

Pervasive PSQL v9 Compatibility with Windows Vista

A Pervasive Software White Paper
January 2007

Table of Contents

OVERVIEW	3
BACKGROUND	3
WINDOWS VISTA EDITIONS	3
WINDOWS VISTA PLATFORM MATRIX	4
PERVASIVE PSQL v9 TEST SCENARIOS	4
PERVASIVE SQL EXCEPTIONS WITH WINDOWS VISTA	5
STANDARD USERS AND ADMINISTRATORS	5
RUN AS ADMINISTRATOR	7
FILE VIRTUALIZATION	7
REGISTRY VIRTUALIZATION	8
INSTALLATION ISSUES	8
SERVER ENGINE ISSUES	10
WORKGROUP ENGINE ISSUES	10
CLIENT COMPONENT ISSUES	11
WINDOWS XP TO WINDOWS VISTA UPGRADE	11
FILE PERMISSION ISSUES	11
REGISTRY PERMISSION ISSUES	12
ODBC.INI REGISTRY PERMISSION ISSUES	12
PERVASIVE CONTROL CENTER (PCC) ISSUES	12
UTILITY ISSUES	13
DOCUMENTATION ISSUES	13
TERMINAL SERVICES RUNNING ON WINDOWS VISTA	14
JAVA RUN-TIME ENGINE (JRE) ISSUES	14
AERO INTERFACE	14
MISCELLANEOUS ISSUES	15
CONCLUSION	15
CONTACT/TRADEMARK INFORMATION	17

OVERVIEW

This report summarizes Pervasive's testing and recommendations for running the various Windows Vista™ editions with the Pervasive PSQL™ v9 database engines (server and workgroup).

The initial release of Pervasive PSQL v9.0 was in March 2005, followed by PSQL v9.1 (Service Pack 1) in June 2005 and the current release, PSQL v9.5 (Service Pack 2), released in May 2006. Windows Vista is scheduled for mass markets in January 2007. This timeframe does not coincide with Pervasive PSQL's release cycle. Pervasive will be able to provide you with supported, recommended solutions and work-arounds for existing versions of Pervasive PSQL v9 running with Windows Vista.

Moving forward, our next release of Pervasive PSQL (likely called PSQL v10) currently scheduled for the second half of 2007 will incorporate full Windows Vista support and compatibility, offering our customers a smooth and seamless transition to Microsoft's Vista and Longhorn platforms. Prior Pervasive.SQL versions, however, are not supported as they are not Windows Vista aware and those products are no longer supported by Pervasive Software.

BACKGROUND

The Windows Vista release has been more than five years in the making and is the longest development cycle in Microsoft's history. With this release come many changes to the Graphical User Interface (GUI) including the new graphics subsystem Aero "Glass", a new security model using User Account Controls (UAC), changes to the Windows Firewall and additional Internet protection around phishing and malicious attacks. This document will focus on the various challenges these new implementations may pose when adopting Windows Vista. The key change in Windows Vista is the UAC requirement. We will provide you with some background into how UAC works with Windows Vista in the section titled Standard Users and Administrators.

WINDOW VISTA EDITIONS

There are six (6) editions of Windows Vista available. Please consult the [Microsoft Windows Vista web site](#) to learn more about what edition is right for you.

Pervasive PSQL v9 is supported with the following 32-bit editions of Windows Vista:

Windows Vista Starter *

Windows Vista Home Basic

Windows Vista Home Premium

Windows Vista Business

Windows Vista Ultimate

Windows Vista Enterprise

*Note: Windows Vista Starter is not currently scheduled to be available in the United States, Canada, the European Union, Australia, New Zealand, or other high-income markets as defined by the World Bank.

WINDOW VISTA PLATFORM MATRIX

The following are the supported PSQL v9 platforms and corresponding Windows Vista Editions.

