modes for logon and communications events

3.2.4 – Java Virtual Machine Arguments

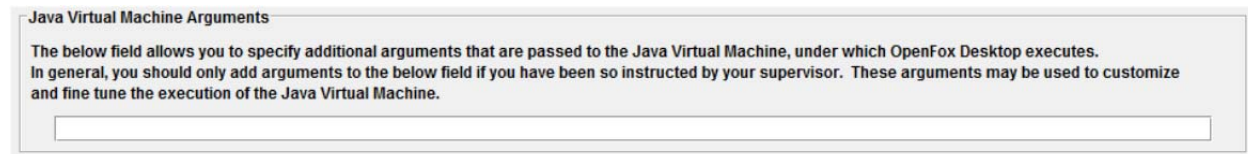This parameter allows you to pass additional arguments to the Java Virtual Machine, under which Desktop runs. These arguments can prove useful to resolve incompatibilities between specific Java versions and specific hardware configurations or operating system environments.

Java Virtual Machine arguments parameter

The most recent and up to date information regarding these arguments can be found on Oracle's Java pages at the following address:

http://www.oracle.com/technetwork/java/javase/tech/vmoptions-jsp-140102.html

3.3 – Terminal Preferences

OpenFox™ Desktop terminal preferences are similar to user preferences, except that they affect the operation of Desktop on a particular device. Terminal preferences stay on the device on which they are set; they do not follow a user around to different terminals. This also means that the terminal preferences affect the experience of all users which log onto Desktop from a particular device. Terminal preferences are accessed through the Terminal Preference item under the Tools pull down menu.
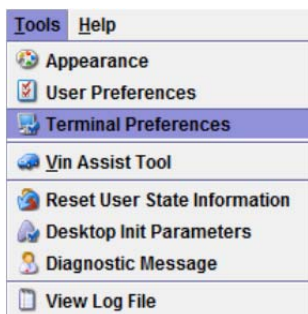
Access to the terminal preferences screen

3.3.1 – Accessibility Preferences

The accessibility preferences are used to enable compatibility with screen reader utilities and other accessibility software packages. Many of these packages will not operate correctly unless the Desktop accessibility mode is enabled. To enable this mode, please select the Enable Accessibility Mode checkbox.
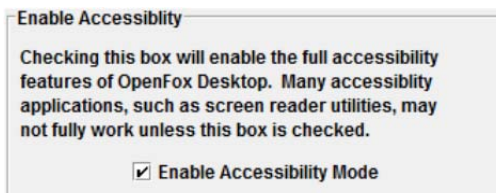
Setting to enable accessibility mode

If you are using a screen reader package with OpenFox™ Desktop, then you may also need to choose a compatibility mode. Currently, Desktop has built in customized support for the JAWS® screen reader software published by Freedom Scientific. Please see the following address for more information:

http://www.freedomscientific.com/products/fs/jaws-product-page.asp

Desktop also includes built in support for other screen readers as well. If you are using the JAWS® software package, then please select the Jaws mode for compatibility. Otherwise, if you are using a different screen reader package, please select the normal mode item.
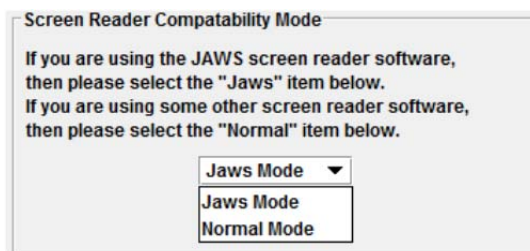
Setting to enable compatibility mode for different screen reader packages

3.3.2 – Browser Preferences
OpenFox™ Desktop and Modules use an HTML browser software package for displaying web formatting information. Examples of this include the Desktop help file window and the Messenger message display. The browser terminal preferences settings allow you to customize whether the text in these displays is anti-aliased. Anti-aliasing is a process intended to remove pixelated edges of text, and tends to make the display look more smooth. However, some users feel that the anti-alias text makes it hard to read certain characters, such as the number two (2).
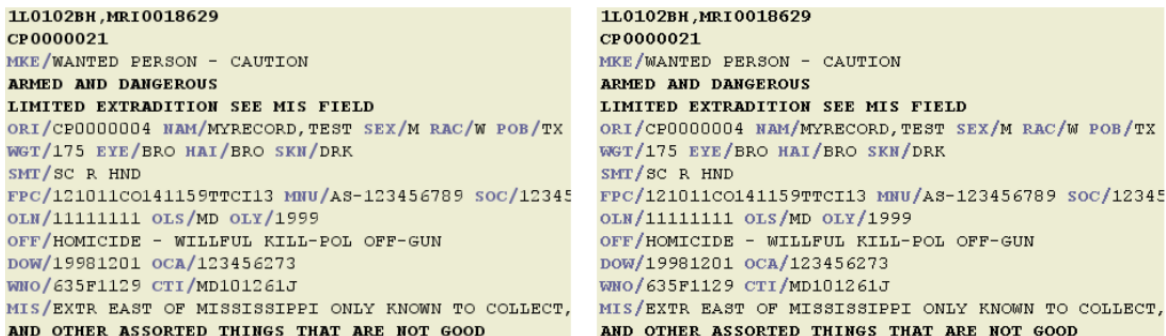
Example of anti-aliasing on the left, and no anti-aliasing on the right

3.3.3 – Sound Preferences

The Desktop sound terminal preferences allow you to change settings which affect the sounds played by Desktop. The first option allows you to simply disable all sounds. If the check box is not selected, then Desktop does not play any sounds.
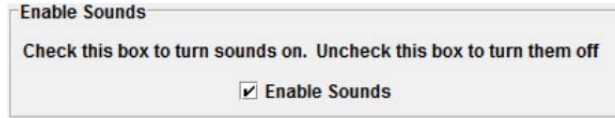
Option to disable all sounds from Desktop

The second setting allows you to choose which audio device is used to play sounds. This setting is most useful in dispatch environments where users want to have sounds played on a specific set of speakers or headphones. Initially, Desktop plays sounds on the default audio device; however if you want to change this, first deselect the Use Default Audio checkbox. Then you can choose a specific audio device from the drop down list as displayed below. You may need to experiment with different settings until you find the correct audio device.
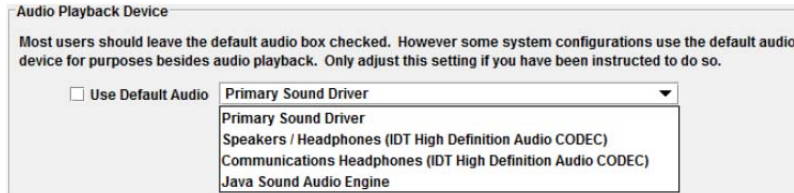
Option to choose a specific audio device for sounds

3.3.4 – Window Preferences

The window terminal preferences allow you to change what information Desktop displays in the window title bar. By default, Desktop displays the station name, the ORI, status text (i.e. what user is logged on), and the text "OpenFox™ Desktop." Below is an example of this information.
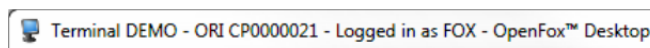
Example of default information displayed in the window title bar
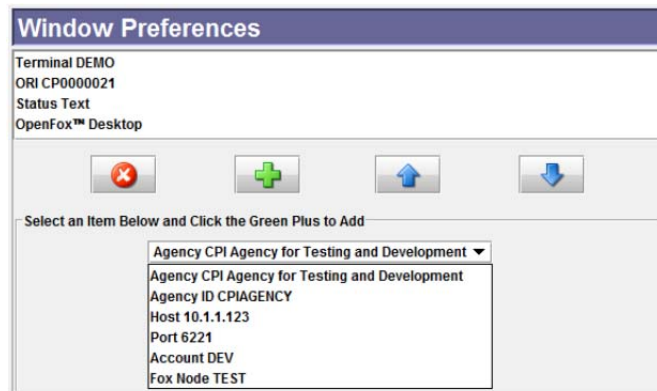
The window terminal preferences screen

The window terminal preferences screen allows you to choose which of the following items of information are displayed in the window title bar:

- **Terminal** – the terminal mnemonic or station name of this device
- **ORI** – the default ORI assigned to this device
- **Agency** – the description of the agency to which this device belongs
- **Agency ID** – the unique identifier of the agency to which this device belongs
- **Host** – the IP address at which this device connects to the message switch
- **Port** – the port number which this device uses to connect to the message switch
- **Account** – a three letter code which identifies the governing agency
- **Fox Node** – a code indicating whether the message switch is a production system, a test system, a development system, etc.
- **Status Text** – displays the status of the Desktop software (this information cannot be removed from the window title bar)
- **OpenFox™ Desktop** – static text identifying the Desktop application (this information cannot be removed from the window title bar)

Chapter 4 – Message Switch Administration

This chapter includes information on performing message switch administration over devices running OpenFox™ Desktop. This chapter is intended for use by the governing agency administrative and support staff. Many of the functions described in this chapter are not available to end users or to information technology support personnel. If you have any questions or believe that you should have access to these functions, please contact your governing agency.

