PSIGEN software inc.

11.x

Update: 06.06.2018

PSIsafe

Architecture

PSIsafe Architecture

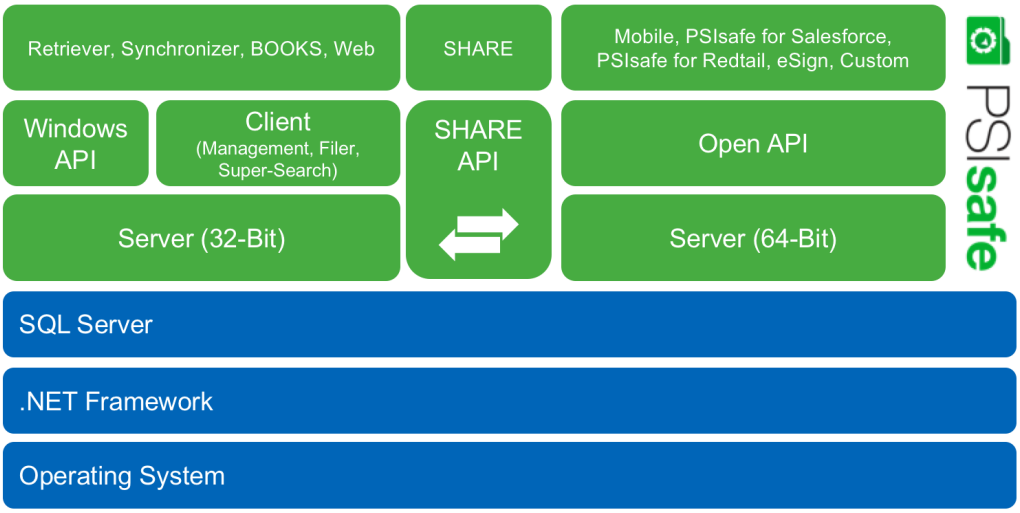
Introduction

PSIsafe is a comprehensive document management and workflow system that can be installed on-premises or hosted by PSIGEN software, inc. and accessed through the internet.

PSIsafe includes a number of components used to create a document management system. The system enhances efficiency by managing and automating the flow of documents throughout an organization. PSIsafe's architecture supports many configurations that operate in standalone or integrated (with other business applications) environments.

This document is designed with IT professionals in mind and outlines each component and the role it provides in the overall system. The technical requirements of each component are also defined to enable fully operational systems that perform at an optimum level.

System Requirement Hierarchy



For more information on system requirements please refer to http://wiki.psigen.com for the latest specifications.

Operation System (OS)

PSIsafe may be installed only on a Windows Operating System (OS). The PSIsafe instance may be access via Windows desktop, modern web browsers, and via modern mobile devices (Apple iOS and Android OS).

.NET Framework

PSIsafe requires Microsoft .NET Framework Version 4.6.1 or later on the server as well as the client machine. The same version of .NET Framework is also required on the server where PSIsafe Open API is installed for, Mobile apps or any Custom integration that use the API.

SQL

The backend used for PSIsafe data is SQL. Microsoft SQL Server 2008 R2 or later are supported. SQL Express editions are also supported and can be used if the number of users is less than 10.

Authentication type is set during registration. Both Windows and SQL authentication are supported.

Client

This consists of

1) Client software: this is the main PSIsafe interface.
2) Management: this is used to configure repositories, users, cabinets, rights and other settings.
3) Filer: utility used to file external documents into PSIsafe.
4) Virtual Printer: printer used to print document from any external application into PSIsafe.
5) Super-Search: this is a quick search module.

Server

The server consists of windows services and is covered in detail under - PSIsafe Server Components.

API

PSIsafe Open API and PSIsafe Windows API allow developers to utilize a development framework to create firm-wide interoperable paperless workflows.

Modules

Several optional modules can increase the flexibility and scalability of PSIsafe electronic document management system. For more information contact sales@psigen.com.

PSIsafe Server Components

Server Services

32-BIT

1) Server Windows Service:
    a. Controls user access to the database and repositories.
    b. Tracks PSIsafe licenses.
    c. Generate and server image previews.
    d. Must be running for usage of PSIsafe software.
2) Full Text Search Windows Service: This service indexes specified cabinets for full text search.
3) Workflow Service: This is used for workflow and other notifications.

64-BIT

1) Server Windows Service:
    a. Required for PSIsafe Open API.
    b. Must have 32-bit server running in conjunction for the usage of the software.

Database

Microsoft SQL database is used as the database for PSIsafe[1]. The database stores links, rights, and information related to documents in the repository. The actual documents are not saved within the database.

Key Directories Used and Location[2]

1) PSIsafe Install Directory:
    a. Service log files.
    b. Update files.
    c. Temporary file transfer location.
    d. Location of Service files and their dependencies.
2) Repositories:
    a. A user designated location(s) to store PSIsafe documents. All documents filed into PSIsafe will reside here. Only the metadata for these documents will be in the SQL database.
3) Distribution\Batch Sync:
    a. A user designated location to store PSIsafe documents related to workflow distribution and batch synchronization.

