

Pervasive PSQL Product Authorization

A Pervasive Software Whitepaper

7/21/2011

Table of Contents

Pervasive PSQL Product Authorization 3

Introduction 3

Product Authorization Basics 3

 Key Generation and Delivery 3

 Validation and Authorization 4

 Product Deauthorization..... 4

Ways to Authorize a Pervasive PSQL Key..... 5

 Online Authorization 5

 Remote Authorization..... 6

 Offline Authorization 6

 Telephone Authorization 7

Hardware Changes, Virtual Machines, Disaster Recovery, and Reusing Keys 8

 General Rule: Deauthorize First 8

 Hardware Changes 8

 Pervasive Notification Viewer 9

 How to Resolve a Failed Validation State 9

 Authorization and Deauthorization for Virtual Machines 10

Disaster Recovery..... 10

Summary 10

Additional Resources 11

Pervasive PSQL Product Authorization

Introduction

Licensing for Pervasive PSQL is enforced by the use of keys. Keys are associated with individual computers and can be authorized and deauthorized. Product authorization is a key validation process verifying that the copy of software is legitimate, correctly licensed and on the appropriate hardware and software platform. Beginning with Pervasive PSQL v10, Pervasive has employed product authorization technology to ensure the validity of copies of Pervasive PSQL. Our goal is to protect against casual copying of our software products and to extend that protection as simply as possible to our ISV, OEM, and Distributor partners. Pervasive has field tested the product authorization process for electronic downloads of PSQL trials and e-commerce purchases for over a year and with the release of PSQL v11, all Pervasive PSQL products use the product authorization process.

This paper will help developers and end users better understand the Pervasive product authorization process and the various ways to authorize Pervasive PSQL.

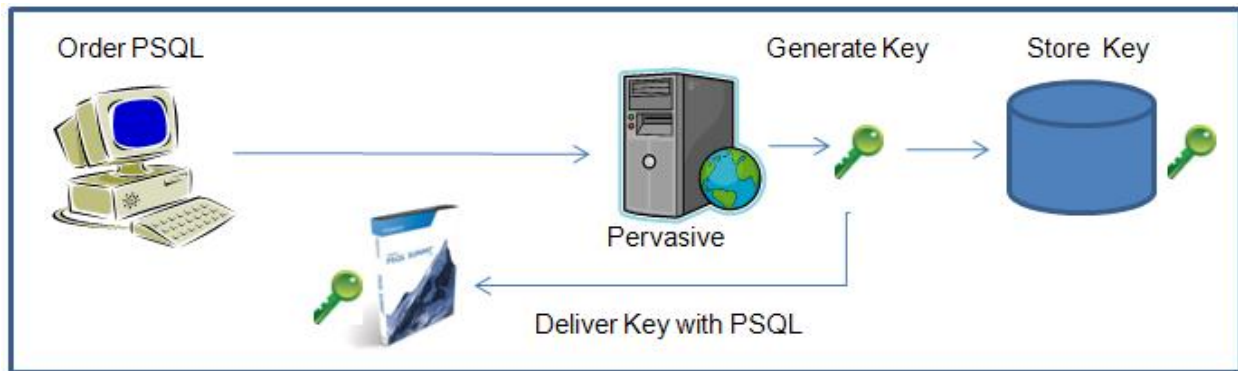
Product Authorization Basics

Product authorization involves three main components: 1) the software, 2) a key, and 3) a process that validates and authorizes the key for the product. The software is typically delivered with a key and that key is applied during installation and validated on the local machine or, more recently, by a remote process requiring an Internet connection. These are the basics of Pervasive PSQL product authorization. The biggest difference between PSQL v10 and earlier versions is that product authorization now uses an Internet connection (except in the case of Telephone Authorization) as part of the validation process. The Pervasive PSQL Product Authorization process can be broken into two main steps: 1) Key Generation and Delivery and 2) Validation and Authorization.