4.1 – Desktop Licenses

Every copy of OpenFox™ Desktop must be registered with a license to gain access to the message switching system. If Desktop attempts to connect without a license, the connection will be closed. If a user tries to launch Desktop without a license, the user is directed to the registration application, which guides the user through the registration process. For more information on registration, please see section [4.3 – License Registration].

An OpenFox™ Desktop license record contains the following information:

- **Product Key** – A unique code that identifies a particular Desktop license
- **License Number** – A sequential database index that identifies a particular Desktop license.
- **Purchasing Agency** – The OpenFox™ agency that is authorized to make changes to a license
- **Assigned Agency** – The OpenFox™ agency that has been assigned to use the license
- **Station** – The terminal mnemonic (i.e. station name) that is assigned to the Desktop terminal which has registered this license
- **Type** – Either normal, pool, or restricted
- **Number of Stations** – If this license is a pool or restricted use license (see below), this field determines the number of concurrent terminals.
- **Modules** – The list of Desktop Modules which may be available to users at this Desktop terminal
- **Hardware Fingerprint** – Displays "TAKEN" if there is a hardware fingerprint associated with this license; otherwise displays "NONE"
- **Expiration Date** – The date on which the license expires and is no longer valid, unless renewed
- **Add Date** – The date on which the license was created
- **Modified Date** – The date on which the license was last modified
- **Status Flags**
    - **REGISTERED vs. NOT REGISTERED –** Indicates whether the license is registered

- o **DEVICE_ID –** If reported, this indicates that the license requires a hardware fingerprint
- o **DISABLED** – If reported, this license has been disabled from use
- o **MOBILE** – If reported, this license is intended for use in a mobile environment

Some of the above data fields are 'locked' by CPI sales staff when licenses are purchased. These fields may never be modified, except by CPI sales personnel. These fields include the following:

- Product Key
- License Number
- Purchasing Agency
- Type
- Number of Stations
- Modules
- Expiration Date
- Add Date
- MOBILE status flag

If you require additional licenses, access to additional software Modules, or need to renew a license that is about to or has expired, please contact your governing agency or the CPI sales department at 1-866-471-6305.

4.1.1 - Normal Licenses
A normal license is intended for use by one device. The device is assigned a particular product key, and the user registers that product key on the target device. When Desktop is launched from that device, it is assigned the terminal mnemonic (i.e. station name) that was used to register the product key.

If a normal license is registered on multiple devices, only one of the devices is able to connect to the message switch at a time. If these devices run Desktop at the same time, they will fight back and forth for the connection to the switch (typically every 30 seconds). If your Desktop session seems to constantly be interrupted, then the license may have been registered on another device.

4.1.2 – Pool Licenses
Pool licenses are intended to be shared among a group of devices, up to 255. Pool licenses do not assign a terminal mnemonic (i.e. station name) to a particular device. Instead, the device has one terminal mnemonic from a group of mnemonics assigned to it when the application is launched. It is very likely that the same device will be assigned different terminal mnemonics each time that it is launched.

Pool licenses are only valid for a certain number (up to 255) of concurrent sessions. If there are already that many Desktop sessions active, and you attempt to launch a new Desktop session, you will not be able to connect to the system.

4.1.3 – Restricted Use Licenses

Restricted use licenses are similar to pool licenses, but they associate a particular terminal mnemonic with a specific device. When Desktop is launched from the device, it is assigned the terminal mnemonic that was used to register the device. In this fashion, restricted use licenses are similar to normal licenses; however restricted use licenses are only valid for a certain number (up to 255) of concurrent sessions.

4.2 – License Reports

Administrative staff can access reports on Desktop licenses through the D1 application, Messenger, or Operator Aid. This section describes these reports and provides examples of the results. The license reports display a similar format and the differences in the reports are mostly in how to find the license that you are looking for.
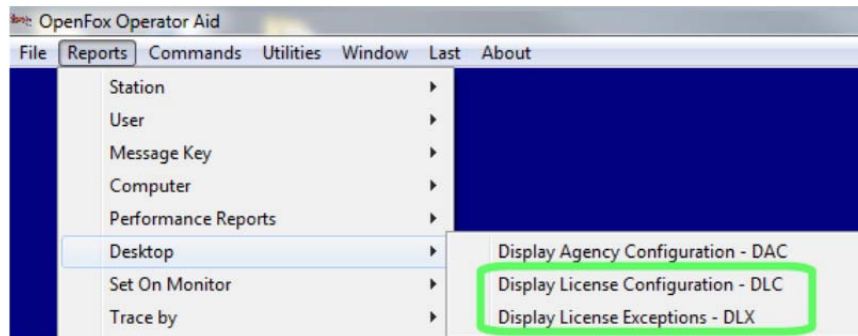
Access to License Reports in Operator Aid

In Operator Aid, the reports are displayed in a table format. Each license reported is a different line in the table, and the fields of each license are listed in the table columns. Please see the user manual for Operator Aid for more information.

Example license report in Operator Aid

When running the reports via command line, each license is displayed in a text format. If there are multiple licenses reported, they are simply listed one after the other. The first license reported is at the top, and the last license reported is at the bottom of the display.

```
PRODUCT_KEY='Z7AVG-MPPY9-Z6GBJ-DBUQC-LAF-YE2'   NBR=       5
ADD=2007 05/09 15:53:33   MOD=2010 03/17 14:53:21   EXPIRE= ** NEVER **
PURCHASE_AGENCY=CPIAGENCY   ASSIGNED_AGENCY=CPIAGENCY
DEFAULT_STATION=DEMO   REGISTERED
MODULES: MESSENGER          OFC             Module#3        Module#4
         Module#5          Module#6         Module#7        CONFIG
         Module#9          Module#10
HARDWARE_FINGERPRINT=NONE
```

Example license report from command line

4.2.1 – License Report by Device

The most commonly requested report is to report the Desktop license that has been registered to a particular terminal. If a user is having problems with their license, or you think something is not setup correctly in the license, then you can access the license report using the terminal mnemonic.

In Operator Aid, select the 'Licenses with Associated Station' item and type the name of the terminal into the box.
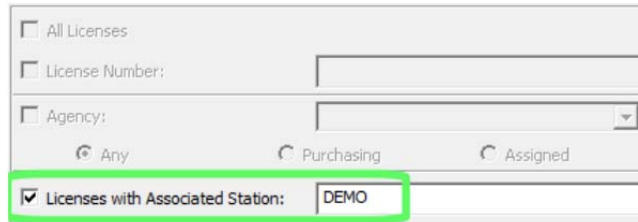
License report by the DMEO station in Operator Aid

From the command line, enter "`/DLC /ASO NAME`" where "`NAME`" is the name of the terminal.

License report by the DEMO station via command line

4.2.2 – License Report by Agency

This report allows you to view all licenses that have a particular agency value in either the purchasing or assigned agency fields. There are three options for this report. You can search for a particular agency in either the purchasing or assigned field. You can search for a particular agency in just the purchasing field, or you can search for a particular agency in just the assigned field.
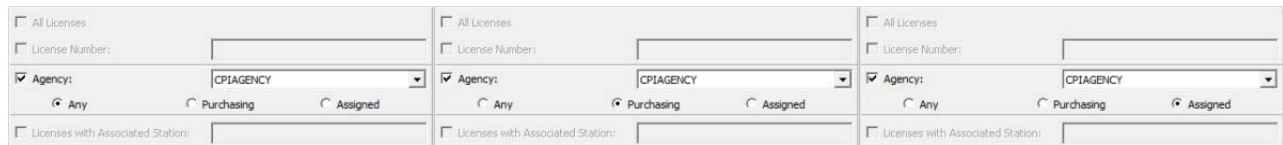
Operator Aid: search for any agency (left), purchasing agency (center), or assigned agency (right)

From the command line, these options are "`/AGY`", "`/PAG`", and "`/AAG`", respectively.

```
/DLC /AGY CPIAGENCY

/DLC /PAG CPIAGENCY

/DLC /AAG CPIAGENCY
```

Command line: search for any agency (top), purchasing agency (center), or assigned agency (bottom)

4.2.3 – Report Unregistered Licenses (System Wide)
Searching for licenses that are not registered is useful when rolling out an install of Desktop to the field. This report allows you to quickly and easily find the next available licenses so you can provide the product key and registration information to the users.

In Operator Aid, you run this report by first running a report of all licenses. When that report is finished, click on the Status Flags column to sort the results by that column. When the arrow in the column points down, the unregistered licenses are displayed at the top of the report.