PSIGEN recommends that a dedicated domain account be created for PSIsafe use with modify access to all locations. This will help secure the repositories from unwanted access.

The default account that runs these windows services is “Local System”. Depending on the PSIsafe system configuration used, the account running these services might have to change.

1) *If the SQL Server Instance name is used instead of the IP address, the SQL Browser service will have to be running.*
2) *The Windows account that runs the Server services should have Modify access to all locations.*

Windows and SQL Accounts

There are two main user accounts required for PSIsafe:

1. Windows account that runs PSIsafe Server Windows Services:
    a. Depending on your configuration, they can be:
        i. Local System.
        ii. Administrator.
        iii. Dedicated Windows user for PSIsafe.
    b. The account that runs the PSIsafe Server services should have **Modify** access to:
        i. The PSIsafe Server Install directory.

ii. All PSIsafe repositories.

iii. Workflow distribution\Batch sync directory.

c. This is the account used for authentication between repository – Client file transfer.

2. SQL account that is used to register PSIsafe

a. This is the account that is used by the PSIsafe Server and Client to communicate with SQL.

b. They can be one of the following:

i. A dedicated PSIsafe SQL user (using SQL Authentication)[3].

ii. Any Active Directory (AD) user (using Windows Authentication)**[4].**

c. Minimum requirements for the account to access: "[CNG_Main]" and "[CNGForms]" DB

i. Security > Login - Server roles should have **Public** set to TRUE.

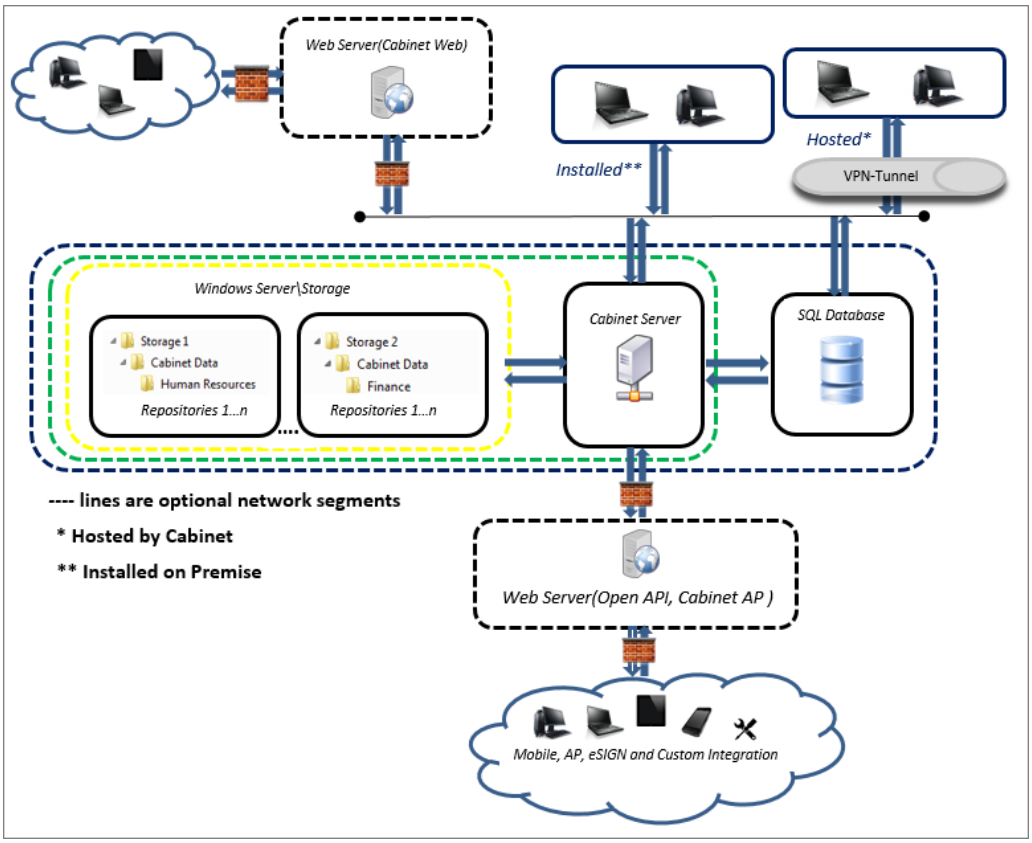
ii. Security > Login - User mappings should have **db_datawriter**, **db_datareader** and **Public** set to TRUE.

iii. Security > Login - Status should have options set to **Grant** and **Enabled**.

3) For SQL Authentication ONLY, Enforce Password expiration has to be set to FALSE. If set to TRUE, when the password expires, the PSIsafe system will not function until registered with the new password. If SQL Authentication is used, the SQL Server Instance has to be set with Mixed Mode Authentication.

