Windgate Software LLC

RISC Analysis and MS Vista/Windows7

Contents

Notes:

This document also uses the term 'Vista' to refer to Windows 7 (since it is still Vista)

If you plan to install Microsoft Office, do it before installing RISC Analysis.

Installing:

1. Save the installer (RSANFull.exe or UA.exe) to local disk

2. Locate the file and Right Click

3. Select 'Run As Admin'
   Select 'Run in xP Compatibility Mode'

4. Run the installer
   This installs RISC Analysis and creates the icon for the Desktop.

5. If this a new install (RSANFull.exe)
   Right Click the Desktop icon and ...
   Select 'Run As Admin'
   Select 'Run in xP Compatibility Mode'

6. If you are installing under the 'Admin' account and a 'User' account will be running RISC:
   Make sure that FULL folder permissions are granted to the user.
   This means Read/Write AND File Create/Delete.
   Start RISC under the User Account, not the Admin Account

7. Start RISC Analysis and submit the registration.

Why do all this?

Vista and Win7 use Virtual Folders.

The problem with Virtual Folders is that the initial program is installed into a 'Virtual Store'. Users get a copy of the program in the Virtual Store.

If the Admin User installs and Runs RISC Analysis for the first time, Vista/Win7 grabs a copy from the VStor. This will be an uninitialized copy (because it hasn't been used yet). When RISC Analysis is used for the first time, a Unique ID is created. This forms the basis of the license ID.

If a subsequent named User logs on to Vista/Win7 and starts the app, there will be no application Virtual Folder for that user until Vista/Win7 creates it. At that point, Vista/Win7 grabs a new uninitialized copy from the VStor. Because this copy is uninitialized, a new Unique ID is created and this becomes a different license ID.

Additionally, attempting to update a program that exists in the VStor can fail for the user because it is the VStor that is updated, not the VFolder for the user.

Vista Specific Issues:

Profile Not Found In Registry/Unable to Initialize the Windows Registry

Cause: Vista 'Locks Down' MS-Office Registry Keys.
Acknowledged as a problem by Microsoft.

Microsoft's Solution:
(requires running Vista as Administrator).

1. Start the Registry Editor
   Click Start -> RUN type Regedit
   Click OK

2. Navigate to
   HKEY_CLASSES_ROOT\TypeLib\{4AFFC9A0-5F99-101B-AF4E-00AA003F0F07}

3. Right Click the Key 8.0
   In the Permissions dialog, select the 'Users Group'
   Under Permissions for 'Users' check 'Full Control'

4. Repeat for Key 9.0

5. Navigate to
   HKEY_CLASSES_ROOT\TypeLib\{000204EF-0000-0000-C000-000000000046}
   Right Click the Key 3.0 and again set permissions

6. Close the registry

'License Not Found' Microsoft Office Error

Cause: Installing 'run-time' MS Access before installing retail MS-Access
Acknowledged as a problem by Microsoft.

Microsoft's Solution:

1. Uninstall MS-Office,

2. Rename the "C:\Access 97 Runtime\msaccess.exe" file to Zmsaccess.exe

3. Reinstall office

4. Rename Zmsaccess.exe back to msaccess.exe

Problems caused by Microsoft, Details.

MS Office

RISC Analysis is developed using MS-Access, an Office component known as a Relational Database Management System (RDBMS).

When Microsoft Access was launched in 1991, many aspects were specifically targeted to independent developers of RDBMS applications.

Microsoft were sufficiently eager to pick up the independent developer market that they created the ISV (Independent Software Vendor) program for Office Developers, and made the "Run-Time" License Royalty Free.

At that time, there were several competing RDBMS platforms. Although they all had their pros and cons, for many developers, the Royalty Free distribution of the run-time db engine was a big plus.

Microsoft were well aware of the importance of this and, via the Office Software Developer Kit (SDK) included an 'Installation Builder' to allow developers to distribute stand-alone (independent of MS-Office) versions of the msaccess.exe run-time executable, each with independent vendor specified user profiles.

Unfortunately, beginning with Office 95, Microsoft reneged on this aspect and caused all installations of msaccess.exe to use the same profile settings, regardless of version level of ms-access.exe, and regardless of run-time or retail version.

This caused several problems:

Running 2 different versions of msaccess.exe (for example 95 and 2.0) would cause both to fail.

Installing the run-time would cause the retail version to fail and visa-versa.

Multiple run-time licenses, from different vendors, and at different version levels would cause a failure.

The absolute stupidity behind this decision by Microsoft was compounded by their complete refusal to listen to the massive outcry from the developer network.