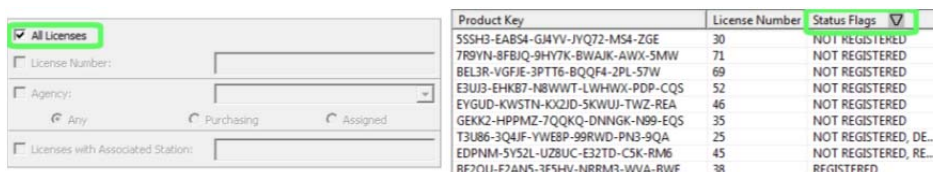| Product Key	License Number	Status Flags ▽
5SSH3-EABS4-GJ4YV-JYQ72-MS4-ZGE	30	NOT REGISTERED
7R9YN-8FBJQ-9HY7K-BWAJK-AWX-5MW	71	NOT REGISTERED
BEL3R-VGFJE-3PTT6-BQQF4-2PL-57W	69	NOT REGISTERED
E3UJ3-EHKB7-N8WWT-LWHWX-PDP-CQS	52	NOT REGISTERED
EYGUD-KWSTN-KX2JD-5KWUJ-TWZ-REA	46	NOT REGISTERED
GEKK2-HPPMZ-7QQKQ-DNNGK-N99-EQS	35	NOT REGISTERED
T3U86-3Q4JF-YWE8P-99RWD-PN3-9QA	25	NOT REGISTERED, DE...
EDPNM-5Y52L-UZBUC-E32TD-C5K-RM6	45	NOT REGISTERED, RE...
BF2QU-F2AN5-3E5HV-NRRM3-WVA-BWE	38	REGISTERED

Operator Aid: First search for all licenses (left), then sort by Status Flags (right)

From the command line, use the "`/UN`" option to search for unregistered licenses. With this option, you can also specify a maximum number of licenses to be returned with the "`/MAX`" option.

```
/DLC /UN /MAX 10
```

Command line example of searching for the next 10 unregistered licenses

4.2.4 – Report Unregistered Licenses by Agency
Whereas the previous report searches system wide for unregistered licenses, you can use this report to restrict that search to a specific agency. This report is useful when rolling out installations of Desktop on an agency basis. You can quickly see the next available licenses for that particular agency.

In Operator Aid, you run this report by first searching for licenses by agency; please see the earlier section for instructions on this. Then you click the Status Flags column to sort the results and put the unregistered licenses at the top of the list. Please see the previous section for instructions on this.

From the command line, you can combine either of the three agency items, "/AGY", "/PAG", or "/AAG", with the "/UN" item to search for unregistered licenses. Also, you can limit the number of licenses returned by the report with the "/MAX" item.

```
/DLC /AGY CPIAGENCY /UN /MAX 10
```

```
/DLC /PAG CPIAGENCY /UN /MAX 10
```

```
/DLC /AAG CPIAGENCY /UN /MAX 10
```

Command line: search for the next 10 unregistered licenses for any agency (top), purchasing agency (center), or assigned agency (bottom)

4.2.5 – Report a Specific License

You can display the report of a specific license by entering the license number (database index value). In Operator Aid, select the License Number item and enter the number in the field.
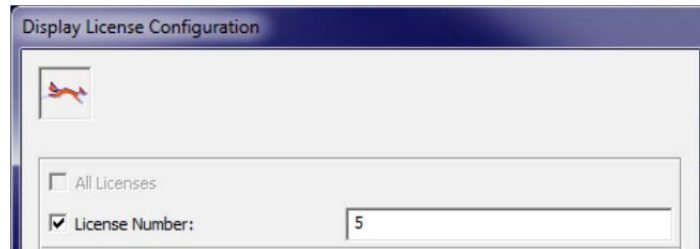
Operator Aid: report for license number 5

From the command line you can choose to either enter the license product key or, with the "/NU" option, the license number.

```
/DLC /NU 5
```

Command line: report for license number 5

```
/DLC Z7AVG-MPPY9-Z6GBJ-DBUQC-LAF-YE2
```

Command line: report for same license by product key

4.2.6 – Report All Licenses
The simplest report is to search for all license records in the system. This report displays the information for every license in the system. In Operator Aid, this option is chosen by selecting the "All Licenses" item.

Operator Aid: Report all licenses

In the command line, this report is chosen by adding the "/ALL" item to the report.

Command line: Report all licenses

4.2.7 – Report Expired Licenses
Depending on the license agreement between an agency and CPI, certain Desktop license records may be set to expire on a particular date. If there is an expiration date on a license, then the device associated with that license will not be able to connect to the message switching system on or after the expiration date. If this situation occurs, the agency needs to renew the license to regain system access.

This report allows you to search for licenses which have already expired or which are about to expire. In Operator Aid, you access this report by choosing the Display License Exceptions item from the Desktop Reports menu.
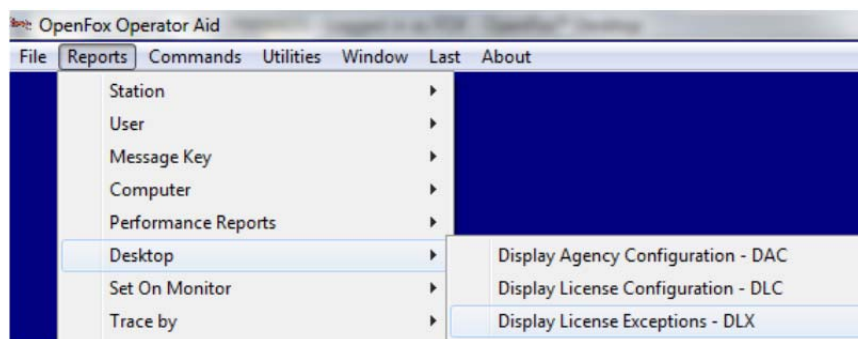
Operator Aid: Access to expired license report

In the Display License Exceptions report window, you can choose to search for licenses which have already expired by selecting the Expired item.
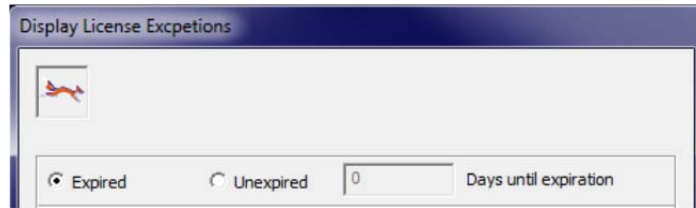
Operator Aid: Search for licenses which have already expired

You can also choose to search for licenses which will expire in the near future. This allows agencies to proactively renew their Desktop license agreement so that their system access remains uninterrupted.

Operator Aid: Search for licenses which will expire in the next 30 days

From the command line, this report is run by typing "/DLX". To search for licenses which have already expired, type "/DLX X" into the software.

Command line: Search for licenses which have already expired
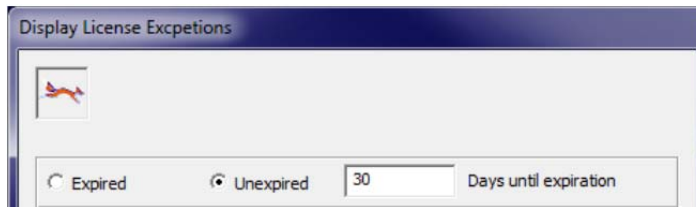
You can also search for licenses which will expire in the near future. Type "/DLX E days" into the software, where "days" is the number of days in the future.

Command line: Search for licenses which will expire in the next 30 days

4.3 – License Registration

When a license is registered by a user, certain information is hard coded into the license record. This information may not be changed unless the license is unregistered through the OpenFox™ Configurator administrative tool. When the license is registered, the following data fields are locked and cannot be modified without unregistering the license:

- Assigned agency
- Station
- Whether the license requires a hardware fingerprint

Unregistering a license is only intended to be necessary when you wish to transfer the use of a Desktop license to a different terminal mnemonic or agency. For more

information on how to deregister a license, please see the section [4.4 – License Administration].

4.3.1 – Registration Example

An example of a unregistered license is displayed below. Note that the default station field is unassigned and the NOT-REGISTERED flag is reported.

Unregistered license example

Following this example, suppose that this license will be registered to the DEMO terminal. The end user has been provided the product key and agency identifier, so the user enters the information into the registration screen and supplies the name DEMO for the default station.
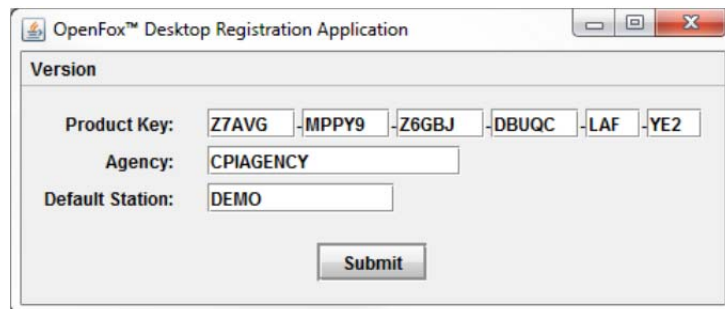
Registration example

After the user has registered the license, the report now shows that the default station has been set to DEMO and the license is REGISTERED.