Key Generation and Delivery

- 1) When a copy of PSQL is ordered from the Pervasive website, downloaded as a trial, or purchased from a Pervasive partner a key is generated and delivered with the product or via email.
- 2) A copy of that key is stored in a Pervasive server to be used as part of the validation and authorization process.

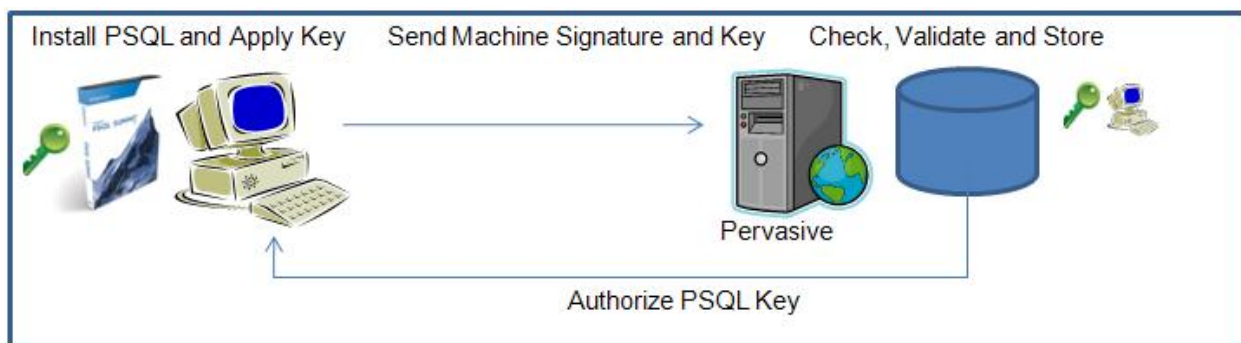
Key Generation and Delivery



Validation and Authorization

- 1) The authorization process is started after you install PSQL by inputting the key using the PSQL License Administrator. The authorization process can be started during the installation process of PSQL, or after you install PSQL by inputting the key using the PSQL License Administrator.
- 2) The installation process, or the License Administrator, connects to the Internet to send the key, along with hardware configuration information specific to the machine (a machine signature), to the Pervasive server.
- 3) The server verifies that the key is registered in its database and confirms that the key is not already associated with another machine.
- 4) Once the key has been validated, the server creates a unique installation pairing between the key and the machine signature and authorizes the key for PSQL.

Validation and Authorization



Product Deauthorization

A big part of the control delivered by product authorization is the linking of a copy of software to a specific machine. But, because machines fail, get replaced, or get upgraded it is important to have a way to move a copy of software from one machine to another. This is enabled by Product Deauthorization, which is simply deleting the machine signature associated with a key. The key remains

inactive until it is applied again on the same machine or on another machine. Product deauthorization requires an Internet connection.

Ways to Authorize a Pervasive PSQL Key

Currently, there are four ways to authorize a Pervasive PSQL Key:

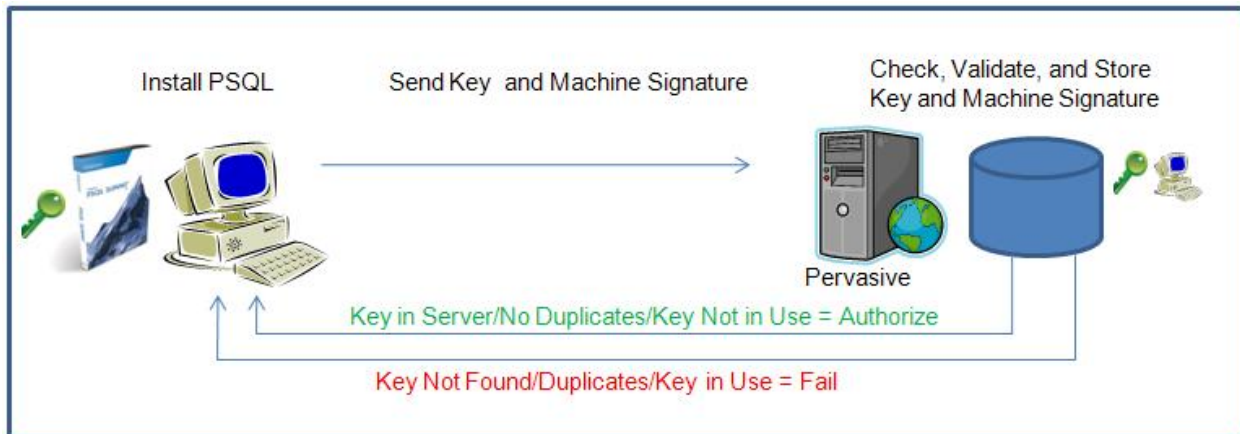
- Online—the machine with PSQL installed is connected to the Internet.
- Remote—the machine with PSQL installed is not connected to the Internet, but is networked to another machine with Internet access.
- Offline—the machine with PSQL installed is isolated from the Internet, but can accept portable storage (for example, a USB drive) from another machine with Internet access.
- Telephone - If Online, Remote, and Offline authorization aren't available, Pervasive PSQL can be authorized with a telephone call.

Online Authorization

Online authorization was described above when covering the basics of Product Authorization. It is worth mentioning again because it is the most common method by which the Pervasive PSQL key is authorized. It is simple, quick and almost unchanged from previous versions of PSQL:

- 1) Install PSQL, input the key, click the Apply button to authorize
or
- 2) Install PSQL, open the License Administrator, input the key, click the Apply button to authorize

Online Authorization



After you input the key and click the Apply button, the process is automatic and takes only a few seconds. Online deauthorization is accomplished through the License Administrator by selecting a key and clicking the Delete button to deauthorize.

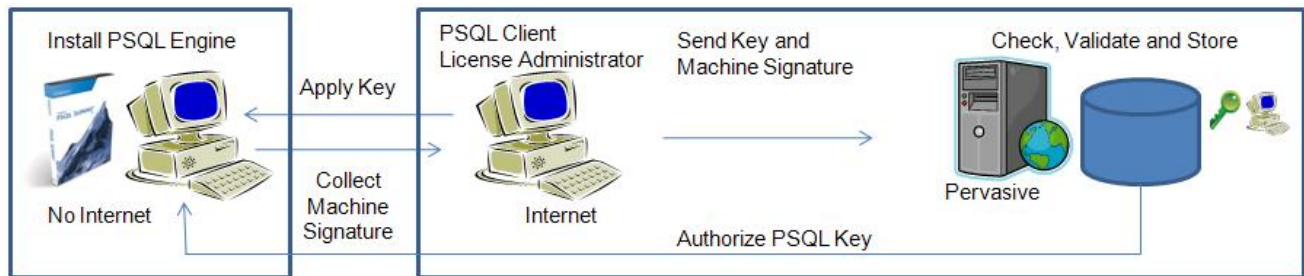
Remote Authorization

Remote authorization is used if the machine running the database engine is not connected to the Internet, but it is connected to another machine that is connected to the Internet.

The following is a typical scenario for using remote authorization:

- 1) Install a PSQL engine (Server or Workgroup) on the non-Internet machine.
- 2) Install a PSQL client on an Internet machine.
- 3) Use the PSQL License Administrator on the Internet machine to access the PSQL engine (Server or Workgroup) on the non-Internet machine.
- 4) Apply the key to authorize PSQL.

Remote Authorization



Remote deauthorization is accomplished using the License Administrator on the PSQL Client machine. Refer to *Pervasive PSQL User's Guide* for details about using the licensing utilities for remote authorization or deauthorization of a key.