	CLIENT	WORKGROUP EDITION	SERVER ENGINE	GUI UTILITIES
Microsoft Windows Vista Starter		X		X
Microsoft Windows Vista Home Basic	X	X		X
Microsoft Windows Vista Home Premium	X	X		X
Microsoft Windows Vista Ultimate	X	X	X	X
Microsoft Windows Vista Business	X	X	X	X
Microsoft Windows Vista Enterprise	X	X	X	X
Microsoft Windows Vista Home Basic x64	X	X		X
Microsoft Windows Vista Home Premium x64	X	X		X
Microsoft Windows Vista Ultimate x64	X	X	X	X
Microsoft Windows Vista Business x64	X	X	X	X
Microsoft Windows Vista Enterprise x64	X	X	X	X

PERVASIVE PSQL v9 TEST SCENARIOS

We have tested Pervasive PSQL v9 in the following configurations:

Server	Client
Windows Vista	Windows Vista
Windows Vista	Windows XP
Windows Server 2003	Windows Vista
Linux Server	Windows Vista
Netware 6.5 Server	Windows Vista
Windows Vista 64-bit*	

*Running on an x64 platform or an x86 platform.

Workgroup	Workgroup
Windows Vista	Windows Vista
Windows Vista	Windows XP
Windows Vista	Windows Server 2003

Note: Pervasive will support the following clients with Windows Vista:

Windows Server 2003
 Windows Server 2000
 Windows XP

PERVASIVE.SQL EXCEPTIONS WITH WINDOWS VISTA

While Pervasive PSQL v9 will be supported with Windows Vista, prior versions of the Pervasive database will not be supported, including:

Pervasive.SQL V8

Pervasive.SQL 2000i

Pervasive.SQL 2000

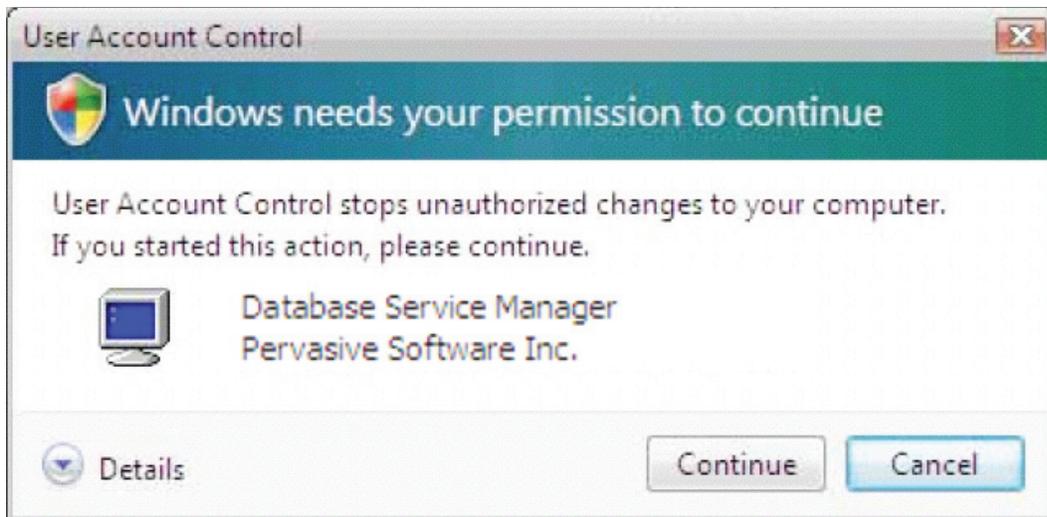
Pervasive.SQL v7

16-bit based applications or components

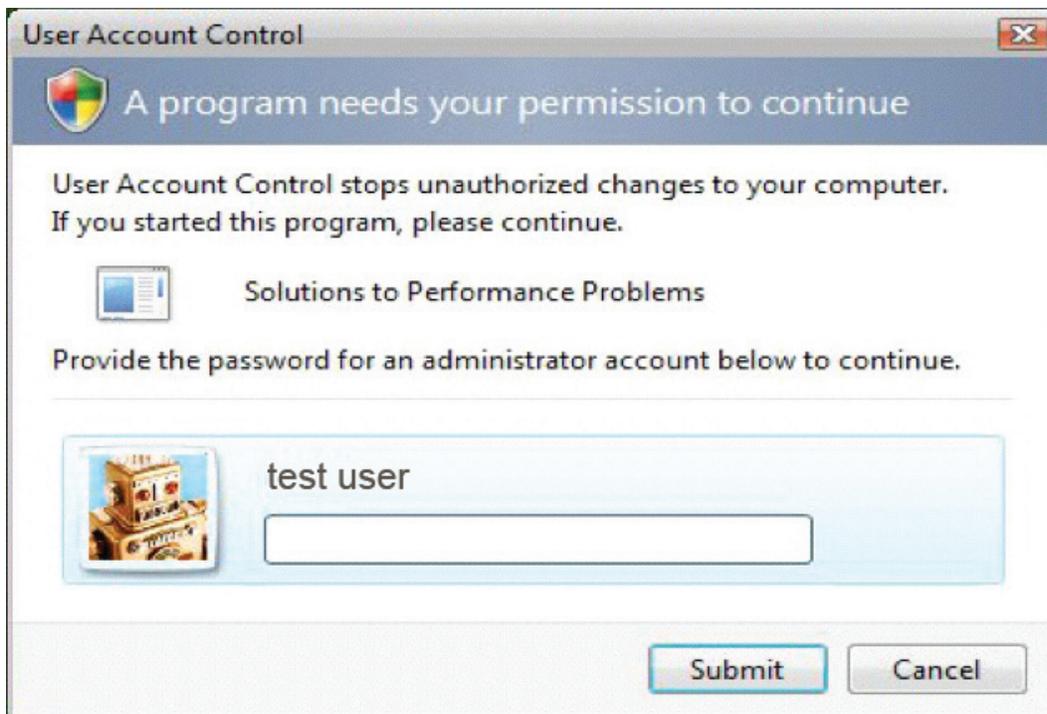
STANDARD USERS AND ADMINISTRATORS

On Windows Vista there are two predominant types of user accounts, standard users and administrators. The first user account that you'll see during the installation will be an administrator (this is separate from the system-wide administrator account that is disabled by default). As part of a secure desktop environment, all Windows Vista users are considered standard users regardless of their group association. In previous versions of Windows, users set up administrator level accounts so that they could perform a variety of functions including: system patching, registry modifications, changing system settings and installation and removal of application programs. This allowed users to make whatever change they wanted without having to change users and login as a different user with higher permissions. This also exposed the system to possible danger as malicious code or executables could then be launched with limited or no protection. With Windows Vista the logon sessions created for standard users and administrators are equally capable of protecting from such threats. With User Account Control (UAC) Windows Vista provides this protection for you regardless of user level. This is how it works:

- When a member of the administrators group logs on (this would include the initial user that was created at setup) the system creates a new logon session. It creates two different tokens representing the same logon session. The first token grants all the permissions and privileges afforded to the administrator while the second token is a restricted token offering far fewer permissions and privileges. This restricted token offers practically the same capabilities and constraints as would be granted to a standard user. Although the user is logged on as an administrator, applications are by default run with limited permissions and privileges. This is where Windows Vista differs dramatically from previous versions.
- When the administrator needs to perform any tasks that require additional permissions or privileges not granted to the restricted token, they will be prompted to run the application using the full security context provided by the unrestricted token. What protects the administrator from malicious code is that this elevation to the unrestricted token is only allowed after the administrator has confirmed the desire to use the unrestricted token by means of a secure prompt provided by the system. Malicious code cannot suppress this prompt and thereby gain complete control over the computer without the user's knowledge.



For standard users, attempts to perform a task that requires additional privileges will result in a prompt to enter an administrator password. The standard user is similar to the users group in previous versions of Windows operating systems.



Remember that the built-in administrator whose account is disabled by default has the privileges that an administrator group had in previous versions of Windows. With Windows Vista each user token is assigned an integrity level that controls their ability to be prompted or allow for execution. Standard user tokens and restricted (non-elevated) administrator tokens have an integrity level of Medium. Unrestricted (elevated) administrator tokens have an integrity level of High. Processes running under the Local System account have an integrity level of System.

RUN AS ADMINISTRATOR

Some of the suggested options include using the Windows-provided option to “Run As Administrator”. While this provides a certain level of functionality it’s not the same as when logged on as an actual administrative user.

The concept of “run as an administrator” is commonly referred to as “elevation” or “creating an elevated process”. Standard users are prompted for administrator credentials while administrators are simply prompted for permission to elevate. Either way the end result is a new process running with an unrestricted administrator token and all the permissions and privileges it affords.

FILE VIRTUALIZATION

With Windows Vista, Microsoft introduces a concept called Virtualization. This feature allows non-Windows Vista written applications to operate in a Windows Vista environment until the application or program is updated for Windows Vista compliancy.