License has been registered

4.3.2 – Registration with Hardware Fingerprint Example
This example walks through the process of registering a license that requires a hardware fingerprint. Once again, we start with the report of a license that is not registered. This report is the same as the first report in the previous example, except that the license reports DEVICE-ID. This means that this license requires a hardware fingerprint. Also, please note that the hardware fingerprint field reports NONE, which indicates there is no fingerprint associated with this license.

```
LICENSE CONFIGURATION REPORT:   12:07 19MAR2013

PRODUCT_KEY='Z7AVG-MPPY9-Z6GBJ-DBUQC-LAF-YE2'  NBR=      5
 ADD=2007 05/09 15:53:33  MOD=2013 03/19 12:07:37  EXPIRE= ** NEVER **
 PURCHASE_AGENCY=CPIAGENCY  ASSIGNED_AGENCY=CPIAGENCY
 DEFAULT_STATION=unassigned  NOT-REGISTERED  DEVICE-ID
 MODULES: MESSENGER        OFC              Module#3         Module#4
          Module#5         Module#6         Module#7         CONFIG
          Module#9         Module#10
HARDWARE FINGERPRINT=NONE
```
Report of an unregistered license which requires a hardware fingerprint

After the user has registered the license, running a report on the same license results in the following display. As in the previous example, the default station field has been set to DEMO and the report displays REGISTERED to indicate the license has been registered; however, also note that the hardware fingerprint field reports TAKEN. This means that the fingerprint has been taken from the device and associated with this license.

```
LICENSE CONFIGURATION REPORT:   12:09 19MAR2013

PRODUCT_KEY='Z7AVG-MPPY9-Z6GBJ-DBUQC-LAF-YE2'  NBR=      5
 ADD=2007 05/09 15:53:33  MOD=2013 03/19 12:07:37  EXPIRE= ** NEVER **
 PURCHASE_AGENCY=CPIAGENCY  ASSIGNED_AGENCY=CPIAGENCY
 DEFAULT_STATION=DEMO  REGISTERED  DEVICE-ID
 MODULES: MESSENGER        OFC              Module#3         Module#4
          Module#5         Module#6         Module#7         CONFIG
          Module#9         Module#10
HARDWARE FINGERPRINT=TAKEN
```
Report of a registered license with associated hardware fingerprint

4.4 – License Administration

If you have been granted the proper authorization, you can manage certain aspects of Desktop licenses through the OpenFox™ Configurator. Please check with your governing agency if you believe that you should have access to this tool. Through the Configurator, administrative and support personnel can perform the following tasks:
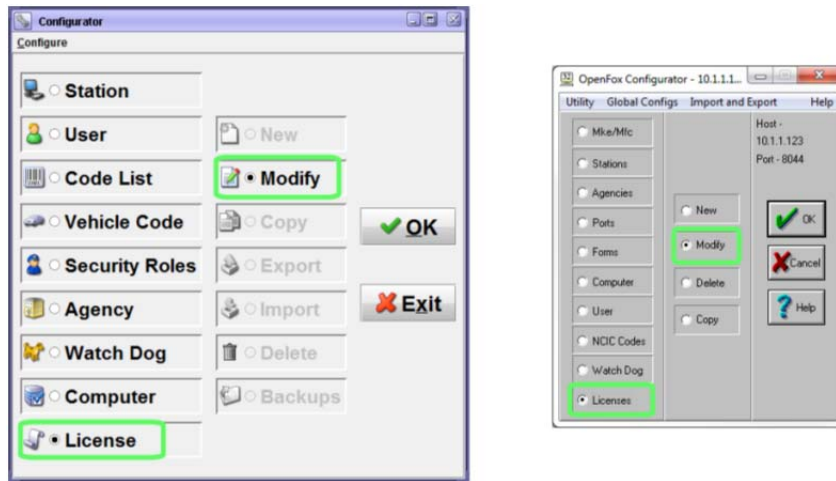
- Unregister licenses
- Change whether an unregistered license requires a hardware fingerprint
- Assign a unregistered license to a particular agency

All other modifications to a license record, such as changing a license to a mobile license, changing which application Modules for which a license is valid, etc., can only

be performed by CPI sales and support staff. If you would like to change a license or procure additional licenses, please contact CPI.

It is very important to remember that you are only allowed to manage a license record if the agency identified on your user profile matches the purchasing agency of the license. If these agency identifiers do not match, then you are not allowed to access the license in Configurator. You are not even able to see such licenses in the Configurator list window.

To get started with license administration, open the OpenFox™ Configurator application, and then select License Modify.

Configurator 7.0 and higher (left), Configurator before 7.0 (right)

4.4.1 – Unregister a License
Unregistering a license allows you to change the fields that are set when the license is registered. This includes the assigned agency, the station, and whether the license requires a hardware fingerprint. This information may not be changes if a license is registered; it must be unregistered first.

Please use caution when unregistering licenses. Unregistering a license will invalidate any device which has been registered with that license. If a user attempts to launch Desktop from such a device, they will be unable to access the system until that device is registered.

To unregister a license, first pull up the license record by entering the license product key into the Configurator. In Configurator 7.0 and later, you can also pull up the license record from a search window. Please see the Configurator user manual for more information on this topic.
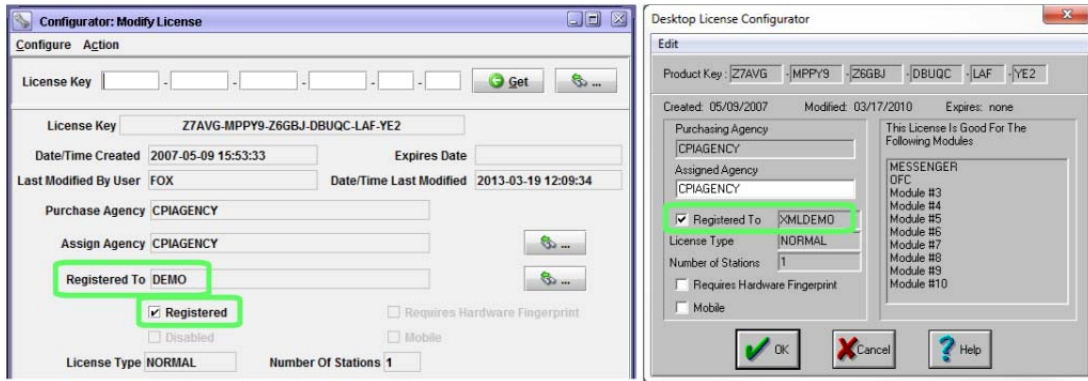
Registered license display in Configurator 7.0 and higher (left), and Configurator before 7.0 (right)

Mark the license as unregistered by removing the check mark from the Registered check box. Then click OK or Apply to save your changes.

4.4.2 – Change Whether a License Requires a Hardware Fingerprint

You can only change whether a license requires a hardware fingerprint if the license is currently unregistered. You will be unable to modify this field if you open a registered license in Configurator. If the license to which you want to make the change is registered, then you will need to unregister the license first. Please see the previous section for instructions on how to do this.

Open the license in Configurator and then modify the Requires Hardware Fingerprint check box. If there is a check mark in the box, then the license requires a hardware fingerprint. If the check box is empty, then this license does not require the fingerprint. After making your changes, click OK or Apply to save your changes.
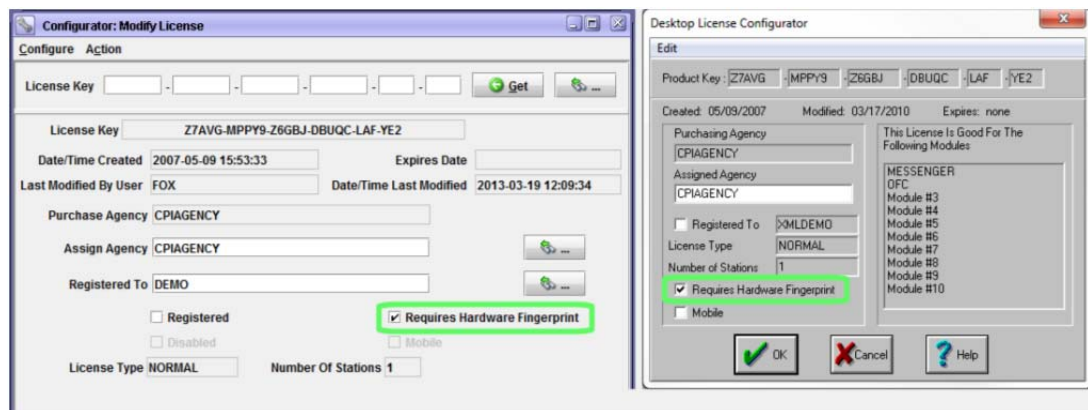
The requires hardware fingerprint setting in Configurator 7.0 and higher (left) and before 7.0 (right)

4.4.3 – Assign a License to a Particular Agency
You can only change to which agency a license is assigned if the license is currently unregistered. You will be unable to modify this field if you open a registered license in Configurator. If the license to which you want to make the change is registered, then you will need to unregister the license first. Please see the earlier section for instructions on how to do this.