4) If PSIsafe Web is used, SQL Authentication for PSIsafe registration is recommended. Windows authentication is not appropriate for an Internet environment, because user credentials are not encrypted or required. However, if Windows Authentication must be used, the identity in the application pool for Web should have the minimum requirements mentioned in 2c.

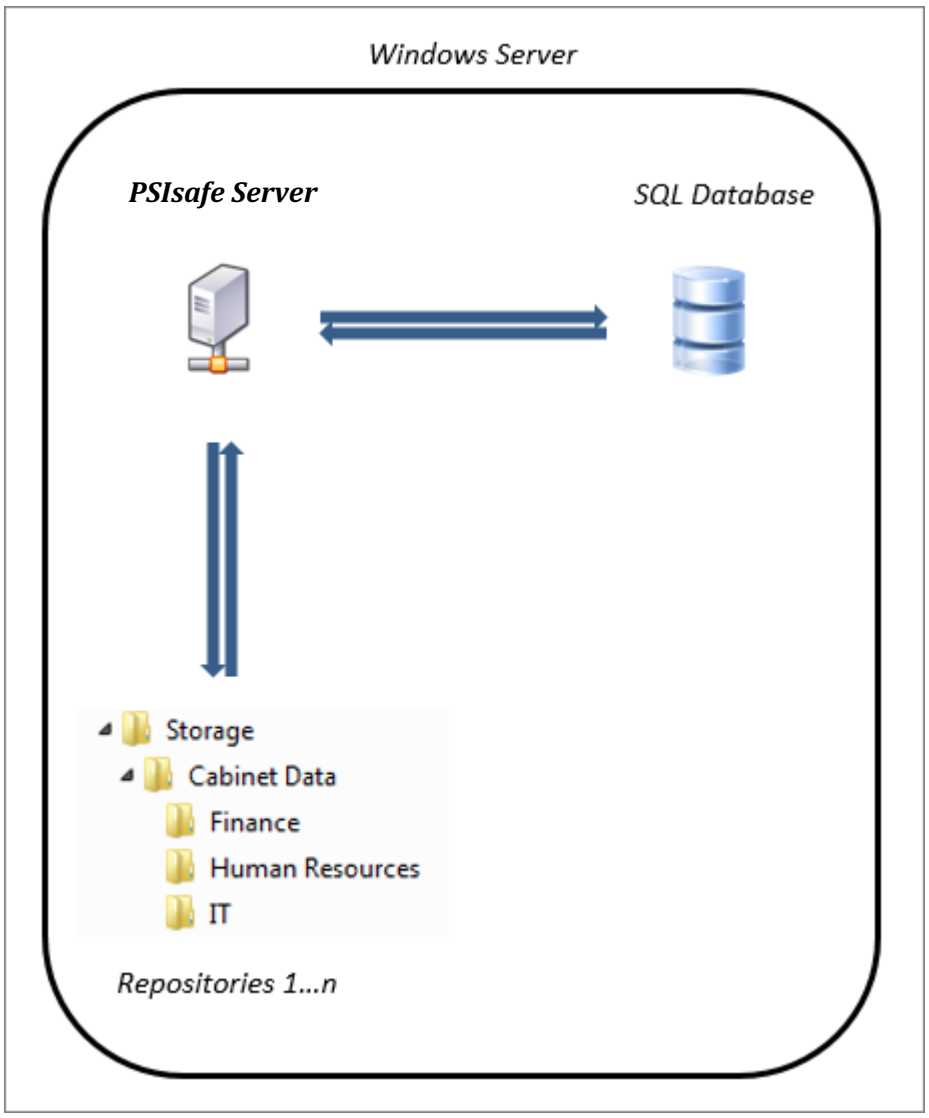
Safe System Configurations



The server may be configured in a few different ways. For the hosted scenario, the server configuration is handled by PSIsafe. For on-premises, an optimum server configuration may be selected to accommodate the number of users, estimated volume of data files, average file size, available storage, and available hardware. There are four (4) common server configurations designed to support a wide range of environments.