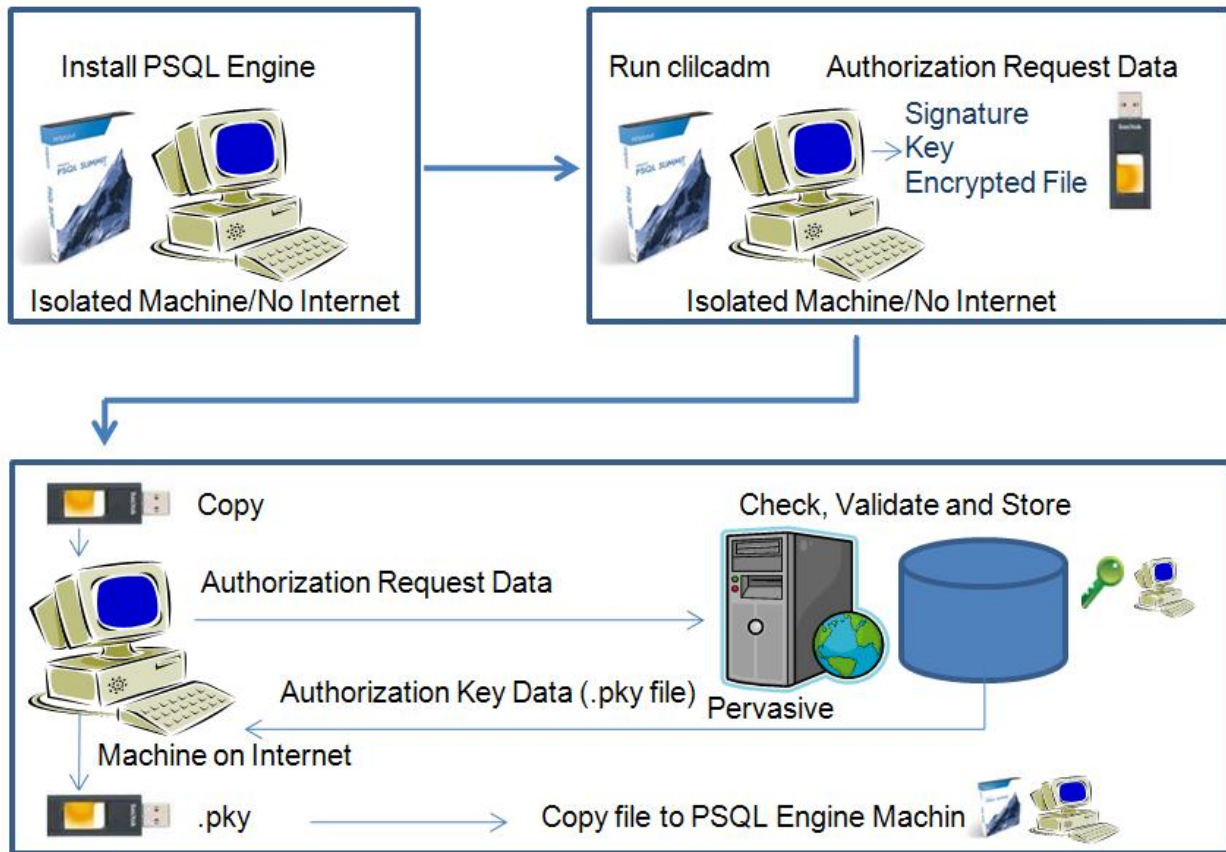
Offline Authorization

Offline authorization involves applying a key on a machine that is not connected to the Internet or connected to machine that has an Internet connection. This necessitates moving files required for authorization between the machine on which the PSQL engine is installed and another machine that is connected to the Internet. The example below uses a USB flash drive for transferring files but any portable storage device will do as long as the device is read/write capable.

- 1) Install a PSQL engine (Server or Workgroup) on the machine with no Internet connection.
- 2) Using the command line License Administrator, generate an Authorization Request Data file (run the `clilcadm` utility to collect the machine signature information for the Offline Machine and combine it with the key data in an encrypted file to carry to the Internet Machine). Save the Authorization Request Data file to a USB drive.