Open the license in Configurator and then modify the Assigned Agency field. If this field is blank, then any terminal in the system can register this license, provided that the user has the product key. If you put an agency identifier in this field, then this license will only be able to be registered from a terminal that belongs to that agency. After making your changes, click OK or Apply to save your changes.
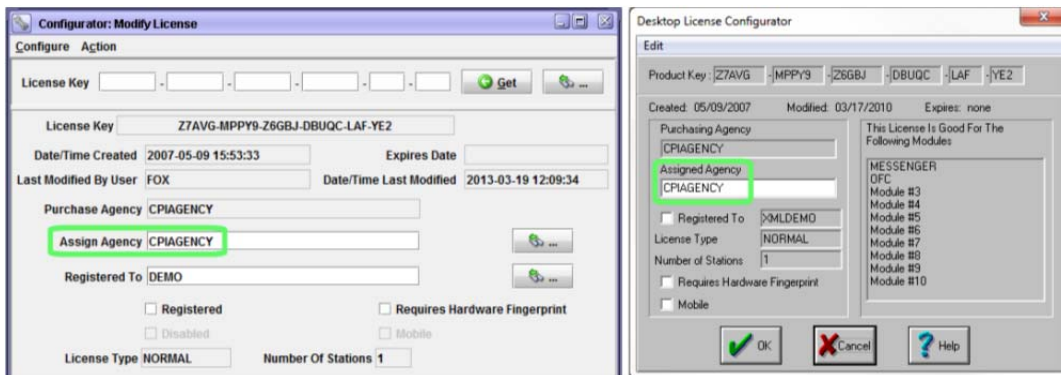
The assigned agency field in Configurator 7.0 and higher (left) and before 7.0 (right)

4.5 – Station Configurations

Every device that runs OpenFox™ Desktop must have a station record configured in the OpenFox™ Message Switch. The station configuration defines several aspects of the device and these are listed below:

- **Station Class** – Defines the type of device, for OpenFox™ Desktop devices, the class must be either 'MSNGR' for desktop devices or 'MMOB' for mobile devices.
- **Station Name** – Also called the terminal mnemonic, this field defines the name of the device as it is known on the switch. Using the station name, another device connected to the switch can directly address messages (such as AM messages) to this device.
- **ORI** – This field defines the 9 character ORI that is assigned to this device.
- **Agency** – Identifies the agency to which this station belongs
- **Authority** – Defines the authority granted to this device. This authority level is combined with the user's authority to create a session authority. Please see section [4.8 – Session Authority] for more information.
- **Acknowledge** – Determines whether this device has ACK message sent back to it when a message is submitted to the switch.

- **Legacy NCIC / NCIC 2000** – Determines if this device uses NCIC 2000 or legacy NCIC message formats. All devices running OpenFox™ Desktop use NCIC 2000 formats.
- **Image Capable** – Determines if the switch should send NCIC formatted images to this device. All devices running OpenFox™ Desktop support images.

Screen shots of sample OpenFox™ Desktop station configurations are provided below. Because the screens have significantly changed in Configurator version 7.0, samples are provided for systems running Configurator 7.0 and higher and for systems running a version prior to 7.0. For more information regarding the specific fields available in these screens, please refer to the OpenFox™ Configurator user guide.
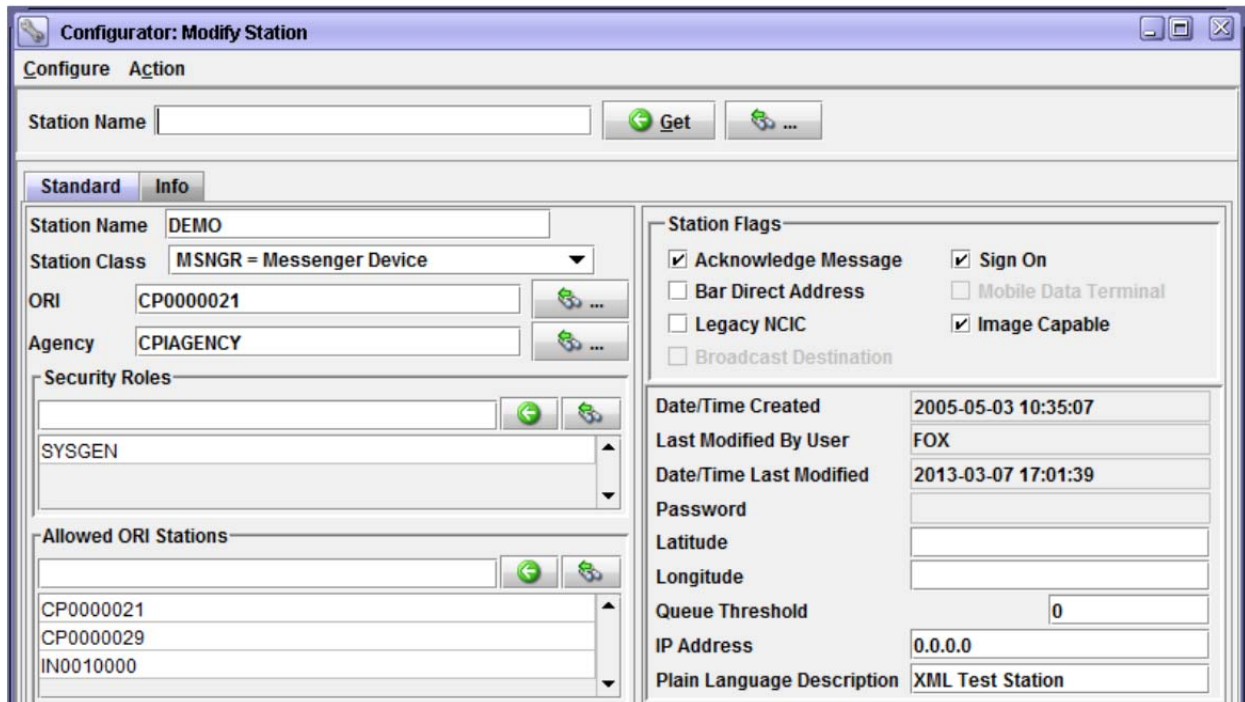
Configurator 7.0 and higher station configuration screen
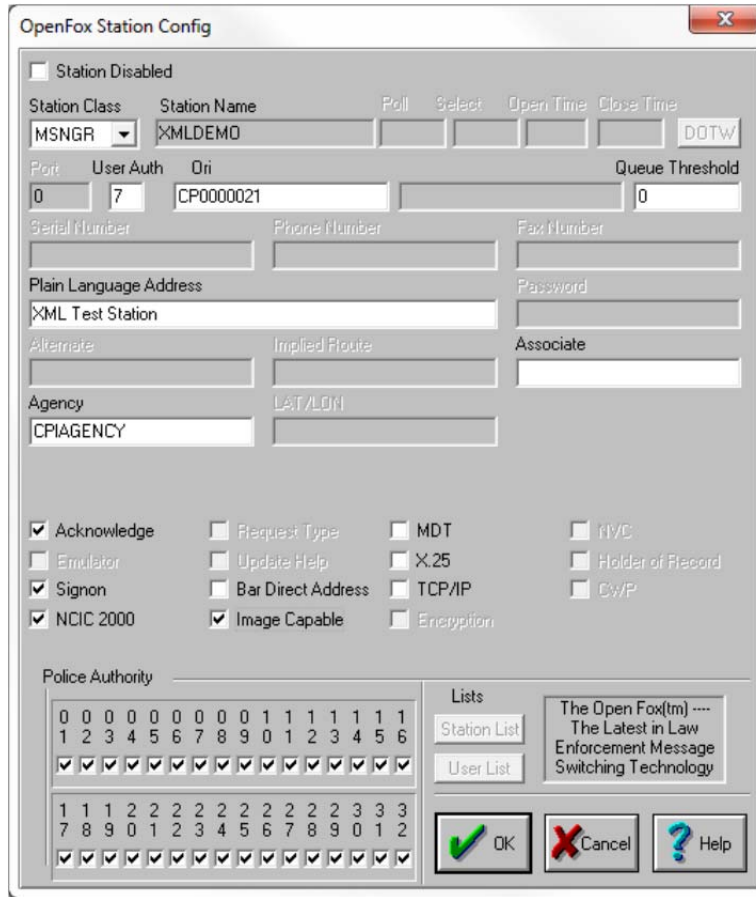
Station configuration screen for versions of Configurator prior to 7.0

4.6 – ORI Configurations

ORI configurations, in conjunction with station configurations, determine which ORIs may be used by a Desktop terminal. Some Modules (i.e. Messenger) may present the user with a list of ORIs that are available for use. The rules to determine whether an ORI is allowed for use by a particular Desktop device are slightly different for Configurator 7.0 and higher systems and those systems running a version of Configurator prior to version 7.0.