Microsoft documents file virtualization as a way of addressing cases where applications or programs need to store information in a protected system-wide location. System-wide locations are:

C:\Windows

C:\Program Files

Registry Key – HKEY_LOCAL_MACHINE

Virtualization is only used when non administrator group user attempts to write to a file in the protected location. Windows Vista will redirect the users request to a virtualized specific path for that user. This is located in the \Virtual Store\... directory. This feature remains in place until the user is granted necessary permissions to the files. Virtualization has no impact to the application unless multiple users are required to share updated information in that common file.

Example:

Suppose User A is running under a limited user account and uses Notepad to save a text file to \Program Files\foo.txt. Virtualization would allow this file to be saved successfully. The write is redirected to \Virtual Store\ (The User’s account security identifier (-SID))\Program Files\foo.txt. In the \Program Files\ directory with Windows Explorer, User A will see the file foo.txt, since Windows Explorer properly shows User A’s virtualized files. On the same machine, User B logs into the system. However, after logging in, User B will NOT see the file foo.txt in the \Program Files\ directory. If User B then writes the \Program files\foo.txt file, that write will also virtualize to User B’s virtual store. The files User A writes remain independent of the file User B writes.

As you can imagine this works only in cases where users are not sharing data that is stored in a common file. We will discuss the impact of this in the section title File Permission Issues.

REGISTRATION VIRTUALIZATION

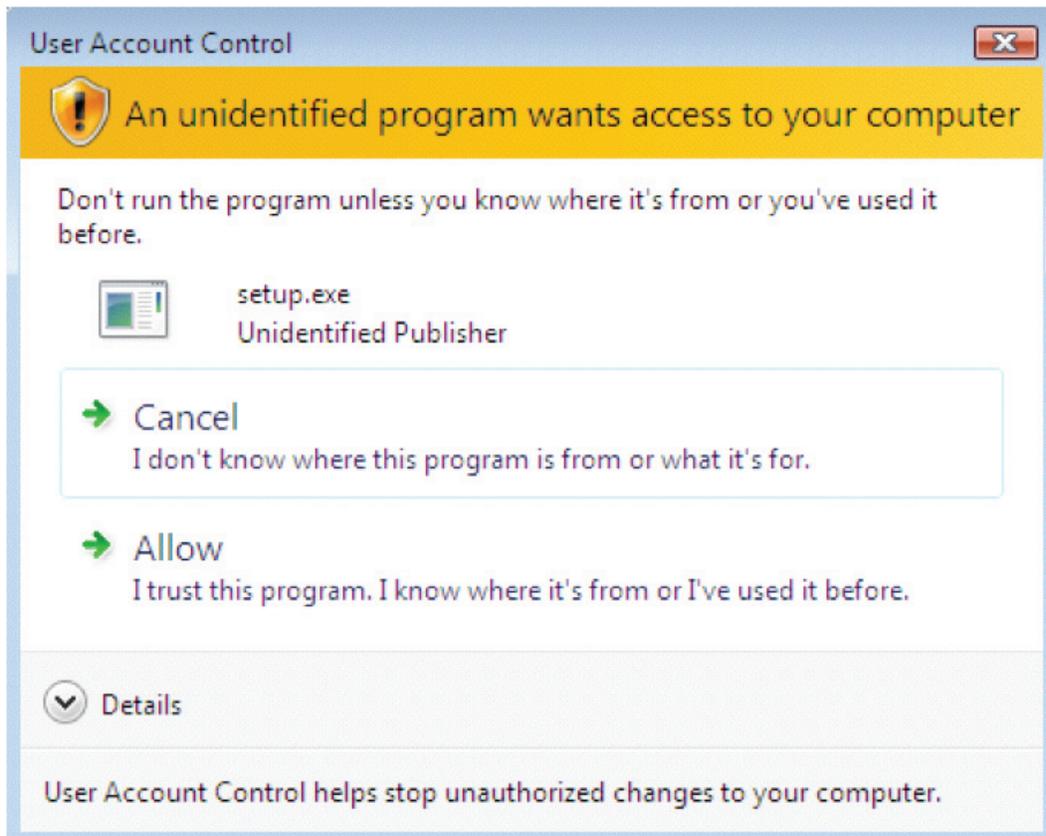
Registry virtualization is similar to file virtualization but it applies to the Windows registry keys stored under HKEY_LOCAL_MACHINE. This feature permits applications that rely on the ability to store configuration information in HKEY_LOCAL_MACHINE->SOFTWARE to continue to when they are run under a limited user account. For these users the corresponding keys and data are redirected to HKEY_CLASSES_ROOT->VirtualStore->SOFTWARE. This means that each user will maintain their virtualized copy of any values that would have been written to HKEY_LOCAL_MACHINE.