- 3) If the machine with Internet connectivity does not have PSQL installed, also copy the licgetauth.exe file from the Pervasive PSQL bin folder to the USB drive.
- 4) Copy the Authorization Request Data and the licgetauth.exe files from the USB drive to the Internet Machine
- 5) Send the Authorization Request Data to the Pervasive server and retrieve the Authorization Key Data (run licgetauth.exe to send the key and machine signature information to the server and return the authorization data).
- 6) The output of this process is a .pky file including the Authorization Key Data needed to authorize Pervasive PSQL on the Offline Machine. Save the .pky file to a USB drive.
- 7) Bring the USB drive to the Offline Machine and apply the Authorization Key Data file (run the clicladm utility).

Offline Authorization



Telephone Authorization

In the event that online, remote, or offline key authorization is not possible (for example, when you have no Internet connection), Pervasive PSQL can be authorized using a telephone. Telephone

authorization requires a working Pervasive PSQL v11 Server or Workgroup engine installed and a valid product key.

Telephone authorization is available from 9:00 AM to 5:00 PM Central Time (Austin) by calling 1-800-287-4383 or +1-512-231-6000.

To authorize a key using telephone authorization:

- 1) At a DOS prompt, type clipaadm.exe.
- 2) At the prompt, enter the product key. The PSQL Phone Authorization Utility returns an authorization code used to complete telephone authorization.
- 3) Call Pervasive at 1-800-287-4383 or +1-512-231-6000 to complete telephone authorization.
- 4) Provide the authorization code to Pervasive staff and they will provide you an Authorization data string.
- 5) Enter the Authorization data string at the DOS prompt as the final step of Telephone authorization.

Hardware Changes, Virtual Machines, Disaster Recovery, and Reusing Keys

General Rule: Deauthorize First

When uninstalling Pervasive PSQL, upgrading a server running PSQL, cloning a virtual machine or moving Pervasive PSQL to another system – **always delete (deauthorize) the PSQL key first**. This way you can be sure that the key used to authorize your copy of PSQL will not already be associated with a machine signature and can be used to reauthorize PSQL whenever and wherever needed.

Hardware Changes

Always deauthorize (delete) the Pervasive PSQL key before making changes to hardware. Here is why. When the PSQL engine starts, it checks to confirm that the machine signature related to that installation of PSQL is unchanged. Changes to three or more of the attributes that make up the machine signature will cause the key state to change from Active to Failed Validation. For virtual machines, any changes in the machine signature attributes (except memory) will cause the key state to change to Failed Validation. If the Failed Validation state is not corrected in a specific time period (usually 14 days but may be different depending on PSQL version and what company created the key), the key will become Disabled. Note: the Failed Validation key state feature is not available on releases of Pervasive PSQL prior to v11 SP1. For those releases, the hardware changes described above will cause the key to go directly to a Disabled state.

Pervasive Notification Viewer

The Pervasive Notification Viewer is a Windows and Linux tray application that creates a notice whenever the PSQL key state changes - for example when a hardware change moves the key state from Active to Failed Validation. Notices are repeated daily until the issue is resolved. The Notification Viewer also provides information about the reason for the validation failure and includes steps to use to resolve the issue. Note: The Notification Viewer is not available in versions of Pervasive PSQL prior to PSQL v11 SP1.



Notification Viewer Normal



Notification Viewer Alert

Notifications

Today

Key Validation Failed Mon, 11 Jul 2011 16:53:51
Key 4KXR3-8GFFB-M4F2Q-68YK3-XXYDW-6WQP failed validation.

Previous 7 Days

Older

Key Active Thu, 30 Jun 2011 09:18:57
Key 4KXR3-8GFFB-M4F2Q-68YK3-XXYDW-6WQP is now active

Key Validation Failed Thu, 30 Jun 2011 09:14:53
Key 4KXR3-8GFFB-M4F2Q-68YK3-XXYDW-6WQP failed validation.