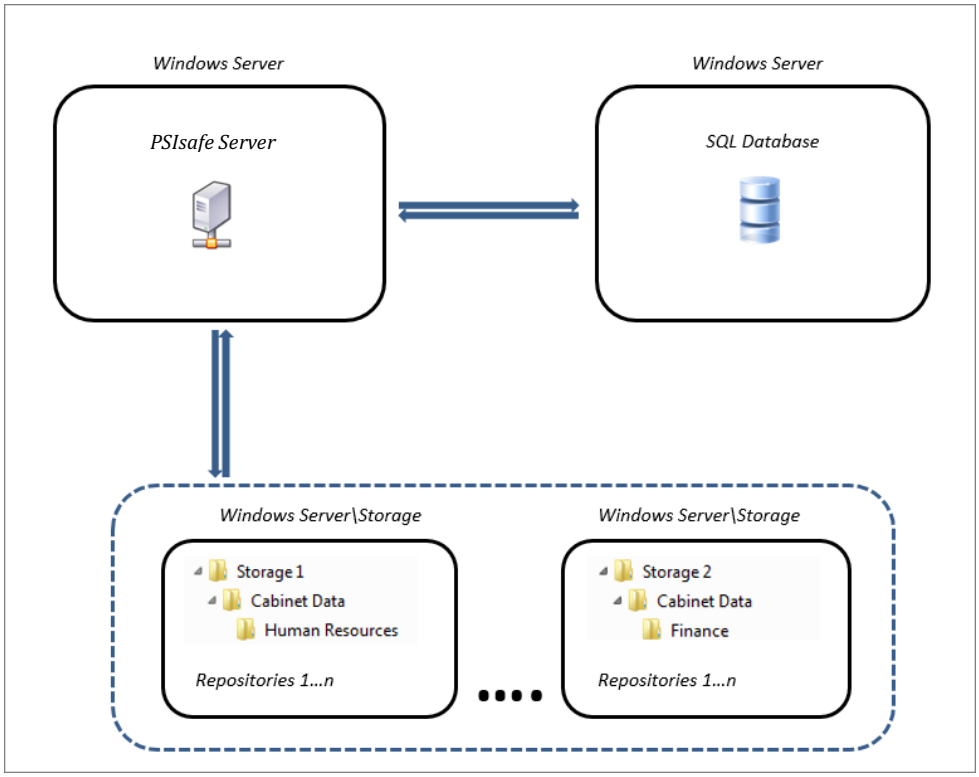
PSIsafe System Configuration 1

One server is used with to host the PSIsafe Server, SQL server, and repository instance. This is often used for demonstration environments, and sometimes used for testing environment.



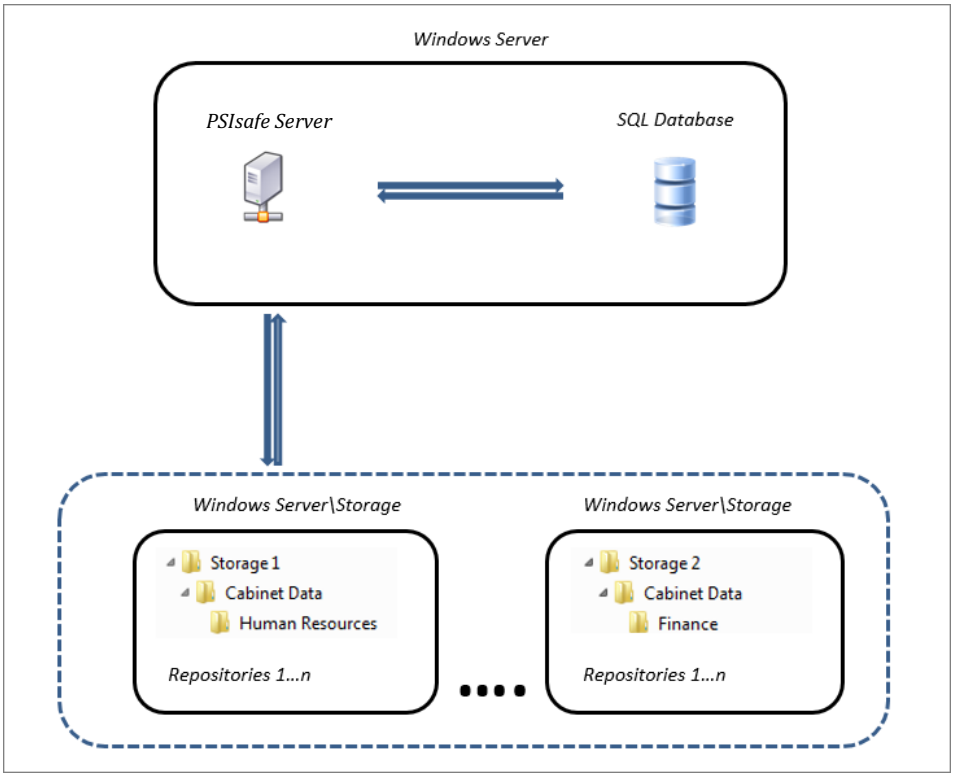
PSIsafe System Configuration 2

PSIsafe Server and SQL server are installed on separate servers, and the repositories reside on one or more server\storage devices. This configuration is generally used in medium- to large-sized installations.