INSTALLATION ISSUES

Pervasive requires that PSQL products be installed as an Administrator or member of the Administrative group. This is consistent with previous versions and operating system platforms. The installation under Windows Vista performs similarly to previous versions (such as Windows XP) with the following exceptions.

Unsigned Application Warning

During the execution on the PSQL v9 setup.exe, Windows Vista will detect that you are running an unsigned application. This is regardless of the type of account you're running (Standard or Administrator).



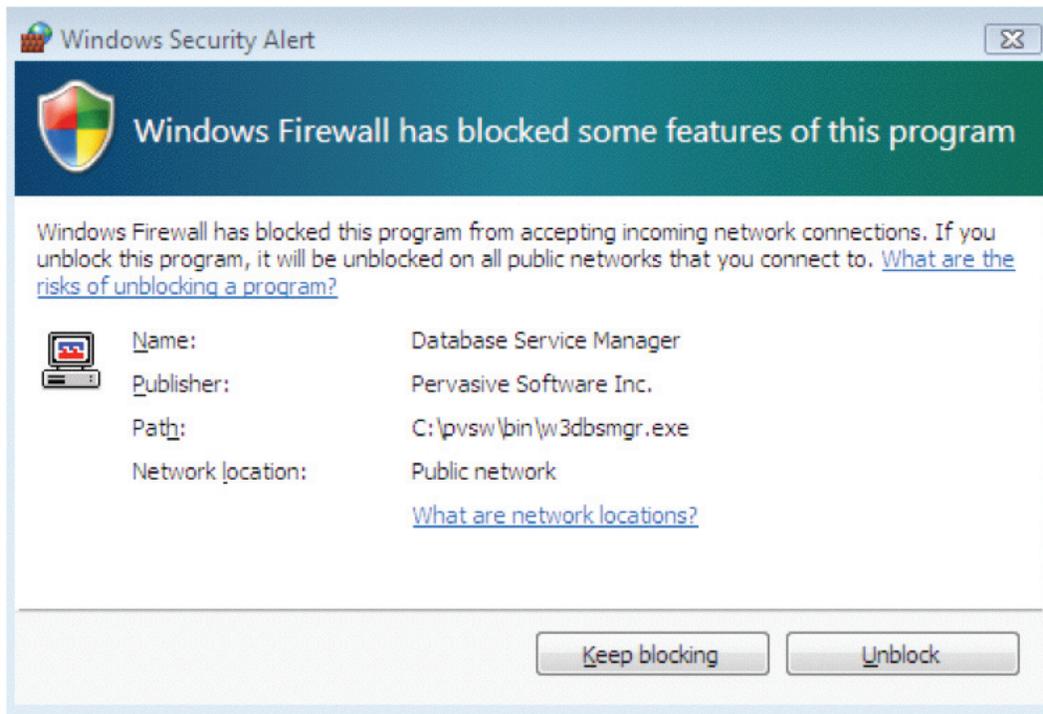
Suggestion

If you want to install the PSQL v9 application, accept this prompt and the installation will be allowed to continue.

Note: If the Pervasive installation is being executed or called by another program you may not receive this message. This also applies to application installs that perform a silent PSQL v9 installation.

Firewall – Windows Security Alert

Upon completion of the installation, or if Pervasive System Analyzer (PSA) is executed the following Windows Security Alert may be displayed:



Suggestion

If your application requires remote clients (WAN or LAN) to access the database server or engine we recommend you accept and Unblock the Pervasive program.