For Configurator 7.0 and higher, an ORI is in the allowed list if any of the following items are true:

- It is defined as the ORI on the station configuration record
- It is listed in the Allowed ORI Stations field on the station record
- The station is listed in the Deliver To Stations field on the ORI record

Configurator 7.0 and higher: station configuration (left) and ORI configuration (right)

For Configurator versions prior to 7.0, an ORI is in the allowed list if any of the following items are true:

- It is defined as the ORI on the station record
- The station is the alternate station (or alternate station list) on the ORI record
- The station is the associated station (or associated station list) on the ORI record
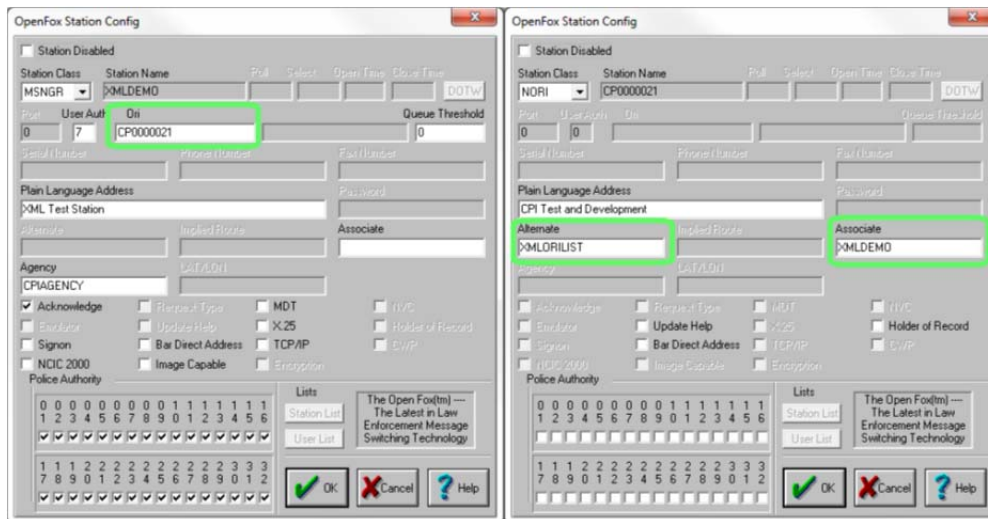
Configurator prior to 7.0: station configuration (left) and ORI configuration (right)

4.7 – User Configurations

Each individual person that logs onto OpenFox™ Desktop must have a user configuration record in the message switch. The user configuration defines several aspects of the individual's access to the system, and these are listed below:

- **User ID** – Defines the identifier that the user must use to log onto the system
- **Last and First Name** – Identifies the user's full name
- **Certification Date** – The date on which the user's certification expires
- **Training Date** – The date on which the user was last trained
- **Authentication Method/Detail** – Defines the method used by this individual to authenticate against the system
- **Agency** – Defines the agency to which this user belongs. Please note that in Configurator 7.0 and higher systems, a user may have multiple profiles, which allows the user to belong to multiple agencies.
- **Authority** - Authority granted to the user. This authority level is combined with the station authority to create a session authority. Please see section [4.8 – Session Authority] for more information. Please note that in Configurator 7.0 and higher systems, a user may have multiple profiles, which allows the user to have different levels of authority based on from where they access the system.

Screen shots of sample OpenFox™ Desktop user configurations are provided below. Because the screens have significantly changed in Configurator version 7.0, samples are provided for systems running Configurator 7.0 and higher and for systems running a version prior to 7.0. For more information regarding the specific fields available in these screens, please refer to the OpenFox™ Configurator user guide.
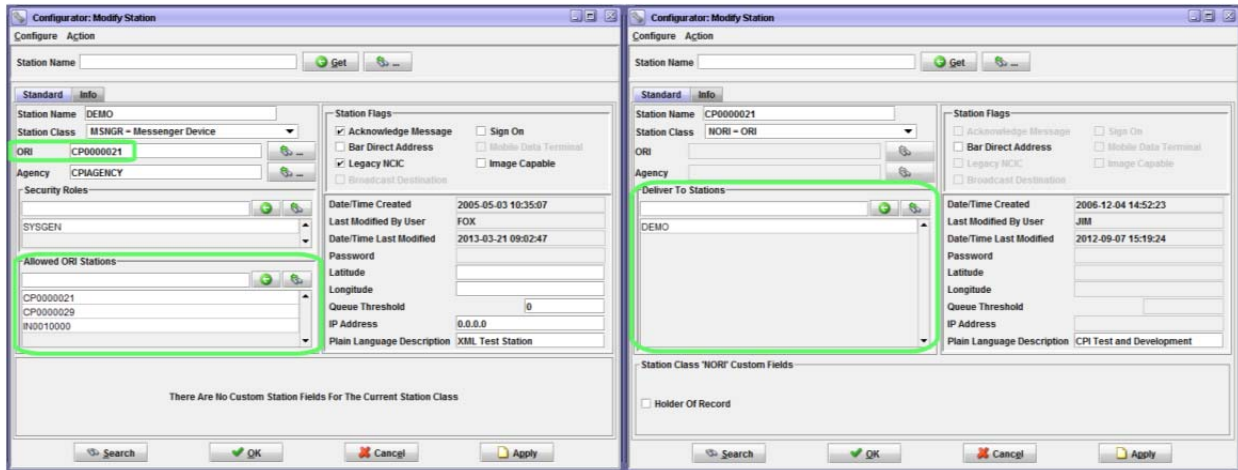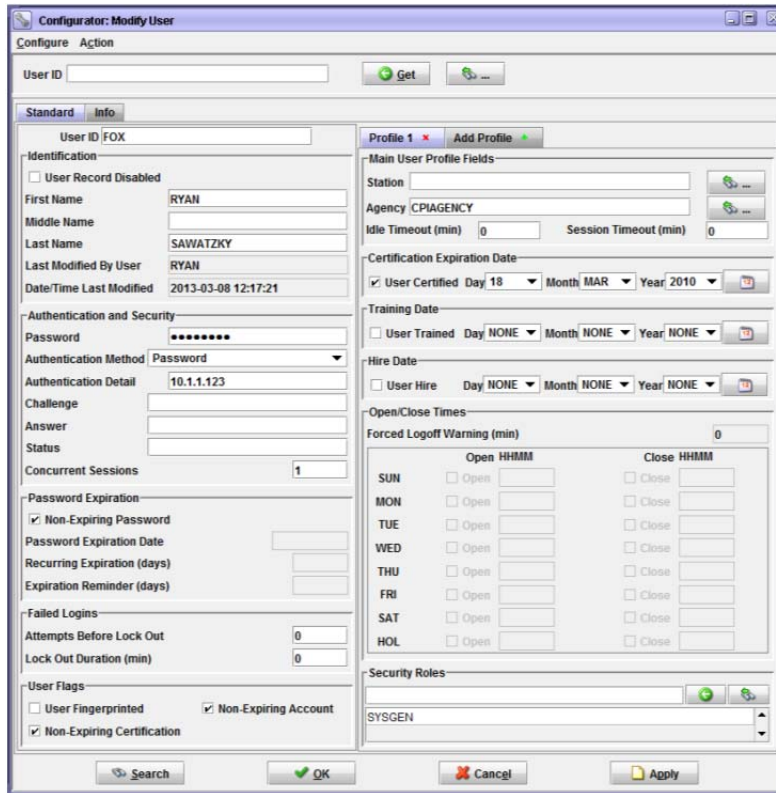
Configurator 7.0 and higher user configuration screen
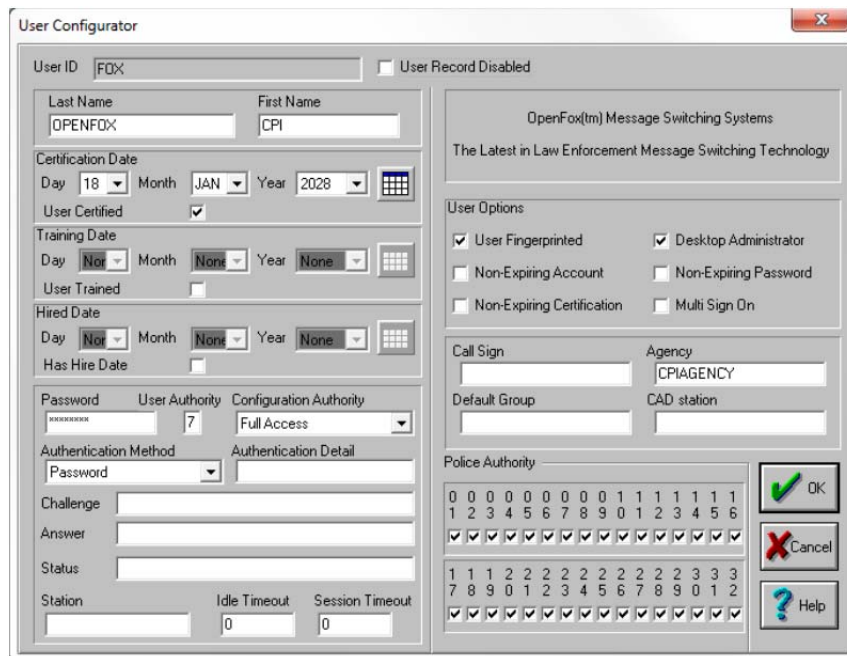
Configurator prior to 7.0 user configuration screen

4.8 – Session Authority

When a user logs onto the OpenFox™ Message Switch from a Desktop device, the switch examines the user configuration record and the station configuration record to determine the authority granted to this user session. The central principle of the session authority is as follows:

A particular authority level is available if and only if the authority is granted by the user configuration and by the station configuration.