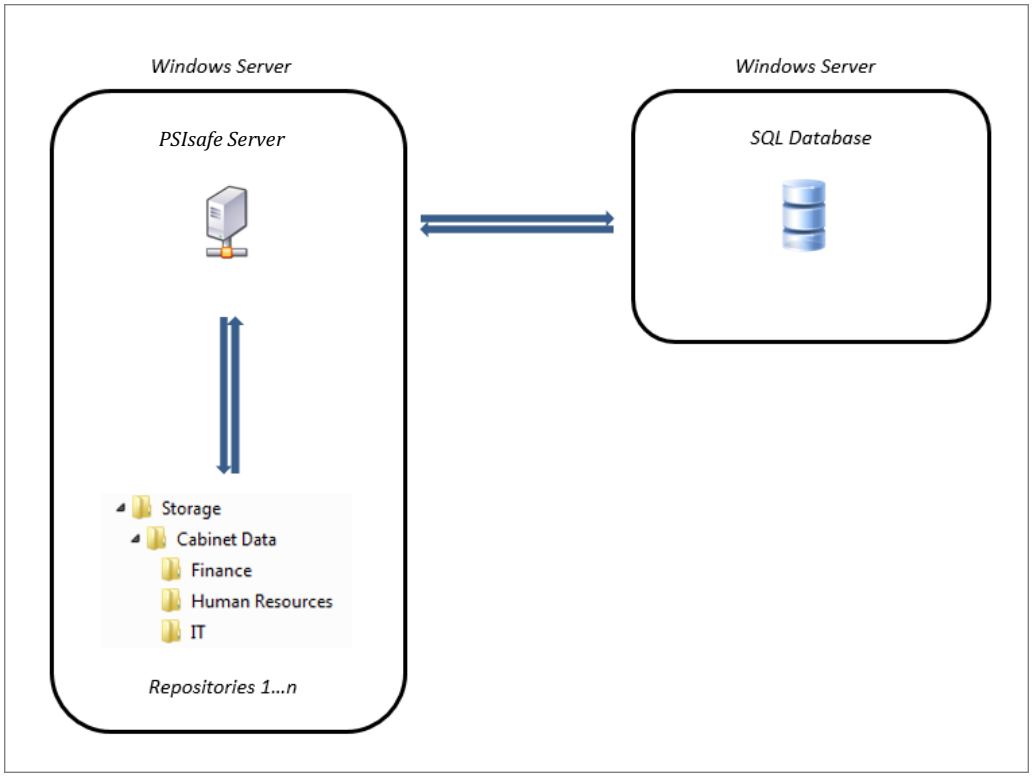
PSIsafe System Configuration 3

PSIsafe Server and SQL server are installed on the same server, and the repositories reside on one or more server\storage devices. This configuration is generally used in small- to medium-sized installations.



PSIsafe System Configuration 4

PSIsafe Server is installed on the same server as the repository, while SQL server is installed on a separate server. This configuration is generally used in small-sized installations.



Repository

Repository is a user designated location to store PSIsafe documents. Repositories can be on the same server as the PSIsafe Server or on a different server. Since repositories are used for storing documents, it is essential to analyze your storage requirements before you designate your repository.

Repository paths are relative to the location of the PSIsafe server. If the repository is located on a different server, its path set in PSIsafe Management should be denoted using a UNC naming convention. If the repository is on the same server as the PSIsafe Server, its path should be denoted using the drive letter. This includes storage devices attached to the PSIsafe Server.

Repository Examples

1. PSIsafe Server installed and repositories located on Server A:
    a. Path: D:\PSIsafe_Data\.
    b. PSIsafe Service Account: “Local System” (Default).
    c. Provide Modify Access to “SYSTEM” to the repository path.
    d. To restrict access to repositories, follow 2b-2e.
2. PSIsafe Server installed on Server A and repository located on Server B:
    a. Path: \\Server B\PSIsafe_Data\.
    b. PSIsafe Service Account: “PSIsafeSvc” (Administrator or PSIsafe dedicated user).
    c. Provide Modify Access to “PSIsafeSvc” to the repository path.
    d. Provide Modify Access to “PSIsafeSvc” to the PSIsafe Server Install directory.
    e. Provide Modify Access to “PSIsafeSvc” to the distribution\batch sync directory.

Note: It is strongly recommended that the access to the repository be limited to the account operating the PSIsafe Server service.

Connectivity

Client

a. Connects to PSIsafe Server and SQL Server.
b. Uses .NET Remoting\TCP sockets for file transfer.

c. Uses TCP Socket Port 11000.

d. Uses Remoting Port 8993 for Channel type “HTTP”.

e. Uses Remoting Port 8994 for channel type “TCP”.

f. Requires PSIsafe Server IP address configured to connect

g. Requires PSIsafe Server Services running to connect

h. Management requires MSDTC enabled (See Appendix A)

Server

a. Connects to SQL Server.

b. Handles file transfer request from client to and from repository.

It may be necessary to configure exceptions in Advanced Windows Firewall settings to exclude the following for connectivity for most Windows operating systems.

- Cabinet Ports 8994, 8993 and 11000.
- SQL TCP Port 1433.
- SQL UDP Port 1434.
- SQL server instance.