Note: The program name will be different depending on what engine you're installing or executing. Pervasive recommends you allow the following programs access if needed:

Pervasive Workgroup Engine = w3dbsmgr.exe

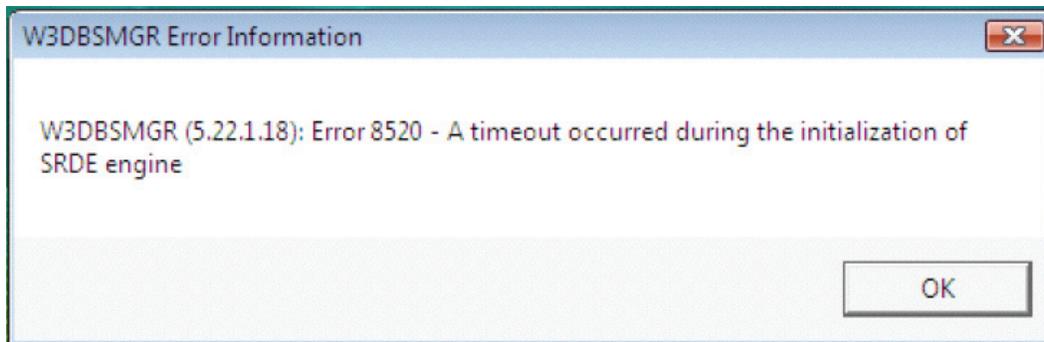
Pervasive Server Engine = ntdbsmgr.exe

SERVER ENGINE ISSUES

PSQL v9 Server engine testing reported zero errors or issues.

WORKGROUP ENGINE ISSUES

PSQL Workgroup engine is unable to start properly after performing an initial installation on Windows Vista and then logging off. This issue occurs regardless of how you are logged into the system (standard user or administrative user). Most users will receive the following message:



We have listed several workaround suggestions to solve this problem. The suggestions are ordered by best choice followed by specific solution for a particular user type. Pervasive highly recommends that users select the first option to solve the known issue for all users.

Allow members of all groups start the Workgroup Engine

Suggestions

Pervasive offers the [Pervasive PSQL Service Utility](#) for Windows Vista that will automatically set-up both the Workgroup Engine and/or the Client Cache Engine to run as a service, this is available from the Pervasive Component Zone.

More information is available in the section titled [Pervasive Windows's Vista Knowledge Base articles](#).

Members of the Administrator group are unable to start the Workgroup Engine

Suggestions

- 1) Configure the Workgroup Engine to run "as a service". This will allow the engine to start at boot time using the "local system" account.
- 2) Right click on the w3dbsmgr.exe and run Workgroup engine via Run As Administrator.

Using the standard/default view (not Classic via control panel) use the following steps to configure the needed requirements:

Add Global Privilege (SeCreateGlobalPrivilege) to the standard user group and users. Here are the steps, remember this only works for standard users.

- 1) Create a new group called psql through Control Panel > System and Maintenance > Administrative Tools > Computer Management > System Tools > Local Users and Groups > Groups > New Group.

- 2) Grant the psql group Create Global Objects privilege through Control Panel > System and Maintenance > Administrative Tools > Local Security Policy > Local Policy > User Rights Assignment > Create Global Objects policy.
- 3) Add the psql group to the list of users/groups with Create Global Objects privilege.
- 4) Add all PSQL users to the psql group.
- 5) Verify that the “Start Workgroup Engine” is in the Startup folder for “All Users” or manually add by creating the following shortcut:
`C:\PVSW\bin\w3dbsmgr.exe -SRDE`
- 6) Logon on as a standard user

CLIENT COMPONENT ISSUES

Windows Vista does not provide a Netware Client to connect to a Netware server.

Suggestions

At this time we are not aware of any Novell Netware client for Windows Vista.

Cache engine is unable to load

Suggestions

Pervasive recommends running the Workgroup Engine as a service and this will address this problem.

WINDOWS XP TO WINDOWS VISTA UPGRADE

Windows Vista allows users to upgrade from certain versions to pre-determined Windows Vista editions. Pervasive has tested this configuration with no noted issues. See the following c|net article for more information: [Holiday PC buyers get Windows Vista upgrade promise.](#)

FILE PERMISSION ISSUES

Windows Vista uses a concept called file virtualization. This process allows users to maintain their own copy of a restricted object that are not available to them as a standard user, Pervasive writes to two key files that will become virtualized for standard users; DBNAMES.CFG and PVSW.LOG. While it is possible to change the location of DBNAMES.CFG (via PCC), PVSW.LOG can not be changed.

The following files are required to have read/write permissions so that all users to be able to access.