Their 'fix' was to just not install msaccess.exe from the Office set-up if it already existed on the system. Consequently, although RISC Analysis uses a custom installer to isolate itself from other run-time Access Applications, the Microsoft Office installer will search the system for msaccess.exe and not allow itself to install if it finds a version already existing.

For this reason, MS-Office must be installed prior to installing RISC Analysis.

(For us, the simplest solution would be to just rename the msaccess.exe run-time - but that would violate our run-time distribution license).

Vista - User Profiles and Security.

Prior versions of basic Windows (the version that ships with most PCs) did not invoke user accounts unless specific profiles were set-up. Even then, an account established as Admin was a pseudo Admin account inheriting permissions from the main Admin, with the main Admin account being hidden from the user.

Higher versions of Windows ('Small Office', 'Enterprise', 'Server' etc.) do make available the main Admin profile in order to assign User and Group permissions. This has been the case since Windows NT and is similar with Vista.

For the 'Home' versions of Vista a default 'Admin' account already exists but again, this is a pseudo Admin account with permissions inherited from the main Admin (which is still hidden).

Where things differ is in the requirement to assign an initial user. Consequently, at a minimum a Vista system will have two users (Pseudo Admin and Initial User). The Initial User and Pseudo Admin accounts should generally have the same permissions.

However, and depending on the version of Vista, a program being installed by a 'User account' may sometimes not inherit the same permissions as the User, even if that user has the same permissions as the pseudo Admin account.

Additionally with Vista, some Read/Write operations are explicitly denied, and access to the Windows Registry is significantly restricted.

RISC Analysis must have full permissions for its install folder, including Read/Write and File Create/Delete. The easiest way to confirm this is to set the start-up properties via the desktop icon (per page 2).

Vista - Virtual Folders

Vista's Virtual Folders implementation is poorly thought out and problematic.

Unlike previous versions of Windows, Vista maintains a hidden 'core' of files and folders that are generally unavailable to default users. When a user starts Vista and logs on, the system 'fetches' only the files and folders associated with that user profile, as a Virtual folder.

Additionally, and the root of the problem, Vista assumes that a program being newly installed is just for the Current User. Prior versions of Windows generally assumed that a program being installed was for All Users unless specified otherwise.

Why is this a problem?

Like most software vendors, we need to collect certain info from the system in order to start the program correctly. For example, different Operating Systems and different system configs often require different start-up parameters.

Additionally, we need to know that a particular license is legitimately authorized and not a cloned or pirated copy.

In the past, many software vendors provided a license key with the physical software (a hard key). This essentially allowed anyone with the license key to install the software on any number of systems.

With the advent of file downloads, a physical key per software package was unworkable. Many vendors, including Microsoft, began using values based on the physical hardware of the target system to generate a System Unique ID (SUID). Under this system, the H/W values are normally used to seed an algorithm that results in the final SUID.

However, using hardware values alone presents many problems, including non unique and missing values. Also, if a hardware driver has no instructions to poll for the S/N on start-up (and update the registry), a manually modified registry value will be the one reported by the operating system.

Typically, major system vendors do not set up each PC one by one. They create a single system and then clone the hard drive to all other systems configured with the same hardware. In other words, if you buy 10 systems from the same source at the same time, there is a good chance that, regardless of the S/N physically on a given component, the operating System will report many of the component S/Ns as the same across all 10 systems. This makes hardware values alone unreliable.

The normal solution is to use hardware values and 'another value' to generate a unique SUID at the time the program is first used or initialized. This way, if say two identical systems have the same hardware values, one can still determine which license is which.

So, to recap, most software programs available today do not ship with a 'hard coded' software key. The key is created 'on the fly' when the program is first started. Often, this uses a mix of Hardware values and other values.

Going back to Vista's method of Virtual folders and hidden cores, it means that when a program is installed, and the installer has finished, an uninitialized (clean/virgin) copy of the newly installed program is placed in the hidden core.

When a user starts the program for the first time, a copy of the uninitialized program is taken from the core and placed in the user's virtual folder. At that point, the program runs its 'First Time Used' sub routine to set up local parameters and initialize the software key. Therefore, the program has initialized, but only in the current user's virtual folder.

If a second User Account starts the program, Vista will see that the second user has no virtual folder for the program. At that point, Vista again takes a copy from the hidden core and presents it to the Second User's virtual folder. Since this copy again came from the hidden core (and is still uninitialized), the program starts and again runs its 'First Time Used' sub routine.

On the Vista platform, it is therefore important to set the 'Run as Administrator' option before starting RISC Analysis for the first time. Otherwise, if 'Run as Admin' is invoked after the initial registration, Vista will clone an uninitialized copy to the Admin virtual folder and RISC Analysis will quite correctly run its 'First Time Used' sub routine. This then results is two separate software keys on the same system.