Deployment

Deployment involves the following:

1. Prerequisites (If necessary):
    a. .NET Framework.
    b. SQL Database.
    c. Create SQL account for Cabinet if using SQL Authentication.
    d. Create Windows Active Directory account for PSIsafe if using dedicated user to run PSIsafe services.
2. Server Install:
    a. Done using Deployment Wizard.
    b. Auto registered for ten (10) days.
3. Client Install:
    a. Can be done manually on each machine or through a push using group policy.

b. If done manually, PSIsafe Server Address should be configured for each machine. If pushed through group policy refer to Appendix B.

4. Registration
    a. Information required for registration:
        i. Cabinet Server IP Address.
        ii. SQL Server Instance.
        iii. SQL Database Name (Default: CNG_Main).
        iv. Type of Authentication.
        v. Registration key.
5. PSIsafe configuration using PSIsafe Management
    a. Users.
    b. Repository.
    c. Cabinets.
    d. Rights.
    e. Templates.
    f. Others.

Updating PSIsafe Server and Client

The update is applied to the PSIsafe Server. On next Client login, the update version is detected and applied locally.

- To update to latest PSIsafe version on PSIsafe Server:
    - Download update file from PSIGEN support site to the PSIsafe Server being upgraded.
    - Run “Server Update Executable”.
- Update workstations to current version:
    - Login to PSIsafe from workstation.
    - Update is detected.
    - Follow the default update instructions.
- If the PSIsafe user does not have modify access to Client installation directory, then group policy can be used to uninstall and reinstall the client.

Utilizing the PSIsafe APIs

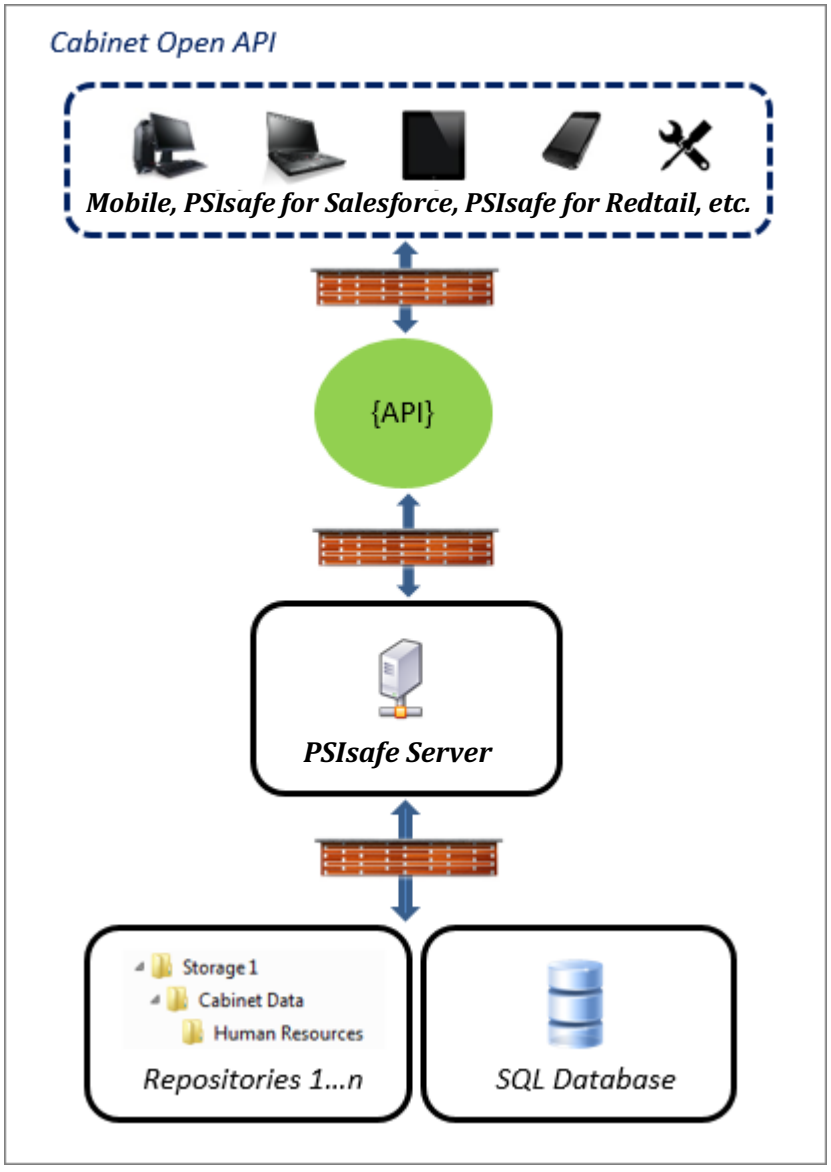
Currently, PSIsafe offers two varieties of the PSIsafe Application Programming Interfaces (APIs): **PSIsafe Windows API** (32-bit) and **PSIsafe Open API** (64-bit).