If an authority level is not granted by the user configuration, or if an authority level is not granted by the station configuration, then that authority level is not available for this user session. Because the structure of OpenFox™ authority levels is vastly different between systems running Configurator version 7.0 and higher and those systems running an earlier version of Configuration, these cases are describes separately.

4.8.1 – Session Authority for Configurator 7.0 and Higher
The authority levels of Configuration 7.0 and higher systems are managed through configurable records called security roles. System administrators can create/modify/delete security roles, and administrators control the security roles that are assigned to stations and user profiles. Security roles organize authority levels into four different categories.

- Transaction – A list of MKE transactions that are allowed to be submitted
- Command – A list of OpenFox™ commands that may be run
- Other – A list of miscellaneous OpenFox™ authorities
- Granted Roles – A list of security roles included in this security role

Please refer to the OpenFox™ Systems Guide for further discussion regarding the specific details of security roles. A common misconception regarding session authority is that only the security roles shared between the user and station are valid for the user session. This is not the case. The process of determining the session authority is more involved, and this process is described over the following sections.

Because this topic is technical in nature, we will consider an example as this process is described. Hopefully, this will help to make the steps of this process more clear. In our example we will consider four security roles. These example security roles are designed to be simple rather than accurate examples of how real security roles are configured on production systems.

- `BASIC_QUERY` – grants access to the most common queries (i.e. QW, DQ, and RQ)
- `ADVANCED_QUERY` – includes the basic query role and grants access to advanced queries such as criminal history and NICS queries (i.e. QH, QR, IQ, QNP, QNR)
- `RECORD_MAINTENANCE` – grants access to transactions used to maintain hot file records (i.e. MW, XW, CW)

- **FULL_ACCES_NO_CCH** – grants access to every transaction defined in the system except for criminal history queries (i.e. QH, QR, IQ)

4.8.1.1 – Station Security Roles

A station configuration contains a list of security roles which are granted to the device. This list is found in the following location on the station configuration screen. Following along our example, this station is in a location that system administrators have decided is not suitable for the return of criminal history information. Thus this station has been assigned the security role FULL_ACCESS_NO_CCH.
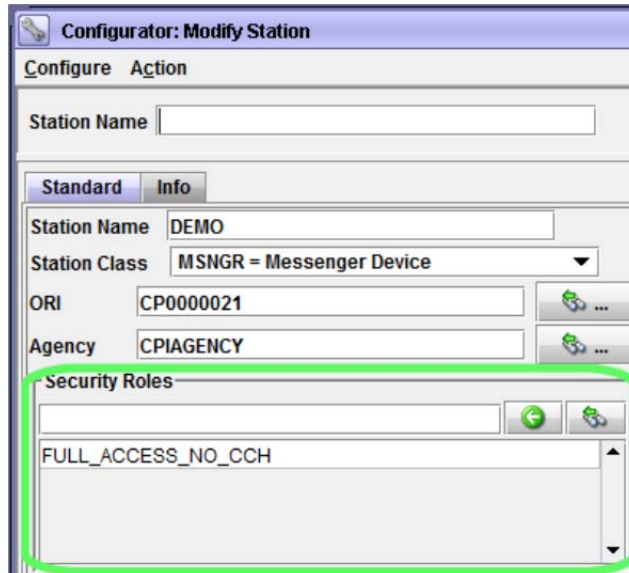
Security roles granted to a station

4.8.1.1 – User Profile Security Roles

Security roles are not granted directly to a user configuration. Instead, they are granted to a user profile. Most user configuration records contain one and only one user profile; however some users may have multiple profiles. Multiple profiles are intended to address the situation when the same individual has multiple roles, where the user accesses the system from different devices or agencies.

When a user logs onto the message switch, it determines which profile is active. It does so by searching for a profile that matches certain criteria. It first searches for a profile that matches the most important criteria. If no match is found, then it searches for a profile that matches the next most important criteria. If no match is found, then it proceeds to the next criteria. It continues in this fashion until it either finds a matching profile, or until it has exhausted the list of criteria. If no matching profile is found, then the user is not able to log onto the system.

When the system searches the profiles, it does so in a sequential order. The first profile searched is profile #1, then profile #2, profile #3, and so on for all profiles on the user record. If no matching profile is found, then it considers the next criteria, and once more

it starts with profile #1, then profile #2, and so on. The matching criteria are described below in order of decreasing importance. The most important criteria is listed first.

- **Exact Station Match** – The station from which the user is logging on exactly matches the station name defined in this profile
- **List Match** – The station from which the user is logging on is a member of the LIST station defined in this profile
- **Server Match** – The station from which the user is logging on is associated with the SERVER station defined in this profile
- **Agency Match** – The station from which the user is logging on belongs to the agency defined in this profile AND the station field in this profile is blank
- **Default Profile** – This profile has a blank agency field and blank station field
- **Reject Logon** – If no matching profile is found then reject the logon attempt

Once the system has determined which user profile is active, it examines the security roles that are assigned to that profile. Continuing in our example, this user profile has been assigned the `ADVANCED_QUERY` and the `RECORD_MAINTENANCE` security roles.
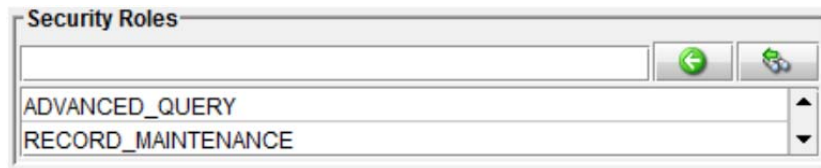
Security roles granted to a user profile

4.8.1.2 – Security Role Exploration
When a user logs onto the message switch, the switch has a list of security roles from the station configuration and a list of security roles from the user profile. The next step in determining the session authority is to explore the two lists of security roles. This step is necessary because security roles may include other security roles. Even in the case where system administrators have chosen to never allow security roles to contain other security roles, this step is still required because user profiles and stations can be assigned multiple security roles.

The security roles assigned to the station are explored to build a single master list of authorities. Similarly the security roles assigned to the active user profile are explored to build a single master list of authorities. Following our example, the station configuration only lists a single security role, and that security role does not include any other security roles. Thus, the list of authorities for the station may simply be copied from the FULL_ACCESS_NO_CCH security role. Thus, the station is granted the following authorities:

Full Access No CCH
CW
DQ
MC
MW
QNP
QNR
QW
RQ
XW

Authority list for station

The active user profile is assigned two security roles: ADVANCED_QUERY and RECORD_MAINTENANCE. Thus, these two security roles are explored, and the authorities granted by each role is combined into a single list.

Advanced Query	Record Maintenance		User Profile Authorities
IQ	CW		CW
QH	MW		IQ
QNP	XW		MW
QNR			QH
QR			QNP
Basic Query (role)			QNR
			QR
			XW
			Basic Query (role)

Security roles for user profile are combined into a single list

However, the list of authorities includes the basic query security role. This security role must also be explored and have the list of authorities which it grants added into the list.

User Profile Authorities	Basic Query		User Profile Authorities
CW	DQ		CW
IQ	QW		DQ
MW	RQ		IQ
QH			MW
QNP			QH
QNR			QNP
QR			QNR
XW			QR
Basic Query (role)			QW
			RQ
			XW

The basic query role is explored and added into the master list of user profile authorities

4.8.1.4 – Determining the Session Authority

The final step in this process is to combine the list of authorities granted by the station and the list of authorities granted by the active user profile. The security roles have already been fully explored as described in the previous section, so there is no longer any concerns about multiple security roles or security roles which include other roles. This step is a simple matter of applying the central principle of the session authority. Thus, the system determines the session authority by only granting authority levels that are in the list of authorities granted by the station and in the list of authorities granted by the active user profile.