Name	Default location
PVSW.log	Windows
DBNAMES.CFG	Windows

Suggestion

Change the existing permissions to full control or add write permissions for each required user. If these permissions are not modified, Windows Vista will create virtualized images that cannot be shared or viewed by others.

REGISTRY PERMISSION ISSUES

Registry virtualization is identical to file virtualization however this just affects item located in `HKEY_LOCAL_MACHINE\SOFTWARE`. The registry key is used by Pervasive to store system settings and configurations under `HKL_MACHINE\SOFTWARE\PERVASIVE*`

Suggestion

Change the existing permissions to full control for `HKL_MACHINE\SOFTWARE\PERVASIVE` to allow standard users to write to the registry without created virtualized keys

Note: This is not required if standard users do not have access to the Pervasive Control Center (PCC).

ODBC.INI REGISTRY PERMISSION ISSUES

Certain applications create and update Data Source Name (DSN) entries, these items are stored in the Windows registry under: `HKL_MACHINE\SOFTWARE\ODBC*`

These items will become virtualized for standard users and could cause a problem for certain applications.

Suggestions

Change the existing permissions to full control for `HKL_MACHINE\SOFTWARE\ODBC` to allow standard users to write to the registry without created virtualized keys.

PERVASIVE CONTROL CENTER (PCC) ISSUES

In certain cases standard users are unable to create system Data Source Names (DSN) from within PCC. This behavior is consistent with ODBC Administrator operation.

Suggestions

Pervasive recommends that these operations only be performed by a member of the administrative group and not standard users. This issue will be addressed in a future release.

Standard Users are unable to Start and Stop Services from within PCC

Suggestions

Pervasive recommends that these operations only be performed by a member of the administrative group and not standard users. This issue will be addressed in a future release.

UTILITY ISSUES

Butil —stat operations returns a Butil -149 and fails when trying to create the required temporary file.

Suggestions

Pervasive recommends using the Maintenance utility to perform this operation. This will be addressed in a future release.

Pervasive System Analyzer does not recognize the Windows Vista Operation System in the system information screen.

Suggestions

This is a known issue and will be addressed in a future release.

Pervasive System Analyzer does not complete successfully as a standard user when performing Archive, Restore or Delete functions.

Suggestions

Pervasive recommends that these operations only be performed by a member of the administrative group. This issue will be addressed in a future release.

DOCUMENTATION ISSUES

All Pervasive online Java help file work as expected. However, because WinHelp (.hlp) is not supported in Windows Vista the following utilities help files are not available:

- Monitor
- Maintenance
- Export Wizard
- ODBC Administrator

Suggestions

Users can download a Microsoft provided WinHelp program from the Microsoft Download Center; this will allow users to view the 32bit WinHelp files on Windows Vista.

Note: Third-party software vendors are prohibited from redistributing the WinHelp program so Pervasive is unable to provide it as a solution. See Microsoft Knowledge Base for the following [WinHelp Article](http://support.microsoft.com/kb/917607) (<http://support.microsoft.com/kb/917607>).

TERMINAL SERVICES RUNNING ON WINDOWS VISTA

Both the Pervasive PSQL v9 database engines and clients can be installed on Windows Terminal Services with users running Remote Desktop. The following issue was noted when using remote desktop under Windows Vista.

Terminal services clients are able to change the PSQL v9 configuration on the server. This is different than the behavior today where only console users are allowed to modify.

Suggestions

Pervasive Suggests adding the following registry key to the server registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Pervasive Software\Utilities Interface\
Settings\RestrictedAccessOnWTSCient
```

“RestrictedAccessOnWTSCient” should be set as a DWORD and the value set to 1

JAVA RUN-TIME ENGINE (JRE) ISSUES

Pervasive PSQL v9 utilizes the Sun Microsystems Java Runtime Engine (JRE) 1.5.0_05 as a core component of the Pervasive Control Center (PCC). Sun Microsystems recommends that users upgrade to the latest version of the JRE which is version 6.0 (or version 1.5.0.10 or higher) to ensure Windows Vista compatibility.

Suggestions

While Pervasive has no known issues related to the JRE we strongly encourage users to evaluate the latest version and upgrade to ensure compatibility.

JDBC based applications may experience incorrect date/time formats when getting and storing data and time strings.

Suggestions

This issue has been fixed by Sun Microsystems and is fixed as part of the latest 1.6.0 or 1.5.0.10 releases.

AERO INTERFACE

Windows Vista introduces the new Aero “glass” interface that allows rich multi-dimensional viewing. The following exceptions have been noted:

Some Pervasive Control Center (PCC) screens have difficulty in switching out of the Aero interface mode.

Suggestions

This issue is resolved by applying the latest Windows Vista compliant JRE as noted above under Java Run-Time Engine (JRE) Issues.

MISCELLANEOUS ISSUES

The following are issues noted in our testing that were unrelated to database compatibility or Pervasive PSQL v9 issues. We have listed these items for informational purposes.

Testing results indicated that the floating point precision has changed with Windows Vista as compared to prior operating systems. There were two types of changes noted:

Real Data Types — appear to have higher limits, the following SQL statement illustrates this:

```
STATEMENT #315: alter table t1(add c1 float default -2.2250738585072e-309 )
SQL statement complete.
      Status Expected: -1, 22003, 0
      Status Received: 0, 00000, 0
```

Numeric Conversion Changes — It appears that the precision is now different, the following SQL statement illustrates this:

```
select CONVERT('1998-01-02 23:59:59.997',SQL_FLOAT)
*** error
select CONVERT('1998-01-02 23:59:59.997',SQL_FLOAT)
      Status Expected: -1, S1000, 0
      Status Received: -1, 00000, 0
```

CONCLUSION

For most users, adopting Windows Vista will require additional steps to perform operations that were previously handled as either a standard user or administrative user. The level of user interaction with the User Account Control (UAC) will vary based on application and security requirements.

Most users will not see any difference between Windows Vista and other Microsoft platforms when running PSQL v9 server. For Workgroup users, the change is a bit more significant and users should evaluate the options for running in a standalone or peer-to-peer environment.

Pervasive anticipates that adoption for Windows Vista will increase in late half of 2007 with widespread adoption in 2008. Based on analyst and media reports this is consistent with most assumptions. With the release of Pervasive PSQL v10, users will be able to seamlessly work with Windows Vista and UAC regardless of the user account types (Standard or Administrative).

In conjunction with this report, Pervasive recommends that users research the various Microsoft and independent Web sites to learn more about Windows Vista. While we have provided some background it is important for the reader to do additional research to ensure they understand the changes in Windows Vista that may affect users, applications, and security requirements.

Pervasive's Windows Vista Knowledge Base Articles:

Pervasive PSQL Support Policy for New Versions of Supported Operating Systems

[Solution ID: 00017590](#)

Does Pervasive PSQL support Microsoft Windows Vista?

[Solution ID: 00017583](#)

Pervasive Software's Statement of Support for Microsoft Windows Vista

[Solution ID: 00017768](#)

Pervasive Product Life Cycle

[Solution ID: 00014859](#)

Pervasive PSQL Workgroup v9 returns Error 8520 when run on Windows Vista

[Solution ID: 00017849](#)

SRDE returns Error 8520 on Windows Vista

[Solution ID: 00017857](#)

SRDE returns Error 8520 after initial install on Windows Vista

[Solution ID: 00017856](#)

Additional references include:

Windows Vista Home site

<http://www.microsoft.com/windowsvista>

Windows Vista Get Ready site

<http://www.microsoft.com/windowsvista/getready>

Windows Vista Editions

<http://www.microsoft.com/windowsvista/getready/editions>

Windows Vista Blog

<http://windowsvistablog.com>

SuperSite for Windows

<http://www.winsupersite.com/vista>

The Helpware Group

<http://www.helpware.net/VistaCompat.htm>

eWEEK Windows Vista

<http://www.eweek.com/category2/0,1874,1840947,00.asp>

ZDNet Windows Vista RTM

http://review.zdnet.com/Windows_Vista_RTM/4505-3672_16-32137426.html

Contact Information

Pervasive Software Inc.
12365-B Riata Trace Parkway
Austin, Texas 78727

United States

800.287.4383
512.231.6000
Fax: 512.231.6010
info@pervasive.com

EMEA

+800.1212.3434
cic@pervasive.com

<http://www.pervasive.com>

© 2007 Pervasive Software Inc. All rights reserved. All Pervasive brand and product names are trademarks or registered trademarks of Pervasive Software Inc. in the United States and other countries. Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. All other marks are the property of their respective owners.