PSIsafe Windows API (32-bit)

The PSIsafe Windows API can be used programmatically to integrate Windows based programs to PSIsafe. It provides a set of functions to which developers can perform tasks such as filing external documents into PSIsafe or open a PSIsafe folder in a custom windows application. The API is written using .NET Framework.

PSIsafe Open API (64-bit)

The PSIsafe Open API is a REST compliant web service. The Open API allows communication with PSIsafe over the Internet using open standards. All data transmission between the target application and the PSIsafe Open API is performed using the JSON open standards format. The Open API does not require a specific development language or development environment. For .NET users, a Portable Class Library (PCL) which sits on top of the PSIsafe Open API is available.



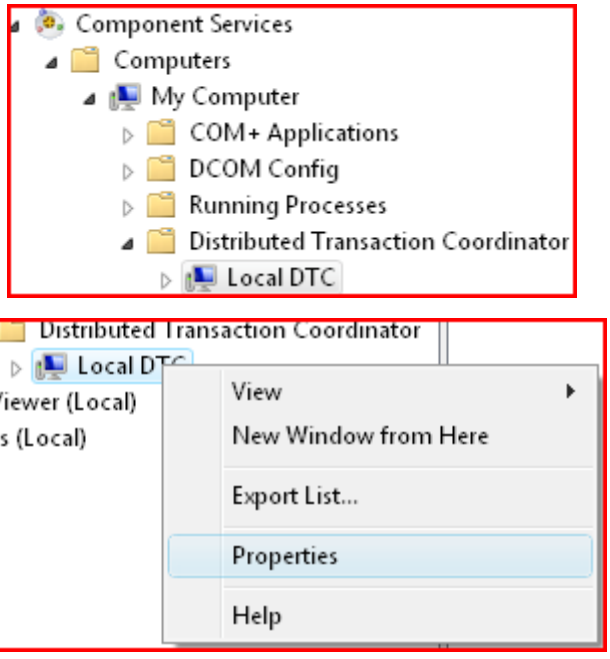
Appendix A: Microsoft Distributed Transaction Coordinator (MSDTC)

Overview

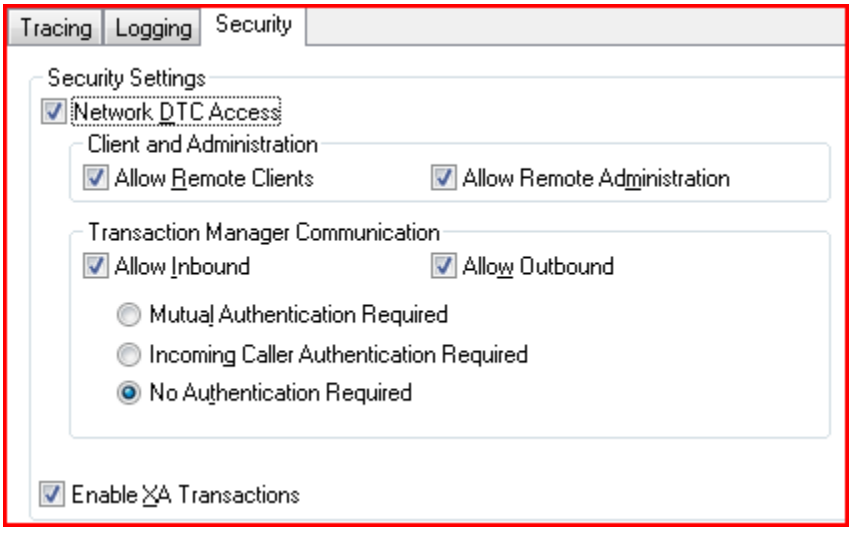
Distributed Transactions are used in PSIsafe Management. These require Transaction Managers (TM). On a Windows platform it is MSDTC. To enable PSIsafe Management functionality, MSDTC has to be configured on the PSIsafe Server and SQL Server (If different from PSIsafe Server).

Settings

1. Click on START: Type *comexp.msc* and Press ENTER
2. Select Component Services, Drill down to Local DTC, right-click and select Properties.



3. Check the following settings under the Security tab:



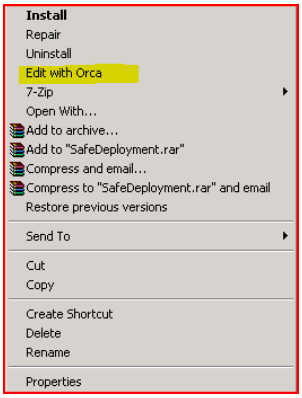
Appendix B: Transform File for Client Deployment

The IP Address or fully qualified domain name to the PSIsafe Server has to be set at all client workstations. Microsoft Group Policies may also be leveraged to reduce effort during deployment and configuration. The policy can be used to push the deployment file out along with a transform file that is created with the PSIsafe Server address.