Following our example, the authority list for our station is combined with the authority list for our active user profile. All the authorities match up except for the CCH transactions (IQ, QH and QR) which are not granted by the station roles, and the MC transaction which is not granted by the user profile roles. Because these transactions do not appear in both the list of authorities for our station and the list of authorities for our user profile, they are not granted for this session.

User Profile Authorities	Station Authorities		Session Authority
CW	CW		CW
DQ	DQ		DQ
IQ			MW
	MC		QNP
MW	MW		QNR
QH			QW
QNP	QNP		RQ
QNR	QNR		XW
QR			
QW	QW		
RQ	RQ		
XW	XW		

User profile and station authorities are combined into the session authority

4.8.2 – Session Authority for Configurator Versions Prior to 7.0

The authority levels of systems running a Configurator version prior to 7.0 consist of three different levels of authority. These are the user authority, the configuration authority, and the police authority. Each of these are described below, and for more information on authority levels, please see the OpenFox™ Systems Administration guide.

4.8.2.1 – User Authority

The user authority is a number between zero (0) and seven (7). User authority levels are hierarchical. That means that user authority level two (2) includes all system access granted by authority levels one (1) and zero (0). User authority level three includes all system access granted by levels two (2), one (1), and zero (0).

The session user authority level is equal to the value on the user configuration or the station configuration, whichever one is lower. For example, if the user configuration grants a level of five (5) and the station configuration grants a level of three (3), then the session authority will grant a level of three (3).
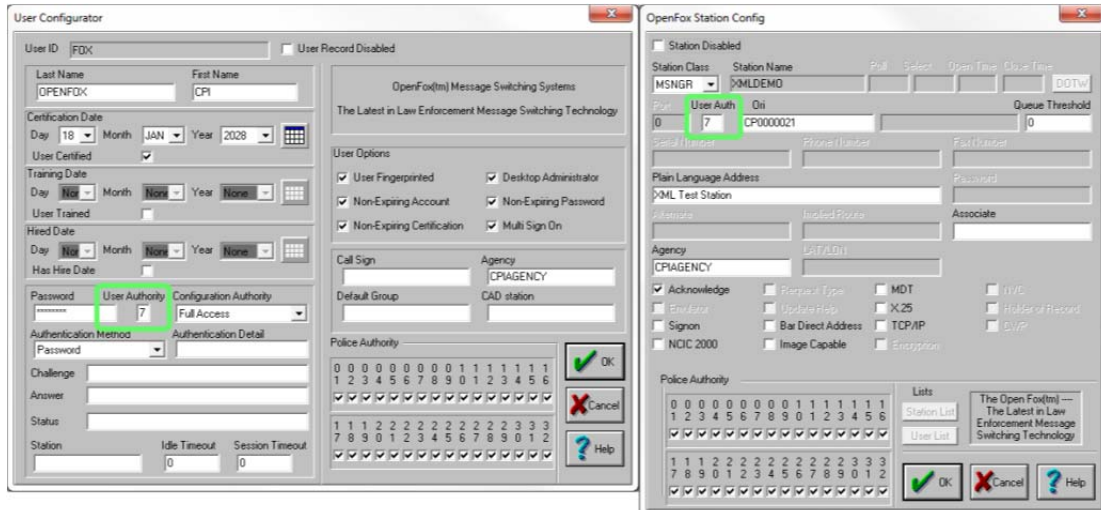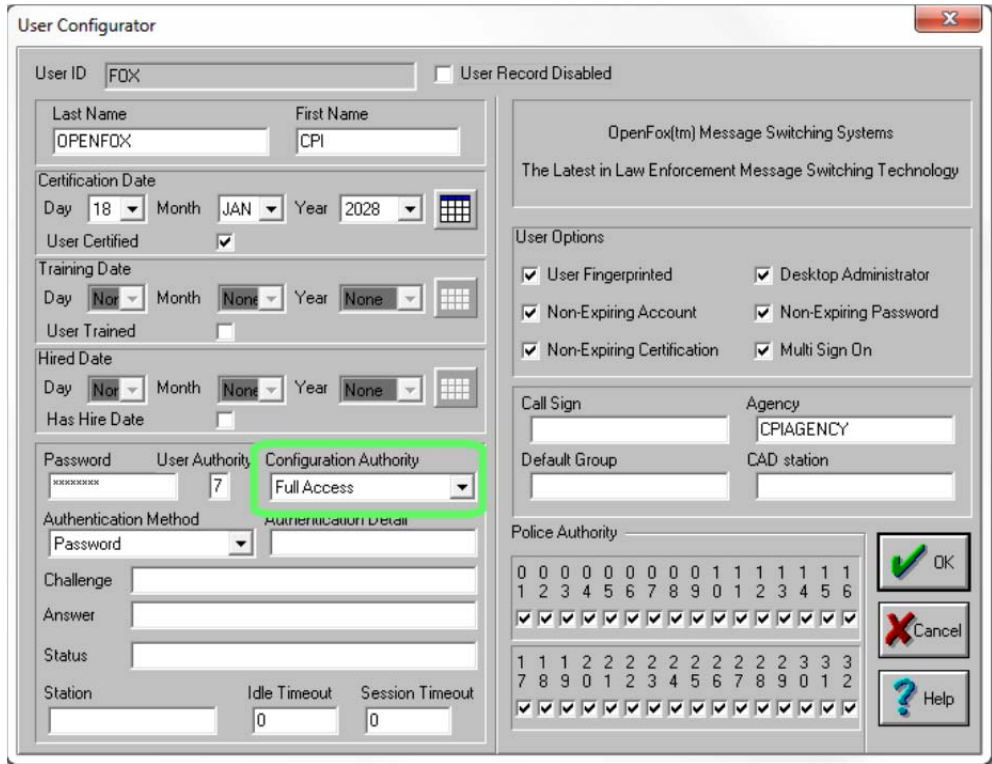
User authority on a user configuration (left) and on a station configuration (right)

4.8.2.2 – Configuration Authority
The configuration authority defines the level of access to the Configurator software. There are four different levels or access, and these are defined below. There is no configuration authority setting on the station configuration. This setting only appears on the user configuration record. Thus, the session configuration authority is equal to the value set in the user configuration.

- None – The user is not able to access the Configurator.
- Users of Agency – The user is able to create/modify/delete user records which belong to the same agency. The user is also able to modify the agency configuration record.
- All Users – The user is able to create/modify/delete any user record in the system.
- Full Access – The user is granted full and unrestricted access to all features in the Configurator.

Configuration authority on a user configuration

4.8.2.3 – Police Authority
The police authority consists of thirty two (32) separate and independent authority levels. Unlike user authority levels, police authority levels are non-hierarchical. This means that a police authority level of three (3) *does not* include the authority granted by levels one (1) or two (2). Typically, police authority levels control what transactions can be submitted to the message switch, however some systems use police authority levels to control other aspects of system access. If you have questions regarding this topic, please contact the CPI Support Center.
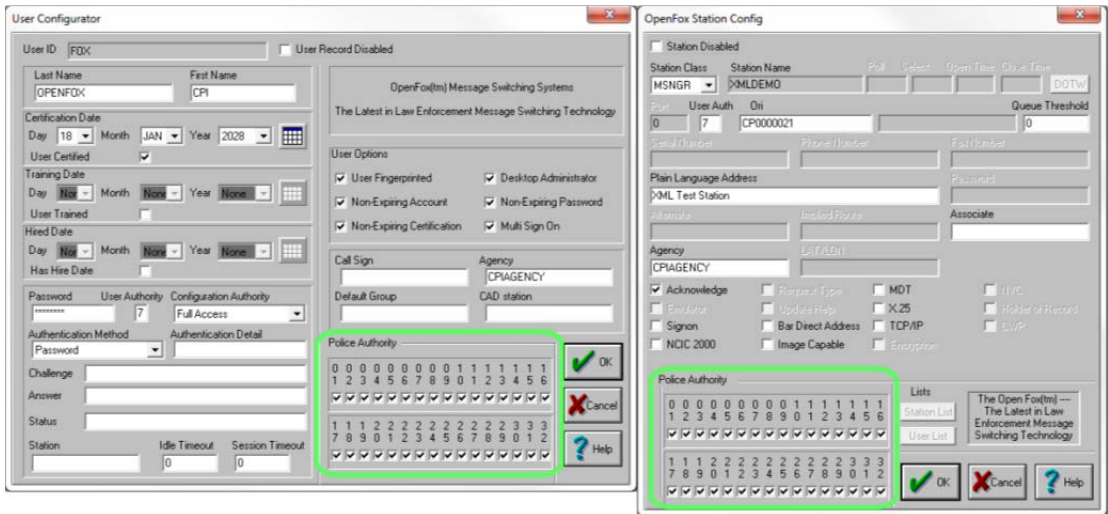
Police authority on a user configuration (left) and a station configuration (right)