Details

The state of key **4KXR3-8GFFB-M4F2Q-68YK3-XXYDW-6WQP** has changed from "active" to "failed validation." Pervasive PSQL has detected the following validation failure:

- Changes to machine signature. One or more of the following: Computer Name, CPU Type.

Pervasive PSQL will function normally for **14** more days.

You need to resolve the validation failure to restore the key to the "active" state before the **14** days expire. Otherwise, the key changes state to "disabled" and the database engine can no longer access data files. If necessary for further troubleshooting, also review the messages in the other log repositories used by Pervasive PSQL, such as the operating system event log or PVS.W.LOG.

Corrective Action:

- Set the machine signature tokens Computer Name, CPU Type to match their value when the key was initially applied. For example, you initially applied the key on a machine named "First_Name." Then you changed the machine name from "First_Name" to "Second_Name," which caused the violation. Re-name the machine back to "First_Name."
- Perform a validation action with License Administrator. Click "Validate" in the graphical user interface or use the -validate option with the command line interface.
- Verify with License Administrator that the state of key **4KXR3-8GFFB-M4F2Q-68YK3-XXYDW-6WQP** returns to "active." Visually check the "State" column in the graphical user interface or use the -interpret option with the command line interface.

Please contact the vendor of the application for further assistance.

3 notification(s)

Notification Viewer Details

How to Resolve a Failed Validation State

There are two ways to return a key to the Active state from Failed Validation. The first is to return the machine to its original state (before the validation check failed), deauthorize (delete) the key, make the hardware changes and reauthorize (re-apply) the key. The second option is to contact Pervasive Support

(or, if you got your copy of Pervasive PSQL from an OEM, contact the OEM) and ask to have the key repaired. Repairing the key puts it into a state where it can be deauthorized and reauthorized on the machine.

Note: If a permanent license is deauthorized, all of the user count increases (UCI's) associated with that license are deauthorized also.

Authorization and Deauthorization for Virtual Machines

The authorization process collects unique machine signature information from each instance of a virtual machine. Therefore, each image (including clones and copies) requires its own key. Authorization and deauthorization for virtual machines work the same way as online authorization.

Note that, except for memory allocation changes, changing the configuration of a virtual machine alters the machine signature just as it would for a physical machine. When changing a configuration, copying or moving a virtual machine, deauthorize (delete) the Pervasive PSQL key first. This is the best way to ensure reauthorization on the new virtual machine.

Disaster Recovery

If the machine running Pervasive PSQL fails, it does not automatically connect to the remote Pervasive server and deauthorize the PSQL key. The key associated with that machine signature, as far as the Pervasive server is aware, is still active. This means the key cannot be used for any other system. The only way to get the key into a state where it can be reauthorized is to contact Pervasive Support and have the key reset. Support hours are Monday through Friday 9:00 AM to 5:00 PM CST:

- In the U.S. at 800.287.4383 (select option 1, then option 2)
- In Europe at 00800.1212.3434

If the server failure occurs outside of Pervasive's normal hours and a working system is needed immediately, download a temporary version of PSQL from the Pervasive website at <http://www.pervasivedb.com/download/Pages/PDBDownloads.aspx>. The download process will deliver a 20-user Server or 5-user Workgroup with a 30 day license that can be used to enable a standby system until Pervasive can reset the key or the server is repaired.

Summary

Product authorization helps Pervasive and its partners protect their software and ensure that customers get valid copies of software. Of the three ways to authorize a PSQL key, the great majority of product

authorization will be simple online authorization. Most end users will see very little difference in licensing between PSQL v10 and previous versions.

Additional Resources

Read the License Administration documentation in the *Pervasive User Guide*:

<http://www.pervasivedb.com/support/Pages/Documentation.aspx>

Status Codes pertaining to key authorization:

License Administrator – 7063 – 7127

Authorization/Deauthorization – 7201 – 7399

Read the PSQL License Authorization FAQ: <http://www.pervasivedb.com>