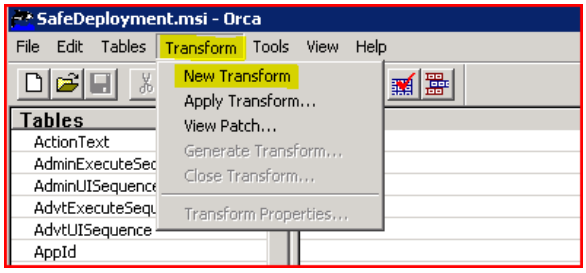
- NOTE: This requires ORCA – An MSI file editor.
- MSDN Page about ORCA: http://msdn.microsoft.com/en-us/library/aa370557(v=vs.85).aspx

Configuring a Client Transform File for Group Policy

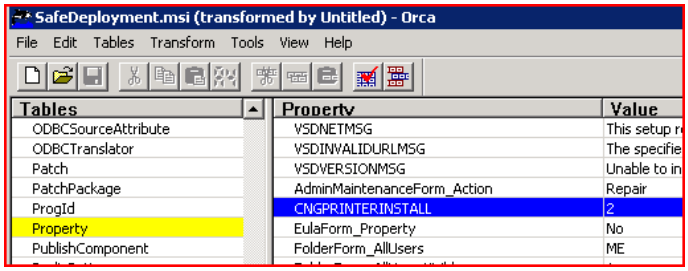
1. Make a Copy of SafeDeployment.msi.
2. Edit this file using ORCA.



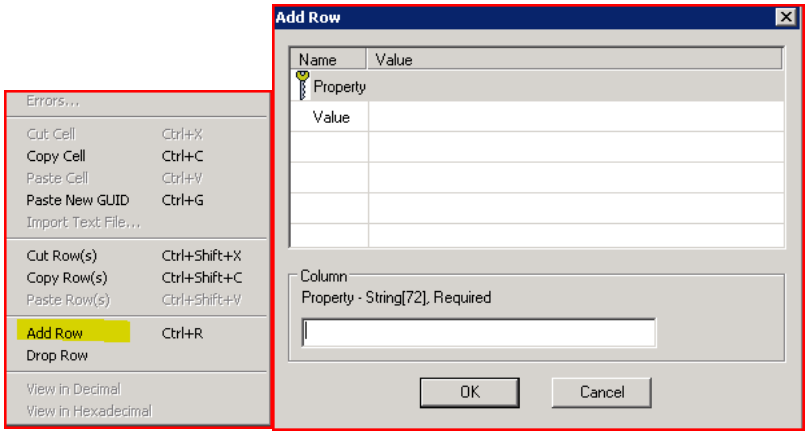
3. In menu, Click on “Transform > New Transform..”.



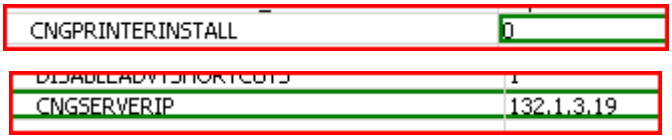
4. Now, select “Property” item on the left column.

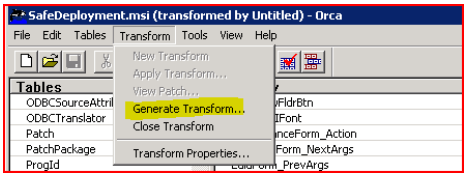


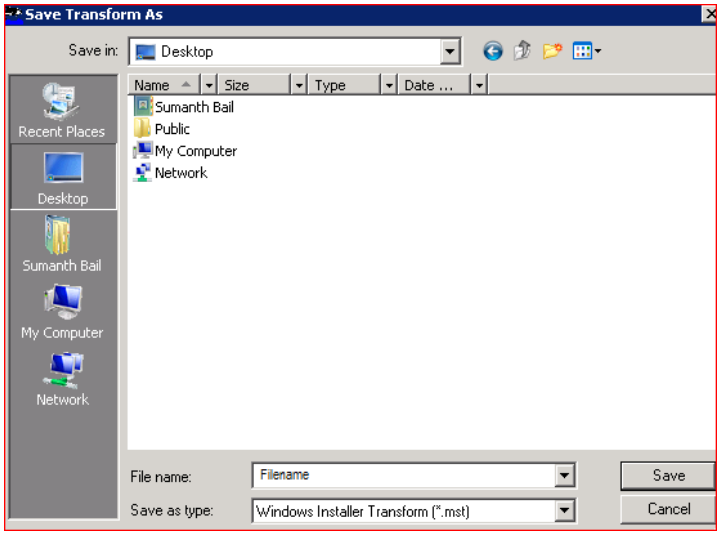
5. To not install the PSIsafe Printer, modify the following entry.
6. Set CNGPrinterInstall = 0 (No install of printer).
7. Property: CNGPRINTERINSTALL.
8. Value: 0.
9. Then, right-click, select “Add Row”.



10. Set the following values.
11. Property: CNGSERVERIP.
12. Value: 132.1.3.19 *(note: the value is the IP of the PSIsafe Server).*







13. This transform file can be used to push using group policy.